TLP:WHITE

CAMPAGNE D'ATTAQUE DU MODE OPÉRATOIRE *APT31*

DESCRIPTION ET CONTRE-MESURES

Version 1.0

15 décembre 2021

TLP:WHITE

Sommaire

Résumé

En janvier 2021, l'ANSSI est informée d'une vaste campagne d'attaques à l'encontre d'entités françaises liée au mode opératoire d'attaque (MOA) *APT31*.

Les investigations réalisées par l'ANSSI ont permis d'analyser l'ensemble de la chaîne de compromission du mode opératoire. La connaissance acquise permet de suivre les activités malveillantes afin d'agir en prévenant des compromissions, et en réaction, en découvrant des victimes déjà compromises.

Une particularité de ce mode opératoire réside dans l'utilisation d'une infrastructure d'anonymisation constituée d'un ensemble de routeurs compromis organisés sous la forme d'un réseau maillé. Ce dernier est orchestré à l'aide d'un code malveillant baptisé **Pakdoor** par l'ANSSI.

Il n'a pas été possible de mettre en évidence de critères de ciblage du MOA, qu'ils soient sectoriels ou thématiques. Il est possible d'émettre l'hypothèse que le mode opératoire ait une démarche opportuniste d'intrusion sur des systèmes d'information d'entités françaises, avant d'exploiter les accès obtenus selon ses besoins.

Faisant suite à la publication sur le site du CERT-FR le 21 juillet 2021 d'indicateurs de compromission liés à cette campagne [1], ce rapport présente les informations techniques liées à cette campagne d'attaque : la chaine d'infection (section 1), l'analyse de l'infrastructure d'attaque (section 2) et la victimologie observée (section 3).

1. Voir `https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003/` pour plus d'informations

1. Chaine d'infection

L'ensemble des techniques, tactiques et procédures observées lors des différentes compromissions se trouve en annexe A.2.

1.1. Reconnaissance

1.1.1. Navigation web

L'analyse du trafic provenant de l'infrastructure d'anonymisation de l'attaquant décrite en section 2 a permis de mettre en évidence des actions de reconnaissance.

De nombreuses connexions correspondant à de la simple navigation sur des sites Internet légitimes ont été identifiées, sans aucune trace ou tentative de compromission liée.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Reconnaissance	T1593.002	Search Open Websites/Domains : Search Engines	Collecte d'informations depuis les sites web de ses cibles
Reconnaissance	T1594	Search Victim-Owned Websites	Collecte d'informations depuis les sites web de ses cibles

1.1.2. Hameçonnage ciblé

APT31 utilise le service GMass depuis au moins 2018 pour ses campagnes d'hameçonnage.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Reconnaissance	T1598.003	Phishing for Information : Spearphishing Link	Lien présent dans un courriel - image 0 pixel

1.2. Vecteurs d'intrusion

1.2.1. *Brute force*

Le mode opératoire *APT31* utilise des méthodes de *brute force* lorsqu'il ne dispose pas de mot de passe, ou après l'obtention de condensats de mots de passe, pour se connecter à des services exposés.

En plus des services d'accès à distance tels que les services VPN, du *brute force* a été observé sur le protocole de découverte automatique de serveur Exchange (*Autodiscover*). En effet, une vulnérabilité permet de récupérer les mots de passe des utilisateurs [2].

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Credential Access	T1110.001	Brute Force : Password Guessing	Utilisation d'identifiants de comptes locaux
Credential Access	T1110.003	Brute Force : Password Spraying	
Initial Access	T1190	Exploit Public-Facing Application	Exploitation de vulnérabilité Autodiscover

2. Voir https://www.guardicore.com/labs/autodiscovering-the-great-leak/ pour plus d'informations sur cette vulnérabilité.

1.2.2. Utilisation de comptes légitimes

Au cours de cette campagne, l'une des méthodes d'intrusion observée est l'utilisation de comptes locaux valides pour se connecter à des services exposés sur Internet, tels que :

- VPN ;
- RDP ;
- Office365.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Initial Access	T1078.003	Valid Accounts : Local Accounts	Utilisation de comptes locaux
Initial Access	T1078.004	Valid Accounts : Cloud Accounts	Utilisation de comptes locaux

1.2.3. Exploitations de vulnérabilités

Proxylogon

L'un des moyens utilisés par *APT31* pour compromettre ses victimes, est l'exploitation de la *CVE-2021-27065* aussi appelée *ProxyLogon*. Cette dernière a été observée au plus tôt le 2 mars 2021, soit le même jour que l'annonce publique par Microsoft de cette vulnérabilité [3].

La concomitance des dates de publication par Microsoft et de l'exploitation par *APT31* laisse supposer que ce dernier, comme d'autres modes opératoires, ait eu accès à la vulnérabilité avant la publication de Microsoft [4].

Fortinet

Le MOA exploite la vulnérabilité *CVE-2018-13379* affectant des produits VPN Fortinet. L'exploitation de cette vulnérabilité a permis au MOA d'obtenir des identifiants d'utilisateurs utilisant ce service VPN [5].

Injection SQL

Le mode opératoire *APT31* utilise des injections de code SQL pour compromettre des sites web exposés.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Initial Access	T1190	Exploit Public Facing Application	Exploitation de vulnérabilités ProxyLogon Injection SQL et FortiOS

1.3. Code malveillant déposé

Les investigations réalisées ont montré que l'attaquant dispose de plusieurs codes permettant d'exécuter un implant **Beacon Cobalt Strike**.

La liste des outils également utilisés par le mode opératoire est disponible en annexe A.1.

3. Voir `https://proxylogon.com/` pour plus d'informations sur cette vulnérabilité.
4. Voir `https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/` pour plus d'informations
5. Voir `https://www.fortiguard.com/psirt/FG-IR-13-384` pour plus d'informations sur cette vulnérabilité.

1.4. Persistance

1.4.1. Tâches planifiées

Le MOA *APT31* crée et supprime des tâches planifiées pour exécuter ses codes malveillants. Ces tâches sont placées dans le répertoire par défaut de WINDOWS « `\Windows\System32\Tasks` ».

Les chemins et noms de tâches planifiées suivants ont été observés :

- `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, tactique et procédure utilisée :

Phase	ATT&CK	Name	Commentaire
Persistence	T1053.005	Scheduled Task/Job : Scheduled Task	Utilisation de tâches planifiées pour exécuter des codes malveillants

1.4.2. Comptes et services

Le MOA *APT31* utilise des comptes utilisateurs à privilèges du système d'information de sa victime pour maintenir ses accès. En effet, il utilise ces identifiants pour se connecter aux différents services exposés sur Internet.

Dans le but de maintenir sa présence sur le réseau de sa victime, le MOA peut créer des comptes, sur l'*Active Directory* ou localement, qui imitent le nom de personnes ayant des privilèges élevés ainsi que des services et applications légitimes.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Persistence	T1078.002	Valid Accounts : Domain Accounts	Utilisation de comptes locaux
Persistence	T1078.003	Valid Accounts : Local Accounts	Utilisation de comptes locaux
Persistence	T1133	External Remote Services	Utilisation de comptes locaux
Persistence	T1078.001	Valid Accounts : Default Accounts	Utilisation de comptes locaux
Persistence	T1136.002	Create Accounts : Domain Accounts	Création de compte à privilèges

1.4.3. *Web shell*

Après avoir compromis une première machine sur le réseau de sa victime, le MOA dépose des *web shells* pour maintenir son accès.

Technique, tactique et procédure utilisée :

Phase	ATT&CK	Name	Commentaire
Persistence	T1505.003	Server Software Component : Web Shell	Dépot de WebShell apres compromission

1.5. Élévation de privilèges

1.5.1. Exploitation de vulnérabilité

L'exploitation de la vulnérabilité « `CVE-2021-26885` » affectant l'application *WalletService* de WINDOWS est utilisée par le MOA pour accroitre ses privilèges [6].

Le MOA utilise l'outil **Juicy Potato** qui permet d'exécuter du code avec les privilèges *System*.

Techniques, tactique et procédure utilisée :

Phase	ATT&CK	Name	Commentaire
Privilege Escalation	T1068	Exploitation for Privilege Escalation	Exploitation de la CVE-2021-26885
Privilege Escalation	T1134.005	Access Token Manipulation : SID-History Injection	Outil Juicy Potato

1.5.2. Collecte mémoire

Le MOA détourne le programme légitime « `comsvcs.dll` » pour effectuer des *dumps* de la mémoire, ce qui permet de récupérer les informations présentes dans les processus, en particulier *local security authority subsystem service* (LSASS). Exemple de *dump* observé :

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

Technique, tactique et procédure utilisée :

Phase	ATT&CK	Name	Commentaire
Credential Access	T1003.001	OS Credential Dumping : LSASS Memory	Récupération de la zone mémoire de LSASS
Credential Access	T1003.005	OS Credential Dumping : Cached Domain Credentials	Récupération de la zone mémoire de processus

1.6. Méthodes d'évasions

1.6.1. Pare-feu

L'attaquant crée des règles de filtrage sur les pare-feux dans le but de pouvoir joindre son infrastructure depuis le réseau de sa victime. Pour le nom de ces règles, le MOA usurpe le nom d'applications légitimes. En effet, la création de la règle nommée « `Xbox Game Center` » a été observée.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Defense Evasion	T1036.005	Masquerading : Match Legitimate Name or Location	Utilisation de noms de logiciels légitimes
Defense Evasion	T1562.004	Impair Defenses : Disable or Modify System Firewall	Ajout de règles de sortie

1.6.2. Antivirus

L'attaquant utilise les règles d'exception mises à disposition par l'antivirus WINDOWS DEFENDER pour désactiver ou activer la surveillance de répertoires spécifiques par ce dernier. Ci-dessous un exemple de mise en place de règles en Powershell :

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

6. Voir `https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26885` pour plus d'informations sur cette vulnérabilité.

Technique, tactique et procédure utilisée :

Phase	ATT&CK	Name	Commentaire
Defense Evasion	T1562.001	Impair Defenses : Disable or Modify Tools	Désactivation de Windows Defender

1.6.3. Suppression de fichier

Le MOA supprime certains de ses outils et fichiers après utilisation pour dissimuler ses traces.

Technique, tactique et procédure utilisée :

Phase	ATT&CK	Name	Commentaire
Defense Evasion	T1070.004	Indicator Removal on Host : File Deletion	Suppression de codes et fichiers temporaires

1.6.4. Usurpation

APT31 utilise des noms de services légitimes pour dissimuler ses codes. Par ailleurs, le MOA utilise la nomenclature du réseau de ses victimes pour choisir un nom approprié aux machines qu'il contrôle.

Phase	ATT&CK	Name	Commentaire
Defense Evasion	T1036.004	Masquerading : Masquerade Task or Service	Usurpation du service perfmon.exe
Defense Evasion	T1036.005	Masquerading : Match Legitimate Name or Location	Renommage de machine avec la nomenclature du réseau

1.7. Exploration

APT31 privilégie les outils nativement présents sur l'environnement de ses victimes à la fois pour connaître les services en cours d'exécution ainsi que pour connaître les autres machines présentes sur le réseau. Ces outils sont :

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

En plus de ces outils, le MOA utilise également l'outil **Active Directory Explorer** pour collecter des informations sur les différents comptes.

Technique, tactique et procédure utilisée :

Phase	ATT&CK	Name	Commentaire
Discovery	T1057	Process Discovery	Commande tasklist
Discovery	T1049	System Network Connections Discovery	Commande netstat
Discovery	T1087.002	Account Discovery : Domain Account	Commande net
Discovery	T1046	Network Service Scanning	Scan de services réseau RDP SMB et LDAP
Discovery	T1087.001	Account Discovery	Outil AD explorer

1.8. Latéralisation

Dans l'objectif de se latéraliser à l'intérieur du réseau de sa victime, le MOA *APT31* utilise les protocoles *Remote Desktop Protocol* (RDP) et *File Transfert Protocol* (FTP). L'utilisation du protocole *Server Message Block* (SMB) pour transférer ses codes et outils a également été observé.

Ces différents protocoles sont utilisés en usurpant les comptes locaux.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Lateral Movement	T1021.001	Remote Services : Remote Desktop Protocol	Utilisation de comptes locaux
Lateral Movement	T1021.002	Remote Services : SMB/Windows Admin Shares	Utilisation de comptes locaux
Lateral Movement	T1570	Lateral Tool Transfer	Utilisation de comptes locaux
Lateral Movement	T1210	Exploitation of Remote Services	Service RDP

1.9. Collecte de données

Au cours de cette campagne, le MOA a collecté plusieurs types de données comme des bases de registres et des courriels. Les données collectées sont parfois compressées à l'aide de l'outil WinRAR avant une éventuelle exfiltration.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Collection	T1560.001	Archive Collected Data : Archive via Utility	Utilisation de fichier rar
Collection	T1005	Data from Local System	Collecte d'éléments de la base de registre
Collection	T1114.001	Email Collection : Local Email Collection	Collecte de boite de courriels

1.10. Exfiltration

Au cours de cette campagne, l'attaquant a pu exfiltrer des bases de données d'utilisateurs, des courriels ainsi que des données métier sensibles.

1.10.1. Création de comptes courriel

Pour exfiltrer des données depuis un serveur Microsoft *Exchange*, le MOA peut utiliser la fonctionnalité d'emprunt d'identité (ou rôle *ApplicationImpersonation*). Cette dernière permet de donner à un compte de service accès à plusieurs boîtes aux lettres. Pour ce faire, le MOA *APT31* crée des comptes nommés « `HealthMailbox<*>` » (où * représente 7 caractères alphanumériques) sur des serveurs Microsoft *Exchange*.

Ces comptes tentent ainsi d'usurper les comptes légitimes *HealthMailbox* qui ont le format suivant : « `HealthMailbox<`*GUID*`>` ».

1.10.2. *Domain Name System* (DNS)

Le MOA utilise Cobalt Strike pour exfiltrer les données collectées à travers le protocole DNS.

1.10.3. *Server Message Block* (SMB)

Le MOA utilise le protocole de partage de fichier distant SMB pour exfiltrer de grandes quantités de données.

Techniques, tactiques et procédures utilisées :

Phase	ATT&CK	Name	Commentaire
Exfiltration	T1048.003	Exfiltration Over Alternative Protocol : Obfuscated Non-C2 Protocol	Utilisation des protocoles DNS et SMB
Exfiltration	T1567	Exfiltration Over Web Service	Comptes exchange
Defense Evasion	T1078.003	Valid Accounts : Local Accounts	Création de comptes *HealthMailbox*

2. Infrastructure d'anonymisation

2.1. Équipements ciblés

L'infrastructure utilisée lors de cette campagne est constituée d'un ensemble de machines compromises et plus particulièrement de routeurs *Small Office / Home Office* (SOHO). Ces derniers sont principalement des routeurs des marques Pakedge, Sophos et Cisco.

Environ un millier d'adresses IP utilisées par l'attaquant au cours de cette campagne ont été découvertes [7]. 623 de ces IP ont pu être reliées à une marque, voire un modèle de routeurs, grâce aux services qu'ils exposent. L'analyse des certificats TLS exposés ne permet cependant pas de caractériser formellement les équipements réseaux. En effet, plusieurs équipent peuvent se trouver derrière une même IP. Néanmoins, l'analyse statistique de ce sous ensemble d'adresses IP permet d'observer une sur-représentation de certaines marques de routeurs.

2.1.1. Pakedge

Les routeurs de la marque Pakedge représentent environ 64% des machines compromises identifiées. Parmi ces routeurs, des compromissions ont été effectivement observées sur les modèles suivants :

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

2.1.2. Autres routeurs

Bien que les routeurs de la marque Pakedge représentent une part importante des routeurs identifiés, les autres marques suivantes ont été observées :

- Sophos Cyberoam ;
- Cisco (modèles RV042 et RV042G).

La méthode utilisée par le MOA *APT31* pour compromettre ces équipements réseau n'a pas été identifiée, cependant plusieurs hypothèses sont possibles :

- Les différentes marques de routeurs ont un microgiciel en commun qui présenterait des vulnérabilités. Par exemple, la vulnérabilité affectant *Realtek Managed Switch Controller* rend vulnérable plusieurs modèles de routeur de différentes marques dont Pakedge et Cisco [8].
- Plusieurs vulnérabilités différentes auraient été utilisées sur chaque marque et modèle de routeurs.

7. L'ensemble de ces adresses IP ne peut être partagé pour des raisons de confidentialité
8. Voir `https://www.exploit-db.com/exploits/47442` pour plus d'informations sur cette vulnérabilité.

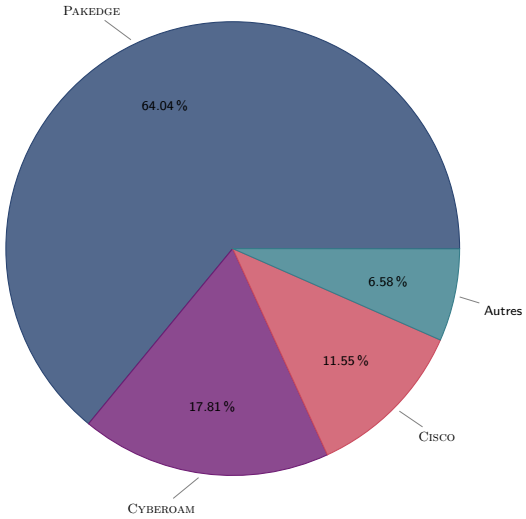

FIG. 2.1. – Répartition des différentes marques de routeurs identifiées

2.2. Pakdoor

Afin d'administrer les routeurs compromis et pour les faire communiquer entre eux, *APT31* installe une porte dérobée sophistiquée sur ces derniers. Celle-ci n'étant pas connue en source ouverte, elle a été nommée **Pakdoor** par l'ANSSI.

L'analyse détaillée de ce code est disponible dans le rapport « `APT31 : Pakdoor` ».

2.3. Représentation de l'infrastructure d'anonymisation

Les éléments fournis par des partenaires de l'ANSSI ainsi que l'analyse du code **Pakdoor** permettent de représenter l'infrastructure d'anonymisation sous la forme suivante :

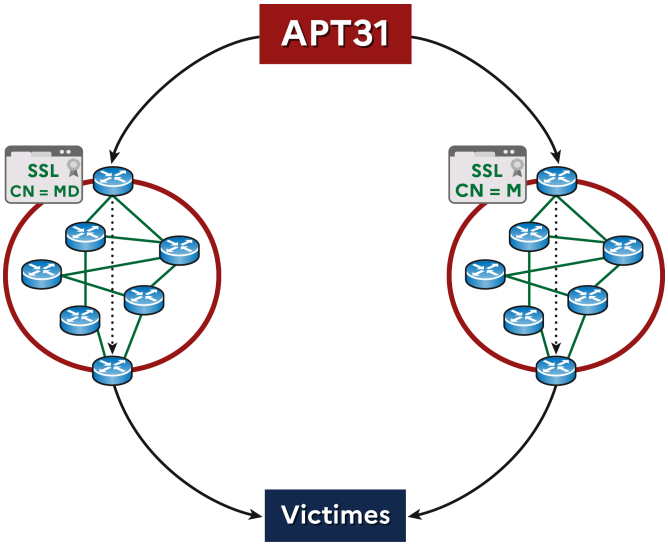

FIG. 2.2. – Schéma de l'infrastructure utilisée par le MOA *APT31* lors de la campagne d'attaque

2.4. Utilisation de l'infrastructure d'anonymisation

L'infrastructure de commande et de contrôle (C2) utilisée par *APT31* repose sur l'infrastructure d'anonymisation. En effet, des noms de domaines utilisés par des implants **Beacon Cobalt Strike** du MOA résolvent des IP correspondantes à des routeurs compromis [9].

La variété d'utilisation de cette infrastructure laisse penser qu'il s'agit de la principale couche d'anonymisation de l'ensemble des communications des opérateurs du MOA *APT31* vers Internet.

3. Victimologie

L'analyse des différentes cibles de cette campagne permet de constater un ciblage large. Il est ainsi probable que dans le cadre de cette campagne, le MOA *APT31* ait eu une approche opportuniste dans le choix de ses victimes.

9. Voir `https://www.sekoia.io/en/walking-on-apt31-infrastructure-footprints/` pour plus d'informations

A. Annexes

A.1. Outils

Outils utilisés par le MOA au cours de cette campagne.

A.1.1. WinRAR

WinRAR est un outil librement disponible permettant de faire de la compression de données. Il peut notamment être utilisé en amont d'une phase exfiltration.

Pour plus d'information, voir `https://www.win-rar.com`.

A.1.2. Active Directory Explorer

Active Directory Explorer est un outil créé et mis à disposition par MICROSOFT pour visualiser et modifier un *Active Directory*.

Pour plus d'information, voir `https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer`.

A.1.3. Metasploit

Metasploit est un outil utilisé pour exploiter des vulnérabilités sur une machine distante.

Pour plus d'information, voir `https://www.metasploit.com/`.

A.1.4. RCMD

Le MOA utilise la fonction « `Create_read()` » du projet GITHUB **Scripts-AllInThere** créé par le compte ZX7FFA4512-VBS. Cette fonction permet d'écrire le résultat d'une fonction passée en argument dans la base de registre de WINDOWS.

Pour plus d'information, voir
`https://github.com/Zx7ffa4512-VBS/Scripts-AllInThere/blob/master/RCMD.vbs`.

A.1.5. Juicy Potato

Juicy Potato est un outil permettant sous WINDOWS d'usurper un compte de service pour executer des commandes avec des privilèges *System*.

Pour plus d'information, voir `https://github.com/ohpe/juicy-potato`.

A.1.6. Cobalt Strike

Le MOA peut utiliser l'outil de post-exploitation **Cobalt Strike** pour communiquer avec ses outils situés sur le réseau de ses victimes.

Pour plus d'information, voir `https://www.cobaltstrike.com`.

Fichier de configuration observé lors de cette campagne :

```
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, tactiques et procédures

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 - 15 décembre 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