

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

par Equipe CERT | Oct 18, 2022 | CERT, Cyber Threat Intelligence

Search

Rechercher

Recent Posts

China :
Vulnerabilities as a
strategic resource

A stalker in the box: infrastructure linking PandoraHVC and Mesh Central

The EV Code Signature Market for eCrime

Kerberos OPSEC: Offense & Detection Strategies for Red and Blue Team – Part 2 : AS_REP Roasting

Matanbuchus & Co:
Code Emulation and
Cybercrime
Infrastructure
Discovery

Archives

Sélectionner un mo

Categories

Actualités

Avis de vulnérabilité

Bulletin d'analyse

CERT

Conseil SSI

Cyber Threat Intelligence

Engineering

Evaluation Sécurité

Evenement

Recherche et
Développement

Red Teaming

DSSI à temps partagé

En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies afin de réaliser des statistiques de visites.



Our deep 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 actionable 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

APT27 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 (a.k.a LuckyMouse, EmissaryPanda, Iron Tiger or Mustang Panda) is a supposed nation state cyber threat actor linked to RPC government. 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 government'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.

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

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

```
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)
```

```
cmd.exe wmic [IP] [DOMAIN] [ACCOUNT]  
[PASSWORD]
```

Persistence

Typical next step after a successful initial intrusion is to ensure persistence within the target's network and be sure that attacker's will not be kick-out easily.

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 exhaustive):

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

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).

First, a legitimate program (linked to CyberArk software) (`vfhost.exe / mspeng.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 finally 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.

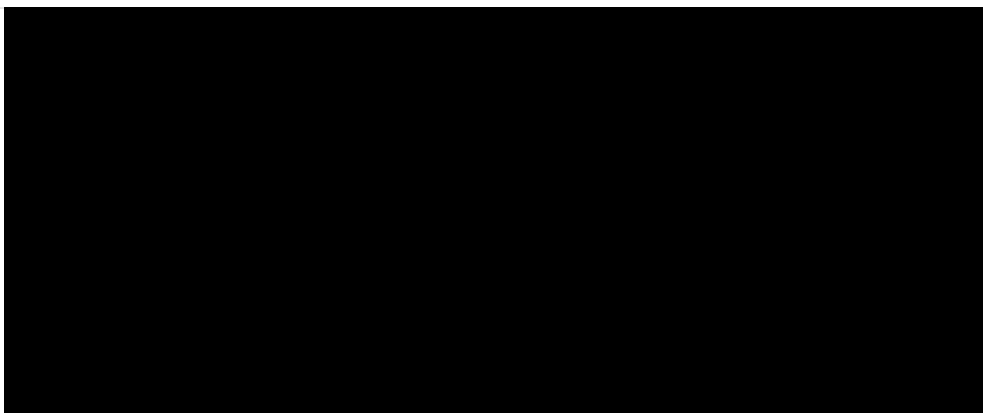
```
%ProgramData%\windefenders\  
%ProgramData%\windefenders\config.ini  
%ProgramData%\windefenders\msmpeng.exe  
%ProgramData%\windefenders\thumb.dat  
%ProgramData%\windefenders\vftrace.dll  
%ProgramFiles%\Common Files\windefenders\  
%ProgramFiles%\Common Files\windefenders\config.ini  
%ProgramFiles%\Common 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\windefen  
ders  
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windefenders
```

CERT Intrinsic made a tool to extract HyperBro configuration from Stage 2 samples.

Description

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.

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 configuration



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		Remote Services: SMB



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

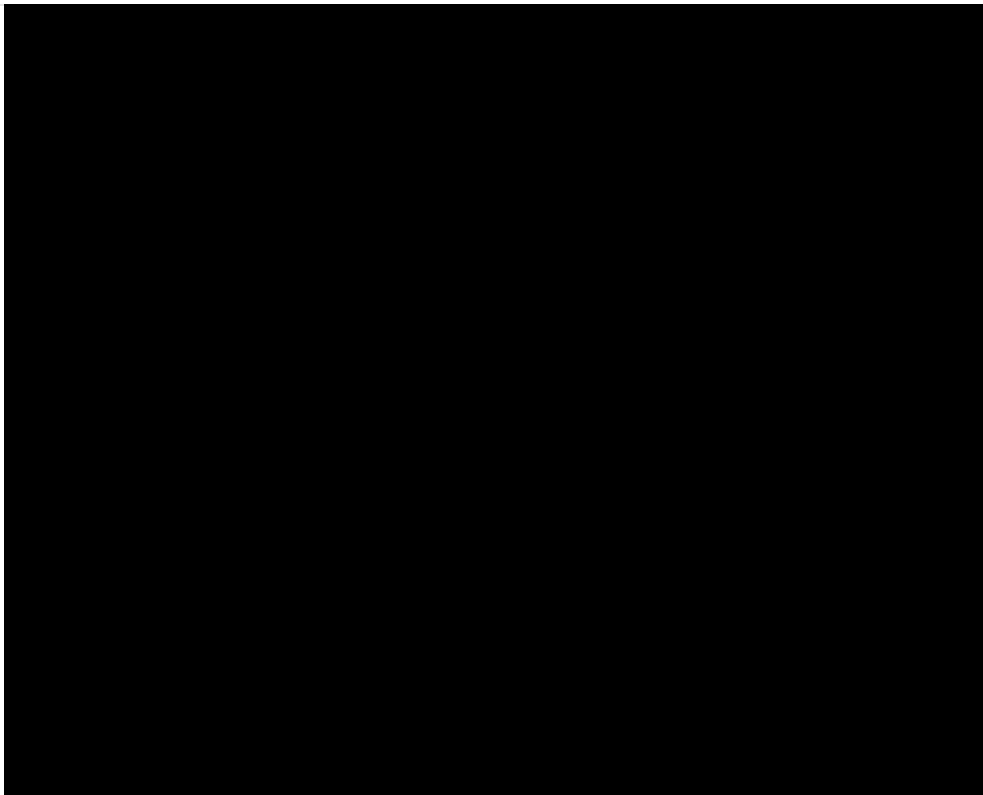
HOST_A      DNS_NAME
Windows Server      [REDACTED]
....

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
```

They also used Remote Desktop protocol, to connect to computers within the targeted organisation's network, and admin shares to move laterally.

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

In order to stealth authentication materials on compromised hosts, adversaries relied on the mimikatz tool. However, they tried to stay stealthy and used the sysinternal's procdump tool, renamed in **error.log** to bypass Windows Defender detection and dump lsass process memory :



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 or Modify Tools
Defense Evasion	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control (UAC bypass using CMSTPLUA COM interface)

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

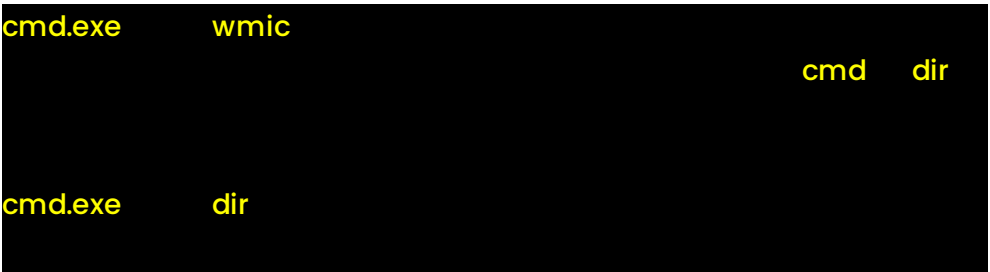
Tactic ID	Technique ID	Technique Name
Command and Control	T1090.001	Proxy: Internal Proxy
Command and Control	T1071.001	Application Layer Protocol: Web Protocols

cmd.exe	wmic	127.0.0.1	9080
---------	------	-----------	------

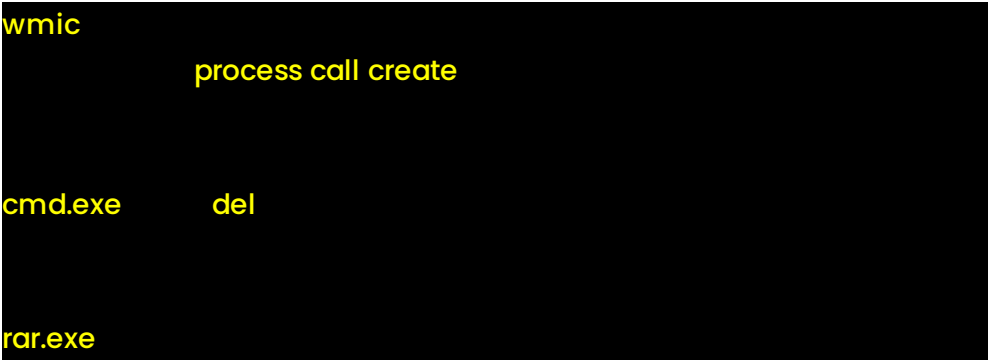
Tactic ID	Technique ID	Technique Name
Collection	T1560.001	Archive Collected Data: Archive via Utility
Collection	T1114.001	Email Collection: Local Email collection
Collection	T1074.001	Data Staged : Local Data Staging
Collection	T1074.002	Data Staged: Remote Data



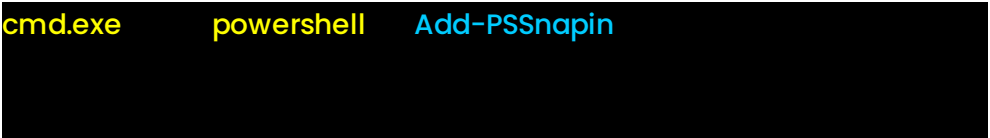
Operators then browsed directories in order to find personal information and data related to research and development, leveraging **dir** command and **wmic** to look for files on network shares.



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.



Besides, APT27 operators collected data about mailboxes on the Exchange server, using **Get-Mailbox** powershell command, as shown below :



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

[...]

```
. \Program Files\Microsoft\Exchange
Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resour
ces\error.part025.rar
```

```
. \Program Files\Microsoft\Exchange
Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resour
ces\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.

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.

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

- HFS-Consulting AG Incident Response Report
- BfV Cyber-Brief Nr. 01/2022
- Palo Alto Networks
- TrendMicro

Intrinsic

Notre métier ? Protéger le vôtre

© 2023 Intrinsec Sécurité

Mentions légales

Protection des données

personnelles

INTRINSEC

Nos expertises

Ressources utiles

Notre entreprise

Votre carrière

Contactez-nous


SUIVEZ-NOUS



En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies afin de réaliser des statistiques de visites.

Ok En savoir plus

📞 Une question ? Contactez notre standard : 01 41 91 58 61 – Un incident de sécurité ? Faites-vous assister : 01 47 28 38 39



Vos objectifs ▾


Nos expertises ▾

Rejoignez-nous ▾

L'entreprise ▾

Actualités ▾

Contact

 ▾