TLP: AMBER

Classification
RESTRICTED

Express Attack Brief 014

A BlackCat helped by a Raccoon

Version:	**1.0**
Publication date:	**2022-12-22**
Prepared for:	**NCC Group**

Table of contents

Document information **3**
Document purpose 3
Document structure 3
Document classification 3

1. Attack overview **4**
1.1. Attack description 4
1.2. Attack path summary 4

2. Attack path **5**
2.1. Download and execution of Credential Stealer 5
2.2. Login with stolen VPN credentials 6
2.3. Network Discovery over VPN 7
2.4. Move laterally over RDP 8
2.5. Disable Microsoft Windows Defender 9
2.6. Use Scheduled Tasks to execute the ExMatter Exfiltration tool 11
2.7. BlackCat Ransomware Execution 14

3. MITRE ATT&CK TTPs **20**

Document information

Document purpose

This document has been prepared for NCC Group.

This document describes the attack path observed during a recent cyber security incident. It presents the steps taken by the threat actor, including associated Tactic, Technique, and Procedure (TTP) details. Where possible the TTPs are expressed in MITRE ATT&CK terminology to aid in correlation and cross-referencing with other threat intelligence sources.

This document is aimed at helping readers learn from the incident and prepare to defend against possible future attacks. Its attack path structure is designed to show how the latest cyber attacks actually happen in the real world. The inclusion of TTP details allows readers to map the attack steps to their own organization, validating their security posture, and feeding into their risk management process.

Document structure

Chapter 1 describes the overall attack and gives a summary of the steps taken by the threat actor.

Chapter 2 describes the attack steps in detail, including possible prevention and detection opportunities where appropriate.

Chapter 3 lists the MITRE ATT&CK TTPs observed in the attack in a convenient table format.

Document classification

This document is shared with NCC Group as **TLP:AMBER** according to the Traffic Light Protocol (TLP). Recipients may only share this document with members of their own organization. Recipients may additionally share this document with their IT service providers for the sole purpose of validating or improving the security delivered to the recipients.

This document is classified as **RESTRICTED**. Any information published in this document is intended exclusively for NCC Group. Any use by a party other than NCC Group is prohibited unless explicitly granted by NCC Group. The information contained in this document may be **RESTRICTED** in nature and fall under a pledge of secrecy.

Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. NCC Group cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by its contained information.

1. Attack overview

1.1. Attack description

Timeframe	2022 Q3
Threat type	Ransomware
Sector relevance	All sectors
Geographic relevance	Global

This EAB describes the compromise of a company network. For this attack to take place, VPN credentials were abused followed by succesful exfiltration of data and encryption of all files on the servers in that network.

The attack started with the download and execution of a file which turned out to be a credential stealer. This allowed the attacker to gain access to the VPN credentials of the user account of an employee working at the victim company. With those credentials, the attacker logged into the VPN solution of the victim company and proceeded with trying to gain information about the victim's network.

Next, the attacker used Microsoft Remote Desktop to laterally move through the network to different servers. One of those servers was the Domain Controller. Once the attacker gained foothold on the Domain Controller, different tools and techniques were used to distribute a data exfiltration tool known as ExMatter, evade anti-virus, obtain persistance and finaly distribute BlackCat ransomware.

1.2. Attack path summary

Time	Tactic	Action	Target tech
Day 1, 07:35	Execution, Credential Access	Download and execution of Credential Stealer	Windows
Day 17, 23:11	Initial Access	Login with stolen VPN credentials	Windows
Day 17, 23:12	Discovery	Network Discovery over VPN	Windows
Day 18, 00:04	Lateral Movement	Move laterally over RDP	Windows
Day 18, 00:04	Defense Evasion	Disable Microsoft Windows Defender	Windows
Day 18, 00:23	Execution, Exfiltration	Use Scheduled Tasks to execute the ExMatter Exfiltration tool	Windows
Day 18, 01:44	Execution, Defense Evasion, Impact	BlackCat Ransomware Execution	Windows

Times of day are expressed in the primary timezone of the victim organization where our incident response activities took place.

2. Attack path

This chapter describes the attack steps in detail, including possible prevention and detection opportunities where appropriate.

2.1. Download and execution of Credential Stealer

Timestamp	Day 1, 07:35
Techniques	**T1204.002** Malicious File to achieve **TA0002** Execution **T1555** Credentials from Password Stores to achieve **TA0006** Credential Access
Tools	Raccoon Credential Stealer
Target tech	Windows

The adversary most likely gained access to the VPN solution of the victim organization with VPN credentials that were stolen using Raccoon infostealer. Using those stolen credentials, the adversary was able to successfully authenticate to the victim company's network.

The use of information stealers is a wider trend that is observed by Fox-IT. The malware is often spread using sites that distribute irregular and or pirated software. In this case, the execution of a file called Setup1.exe on an employee workstation most likely led to the infection with the information stealer. After infection, a compromised system communicates with a C2 server in order to retrieve different configuration files. Those files are then loaded onto the compromised system with the objective to steal session cookies, retrieve web browser credential databases and extract data from it, such as usernames and passwords. This information is later often used to facilitate ransomware attacks or sold to the highest bidder through so called 'inital access brokers'.

Prevention

Behavior Prevention on Endpoint

Source: ATT&CK mitigation M1040 in the context of technique T1204.002
Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior.

On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria). Note: cloud-delivered protection must be enabled for certain rules. (Microsoft: Use attack surface reduction rules to prevent malware infection, 2021-07-02)

Execution Prevention

Source: ATT&CK mitigation M1038 in the context of technique T1204.002
Block execution of code on a system through application control, and/or script blocking.

Application control may be able to prevent the running of executables masquerading as other files.

Detection

Monitor File Creation

Source: ATT&CK data component File Creation in the context of technique T1204.002
Monitor for newly constructed files that are downloaded and executed on the user's computer.

Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning powershell.exe).

Implementation 1 : Batch File Write to System32

Detection Pseudocode

```
batch_files = filter files where ( extension =".bat" AND file_path = "C:
\Windows\system32*" )
```

Detection Notes

- For Windows, Sysmon Event ID 11 (File create) can be used to track file creation events. This event also provides the Process ID of the process that created the file, which can be correlated with process creation events (e.g., Sysmon Event ID 1) to determine if the file was downloaded from an external network.
- For MacOS, utilities that work in concert with Apple's Endpoint Security Framework such as File Monitor can be used to track file creation events.

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1555
Monitor executed commands and arguments that may search for common password storage locations to obtain user credentials.

Monitor File Access

Source: ATT&CK data component File Access in the context of technique T1555
Monitor for files being accessed that may search for common password storage locations to obtain user credentials.

2.2. Login with stolen VPN credentials

Timestamp	Day 17, 23:11
Techniques	**T1078.002** Domain Accounts to achieve **TA0001** Initial Access **T1133** External Remote Services to achieve **TA0001** Initial Access
Tools	VPN
Target tech	Windows

The adversary most likely gained access to the VPN solution of the victim company with VPN credentials that were stolen by virtue of the Raccoon stealer. With those stolen credentials, the adversary was able to successfully authenticate to the victim company's network.

Prevention

Multi-factor Authentication

Source: ATT&CK mitigation M1032 in the context of technique T1078.002
Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

Integrating multi-factor authentication (MFA) as part of organizational policy can greatly reduce the risk of an adversary gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs.

Privileged Account Management

Source: ATT&CK mitigation M1026 in the context of technique T1078.002
Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

Audit domain account permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account. Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled and use of accounts is segmented, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers. Limit credential overlap across systems to prevent access if account credentials are obtained.

User Training

Source: ATT&CK mitigation M1017 in the context of technique T1078.002
Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.

Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications.

Detection

Monitor Logon Session Creation

Source: ATT&CK data component Logon Session Creation in the context of technique T1078.002
Monitor for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account.

Monitor User Account Authentication

Source: ATT&CK data component User Account Authentication in the context of technique T1078.002
Monitor for an attempt by a user to gain access to a network or computing resource, often by the use of domain authentication services, such as the System Security Services Daemon (sssd) on Linux

Detection Notes

- For Windows, Security Logs events, including Event ID 4624, can be monitored to track user login behavior.
- For Linux, auditing frameworks that support File Integrity Monitoring (FIM), including the audit daemon (auditd), can be used to alert on changes to files that store login information. These files include: `/etc/login.defs`, `/etc/securetty`, `/var/log/faillog`, `/var/log/lastlog`, `/var/log/tallylog`.
- For MacOS, auditing frameworks that support capturing information on user logins, such as OSQuery, can be used to audit user account logins and authentications.

2.3. Network Discovery over VPN

Timestamp	Day 17, 23:12
Techniques	**T1046** Network Service Discovery to achieve **TA0007** Discovery

Tools	VPN
Target tech	Windows

With access to the network, the adversary continued its efforts in trying to gain foothold in the network by conducting reconnaissance. The adversary used the compromised VPN-account to scan and authenticate to a number of servers in the network. As the adversary abused this VPN account, no forensic traces related to any of the tooling could be found on the victim's systems, except for traces of a large number of authentications that took place on different servers within a very short time period.

Prevention

Disable or Remove Feature or Program

Source: ATT&CK mitigation M1042 in the context of technique T1046
Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.

Network Intrusion Prevention

Source: ATT&CK mitigation M1031 in the context of technique T1046
Use intrusion detection signatures to block traffic at network boundaries.

Use network intrusion detection/prevention systems to detect and prevent remote service scans.

Network Segmentation

Source: ATT&CK mitigation M1030 in the context of technique T1046
Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.

Ensure proper network segmentation is followed to protect critical servers and devices.

Detection

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1046
Monitor executed commands and arguments that may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation.

Monitor Network Traffic Flow

Source: ATT&CK data component Network Traffic Flow in the context of technique T1046
Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

2.4. Move laterally over RDP

Timestamp	Day 18, 00:04
Techniques	**T1021.001** Remote Desktop Protocol to achieve **TA0008** Lateral Movement

Tools	Remote Desktop Protocol
Target tech	Windows

After reconnaissance, the adversary opened a Remote Desktop session with the Domain Controller with the Domain Administrator account. It was unclear how the attacker gained access to the privileged Administrator account.

Prevention

Audit

Source: ATT&CK mitigation M1047 in the context of technique T1021.001
Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

Audit the Remote Desktop Users group membership regularly. Remove unnecessary accounts and groups from Remote Desktop Users groups.

Multi-factor Authentication

Source: ATT&CK mitigation M1032 in the context of technique T1021.001
Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

Use multi-factor authentication for remote logins. (Berkeley Security, University of California: Securing Remote Desktop for System Administrators, 2014-11-04)

Detection

Monitor Logon Session Creation

Source: ATT&CK data component Logon Session Creation in the context of technique T1021.001
Monitor for user accounts logged into systems associated with RDP (ex: Windows EID 4624 Logon Type 10). Other factors, such as access patterns (ex: multiple systems over a relatively short period of time) and activity that occurs after a remote login, may indicate suspicious or malicious behavior with RDP.

Monitor Network Connection Creation

Source: ATT&CK data component Network Connection Creation in the context of technique T1021.001
Monitor for newly constructed network connections (typically over port 3389) that may use Valid Accounts (T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Other factors, such as access patterns and activity that occurs after a remote login, may indicate suspicious or malicious behavior with RDP.

2.5. Disable Microsoft Windows Defender

Timestamp	Day 18, 00:04
Techniques	**T1562.001** Disable or Modify Tools to achieve **TA0005** Defense Evasion
Tools	Windows Defender, Windows Registry
Target tech	Windows

The adversary focused on preventing any anti-virus from detecting further malicious activity and tools. For this purpose, Microsoft Windows Defender was disabled on a large number of the affected systems.

Prevention

Restrict File and Directory Permissions

Source: ATT&CK mitigation M1022 in the context of technique T1562.001
Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

Ensure proper process and file permissions are in place to prevent adversaries from disabling or interfering with security services.

Restrict Registry Permissions

Source: ATT&CK mitigation M1024 in the context of technique T1562.001
Restrict the ability to modify certain hives or keys in the Windows Registry.

Ensure proper Registry permissions are in place to prevent adversaries from disabling or interfering with security services.

User Account Management

Source: ATT&CK mitigation M1018 in the context of technique T1562.001
Manage the creation, modification, use, and permissions associated to user accounts.

Ensure proper user permissions are in place to prevent adversaries from disabling or interfering with security services.

Detection

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1562.001
Monitor for the execution of commands and arguments associated with disabling or modification of security software processes or services such as `Set-MpPreference-DisableScriptScanning 1` in Windows,`sudo spctl --master-disable` in macOS, and `setenforce 0` in Linux. Furthermore, on Windows monitor for the execution of taskkill.exe or Net Stop commands which may deactivate antivirus software and other security systems.

Monitor Process Termination

Source: ATT&CK data component Process Termination in the context of technique T1562.001
Monitor processes for unexpected termination related to security tools/services. Specifically, before execution of ransomware, monitor for rootkit tools, such as GMER, PowerTool or TDSSKiller, that may detect and terminate hidden processes and the host antivirus software.

Monitor Service Metadata

Source: ATT&CK data component Service Metadata in the context of technique T1562.001
Monitor for telemetry that provides context of security software services being disabled or modified. In cloud environments, monitor virtual machine logs for the status of cloud security agents.

Monitor Windows Registry Key Modification

Source: ATT&CK data component Windows Registry Key Modification in the context of technique T1562.001
Monitor for changes made to Windows Registry keys and/or values related to services and startup programs that correspond to security tools such as HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender.

2.6. Use Scheduled Tasks to execute the ExMatter Exfiltration tool

Timestamp	Day 18, 00:23
Techniques	**T1053.005** Scheduled Task to achieve **TA0002** Execution **T1048** Exfiltration Over Alternative Protocol to achieve **TA0010** Exfiltration
Tools	ExMatter
Target tech	Windows

As detection was no longer active on most systems, the adversary installed a data exfiltration tool. Although the filename of the tool was sync_enc.exe, reverge engineering efforts showed that the actual file was a tool better known as ExMatter.

This exfiltration tool is often used by different ransomware operators. It was designed to collect and exfiltrate a variety of files from the local file system and from mounted shared folders. Analysis of the exfiltration tool showed that it tries to collect files with the following extensions:

- .pdf
- .doc(x)
- .xls(x)
- .png
- .jp(e)g
- .txt
- .rdp
- .sql
- .msg
- .pst
- .zip
- .rtf
- .ipt
- .dwg

Next, analysis of the executable showed that after collecting these files, exfiltrating occurs over one of three protocols and ports:

- FTP (port 21)
- SFTP (port 22)
- WebDav (port 80)

The firewall logs that were subject of the investigation indicated that, in this particular case, files were extracted over SFTP.

Prevention

Operating System Configuration

Source: ATT&CK mitigation M1028 in the context of technique T1053.005
Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.

Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies >

Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. (Microsoft: Domain controller: Allow server operators to schedule tasks, 2012-11-15)

Operating System Configuration

Source: ATT&CK mitigation M1028 in the context of technique T1053.005
Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.

Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. (Microsoft: Domain controller: Allow server operators to schedule tasks, 2012-11-15)

Network Intrusion Prevention

Source: ATT&CK mitigation M1031 in the context of technique T1048
Use intrusion detection signatures to block traffic at network boundaries.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level.

Network Segmentation

Source: ATT&CK mitigation M1030 in the context of technique T1048
Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.

Follow best practices for network firewall configurations to allow only necessary ports and traffic to enter and exit the network. (Microsoft: Perimeter Firewall Design, 2004-02-06)

Detection

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1053.005
Monitor executed commands and arguments for actions that could be taken to gather tasks may also be created through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Implementation 1 : New processes whose command line includes commands that create or modify scheduled tasks with a suspicious script, extension or user writable path

Detection Pseudocode

```
suspicious_processes = filter ProcessId, ProcessFilePath, command_line,
ProcessParentFilePath,ProcessParentCommandLine where (EventId == "1" OR EventId ==
"4688") AND command_line LIKE '%SCHTASKS%' AND (command_line LIKE '%/CREATE%' OR
command_line LIKE '%/CHANGE%') AND (command_line LIKE '%.cmd%' OR command_line LIKE
'%.ps1%' OR command_line LIKE '%.vbs%' OR command_line LIKE '%.py%' OR command_line LIKE
'%.js%' OR command_line LIKE '%.exe%' OR command_line LIKE '%.bat%' OR command_line LIKE
'%javascript%' OR command_line LIKE '%powershell%' OR command_line LIKE '%rundll32%' OR
command_line LIKE '%wmic%' OR command_line LIKE '%cmd%' OR command_line LIKE '%cscript%'
OR command_line LIKE '%wscript%' OR command_line LIKE '%regsvr32%' OR command_line LIKE
'%mshta%' OR command_line LIKE '%bitsadmin%' OR command_line LIKE '%certutil%' OR
command_line LIKE '%msiexec%' OR command_line LIKE '%javaw%' OR command_line LIKE '%
[%]APPDATA[%]%' OR command_line LIKE '%\\AppData\\Roaming%' OR command_line LIKE '%
[%]PUBLIC[%]%' OR command_line LIKE '%C:\\Users\\Public%' OR command_line LIKE '%
[%]ProgramData[%]%' OR command_line LIKE '%C:\\ProgramData%' OR command_line LIKE '%
[%]TEMP[%]%' OR command_line LIKE '%\\AppData\\Local\\Temp%' OR command_line LIKE '%\
\Windows\\PLA\\System%' OR command_line LIKE '%\\tasks%' OR command_line LIKE '%\
\Registration\\CRMLog%' OR command_line LIKE '%\\FxsTmp%' OR command_line LIKE '%\\spool\
\drivers\\color%' OR command_line LIKE '%\\tracing%' OR)
```

Monitor File Modification

Source: ATT&CK data component File Modification in the context of technique T1053.005
Monitor Windows Task Scheduler stores in %systemroot%\System32\Tasks for change entries related to scheduled tasks that do not correlate with known software, patch cycles, etc.

Monitor Process Creation

Source: ATT&CK data component Process Creation in the context of technique T1053.005
Monitor for newly constructed processes and/or command-lines that execute from the svchost.exe in Windows 10 and the Windows Task Scheduler taskeng.exe for older versions of Windows. (Loobeek, L: leoloobeek Status, 2017-12-08) If scheduled tasks are not used for persistence, then the adversary is likely to remove the task when the action is complete.

Implementation 1 : New processes whose parent processes are svchost.exe or taskeng.exe

Detection Pseudocode

```
suspicious_processes = filter ProcessId, ProcessFilePath, ProcessParentFilePath where
(EventId == "1" OR EventId == "4688") AND (ProcessParentFilePath LIKE '%svchost.exe%' OR
ProcessParentFilePath LIKE '%taskeng.exe%')
```

Detection Notes

- Look for instances of `schtasks.exe` running as processes. The `command_line` field is necessary to disambiguate between types of schtasks commands. These include the flags `/create` , `/run`, `/query`, `/delete`, `/change`, and `/end`.

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1048
Monitor executed commands and arguments that may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.

Monitor Network Connection Creation

Source: ATT&CK data component Network Connection Creation in the context of technique T1048
Monitor for newly constructed network connections that are sent or received by untrusted hosts.

Monitor Network Traffic Content

Source: ATT&CK data component Network Traffic Content in the context of technique T1048
Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider

correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

Monitor Network Traffic Flow

Source: ATT&CK data component Network Traffic Flow in the context of technique T1048
Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

2.7. BlackCat Ransomware Execution

Timestamp	Day 18, 01:44
Techniques	**T1053.005** Scheduled Task to achieve **TA0002** Execution **T1070.001** Clear Windows Event Logs to achieve **TA0005** Defense Evasion **T1112** Modify Registry to achieve **TA0005** Defense Evasion **T1486** Data Encrypted for Impact to achieve **TA0040** Impact
Tools	BlackCat
Target tech	Windows

The adversary used scheduled tasks to execute BlackCat ransomware on multiple hosts.

This ransomware encrypts files with AES and ChaCha20 encryption algorithms. It can be configured with a JSON file, allowing ransomware operators to customize folder, file and extension controls, configuring self-destruct options and more. Upon execution, the ransomware service creates a unique Tor .onion domain for a new victim company. On this Tor network site, the leaked data is index and can be browsed without downloading the complete data leak, making the whole data set easily available to everbody who has interest.

The ransomware executable changed the filenames of encrypted files to [filename].[original_extension].<7-random letters and numbers>. The investigation material indicated that group policy objects were updated and PsExec was executed on the affected servers. Fox-IT suspects that ransomware was deployed by manipulating group policy objects. This deployment method is also consistent with the modus operandi BlackCat actor. However, the deployment method could be verified due to a lack of evidence on the domain controllers.

After encrypting all files, the ransomware utilized several legitimate executables to maximise the impact of the attack. These executables are listed in the table below.

Executable	Command	Impact
vssadmin.exe	vssadmin.exe Delete Shadows /all /quiet	Deletes backups to prevent recovery
wmic.exe	wmic.exe Shadowcopy Delete	Delete shadow copies
reg.exe	reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f	Modify the registry to change MaxMpxCt settings; Executed to increase the number of outstanding requests allowed
wevtutil.exe	for /F \"tokens=*\" %1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%1\"	Clear Eventlogs
net.exe	net.exe net use \\[computer name] /user:[domain]\[user] [password] /persistent:no	Mount network shares

Prevention

Remote Data Storage

Source: ATT&CK mitigation M1029 in the context of technique T1070.001
Use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information.

Automatically forward events to a log server or data repository to prevent conditions in which the adversary can locate and manipulate data on the local system. When possible, minimize time delay on event reporting to avoid prolonged storage on the local system.

Restrict Registry Permissions

Source: ATT&CK mitigation M1024 in the context of technique T1112
Restrict the ability to modify certain hives or keys in the Windows Registry.

Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.

Behavior Prevention on Endpoint

Source: ATT&CK mitigation M1040 in the context of technique T1486
Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior.

On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware. (Microsoft: Use attack surface reduction rules to prevent malware infection, 2021-07-02)

Data Backup

Source: ATT&CK mitigation M1053 in the context of technique T1486
Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.

Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. (Ready.gov: IT Disaster Recovery Plan, 2019-03-15) 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. Consider enabling versioning in cloud environments to maintain backup copies of storage objects. (Gietzen, S: S3 Ransomware Part 2: Prevention and Defense, 2021-04-14)

Detection

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1053.005
Monitor executed commands and arguments for actions that could be taken to gather tasks may also be created through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Implementation 1 : New processes whose command line includes commands that create or modify scheduled tasks with a suspicious script, extension or user writable path

Detection Pseudocode

```
suspicious_processes = filter ProcessId, ProcessFilePath, command_line,
ProcessParentFilePath,ProcessParentCommandLine where (EventId == "1" OR EventId ==
"4688") AND command_line LIKE '%SCHTASKS%' AND (command_line LIKE '%/CREATE%' OR
command_line LIKE '%/CHANGE%') AND (command_line LIKE '%.cmd%' OR command_line LIKE
'%.ps1%' OR command_line LIKE '%.vbs%' OR command_line LIKE '%.py%' OR command_line LIKE
'%.js%' OR command_line LIKE '%.exe%' OR command_line LIKE '%.bat%' OR command_line LIKE
'%javascript%' OR command_line LIKE '%powershell%' OR command_line LIKE '%rundll32%' OR
command_line LIKE '%wmic%' OR command_line LIKE '%cmd%' OR command_line LIKE '%cscript%'
OR command_line LIKE '%wscript%' OR command_line LIKE '%regsvr32%' OR command_line LIKE
'%mshta%' OR command_line LIKE '%bitsadmin%' OR command_line LIKE '%certutil%' OR
command_line LIKE '%msiexec%' OR command_line LIKE '%javaw%' OR command_line LIKE '%
[%]APPDATA[%]%' OR command_line LIKE '%\\AppData\\Roaming%' OR command_line LIKE '%
[%]PUBLIC[%]%' OR command_line LIKE '%C:\\Users\\Public%' OR command_line LIKE '%
[%]ProgramData[%]%' OR command_line LIKE '%C:\\ProgramData%' OR command_line LIKE '%
[%]TEMP[%]%' OR command_line LIKE '%\\AppData\\Local\\Temp%' OR command_line LIKE '%\
\Windows\\PLA\\System%' OR command_line LIKE '%\\tasks%' OR command_line LIKE '%\
\Registration\\CRMLog%' OR command_line LIKE '%\\FxsTmp%' OR command_line LIKE '%\\spool\
\drivers\\color%' OR command_line LIKE '%\\tracing%' OR)
```

Monitor Process Creation

Source: ATT&CK data component Process Creation in the context of technique T1053.005
Monitor for newly constructed processes and/or command-lines that execute from the svchost.exe in Windows 10 and the Windows Task Scheduler taskeng.exe for older versions of Windows. (Loobeek, L: leoloobeek Status, 2017-12-08) If scheduled tasks are not used for persistence, then the adversary is likely to remove the task when the action is complete.

Implementation 1 : New processes whose parent processes are svchost.exe or taskeng.exe

Detection Pseudocode

```
suspicious_processes = filter ProcessId, ProcessFilePath, ProcessParentFilePath where
(EventId == "1" OR EventId == "4688") AND (ProcessParentFilePath LIKE '%svchost.exe%' OR
ProcessParentFilePath LIKE '%taskeng.exe%')
```

Detection Notes

- Look for instances of `schtasks.exe` running as processes. The `command_line` field is necessary to disambiguate between types of schtasks commands. These include the flags `/create` , `/run`, `/query`, `/delete`, `/change`, and `/end`.

Monitor Scheduled Job Creation

Source: ATT&CK data component Scheduled Job Creation in the context of technique T1053.005
Monitor for newly constructed scheduled jobs by enabling the “Microsoft-Windows-TaskScheduler/Operational” setting within the event logging service. (Satyajit321: Scheduled Tasks History Retention settings, 2015-11-03) Several events will then be logged on scheduled task activity, including: Event ID 106 on Windows 7, Server 2008 R2 - Scheduled task registered; Event ID 4698 on Windows 10, Server 2016 - Scheduled task created; Event ID 4700 on Windows 10, Server 2016 - Scheduled task enabled; Event ID 4701 on Windows 10, Server 2016 - Scheduled task disabled

Implementation 1 : New schedule tasks whose content includes suspicious scripts, extensions or user writable path

Detection Pseudocode

```
suspicious_scheduled_jobs = filter UserName, JobName, JobContent where EventId == "4698"
AND (JobContent LIKE '%.cmd%' OR JobContent LIKE '%.ps1%' OR JobContent LIKE '%.vbs%' OR
JobContent LIKE '%.py%' OR JobContent LIKE '%.js%' OR JobContent LIKE '%.exe%' OR
JobContent LIKE '%.bat%' OR JobContent LIKE '%javascript%' OR JobContent LIKE
'%powershell%' OR JobContent LIKE '%wmic%' OR JobContent LIKE '%rundll32%' OR JobContent
LIKE '%cmd%' OR JobContent LIKE '%cscript%' OR JobContent LIKE '%wscript%' OR JobContent
LIKE '%regsvr32%' OR JobContent LIKE '%mshta%' OR JobContent LIKE '%bitsadmin%' OR
JobContent LIKE '%certutil%' OR JobContent LIKE '%msiexec%' OR JobContent LIKE '%javaw%'
OR JobContent LIKE '%[%]APPDATA[%]%' OR JobContent LIKE '%\\AppData\\Roaming%' OR
JobContent LIKE '%[%]PUBLIC[%]%' OR JobContent LIKE '%C:\\Users\\Public%' OR JobContent
LIKE '%[%]ProgramData[%]%' OR JobContent LIKE '%C:\\ProgramData%' OR JobContent LIKE '%
[%]TEMP[%]%' OR JobContent LIKE '%\\AppData\\Local\\Temp%' OR JobContent LIKE '%\
\Windows\\PLA\\System%' OR JobContent LIKE '%\\tasks%' OR JobContent LIKE '%\
\Registration\\CRMLog%' OR JobContent LIKE '%\\FxsTmp%' OR JobContent LIKE '%\\spool\
\drivers\\color%' OR JobContent LIKE '%\\tracing%')
```

Detection Notes

- Detection of the creation or modification of Scheduled Tasks with a suspicious script, extension or user writable path. Attackers may create or modify Scheduled Tasks for the persistent execution of malicious code. This detection focuses at the same time on EventIDs 4688 and 1 with process creation (SCHTASKS) and EventID 4698, 4702 for Scheduled Task creation/ modification event log.

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1070.001
Monitor executed commands and arguments for actions that would delete Windows event logs (via PowerShell) such as `Remove-EventLog -LogName Security`.

Detection Notes

- Event ID 4104 (from the Microsoft-Windows-Powershell/Operational log) captures Powershell script blocks, which can be analyzed and used to detect on attempts to Clear Windows Event Logs. In particular, Powershell has a built-in Clear-EventLog cmdlet that allows for a specified log to be cleared.

Monitor File Deletion

Source: ATT&CK data component File Deletion in the context of technique T1070.001
Monitor for unexpected deletion of Windows event logs (via native binaries) and may also generate an alterable event (Event ID 1102: “The audit log was cleared”)

Monitor OS API Execution

Source: ATT&CK data component OS API Execution in the context of technique T1070.001
Monitor for Windows API calls that may clear Windows Event Logs to hide the activity of an intrusion.

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1112
Monitor executed commands and arguments for actions that could be taken to change, conceal, and/or delete information in the Registry. The Registry may also be modified through Windows system

management tools such as Windows Management Instrumentation and PowerShell, which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Monitor Process Creation

Source: ATT&CK data component Process Creation in the context of technique T1112
Monitor processes and command-line arguments for actions that could be taken to change, conceal, and/or delete information in the Registry. (i.e. reg.exe, regedit.exe)

Implementation 1 : Suspicious Processes

Detection Pseudocode

```
reg_processes = filter processes where ( (event_id == "1" OR event_id == "4688") AND (exe == "reg.exe" AND parent_exe == "cmd.exe") )
cmd_processes = filter processes where ( (event_id == "1" OR event_id == "4688") AND (exe == "cmd.exe" AND parent_exe != "explorer.exe"") )
reg_and_cmd_processes = join (reg_processes, cmd_processes) where (reg.parent_pid == cmd.pid and reg.hostname == cmd.hostname)
```

Detection Notes

- Pseudocode Event IDs are for Sysmon (Event ID 1 - process create) and Windows Security Log (Event ID 4688 - a new process has been created).
- The Detection Pseudocode is oriented around detecting invocations of Reg (S0075) where the parent executable is an instance of cmd.exe that wasn't spawned by explorer.exe. The built-in utility reg.exe provides a command-line interface to the registry, so that queries and modifications can be performed from a shell, such as cmd.exe. When a user is responsible for these actions, the parent of cmd.exewill typically be explorer.exe. Occasionally, power users and administrators write scripts that do this behavior as well, but likely from a different process tree. These background scripts must be baselined so they can be tuned out accordingly.

Monitor Windows Registry Key Modification

Source: ATT&CK data component Windows Registry Key Modification in the context of technique T1112
Monitor for changes made to windows registry keys or values. Consider enabling Registry Auditing on specific keys to produce an alertable event (Event ID 4657) whenever a value is changed (though this may not trigger when values are created with Reghide or other evasive methods). (Miroshnikov, A. & Hall, J: 4657(S): A registry value was modified, 2017-04-18) Changes to Registry entries that load software on Windows startup that do not correlate with known software, patch cycles, etc., are suspicious, as are additions or changes to files within the startup folder. Changes could also include new services and modification of existing binary paths to point to malicious files. If a change to a service-related entry occurs, then it will likely be followed by a local or remote service start or restart to execute the file.

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1486
Monitor executed commands and arguments for actions involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit

Monitor File Modification

Source: ATT&CK data component File Modification in the context of technique T1486
Monitor for changes made to files in user directories.

Monitor Process Creation

Source: ATT&CK data component Process Creation in the context of technique T1486
Monitor for newly constructed processes and/or command-lines involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit.

3. MITRE ATT&CK TTPs

This chapter lists the MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) of the attack described in this report. The TTPs are listed in the order they were observed in the attack. They are formatted in a table to facilitate ingestion of this data into other tools, such as Threat Intelligence Platforms (TIPs).

Note that each tactic-technique-procedure combination is listed here, which can lead to apparent duplication. For example, if a procedure is linked to more than one technique, it will be listed repeatedly for each technique.

Tactic	Technique	Procedure
TA0002 Execution	**T1204.002** Malicious File	The adversary most likely gained access to the VPN solution of the victim organization with VPN credentials that were stolen using Raccoon infostealer. Using those stolen credentials, the adversary was able to successfully authenticate to the victim company's network.
TA0006 Credential Access	**T1555** Credentials from Password Stores	The adversary most likely gained access to the VPN solution of the victim organization with VPN credentials that were stolen using Raccoon infostealer. Using those stolen credentials, the adversary was able to successfully authenticate to the victim company's network.
TA0001 Initial Access	**T1078.002** Domain Accounts	The adversary most likely gained access to the VPN solution of the victim company with VPN credentials that were stolen by virtue of the Raccoon stealer. With those stolen credentials, the adversary was able to successfully authenticate to the victim company's network.
TA0001 Initial Access	**T1133** External Remote Services	The adversary most likely gained access to the VPN solution of the victim company with VPN credentials that were stolen by virtue of the Raccoon stealer. With those stolen credentials, the adversary was able to successfully authenticate to the victim company's network.
TA0007 Discovery	**T1046** Network Service Discovery	With access to the network, the adversary continued its efforts in trying to gain foothold in the network by conducting reconnaissance. The adversary used the compromised VPN-account to scan and authenticate to a number of servers in the network. As the adversary abused this VPN account, no forensic traces related to any of the tooling could be found on the victim's systems, except for traces of a large number of authentications that took place on different servers within a very short time period.
TA0008 Lateral Movement	**T1021.001** Remote Desktop Protocol	After reconnaissance, the adversary opened a Remote Desktop session with the Domain Controller with the Domain Administrator account. It was unclear how the attacker gained access to the privileged Administrator account.
TA0005 Defense Evasion	**T1562.001** Disable or Modify Tools	The adversary focused on preventing any anti-virus from detecting further malicious activity and tools. For this purpose, Microsoft Windows Defender was disabled on a large number of the affected systems.
TA0002 Execution	**T1053.005** Scheduled Task	As detection was no longer active on most systems, the adversary installed a data exfiltration tool. Although the filename of the tool was sync_enc.exe, reverge engineering efforts showed that the actual file was a tool better known as ExMatter.
TA0010 Exfiltration	**T1048** Exfiltration Over Alternative Protocol	As detection was no longer active on most systems, the adversary installed a data exfiltration tool. Although the filename of the tool was sync_enc.exe, reverge engineering efforts showed that the actual file was a tool better known as ExMatter.
TA0002 Execution	**T1053.005** Scheduled Task	The adversary used scheduled tasks to execute BlackCat ransomware on multiple hosts.
TA0005 Defense Evasion	**T1070.001** Clear Windows Event Logs	The adversary used scheduled tasks to execute BlackCat ransomware on multiple hosts.
TA0005 Defense Evasion	**T1112** Modify Registry	The adversary used scheduled tasks to execute BlackCat ransomware on multiple hosts.
TA0040 Impact	**T1486** Data Encrypted for Impact	The adversary used scheduled tasks to execute BlackCat ransomware on multiple hosts.