ALPHV AKA BLACKCAT WITH NEW ATTACK STRATEGY

RANSOMWARE GANG

CRYPTO VIRUS, LOADER, STEALER, TROJAN, FILES LOCKER

Vairav Advisory Report

14th July 2023

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 014441540

Mobile: +977-9820105900

Email: mail@vairav.net

Summary

ALPHV, also known as BlackCat, the well-known ransomware organization, claimed responsibility for a specific attack on Bangladesh Krishi Bank. On July 7, 2023, ALPHV announced that they had successfully infiltrated the bank's security, getting access to critical data, and causing the bank's operations to be completely paralyzed. Since then, cyber security researchers have identified evidence of additional malicious actions linked to the BlackCat alias ALPHV ransomware gang. The malware was distributed via cloned respectable company websites, including a prominent file-transferring service called WinSCP. Furthermore, BlackCat was seen using SpyBoy Terminator to undermine the effectiveness of anti-malware protection methods.

Key Points

- The study focuses on malicious groups' (BlackCat) use of malvertising to propagate malware via cloned webpages, particularly emphasizing the WinSCP utility.
- To drive victims into paying the ransom, it employs triple extortion.
- BlackCat has ties to two defunct RaaS organizations, DarkSide and BlackMatter, demonstrating their use of established networks and substantial expertise in the RaaS industry.
- It targets organizations in various industries, including finance, professional services, legal services, technology, energy, health care, and manufacturing.
- Its most used tools are: BlackCat, GO Simple Tunnel, LaZagne, MEGAsync, Mimikatz, PsExec, WebBrowserPassView.

Introduction of Cyber Adversary

ALPHV is a ransomware-as-a-service (RaaS) gang that also goes by the names ALPHV-ng, BlackCat, and Noberus. ALPHV has emerged as a key factor in the sphere of cybercrime since its inception in November 2021, deploying innovative tactics and inflicting extensive damage across numerous businesses. ALPHV runs under the RaaS umbrella, providing affiliates looking to conduct ransomware operations with a highly adaptable and adjustable platform. Affiliates from other RaaS companies have been tempted by this technique by the promise of a hefty 90% return and the capacity to perform complex attacks with relative simplicity. BlackCat, a strain of ransomware notorious for its sophistication and evasive qualities, is at the center of ALPHV's arsenal. BlackCat is built to be durable, making typical security measures difficult to remove and disable. It utilizes numerous approaches like changing system files and settings to achieve persistence within the infiltrated network.

BlackCat's ransom demands have reached astonishing proportions, with the largest documented at $14 million. While incentives are given for early payment, organizations must carefully examine the dangers and ethical consequences of caving to ransom demands. The recent breach of Bangladesh Krishi Bank highlighted the significance of ALPHV's actions. ALPHV successfully entered the bank's network, remaining unnoticed for 12 days while methodically studying internal documents and extracting over 170GB of important data. Among the exposed data are extremely sensitive financial records, personnel information, and the bank's SQL backup. The effects of this breach go beyond the bank, possibly revealing personal information and having long-term consequences for both the impacted individuals and the institution.

Tactics, Techniques, and Procedure

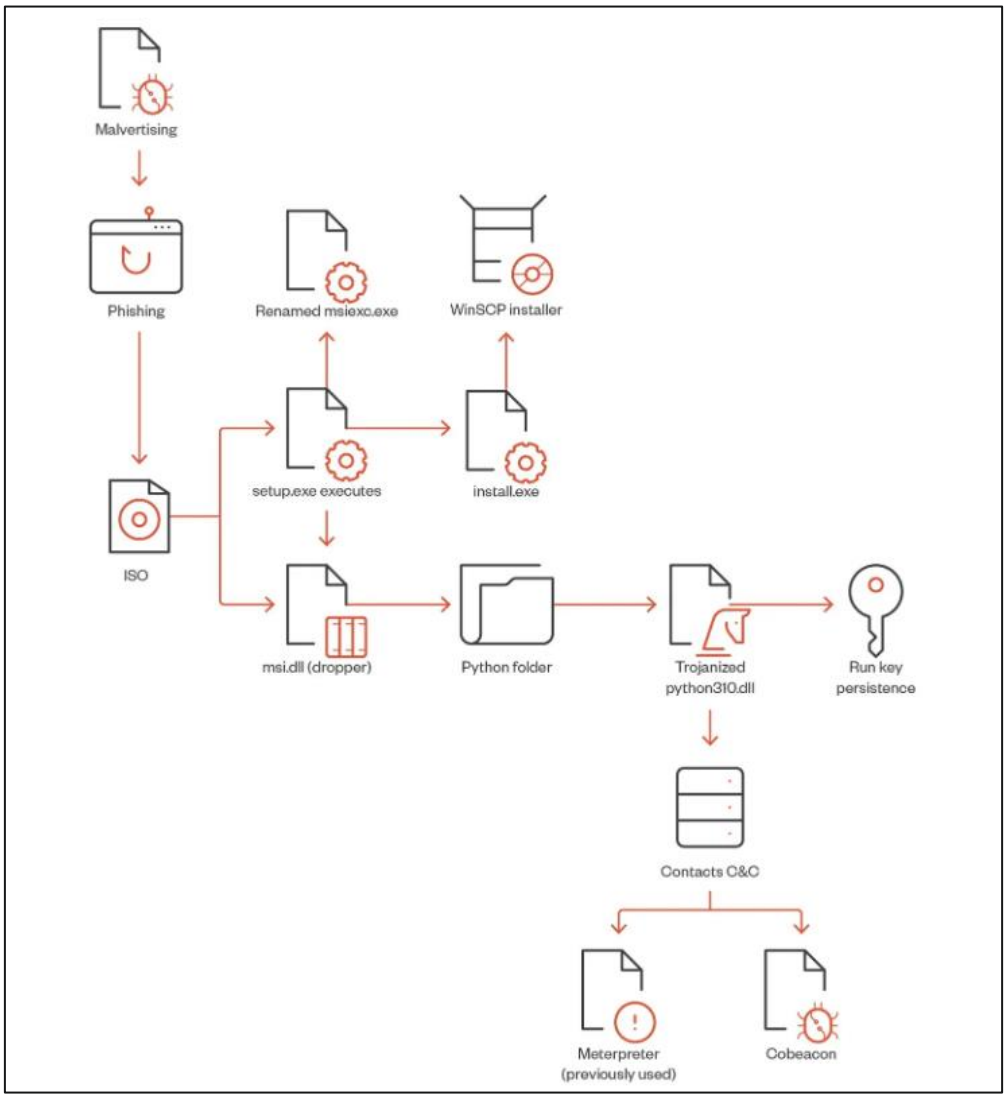


Figure 1: Infection chain of the observed attack (Trend Micro, 2023).

Malicious actors used malvertising tactics to spread malware via legitimate organizations' duplicated websites. They specifically targeted a webpage affiliated with WinSCP, a well-known open-source Windows file transfer program. Malware distributors make use of advertising networks like Google ads, which allow businesses to display customized advertisements to increase traffic and revenue. Malvertising is a technique used by malware distributors to display harmful advertising that tricks unwary search engine users into downloading malware.

The several unauthorized and malicious actions found within their network are:

- Steal top-level administrator privileges, which were then used for unauthorized purposes.
- Attempts to develop persistence and acquire backdoor access to the customer environment by remote management solutions such as AnyDesk.
- Attempts to obtain credentials and gain unauthorized access to backup servers.

Infection chain

The infection process begins when an individual searches for “WinSCP Download” on a search engine. Malicious advertising for the WinSCP program displays above the organic search results. When the user clicks on the ad, they are sent to a dubious website that offers a lesson on automating file transfers with WinSCP. The user is subsequently forwarded from this first page to a cloned WinSCP download page hosted on the domain winsccp[.]com.

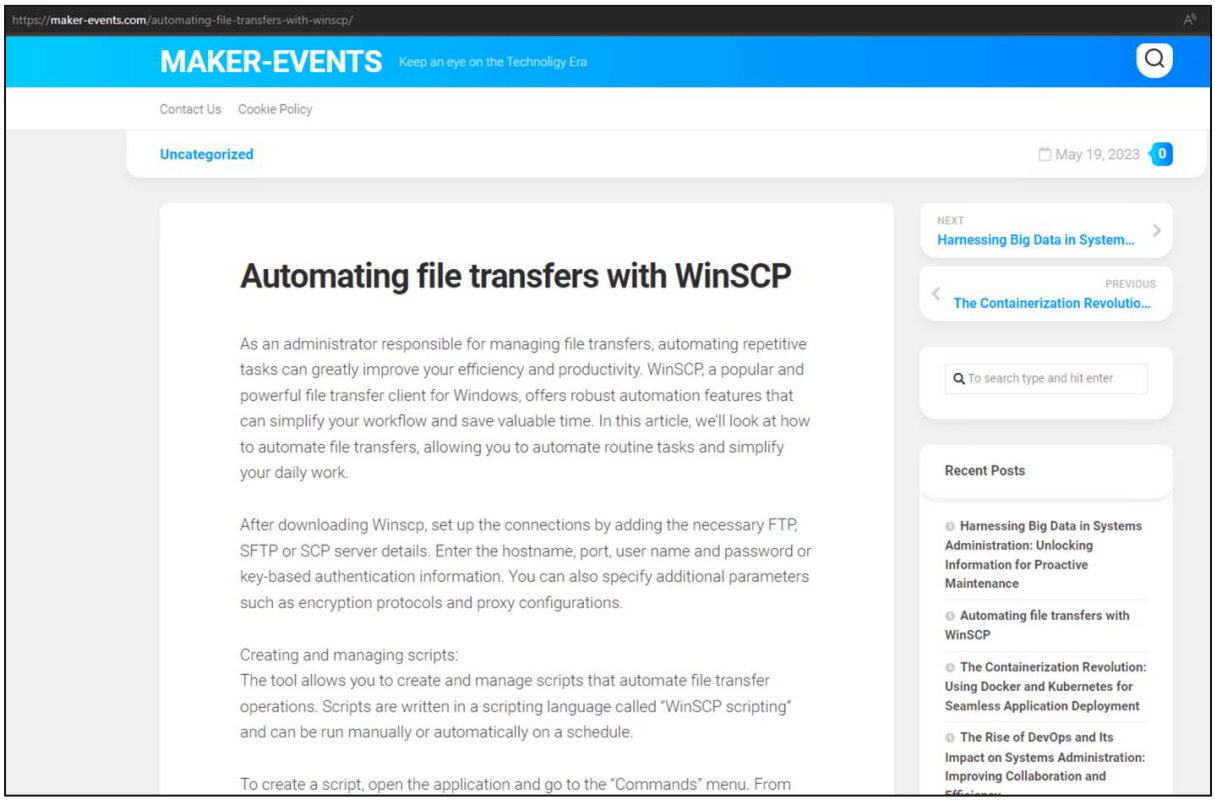


Figure 2: A malvertisement from a suspicious site.

An ISO file is downloaded when you click this page's "Download" button. The ISO file is received from hxxps://events.drdivyaclinic[.]com, an infected WordPress webpage. It's worth mentioning that the malicious actor recently changed the URL of their final payload to use the file-sharing site 4shared.

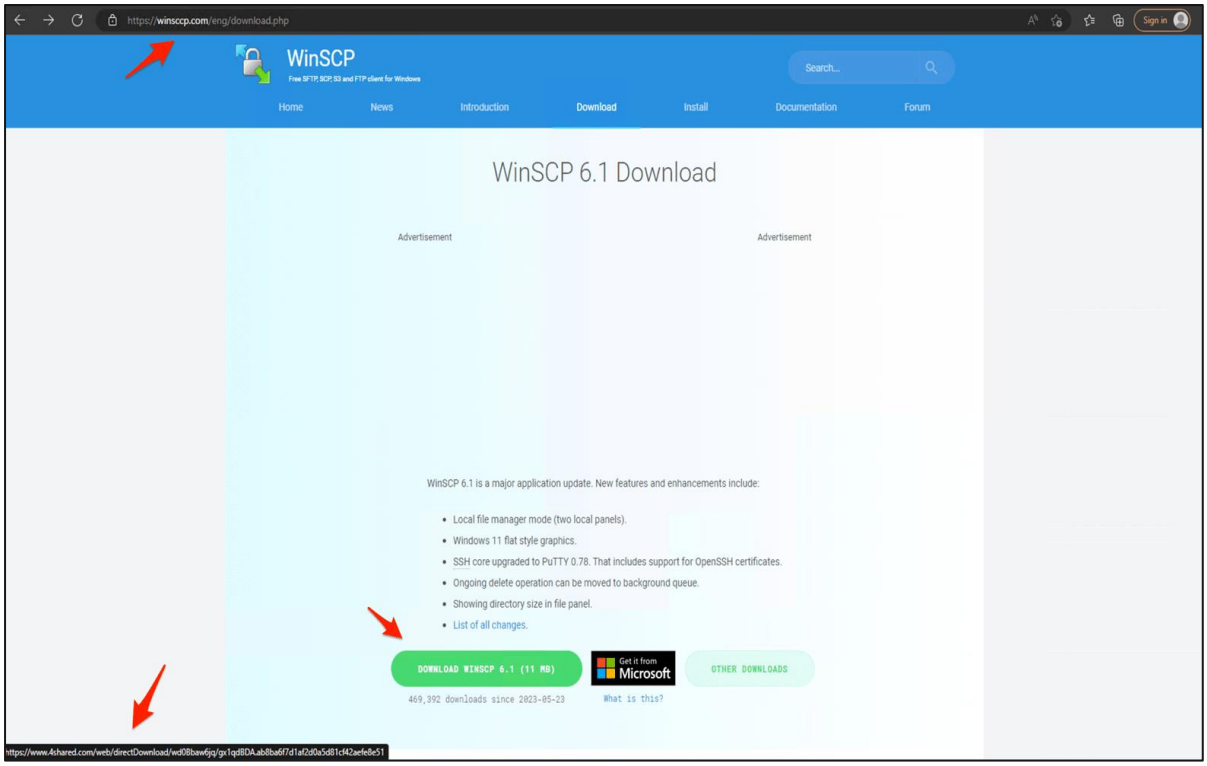
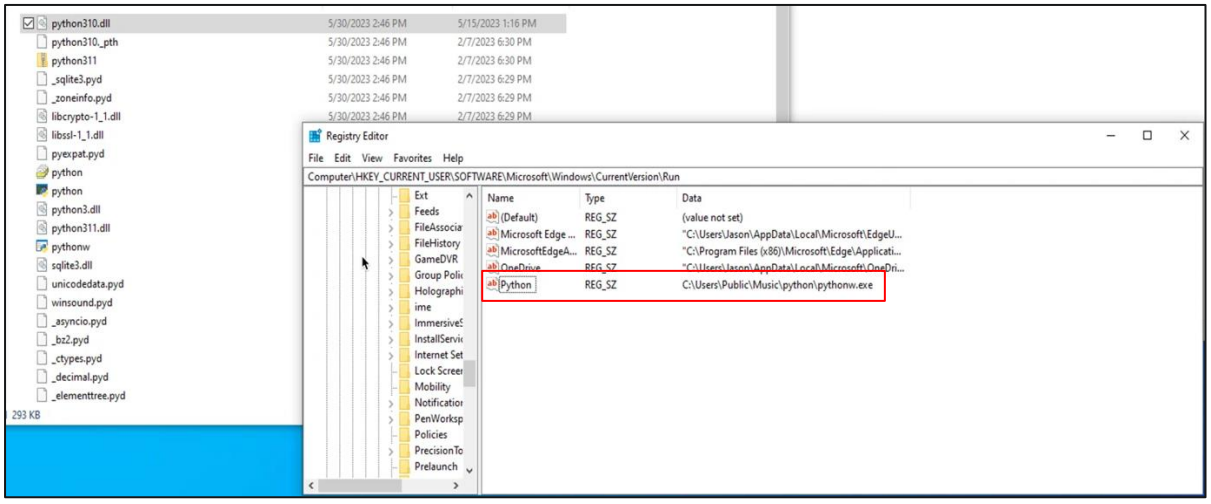


Figure 3: Download the site of malware.

The total infection route consists of sending the first loader, retrieving the bot core, and finally releasing the payload, which is usually a backdoor. When the ISO is mounted, it contains two files: setup.exe and msi.dll. The specifics for these two files:

- **Setup.exe:** A renamed msiexec.exe executable.
- **Msi.dll:** A delayed-loaded DLL (loaded only when a user's code attempts to reference a symbol included inside the DLL) that will serve as a dropper for a genuine WinSCP installation and a malicious Python execution environment responsible for obtaining Cobalt Strike beacons.

When setup.exe is run, it calls msi.dll, which then extracts a Python folder from the DLL RCDATA area as a true installer for WinSCP to be installed on the PC. Python3.10 will be installed twice as a legal Python installation in %AppDataLocal%\Python-3.10.10 and once as a trojanized python310.dll installation in %Public%\Music\python. Finally, the DLL will establish a persistence mechanism that will generate a run key called “Python” with the value C:\Users\Public\Music\python\pythonw.exe.



When the program pythonw.exe is launched, it loads a modified/trojanized obfuscated python310.dll with a Cobalt Strike beacon that connects to a command-and-control server. The machine also had many scheduled processes that executed batch files for persistence. These batch files run Python programs that result in the execution of Cobalt Strike beacons in memory. Surprisingly, the Python scripts employ the marshal module to run a pseudo-compiled (.pyc) code that downloads and executes the malicious beacon module in memory. The anti-antivirus or anti-endpoint detection and response (EDR) SpyBoy terminator is used to tamper with agent protection. They utilized the PuTTY Secure Copy client (PSCP) to transmit the acquired information to exfiltrate the customer data.

Investigating one of the threat actor's C&C domains led to the identification of a possibly associated Cl0p ransomware file. After the threat actors had downloaded the important data from the victim, they threatened them to pay the ransom amount, or else they would publicize the sensitive data of the compromised infrastructure.

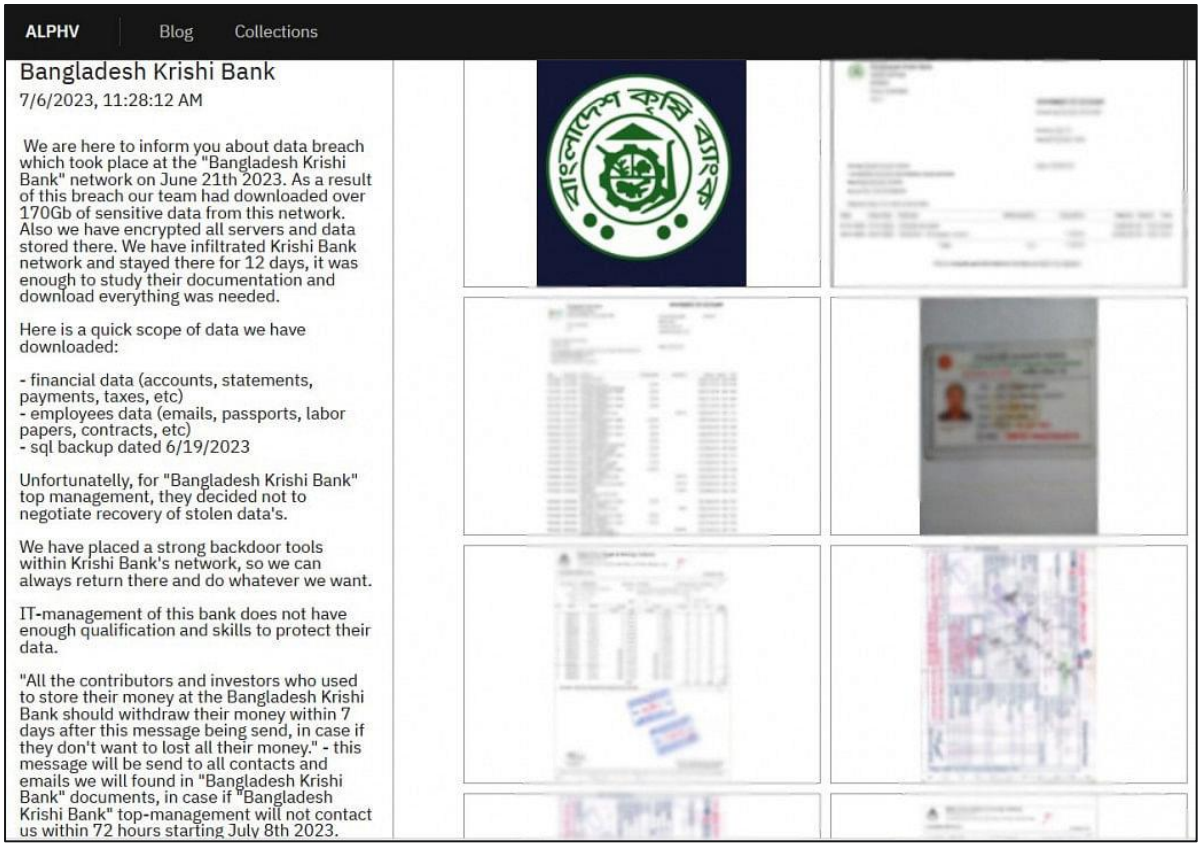


Figure 4: Message to Bangladesh Krishi Bank by BlackCat.

Detection

For each attack approach listed, below is a full description of detection and threat-hunting rules and processes:

1. AdFind

AdFind is used to retrieve and show information from Active Directory environments. They explicitly retrieve information on the operating system by using:

```
adfind.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName
```

Detection: Monitor for suspicious command-line executions containing the “adfind.exe” command, specifically targeting Active Directory (AD) environments.

Rule:

```
title: Suspicious AdFind Execution
id: 75df3b17-8bcc-4565-b89b-c9898acef911
status: experimental
description: Detects the execution of a AdFind for Active Directory enumeration
references:
  - https://social.technet.microsoft.com/wiki/contents/articles/7535.adfind-command-examples.aspx
  -https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/fin6/Emulation_Plan/Phase1.md
  - https://thedfirreport.com/2020/05/08/adfind-recon/
author: FPT.EagleEye Team, omkar72, oscd.community
date: 2020/09/26
modified: 2021/05/12
tags:
  - attack.discovery
  - attack.t1018
  - attack.t1087.002
  - attack.t1482
  - attack.t1069.002
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    CommandLine|contains:
      - 'objectcategory'
      - 'trustdmp'
      - 'dcmodes'
      - 'dclist'
      - 'computers_pwdnotreqd'
    Image|endswith: '\adfind.exe'
  condition: selection
falsepositives:
  - Administrative activity
level: medium
```

Threat Hunting:

- Inspect “adfind.exe” for instances in which it is used to extract password hashes, user accounts, or other sensitive information.
- Check command outputs and parameters for any unusual or suspicious patterns.

2. PowerShell Get-ADUser

The threat actor gathers user data using the “Get-ADUser” PowerShell cmdlet and saves it as a CSV file. A few of the attributes they get are EmailAddress, GivenName, Surname, DisplayName, sAMAccountName, Title, Department, OfficePhone, MobilePhone, Fax, Enabled, and LastLogonDate.

Detection: Keep an eye out for PowerShell executions that utilize the “Get-ADUser” cmdlet with an unusually large number of property options.

Rule:

```
title: AD User Enumeration
id: ab6bffca-beff-4baa-af11-6733f296d57a
description: Detects access to a domain user from a non-machine account
status: experimental
date: 2020/03/30
modified: 2021/08/09
author: Maxime Thiebaut (@0xThiebaut)
references:
  - https://www.specterops.io/assets/resources/an_ace_up_the_sleeve.pdf
  - http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html
  - https://docs.microsoft.com/en-us/windows/win32/adschema/attributes-all # For further investigation of the accessed properties
tags:
  - attack.discovery
  - attack.t1087       # an old one
  - attack.t1087.002
logsource:
  product: windows
  service: security
  definition: Requires the "Read all properties" permission on the user object to be audited for the "Everyone" principal
detection:
  selection:
    EventID: 4662
    ObjectType|contains: 'bf967aba-0de6-11d0-a285-00aa003049e2'
    # Using contains as the data commonly is structured as "%{bf967aba-0de6-11d0-a285-00aa003049e2}"
    # The user class (https://docs.microsoft.com/en-us/windows/win32/adschema/c-user)
  filter:
    - SubjectUserName|endswith: '$' # Exclude machine accounts
    - SubjectUserName|startswith: 'MSOL_' # https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions#ad-ds-connector-account
  condition: selection and not filter
falsepositives:
  - Administrators configuring new users.
level: medium
```

Threat Hunting:

- Search for instances where “Get-ADUser” is used with the “-Filter *” option and properties such as “EmailAddress”, “GivenName”, “Surname”’ etc. Inspect the output for potential unauthorized data exfiltration or reconnaissance.

3. AccessChk64

To inspect permissions on files, folders, registry keys, processes, services, shares, semaphores, and other objects described in the Windows Object Manager, the command-line utility AccessChk64 is used.

Detection: Monitor command-line executions containing the “accesschk64.exe” command.

Rule:

```
title: Permission Check Via Accesschk.EXE
id: c625d754-6a3d-4f65-9c9a-536aea960d37
status: test
description: Detects the usage of the "Accesschk" utility, an access and privilege audit tool developed by SysInternal and often being abused by attacker to verify process privileges
references:
  - https://speakerdeck.com/heirhabarov/hunting-for-privilege-escalation-in-windows-environment?slide=43
  - https://www.youtube.com/watch?v=JGs-aKf2OtU&ab_channel=OFFZONEMOSCOW
  -https://github.com/carlospolop/PEASS-ng/blob/fa0f2e17fbc1d86f1fd66338a40e665e7182501d/winPEAS/winPEASbat/winPEAS.bat
  - https://github.com/gladiatx0r/Powerless/blob/04f553bbc0c65baf4e57344deff84e3f016e6b51/Powerless.bat
author: Teymur Kheirkhabarov (idea), Mangatas Tondang, oscd.community, Nasreddine Bencherchali (Nextron Systems)
date: 2020/10/13
modified: 2023/02/20
tags:
  - attack.discovery
  - attack.t1069.001
logsource:
  product: windows
  category: process_creation
detection:
  selection_img:
    - Product|endswith: 'AccessChk'
    - Description|contains: 'Reports effective permissions'
    - Image|endswith:
      - '\accesschk.exe'
      - '\accesschk64.exe'
    - OriginalFileName: 'accesschk.exe'
  selection_cli:
    CommandLine|contains: # These are the most common flags used with this tool. You could add other combinations if needed
      - 'uwcqv '
      - 'kwsu '
      - 'qwsu '
      - 'uwdqs '
  condition: all of selection*
fields:
  - IntegrityLevel
  - Product
  - Description
  - CommandLine
```

```
falsepositives:
   - System administrator Usage
level: medium
```

Threat Hunting:

- Look for cases where “accesschk64.exe” is used to verify access rights and security permissions. Look for patterns of privilege escalation attempts, unusual privilege enumeration, or the detection of weak access control settings.

4. findstr

The threat actor searches through the XML files in a specified directory for the string “cpassword” using the Windows “findstr” command-line tool. This suggests a possible effort to locate Group Policy Preferences using out-of-date password-storing techniques.

Detection: Monitor command-line executions containing the “findstr” command targeting specific file paths containing the passwords.

Rule:

```
title: Findstr Suspicious ParentCommandLine
id: ccb5742c-c248-4982-8c5c-5571b9275ad3
related:
   - id: fe63010f-8823-4864-a96b-a7b4a0f7b929
     type: derived
status: experimental
description: Detects findstring commands with a suspicious ParentCommandLine
references:
   -https://github.com/redcanaryco/atomic-red-
team/blob/02cb591f75064ffe1e0df9ac3ed5972a2e491c97/atomics/T1057/T1057.md#atomic-test-6---discover-specific-process---
tasklist
author: frack113
date: 2023/07/06
tags:
   - attack.discovery
   - attack.t1057
logsource:
   category: process_creation
   product: windows
detection:
   selection_findstr_img:
      - Image|endswith: '\findstr.exe'
      - OriginalFileName: 'FINDSTR.EXE'
   selection_findstr_parent:
      ParentCommandLine|contains: 'tasklist'
   filter_optional_httpd:
      CommandLine|contains: 'httpd.exe'
   condition: all of selection_findstr_* and not 1 of filter_optional_*
falsepositives:
   - Unknown
level: medium
```

Threat Hunting: Look for instances where the “findstr” command is used to look for certain strings, such as “cpassword”, in XML files at important points. Look at these situations to see if any possible weak password-storing techniques may be found.

5. PowerShell script execution

The threat actor uses PowerShell scripts like “Invoke-FindLocalAdminAccess” and “PowerView” to locate local administrator access on computers or acquire data about the Active Directory (AD) infrastructure.

Detection: Monitoring PowerShell execution for suspicious or malicious script invocations.

Rule:

```
title: Malicious PowerShell Scripts - PoshModule
id: 41025fd7-0466-4650-a813-574aaacbe7f4
related:
  - id: f331aa1f-8c53-4fc3-b083-cc159bc971cb
    type: similar
  - id: bf7286e7-c0be-460b-a7e8-5b2e07ecc2f2
    type: obsoletes
status: experimental
description: Detects the execution of known offensive powershell scripts used for exploitation or reconnaissance
references:
  - https://github.com/PowerShellMafia/PowerSploit
  - https://github.com/NetSPI/PowerUpSQL
  - https://github.com/CsEnox/EventViewer-UACBypass
  - https://github.com/AlsidOfficial/WSUSpendu/
  - https://github.com/nettitude/Invoke-PowerThIEf
  - https://github.com/S3cur3Th1sSh1t/WinPwn
  - https://github.com/S3cur3Th1sSh1t/PowerSharpPack/tree/master/PowerSharpBinaries
  - https://github.com/BC-SECURITY/Invoke-ZeroLogon/blob/111d17c7fec486d9bb23387e2e828b09a26075e4/Invoke-ZeroLogon.ps1
  - https://github.com/xorrior/RandomPS-Scripts/blob/848c919bfce4e2d67b626cbcf4404341cfe3d3b6/Get-DXWebcamVideo.ps1
  - https://github.com/rvrsh3ll/Misc-Powershell-Scripts/blob/6f23bb41f9675d7e2d32bacccff75e931ae00554/OfficeMemScraper.ps1
  - https://github.com/dafthack/DomainPasswordSpray/blob/b13d64a5834694aa73fd2aea9911a83027c465a7/DomainPasswordSpray.ps1
  - https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/ # Invoke-TotalExec
  - https://research.nccgroup.com/2022/06/06/shining-the-light-on-black-basta/ # Invoke-TotalExec
  - https://github.com/HarmJ0y/DAMP
  - https://github.com/samratashok/nishang
  - https://github.com/DarkCoderSc/PowerRunAsSystem/
  - https://github.com/besimorhino/powercat
author: frack113, Nasreddine Bencherchali
date: 2023/01/23
tags:
  - attack.execution
  - attack.t1059.001
logsource:
  product: windows
  category: ps_module
  definition: 0ad03ef1-f21b-4a79-8ce8-e6900c54b65b
detection:
  selection_generic:
    ContextInfo|contains:
      - 'Add-ConstrainedDelegationBackdoor.ps1'
```

```
- 'Add-Exfiltration.ps1'
- 'Add-Persistence.ps1'
- 'Add-RegBackdoor.ps1'
- 'Add-RemoteRegBackdoor.ps1'
- 'Add-ScrnSaveBackdoor.ps1'
- 'Check-VM.ps1'
- 'ConvertTo-ROT13.ps1'
- 'Copy-VSS.ps1'
- 'Create-MultipleSessions.ps1'
- 'DNS_TXT_Pwnage.ps1'
- 'Do-Exfiltration.ps1'
- 'DomainPasswordSpray.ps1'
- 'Download_Execute.ps1'
- 'Download-Execute-PS.ps1'
- 'Enabled-DuplicateToken.ps1'
- 'Enable-DuplicateToken.ps1'
- 'Execute-Command-MSSQL.ps1'
- 'Execute-DNSTXT-Code.ps1'
- 'Execute-OnTime.ps1'
- 'ExetoText.ps1'
- 'Exploit-Jboss.ps1'
- 'Find-AVSignature.ps1'
- 'Find-Fruit.ps1'
- 'Find-GPOLocation.ps1'
- 'Find-TrustedDocuments.ps1'
- 'FireBuster.ps1'
- 'FireListener.ps1'
- 'Get-ApplicationHost.ps1'
- 'Get-ChromeDump.ps1'
- 'Get-ClipboardContents.ps1'
- 'Get-ComputerDetail.ps1'
- 'Get-FoxDump.ps1'
- 'Get-GPPAutologon.ps1'
- 'Get-GPPPassword.ps1'
- 'Get-IndexedItem.ps1'
- 'Get-Keystrokes.ps1'
- 'Get-LSASecret.ps1'
- 'Get-MicrophoneAudio.ps1'
- 'Get-PassHashes.ps1'
- 'Get-PassHints.ps1'
- 'Get-RegAlwaysInstallElevated.ps1'
- 'Get-RegAutoLogon.ps1'
- 'Get-RickAstley.ps1'
- 'Get-Screenshot.ps1'
- 'Get-SecurityPackages.ps1'
- 'Get-ServiceFilePermission.ps1'
- 'Get-ServicePermission.ps1'
- 'Get-ServiceUnquoted.ps1'
- 'Get-SiteListPassword.ps1'
- 'Get-System.ps1'
- 'Get-TimedScreenshot.ps1'
- 'Get-UnattendedInstallFile.ps1'
- 'Get-Unconstrained.ps1'
- 'Get-USBKeystrokes.ps1'
- 'Get-VaultCredential.ps1'
- 'Get-VulnAutoRun.ps1'
- 'Get-VulnSchTask.ps1'
- 'Get-WebConfig.ps1'
- 'Get-WebCredentials.ps1'
- 'Get-WLAN-Keys.ps1'
- 'Gupt-Backdoor.ps1'
- 'HTTP-Backdoor.ps1'
- 'HTTP-Login.ps1'
- 'Install-ServiceBinary.ps1'
- 'Install-SSP.ps1'
- 'Invoke-ACLScanner.ps1'
- 'Invoke-ADSBackdoor.ps1'
- 'Invoke-AmsiBypass.ps1'
- 'Invoke-ARPScan.ps1'
```

```
- 'Invoke-BackdoorLNK.ps1'
- 'Invoke-BadPotato.ps1'
- 'Invoke-BetterSafetyKatz.ps1'
- 'Invoke-BruteForce.ps1'
- 'Invoke-BypassUAC.ps1'
- 'Invoke-Carbuncle.ps1'
- 'Invoke-Certify.ps1'
- 'Invoke-ConPtyShell.ps1'
- 'Invoke-CredentialInjection.ps1'
- 'Invoke-CredentialsPhish.ps1'
- 'Invoke-DAFT.ps1'
- 'Invoke-DCSync.ps1'
- 'Invoke-Decode.ps1'
- 'Invoke-DinvokeKatz.ps1'
- 'Invoke-DllInjection.ps1'
- 'Invoke-DowngradeAccount.ps1'
- 'Invoke-EgressCheck.ps1'
- 'Invoke-Encode.ps1'
- 'Invoke-EventViewer.ps1'
- 'Invoke-Eyewitness.ps1'
- 'Invoke-FakeLogonScreen.ps1'
- 'Invoke-Farmer.ps1'
- 'Invoke-Get-RBCD-Threaded.ps1'
- 'Invoke-Gopher.ps1'
- 'Invoke-Grouper2.ps1'
- 'Invoke-Grouper3.ps1'
- 'Invoke-HandleKatz.ps1'
- 'Invoke-Interceptor.ps1'
- 'Invoke-Internalmonologue.ps1'
- 'Invoke-Inveigh.ps1'
- 'Invoke-InveighRelay.ps1'
- 'Invoke-JSRatRegsvr.ps1'
- 'Invoke-JSRatRundll.ps1'
- 'Invoke-KrbRelay.ps1'
- 'Invoke-KrbRelayUp.ps1'
- 'Invoke-LdapSignCheck.ps1'
- 'Invoke-Lockless.ps1'
- 'Invoke-MalSCCM.ps1'
- 'Invoke-Mimikatz.ps1'
- 'Invoke-MimikatzWDigestDowngrade.ps1'
- 'Invoke-Mimikittenz.ps1'
- 'Invoke-MITM6.ps1'
- 'Invoke-NanoDump.ps1'
- 'Invoke-NetRipper.ps1'
- 'Invoke-NetworkRelay.ps1'
- 'Invoke-NinjaCopy.ps1'
- 'Invoke-OxidResolver.ps1'
- 'Invoke-P0wnedshell.ps1'
- 'Invoke-P0wnedshellx86.ps1'
- 'Invoke-Paranoia.ps1'
- 'Invoke-PortScan.ps1'
- 'Invoke-PoshRatHttp.ps1'
- 'Invoke-PoshRatHttps.ps1'
- 'Invoke-PostExfil.ps1'
- 'Invoke-PowerDump.ps1'
- 'Invoke-PowerShellIcmp.ps1'
- 'Invoke-PowerShellTCP.ps1'
- 'Invoke-PowerShellTcpOneLine.ps1'
- 'Invoke-PowerShellTcpOneLineBind.ps1'
- 'Invoke-PowerShellUdp.ps1'
- 'Invoke-PowerShellUdpOneLine.ps1'
- 'Invoke-PowerShellWMI.ps1'
- 'Invoke-PowerThIEf.ps1'
- 'Invoke-PPLDump.ps1'
- 'Invoke-Prasadhak.ps1'
- 'Invoke-PsExec.ps1'
- 'Invoke-PsGcat.ps1'
- 'Invoke-PsGcatAgent.ps1'
- 'Invoke-PSInject.ps1'
```

```
- 'Invoke-PsUaCme.ps1'
- 'Invoke-ReflectivePEInjection.ps1'
- 'Invoke-ReverseDNSLookup.ps1'
- 'Invoke-Rubeus.ps1'
- 'Invoke-RunAs.ps1'
- 'Invoke-SafetyKatz.ps1'
- 'Invoke-SauronEye.ps1'
- 'Invoke-SCShell.ps1'
- 'Invoke-Seatbelt.ps1'
- 'Invoke-ServiceAbuse.ps1'
- 'Invoke-SessionGopher.ps1'
- 'Invoke-ShellCode.ps1'
- 'Invoke-SMBScanner.ps1'
- 'Invoke-Snaffler.ps1'
- 'Invoke-Spoolsample.ps1'
- 'Invoke-SSHCommand.ps1'
- 'Invoke-SSIDExfil.ps1'
- 'Invoke-StandIn.ps1'
- 'Invoke-StickyNotesExtract.ps1'
- 'Invoke-Tater.ps1'
- 'Invoke-Thunderfox.ps1'
- 'Invoke-ThunderStruck.ps1'
- 'Invoke-TokenManipulation.ps1'
- 'Invoke-Tokenvator.ps1'
- 'Invoke-TotalExec.ps1'
- 'Invoke-UrbanBishop.ps1'
- 'Invoke-UserHunter.ps1'
- 'Invoke-VoiceTroll.ps1'
- 'Invoke-Whisker.ps1'
- 'Invoke-WinEnum.ps1'
- 'Invoke-winPEAS.ps1'
- 'Invoke-WireTap.ps1'
- 'Invoke-WmiCommand.ps1'
- 'Invoke-WScriptBypassUAC.ps1'
- 'Invoke-Zerologon.ps1'
- 'Keylogger.ps1'
- 'MailRaider.ps1'
- 'New-HoneyHash.ps1'
- 'OfficeMemScraper.ps1'
- 'Offline_Winpwn.ps1'
- 'Out-CHM.ps1'
- 'Out-DnsTxt.ps1'
- 'Out-Excel.ps1'
- 'Out-HTA.ps1'
- 'Out-Java.ps1'
- 'Out-JS.ps1'
- 'Out-Minidump.ps1'
- 'Out-RundllCommand.ps1'
- 'Out-SCF.ps1'
- 'Out-SCT.ps1'
- 'Out-Shortcut.ps1'
- 'Out-WebQuery.ps1'
- 'Out-Word.ps1'
- 'Parse_Keys.ps1'
- 'Port-Scan.ps1'
- 'PowerBreach.ps1'
- 'powercat.ps1'
- 'PowerRunAsSystem.psm1'
- 'PowerSharpPack.ps1'
- 'PowerUp.ps1'
- 'PowerUpSQL.ps1'
- 'PowerView.ps1'
- 'PSAsyncShell.ps1'
- 'RemoteHashRetrieval.ps1'
- 'Remove-Persistence.ps1'
- 'Remove-PoshRat.ps1'
- 'Remove-Update.ps1'
- 'Run-EXEonRemote.ps1'
- 'Schtasks-Backdoor.ps1'
```

```
        - 'Set-DCShadowPermissions.ps1'
        - 'Set-MacAttribute.ps1'
        - 'Set-RemotePSRemoting.ps1'
        - 'Set-RemoteWMI.ps1'
        - 'Set-Wallpaper.ps1'
        - 'Show-TargetScreen.ps1'
        - 'Speak.ps1'
        - 'Start-CaptureServer.ps1'
        - 'Start-WebcamRecorder.ps1'
        - 'StringToBase64.ps1'
        - 'TexttoExe.ps1'
        - 'VolumeShadowCopyTools.ps1'
        - 'WinPwn.ps1'
        - 'WSUSpendu.ps1'
    selection_invoke_sharp:
      ContextInfo|contains|all:
        - 'Invoke-Sharp' # Covers all "Invoke-Sharp" variants
        - '.ps1'
    condition: 1 of selection_*
falsepositives:
    - Unknown
level: high
```

Threat Hunting:

- Look for instances where PowerShell commands are used to execute scripts like “Invoke-FindLocalAdminAccess” or “PowerView”. Investigate these commands for signs of malicious activities, such as lateral movement or reconnaissance.

6. WMI for remote execution

The threat actor employs WMI (Windows Management Instrumentation) to remotely launch the CoBeacon backdoor across the environment, executing a command using “wmic” and specifying the remote node and process to create.

Detection: Monitor WMI command-line executions, especially with remote node specifications.

Rule:

```
title: Suspicious Process Created Via Wmic.EXE
id: 3c89a1e8-0fba-449e-8f1b-8409d6267ec8
related:
    - id: 526be59f-a573-4eea-b5f7-f0973207634d # Generic
      type: derived
status: test
description: Detects WMIC executing "process call create" with suspicious calls to processes such as "rundll32", "regsrv32", etc.
references:
    - https://thedfirreport.com/2020/10/08/ryuks-return/
    - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
author: Florian Roth (Nextron Systems), Nasreddine Bencherchali (Nextron Systems)
date: 2020/10/12
modified: 2023/02/14
tags:
    - attack.execution
```

```
    - attack.t1047
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains|all:
            - 'process '
            - 'call '
            - 'create '
        CommandLine|contains:
            # Add more susupicious paths and binaries as you see fit in your env
            - 'rundll32'
            - 'bitsadmin'
            - 'regsvr32'
            - 'cmd.exe /c '
            - 'cmd.exe /k '
            - 'cmd.exe /r '
            - 'cmd /c '
            - 'cmd /k '
            - 'cmd /r '
            - 'powershell'
            - 'pwsh'
            - 'certutil'
            - 'cscript'
            - 'wscript'
            - 'mshta'
            - '\Users\Public\'
            - '\Windows\Temp\'
            - '\AppData\Local\'
            - '%temp%'
            - '%tmp%'
            - '%ProgramData%'
            - '%appdata%'
            - '%comspec%'
            - '%localappdata%'
    condition: selection
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Unknown
level: high
```

Threat Hunting: Investigate instances where WMI commands are used to remotely launch processes, such as “pythonw.exe”, along with suspicious script names or locations. Identify potential signs of unauthorized remote access or command execution.

7. Python script execution

The threat actor uses a Python script, potentially containing the marshal module, to execute pseudo-compiled code for tools like LaZagne. These scripts aim to obtain high-privileged credentials and escalate privileges.

Detection: Monitor for suspicious Python script execution, particularly involving known credential harvesting tools.

Rule:

```
title: Python Inline Command Execution
id: 899133d5-4d7c-4a7f-94ee-27355c879d90
status: experimental
description: Detects execution of python using the "-c" flag. This is could be used as a way to launch a reverse shell or execute live
python code.
references:
  - https://docs.python.org/3/using/cmdline.html#cmdoption-c
  - https://www.revshells.com/
  - https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
author: Nasreddine Bencherchali (Nextron Systems)
date: 2023/01/02
modified: 2023/02/17
tags:
  - attack.execution
  - attack.t1059
logsource:
  category: process_creation
  product: windows
detection:
  selection_img:
    - OriginalFileName: 'python.exe'
    - Image|endswith:
      - 'python.exe' # no \ bc of e.g. ipython.exe
      - 'python3.exe'
      - 'python2.exe'
  selection_cli:
    CommandLine|contains: ' -c'
  filter_python: # Based on baseline
    ParentImage|startswith: 'C:\Program Files\Python'
    ParentImage|endswith: '\python.exe'
    ParentCommandLine|contains: '-E -s -m ensurepip -U --default-pip'
  filter_vscode:
    ParentImage|endswith: '\AppData\Local\Programs\Microsoft VS Code\Code.exe'
  condition: all of selection_* and not 1 of filter_*
falsepositives:
  - Python libraries that use a flag starting with "-c". Filter according to your environment
level: medium
```

Threat Hunting:

- Search for instances where Python scripts with the “-c” module are executed and analyze the script content for signs of the reverse shell.

8. PsExec

The threat actor utilizes PsExec to download additional tools and move laterally across the environment, potentially for further exploitation or reconnaissance.

Detection: Monitor for the presence and execution of PsExec, a common tool used for remote execution and administration in Windows environments.

Rule:

```
title: PsExec Service File Creation
id: 259e5a6a-b8d2-4c38-86e2-26c5e651361d
related:
  - id: 42c575ea-e41e-41f1-b248-8093c3e82a28
    type: derived
status: test
description: Detects default PsExec service filename which indicates PsExec service installation and execution
references:
  - https://www.jpcert.or.jp/english/pub/sr/ir_research.html
  - https://jpcertcc.github.io/ToolAnalysisResultSheet
author: Thomas Patzke
date: 2017/06/12
modified: 2022/10/26
tags:
  - attack.execution
  - attack.t1569.002
  - attack.s0029
logsource:
  category: file_event
  product: windows
detection:
  selection:
    TargetFilename|endswith: '\PSEXESVC.exe'
  condition: selection
fields:
  - EventID
  - CommandLine
  - ParentCommandLine
  - ServiceName
  - ServiceFileName
  - TargetFilename
  - PipeName
falsepositives:
  - Unknown
level: low
```

Threat Hunting:

Analyze command-line executions for the presence of PsExec, focusing on instances where it is used for remote process initiation or executing commands on remote systems, indicating potential unauthorized lateral movement or privilege escalation.

These rules and procedures must be used in conjunction with centralized log monitoring, anomaly detection, behavior-based analysis, and full endpoint security solutions for successful detection and threat hunting. Review and update these guidelines often to keep current with changing threat environments and alert to prospective attacks.

MITRE ATT&CK techniques

Tactic	Technique
Resource Development	Obtain Capabilities (T1588) • Digital Certificate (T1588.004)
Execution	Shared Modules (T1129)
	Native API (T1106)
	Inter-Process Communication (T1559) • Component Object Model (T1559.001)
	Scheduled Task/Job (T1053)
	Command and Scripting Interpreter (T1059)
	Command and Scripting Interpreter (T1059) • PowerShell (T1059.001) • Windows Command Shell (T1059.003)
	User Execution (T1204) • Malicious File (T1204.002)
	System Services (T1569) • Service Execution (T1569.002)
	Windows Management Instrumentation (T1047)
Persistence	Boot or Logon Autostart Execution (T1547) • Registry Run Keys / Startup Folder (T1547.001) • Shortcut Modification (T1547.009)
	Scheduled Task/Job (T1053)
	Event Triggered Execution (T1546) • Component Object Model Hijacking
	Hijack Execution Flow (T1574) • DLL Search Order Hijacking (T1574.001) • DLL Side-Loading (T1574.002)
	Create or Modify System Process (T1543) • Windows Service (T1543.003)
	Account Manipulation (T1098)

	• Device Registration (T1098.005)
Privilege Escalation	Process Injection (T1055) • Extra Window Memory Injection (T1055.011)
	Boot or Logon Autostart Execution (T1547) • Registry Run Keys / Startup Folder (T1547.001) • Shortcut Modification (T1547.009)
	Scheduled Task/Job (T1053)
	Event Triggered Execution (T1546) • Component Object Model Hijacking
	Process Injection (T1055) • Thread Execution Hijacking (T1055.003) • Asynchronous Procedure Call (T1055.004)
	Hijack Execution Flow (T1574) • DLL Side-Loading (T1574.002) • DLL Search Order Hijacking (T1574.001)
	Create or Modify System Process (T1543) • Windows Service (T1543.003)
	Process Injection (T1055) • Dynamic-link Library Injection (T1055.001)
	Create or Modify System Process (T1543)
	Abuse Elevation Control Mechanism (T1548) • Bypass User Account Control (T1548.002)
	Access Token Manipulation (T1134) • Token Impersonation/Theft (T1134.001)
	Abuse Elevation Control Mechanism (T1548)
	Indicator Removal (T1070) • File Deletion (T1070.004) • Timestomp (T1070.006)
	Process Injection (T1055) • Dynamic-link Library Injection (T1055.001)

Defense Evasion	• Thread Execution Hijacking (T1055.003) • Asynchronous Procedure Call (T1055.004) • Extra Window Memory Injection (T1055.011)
	Obfuscated Files or Information (T1027)
	Modify Registry (T1112)
	Deobfuscate/Decode Files or Information (T1140)
	Masquerading (T1036) • Double File Extension (T1036.007)
	Debugger Evasion (T1622)
	Hijack Execution Flow (T1574) • DLL Search Order Hijacking (T1574.001) • DLL Side-Loading (T1574.002)
	Virtualization/Sandbox Evasion (T1497) • Time Based Evasion (T1497.003)
	System Binary Proxy Execution (T1218) • Regsvr32 (T1218.010) • Rundll32 (T1218.011)
	Abuse Elevation Control Mechanism (T1548) • Bypass User Account Control (T1548.002)
	Access Token Manipulation (T1134)
	File and Directory Permissions Modification (T1222)
	Hide Artifacts (T1564) • Hidden Window (T1564.003)
	Obfuscated Files or Information (T1027) • Software Packing (T1027.002) • Indicator Removal from Tools (T1027.005) • Dynamic API Resolution (T1027.007)
	Access Token Manipulation (T1134) • Token Impersonation/Theft (T1134.001)
	Abuse Elevation Control Mechanism (T1548)

	Direct Volume Access (T1006)
	Impair Defenses (T1562) • Disable or Modify Tools (T1562.001)
Credential Access	Input capture (T1056) • Keylogging (T1056.001)
	Unsecured Credentials (T1552) • Credentials in Registry (T1552.002)
	Credentials from Password Stores (T1555)
Discovery	File and Directory Discovery (T1083)
	Process Discovery (T1057)
	Query Registry (T1012)
	System Information Discovery (T1082)
	System Service Discovery (T1007)
	System Location Discovery (1614) • System Language Discovery (T1614.001)
	Debugger Evasion (T1622)
	Application Window Discovery (T1010)
	System Owner/User Discovery (T1033)
	Software Discovery (T1518)
	Virtualization/Sandbox Evasion (T1497) • Time Based Evasion (T1497.003)
	System Time Discovery (T1124)
	System Network Connections Discovery (T1049)
	System Network Configuration Discovery (T1016)
	Network Share Discovery (T1135)
Lateral Movement	Lateral Tool Transfer (T1570)
	Remote Services (T1021) • Remote Desktop Protocol (T1021.001)
Collection	Archive Collected Data (T1560)
	Data Staged (T1074)

	• Local Data Staging (T1074.001)
	Input capture (T1056) • Keylogging (T1056.001) • Credential API Hooking (T1056.004)
	Data from Local System (T1005)
	Screen Capture (T1113)
	Clipboard Data (T1115)
	Email Collection (T1114) • Local Email Collection (T1114.001)
	Data from Information Repositories (T1213)
	Automated Collection (T1119)
Command and Control	Ingress Tool Transfer (T1105)
	Application Layer Protocol (T1071) • Web Protocols (T1071.001)
	Encrypted Channel (T1573) • Asymmetric Cryptography (T1573.002)
	Application Layer Protocol (T1071) • Mail Protocols (T1071.003) • DNS (T1071.004)
	Non-Standard Port (T1571)
	Non-Application Layer Protocol (T1095)
	Web Service (T1102)
	Data Encoding (T1132)
	Proxy (T1090)
Exfiltration	Exfiltration Over C2 Channel (T1041)
	Scheduled Transfer (T1029)
Impact	Data Encrypted for Impact (T1486)
	Service Stop (T1489)
	System Shutdown/Reboot (T1529)

Indicators of Compromise (IOCs)

SHA-256	Detection name
25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c	Trojan.Win64.COBEACON.SWG
4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a	Trojan.Win64.COBEACON.SWG
13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe	Trojan.Win64.COBEACON.SWG
Troj.Win32.TRX.XXPE50FFF069	
8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5	Trojan.Win64.COBEACON.SWG
bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef	Trojan.Win64.COBEACON.SWG
c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe	Trojan.Win64.COBEACON.SWG
3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce	Trojan.Win64.COBEACON.SWG
21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839	Trojan.Win64.COBEACON.SWG
e5db80c01562808ef2ec1c4b8f3f033ac0ed758d	Backdoor.Python.COBEACON.C
cfbde85bdb62054b5b9eb4438c3837b9f1a69f61	Backdoor.Python.COBEACON.C
3b14559a6e33fce120a905fde57ba6ed268a51f1	Backdoor.Python.COBEACON.C
aae1b17891ec215a0e238f881be862b4f598e46c	Backdoor.Python.COBEACON.C
c82b28daeb33d94ae3cafbc52dbb801c4a5b8cfa	Backdoor.Python.COBEACON.C
d2663fc6966c197073c7315264602b4c6ba9c192	Trojan.BAT.COBEACON.AO
c7568d00ae38b3a4691a413ed439a0e3fb5664b1	Trojan.BAT.COBEACON.AO
61e41be7a9889472f648a5a3d0b0ab69e2e056c5	Trojan.BAT.COBEACON.AO
69ffad6be67724b1c7e8f65e8816533a96667a36	Trojan.XML.COBEACON.F
c1516915431cb55703b5a88d94ef6de0ac67190a	Trojan.XML.COBEACON.F
a7b1853348346d5d56f4c33f313693a18b6af457	Trojan.XML.COBEACON.F
ac8e3146f41845a56584ce5e8e172a56d59aa804	Trojan.XML.COBEACON.F
e5d434dfa2634041cdbdac1dec58fcd49d629513	Trojan.BAT.KILLAV.WLEBG
42da9e9e3152c1d995d8132674368da4be78bf6a	Trojan.BAT.COBEACON.AO.dldr
5cbb6978c9d01c8a6ea65caccb451bf052ed2acd	HackTool.Win32.Adfind.VSNW1FE23
a9310c3f039c4e2184848f0eb8e65672f9f11240	TrojanSpy.Python.CREAL.A
5e36a649c82fa41a600d51fe99f4aa8911b87828	HackTool.Python.LaZagne.AD
5263a135f09185aa44f6b73d2f8160f56779706d	HackTool.PS1.VeeamCreds.A
75d02e81cc326e6a0773bc11ffa6fa2f6fa5343e	TROJ.Win32.TRX.XXPE50FFF069
9d85cb2c6f1fccc83217837a63600b673da1991a	TROJ.Win32.TRX.XXPE50FFF069
2f2eb89d3e6726c6c62d6153e2db1390b7ae7d01	TROJ.Win32.TRX.XXPE50FFF069
7d500a2cd8ea7e455ae1799cb4142bb2abac3ae1	TROJ.Win32.TRX.XXPE50FFF069
0362c710e4813020147f5520a780a15ef276e229	Troj.Win32.TRX.XXPE50FFF069
Troj.Win32.TRX.XXPE50FFF069R450C	
TROJ.Win32.TRX.XXPE50FLM011	
fb2ef2305511035e1742f689fce928c424aa8b7d	Troj.Win32.TRX.XXPE50FFF069

Troj.Win32.TRX.XXPE50FFF069R450C	
TROJ.Win32.TRX.XXPE50FLM011	
7874d722a6dbaef9e5f9622d495f74957da358da	Troj.Win32.TRX.XXPE50FFF069
Troj.Win32.TRX.XXPE50FFF069R450C	
TROJ.Win32.TRX.XXPE50FLM011	
06e3f86369046856b56d47f45ea2f7cf8e240ac5	Troj.Win32.TRX.XXPE50FFF069
Troj.Win32.TRX.XXPE50FFF069R450C	
TROJ.Win32.TRX.XXPE50FLM011	
36b454592fc2b8556c2cb983c41af4d2d8398ea2	Troj.Win32.TRX.XXPE50FFF068
337ca5eefe18025c6028d617ee76263279650484	TROJ_GEN.R002C0DCS23
e862f106ed8e737549ed2daa95e5b8d53ed50f87	TROJ_GEN.R002C0PFK23
2a85cdfb1c3434d73ece7fe60d6d2d5c9b7667dd	Troj.Win32.TRX.XXPE50FFF068
d883be0ee79dec26ef8c04e0e2857a516cff050c	TROJ.Win32.TRX.XXPE50FLM011
a0f1a8462cb9105660af2d4240e37a27b5a9afad	Ransom.Win32.BLACKCAT.SMYPCC5
ab0eade9b8d24b09e32aa85f78a51b777861debc	Ransom.Win32.BLACKCAT.SMYPCC5
0cc0e1cbf4923d2ce7179064c244fe138dcb3ce8	Ransom.Win32.BLACKCAT.SMYPCC5
3789a218c966f175067242975e1cb44abdef81ec	Ransom.Win32.BLACKCAT.SMYPCC5
83c5f8821f9a07e0318beaa4bcf0b7ef21127aa8	Ransom.Win32.BLACKCAT.SMYPCC5
08f63693bb40504b71fe3e4e4d9e7142c011aeb1	Ransom.Win32.BLACKCAT.SMYPCC5
b34bb1395199c7b168d9204833fdfd13d542706d	Ransom.Win32.BLACKCAT.SMYPCC5
5c6aa1a5bd7572ac8e91eaa5c9d6096f302f775b	Ransom.Win32.BLACKCAT.SMYPCC5
9480a79b0b6f164b1148c56f43f3d505ee0b7ef3	Ransom.Win32.BLACKCAT.SMYPCC5
7874d722a6dbaef9e5f9622d495f74957da358da	Ransom.Win32.BLACKCAT.SMYPCC5
9b1ebbe03949e0c16338595b1772befe276cd10d	Ransom.Win32.BLACKCAT.SMYPCC5
801950ed376642e537466795f92b04e13a4fcc2a	Ransom.Win32.BLACKCAT.SMYPCC5
1ca4e3fdcdf8a9ab095cfa0629750868eb955eb7	Ransom.Win32.BLACKCAT.SMYPCC5
42920e4d15428d4e7a8f52ae703231bdf0aec241	Ransom.Win32.BLACKCAT.SMYPCC5
06e3f86369046856b56d47f45ea2f7cf8e240ac5	Ransom.Win32.BLACKCAT.SMYPCC5
f42e97901a1a3b87b4f326cb9e6cbdb98652d900	Ransom.Win32.BLACKCAT.SMYPCC5
d125c4f82e0bbf369caf1be524250674a603435c	Ransom.Win32.BLACKCAT.SMYPCC5
03d7bc24d828abaf1a237b3f418517fada8ae64f	Ransom.Win32.BLACKCAT.SMYPCC5
c133992ea87f83366e4af5401a341365190df4e7	Ransom.Win32.BLACKCAT.SMYXCCN.note
b35be51d727d8b6f8132850f0d044b838fec001d	Ransom.Win32.BLACKCAT.SMYXCCN.note
fd84cf245f7a60c38ac7c92e36458c5ea4680809	Ransom.Win32.BLACKCAT.SMYXCCN.note
946c0a0c613c8ac959d94bb2fd152c138fc752da	Ransom.Win32.BLACKCAT.SMYXCCN.note
7b3051f8d09d53e7c5bc901262f5822f1999caae	Ransom.Win32.BLACKCAT.SMYXCCN.note
eeff22b4a442293bf0f5ef05154e8d4c7a603005	Ransom.Win32.BLACKCAT.SMYXCCN.note
2547d2deedc385f7557d5301c19413e1cbf58cf8	Ransom.Win32.BLACKCAT.SMYXCCN.note
0437f84967de62d8959b89d28a56e40247b595d8	Ransom.Win32.BLACKCAT.SMYXCCN.note
105d33c00847ccd0fb230f4a7457e8ab6fb035fc	Ransom.Win32.BLACKCAT.SMYXCCN.note
5831b3a830690c603fd093329dce93b9a7e83ad3	Ransom.Win32.BLACKCAT.SMYXCCN.note
a5c164b734a8b61d8af70257e23d16843a4c72e3	Ransom.Win32.BLACKCAT.SMYXCCN.note

1aff9fd8fdc0eae3c09a3ee6b4df2cdb24306498	Ransom.Win32.BLACKCAT.SMYXCCN.note
3d4051c65d1b5614af737cb72290ec15b71b75bd	Ransom.Win32.BLACKCAT.SMYXCCN.note
a116ef48119c542a2d864f41dbbb66e18d5cd4e6	Ransom.Win32.BLACKCAT.SMYXCCN.note
508e7522db24cca4913aeed8218975c539d3b0a4	Ransom.Win32.BLACKCAT.SMYXCCN.note
72603dadebc12de4daf2e12d28059c4a3dcf60d0	Ransom.Win32.BLACKCAT.SMYXCCN.note
930bd974a2d01393636fdb91ca9ac53256ff6690	Ransom.Win32.BLACKCAT.SMYXCCN.note
a9a03d39705bd1d31563d7a513a170c99f724923	Ransom.Win32.BLACKCAT.SMYXCCN.note
c14bd9ad77d8beca07fb17dc34f8a5f636e621b5	Ransom.Win32.BLACKCAT.SMYXCCN.note
01b122eb0edb6274b3743458e375e34126fd2f9a	Ransom.Win32.BLACKCAT.SMYXCCN.note
b98bb7b4c3b823527790cb62e26d14d34d3e499b	Ransom.Win32.BLACKCAT.SMYXCCN.note
381058a5075ce06605350172e72c362786e8c5e3	Ransom.Win32.BLACKCAT.SMYXCCN.note
75e9d507b1a1606a3647fe182c4ed3a153cecc2c	Ransom.Win32.BLACKCAT.SMYXCCN.note
cd485054625ea8ec5cf1fe0e1f11ede2e23dde00	Ransom.Win32.BLACKCAT.SMYXCCN.note
c9cdfdc45b04cca45b64fedca7c372f73b42cab2	Ransom.Win32.BLACKCAT.SMYXCCN.note
31d4dadd11fe52024b1787a20b56700e7fd257f8	Ransom.Win32.BLACKCAT.SMYXCCN.note
0fe306dc12ba6441ba2a5cab1b9d26638c292f9c	Ransom.Win32.BLACKCAT.SMYXCCN.note
bc0fb6b220045f54d34331345d1302f9a00b3580	Ransom.Win32.BLACKCAT.SMYXCCN.note
b4f59fe2ee3435b9292954d1c3ef7e74c233abea	Ransom.Win32.BLACKCAT.SMYXCCN.note
aee0b252334b47a6e382ce2e01de9191de2e6a7a	Ransom.Win32.BLACKCAT.SMYXCCN.note
92673b91d2c86309f321ade6a86f0c9e632346d8	Ransom.Win32.BLACKCAT.SMYXCCN.note
de7fb8efa05ddf5f21a65e940717626b1c3d6cb4	Ransom.Win32.BLACKCAT.SMYXCCN.note
5f455dcdca66df904189970828995051997 1bb76	Ransom.Win32.BLACKCAT.SMYXCCN.note
5ed1b9810ee12d2b9b358dd09c6822588bbb4a83	Ransom.Win32.BLACKCAT.SMYXCCN.note
c779a4a98925bc2f7feac91c1867a3f955462fc2	Ransom.Win32.BLACKCAT.SMYXCCN.note
cb358aa4ed50db8270f3ee7ea5848b8c16fa21fe	Ransom.Win32.BLACKCAT.SMYXCCN.note
5ec6b30dacfced696c0145a373404e63763c2fa8	Ransom.Win32.BLACKCAT.SMYXCCN.note
f2f5137c28416f76f9f4b131f85252f8273baee8	Ransom.Win32.BLACKCAT.SMYXCCN.note
12534212c7d4b3e4262edc9dc2a82c98c2121d04	Ransom.Win32.BLACKCAT.SMYXCCN.note
bc09ee8b42ac3f6107ab5b51a2581a9161e53925	Ransom.Win32.BLACKCAT.SMYXCCN.note
152400be759355ec8dd622ec182c29ce316eabb1	Ransom.Win32.BLACKCAT.SMYXCCN.note
379e497d0574fd4e612339440b603f380093655c	Ransom.Win32.BLACKCAT.SMYXCCN.note
141c7b9be4445c1aad70ec35ae3fe02f5f8d37ac	Ransom.Win32.BLACKCAT.SMYXCCN.note
27e9e6a54d73dcb28b5c7dfb4e2e05aaba913995	Ransom.Win32.BLACKCAT.SMYXCCN.note
ad981cd18f58e12db7c9da661181f6eb9a1754f3	Ransom.Win32.BLACKCAT.SMYXCCN.note
4829eaa38bd061773ceefe175938a2c0d75a75f3	Ransom.Win32.BLACKCAT.SMYXCCN.note
b0d61d1eba9ebf6b7eabcd62b70936d1a343178e	Ransom.Win32.BLACKCAT.SMYXCCN.note
014c277113c4b8c4605cb91b29302cdedbc2044e	Ransom.Win32.BLACKCAT.SMYXCCN.note
974c1684cf0f3a46af12ba61836e4c161fd48cb5	Ransom.Win32.BLACKCAT.SMYXCCN.note
913414069259e760e201d0520ce35fe22cf3c285	Ransom.Win32.BLACKCAT.SMYXCCN.note

Table 1: IOCS related to files.

Domains	IP
hxxps://cuororeresteadntno[.]com/how-to-work-with-ftp-ftps-connection-through-winscp/ hxxps://airplexacrepair[.]com/the-key-to-secure-remote-desktop-connections-a-comprehensive-guide/ hxxps://maker-events[.]com/automating-file-transfers-with-winscp/ hxxps://winsccp[.]com/WLPuVHrN hxxps://anydeesk[.]net hxxps://events[.]drdivyaclinic[.]com/wp-content/task/update/WinSCP-5[.]21[.]8-Setup[.]iso hxxps://www[.]4shared[.]com/web/directDownload/wd0Bbaw6jq/gx1qdBDA[.]ab8ba6f7d1af2d0a5d81cf42aefe8e51 hxxps://www[.]yb-lawyers[.]com/wp-content/ter/anyconnect/AnyDesk[.]iso hxxps://mm[.]onemakan[.]ml//wp/wp-content/winscp/smart/WinSCP-5[.]21[.]8-Setup[.]iso hxxps://167[.]88[.]164[.]40/python/pp2 hxxps://172[.]86[.]123[.]127:8443/work2z hxxps://172[.]86[.]123[.]127:8443/work2 hxxps://172[.]86[.]123[.]226:8443/work3z hxxps://172[.]86[.]123[.]226:8443/work3 hxxps://193[.]42[.]32[.]58:8443/work2z hxxps://193[.]42[.]32[.]58/python/pp hxxps://193[.]42[.]32[.]58:8443/zakrep hxxps://104[.]234[.]147[.]134/python/pp3[.]py http://45[.]12[.]253[.]50:447/work2 hxxps://45[.]66[.]230[.]240/python/pp3[.]py hxxps://45[.]66[.]230[.]240:8443/work1 http://45[.]66[.]230[.]240/python/pp hxxps://firstclassbale[.]com/python/pp3[.]py aleagroupdevelopment[.]com azurecloudup[.]online cloudupdateservice[.]online devnetapp[.]com situotech[.]com http://104[.]234[.]147[.]134/python/python[.]zip hxxps://167[.]88[.]164[.]40/python/python[.]zip http://172[.]86[.]123[.]226/python/python[.]zip hxxps://45[.]66[.]230[.]240/python/python[.]zip hxxps://closeyoueyes[.]com/python/python[.]zip hxxps://firstclassbale[.]com/python/python[.]zip hxxps://167[.]88[.]164[.]40/python/unzip[.]bat http://172[.]86[.]123[.]226/python/unzip[.]bat http://104[.]234[.]147[.]134/python/unzip[.]bat hxxps://45[.]66[.]230[.]240/python/unzip[.]bat hxxps://closeyoueyes[.]com/python/unzip[.]bat hxxps://firstclassbale[.]com/python/unzip[.]bat hxxps://167[.]88[.]164[.]40/python/pp3[.]py http://172[.]86[.]123[.]226/python/pp3[.]py ccloseyoueyes[.]com/python/pp3[.]py hxxp://bigallpack[.]com/union/desktop	172[.]86[.]123[.]127 172[.]86[.]123[.]226 45[.]66[.]230[.]240 45[.]12[.]253[.]50 193[.]42[.]32[.]58 104[.]234[.]11[.]226 141[.]98[.]6[.]56 166[.]0[.]95[.]43 167[.]88[.]164[.]91 193[.]42[.]32[.]143 45[.]12[.]253[.]51 45[.]66[.]230[.]215 45[.]81[.]39[.]175 45[.]81[.]39[.]176 84[.]54[.]50[.]116 85[.]217[.]144[.]233 104[.]234[.]11[.]236 157[.]254[.]195[.]108 157[.]254[.]195[.]83 167[.]88[.]164[.]40

Figure 5: IOCs related to Domain and IP.

Threat Summary	
Name	BlackCat aka AlphaVM, AlphaV, or ALPHV
Threat Type	Crypto virus, Loader, Stealer, Trojan, Files Locker
Encrypted Files Extension	Varies (depending on the version and variant)
Ransom Message	The ransom message typically includes instructions on paying the ransom and regaining access to the encrypted files. It may also include threats of data exposure or permanent file loss if the ransom is not paid.
Detection Names	Trojan.Ransom.BlackCat Ransom.Win32.BlackCat Ransom:Win32/BlackCat W32/BlackCat.Ransomware
Symptoms	• Encrypted files with a modified extension. • Display of ransom notes or messages demanding payment. • Restricted access to encrypted files. • Slow system performance or crashes.
Additional Information	It is a ransomware-as-a-service (RaaS) operation.
Distribution methods	Malvertising, Exploiting vulnerabilities, social engineering
Damage	BlackCat ransomware poses significant risks, including the encryption of critical files and data, potential exposure of sensitive information, disruption of business operations, and financial losses.
Malware Removal (Windows)	Conduct a thorough computer scan using trusted antivirus software.

Vairav Recommendations

We strongly advise applying the following complete procedures to properly mitigate and prevent ransomware attacks:

1. Implement Regular Data Backups

Regular data backups are essential because they provide an effective way of restoring the data in the event of a ransomware attack. Backing up vital data regularly ensures that even if the files are encrypted by ransomware, one can restore them from a safe backup source. Offline or isolated network storage methods are advised to keep backups safe during an attack.

2. Develop an Incident Response Plan

It is critical to have a well-defined incident response strategy in place before reacting to a ransomware attack. The strategy should outline specific processes and responsibilities for isolating affected systems, alerting key stakeholders, and beginning the recovery process. Organizations that have an established and rehearsed response strategy can reduce downtime, limit the attack, and swiftly resume operations.

3. Restrict Execution of Files from Untrusted Sources

Ransomware frequently penetrates organizations via malicious email attachments, untrustworthy website downloads, or illegal software. Implementing strict security measures, such as application whitelisting or sandboxing solutions, to prohibit the execution of files from untrusted sources, aids in the prevention of harmful code execution. This gives an extra layer of defense and lowers the risk.

4. **Keep Systems and Software Updated**

Regularly upgrading operating systems, software programs, and firmware is critical because it helps to fix security weaknesses that ransomware attackers can exploit. Updates and patches are released by software manufacturers to address known vulnerabilities, therefore staying up to date is critical for ensuring a safe computer environment.

5. **Implement the Least Privilege Principle**

The principle of least privilege guarantees that employees are only provided the access rights and privileges required to carry out their job tasks. Organizations may lower the attack surface for ransomware by restricting access to essential systems and sensitive data. In the case of a successful ransomware outbreak, limiting user rights can reduce the damage and prevent lateral network migration.

6. **Use Robust Antivirus and Anti-Malware Solutions:**

Using trusted antivirus and anti-malware software adds an extra layer of protection against ransomware. These technologies aid in detecting and preventing harmful files and actions, including known ransomware incidents. Maintaining them ensures that you have the most recent virus definitions to identify and prevent new threats.

7. **Implement Multi-factor Authentication (MFA)**

Multi-factor authentication strengthens the security of your organization's systems and accounts. MFA helps prevent unwanted access even if a user's credentials are compromised by requiring multiple authentication factors, such as a password and a unique verification code. This greatly decreases the possibility of attackers obtaining control of important systems and data.

8. **Enable Firewall and Intrusion Detection/Prevention Systems**

Firewalls serve as a line of defense between the internal network and external threats. Configuring firewalls to filter incoming and outgoing network traffic aids in the prevention of intrusion and suspicious connections. It monitors network traffic for malicious activity signals and responds quickly to prevent possible ransomware attacks.

9. **Engage with cybersecurity professionals.**

If your organization lacks the necessary expertise or resources to effectively manage the aftermath of a breach, it is advisable to seek assistance from a trusted cybersecurity firm. Engaging with a reputable cybersecurity professional can provide valuable support in incident response, forensic analysis, and implementing security enhancements.

It is important to remember that the cyber adversaries behind ransomware gangs are likely to constantly evolve their methods, tools, and techniques to evade detection and continue to be successful in their attacks. Therefore, organizations and individuals must stay informed about the latest TTPs of the BlackCat ransomware gang and take proactive steps to protect themselves.

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4441540

Mobile: +977-9820105900

Email: mail@vairav.net

Website: https://vairav.net