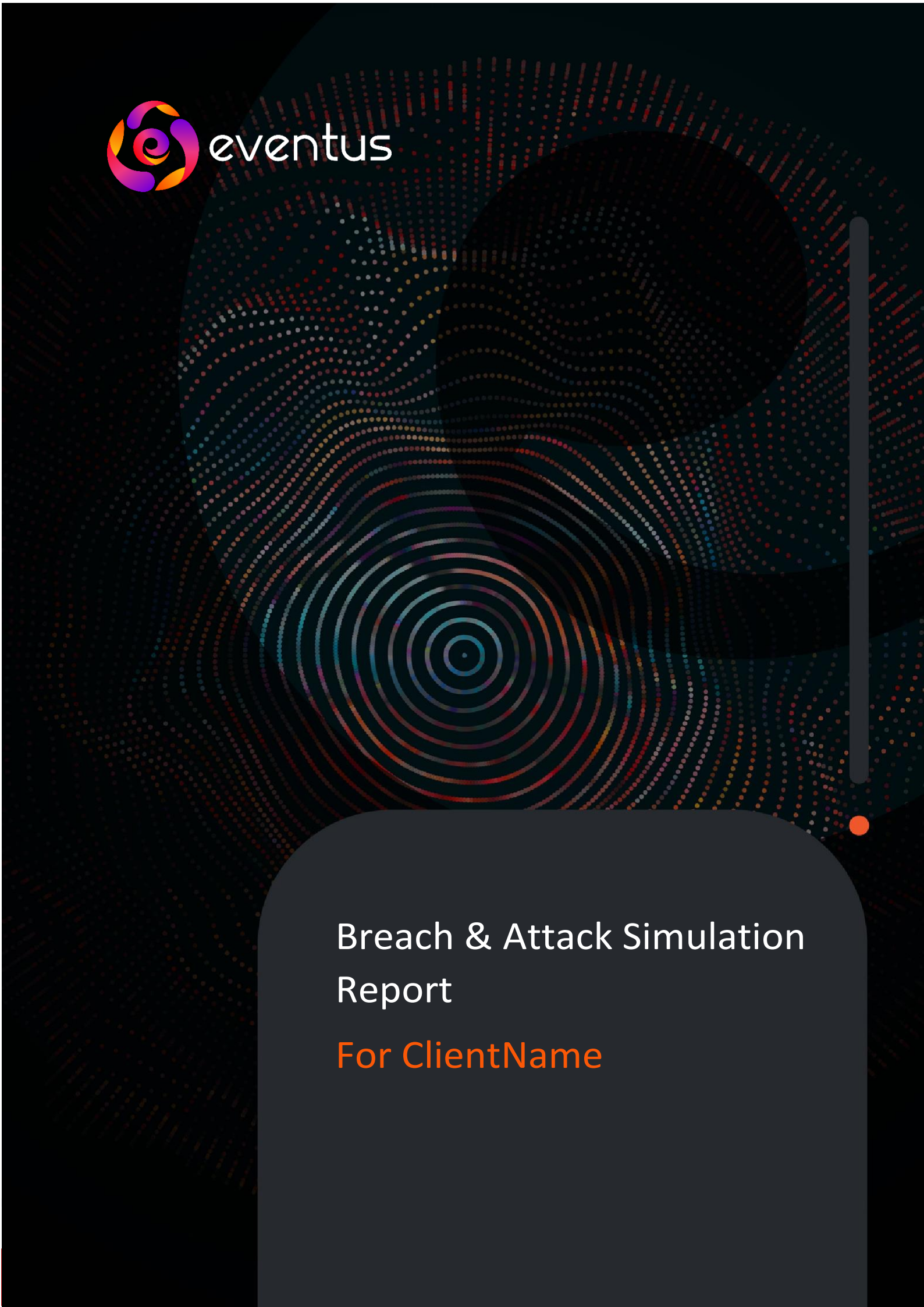


Breach & Attack Simulation Report

For ClientName

About Eventus

We are pleased to introduce ourselves as

"Your Customer Success Partner in Cyber Security."

Established in the year 2017, we are team of highly skilled professionals who deliver excellence in next generation cyber security services and custom-tailored solutions for your enterprises by defining proof of value and measuring it continuously to achieve customer success.

At Eventus the delivery team has certifications from Offensive Security, AWS, Google, Fortinet, Trend Micro, EC-Council, ISACA, ISC2, ISO. This provides and assurance of provision of the services with high quality and in-accordance with the industry standards.

Eventus is also empanelled by CERT-In for providing information Security Auditing Service.

Below is "Our Engagement Model":

Cyber Resilience: Red Teaming, Breach Attack Simulation, Adversary Services, Penetration Testing, OSINT, Application Security, Cloud Security, DevSecOps practices

Cyber Defense: Powered by Trend Micro SIEM and SOAR platform delivering 24x7 Monitoring, Deep Analysis, Incident Response, Threat Hunting, Threat intelligence, Custom playbooks and incident lifecycle support and Digital Forensics. We also provide Managed XDR Services.

Customer Success: Proactive Health assessment, Solution Effectiveness, Migration and Deployment services, Customer enablement, Cloud Posture Assessment, Security Maturity Assessment

At Eventus Security, we deliver a comprehensive engagement model for cyber security which starts with helping enterprise to assess the effectiveness of existing cyber security solutions and identifying the gap. We provide services out customers' needs to go beyond cyber security to become cyber resilient, helping clients to identify, prioritize, emulate and eliminate threats more effectively and at more advanced levels.

We thank you for considering our security services and requesting a proposal. We look forward to extending the expertise of our passionate, world-class professionals to achieve your security objectives.

Maturity Model

Below are the assessment types which can enterprise or organization can opt to understand the current security posture. The assessment types are in increasing order where Adversary emulation offers full in depth understanding of the resiliency of the enterprise and vulnerability scanning acts as the enablement to understand the security posture.

With more refine tuning the assessment type Over the time of evolution the assessment type has been clubbed into Red Team Exercise which includes vulnerability assessment, penetration testing and adversary emulation. These whole assessment types fit into the **continuous evaluation** phase of red teaming exercise.

Vulnerability Scanning: In this assessment the goal is to identify known vulnerabilities on target systems and applications.

Penetration Testing: Penetration Testing goes a step further and exploits the vulnerabilities identified. This is the main differentiator from vulnerability assessment where vulnerabilities are only being verified. Penetration Testing involves exploiting vulnerabilities under controlled circumstances.

Adversary Emulation: Adversary emulation is a type of ethical hacking engagement where a Red Team imitates how an attacker operates, leveraging frameworks like MITRE ATT&CK to identify specific tactics, techniques, and procedures (TTPs) that a real threat actor might use against an organization. Rather than focusing on attacks less likely to occur, these engagements draw upon Cyber Threat Intelligence to identify adversaries with the intent, opportunity, and capability to attack.

Document Details

This report remains the property of Eventus Security and should not be redistributed outside the organization without the explicit permission of the Information Security Testing team.

Document History

Below table outlines the version history of the document.

Version	Date	Author	Remark
0.1	02/08/2023	Pravin Singh	Document Creation (Draft)
0.2	03/08/2023	Jay Thakker	Review Comments
1.0	04/08/2023	Pravin Singh	Document Release

Table of Contents

Project Summary

Eventus Security Team has been presented with a requirement to undertake a Breach Attack Simulation for Client.

The scope of this exercise was to perform Internal Breach Attack Simulation. The overall activity aimed to determine the resiliency of the implemented security solutions and identify the gaps so as the security solutions can be fine-tuned, and awareness can be made to prevent the organization from real world threat actors.

A total of **17** campaigns were executed for endpoint, Network & Data exfiltration considering the threat profile of the client and industry client operates into. The security solutions have prevented all **7** campaigns.

Note: Tests and actions are conducted under controlled conditions: tests that could have a high probability of causing disruption to systems and services are excluded.

Technical Findings

Breach & Attack Simulation leverages the post threat Intelligence phases of the MITRE ATT&CK framework which is used to determine the robustness of the organization's defenses. To perform this activity, 4 campaigns were selected to execute on the endpoint. The endpoint was protected with <OEM> security solution.

Endpoint Simulation Summary

1. BlackByte Ransomware Campaign 2021

BlackByte ransomware was first publicly identified in July 2021. Besides spreading via a JScript file, BlackByte operators gain initial access by exploiting the Proxy Shell vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) present on the Microsoft Exchange server in some cases. After successfully exploiting the victim, the ransomware uses Cobalt Strike beacons to allow more functionality like credential dumping, remote connection, and worming. The group has so far attacked companies in the manufacturing, mining, food, beverage, healthcare, and construction sectors from different countries.

#	Actions	Tactic ID	Description	Action
1	Execute .NET Dll via Modified DotNetToJScript	T1218	In this action, a .NET Dll is executed from a JScript file by using a modified version of DotNetToJScript technique.	Blocked
2	Shellcode Injection on wuauclt.exe via Early Bird APC Queue Code Injection	T1055	In this action, a shellcode is injected into the wuauclt.exe process by using the Early Bird APC Queue Code Injection technique.	Not Blocked
3	Create a Mutex for BlackByte Ransomware via Powershell Command	T1543	In this action, malware creates a mutex named {1f07524d-fb13-4d5e-8e5c-c3373860df25}.	Not Blocked
4	Gather System Language via Powershell	T1082	In this action, an attacker is trying to gather system language via GET-WinSystemLocale command	Not Blocked
5	Registry Modification for BlackByte Ransomware Propagation	T1112	In this action, some registry modifications are made to elevate local privilege, connect mapped drives, enable long paths for the preparation of BlackByte Ransomware propagation.	Blocked
6	Delete Shadow Copy via WMI Objects	T1490	In this action, shadow copies are deleted via WMI objects	Blocked
7	Encrypt a File via BlackByte Encryptor	T1486	In this action, an attacker is trying to encrypt a file via the encryptor of the BlackByte ransomware.	Blocked
8	Write a File that Contains BlackByte Ransom Note and Open It	T1491	In this action, BlackByte ransomware is trying to write a file in TMP to inform the victim and open it using notepad.exe.	Not Blocked
Overall Campaign Result				Blocked

Below output is showing the actions which are not blocked:

Action 1: Shellcode Injection on wuauclt.exe via Early Bird APC Queue Code Injection

Command 1: cmd.exe /c "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\BlackBytePI.exe"

Command 2: cmd.exe /c timeout 5 && tasklist /svc | findstr /i notepad

Terminal Output:

```
Waiting for 5 seconds, press a key to continue ...43210
notepad.exe                  3792 N/A
```

Prevention: This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly.

Reference link: https://attack.mitre.org/techniques/T1055/

Action 2: Create a Mutex for BlackByte Ransomware via Powershell Command

Command 1: powershell.exe -c "$mtx = New-Object System.Threading.Mutex($false, '{1f07524d-fb13-4d5e-8e5c-c3373860df25} '); $mtx.Dispose();"

Prevention: This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Reference link: https://attack.mitre.org/techniques/T1543/

Action 3: Gather System Language via Powershell

Command 1: powershell.exe -c "GET-WinSystemLocale"

Terminal Output:

```
LCID             Name           DisplayName
----             ----           -----------
1033             en-US          English (United States)
```

Prevention: Execution Guardrails likely should not be mitigated with preventative controls because it may protect unintended targets from being compromised. If targeted, efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior if compromised.

Reference link: https://attack.mitre.org/techniques/T1480/

Action 4: Write a File that Contains BlackByte Ransom Note and Open It

Command 1: cmd.exe /c notepad.exe "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\BlackByteRestore.txt"

Prevention: Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data.[1] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

Reference link: https://attack.mitre.org/techniques/T1491/

2. BlackCat Ransomware Campaign 2022

The BlackCat ransomware, also known as ALPHV, is a prevalent threat and a prime example of the growing ransomware-as-a-service (RaaS) gig economy. First observed in November 2021, BlackCat initially made headlines because it was one of the first ransomware families written in the Rust programming language. By using a modern language for its payload, this ransomware attempts to evade detection, especially by conventional security solutions that might still be catching up in their ability to analyze and parse binaries written in such language. BlackCat can also target multiple devices and operating systems.

#	Actions	Tactic ID	Description	Action
1	Create Scheduled Task by using Alternate Data Streams (ADS)	T1053	In this action, an attacker is trying to create a scheduled task by using Alternate Data Streams (ADS).	**Blocked**
2	Execute Commands by using Image File Execution Options	T1546	In this action, the attacker is trying to execute commands by using the Image File Execution Options technique.	**Blocked**
3	Add a Local Admin Account	T1136	In this action, added an account as a local admin. Also, it added to the administrators group.	**Blocked**
4	Gather Information about Target Domain using ADRecon	T1018	In this action, an attacker is trying together information about the target domain by using ADRecon tool.	**Not Blocked**
5	Display the UUID of Device over WMI	T1082	In this action, the attacker tries to display the UUID of the device over WMI.	**Not Blocked**
6	Increase the Number of Outstanding Requests Allowed via Registry	T1112	In this action, an attacker is trying to increase the number of outstanding requests allowed (for example, SMB requests when distributing ransomware via its PsExec methodology).	**Not Tested**
7	Delete Shadow Copy by using Vssadmin Variant-2	T1490	In this action, shadow copy is deleted by using Vssadmin command of Windows.	**Not Tested**
8	Delete Shadow Copy via WMI Objects	T1490	In this action, shadow copies are deleted via WMI objects.	**Not Tested**
9	Clear All Event Logs Variant-2	T1070	In this action, an attacker is trying to clear all event logs in the victim system.	**Not Tested**
10	Encrypt a File (dummy.txt) using Encryptor.exe	T1486	In this action, an encryptor.exe encrypts a text file using AES.	**Not Tested**

11	Write a File that Contains BlackCat Ransom Note and Open It	T1491	In this action, BlackCat ransomware is trying to write a file in TMP to inform the victim and open it using notepad.exe.	**Not Tested**
12	Dump Lsass Process Memory by using Procdump	T1003	In this action, an attacker is trying to dump lsass by using Ms internal tool procdump	**Blocked**
13	Enable WDigest Authentication via Registry	T1112	In this action, an attacker is trying to enable WDigest Authentication via registry to enforce the storage of credentials in plaintext on future logins.	**Blocked**
Overall Campaign Result				**Blocked**

Below output is showing the actions which are not blocked:

Action 1: Gather Information about Target Domain using ADRecon.

Command 1: powershell.exe -c "$ep=Get-ExecutionPolicy;If ($ep -ne 'Unrestricted') {Set-ExecutionPolicy Unrestricted -scope CurrentUser -Force}; Get-ExecutionPolicy"

Terminal output:

```
Unrestricted
```

Command 2: powershell.exe -c Unblock-File 'C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\ADRecon.ps1'; & 'C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\ADRecon.ps1'; & dir 'C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\ADRecon*'

Terminal output:

```
At C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\ADRecon.ps1:1 char:1
+ <#
+ ~~
This script contains malicious content and has been blocked by your antivirus soft
    + CategoryInfo          : ParserError: (:) [], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1018/

Action 2: Display the UUID of Device over WMI

Command 1: cmd.exe /c wmic csproduct get UUID

Terminal output:

```
UUID

EC281BA1-8821-BCCB-6AC7-B4D984F2C4BD
```

Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about the operating system and underlying hardware, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1082/

3. Play Ransomware Campaign 2022

Play (aka PlayCrypt) is a ransomware group that emerged in June 2022 and specifically targets organizations in the Latin America. Organizations in Hungary, India, Netherlands and Spain also experienced Play attacks. Play ransomware traverses the files on the file system and encrypts the contents of files. This ransomware creates ransom note on the root directory of main drive.

#	Actions	Tactic ID	Description	Action
1	Gather Information about Target Domain and OS using Adfind	T1018	In this action, an attacker is trying together information about the target domain and OS by using Adfind.exe.	Blocked
2	List Domain Controllers using nltest	T1018	In this action, an attacker is trying to list domain controllers in the target environment by using nltest command.	Not Blocked
3	Create a Firewall Rule using Netsh	T1090	In this action, the malware uses the command cmd.exe /c netsh firewall add port opening TCP 443 "adp" and makes the victim machine function as a proxy server.	Blocked
4	Create CobaltStrike Default Named Pipes	T1106	In this action, the attacker creates a named pipe for C2 communication with the default name convention of CobaltStrike.	Blocked
5	Create a New Scheduled Task by using schtasks	T1543	In this action, the attacker is trying to create a new scheduled task.	Blocked
6	Gather Disk Information from the Target via WMIC.exe	T1082	In this action an attacker is trying to gather info from disks such as free space and size	Not Blocked
7	Execute Commands by using Winpeas Windows Privilege Escalation Tool	T1059	In this action, an attacker is trying to execute commands by using Winpeas Windows Privilege Escalation Tool.	Blocked
8	Execute BloodHound Tool's Ingestor (Invoke-BloodHound) Function Variant-2	T1087	In this action, an attacker is trying to execute Invoke-BloodHound function by using BloodHound tool's Ingestor.	Blocked
9	Gather credentials using Mimikatz (2.2.0 20220919) Tool	T1003	Mimikatz is a credential dumper tool capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.	Blocked
10	Dump Address Space of lsass.exe via Procdump	T1003	In this action, Procdump is used to dump the memory of the LSASS.exe process. Dump of this process can be used for credential dumping by the attacker.	Blocked
11	Perform Kerberoasting Attack by using Rubeus Tool (SigFlip)	T1558	In this action, an attacker is trying to execute the Kerberoasting attack by using Rubeus post-exploitation tool.	Blocked
12	Execute a Command by using the PsExec	T1021	In this action, an attacker is trying to execute a command on a machine by using the PsExec.	Blocked
13	Write a File that Contains Play Ransom Note and Open It	T1491	In this action, Play ransomware is trying to write a file in C drive to inform the victim and open it using notepad.exe.	Blocked

Overall Campaign Result	Blocked

Below output is showing the actions which are not blocked:

Action 1: List Domain Controllers using nltest

Command 1: cmd.exe /c nltest /dclist:

Terminal output:

```
The command completed successfully
Cannot find DC to get DC list from.Status = 1355 0x54b ERROR_NO_SUCH_DOMAIN
```

Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1018/

Action 2: Gather Disk Information from the Target via WMIC.exe

Command 1: wmic.exe logicaldisk get size,freespace,caption

Terminal Output:

```
Caption  FreeSpace    Size

C:       64785076224  107372081152
```

Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about the operating system and underlying hardware, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1082/

4. Emotet Ransomware Campaign 2022

Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. In June 2022, a threat actor was observed gaining access to an environment via Emotet and operating for an eight-day period. During this activity, it was observed that they installed their malware via shortcuts with LNK extension, collected information in the system with the ADFind tool, and remained in the system through the registry.

#	Actions	Tactic ID	Descriptions	Action
1	Display a List of Domain Computers Using "net" Command	T1018	In this action, an attacker is trying to list the computers registered to the domain by making a group query.	Blocked
2	List Domain Admins using Net Utility	T1069	In this action, the attacker is trying to list Domain Admins in the target environment by using net utility.	Blocked
3	Gather Trusted Domains via Nltest Command Variant-2	T1482	In this action, an attacker is trying to gather information on domain trusts with nltest command	Blocked
4	Display the Groups using "whoami"	T1033	In this action, an attacker is trying to display groups and the current user information	Not Blocked
5	List Domain Controllers using nltest	T1018	In this action, an attacker is trying to list domain controllers in the target environment by using nltest command.	Not Blocked
6	Display a List of Enterprise Admins Using "net" Command	T1018	In this action, an attacker is trying to list the names of users belonging to the Enterprise Admins group.	Blocked
7	Gather Information about Target Domain using Adfind.bat	T1018	In this action, an attacker is trying together information about the target domain by using Adfind.exe script.	Blocked
8	Display all current TCP/IP network configuration using "ipconfig /all"	T1016	"ipconfig" displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.	Not Blocked
9	Check Zerologon Vulnerability via SharpZeroLogon Tool	T1210	In this action, The attacker is trying to exploit Zerologon (CVE-2020-1472) vulnerability in order to acquire Domain Admin privileges by using the SharpZeroLogon tool.	Blocked
10	Execute Shellcode Loader DLL using rundll32.exe	T1218	In this action, an attacker is trying to execute a loader DLL generated by ScareCrow in order to execute embedded shellcode.	Not Blocked
11	Create a new registry key "ServiceDll" in HKLM hive	T1112	In this action, Reg.exe command-line utility creates a new registry key in HKLM hive for persistence.	Blocked
12	Encrypt All the Files and Leave a Ransom Note	T1059	In this action, an attacker is trying to encrypt all the files. Then left a ransom note to the folder.	Not Blocked
13	Write a File that Contains Emotet Ransom Note and Open It	T1491	In this action, Emotet ransomware is trying to write a file in C drive to inform the victim and open it using explorer.exe.	Blocked
14	Execute a DLL via Rundll32 over LNK File	T1566	In this action, an attacker is trying to execute a dll via Rundll32.exe over a malicious shorcut (.LNK) file.	Not Blocked

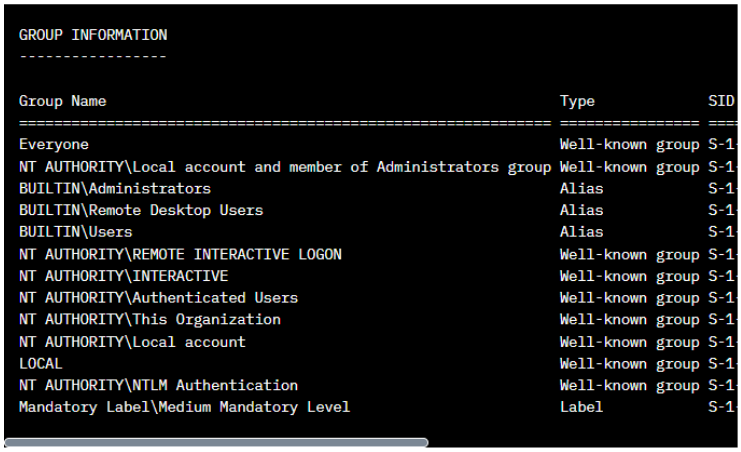
Overall Campaign Result	Blocked

Below output is showing the actions which are not blocked:

Action 1: Display the Groups using "whoami"

Command 1: cmd.exe /c whoami /groups

Terminal output:



Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about system users, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1033/

Action 2: List Domain Controllers using nltest

Command 1: cmd.exe /c nltest /dclist:

Terminal output:

Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information on remotely available systems, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1018/

Action 3: Display all current TCP/IP network configuration using "ipconfig /all"

Command 1: cmd.exe /c ipconfig /all

Terminal output:

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : BAS-SEC-SRV
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Peer-Peer
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ap-south-1.ec2-utilities.amazonaws.com
                                       us-east-1.ec2-utilities.amazonaws.com
                                       ec2.internal
                                       bhfl-mgmtaws.com

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : bhfl-mgmtaws.com
   Description . . . . . . . . . . . : AWS PV Network Device #0
   Physical Address. . . . . . . . . : 02-E8-56-B4-33-9E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.31.7.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, May 11, 2023 8:01:33 AM
   Lease Expires . . . . . . . . . . : Thursday, May 11, 2023 11:01:35 AM
   Default Gateway . . . . . . . . . : 10.31.7.1
   DHCP Server . . . . . . . . . . . : 10.31.7.1
   DNS Servers . . . . . . . . . . . : 10.31.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about a system's network configuration, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate

Reference link: https://attack.mitre.org/techniques/T1016/

Action 4: Execute Shellcode Loader DLL using rundll32.exe

Command 1: cmd.exe /c rundll32.exe "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\sspiclli.dll",Start & timeout 5 & tasklist /svc | findstr /i notepad

Terminal output:

```
Waiting for 5 seconds, press a key to continue ...□4□3□2□1□0
notepad.exe                  6300 N/A
```

Prevention: Certainly, signed binaries that can be used to execute other programs may not be necessary within a given environment. Use application whitelisting configured to block execution of these scripts if they are not required for a given system or network to prevent potential misuse by adversaries.

Reference link: https://attack.mitre.org/techniques/T1218/

Action 5: Encrypt All the Files and Leave a Ransom Note

Command 1: C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\encryptor.exe /E 357033.rtf /AES

Terminal output:

```
C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\357033.rtf is encrypted.
SUCCESS: Bye! :-)
```

Command 2: C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\encryptor.exe /E "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\112895.txt" /AES

Terminal output:

```
C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\112895.txt is encrypted.
SUCCESS: Bye! :-)
```

Command 3: cmd.exe /c echo "Hello this is a ransom note!" >> "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\assasin.bmp"

Prevention: Audit and/or block command-line interpreters by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1059/

Action 6: Execute a DLL via Rundll32 over LNK File

Command 1: cmd.exe /c cd "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2" & .\notepadSpawn.lnk

Command 2: cmd.exe /c timeout 5 && tasklist /svc | findstr /i notepad

Terminal output:

```
Waiting for 5 seconds, press a key to continue ...□4□3□2□1□0
notepad.exe                  2808 N/A
```

Prevention: Anti-virus can automatically quarantine suspicious files. Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity. Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. Users can be trained to identify social engineering techniques and phishing emails.

Reference link: https://attack.mitre.org/techniques/T1566/

5. TA505 Ransomware Campaign 2020

TA505 is a financially motivated threat group that has been active since at least 2014. This is the group behind the infamous Dridex banking trojan and Locky ransomware, delivered through malicious email campaigns via Necurs botnet.

#	Actions	Tactic ID	Descriptions	Action
1	Execute WMI commands	T1047	In this action, an attacker is trying to execute WMI commands to reconnaissance.	Not Blocked
2	Gather System Information	T1082	In this action, The Attacker is trying to gather information about the target system.	Not Blocked
3	Dump Saved Browser Credentials using Lazagne Tool	T1555	In this action, an attacker is trying to dump saved browser credentials using the Lazagne tool.	Blocked
4	Dump Saved Mail Credentials Lazagne Tool	T1555	In this action, an attacker is trying to dump saved mail credentials using the Lazagne tool.	Blocked
5	Bypass User Access Control via sdclt.exe Variant-1	T1548	In this action, an attacker is trying to bypass UAC and open a notepad from an elevated cmd by modifying registry that affects sdclt.exe.	Blocked
6	Elevate Privileges to SYSTEM by using Psgetsystem	T1134	In this action, the attacker is trying to elevate privileges to SYSTEM account by a process which already has these privileges (lsass.exe) to start a new process with the stolen token.	Blocked
7	Execute Invoke-Mimikatz (with AMSI Bypass)	T1003	In this action, an attacker is trying to execute Invoke-Mimikatz to get plaintexts passwords, hash, PIN code and kerberos tickets from memory on the machine.	Blocked
8	Create a New Registry Key for Autorun of dummy.exe Variant-1	T1547	In this action, an attacker is trying to add the dummy.exe file to autorun hive as a key (DelegateExecute) for persistence.	Not Blocked
9	Encrypt a File (encfile.txt) using Encryptor.exe Variant-2	T1486	In this action, an encryptor.exe encrypts a text file using AES.	Not Blocked
10	Copy the H1N1 Malware to USB Drive	T1091	In this action, an attacker is trying to copy a malware to the USB drive.	Blocked
Overall Campaign Result				Not Blocked

Below output is showing the actions which are not blocked:

Action 1: Execute WMI commands

Command 1: powershell.exe -c "if((Get-WmiObject -class Win32_ComputerSystem).PartOfDomain){Write-Host $((Get-WmiObject -class Win32_ComputerSystem).Domain)}else{Write-Host 'Not part of a domain'}"

Terminal output:

```
Not part of a domain
```

Command 2: powershell.exe -c "gwmi win32_group -Filter """"Domain='$env:computername' and SID='S-1-5-32-544'""""

Terminal output:

```
Caption                    Domain      Name           SID
-------                    ------      ----           ---
BAS-SEC-SRV\Administrators BAS-SEC-SRV Administrators S-1-5-32-544
```

Command 3: powershell.exe -c "$user=[Security.Principal.WindowsIdentity]::GetCurrent();$res=(New-Object Security.Principal.WindowsPrincipal $user).IsInRole([Security.Principal.WindowsBuiltinRole]::Administrator);Write-Host $res"

Terminal output:

```
False
```

Prevention: Disabling WMI or RPCS may cause system instability and should be evaluated to assess the impact to a network. By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI. Prevent credential overlap across systems of administrator and privileged accounts.

Reference link: https://attack.mitre.org/techniques/T1047/

Action 2: Gather System Information

Command 1: cmd.exe /c systeminfo >> "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\temp.ini" && tasklist >> "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\temp.ini" && makecab "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\temp.ini" "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\temp.cab"

Terminal output:

```
Cabinet Maker - Lossless Data Compression Tool

  0.00% - temp.ini (1 of 1)
100.00% - temp.ini (1 of 1)
  0.00% [flushing current folder]
 97.22% [flushing current folder]
  0.92% [flushing current folder]
100.00% [flushing current folder]
```

Prevention: Identify unnecessary system utilities or potentially malicious software that may be used to acquire information about the operating system and underlying hardware, and audit and/or block them by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1082/

Action 3: Create a New Registry Key for Autorun of dummy.exe Variant-1

Command 1: reg.exe add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "DelegateExecute" /d "C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\dummy.exe"

Terminal output:

```
The operation completed successfully.
```

Prevention: This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Reference link: **https://attack.mitre.org/techniques/T1547/**

Action 4: Encrypt a File (encfile.txt) using Encryptor.exe Variant-2

Command 1: C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\encryptor.exe /E 112895.txt /AES

Terminal output:

```
C:\Users\Digvijay.Deshmukh\AppData\Local\Temp\2\112895.txt is encrypted.
SUCCESS: Bye! :-)
```

Prevention: Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. In some cases, the means to decrypt files affected by a ransomware campaign is released to the public. Research trusted sources for public releases of decryptor tools/keys to reverse the effects of ransomware. Identify potentially malicious software and audit and/or block it by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Reference link: https://attack.mitre.org/techniques/T1486/

Network Simulation Summary

1. Cobalt Threat Group Campaign Malware Download Threat – 2(LAN-Network)

This threat includes downloading variants of malware used in Cobalt Threat Group campaigns.

#	Actions	Description	Action
1	Trojan used in Cobalt Group APT Campaign .DOC File Download Variant-11	This attack includes downloading a .doc file of trojan used in Cobalt Group APT campaign. This trojan hooks API calls and document spawns new processes. Furthermore, it terminates other processes using taskkill program and contacts with its own C&C servers.	Blocked
2	Cobalt Trojan .EXE File Download Variant-11	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
3	Cobalt Trojan .EXE File Download Variant-12	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
4	Cobalt Trojan .EXE File Download Variant-13	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
5	Cobalt Trojan .EXE File Download Variant-14	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
6	Malware used by Cobalt Threat Group .EXE File Download Variant-15	This attack includes downloading a .exe payload of the Cobalt trojan. Cobalt opens the clipboard and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, it modifies proxy settings and it contacts with its own C&C servers.	Blocked
7	Coolpants Backdoor Malware used by Cobalt APT Group .DLL File Download Variant-1	This attack includes downloading a .dll payload file of the Coolpants Backdoor Malware of Cobalt Group which targets financial organizations. Coolpants Backdoor Malware spawns new processes and touches files in the Windows directory.	Blocked
8	ThreadKit Malware used by Cobalt Threat Group .RTF File Download Variant-1	This attack includes downloading a .rtf payload file of the ThreadKit malware used by Cobalt threat group. ThreadKit is a Microsoft Office document exploit builder kit first uncovered in October 2017. Furthermore, it queries sensitive IE security settings and contacts with its own C&C servers.	Blocked
Overall Campaign Result			Blocked

2. APT32 Threat Group Campaign Malware Download Threat – 3 (LAN-Network)

This threat includes downloading variants of malware used in APT32 Threat Group campaigns.

#	Actions	Description	Action
1	Trojan used by APT32 Threat Group .RTF File Download Variant-7	This attack includes downloading a .rtf file of the APT32 Threat Group attacks. It contains ability such as open the clipboard, retrieve keyboard strokes and it posts files to a webserver. It spawns the Microsoft Equation Editor. Also, it contacts with its own C&C servers.	Blocked
2	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-7	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	Blocked
3	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-8	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	Blocked
4	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-8	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	Blocked
5	Trojan used by APT32 Threat Group .EXE File Download Variant-8	This attack includes downloading a .exe file of the trojan used by APT32 Threat Group. The APT32 Threat Group conducts cyber espionage mainly in countries in Southeast Asia and East Asia. Furthermore, it hooks API calls and contacts with its own C&C servers.	Blocked
6	Trojan used by APT32 Threat Group .RTF File Download Variant-8	This attack includes downloading a .rtf file of the APT32 Threat Group attacks. It reads the keyboard layout followed by a significant code branch decision. It spawns the Microsoft Equation Editor.	Blocked
7	Trojan used by APT32 Threat Group .EXE File Download Variant-9	This attack includes downloading a .exe file of the APT32 Threat Group attacks. It posts files to a webserver and it reads information such as active computer name, cryptographic machine GUID. It spawns the Microsoft Equation Editor. Also, it contacts with its own C&C servers.	Blocked
8	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-9	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	Blocked
9	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-9	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	Blocked
10	Trojan used by APT32 Threat Group .EXE File Download Variant-18	This attack includes downloading a .exe file of the trojan used by APT32 Threat Group. The APT32 Threat Group conducts cyber espionage mainly in countries in Southeast Asia and East Asia. Furthermore, it hooks API calls and contacts with its own C&C servers.	Blocked

11	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-10	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	**Blocked**
12	Trojan used by APT32 Threat Group .RTF File Download Variant-10	This attack includes downloading a .rtf file of the APT32 Threat Group attacks. The group is believed to be Vietnam-based. It posts files to a webserver and it spawns the Microsoft Equation Editor. Also, it contacts with its own C&C servers.	**Blocked**
13	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-10	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	**Blocked**
14	Trojan used by APT32 Threat Group .EXE File Download Variant-10	This attack includes downloading a .exe file of the trojan used by APT32 Threat Group. The APT32 Threat Group conducts cyber espionage mainly in countries in Southeast Asia and East Asia. Furthermore, it hooks API calls and contacts with its own C&C servers.	**Blocked**
15	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-11	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	**Blocked**
16	Trojan used by APT32 Threat Group .EXE File Download Variant-11	This attack includes downloading a .exe file of the trojan used by APT32 Threat Group. The APT32 Threat Group conducts cyber espionage mainly in countries in Southeast Asia and East Asia. Furthermore, it hooks API calls and contacts with its own C&C servers.	**Blocked**
17	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-11	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	**Blocked**
18	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-12	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	**Blocked**
19	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-12	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	**Blocked**
20	Trojan used by APT32 Threat Group .EXE File Download Variant-12	This attack includes downloading a .exe file of the trojan used by APT32 Threat Group. The APT32 Threat Group conducts cyber espionage mainly in countries in Southeast Asia and East Asia. Furthermore, it hooks API calls and contacts with its own C&C servers.	**Blocked**

21	Trojan used by APT32 Threat Group .EXE File Download Variant-13	This attack includes downloading a .exe file of the trojan used by APT32 Threat Group. The APT32 Threat Group conducts cyber espionage mainly in countries in Southeast Asia and East Asia. Furthermore, it hooks API calls and contacts with its own C&C servers.	Blocked
22	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-13	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	Blocked
23	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-13	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	Blocked
24	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-14	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	Blocked
25	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-14	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	Blocked
26	Trojan used by APT32 Threat Group .EXE File Download Variant-14	This attack includes downloading a .exe file of the trojan used by APT32 Threat Group. The APT32 Threat Group conducts cyber espionage mainly in countries in Southeast Asia and East Asia. Furthermore, it hooks API calls and contacts with its own C&C servers.	Blocked
27	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-15	This attack includes downloading a .dll file of the KerrDown downloader malware used by APT32 threat group. This malware is delivered a malicious macro in a Word Document. Furthermore, this DLL retrieves a Cobalt Strike Beacon variant from a remote URL, decrypts it, and executes it in memory.	Blocked
28	Denis Backdoor Malware used by APT32 Threat Group .EXE File Download Variant-15	This attack includes downloading a .exe payload file of the Denis backdoor malware. Denis is a simple backdoor developed by the APT32 Threat Group, well-observed in-the-wild and renowned for using DNS tunneling as a transport mechanism for C2 communications.	Blocked
29	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-16	This attack includes downloading a .dll file of the KerrDown Malware Downloader used by APT32 (OceanLotus) group. This sample is designed to be executed by using the DLL Side-Loading technique with a legitimate winword.exe binary. It hooks API calls and uses Service Control Manager for execution. This sample also tries to connect to the C2 server.	Blocked
30	KerrDown Downloader Malware used by APT32 Threat Group .DLL File Download Variant-17	This attack includes downloading a .dll file of the KerrDown Malware Downloader used by APT32 (OceanLotus) group. This sample is designed to be executed by using the DLL Side-Loading technique with a legitimate GoogleUpdate.exe binary. It extracts malicious files	Blocked

		to the target system and uses scheduled tasks for persistence. This sample also tries to connect to its C2 server.	
Overall Campaign Result			**Blocked**

3. Lazarus Threat Group Campaign Malware Download Threat – 3 (LAN-Network)

This threat includes downloading variants of malware used in Lazarus Threat Group campaign.

#	Actions	Descriptions	Action
1	Dacls RAT used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .EXE payload file of the Dacls RAT used by Lazarus threat group. Dacls is a new type of remote-control software targeting both Windows and Linux environment. This attack queries kernel debugger information. It also reads the active computer name and the cryptographic machine GUID.	Blocked
2	Keymarble RAT Malware used by Lazarus Group Threat Group .EXE File Download Variant-2	This attack includes downloading an .exe payload file of the Keymarble RAT Malware used by Lazarus Group. Keymarble monitors specific registry key for changes. When executed, it de-obfuscates its application programming interfaces (APIs) and using port 443, attempts to connect to the hard-coded IP addresses.	Blocked
3	VHD Ransomware used by Lazarus Threat Group .DLL File Download Variant-2	This attack includes downloading a .dll of the VHD ransomware used by Lazarus threat group. The ransomware itself is nothing special, its written in C and crawls all connected disks to encrypt files and delete any folder called System Volume Information. The program also stops processes that could be locking important files, such as Microsoft Exchange and SQL Server.	Blocked
4	PowerRatankba Trojan Downloader Used by Lazarus Threat Group in FastCash 2.0 Campaign .EXE File Download Variant-2	This attack includes downloading a .ps1 file of PowerRatankba Trojan of Lazarus Threat Group FastCash 2.0 Campaign. Lazarus Group is a threat group likely backed by the North Korea government. It queries kernel debugger information. It reads information such as active computer name, cryptographic machine GUID. It contacts with its own C&C servers.	Blocked
5	Dtrack RAT used by Lazarus Group .EXE File Download Variant-2	This attack includes downloading a .exe file of the Dtrack RAT used by Lazarus Group. Dtrack RAT is being used to attack the financial sector and research centers in India. The malicious code is embedded into a binary of a harmless executable. This RAT is designed to be planted on victim's malware and also known as ATMDtrack. It writes data to a remote process and uses anti-debugging techniques to evade analysis.	Blocked
6	VHD Ransomware used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .exe of the VHD ransomware used by Lazarus threat group. The ransomware itself is nothing special, its written in C and crawls all connected disks to encrypt files and delete any folder called System Volume Information. The program also stops processes that could be locking important files, such as Microsoft Exchange and SQL Server.	Blocked
7	Dropper used by Lazarus Threat Group in .HWP File Download Variant-2	This attack includes downloading a .HWP dropper file used by Lazarus Threat Group. The Lazarus Threat Group has been observed making targeted attacks on security researchers and journalists. The group is known for historically targeting individuals	Not Blocked

		of interest to the North Korean regime; including journalists, diplomats, and government employees. This sample drops malicious vbs file in order to download the main malicious executable.	
8	HOPLIGHT Trojan used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading an .exe file of the HOPLIGHT Trojan used by Lazarus Group Threat Group. This malware sends traffic on typical HTTP outbound port, but without HTTP header, contains ability to enumerate processes/modules/threads. Furthermore, it contacts with its own C&C servers.	Blocked
9	MagicRAT RAT used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading an .EXE file of the MagicRAT RAT used by Lazarus threat group. MagicRAT is a remote access trojan (RAT) that programmed in C plus plus programming language and uses the Qt Framework to make human analysis harder. This RAT was found on victims that had been initially compromised through the exploitation of publicly exposed VMware Horizon platforms.	Blocked
10	Trojan used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .EXE dropper file used by Lazarus Threat Group. The Lazarus Threat Group has been observed making targeted attacks on security researchers and journalists. The group is known for historically targeting individuals of interest to the North Korean regime; including journalists, diplomats, and government employees. This is the main malicious executable to compromise the target system.	Blocked
11	TigerRAT RAT used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading an .EXE file of the TigerRAT RAT used by Lazarus threat group. TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of Operation ByteTiger. This implant consists of several RAT capabilities such as gathering system information and run arbitrary commands on the endpoint.	Blocked
12	Malware used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .exe of the trojan used by Lazarus threat group. This trojan modifies auto-execute functionality by setting/creating a value in the registry and reads the active computer name. Furthermore, this malicious file contacts with its own C&C servers.	Blocked
13	Lazarus Group's Trojan .DLL File Download Variant-2	This attack includes downloading a .DLL payload file of the Lazarus Group Trojan which spawns new processes and posts files to a web server. Also, it contacts with its own C&C servers.	Blocked
14	Malware used by Lazarus Threat Group .MACHO File Download Variant-2	This attack includes downloading a .macho of the malware used by Lazarus threat group. The campaign has been using lures for attractive job offers since at least 2020, but this year novel macOS malware was discovered with embedded PDF documents advertising jobs vacancies and attempting to masquerade as legitimate processes with names such as wifianalyticsagent and safarifontsagent. This multi-stage malware first installs a LaunchAgent for persistence in the users local folder, obviating the	Blocked

		need for further permissions, although on macOS Ventura that does now at least raise an alert notification. The second stage in the Crypto.com variant is a bare-bones application bundle named WifiAnalyticsServ.app (FinderFontsUpdater.app in the Coinbase variant). with the bundle identifier finder.fonts.extractor. The second-stage extracts and executes a third-stage binary, wifianalyticsagent, which serves as a downloader for an unretrieved fourth stage from a C2 at market.	
15	BankShot Trojan Used by Lazarus Group APT Campaign .EXE File Download Variant-3	This attack includes downloading an .exe file of BankShot Trojan of Lazarus Group APT Campaign. It reads terminal service related keys, and It possibly checks for the presence of an Antivirus engine	**Blocked**
16	Malware used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading a .exe of the trojan used by Lazarus threat group. This trojan modifies auto-execute functionality by setting/creating a value in the registry and reads the active computer name. Furthermore, this malicious file contacts with its own C&C servers.	**Blocked**
17	VHD Ransomware used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading a .exe of the VHD ransomware used by Lazarus threat group. The ransomware itself is nothing special, its written in C and crawls all connected disks to encrypt files and delete any folder called System Volume Information. The program also stops processes that could be locking important files, such as Microsoft Exchange and SQL Server.	**Blocked**
18	Dtrack RAT used by Lazarus Group .EXE File Download Variant-3	This attack includes downloading a .exe file of the Dtrack RAT used by Lazarus Group. Dtrack RAT is being used to attack the financial sector and research centers in India. The malicious code is embedded into a binary of a harmless executable. This RAT is designed to be planted on victim's malware and also known as ATMDtrack. It writes data to a remote process and uses anti-debugging techniques to evade analysis. The malware also posts data to a webserver.	**Blocked**
19	MagicRAT RAT used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading an .EXE file of the MagicRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). MagicRAT is a remote access trojan (RAT) that programmed in C plus plus programming language and uses the Qt Framework to make human analysis harder. This RAT was found on victims that had been initially compromised through the exploitation of publicly exposed VMware Horizon platforms.	**Blocked**
20	RAT Malware used by Lazarus Threat Group .DOCX File Download Variant-3	This attack includes downloading a .DOCX file of the RAT Malware used by Lazarus Threat Group. Its been used template injection technique in these methods while malicious documents operating. The first methods template contains VBA RAT that performs following actions; collects victims info, identifies the AV product	**Blocked**

		running on a victims machine, executes shell-codes, deletes files, uploads and downloads files, reads disk and file systems information. The second methods template is an exploit for CVE-2021-26411 which is trying to execute a shell-code to use same VBA RAT.	
21	HOPLIGHT Trojan used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading an .exe file of the HOPLIGHT Trojan used by Lazarus Group Threat Group. This malware sends traffic on typical HTTP outbound port, but without HTTP header, contains ability to enumerate processes/modules/threads. Furthermore, it contacts with its own C&C servers.	**Blocked**
22	Malware used by Lazarus Threat Group .MACHO File Download Variant-3	This attack includes downloading a .macho of the malware used by Lazarus threat group. The campaign has been using lures for attractive job offers since at least 2020, but this year novel macOS malware was discovered with embedded PDF documents advertising jobs vacancies and attempting to masquerade as legitimate processes with names such as wifianalyticsagent and safarifontsagent. This multi-stage malware first installs a LaunchAgent for persistence in the users local folder, obviating the need for further permissions, although on macOS Ventura that does now at least raise an alert notification. The second stage in the Crypto.com variant is a bare-bones application bundle named WifiAnalyticsServ.app (FinderFontsUpdater.app in the Coinbase variant). with the bundle identifier finder.fonts.extractor. The second-stage extracts and executes a third-stage binary, wifianalyticsagent, which serves as a downloader for an unretrieved fourth stage from a C2 at market.	**Not Blocked**
23	TigerRAT RAT used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading an .EXE file of the TigerRAT RAT used by Lazarus threat group. TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of Operation ByteTiger. This implant consists of several RAT capabilities such as gathering system information and run arbitrary commands on the endpoint.	**Blocked**
24	Copperhedge Backdoor used by Lazarus Group Threat Group .DLL File Download Variant-3	This attack includes downloading a .DLL file of the Copperhedge Malware used by Lazarus Group Threat Group. It writes data to a remote process and tries to sleep for a long time (more than two minutes) to bypass virtual machines.	**Blocked**
25	Hermes Ransomware used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading a .exe of the Hermes ransomware used by Lazarus threat group. The Hermes ransomware tries to delete registry keys using reg.exe and collects the piece of information about of the victim such as cryptographic machine GUID, windows installation date, windows installation language etc and encrypts victim's files.	**Blocked**
26	TigerRAT RAT used by Lazarus Threat Group	This attack includes downloading an .EXE file of the TigerRAT RAT used by Lazarus threat group. TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of Operation ByteTiger. This	**Blocked**

	.EXE File Download Variant-4	implant consists of several RAT capabilities such as gathering system information and run arbitrary commands on the endpoint.	
27	HOPLIGHT Trojan used by Lazarus Threat Group .EXE File Download Variant-4	This attack includes downloading an .exe file of the HOPLIGHT Trojan used by Lazarus Group Threat Group. This malware sends traffic on typical HTTP outbound port, but without HTTP header, contains ability to enumerate processes/modules/threads. Furthermore, it contacts with its own C&C servers.	**Blocked**
28	BankShot Trojan Used by Lazarus Group APT Campaign .DLL File Download Variant-4	This attack includes downloading a .dll file of BankShot Trojan of Lazarus Group APT Campaign. It spawns new processes.	**Blocked**
29	Hermes Ransomware used by Lazarus Threat Group .EXE File Download Variant-4	This attack includes downloading a .exe of the Hermes ransomware used by Lazarus threat group. The Hermes ransomware tries to delete registry keys using reg.exe and collects the piece of information about of the victim such as cryptographic machine GUID, windows installation date, windows installation language etc and encrypts victim's files.	**Blocked**
30	Copperhedge Backdoor used by Lazarus Group Threat Group .DLL File Download Variant-4	This attack includes downloading a .DLL file of the Copperhedge Malware used by Lazarus Group Threat Group. It posts files to a webserver, writes data to a remote process and contacts three domains and a host.	**Blocked**
31	Malware used by Lazarus (Hidden Cobra) Group .EXE File Download Variant-4	This attack includes downloading an .EXE file of the trojan used by Lazarus Threat Group. This sample spawns new malicious processes and uses rundll32 technique for execution. It also drops files to the target system and hooks other running processes.	**Blocked**
Overall Campaign Result			**Not Blocked**

Below output is showing the actions which are not blocked:

Action 1: Dropper used by Lazarus Threat Group in .HWP File Download Variant-2

File name: 855653.hwp

SHA1:9d6fa64e0c0f3ec7442cb72bfaa016c3e3d7ff52

SHA256:81ee247eb8d9116893e5742d12b2d8cd2835db3f751d6be16c2e927b892c5dc7

MD5:c155f49f0a9042d6df68fb593968e110

Action 2: Malware used by Lazarus Threat Group .MACHO File Download Variant-3

File Name: 763984.macho

SHA1:605214c45f2d7ea8d41125558dd8ad3b6ae92b57

SHA256:49046dfeaefc59747e45e013f3ab5a2895b4245cfaa218dd2863d86451104506

MD5: ded8cac968d278aeb2889dc7552e46e1

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis.

4. Cobalt Threat Group Campaign Malware Download Threat – 2 (On-prem)

This threat includes downloading variants of malware used in Cobalt Threat Group campaigns.

#	Actions	Description	Action
1	Trojan used in Cobalt Group APT Campaign .DOC File Download Variant-11	This attack includes downloading a .doc file of trojan used in Cobalt Group APT campaign. This trojan hooks API calls and document spawns new processes. Furthermore, it terminates other processes using taskkill program and contacts with its own C&C servers.	Blocked
2	Cobalt Trojan .EXE File Download Variant-11	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
3	Cobalt Trojan .EXE File Download Variant-12	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
4	Cobalt Trojan .EXE File Download Variant-13	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
5	Cobalt Trojan .EXE File Download Variant-14	This attack includes downloading a .exe payload of the Cobalt trojan which targeted the banks. Cobalt accesses potentially sensitive information from local browsers and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, Cobalt contacts with its own C&C servers.	Blocked
6	Malware used by Cobalt Threat Group .EXE File Download Variant-15	This attack includes downloading a .exe payload of the Cobalt trojan. Cobalt opens the clipboard and reads the cryptographic machine GUID, active computer name of Windows. Furthermore, it modifies proxy settings and it contacts with its own C&C servers.	Blocked
7	Coolpants Backdoor Malware used by Cobalt APT Group .DLL File Download Variant-1	This attack includes downloading a .dll payload file of the Coolpants Backdoor Malware of Cobalt Group which targets financial organizations. Coolpants Backdoor Malware spawns new processes and touches files in the Windows directory.	Blocked
8	ThreadKit Malware used by Cobalt Threat Group .RTF File Download Variant-1	This attack includes downloading a .rtf payload file of the ThreadKit malware used by Cobalt threat group. ThreadKit is a Microsoft Office document exploit builder kit first uncovered in October 2017. Furthermore, it queries sensitive IE security settings and contacts with its own C&C servers.	Blocked
Overall Campaign Result			Not Blocked

5. Lazarus Threat Group Campaign Malware Download Threat – 2 (On-Prem)

This threat includes downloading variants of malware used in Lazarus Threat Group campaign.

#	Actions	Description	Action
1	Destover Trojan .EXE File Download Variant-1	This attack includes downloading an .exe payload file of the Destover trojan. Destover is a disk-wiping malware and it seen in the 2017 bank attacks. The disk-wiping malware linked to Lazarus Group and used in the Sony Pictures attacks.	Blocked
2	HOPLIGHT Trojan used by Lazarus Threat Group .DLL File Download Variant-1	This attack includes downloading a .DLL file of the HOPLIGHT Trojan used by Lazarus Group Threat Group. Lazarus Group (also known as APT38, Hidden Cobra, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team) is a threat group likely backed by the North Korea government. This malware sends traffic on typical HTTP outbound port, but without HTTP header, contains ability to enumerate processes/modules/threads. Furthermore, it contacts with its own C&C servers.	Blocked
3	PowerRatankba Trojan Downloader Used by Lazarus Threat Group in FastCash 2.0 Campaign .PS1 File Download Variant-1	This attack includes downloading a .ps1 file of PowerRatankba Trojan of Lazarus Threat Group FastCash 2.0 Campaign. Lazarus Group is a threat group likely backed by the North Korea government. The group has targeted financial institutions world-wide. It spawns a lot of processes. It queries the logged on user, group or privileges using Whoami and reads the cryptographic machine GUID it contacts with its own C&C servers.	Blocked
4	Dacls RAT used by Lazarus Threat Group .ZIP File Download Variant-1	This attack includes downloading a .zip payload file of the Dacls RAT used by Lazarus threat group. This Mac version is at least distributed via a Trojanized two-factor authentication application for macOS called MinaOTP, mostly used by Chinese speakers. Similar to the Linux variant, it boasts a variety of features including command execution, file management, traffic proxying and worm scanning.	Blocked
5	Blindingcan RAT .DLL File Download Variant-1	This attack includes downloading a .dll payload file of the Blindingcan RAT. It refers to malicious cyber activity by the North Korean government as Lazarus Group. Blindingcan includes malware behaviours related to Lazarus Group, suggested response actions and recommended mitigation techniques. Samples contains built-in functions for remote operations that provide various capabilities on a victim's system. It spawns new processes and installs hooks/patches the running process.	Blocked
6	PowerRatankba Trojan Downloader Used by Lazarus Threat Group in FastCash 2.0 Campaign .EXE File Download Variant-1	This attack includes downloading a .exe file of PowerRatankba Trojan of Lazarus Threat Group FastCash 2.0 Campaign. Lazarus Group is a threat group likely backed by the North Korea government. The group has targeted financial institutions world-wide. It queries kernel debugger information. It reads information such as active computer name, cryptographic machine GUID. It modifies file/console tracing settings (often used to hide footprints on system). it contacts with its own C&C servers.	Blocked
7	BankShot Trojan Used by Lazarus Group APT Campaign .EXE File Download Variant-1	This attack includes downloading an .exe file of BankShot Trojan of Lazarus Group APT Campaign. The U.S. Government refers to the malicious cyber activity by the North Korean government as the Lazarus Group. It reads terminal service related keys, and It contains the ability to query the machine time, timezone and machine version.	Blocked

8	Trojan used by Lazarus Group .XLS File Download Variant-1	This attack includes downloading an .xls payload file of the office malware used by Lazarus Group. This document malware monitors specific registry key for changes. When executed, it de-obfuscates its application programming interfaces (APIs) and using port 443, attempts to connect to the hard-coded IP addresses.	Blocked
9	Ratankba Malware used by Lazarus Group .EXE File Download Variant-1	This attack includes downloading an .exe payload file of a Hacktool that dowloading by Ratankba Malware. This Hacktool shows distinctive characteristics shared with malware previously associated with Lazarus Group.	Blocked
10	CROWDEDFLOUNDER RAT used by LazarusThreat Group .DLL File Download Variant-1	This attack includes downloading a .DLL payload file of the CROWDEDFLOUNDER RAT used by Lazarus threat group. CROWDEDFLOUNDER aims to can listen as a proxy for commands or connect to a remote server to receive commands.This attack queries kernel debugger information. This sample queries process information and reads the system or video BIOS version	Blocked
11	Dacls RAT used by Lazarus Threat Group .SMI File Download Variant-1	This attack includes downloading a .smi payload file of the Dacls RAT used by Lazarus threat group. This Mac version is at least distributed via a Trojanized two-factor authentication application for macOS called MinaOTP, mostly used by Chinese speakers. Similar to the Linux variant, it boasts a variety of features including command execution, file management, traffic proxying and worm scanning.	Blocked
12	ValeforBeta Trojan used by Lazarus Threat Group .EXE File Download Variant-1	This attack includes downloading an .EXE file of the trojan used by Lazarus Threat Group. The assault group Lazarus (also known as the Hidden Cobra) conducts various offensive operations.ValeforBeta have been used in attacks against Japanese organizations. Besides arbitrary code execution from a remote network, it just uploads and downloads files.	Blocked
13	Keymarble RAT Malware used by Lazarus Group Threat Group .EXE File Download Variant-1	This attack includes downloading an .exe payload file of the Keymarble RAT Malware used by Lazarus Group. Keymarble monitors specific registry key for changes. When executed, it de-obfuscates its application programming interfaces (APIs) and using port 443, attempts to connect to the hard-coded IP addresses.	Blocked
14	Dtrack RAT used by Lazarus Group .EXE File Download Variant-1	This attack includes downloading a .exe file of the Dtrack RAT used by Lazarus Group. Dtrack RAT is being used to attack the financial sector and research centers in India. The malicious code is embedded into a binary of a harmless executable. This RAT is designed to be planted on victim's malware and also known as ATMDtrack. It writes data to a remote process and uses anti-debugging techniques to evade analysis.	Blocked
15	Dropper used by Lazarus Threat Group in .HWP File Download Variant-1	This attack includes downloading a .HWP dropper file used by Lazarus Threat Group. The Lazarus Threat Group has been observed making targeted attacks on security researchers and journalists. The group is known for historically targeting individuals of interest to the North Korean regime; including journalists, diplomats, and government employees. This sample drops malicious vbs file in order to download the main malicious executable.	Not Blocked
16	YamaBot Trojan used by Lazarus Threat Group .EXE File Download Variant-1	This attack includes downloading a .exe of the YamaBot Trojan used by Lazarus threat group. YamaBot is malware coded in Golang, with slightly different functionality between types created for each platform. This sample communicates with C2 servers using HTTP requests that targets Windows OS. The malware executes certain commands sent from its C2 server.	Blocked

17	Macro-Embedded Malware used by Lazarus Threat Group .DOCX File Download Variant-1	This attack includes downloading a .DOCX file of the Office Malware used by Lazarus APT Group. Researchers identified new campaign on Jan 18th 2022 form Lazarus Group In this campaign, Lazarus conducted spear phishing attacks weaponized with malicious documents that use their known job opportunities theme. Windows Update to executed the malicious payload and GitHub as a command and control server.	Blocked
18	Macro-Embedded Malware used by Lazarus Threat Group .DOC File Download Variant-1	This attack includes downloading a .DOC file of the Office Malware used by Lazarus APT Group. Researchers identified new campaign on Jan 18th 2022 form Lazarus Group In this campaign, Lazarus conducted spear phishing attacks weaponized with malicious documents that use their known job opportunities theme. Windows Update to executed the malicious payload and GitHub as a command and control server.	Blocked
19	RAT Malware used by Lazarus Threat Group .DOCX File Download Variant-1	This attack includes downloading a .DOCX file of the RAT Malware used by Lazarus Threat Group. Lazarus Group is generally believed to be supported by the North Korean government, with their financial motivation gain as a method of overcome long-standing sanctions against the regime. The potential Lazarus threat group aimed to infect victims using with two different methods. Its been used template injection technique in these methods while malicious documents operating. The first methods template contains VBA RAT that performs following actions; collects victims info, identifies the AV product running on a victims machine, executes shell-codes, deletes files, uploads and downloads files, reads disk and file systems information. The second methods template is an exploit for CVE-2021-26411 which is trying to execute a shell-code to use same VBA RAT.	Blocked
20	Backdoor used by Lazarus Group in AppleJeus Campaign .EXE File Download Variant-1	This attack includes downloading an .exe file of the HOPLIGHT Trojan used by Lazarus Group. Lazarus Group (also known as APT38, Hidden Cobra ,Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team) is a threat group likely backed by the North Korea government. North Korea has used AppleJeus malware posing as cryptocurrency trading platforms since at least 2018. This sample installs hooks/patches the running process.	Blocked
21	TigerRAT RAT used by Lazarus Threat Group .EXE File Download Variant-1	This attack includes downloading an .EXE file of the TigerRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of Operation ByteTiger. This implant consists of several RAT capabilities such as gathering system information and run arbitrary commands on the endpoint.	Blocked
22	MagicRAT RAT used by Lazarus Threat Group .EXE File Download Variant-1	This attack includes downloading an .EXE file of the MagicRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). MagicRAT is a remote access trojan (RAT) that programmed in C plus plus programming language and uses the Qt Framework to make human analysis harder. This RAT was found on victims that had been initially compromised through the exploitation of publicly exposed VMware Horizon platforms.	Not Blocked
23	Blindingcan Trojan used by Lazarus Threat Group .DLL File Download Variant-2	This attack includes downloading a .DLL payload file of the Blindingcan Trojan used by Lazarus Threat Group. The malware runs when a loader loads a DLL file and some part of code in BLINDINGCAN is obfuscated using RC4. Blindingcan performs multiple functions including the	Blocked

		following; operation on files (create a list, delete, move, modify timestamp, copy), upload/download files and execute arbitrary shell command. It broadcasts a large number of ARP requests.	
24	ELECTRICFISH Trojan used by Lazarus Group .EXE File Download Variant-2	This attack includes downloading an .exe file of the ELECTRICFISH Trojan used by Lazarus Group. Lazarus Group (also known as APT38, Hidden Cobra, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team) is a threat group likely backed by the North Korea government. This malware is a command-line utility and its primary purpose is to tunnel traffic between two IP addresses.	Blocked
25	Hermes Ransomware used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .exe of the Hermes ransomware used by Lazarus threat group. The Hermes ransomware tries to delete registry keys using reg.exe and collects the piece of information about of the victim such as cryptographic machine GUID, windows installation date, windows installation language etc and encrypts victim's files.	Blocked
26	RAT Malware used by Lazarus Threat Group .DOCX File Download Variant-2	This attack includes downloading a .DOCX file of the RAT Malware used by Lazarus Threat Group. Lazarus Group is generally believed to be supported by the North Korean government, with their financial motivation gain as a method of overcome long-standing sanctions against the regime. The potential Lazarus threat group aimed to infect victims using with two different methods. Its been used template injection technique in these methods while malicious documents operating. The first methods template contains VBA RAT that performs following actions; collects victims info, identifies the AV product running on a victims machine, executes shell-codes, deletes files, uploads and downloads files, reads disk and file systems information. The second methods template is an exploit for CVE-2021-26411 which is trying to execute a shell-code to use same VBA RAT.	Blocked
27	Copperhedge Backdoor used by Lazarus Group Threat Group .DLL File Download Variant-2	This attack includes downloading a .DLL file of the Copperhedge Malware used by Lazarus Group Threat Group. Lazarus Group (often referred to Hidden Cobra) is an APT group linked to North Korea. The Copperhedge is a malware that is a full-featured RAT that comes in different variants. It spawns new processes and installs hooks/patches the running process and creates files in the Windows directory to make it persistent.	Blocked
28	BankShot Trojan Used by Lazarus Group APT Campaign .EXE File Download Variant-2	This attack includes downloading an .exe file of BankShot Trojan of Lazarus Group APT Campaign. The U.S. Government refers to the malicious cyber activity by the North Korean government as the Lazarus Group. It reads terminal service related keys, and It contains the ability to download files from the internet.	Blocked
29	Dacls RAT used by Lazarus Threat Group .ZIP File Download Variant-2	This attack includes downloading a .zip payload file of the Dacls RAT used by Lazarus threat group. This Mac version is at least distributed via a Trojanized two-factor authentication application for macOS called MinaOTP, mostly used by Chinese speakers. Similar to the Linux variant, it boasts a variety of features including command execution, file management, traffic proxying and worm scanning.	Blocked
30	Volgmer Backdoor Malware Used by Lazarus Group APT Campaign .DLL File Download Variant-2	This attack includes downloading a .dll file of Volgmer Backdoor Malware of Lazarus Group APT Campaign. The U.S. Government refers to the malicious cyber activity by the North Korean government as Lazarus Group. It contains a known anti-VM trick and a known packer. This .dll file is used by Volgmer Trojan Dropper.	Blocked

31	Blindingcan RAT .DOCX File Download Variant-2	This attack includes downloading a .docx payload file of the Blindingcan RAT. It refers to malicious cyber activity by the North Korean government as Lazarus Group. Blindingcan includes malware behaviours related to Lazarus Group, suggested response actions and recommended mitigation techniques. Samples contains built-in functions for remote operations that provide various capabilities on a victim's system. It contacts three domains and three hosts.	Blocked
Overall Campaign Result			Not Blocked

Below output is showing the actions which are not blocked:

Action 1: Dropper used by Lazarus Threat Group in .HWP File Download Variant-1

File name: 821190.hwp

SHA1:40359e0e92a99b428778ac4e9d70fbc4d5307961

SHA256:dbbecbafd905f0b4a2c8194cba3c879d2b933094be9bf27ae69295b4d1de2055

MD5:f17502d3e12615b0fa8868472a4eabfb

Action 2: MagicRAT RAT used by Lazarus Threat Group .EXE File Download Variant-1

File name: 323083.exe

SHA1:a3555a77826df6c8b2886cc0f40e7d7a2bd99610

SHA256:f6827dc5af661fbb4bf64bc625c78283ef836c6985bb2bfb836bd0c8d5397332

MD5:b4c9b903dfd18bd67a3824b0109f955b

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis.

6. Lazarus Threat Group Campaign Malware Download Threat – 3 (On-Prem)

This threat includes downloading variants of malware used in Lazarus Threat Group campaign.

#	Actions	Description	Action
1	Dacls RAT used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .EXE payload file of the Dacls RAT used by Lazarus threat group. Dacls is a new type of remote-control software targeting both Windows and Linux environment. This attack queries kernel debugger information. It also reads the active computer name and the cryptographic machine GUID.	Blocked
2	Keymarble RAT Malware used by Lazarus Group Threat Group .EXE File Download Variant-2	This attack includes downloading an .exe payload file of the Keymarble RAT Malware used by Lazarus Group. Keymarble monitors specific registry key for changes. When executed, it de-obfuscates its application programming interfaces (APIs) and using port 443, attempts to connect to the hard-coded IP addresses.	Blocked
3	VHD Ransomware used by Lazarus Threat Group .DLL File Download Variant-2	This attack includes downloading a .dll of the VHD ransomware used by Lazarus threat group. This first incident occurred in Europe and had two important features, a very unknown family of ransomware and a spreading technique reminiscent of APT groups. The ransomware itself is nothing special, its written in C and crawls all connected disks to encrypt files and delete any folder called System Volume Information. The program also stops processes that could be locking important files, such as Microsoft Exchange and SQL Server.	Blocked
4	PowerRatankba Trojan Downloader Used by Lazarus Threat Group in FastCash 2.0 Campaign .EXE File Download Variant-2	This attack includes downloading a .ps1 file of PowerRatankba Trojan of Lazarus Threat Group FastCash 2.0 Campaign. Lazarus Group is a threat group likely backed by the North Korea government. The group has targeted financial institutions world-wide. It queries kernel debugger information. It reads information such as active computer name, cryptographic machine GUID. It contacts with its own C&C servers.	Blocked
5	Dtrack RAT used by Lazarus Group .EXE File Download Variant-2	This attack includes downloading a .exe file of the Dtrack RAT used by Lazarus Group. Dtrack RAT is being used to attack the financial sector and research centers in India. The malicious code is embedded into a binary of a harmless executable. This RAT is designed to be planted on victim's malware and also known as ATMDtrack. It writes data to a remote process and uses anti-debugging techniques to evade analysis.	Blocked
6	VHD Ransomware used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .exe of the VHD ransomware used by Lazarus threat group. This first incident occurred in Europe and had two important features, a very unknown family of ransomware and a spreading technique reminiscent of APT groups. The ransomware itself is nothing special, its written in C and crawls all connected disks to encrypt files and delete any folder called System Volume Information. The program also stops processes that could be locking important files, such as Microsoft Exchange and SQL Server.	Blocked
7	Dropper used by Lazarus Threat Group in .HWP File Download Variant-2	This attack includes downloading a .HWP dropper file used by Lazarus Threat Group. The Lazarus Threat Group has been observed making targeted attacks on security researchers and journalists. The group is known for historically targeting individuals of interest to the North Korean regime; including journalists, diplomats, and government employees. This sample drops malicious vbs file in order to download the main malicious executable.	Not Blocked
8	HOPLIGHT Trojan used by Lazarus Threat	This attack includes downloading an .exe file of the HOPLIGHT Trojan used by Lazarus Group Threat Group. Lazarus Group (also known as	Blocked

	Group .EXE File Download Variant-2	APT38, Hidden Cobra, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team) is a threat group likely backed by the North Korea government. This malware sends traffic on typical HTTP outbound port, but without HTTP header, contains ability to enumerate processes/modules/threads. Furthermore, it contacts with its own C&C servers.	
9	MagicRAT RAT used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading an .EXE file of the MagicRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). MagicRAT is a remote access trojan (RAT) that programmed in C plus plus programming language and uses the Qt Framework to make human analysis harder. This RAT was found on victims that had been initially compromised through the exploitation of publicly exposed VMware Horizon platforms.	**Blocked**
10	Trojan used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .EXE dropper file used by Lazarus Threat Group. The Lazarus Threat Group has been observed making targeted attacks on security researchers and journalists. The group is known for historically targeting individuals of interest to the North Korean regime; including journalists, diplomats, and government employees. This is the main malicious executable to compromise the target system.	**Blocked**
11	TigerRAT RAT used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading an .EXE file of the TigerRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of Operation ByteTiger. This implant consists of several RAT capabilities such as gathering system information and run arbitrary commands on the endpoint.	**Blocked**
12	Malware used by Lazarus Threat Group .EXE File Download Variant-2	This attack includes downloading a .exe of the trojan used by Lazarus threat group. This trojan modifies auto-execute functionality by setting/creating a value in the registry and reads the active computer name. Furthermore, this malicious file contacts with its own C&C servers.	**Blocked**
13	Lazarus Group's Trojan .DLL File Download Variant-2	This attack includes downloading a .DLL payload file of the Lazarus Group Trojan which spawns new processes and posts files to a web server. Also, it contacts with its own C&C servers.	**Blocked**
14	Malware used by Lazarus Threat Group .MACHO File Download Variant-2	This attack includes downloading a .macho of the malware used by Lazarus threat group. The campaign has been using lures for attractive job offers since at least 2020, but this year novel macOS malware was discovered with embedded PDF documents advertising jobs vacancies and attempting to masquerade as legitimate processes with names such as wifianalyticsagent and safarifontsagent. This multi-stage malware first installs a LaunchAgent for persistence in the users local folder, obviating the need for further permissions, although on macOS Ventura that does now at least raise an alert notification. The second stage in the Crypto.com variant is a bare-bones application bundle named WifiAnalyticsServ.app (FinderFontsUpdater.app in the Coinbase variant). with the bundle identifier finder.fonts.extractor. The second-stage extracts and executes a third-stage binary, wifianalyticsagent, which serves as a downloader for an unretrieved fourth stage from a C2 at market.	**Blocked**

15	BankShot Trojan Used by Lazarus Group APT Campaign .EXE File Download Variant-3	This attack includes downloading an .exe file of BankShot Trojan of Lazarus Group APT Campaign. The U.S. Government refers to the malicious cyber activity by the North Korean government as the Lazarus Group. It reads terminal service related keys, and It possibly checks for the presence of an Antivirus engine	Blocked
16	Malware used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading a .exe of the trojan used by Lazarus threat group. This trojan modifies auto-execute functionality by setting/creating a value in the registry and reads the active computer name. Furthermore, this malicious file contacts with its own C&C servers.	Blocked
17	VHD Ransomware used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading a .exe of the VHD ransomware used by Lazarus threat group. This first incident occurred in Europe and had two important features, a very unknown family of ransomware and a spreading technique reminiscent of APT groups. The ransomware itself is nothing special, its written in C and crawls all connected disks to encrypt files and delete any folder called System Volume Information. The program also stops processes that could be locking important files, such as Microsoft Exchange and SQL Server.	Blocked
18	Dtrack RAT used by Lazarus Group .EXE File Download Variant-3	This attack includes downloading a .exe file of the Dtrack RAT used by Lazarus Group. Dtrack RAT is being used to attack the financial sector and research centers in India. The malicious code is embedded into a binary of a harmless executable. This RAT is designed to be planted on victim's malware and also known as ATMDtrack. It writes data to a remote process and uses anti-debugging techniques to evade analysis. The malware also posts data to a webserver.	Blocked
19	MagicRAT RAT used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading an .EXE file of the MagicRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). MagicRAT is a remote access trojan (RAT) that programmed in C plus plus programming language and uses the Qt Framework to make human analysis harder. This RAT was found on victims that had been initially compromised through the exploitation of publicly exposed VMware Horizon platforms.	Blocked
20	RAT Malware used by Lazarus Threat Group .DOCX File Download Variant-3	This attack includes downloading a .DOCX file of the RAT Malware used by Lazarus Threat Group. Lazarus Group is generally believed to be supported by the North Korean government, with their financial motivation gain as a method of overcome long-standing sanctions against the regime. The potential Lazarus threat group aimed to infect victims using with two different methods. Its been used template injection technique in these methods while malicious documents operating. The first methods template contains VBA RAT that performs following actions; collects victims info, identifies the AV product running on a victims machine, executes shell-codes, deletes files, uploads and downloads files, reads disk and file systems information. The second methods template is an exploit for CVE-2021-26411 which is trying to execute a shell-code to use same VBA RAT.	Not Blocked
21	HOPLIGHT Trojan used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading an .exe file of the HOPLIGHT Trojan used by Lazarus Group Threat Group. Lazarus Group (also known as APT38, Hidden Cobra, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team) is a threat group likely backed by the North Korea government. This malware sends traffic on typical HTTP	Blocked

		outbound port, but without HTTP header, contains ability to enumerate processes/modules/threads. Furthermore, it contacts with its own C&C servers.	
22	Malware used by Lazarus Threat Group .MACHO File Download Variant-3	This attack includes downloading a .macho of the malware used by Lazarus threat group. The campaign has been using lures for attractive job offers since at least 2020, but this year novel macOS malware was discovered with embedded PDF documents advertising jobs vacancies and attempting to masquerade as legitimate processes with names such as wifianalyticsagent and safarifontsagent. This multi-stage malware first installs a LaunchAgent for persistence in the users local folder, obviating the need for further permissions, although on macOS Ventura that does now at least raise an alert notification. The second stage in the Crypto.com variant is a bare-bones application bundle named WifiAnalyticsServ.app (FinderFontsUpdater.app in the Coinbase variant). with the bundle identifier finder.fonts.extractor. The second-stage extracts and executes a third-stage binary, wifianalyticsagent, which serves as a downloader for an unretrieved fourth stage from a C2 at market.	**Not Blocked**
23	TigerRAT RAT used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading an .EXE file of the TigerRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of Operation ByteTiger. This implant consists of several RAT capabilities such as gathering system information and run arbitrary commands on the endpoint.	**Blocked**
24	Copperhedge Backdoor used by Lazarus Group Threat Group .DLL File Download Variant-3	This attack includes downloading a .DLL file of the Copperhedge Malware used by Lazarus Group Threat Group. Lazarus Group (often referred to Hidden Cobra) is an APT group linked to North Korea. The Copperhedge is a malware that is a full-featured RAT that comes in different variants. It writes data to a remote process and tries to sleep for a long time (more than two minutes) to bypass virtual machines.	**Blocked**
25	Hermes Ransomware used by Lazarus Threat Group .EXE File Download Variant-3	This attack includes downloading a .exe of the Hermes ransomware used by Lazarus threat group. The Hermes ransomware tries to delete registry keys using reg.exe and collects the piece of information about of the victim such as cryptographic machine GUID, windows installation date, windows installation language etc and encrypts victim's files.	**Blocked**
26	TigerRAT RAT used by Lazarus Threat Group .EXE File Download Variant-4	This attack includes downloading an .EXE file of the TigerRAT RAT used by Lazarus threat group. Lazarus threat group is a state-sponsored APT attributed to North Korea by the U.S. Cyber Security & Infrastructure Agency (CISA). TigerRAT is an implant disclosed in 2021 by KISA and KRCERT as part of Operation ByteTiger. This implant consists of several RAT capabilities such as gathering system information and run arbitrary commands on the endpoint.	**Blocked**
27	HOPLIGHT Trojan used by Lazarus Threat Group .EXE File Download Variant-4	This attack includes downloading an .exe file of the HOPLIGHT Trojan used by Lazarus Group Threat Group. Lazarus Group (also known as APT38, Hidden Cobra, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team) is a threat group likely backed by the North Korea government. This malware sends traffic on typical HTTP outbound port, but without HTTP header, contains ability to enumerate processes/modules/threads. Furthermore, it contacts with its own C&C servers.	**Blocked**

28	BankShot Trojan Used by Lazarus Group APT Campaign .DLL File Download Variant-4	This attack includes downloading a .dll file of BankShot Trojan of Lazarus Group APT Campaign. The U.S. Government refers to the malicious cyber activity by the North Korean government as the Lazarus Group. It spawns new processes.	Blocked
29	Hermes Ransomware used by Lazarus Threat Group .EXE File Download Variant-4	This attack includes downloading a .exe of the Hermes ransomware used by Lazarus threat group. The Hermes ransomware tries to delete registry keys using reg.exe and collects the piece of information about of the victim such as cryptographic machine GUID, windows installation date, windows installation language etc and encrypts victim's files.	Blocked
30	Copperhedge Backdoor used by Lazarus Group Threat Group .DLL File Download Variant-4	This attack includes downloading a .DLL file of the Copperhedge Malware used by Lazarus Group Threat Group. Lazarus Group (often referred to Hidden Cobra) is an APT group linked to North Korea. The Copperhedge is a malware that is a full-featured RAT that comes in different variants. It posts files to a webserver, writes data to a remote process and contacts three domains and a host.	Blocked
31	Malware used by Lazarus (Hidden Cobra) Group .EXE File Download Variant-4	This attack includes downloading an .EXE file of the trojan used by Lazarus Threat Group. This sample spawns new malicious processes and uses rundll32 technique for execution. It also drops files to the target system and hooks other running processes.	Blocked
Overall Campaign Result			Not Blocked

Below output is showing the actions which are not blocked:

Action 1: Dropper used by Lazarus Threat Group in .HWP File Download Variant-2

File name: 855653.hwp

SHA1:9d6fa64e0c0f3ec7442cb72bfaa016c3e3d7ff52

SHA256:81ee247eb8d9116893e5742d12b2d8cd2835db3f751d6be16c2e927b892c5dc7

MD5:c155f49f0a9042d6df68fb593968e110

Action 2: Malware used by Lazarus Threat Group .MACHO File Download Variant-3

File name: 763984.macho

SHA1:605214c45f2d7ea8d41125558dd8ad3b6ae92b57

SHA256:49046dfeaefc59747e45e013f3ab5a2895b4245cfaa218dd2863d86451104506

MD5: ded8cac968d278aeb2889dc7552e46e1

Action 3: RAT Malware used by Lazarus Threat Group .DOCX File Download Variant-3

File name: 863743.docx

SHA1: d2e9dcec8fbf4f44db5795bdbd736e7ff2c7c23e

SHA256: fffe061643271155f29ae015bca89100dec6b4b655fe0580aa8c6aee53f34928

MD5: 6775e38ea2ad51f95f090d37fc3ab484

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis.

7. Molerats Threat Group Campaign Malware Download Threat – 2 (On-Prem)

This threat includes downloading variants of malware used in Molerats Threat Group campaigns.

#	Actions	Description	Action
1	NeD Worm used by Molerats Threat Group in Operation JOKAA .EXE File Download Variant-15	This attack includes downloading a .exe payload file of the NeD Worm malware used by Molerats Threat Group in Operation JOKAA. NeD worm malware modifies system certificates settings and queries sensitive IE security settings. Furthermore, it contacts with its own C&C servers and uses Pastebin as C&C server.	**Blocked**
2	Backdoor used by Molerats Threat Group .EXE File Download Variant-3	This attack includes downloading an .EXE file of the backdoor used by Molerats Threat Group. Researchers identified several macro-based MS office files uploaded from Middle Eastern countries such as Jordan to OSINT sources such as VT. The backdoor creates a file inside the victim specific folder on Dropbox which is used to fetch C2 commands. The file name is a random string of 15 characters. Also uses command codes instead of plaintext strings to determine the action to be performed	**Blocked**
3	Backdoor used by Molerats Threat Group .EXE File Download Variant-2	This attack includes downloading an .EXE file of the backdoor used by Molerats Threat Group. Researchers identified several macro-based MS office files uploaded from Middle Eastern countries such as Jordan to OSINT sources such as VT. The backdoor creates a file inside the victim specific folder on Dropbox which is used to fetch C2 commands. The file name is a random string of 15 characters. Also uses command codes instead of plaintext strings to determine the action to be performed	**Blocked**
4	Backdoor used by Molerats Threat Group .EXE File Download Variant-1	This attack includes downloading an .EXE file of the backdoor used by Molerats Threat Group. Researchers identified several macro-based MS office files uploaded from Middle Eastern countries such as Jordan to OSINT sources such as VT.. The backdoor creates a file inside the victim specific folder on Dropbox which is used to fetch C2 commands. The file name is a random string of 15 characters. Also uses command codes instead of plaintext strings to determine the action to be performed	**Blocked**
5	Dropper used by Molerats Threat Group .PPTX File Download Variant-1	This attack includes downloading an .PPTX file of the dropper used by Molerats Threat Group. Researchers identified several macro-based MS office files uploaded from Middle Eastern countries such as Jordan to OSINT sources such as VT. These files contained decoy themes related to geo-political conflicts between Israel and Palestine. Such themes have been used in previous attack campaigns waged by the Molerats APT. The macro code is not complex or obfuscated. It simply executes a command using cmd.exe which in turn performs the following operations. Executes a PowerShell command to download and drop the Stage-2 payload from the attacker url to the path ProgramData. Renames document.htm to servicehost.exe. Executes servicehost.exe which is .Net based backdoor.	**Blocked**

6	Dropper used by Molerats Threat Group .DOCX File Download Variant-1	This attack includes downloading an .DOCX file of the dropper used by Molerats Threat Group. Researchers identified several macro-based MS office files uploaded from Middle Eastern countries such as Jordan to OSINT sources such as VT. These files contained decoy themes related to geo-political conflicts between Israel and Palestine. Such themes have been used in previous attack campaigns waged by the Molerats APT. The macro code is not complex or obfuscated. It simply executes a command using cmd.exe which in turn performs the following operations. Executes a PowerShell command to download and drop the Stage-2 payload from the attacker url to the path ProgramData. Renames document.htm to servicehost.exe. Executes servicehost.exe which is .Net based backdoor.	**Blocked**
7	Dropper used by Molerats Threat Group .DOC File Download Variant-1	This attack includes downloading an .DOC file of the dropper used by Molerats Threat Group. Researchers identified several macro-based MS office files uploaded from Middle Eastern countries such as Jordan to OSINT sources such as VT. These files contained decoy themes related to geo-political conflicts between Israel and Palestine. Such themes have been used in previous attack campaigns waged by the Molerats APT. The macro code is not complex or obfuscated. It simply executes a command using cmd.exe which in turn performs the following operations. Executes a PowerShell command to download and drop the Stage-2 payload from the attacker url to the path ProgramData. Renames document.htm to servicehost.exe. Executes servicehost.exe which is .Net based backdoor.	**Blocked**
Overall Campaign Result			**Blocked**

Data Exfiltration Summary

1. Critical OS Data Exfiltration Campaign

This campaign includes exfiltrating documents that contains critical operating system data.

#	Actions	Descriptions	Action
1	The Security Account Manager (SAM) Database File Exfiltration from Windows OS	This attack includes uploading SAM file obtained from a compromised Windows system. The user passwords are stored in a hashed format in a registry hive either as a LM hash or as a NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.	**Not Blocked**
Overall Campaign Result			**Not Blocked**

Below output is showing the actions which are not blocked:

Action 1: The Security Account Manager (SAM) Database File Exfiltration from Windows OS.

File name: 497757.sam

SHA1:0e913800275a27c084c472df39b8061c6e88ae0e

SHA256:2a1ab24e27cf7c2f33641f58d8bd55ec0a820dc0689813fd367a851627f2df24

MD5:018fa5fdc1eaf324c55effce03511532

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis.

2. Financial Data Exfiltration Campaign

This campaign includes exfiltrating documents that contains financial data.

#	Actions	Description	Action
1	United Arab Emirates Financial Data Information Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .pdf format: Name Surname, Emirates ID, IBAN, Credit Card Number.	Not Blocked
2	U.K. Financial Data Information Exfiltration DOCX Format (25 records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .docx format: name, swiftcode, IssuingNetwork, card number. .	Not Blocked
3	U.K. Financial Data Information Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .pdf format: name, swiftcode, IssuingNetwork, card number.	Not Blocked
4	United Arab Emirates Financial Data Information Exfiltration XLSX Format (25 records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .xlsx format: Name Surname, Emirates ID, IBAN, Credit Card Number.	Not Blocked
5	United Arab Emirates Financial Data Information Exfiltration PNG Format (25 records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .png format: Name Surname, Emirates ID, IBAN, Credit Card Number.	Not Blocked
6	United Arab Emirates Financial Data Information Exfiltration CSV Format (25 records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .csv format: Name Surname, Emirates ID, IBAN, Credit Card Number.	Not Blocked
7	U.K. Financial Data Information Exfiltration XLSX Format (25 records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .xlsx format: name, swiftcode, IssuingNetwork, card number.	Not Blocked
8	U.K. Financial Data Information Exfiltration CSV Format (25 records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .csv format: name, swiftcode, IssuingNetwork, card number.	Not Blocked
9	United Arab Emirates Financial Data Information Exfiltration DOCX Format (25 records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .docx format: Name Surname, Emirates ID, IBAN, Credit Card Number.	Not Blocked
10	U.K. Financial Data Information Exfiltration PNG Format (25 records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .png format: name, swiftcode, IssuingNetwork, card number.	Not Blocked
Overall Campaign Result			Not Blocked

Action 1: United Arab Emirates Financial Data Information Exfiltration PDF Format (25 records)

File name: 227448.pdf

SHA1:8e3db48339a77fe8f196f404557b90cc416bd74b

SHA256:fd77ed25f2345c1d23cf18f059dd1073b149ef0152bbc1e03fd167146d1d01eb

MD5:5cbdbc2d195832262eadff65e390bfbf

Action 2: U.K. Financial Data Information Exfiltration DOCX Format (25 records)

File name: 254809.docx

SHA1:1c8db76dcbb8b1f71468dac4b9f118a027a4e9e5

SHA256:95bfe431763c6691c752d901148b594bf01f33987a480113f175a15d53739091

MD5:6b7591243a3d7a4adf71ab1c5c7e0c58

Action 3: U.K. Financial Data Information Exfiltration PDF Format (25 records)

File name: 372419.pdf

SHA1:26d02743bde6fddaf7533c00a4be590ce95f5d92

SHA256:982df81c3d7af02ca0bc0b75b892a8dc13573d74d4ef4797e83ed3a1d14067aa

MD5:419580957da7a5789b8d54a109c32eab

Action 4: United Arab Emirates Financial Data Information Exfiltration XLSX Format (25 records)

File name: 413128.xlsx

SHA1:57994dcc2c4ef387ce519be34a0262ea614b45c9

SHA256:cd536aaa3547b76eac6e3bdfa2e92ac864469faeacb795be69530fc708d099fa

MD5:30bcf4b879960972c70923dcbabad9a3

Action 5: United Arab Emirates Financial Data Information Exfiltration PNG Format (25 records)

File name: 504315.png

SHA1:9fc4f90e8778ba3f26594f4f75d4a20b28400419

SHA256:2c743b82702ce200866c88c8b79e25ad933541d858cf49c7a0420e855aa5a371

MD5:ad99d45ecb838666a5b6ad9b4baa7efe

Action 6: United Arab Emirates Financial Data Information Exfiltration CSV Format (25 records)

File name: 583489.csv

SHA1:9987926e54a0bfc72d798a739b62c0ed63a846e7

SHA256:7ab768c6d88e209b6ab79148dc80e01cf1019fd658256bfc1f86070312b1383d

MD5:7a651b6375abd99ab51e59b8b17258d6

Action 7: U.K. Financial Data Information Exfiltration XLSX Format (25 records)

File name : 591554.xlsx

SHA1:ec757aa6730e66e6f8150c80780ab0ab64175fe5

SHA256:b59ae51fdde0336110fe3640af34d9cdcd1992e65078ba88a45374145c36bb7a

MD5:800485eb729cb03c0885b2dc8b52a9fb

Action 8: U.K. Financial Data Information Exfiltration CSV Format (25 records)

File name : 614014.csv

SHA1:718edd0a87f362b074631fd783c6beb767528f39

SHA256:049461409e160d0dc25dc96922571919c63736f80a6fe1f25051ee08fea4613c

MD5:282aeffcd23c34cc323e14c0f61f3352

Action 9: United Arab Emirates Financial Data Information Exfiltration DOCX Format (25 records)

File name: 684605.docx

SHA1:d3e04d8f0116e5004cf1776f9e0923efe32db453

SHA256:0f96c47319f2a75c062a4194aa9f11c8b7295263faf2d037d8a900fb33e2c8f9

MD5:c709d00f59e11c37b0cc66adf0a27e05

Action 10: U.K. Financial Data Information Exfiltration PNG Format (25 records)

File name: 862252.png

SHA1:c7d13d3cdfd684388a9e932dd5a3beaf1ff24aa8

SHA256:945a8be52827edff37767e003fc04d839c31ce43e82f4d2a2a0f3c9cf77b1ffe

MD5:8d7b2c483637b23ea1d3822c451a6c79

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis.

3. Personally Identifiable Information (PII) Data Exfiltration Campaign

This campaign includes exfiltrating documents that contains Personally Identifiable Information (PII) data.

#	Actions	Descriptions	Action
1	TR PII Exfiltration including ID Card Serial and Number, National Identifier and Full Name in XLSX Format (200 Records)	This attack includes uploading a .xlsx file that contains ID card serial and number, national identifier (TC kimlik no) and full name in .xlsx Format. his file contains personally identifiable information (PII), which is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail and organizational harms may include a loss of public trust, legal liability, or remediation costs.	Not Blocked
2	TR PCI Exfilration including Full Name, E-mail, Username, Password and MD5 Hash in XML format (500 records)	This attack includes uploading a .xml file that contains name, surname, e-mail address, username, password and MD5 hash of the passsword. This file contains personally identifiable information (PII), which is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail; and organizational harms may include a loss of public trust, legal liability, or remediation costs.	Not Blocked
3	Italy PII Info. Exfiltration including Codice Fiscale in JSON Array Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .JSON array format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
4	Italy PII Info. Exfiltration including Codice Fiscale in HTM Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .HTM format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
5	Italy PII Info. Exfiltration including Codice Fiscale in XML Properties Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XML properties format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
6	Italy PII Info. Exfiltration including Codice Fiscale in JSON Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .JSON format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
7	U.K. Personal Information Online Code of Practice Information Exfiltration PNG Format (25 records)	This attack includes uploading a document that contains the following U.K. Personal Information Online Code of Practice Information specialized for United Kingdom in .png format: name, national insurance number, national health service, swiftcode.	Not Blocked

8	Brazil CPF Number Exfiltration PDF Format (10 Records)	This attack includes uploading a document that contains the following CPF number specialized for Brazil in .pdf format: CPF, Name, Date.	Not Blocked
9	Italy PII Info. Exfiltration including Codice Fiscale in DOCX Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .DOCX format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
10	Italy PII Info. Exfiltration including Codice Fiscale in XML Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XML format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
11	Brazil CPF Number Exfiltration XLSX Format (10 Records)	This attack includes uploading a document that contains the following CPF number specialized for Brazil in .xlsx format: CPF, Name, Date.	Not Blocked
12	Italy PII Info. Exfiltration including Codice Fiscale in DOC Format (500 records)	This attack includes uploading a document that contains the following CPF number specialized for Brazil in .xlsx format: CPF, Name, Date.	Not Blocked
13	Italy PII Info. Exfiltration including Codice Fiscale in SQL Format (500 records)	This attack includes uploading a document that contains the following CPF number specialized for Brazil in .xlsx format: CPF, Name, Date.	Not Blocked
14	Italy PII Info. Exfiltration including Codice Fiscale in PPT Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .DOC format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
15	Italy PII Info. Exfiltration including Codice Fiscale in XLS Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .DOC format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
16	Italy PII Info. Exfiltration including Codice Fiscale in XLSX Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .DOC format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
17	Australia PII Exfiltration including Tax File Number (TFN) in TXT Format (20 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .SQL format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
18	Italy PII Info. Exfiltration including Codice Fiscale in ODT Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .SQL format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
19	US PII Exfiltration including SSN and Full Name in TXT Format (200 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .SQL format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked
20	U.K. Personally Identifiable Information (PII) Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .PPT format. This file contains PII, which is any data that could potentially identify a specific individual.	Not Blocked

21	U.K. Personal Information Online Code of Practice Information Exfiltration XLSX Format (25 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .PPT format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
22	Germany PII Exfiltration including German Tax ID (GTI or Steuer-IdNr.) in TXT Format (20 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .PPT format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
23	TR PII Exfiltration including All National ID Card Information in DOCX Format (3 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XLS format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
24	U.K. Personal Information Online Code of Practice Information Exfiltration DOCX Format (25 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XLS format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
25	US PII Exfiltration including Social Security Number (TFN) in TXT Format (20 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XLS format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
26	Turkey TaxID Exfiltration DOC Format (10 Records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XLSX format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
27	UK PII Exfiltration including National Insurance Number (NINO) and Full Name in CSV Format (1 record)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XLSX format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
28	Italy PII Info. Exfiltration including Codice Fiscale in YAML Format (500 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .XLSX format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
29	U.K. Personally Identifiable Information (PII) Exfiltration PNG Format (25 records)	This attack includes uploading a document that contains the following PII (Personally Identifiable Information) specialized for Australia in .txt format: Tax File Number (TFN). PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
30	International Driver's License Application Data Exfiltration including PII and PCI in PDF Format	This attack includes uploading a document that contains the following PII (Personally Identifiable Information) specialized for Australia in .txt format: Tax File Number (TFN). PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**

31	Italy PII Info. Exfiltration including Codice Fiscale in TXT Format (500 records)	This attack includes uploading a document that contains the following PII (Personally Identifiable Information) specialized for Australia in .txt format: Tax File Number (TFN). PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
32	US PII Exfiltration including Individual Taxpayer identification Number (ITIN) in TXT Format (2 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .ODT format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
33	UK PII Unique Taxpayer Reference (UTR) in TXT Format (20 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .ODT format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
34	U.K. Personal Information Online Code of Practice Information Exfiltration CSV Format (25 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for ITALY in .ODT format. This file contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
35	Italy PII Info. Exfiltration including Codice Fiscale in ODS Format (500 records)	This attack includes uploading a document that contains the following PII (Personally Identifiable Information) specialized for United States in .txt format: SSN (Social Security Number), full name and date of birth. PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
36	U.K. Personally Identifiable Information (PII) Exfiltration XLSX Format (25 records)	This attack includes uploading a document that contains the following PII (Personally Identifiable Information) specialized for United States in .txt format: SSN (Social Security Number), full name and date of birth. PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
37	U.K. Personal Information Online Code of Practice Information Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following PII (Personally Identifiable Information) specialized for United States in .txt format: SSN (Social Security Number), full name and date of birth. PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail; and organizational harms may include a loss of public trust, legal liability, or remediation costs. Sample data: NAME: JAMES SMITH SSN: 148-76-8157 DOB: 01/30/1993	**Not Blocked**
38	U.K. Personally Identifiable Information (PII) Exfiltration CSV Format (25 records)	This attack includes uploading a document that contains the following U.K. Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: name, passportnumber, national health service.	**Not Blocked**

39	Italy PII Info. Exfiltration including Codice Fiscale in HTML Format (500 records)	This attack includes uploading a document that contains the following U.K. Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: name, passportnumber, national health service.	**Not Blocked**
40	U.K. Personally Identifiable Information (PII) Exfiltration DOCX Format (25 records)	This attack includes uploading a document that contains the following U.K. Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: name, passportnumber, national health service.	**Not Blocked**
41	Italy PII Info. Exfiltration including Codice Fiscale in PDF Format (500 records)	This attack includes uploading a document that contains the following U.K. Personal Information Online Code of Practice Information specialized for United Kingdom in .xlsx format: name, national insurance number, national health service, swiftcode.	**Not Blocked**
42	Italy PII Info. Exfiltration including Codice Fiscale in MHT Format (500 records)	This attack includes uploading a document that contains the following U.K. Personal Information Online Code of Practice Information specialized for United Kingdom in .xlsx format: name, national insurance number, national health service, swiftcode.	**Not Blocked**
43	Italy PII Info. Exfiltration including Codice Fiscale in PPS Format (500 records)	This attack includes uploading a document that contains the following U.K. Personal Information Online Code of Practice Information specialized for United Kingdom in .xlsx format: name, national insurance number, national health service, swiftcode.	**Not Blocked**
44	TR PII Exfiltration including National Identifier (TC Kimlik No) and Full Name in PDF Format (100 Records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for Germany in .txt format: German Tax ID (GTI) - Steuerliche Identifikationsnummer (Steuer-IdNr.). PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
45	Turkey IBAN Exfiltration DOC Format (10 Records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for Germany in .txt format: German Tax ID (GTI) - Steuerliche Identifikationsnummer (Steuer-IdNr.). PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
46	TR PII Exfiltration including National Identifier, ID Card, Passport and Driver License IDs in JSON Format (1000 records)	This attack includes uploading a document that contains the following Personally Identifiable Information (PII) specialized for Germany in .txt format: German Tax ID (GTI) - Steuerliche Identifikationsnummer (Steuer-IdNr.). PII is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
47	Italy PII Info. Exfiltration including Codice Fiscale in CSV Format (500 records)	This attack includes uploading a .xlsx file that contains all information in a National ID Card of a citizen of Turkey, such as ID card number, national id number (TC kimlik no), name, surname, father's name, mother's name, place of birth, date of birth, marital status, blood group, place of issue, reason of issue, registration number and issue date. This file contains personally identifiable information (PII), which is any data that	**Not Blocked**

		could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	
48	Italy PII Info. Exfiltration including Codice Fiscale in RTF Format (500 records)	This attack includes uploading a .xlsx file that contains all information in a National ID Card of a citizen of Turkey, such as ID card number, national id number (TC kimlik no), name, surname, father's name, mother's name, place of birth, date of birth, marital status, blood group, place of issue, reason of issue, registration number and issue date. This file contains personally identifiable information (PII), which is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
49	Italy PII Info. Exfiltration including Codice Fiscale in PPTX Format (500 records)	This attack includes uploading a .xlsx file that contains all information in a National ID Card of a citizen of Turkey, such as ID card number, national id number (TC kimlik no), name, surname, father's name, mother's name, place of birth, date of birth, marital status, blood group, place of issue, reason of issue, registration number and issue date. This file contains personally identifiable information (PII), which is any data that could potentially identify a specific individual. The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years.	**Not Blocked**
50	Canada PII Exfiltration including Social Insurance Number (SIN) in TXT Format (20 records)	This attack includes uploading a document that contains the following U.K. Personal Information Online Code of Practice Information specialized for United Kingdom in .docx format: name, national insurance number, national health service, swiftcode.	**Not Blocked**
51	Italy PII Info. Exfiltration including Codice Fiscale in PPSX Format (500 records)	This attack includes uploading a document that contains the following U.K. Personal Information Online Code of Practice Information specialized for United Kingdom in .docx format: name, national insurance number, national health service, swiftcode.	**Not Blocked**
Overall Campaign Result			**Not Blocked**

Action 1: TR PII Exfiltration including ID Card Serial and Number, National Identifier and Full Name in XLSX Format (200 Records)

File name : 145356.xlsx

SHA1:24b8873058b54f510974a88a78d9f62b39f3a5b9

SHA256:2868fcff02ae5e316a97a03f61eefd9db4a233baf94bb153d953c7e06341815f

MD5:8adba31c1a711a10f6d46f18fd06e3b8

Action 2: TR PCI Exfilration including Full Name, E-mail, Username, Password and MD5 Hash in XML format (500 records)

File name : 167804.xml

SHA1:d44d44a8abd87a49475b7dea0c8b0561fd1e429c

SHA256:9eade183853215573891da34d7f83497b8aff544f1a36df36fb2b4c5b22dbec0

MD5:a8365c2678970610b14ec4813189078c

Action 3: Italy PII Info. Exfiltration including Codice Fiscale in JSON Array Format (500 records)

File name : 173732.json

SHA1:b2259ef3a5da592f3cacc44f28e1473dccf91f27

SHA256:c7be4ac133dd53d3ac3acf7eafa75c7938bc581ab46cbd6d3080d29eb27e523c

MD5:6463c95733aaaa5d46e4ae4f0215af40

Action 4: Italy PII Info. Exfiltration including Codice Fiscale in HTM Format (500 records)

File name: 197929.htm

SHA1:4de3c7d8ef28822e1b46612560d122605b43dc74

SHA256:e28b0b8f7e469c8530ded734982fcee197583f34c17b0e28d0ac2bffb986bb9e

MD5:09c0ed580275bab888f97416a8537b05

Action 5: Italy PII Info. Exfiltration including Codice Fiscale in XML Properties Format (500 records)

File name: 207070.xml

SHA1:0a2e1d2ecf360102888618abffa4c82a5607fd2c

SHA256:bb53056452c74cc4cfd92d11003073c27fd4f86f38b98e8d40ae1f4af142bd53

MD5:081e2c2772557d41c22eab22f8204931

Action 6: Italy PII Info. Exfiltration including Codice Fiscale in JSON Format (500 records)

File name: 235262.json

SHA1:f9e75705b8baf03f9ec98b59e2676f8ebfdb34bc

SHA256:383fbafaacc8833a7ff99c3e6c6530bcabdfda61412406abcafb1fa29ad4b21c

MD5:2f2df3c11b95d1af51f1e8a266a340df

Action 7: U.K. Personal Information Online Code of Practice Information Exfiltration PNG Format (25 records)

File name : 238123.png

SHA1:6c9ff2c6a58b52ad14fbf9ef475f45d7a069a91d

SHA256:b49c462572ad3ac37b592cbc401e1fd1b317a6cf82e8ec9c48df524eae8ee746

MD5:5aa6df95387fb0df56693d3a7e5db194

Action 8: Brazil CPF Number Exfiltration PDF Format (10 Records)

File name: 248558.pdf

SHA1:704b1ee938e73f06a758bc4cc9b42de90c6ce15b

SHA256:dd8853f88be63e88e006e71999e40a503d7b8afe77e101019ee713fbb04a2fb7

MD5:dde0d56c598af7c390e74a3df257a929

Action 9: Italy PII Info. Exfiltration including Codice Fiscale in DOCX Format (500 records)

File name: 256262.docx

SHA1:d46a3f5a35a4881eb0832a2b05903dadf9f4534d

SHA256:437fdd89354994ea147ef9227849ff8eab4a1bfcd4904abebc05934965478137

MD5:96c631e0b4adcc03b342cf1abc891cb2

Action 10: Italy PII Info. Exfiltration including Codice Fiscale in XML Format (500 records)

File name: 279979.xml

SHA1:ab0ceb58a32f4dbafb093101aae0ae04fe77d849

SHA256:7df55c1166edba9bb9b373207f5c099f4d105c01826eacc2397149de48725ce5

MD5:610fbdaa4c814809a6e52d5738131107

Action 11: Italy PII Info. Exfiltration including Codice Fiscale in XML Format (500 records)

File name : 279979.xml

SHA1:ab0ceb58a32f4dbafb093101aae0ae04fe77d849

SHA256:7df55c1166edba9bb9b373207f5c099f4d105c01826eacc2397149de48725ce5

MD5:610fbdaa4c814809a6e52d5738131107

Action 12: Brazil CPF Number Exfiltration XLSX Format (10 Records)

File name: 286926.xlsx

SHA1:c83c644368897850fdca56d4bbe826660cee022b

SHA256:e8a851c02f12cc6f7955e601fe551b06cb599d393086be4ea1a7d5dcceb63d93

MD5:99b9b07a284b20ea2257f1322f59e76d

Action 13: Italy PII Info. Exfiltration including Codice Fiscale in DOC Format (500 records)

File name : 296920.doc

SHA1:e45715b6f83786a43f569208d2cd6e2f9b02a9d7

SHA256:37d2ce3cfcfa502e830c6818d1cd6363f1203903e5944635808cbef5a221fc5f

MD5:043a672d86803b2e7cb803fba4360a11

Action 14: Italy PII Info. Exfiltration including Codice Fiscale in SQL Format (500 records)

File name: 297911.sql

SHA1:fb243c1ad7dfef994e156faa86da095059c400d4

SHA256:26e1f24c69e59c6a27b39561ae316074a4f0146c97d9eca453ce86b167a18073

MD5:953ef47ac19e8bd5255d6f4b81cba048

Action 15: Italy PII Info. Exfiltration including Codice Fiscale in PPT Format (500 records)

File name: 298828.ppt

SHA1:cf70e5b0c6202a54e677e6155f4268e270ceed75

SHA256:319d10c3e593c20629d50df9399d779072fa4e69da74574d30b67a02d38e49df

MD5:7fc9c19deec55c0ada63e62469f38175

Action 16: Italy PII Info. Exfiltration including Codice Fiscale in XLS Format (500 records)

File name : 307079.xls

SHA1:18505bb27638f25ace15ba21093936bd9d695373

SHA256:4fea8ee37f600bab3f1ba64bbe3f7bce26c87f45620772a6006f22b7cd25b479

MD5:f025895ecc82b3d8b910bf10d7b43f88

Action 17: Italy PII Info. Exfiltration including Codice Fiscale in XLSX Format (500 records)

File name: 307999.xlsx

SHA1:0fa028de9a5577a401fe529420ca770976989ea8

SHA256:ab62d4971a0244f01b6b4e1fe8025f492596c39dca824e975d56ab9eab22702c

MD5:3d49ff0c38486d18db98b77449f8a731

Action 18: Australia PII Exfiltration including Tax File Number (TFN) in TXT Format (20 records)

File name: 323277.txt

SHA1:fb7e98bb6f3fb0c9ef7fa510aef77c8e99d3272f

SHA256:f1cb3866dd50227b01eddb4b4677730db0ac5a617b0734e17a40cb567cbe6195

MD5:89ae7f1ea1fc3384396e91916e073bf2

Action 19: Italy PII Info. Exfiltration including Codice Fiscale in ODT Format (500 records)

File name: 343969.odt

SHA1:352a09e3f9441b61534e0d357f24ea420a2f69b9

SHA256:fe489c8eb5ad51dcc75282815750c9423f932eb751909b1a94dc44d0410edbb9

MD5:be6c0b3d0774128bda55096168c5f712

Action 20: US PII Exfiltration including SSN and Full Name in TXT Format (200 records)

File name: 350734.txt

SHA1:b25ead140fc9b52ee94578384c1e11cefe948697

SHA256:3422c22bb1884b9ac826ee8551278d89f069edcc816731ff444f745f0eed91c0

MD5:11a3fcc5bd46638c5f9c006b96492c5f

Action 21: U.K. Personally Identifiable Information (PII) Exfiltration PDF Format (25 records)

File name : 351406.pdf

SHA1:a3256d4e25ada6b0c7c91adc5b61706152f6378e

SHA256:9f40baffe32792e33c98985f4cc2bbccb51c3ca94348ce3e7c97b42f5feaea4f

MD5:8d159e57cb7e03c2ba48492ce110f8a1

Action 22: U.K. Personal Information Online Code of Practice Information Exfiltration XLSX Format (25 records)

File name: 403853.xlsx

SHA1:80dd4a3fecb71fe6c0a3a80d74bfe70325196166

SHA256:693d39873700a1434755aacfea4c043440328918f20d0bec9bb7350fd3cfcc8f

MD5:1db411802431dd590e98e148ec71936e

Action 23: Germany PII Exfiltration including German Tax ID (GTI or Steuer-IdNr.) in TXT Format (20 records)

File name: 448434.txt

SHA1:394a8ab9ef4b757a16af42089253a86ff394ef4e

SHA256:bb6c9a75f2bcca5a5fcc38476a846b0041f278b3ac9dea1c24c381d79ea81073

MD5:dacdfc7a92044f64b6077fb458f87cfd

Action 24: TR PII Exfiltration including All National ID Card Information in DOCX Format (3 records)

File name: 449728.docx

SHA1:4089db8c5474563cc3a83212813a094f61b64e4d

SHA256:8d32258f6595241fa3793661a37de3049ea780fc5e34177b43dc50df4bb06e9c

MD5:0a513d3a2f02ce687c19c36ea0a103c0

Action 25: U.K. Personal Information Online Code of Practice Information Exfiltration DOCX Format (25 records)

File name: 486040.docx

SHA1:92ba666b52d1634e529bdb1ac5a8effba4e813bf

SHA256:a6897c848647d4afae993e1f4fc8ff09352b9cb8d6603c3cbc52f0a782e96483

MD5:b50e430c323eda062683b794471535e0

Action 26: US PII Exfiltration including Social Security Number (TFN) in TXT Format (20 records)

File name: 571242.txt

SHA1:b477f8d1a1f8106bf4dc28c569ea77a2c36851a4

SHA256:4c204bb70dd4a9853fe5e03c5a60650496ca95491614a39e7cbf843863eb326c

MD5:b78bb1af0e8d41079d617dc30d0289f8

Action 27: Turkey TaxID Exfiltration DOC Format (10 Records)

File name : 579952.doc

SHA1:ce43ef6226c37e7ece3751321e58cfa1295467ae

SHA256:469f62010d110ea46b4b99cf9a09e2bbddc1c2156a37e40a235c515549bcedf8

MD5:a352262c929e7cf35a1d6ac6280ed566

Action 28: UK PII Exfiltration including National Insurance Number (NINO) and Full Name in CSV Format (1 record)

File name: 597299.yaml

SHA1:d34f0baa0fdf35df4eaeaf56cf4d2e053216a775

SHA256:beac0df7bce3ff918808d6ddde89f6ca5ffd293f3e306e961d6dce7da35e4cb7

MD5:4dd42490d0f7f1e237707c520310350c

Action 29: U.K. Personally Identifiable Information (PII) Exfiltration PNG Format (25 records)

File name : 618999.png

SHA1:6b19b8bd3d9e10f47f9c4ccd66c2bc21f4de1522

SHA256:fa00bd927535a7a4630df818a3c5942cb0dc2e960dace1dbed72042eb053de18

MD5:efe5d07e24cbfe7e15607e58b3a55343

Action 30: International Driver's License Application Data Exfiltration including PII and PCI in PDF Format

File name : 623031.pdf

SHA1:1add52bf672d4f71eb9ea58028da33e857b8a685

SHA256:43d4fe4b56b53389d4434fea3037213e96d97c6d561975c06f81dede6544474b

MD5:17f15bac04491499f13b929d3ce9f759

Action 31: Italy PII Info. Exfiltration including Codice Fiscale in TXT Format (500 records)

File name: 627222.txt

SHA1:2ccbccccbfd4489e098703dab34bb636eb3b3494

SHA256:329a7eeec3fafd98eb84b49b05a5d37948a1d745c44d6f77b0750055f5470463

MD5:3ae7cdce53a0df0ec34ace5d78535301

Action 32: US PII Exfiltration including Individual Taxpayer identification Number (ITIN) in TXT Format (2 records)

File name: 644972.txt

SHA1:881eacd2a8293d6a18fd2d5cc4962b46dff61273

SHA256:3dd9c7be199e8d4ab797d913def7cb51a6da554b8fc2a642987a0ee4b49bc199

MD5:eb6772f398b525386a413f3f374412d0

Action 33: UK PII Unique Taxpayer Reference (UTR) in TXT Format (20 records)

File name: 648173.txt

SHA1:5fca0ad6cce81d2349acf283482ce89f5018d78e

SHA256:64df282710652e2db976ee47884013df4c023479a08ae5e508614a0d7000b20c

MD5:a87f16230163e0a8e05cacfd19da0d6f

Action 34: U.K. Personal Information Online Code of Practice Information Exfiltration CSV Format (25 records)

File name: 668075.csv

SHA1:65b0b6763d6ea092532426d7f8c0ca7899603439

SHA256:7cf81df0d9a8e785f8b3481e8ee540b6d5d325260bef883e8a2e214987a71df1

MD5:06cbfa2e9eb888a7cbc953dec53295ac

Action 35: Italy PII Info. Exfiltration including Codice Fiscale in ODS Format (500 records)

File name: 697929.ods

SHA1:8c4e152ce0f8c0a6a7c33f30374024002d59e8b9

SHA256:9b9a154f2e7ecea085a791c2c12c634592f6f6c17d3005c5df8bcede348e8b89

MD5:5960434854a9c02c6d9b3f972a91f9f7

Action 36: U.K. Personally Identifiable Information (PII) Exfiltration XLSX Format (25 records)

File name: 731173.xlsx

SHA1:6a47be0fb01315faa6510fa8b4218a2a97637f43

SHA256:12f80e6635310848c1c7342702e67758cbfaf997e27bea2258b0426fe37285cf

MD5:fc37d3a2d4ac7047b2dfaed367de8098

Action 37: U.K. Personal Information Online Code of Practice Information Exfiltration PDF Format (25 records)

File name: 752201.pdf

SHA1:148fe5f9f9a3191258f60485a8efc4455d7de421

SHA256:0d86d929ca96430cbbe7050fc12bb84ce7da7e23041b4a0a073a2bade0cfd32e

MD5:a185855f36e04adf5b13c1d613b79df9

Action 38: U.K. Personally Identifiable Information (PII) Exfiltration CSV Format (25 records)

File name: 771545.csv

SHA1:556f568f3f673a3378a3d7e7dedc15e1e810ed43

SHA256:45bfa5f8e253662a9e37e02ce202e38e8f25a35640d16183bc34595604ba8496

MD5:a2a842dc69c52488b4383cc081dd4037

Action 39: Italy PII Info. Exfiltration including Codice Fiscale in HTML Format (500 records)

File name: 779393.html

SHA1:57ee5f96cf35ecbdcaca9794bff17d021efcea18

SHA256:f85364cad926726c3665032ecad82ee042b124a69de96c3abb717a720f2957fd

MD5:609789dfaeb9eff350be4443632f60a5

Action 40: U.K. Personally Identifiable Information (PII) Exfiltration DOCX Format (25 records)

File name: 792614.docx

SHA1:45859f90b9d2915ee9885da9ef02fbd411ef15f3

SHA256:48f7b45ff6c217e12397bc838b982482cdcbe7a4a5df4f2bba65852eb7da2903

MD5:07067625883aeb95b3b5454ba129f868

Action 41: Italy PII Info. Exfiltration including Codice Fiscale in PDF Format (500 records)

File name: 792996.pdf

SHA1:9a7fcfa181f6163871674a79cd34ca207b51aae9

SHA256:94140ce30e9d7e3c94138412fbcfae5edb8004bed4d52952aca6998bb9653479

MD5:6cea0cadbc8fc1f68fc8584631ee0b67

Action 42: Italy PII Info. Exfiltration including Codice Fiscale in MHT Format (500 records)

File name: 793793.mht

SHA1:1a7f78f721a59b3ae3991c3bebcafd22916cc8ca

SHA256:6f02878f4bc31945e6136c26ad9bdb6593ad63aada2f6deb0f9bd487b1e2c3b5

MD5:c929bdf32455a4d65a1f91ad6add6bbd

Action 43: Italy PII Info. Exfiltration including Codice Fiscale in PPS Format (500 records)

File name: 798288.pps

SHA1:80a0e823c06595d6b49d3a2b5de9bda25ac7fbb3

SHA256:463a1b54b7d4c84655eeba48d3b478607aa3f09f3054253a8d0d44a2d4d8c177

MD5:89c1e4ecd1f055c615e6d4786dc7bd64

Action 44: TR PII Exfiltration including National Identifier (TC Kimlik No) and Full Name in PDF Format (100 Records)

File name: 826905.pdf

SHA1:c05a0f5377e9a01d4ce42791c014949fc4a62249

SHA256:f9b4ee50c6fd27d1e4d47915697f3a39123e02d3a506e46f378c71ea3751d985

MD5:3e4459b9ee160a5fc50172b2d5708f5c

Action 45: Turkey IBAN Exfiltration DOC Format (10 Records)

File name: 831662.doc

SHA1:5cdcad0f82a38b35ce94bf05adc63edaff826237

SHA256:589374997456fc30e3e0f62aabf739eee6384f1d4f222d977d190097a88bd7a4

MD5:a1117f3a68e7fa650aaa0fec95884bf6

Action 46: TR PII Exfiltration including National Identifier, ID Card, Passport and Driver License IDs in JSON Format (1000 records)

File name: 837597.json

SHA1:64211b02ba4cc8bbc03de233f7eaa7848c4794ed

SHA256:8125c4725ec22dafa2bd91c4787822bcb0595575586fe9a6f4137645da618b4f

MD5:6941f9a60c7d9bc06515c8bda965f8fa

Action 47: Italy PII Info. Exfiltration including Codice Fiscale in CSV Format (500 records)

File name: 893939.csv

SHA1:8fbb6b916a89245bf98ab189ff8314381d5c4c53

SHA256:c8670bfac06378c332f8cb217deeb66f7efb4cee31f746b1c740886d25de463d

MD5:a2433285cb67c78659567859881d05ed

Action 48: Italy PII Info. Exfiltration including Codice Fiscale in RTF Format (500 records

File name: 894894.rtf

SHA1:9f0516d96e3507c15cf34553efc82be525d8c557

SHA256:e0023d2c32570e6a91955474c3b3fb230d18cac275729e1ac18a09b34b4c7390

MD5:7d4a163e3c1ed4e3e0a1cbd481414d4b

Action 49: Italy PII Info. Exfiltration including Codice Fiscale in PPTX Format (500 records)

File name: 948383.pptx

SHA1:2d60a126b7c656022d8083f0329811b7eea3116c

SHA256:0ab9320e9ff0946a25dd06670ae3019268e6e6aa2c2c0345cacdcfe6c0cfff5c

MD5:938886bcdc316bc93fe9880fb69439da

Action 50: Canada PII Exfiltration including Social Insurance Number (SIN) in TXT Format (20 records)

File name: 993864.txt

SHA1:742f930659f93d819230f74822e4a94565e9de4d

SHA256:e25301f437e5035ea2b661638c2955bddee66bc6254f7198d7bfc7789ec52093

MD5:5086a4e7f170f29bbaeef277346772a7

Action 51: Italy PII Info. Exfiltration including Codice Fiscale in PPSX Format (500 records)

File name: 997666.ppsx

SHA1:a54cb97de7f782ec2a1a2a6f77ae87c88e48d388

SHA256:0fbf3dd03561448b382d15fa2d5e5003c17578e411ef4ac7d3af27fa5ac9f743

MD5:1dc03923479943114acb34eb02e76447

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis.

4. PDF Format Data Exfiltration Campaign

This campaign includes exfiltrating documents with PDF format.

#	Actions	Descr	Action
1	United Arab Emirates Financial Data Information Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .pdf format: Name Surname, Emirates ID, IBAN, Credit Card Number.	**Not Blocked**
2	Brazil CPF Number Exfiltration PDF Format (10 Records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .pdf format: Name Surname, Emirates ID, IBAN, Credit Card Number.	**Not Blocked**
3	UK PCI and PII Information Exfiltration including NINO, Credit Card, Address,Phone Encrypted PDF Format (25 records)	This attack includes uploading a document that contains the following Financial Data Information specialized for United Arab Emirates in .pdf format: Name Surname, Emirates ID, IBAN, Credit Card Number.	**Not Blocked**
4	Spain PCI and PII Info. Exfiltration including Full Credit Card Info in PDF Format (50 records)	This attack includes uploading a document that contains the following CPF number specialized for Brazil in .pdf format: CPF, Name, Date.	**Not Blocked**
5	TR PCI and PII Exfiltration including TC Kimlik No Credit Card in PDF Format (20 records)	This attack includes uploading a document that contains the following CPF number specialized for Brazil in .pdf format: CPF, Name, Date.	**Not Blocked**
6	U.K. Personally Identifiable Information (PII) Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following CPF number specialized for Brazil in .pdf format: CPF, Name, Date.	**Not Blocked**
7	U.K. Financial Data Information Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: full name, NINO, credit card type, credit card number, expire date, CVV2 number, street address, town, region, postcode, country and geolocation information consisted of latitude and longitude.	**Not Blocked**
8	CMS 838 MEDICARE CREDIT BALANCE REPORT Exfiltration PDF Format	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: full name, NINO, credit card type, credit card number, expire date, CVV2 number, street address, town, region, postcode, country and geolocation information consisted of latitude and longitude.	**Not Blocked**
9	Italy PCI and PII Info. Exfiltration including Full	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII)	**Not Blocked**

	Credit Card Info in PDF Format (25 records)	specialized for United Kingdom in .pdf format: full name, NINO, credit card type, credit card number, expire date, CVV2 number, street address, town, region, postcode, country and geolocation information consisted of latitude and longitude.	
10	U.K. Access to Medical Reports Act Information Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for SPAIN in .PDF format. PCI data includes Full Credit Card. This file also contains PII, which is any data that could potentially identify a specific individual. This file includes the following information for 50 persons: Primer Apellido,Segunda Apellido,Nombre, Nomero de Tarjeta,Fecha de Vencimiento,Codigo de Validacion,Marca,Banco.	**Not Blocked**
11	Spain PCI and PII Info. Exfiltration including DNI, CC, IBAN PDF Format (25 records)	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for SPAIN in .PDF format. PCI data includes Full Credit Card. This file also contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
12	International Driver's License Application Data Exfiltration including PII and PCI in PDF Format	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for SPAIN in .PDF format. PCI data includes Full Credit Card. This file also contains PII, which is any data that could potentially identify a specific individual.	**Not Blocked**
13	EDI 837 Healthcare Medical Claims Exfiltration PDF Format	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for Turkey in PDF format: first name, last name, TC kimlik no (national identifier), birth date, birth place, credit card number, expire date, CVV2 number, card issuer bank and credit card type.	**Not Blocked**
14	UK PCI and PII Information Exfiltration including NINO, Credit Card, Address,Phone Unselectable PDF Format (25 records)	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for Turkey in PDF format: first name, last name, TC kimlik no (national identifier), birth date, birth place, credit card number, expire date, CVV2 number, card issuer bank and credit card type.	**Not Blocked**
15	Mexico PCI and PII Info. Exfiltration including CURB CC and CLABE in PDF Format (50 records)	This attack includes uploading a document that contains the following Payment Card Industry (PCI) data and Personally Identifiable Information (PII) specialized for Turkey in PDF format: first name, last name, TC kimlik no (national identifier), birth date, birth place, credit card number, expire date, CVV2 number, card issuer bank and credit card type.	**Not Blocked**

16	Spain PCI and PII Info. Exfiltration including DNI and Full Name in PDF Format (50 records)	This attack includes uploading a document that contains the following U.K. Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: name, passportnumber, national health service.	**Not Blocked**
17	Troy Card Exfiltration PDF Format (10 Records)	This attack includes uploading a document that contains the following U.K. Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: name, passportnumber, national health service.	**Not Blocked**
18	U.K. Personal Information Online Code of Practice Information Exfiltration PDF Format (25 records)	This attack includes uploading a document that contains the following U.K. Personally Identifiable Information (PII) specialized for United Kingdom in .pdf format: name, passportnumber, national health service.	**Not Blocked**
19	Italy PII Info. Exfiltration including Codice Fiscale in PDF Format (500 records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .pdf format: name, swiftcode, IssuingNetwork, card number.	**Not Blocked**
20	TR PII Exfiltration including National Identifier (TC Kimlik No) and Full Name in PDF Format (100 Records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .pdf format: name, swiftcode, IssuingNetwork, card number.	**Not Blocked**
21	UK PCI and PII Information Exfiltration including NINO, Credit Card, Address,Phone PDF Format (25 records)	This attack includes uploading a document that contains the following U.K. Financial Data Information specialized for United Kingdom in .pdf format: name, swiftcode, IssuingNetwork, card number.	**Not Blocked**
Overall Campaign Result			**Not Blocked**

Below output is showing the actions which are not blocked:

Action 1: United Arab Emirates Financial Data Information Exfiltration PDF Format (25 records)

File name: 227448.pdf

SHA1:8e3db48339a77fe8f196f404557b90cc416bd74b

SHA256:fd77ed25f2345c1d23cf18f059dd1073b149ef0152bbc1e03fd167146d1d01eb

MD5:5cbdbc2d195832262eadff65e390bfbf

Action 2: Brazil CPF Number Exfiltration PDF Format (10 Records)

File name: 248558.pdf

SHA1:704b1ee938e73f06a758bc4cc9b42de90c6ce15b

SHA256:dd8853f88be63e88e006e71999e40a503d7b8afe77e101019ee713fbb04a2fb7

MD5:dde0d56c598af7c390e74a3df257a929

Action 3: UK PCI and PII Information Exfiltration including NINO, Credit Card, Address,Phone Encrypted PDF Format (25 records)

File name: 250297.pdf

SHA1:e4f4bbb2405daf6f906e8a8780f6e7603216d2fb

SHA256:d49ad4258c41e2b00429957e345c6dd8018b4f0ab4fae8097506872d2ce49a42

MD5:643936330e7e1597bde929ca555040ad

Action 4: Spain PCI and PII Info. Exfiltration including Full Credit Card Info in PDF Format (50 records)

File name: 260438.pdf

SHA1:04f3ad335a1fecf65dd2e83062d7d48b1f2fb349

SHA256:bb743855c3f0f9495e323c68150630a35de2ecc89649b692c31f8bcc8e59beb2

MD5:ba28d529e4a9e3d032a091e631792f68

Action 5: TR PCI and PII Exfiltration including TC Kimlik No Credit Card in PDF Format (20 records)

File name: 329883.pdf

SHA1:3d23ef706dbdc697bb629587e90f8c7b8dcb20f7

SHA256:87096dce79f5820f79978a46a5d760570e9fc3af62d879de3b62719387acec3c

MD5:aea272febae1ba92c6b3004c33b4b455

Action 6: U.K. Personally Identifiable Information (PII) Exfiltration PDF Format (25 records)

File name: 351406.pdf

SHA1:a3256d4e25ada6b0c7c91adc5b61706152f6378e

SHA256:9f40baffe32792e33c98985f4cc2bbccb51c3ca94348ce3e7c97b42f5feaea4f

MD5:8d159e57cb7e03c2ba48492ce110f8a1

Action 7: U.K. Financial Data Information Exfiltration PDF Format (25 records)

File name: 372419.pdf

SHA1:26d02743bde6fddaf7533c00a4be590ce95f5d92

SHA256:982df81c3d7af02ca0bc0b75b892a8dc13573d74d4ef4797e83ed3a1d14067aa

MD5:419580957da7a5789b8d54a109c32eab

Action 8: CMS 838 MEDICARE CREDIT BALANCE REPORT Exfiltration PDF Format

File name: 389024.pdf

SHA1:eda3ea0b7bf5a3d76daa573737c89e79babf4e06

SHA256:4f0577863a80c6b8b1315d1a6dbf6cccdbd0485fab7c20dbde2deb4c305187e3

MD5:a411144edb27ab44f2703511f85deef3

Action 9: Italy PCI and PII Info. Exfiltration including Full Credit Card Info in PDF Format (25 records)

File name: 406029.pdf

SHA1:c028523d429bfe3119b28456eaffcde81df657ce

SHA256:0c4dcb7d5fd330dde485791aab35cd96d13646722b18beabf6ffc32fb11bcc2f

MD5:7f75288880be4689aa6697fed6d83309

Action 10: U.K. Access to Medical Reports Act Information Exfiltration PDF Format (25 records)

File name: 408357.pdf

SHA1:8d97cc210c9fafec5e53ddedc4120434e043f808

SHA256:0b8fa61272091470aa735cc44cfe8e5ed4daa5dd2051f75d0de7a46f78a91649

MD5:34ffde57de6d3f910e7704d03d8102fd

Action 11: Spain PCI and PII Info. Exfiltration including DNI, CC, IBAN PDF Format (25 records)

File name: 542708.pdf

SHA1:714455d90300d562f779a6197b737fcf9b5b7f35

SHA256:7145fa0115627447b82deb1ce5ccabae1cc61376c20183b95c3a6e2d3a4e3ebf

MD5:a2fe995deb870ac17e98edb93c41657f

Action 12: International Driver's License Application Data Exfiltration including PII and PCI in PDF Format

File name: 623031.pdf

SHA1:1add52bf672d4f71eb9ea58028da33e857b8a685

SHA256:43d4fe4b56b53389d4434fea3037213e96d97c6d561975c06f81dede6544474b

MD5:17f15bac04491499f13b929d3ce9f759

Action 13: EDI 837 Healthcare Medical Claims Exfiltration PDF Format

File name: 624895.pdf

SHA1:da5c95193a2870ade4ea5212ba3d404c8be8b840

SHA256:b40706b3d0017b11d5c51d7233b52d749e9255abc7f09fc8e90d987a7ee514a7

MD5:c53a9f8f7be635dca0c2b31dd9d8b746

Action 14: UK PCI and PII Information Exfiltration including NINO, Credit Card, Address,Phone Unselectable PDF Format (25 records)

File name: 643744.pdf

SHA1:4afe3fe43e796dcc12db87fc99ef62fe0b288f05

SHA256:2eae26d4c19db153b932e074ff41eb097172402da94ae57695c497b53cae6f83

MD5:ebc3dd6866c56507c0b9bc3aae8f1f59

Action 15: Mexico PCI and PII Info. Exfiltration including CURB CC and CLABE in PDF Format (50 records)

File name: 671459.pdf

SHA1:51675deb659688e312ca63aa2cbb8c2e4d355b3d

SHA256:2135e19c4bb7f21f386186db784d8f0e000c1058b665a19d4632b197feb3abca

MD5:b9ec607c0e8e76512ee42f395068c787

Action 16: Spain PCI and PII Info. Exfiltration including DNI and Full Name in PDF Format (50 records)

File name: 714276.pdf

SHA1:d383eb5a999f951aae49b16fc139a6b022c387c5

SHA256:8d8383ed3389b20077a1c3183603f9efd3376b0a533a56dd167cc5e347a9648c

MD5:030cbbf4ac0517a609ee63eddb2990d4

Action 17: Troy Card Exfiltration PDF Format (10 Records)

File name: 717652.pdf

SHA1:f855f669979f9d3207149181502b496164ed02ca

SHA256:f03ba352ec890527f1fd397df4f4afe9839127a05d2d938735a569492c0b6df7

MD5:ba0c26107402e5d53fb5e0f010a0bf8b

Action 18: U.K. Personal Information Online Code of Practice Information Exfiltration PDF Format (25 records)

File name: 752201.pdf

SHA1:148fe5f9f9a3191258f60485a8efc4455d7de421

SHA256:0d86d929ca96430cbbe7050fc12bb84ce7da7e23041b4a0a073a2bade0cfd32e

MD5:a185855f36e04adf5b13c1d613b79df9

Action 19: Italy PII Info. Exfiltration including Codice Fiscale in PDF Format (500 records)

File name: 792996.pdf

SHA1:9a7fcfa181f6163871674a79cd34ca207b51aae9

SHA256:94140ce30e9d7e3c94138412fbcfae5edb8004bed4d52952aca6998bb9653479

MD5:6cea0cadbc8fc1f68fc8584631ee0b67

Action 20: TR PII Exfiltration including National Identifier (TC Kimlik No) and Full Name in PDF Format (100 Records)

File name: 826905.pdf

SHA1:c05a0f5377e9a01d4ce42791c014949fc4a62249

SHA256:f9b4ee50c6fd27d1e4d47915697f3a39123e02d3a506e46f378c71ea3751d985

MD5:3e4459b9ee160a5fc50172b2d5708f5c

Action 21: UK PCI and PII Information Exfiltration including NINO, Credit Card, Address,Phone PDF Format (25 records)

File name: 894785.pdf

SHA1:fa5050ac1220c222d2c52df65f1ead00e5fc7ea4

SHA256:69cad62a2bcdfe319f4d531ccf5b9b45cba1f82d4c60203ae1e8dadbe25c1f8c

MD5:ce77cabc5de5c4802fa4d1cfc5575708

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis.

5. Payment Card Industry (US) Data Exfiltration Campaign

This campaign includes exfiltrating documents that contains Payment Card Industry (PCI) data.

#	Actions	Description	Action
1	US PII and PCI Exfiltration including SSN, CCN, Expire Date and Address in TXT Format (100 records)	This attack includes uploading a document that contains the following PII (Personally Identifiable Information) and PCI (Payment Card Industry) information specialized for United States in .txt format: Full name, Social Security Number (SSN), Credit Card Number (CNN), expire date and address.	**Not Blocked**
Overall Campaign Result			**Not Blocked**

Action 1: US PII and PCI Exfiltration including SSN, CCN, Expire Date and Address in TXT Format (100 records)

File name: 112895.txt

SHA1:cf54eddf33724446cf3146b5a04a1b1b493f2398

SHA256:d4d84ab4273abe4e69a74e6400d699b11ed780207744a39ccb265788645cdea3

MD5:2a8b434ece5e1f5a7bc15071af2898a0

Prevention: Kindly analyze and verify above IOC on security controls. Fine tune the detection rules based on the analysis..

Appendix A | Risk Definitions

Throughout the document, each action for every campaign has been represented according to their respective execution status:

Actions Status	Description
Not Blocked	These actions were not blocked by the security controls solutions
Blocked	These actions were blocked by the security controls solutions
Not Tested	These actions were not tested due to privileges/config requirement doesn't match.

Appendix B | Tool Usage

The following tools were utilized during the assessment:

Tool	Description
Picus	To validate the security controls by simulating real-world ransomware threats.

Appendix C | Eventus Contact Information

Please contact Eventus with any questions regarding the findings, analysis, or recommendations contained in this report.

1. Akshay Kathavale
   Account Manager
   Email: akshay.kathavale@eventustechsol.com
   Mobile: +91- 8446164163

2. Pravin Singh
   Security Specialist
   Email: pravin.singh@eventustechsol.com
   Mobile: +91-7208420701

3. Nikhil Raut
   Security Delivery Lead
   Email: nikhil.raut@eventustechsol.com
   Mobile: +91-8956652763

4. Jay Thakker
   Practice Head
   Email: jay.thakker@eventustechsol.com
   Mobile: +91-7977020491

Disclaimer

It should be noted that it is not possible to completely guarantee the security of any network, system, or application, and as such this report does not constitute and should not be taken as a guarantee of the security of the tested systems and applications. It should also be noted that whilst some risks may be reported as high from a technical perspective, from a business perspective it may be considered acceptable. Also, from the mitigation perspective it is expected to fix the vulnerability throughout the application and not only on reported instances.