APT31 INTRUSION SET CAMPAIGN

DESCRIPTION AND COUNTERMEASURES

Version 1.0

December 15, 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

Table of contents

Summary

In January 2021, ANSSI was informed of a large campaign of attacks against French entities linked to the APT31 intrusion set.

The investigations carried out by ANSSI led to the analysis of the intrusion set's entire chaine of infection. In turn, the knowledge acquired was used to monitor malicious activity and proactively identify already infected victims.

One characteristic of this intrusion set lies in its use of an anonymisation infrastructure consisting of a set of compromised routers organised as a mesh network. This network is orchestrated using a malware named **Pakdoor** by ANSSI.

It has not been possible to identify any targeting criteria used by the intrusion set, whether sectoral or thematic. A reasonable hypothesis is that the use of this intrusion set follows an opportunistic approach to breach the information systems of French entities and then proceeds to exploiting this initial access to reach its goals.

Following the publication of indicators of compromise on the CERT-FR's website on July 21st 2021[1], this report lays out the technical information related to this campaign of attacks: chain of infection (section 1), analysis of the attack infrastructure (section 2) as well as the observed victimology (section 3).

[1] See `https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003/` for more information

1. Infection chain

A full list of the techniques, tactics and procedures observed during the various compromises can be found in appendix A.2.

1.1. Reconnaissance

1.1.1. Web browsing

An analysis of the traffic coming from the attacker's anonymisation infrastructure described in section 2 shed light on some reconnaissance actions.

Several connections have been identified corresponding to straightforward browsing on legitimate websites, with no links to any traces of or attempts at intrusion.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Reconnaissance	T1593.002	Search Open Websites/Domains: Search Engines	Use vitimes website to collect information
Reconnaissance	T1594	Search Victim-Owned Websites	Use vitimes website to collect information

1.1.2. Spearphishing

APT31 has been using the GMass service since at least 2018 for some phishing campaigns.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Reconnaissance	T1598.003	Phishing for Information : Spearphishing Link	0 pixel image

1.2. Intrusion vectors

1.2.1. Brute force

The APT31 intrusion set uses brute force methods to log into exposed services when it does not have a password, or has obtained password hashes.

In addition to remote access services such as VPN services, brute force has been observed on the Exchange server automatic discovery (*Autodiscover*) protocol. A vulnerability does indeed make it possible to recover user passwords[2].

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Credential Access	T1110.001	Brute Force: Password Guessing	Use of local accounts
Credential Access	T1110.003	Brute Force: Password Spraying	
Initial Access	T1190	Exploit Public-Facing Application	Exploit Autodiscover vulnerability

[2] See https://www.guardicore.com/labs/autodiscovering-the-great-leak/ for more information about this vulnerability.

1.2.2. Use of legitimate accounts

During this campaign, one of the intrusion methods observed is the use of valid local accounts to log in to services exposed on the internet, such as:

- VPN;
- RDP;
- OFFICE 365.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Initial Access	T1078.003	Valid Accounts: Local Accounts	Use local accounts
Initial Access	T1078.004	Valid Accounts: Cloud Accounts	Use local accounts

1.2.3. Exploitation of vulnerabilities

Proxylogon

One of the means used by APT31 to compromise its victims is the exploitation of *CVE-2021-27065*, also known as *ProxyLogon*. The earliest trace of this method being exploited dates from 2 March 2021, the same day that MICROSOFT made a public announcement about this vulnerability[3]. This suggests that APT31, like other threat actors, had early access to the vulnerability[4].

Fortinet

The intrusion set exploits the *CVE-2018-13379* vulnerability affecting FORTINET VPN products. By exploiting this vulnerability, the intrusion set was able to obtain the login credentials of users using this VPN service[5].

SQL injection

The APT31 intrusion set uses SQL code injection to compromise exposed websites.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Initial Access	T1190	Exploit Public Facing Application	Exploit ProxyLogon and FortiOS vulnerabilties – SQL injection

1.3. Malicious codes

ANSSI's investigations uncovered instances of malware specific to the threat actor who may run a **Cobalt Strike Beacon**.

A list of other tools used by the intrusion set can be found in appendix A.1.

[3] See `https://proxylogon.com/` for more information about this vulnerability.

[4] See `https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/` for more information

[5] See `https://www.fortiguard.com/psirt/FG-IR-13-384` for more information about this vulnerability.

1.4. Persistence

1.4.1. Scheduled tasks

The APT31 intrusion set creates and deletes scheduled tasks in order to execute its malware. These tasks are placed in the WINDOWS default directory « `\Windows\System32\Tasks` ».

The following paths and names of scheduled tasks were observed:

- `test`
- `QLSearch`
- `chkdsksvc`
- `AgnPtiHe`
- `TLYnpNGy`
- `pOBCQYfo`
- `Microsoft Helps Center`
- `Microsoft\Windows\DirectX\DXGIAdapterlog`
- `Microsoft\Windows\DirectX\DXGIAdapterlogs`
- `Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319 x64`

Technique, tactic and procedure used:

Phase	ATT&CK	Name	Comment
Persistence	T1053.005	Scheduled Task/Job: Scheduled Task	Use scheduled task to execute malwares

1.4.2. Accounts and services

The APT31 intrusion sets uses privileged accounts on the victim's information system to maintain the initial access it has obtained. It then uses these credentials to log onto the various services exposed on the internet.

In order to maintain its foothold on the victim's network, the intrusion set is able to create accounts, in *Active Directory* or locally, which mimic the names of people with higher privileges as well as legitimate services and applications.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Persistence	T1078.002	Valid Accounts: Domain Accounts	Use local accounts
Persistence	T1078.003	Valid Accounts: Local Accounts	Use local accounts
Persistence	T1133	External Remote Services	Use local accounts
Persistence	T1078.001	Valid Accounts: Default Accounts	Use local accounts
Persistence	T1136.002	Create Accounts : Domain Accounts	Create privileged account

1.4.3. Web shell

Once it has succeeded in breaching the first machine on the victim's network, the intrusion set drops web shells in order to keep its access open.

Technique, tactic and procedure used:

Phase	ATT&CK	Name	Comment
Persistence	T1505.003	Server Software Component: Web Shell	Drop WebShell after initial compromise

1.5. Privilege escalation

1.5.1. Vulnerability exploitation

The vulnerability « `CVE-2021-26885` » affecting the WINDOWS *WalletService* application is exploited by the intrusion set in order to increase its privileges [6].

The intrusion set uses the **Juicy Potato** tool to execute code with SYSTEM privileges.

Techniques, tactic and procedure used:

Phase	ATT&CK	Name	Comment
Privilege Escalation	T1068	Exploitation for Privilege Escalation	Exploit CVE-2021-26885
Privilege Escalation	T1134.005	Access Token Manipulation: SID-History Injection	Juicy Potato tool

1.5.2. Memory recovery

The intrusion set hijacks the legitimate program « `comsvcs.dll` » to perform memory dumps, allowing it to recover the information contained in the processes, in particular the *local security authority subsystem service* (LSASS). Example of dump observed:

```
C:\> powershell -c rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 624 C:\Windows\Temp\log.txt
```

Technique, tactic and procedure used:

Phase	ATT&CK	Name	Comment
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	Dump LSASS memory
Credential Access	T1003.005	OS Credential Dumping: Cached Domain Credentials	Dump process memory

1.6. Evasion methods

1.6.1. Firewall

The attacker creates filtering rules on firewalls in order to reach its own infrastructure from the victim's network. When naming these rules, the intrusion set spoofs the name of legitimate applications. For instance, a rule named « `Xbox Game Center` » was uncovered on a victim's infrastructure.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	Use the name of legitimate softwares
Defense Evasion	T1562.004	Impair Defenses: Disable or Modify System Firewall	Add firexall rules

1.6.2. Antivirus

The attacker uses the exception rules provided by WINDOWS DEFENDER to disable or enable the monitoring of specific directories. Below is an example of rules implemented in PowerShell:

```
  PS C:\> Add-MpPreference -ExclusionPath 'C:\Windows\Temp'
```

[6] See `https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26885` for more information about this vulnerability.

Technique, tactic and procedure used:

Phase	ATT&CK	Name	Comment
Defense Evasion	T1562.001	Impair Defenses: Disable or Modify Tools	Desactivate Windows Defender

1.6.3. File deletion

The intrusion set deletes some of its tools and files after use in order to cover up its tracks.

Technique, tactic and procedure used:

Phase	ATT&CK	Name	Comment
Defense Evasion	T1070.004	Indicator Removal on Host: File Deletion	Remove tools and temporary files

1.6.4. Masquerading

APT31 uses names of legitimate services to conceal its codes. In addition, the intrusion set uses the naming convention of a victim's network to choose an appropriate name for the machines under its control.

Phase	ATT&CK	Name	Comment
Defense Evasion	T1036.004	Masquerading: Masquerade Task or Service	Use perfmon.exe legitime service
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location	Match network machins nomenclature

1.7. Discovery

APT31 favours the tools contained natively in the target environment, both to find out which services are being executed and to see which other machines are present on the network. These tools are:

- `tasklist`;
- `netstat`;
- `ipconfig`;
- `net`;
- `ping`.

Moreover, the intrusion set uses the **Active Directory Explorer** tool to recover information about the different accounts.

Technique, tactic and procedure used:

Phase	ATT&CK	Name	Comment
Discovery	T1057	Process Discovery	Use tasklist command
Discovery	T1049	System Network Connections Discovery	Use netstat command for network data collection
Discovery	T1087.002	Account Discovery: Domain Account	Use net command
Discovery	T1046	Network Service Scanning	Network scan for RDP SMB or LDAP services
Discovery	T1087.001	Account Discovery	Use AD explorer tool

1.8. Lateral movement

In order to be able to move laterally within its victim's network, the APT31 intrusion set uses *Remote Desktop Protocol* (RDP) and *File Transfer Protocol* (FTP). It was also observed using the *Server Message Block* (SMB) protocol to transfer its code and tools.

These different protocols are used by masquerading as local accounts.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol	Use local accounts
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	Use local accounts
Lateral Movement	T1570	Lateral Tool Transfer	Use local accounts
Lateral Movement	T1210	Exploitation of Remote Services	Use RDP protocol

1.9. Data collection

During its campaign, the intrusion set collect several data types such as registries and emails. The data collected is sometimes compressed using the WinRAR tool prior to possible exfiltration.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Collection	T1560.001	Archive Collected Data: Archive via Utility	Use rar files
Collection	T1005	Data from Local System	Registry data collection
Collection	T1114.001	Email Collection: Local Email Collection	Email collection

1.10. Exfiltration

During its campaign, the intrusion set was able to exfiltrate user databases, emails and sensitive business data.

1.10.1. Creation of email accounts

In order to exfiltrate data from a Microsoft *Exchange* server, the intrusion set might use the impersonation function (or *ApplicationImpersonation* role). This allows a service account to be granted access to several mailboxes. To do this, the APT31 intrusion set creates accounts named « `HealthMailbox<*>` » (where * represents seven alphanumerical characters) on Microsoft *Exchange* servers.

These accounts then attempt to masquerade as legitimate *HealthMailbox* accounts which take the following format: « `HealthMailbox<`*GUID*`>` ».

1.10.2. *Domain Name System* (DNS)

The intrusion set uses Cobalt Strike to exfiltrate the data collected through the DNS protocol.

1.10.3. *Server Message Block* (SMB)

The intrusion set uses the SMB remote file sharing protocol to exfiltrate large amounts of data.

Techniques, tactics and procedures used:

Phase	ATT&CK	Name	Comment
Exfiltration	T1048.003	Exfiltration Over Alternative Protocol: Obfuscated Non-C2 Protocol	Use of DNS and SMB protocols
Exfiltration	T1567	Exfiltration Over Web Service	Exchange accounts
Defense Evasion	T1078.003	Valid Accounts: Local Accounts	*HealthMailbox* account

2. Anonymisation infrastructure

2.1. Targeted equipment

The infrastructure used during this campaign consists of a network of compromised machines, more specifically of *Small Office/Home Office* (SOHO) routers. These are mainly Pakedge, Sophos and Cisco branded routers.

About a thousand IP addresses used by the attacker during this campaign have been discovered[7]. 623 of these addresses have been linked to one brand and one particular model of routers. This could be determined through the analysis of the exposed services. However, this analysis alone is not sufficient in itself to formally precisely determine which devices were used. Several devices can indeed exist behind a single IP address. A statistical analysis of this subset of IP addresses does, however, reveal an over-representation of certain brands of router.

2.1.1. Pakedge

Pakedge routers represent 64% of the compromised routers identified. Among these routers, the folowing models were identified:

- Pakedge RE-1
- Pakedge RE-2
- Pakedge RK-1
- Pakedge RK-2

2.1.2. Other routers

Although Pakedge routers make up a significant proportion of the routers identified, the following brands were also observed:

- Sophos Cyberoam;
- Cisco (models RV042 and RV042G).

The method used by APT31 to breach these devices has not been identified. The hypotheses are as follows :

- The different brands of routers share a firmware which may present vulnerabilities. For example, the vulnerability affecting *Realtek Managed Switch Controller* could be found in several models of router by different brands, including Pakedge and Cisco[8].
- Different vulnerabilities were exploited on each type of router.

[7] For confidentiality reason, these IP cannot be shared.

[8] See https://www.exploit-db.com/exploits/47442 for more information on this vulnerability.

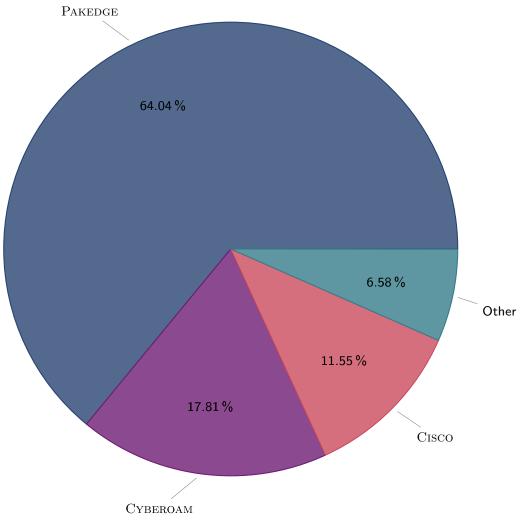

Fig. 2.1. – Breakdown of the different router brands identified

2.2. Pakdoor

In order to manage the infected routers and allow them to communicate with each other, a sophisticated backdoor, named **Pakdoor** by ANSSI, was installed on every machine. Its analysis can be found in the report « `APT31: Pakdoor` ».

2.3. Representation of the anonymisation infrastructure

Using elements provided by ANSSI partners, together with the **Pakdoor** code analysis, it is possible to depict the anonymisation infrastructure as follows:

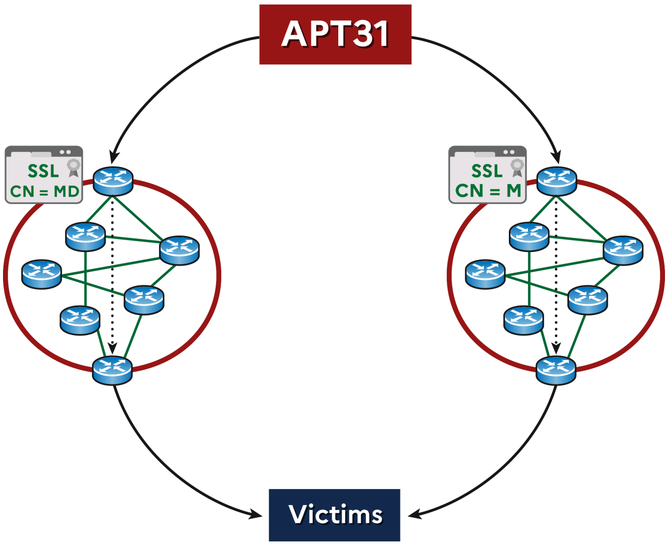

Fig. 2.2. – Diagram of the infrastructure used by the APT31 intrusion set during the attack campaign.

2.4. Use of the anonymisation infrastructure

The threat actor's command and control infrastructure (C2) is based on the anonymisation infrastructure. Indeed, some **Cobalt Strike Beacon** C2 domains were linked to breached routers [9].

APT31 also uses this infrastructure to conduct scans and web browsing. It would appear that the threat actor uses this infrastrcuture as its main anonymisation layer of all of its communications.

3. Victimology

An analysis of the different targets of this campaign reveals that victims were targeted broadly. It is therefore likely that for this campaign, the APT31 intrusion set was opportunistic in its approach to selecting targets.

[9] See `https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/` for more information

A. Appendices

A.1. Tools

Tools used by the intrusion set during this campaign.

A.1.1. WinRAR

WinRAR is a freely available data compression tool. In particular, it can be used upstream of an exfiltration phase.

For more information, see `https://www.win-rar.com`.

A.1.2. Active Directory Explorer

Active Directory Explorer was created and made available by MICROSOFT as an *Active Directory* viewer and editor.

For more information, see `https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer`.

A.1.3. Metasploit

Metasploit is used to exploit vulnerabilities on a remote machine.

For more information, see `https://www.metasploit.com/`.

A.1.4. RCMD

The intrusion set uses the « `Create_read()` » function of the GITHUB **Scripts-AllInThere** project created by the account ZX7FFA4512-VBS. This function is used to write the result of a function entered as an argument in the WINDOWS registry.

For more information, see `https://github.com/Zx7ffa4512-VBS/Scripts-AllInThere/blob/master/RCMD.vbs`.

A.1.5. Juicy Potato

Juicy Potato is a tool used in WINDOWS to masquerade as a service account in order to execute commands with *System* privileges.

For more information, see `https://github.com/ohpe/juicy-potato`.

A.1.6. Cobalt Strike

The intrusion set might use the **Cobalt Strike** post-exploitation tool to communicate with its own tools located on a victim's network.

For more information, see `https://www.cobaltstrike.com`.

Configuration file observed during this campaign:

```
BeaconType                       - Pure DNS
Port                             - 1
SleepTime                        - 900000
MaxGetSize                       - 2098660
Jitter                           - 20
MaxDNS                           - 235
PublicKey_MD5                    - 3cf546012a46ffebc3a0a60a456acaee
C2Server                         - api.last-key[.]com,/search/
UserAgent                        - Mozilla/4.0 (compatible; MSIE 8.0; Win32)
HttpPostUri                      - /Search/
Malleable_C2_Instructions        - Remove 833 bytes from the end
                                   Remove 675 bytes from the beginning
                                   NetBIOS decode 'a'
HttpGet_Metadata                 - ConstHeaders
                                        Host: www.bing.com
                                        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                        Cookie: DUP=Q=GpO1nJpMnam4UllEfmeMdg2&T=283767088&A=1&IG
                                   ConstParams
                                        go=Search
                                        qs=bs
                                        form=QBRE
                                   Metadata
                                        base64url
                                        parameter "q"
HttpPost_Metadata                - ConstHeaders
                                        Host: www.bing.com
                                        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                        Cookie: DUP=Q=GpO1nJpMnam4UllEfmeMdg2&T=283767088&A=1&IG
                                   ConstParams
                                        go=Search
                                        qs=bs
                                   SessionId
                                        base64url
                                        parameter "form"
                                   Output
                                        base64url
                                        parameter "q"
PipeName                         -
DNS_Idle                         - 128.56.57.58
DNS_Sleep                        - 0
SSH_Host                         - Not Found
SSH_Port                         - Not Found
SSH_Username                     - Not Found
SSH_Password_Plaintext           - Not Found
SSH_Password_Pubkey              - Not Found
SSH_Banner                       -
HttpGet_Verb                     - GET
HttpPost_Verb                    - GET
HttpPostChunk                    - 96
Spawnto_x86                      - %windir%\syswow64\rundll32.exe
Spawnto_x64                      - %windir%\sysnative\rundll32.exe
CryptoScheme                     - 0
Proxy_Config                     - Not Found
Proxy_User                       - Not Found
Proxy_Password                   - Not Found
Proxy_Behavior                   - Use IE settings
Watermark                        - 305419896
bStageCleanup                    - False
bCFGCaution                      - False
KillDate                         - 0
bProcInject_StartRWX             - True
bProcInject_UseRWX               - True
bProcInject_MinAllocSize         - 0
ProcInject_PrependAppend_x86     - Empty
ProcInject_PrependAppend_x64     - Empty
ProcInject_Execute               - CreateThread
                                   SetThreadContext
                                   CreateRemoteThread
                                   RtlCreateUserThread
ProcInject_AllocationMethod      - VirtualAllocEx
bUsesCookies                     - True
HostHeader                       -
headersToRemove                  - Not Found
DNS_Beaconing                    - Not Found
DNS_get_TypeA                    - Not Found
DNS_get_TypeAAAA                 - Not Found
DNS_get_TypeTXT                  - Not Found
DNS_put_metadata                 - Not Found
DNS_put_output                   - Not Found
DNS_resolver                     - Not Found
DNS_strategy                     - Not Found
DNS_strategy_rotate_seconds      - Not Found
DNS_strategy_fail_x              - Not Found
DNS_strategy_fail_seconds        - Not Found
```

A.2. Techniques, tactics and procedures

Phases	TTPS
Initial Access	Exploit Public-Facing Application
	External Remote Services
	Valid Accounts
	Valid Accounts: Cloud Accounts
Execution	Windows Management Instrumentation
	Scheduled Task/Job: Scheduled Task
	Service Execution
Persistence	Scheduled Task/Job: Scheduled Task
	Server Software Component: Web Shell
	External Remote Services
	Hijack Execution Flow: DLL Side-Loading
	Valid Accounts: Local Accounts
	Valid Accounts: Domain Accounts
	Create of Modify System Process: Windows Service
	Account Manipulation: Exchange Email Delegate Permissions
	Boot or Logon Initialization Scripts: RC Scripts
	Create Account: Domain Account
	Create Account: Local Account
	DLL Side-Loading
Privilege Escalation	Access Token Manipulation: SID-History Injection
	Exploitation for Privilege Escalation
	Scheduled Task/Job: Scheduled Task
	Valid Accounts: Local Accounts
Defense Evasion	Indicator Removal on Host: File Deletion
	Process Injection: Dynamic-link Library Injection
	Impair Defenses: Disable or Modify System Firewall
	Impair Defenses: Disable or Modify Tools
	DLL Side-Loading
	Masquerading
	Masquerading: Masquerade Task or Service
	Masquerading: Match Legitimate Name or Location
	Modify Registry
	Obfuscated Files or Information
	Process Injection
	Valid Accounts: Local Accounts
Credential Access	OS Credential Dumping: Cached Domain Credentials
	OS Credential Dumping: LSASS Memory
	Brute Force: Password Guessing
	Brute Force: Password Spraying
Discovery	Account Discovery: Domain Account
	Network Service Scanning
	Account Discovery: Local Account
	File and Directory Discovery
	Account Discovery
	Process Discovery
	Remote System Discovery
	System Network Configuration Discovery
	System Network Connections Discovery
	System Service Discovery
Lateral Movement	Exploitation of Remote Services
	Remote Services: SMB/Windows Admin Shares
Collection	Archive Collected Data: Archive via Utility
	Email Collection: Local Email Collection
	Data from Local System
Command and Control	Application Layer Protocol: Web Protocols
	Proxy
Exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
	Exfiltration Over Alternative Protocol

Version 1.0 - December 15, 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN