aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois d'août 2024

2024-09-04 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

Sommaire

1. Synthèse

Ce mois-ci, le CERT aDvens vous propose trois vulnérabilités d'intérêts, en complément de celles déjà publiées.

Au travers de deux articles, les analystes du CERT présentent :

- Une analyse de l'implant KoreanSpritz utilisée par l'APT LAZARUS
- Un tour d'horizon sur les activités des groupes hacktivistes.

2. Vulnérabilités

2.1. CVE-2024-4885

La chercheuse en sécurité Sina Kheirkhah de Summoning Team a découvert une vulnérabilité (CVE-2024-4885) affectant Progress WhatsUp Gold en avril 2024. Cette faille a été corrigée par l'éditeur dans son bulletin de juin 2024. Des tentatives d'exploitation de cette vulnérabilité ont ensuite été observées par la Shadowserver Foundation à partir du 1er août 2024.

Un défaut de contrôle des extensions de fichier dans la fonction *WhatsUp.ExportUtilities.Export.GetFileWithoutZip* de Progress WhatsUp Gold permet à un attaquant non authentifié, en envoyant des requêtes HTTP spécifiquement forgées, de téléverser un script malveillant et de l'exécuter avec les privilèges *iisapppool\Inmconsole*.

2.1.1. Type de vulnérabilité

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

2.1.2. Risque

- Exécution de code arbitraire

2.1.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.1.4. Produits impactés

- Progress WhatsUp Gold versions 2023.1.x antérieures à 2023.1.3

2.1.5. Recommandations

- Mettre à jour Progress WhatsUp Gold vers la version 2023.1.3 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Progress WhatsUp Gold.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2. CVE-2024-28986

Le 15 août 2024, le CISA a ajouté la CVE-2024-28986 à son catalogue des vulnérabilités exploitées. Celle-ci affecte l'outil de bureau à distance *Web Help Desk* de SolarWinds, et a été initialement publiée le 09 août 2024.

Un défaut de désérialisation Java dans SolarWinds Web Help Desk permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire.

2.2.1. Type de vulnérabilité

- **CWE-502**: Deserialization of Untrusted Data

2.2.2. Risque

- Exécution de code arbitraire

2.2.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.2.4. Produits impactés

- SolarWinds Web Help Desk version 12.8.3 et versions antérieures.

2.2.5. Recommandations

- Mettre à jour SolarWinds Web Help Desk vers la version 12.8.3 HF 1 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de SolarWinds.

2.2.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

2.3. CVE-2024-36971

Dans son bulletin de sécurité Android du 05/08/2024, Google signale que le noyau Android est impacté par la CVE-2024-36971, affectant à la base le noyau Linux. Celle-ci est déclarée exploitée par l'éditeur, qui ne l'attribue pas à un acteur de la menace spécifique.

Un défaut de libération de mémoire dans la fonction *_dst_negative_advice()* du noyau Linux permet à un attaquant, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire.

2.3.1. Type de vulnérabilité

- CWE-416 : Use After Free

2.3.2. Risque

- Exécution de code arbitraire

2.3.3. Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Local	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Faible	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.3.4. Produits impactés

- Le noyau Linux version 4.6 antérieures à 6.9.4

2.3.5. Recommandations

- Mettre à jour le noyau Linux vers la version 6.9.4 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Linux.

2.3.6. Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

3. Virologie : analyse d'un échantillon NukeSpeed - KoreanSpritz (APT Lazarus)

3.1. Une nouvelle version

Découvert en juin 2024, KoreanSpritz serait une nouvelle version de logiciel malveillant appartenant à la famille NukeSpeed (alias NukeSped et Manuscript) : un ensemble de portes dérobées et de chevaux de Troie sophistiqués qui sont utilisés par l'APT Lazarus (Corée du Nord).

Développé en C/C++, la porte dérobée KoreanSpritz est un exécutable portable 32-bit dédié aux environnements **Microsoft Windows**.

KoreanSpritz aurait été utilisé pour des activités de cyber-espionnage ciblant des entités sud-coréennes dans les secteurs financier, industriel et gouvernemental.

3.2. Fonctionnalités

Ci-dessous, les principales fonctionnalités du logiciel malveillant KoreanSpritz.

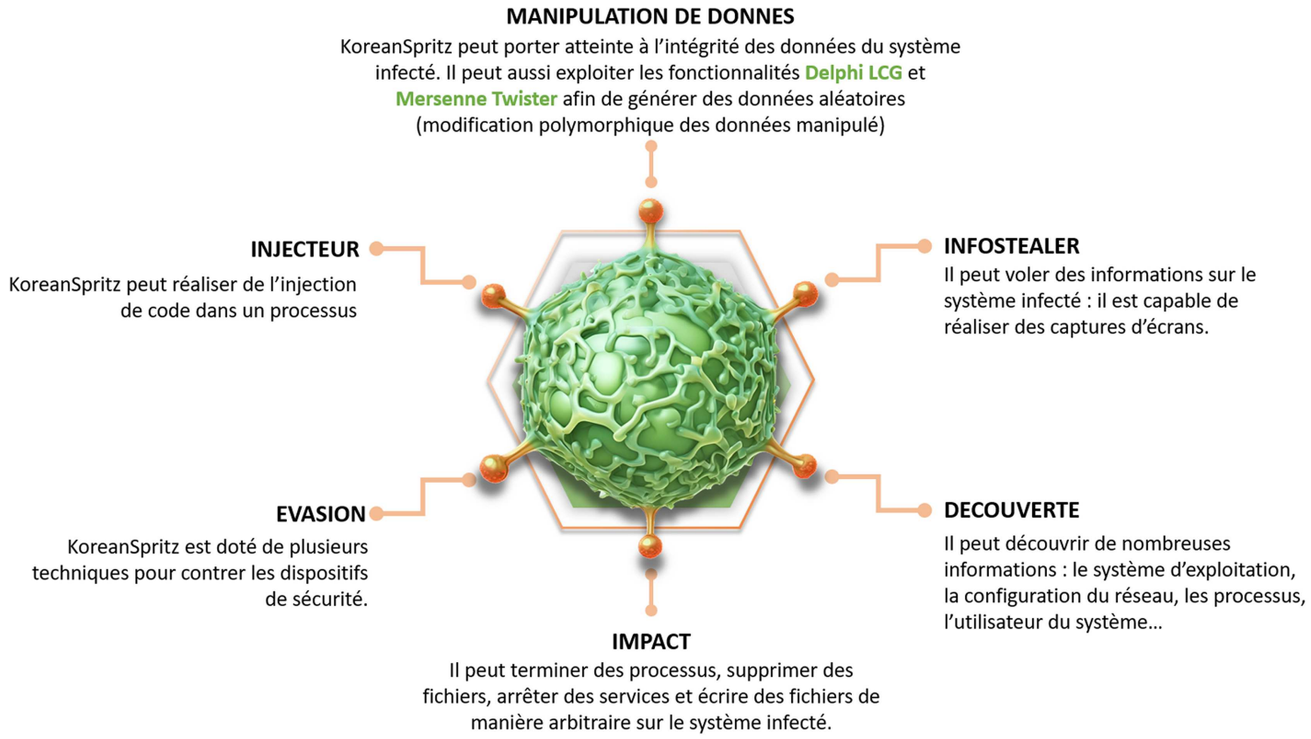
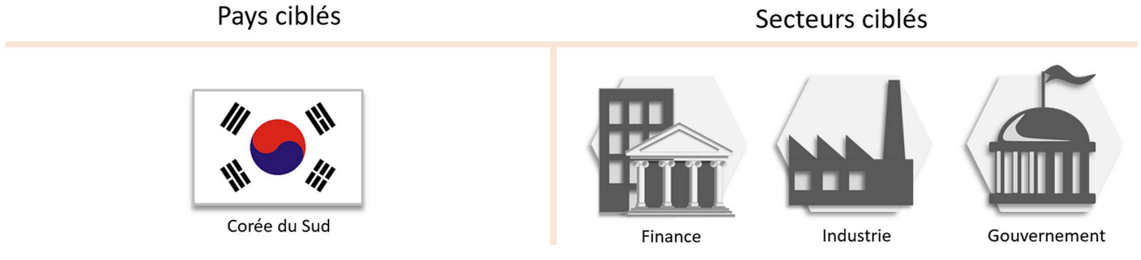


Figure 1. Les fonctionnalités de KoreanSpritz : une porte dérobée multifonction.

3.3. Victimologie



3.4. Analyse de la souche virale

Capture d'écran

KoreanSpritz peut réaliser des captures d'écrans, notamment via la fonction **GetDesktopWindow**.

Fonctions identifiées:

- GetDesktopWindow (USER32.dll)
- CreateCompatibleBitmap (GDI32.dll)
- CreateCompatibleDC (GDI32.dll)
- BitBlt (GDI32.dll)

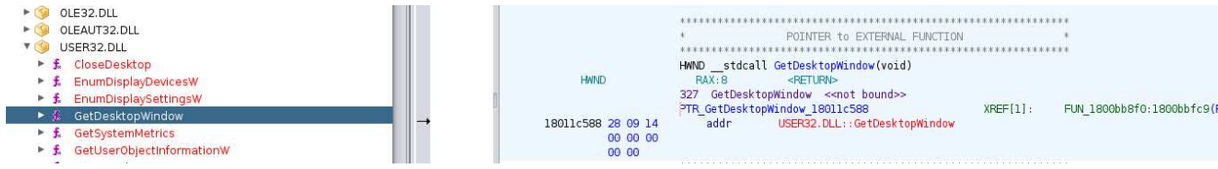


Figure 2. GHIDRA - Code Browsing : fonction GetDesktopWindow.

Injection

KoreanSpritz semble réaliser de l'injection dans des processus :

```
Source : C:\Windows\System32\cmd.exe
Création de processus: C:\Windows\System32\rundll32.exe rundll32.exe
"C:\Users\user\Desktop\pconsnap.dll.dll",#1
```

Ci-dessous, des fonctions utilisées pour manipuler la mémoire lors de l'injection :

- VirtualAlloc (KERNEL32.dll)
- VirtualProtect (KERNEL32.dll)
- OpenProcess (KERNEL32.dll)

Évasion de la défense : anti-virtualisation

Pour détecter l'exécution du maliciel dans un environnement virtualisé, KoreanSpritz recherche certains mots clés sur le système :

May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)	
Source: pconsnap.dll.dll	Binary or memory string: jHGfS
Source: loaddll64.exe, 00000000.00000002.2933846771.000001D16CA38000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.2046518335.000001D16CAA4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000002.2933846771.000001D16CAA4000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.1783305041.000001FC491D3000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000003.1782764478.000001FC491D3000.00000004.00000020.00020000.00000000.sdmp	Binary or memory string: Hyper-V RAW
Source: pconsnap.dll.dll	Binary or memory string: VMcI"!>
Source: rundll32.exe, 00000003.00000003.1782672072.000001FC4921E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.1783459795.000001FC49224000.00000004.00000020.00020000.00000000.sdmp	Binary or memory string: Hyper-V RAW@

Figure 3. Anti-virtualisation : recherche de mots-clés.

KoreanSpritz est capable de marquer des temps d'arrêt pour contrer l'analyse antivirale :

May sleep (evasive loops) to hinder dynamic analysis	
Source: C:\Windows\System32\loaddll64.exe TID: 7432	Thread sleep time: -120000s >= -30000s

Sample execution stops while process was sleeping (likely an evasion)	
Contains medium sleeps (>= 30s)	
Source: C:\Windows\System32\loaddll64.exe	Thread delayed: delay time: 120000

Figure 4. Anti-virtualisation : recherche de mots-clés.

Evasion de la défense : anti-debug

Pour contrer l'analyse via un désassembleur (Rétro-ingénierie), KoreanSpritz manipule des jetons de privilèges lié au debogage ("debug").

```
Source : C:\Windows\System32\loaddll64.exe
Processus : token adjusted Debug
```

Ci-dessous, un exemple de manipulation de jeton (token) :

```
Status : on
Privilège : Debug
Etat : success or wait
Quantité : 1
Adresse source : 7FFDFB8DD9D6
Symbole : AdjustTokenPrivileges
```

Process Token Activities

Token Adjusted

Status	Privilege	Completion	Count	Source Address	Symbol
on	Debug	success or wait	1	7FFDFB8DD9D6	AdjustTokenPrivileges
on	Take Ownership	success or wait	13	7FFDFB8DDDAE	AdjustTokenPrivileges
on	Take Ownership	success or wait	13	7FFDFB8DE34D	AdjustTokenPrivileges
on	Tcb	not all assigned	203	7FFDFB8DDDAE	AdjustTokenPrivileges

Figure 5. Anti-debug.

Découverte

KoreanSpritz réalise de la découverte en interrogeant les registres du système.

- L'utilisateur du système :

```
Clé registre interrogé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion RegisteredOwner
```

- La date d'installation du système d'exploitation :

```
Clé registre interrogé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion InstallDate
```

- La clé du produit Microsoft Windows :

```
Clé registre interrogé : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion ProductId
```

- Identifiant global unique de la cryptographie du système :

```
Clé registre interrogé: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid
```

- Le nom de machine

```
Clé registre interrogé: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
```

Des fonctions sont aussi utilisées par KoreanSpritz pour reconnaitre le réseau.

- Découverte des serveurs qui sont visibles dans un domaine :

```
NetServerEnum (NETAPI32.dll)
```

Communication

Le 28 juin 2024, KoreanSpritz semble avoir communiqué avec l'adresse URL hxxps://www[.]airgreensystem[.]com/DB_command/gallery/bbs_list.php.

Ci-dessous, un exemple de communication entre KoreanSpritz et **Airgreensystem** :

Timestamp	Bytes transferred	Direction	Data
2024-06-28 08:06:32 UTC	302	OUT	POST /DB_command/gallery/bbs_list.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36 Content-Length: 70 Host: www.airgreensystem.com
2024-06-28 08:06:32 UTC	70	OUT	Data Raw: 43 55 37 78 36 3d 45 42 78 77 4e 6e 52 6c 4a 58 4d 45 61 45 68 64 5a 46 64 6e 55 69 4a 69 5a 54 52 34 53 31 42 52 51 31 55 33 65 44 59 78 61 54 51 30 57 6e 46 71 56 57 4e 53 5a 32 45 33 55 6b 78 4f 65 6a 6c 6c Data Ascii: CU7x6=EBxwNnRlJXMEaEhdZFdnUiJiZTR4S1BRQ1U3eDYxaTQ0WnFqVWNSZ2E3UkxOejll
2024-06-28 08:06:33 UTC	420	IN	HTTP/1.1 200 OK Date: Fri, 28 Jun 2024 08:06:32 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=lsvo7qdmn4o8inmvgokvka1fc5; expires=Sat, 29-Jun-2024 08:06:32 GMT; path=/ Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 285 Vary: Accept-Encoding Content-Type: text/html
2024-06-28 08:06:33 UTC	285	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22 30 22 20 6d 61 72 67 69 6e 68 65 69 67 68 74 3d 22 30 22 20 73 74 79 6c 65 3d 22 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 22 3e 3c 73 63 72 69 70 74 3e 46 44 63 37 56 7a 30 5a 51 67 3d 3d 5a 30 4a 59 4e 46 68 71 4d 51 3d 3d 23 36 35 39 39 31 30 39 30 36 36 39 37 35 37 37 30 35 34 30 30 38 38 35 34 33 32 35 35 36 34 35 30 32 30 30 39 36 36 23 32 33 38 33 33 30 37 34 39 33 32 30 38 36 31 30 31 32 30 37 37 39 38 31 31 30 39 39 38 31 36 36 33 34 34 33 36 31 39 23 32 32 32 34 31 36 34 33 39 30 37 31 33 34 31 35 31 33 30 36 38 30 38 30 37 33 39 34 37 36 37 39 32 Data Ascii: <!DOCTYPE html><html><head></head><body marginwidth="0" marginheight="0" style="background-color:transparent"><script>FDc7Vz0ZQg==Z0JYNFhqMQ==#659910906697577054008854325564502009 66#2383307493208610120779811099816634436 19#222416439071341513068080739476792

Figure 6. Communication bidirectionnelle entre KoreanSpritz et Airgreensystem.

La société **Airgreensystem** est localisée en Corée du Sud et semble légitime.

Figure 7. Airgreensystem : une société sud-coréenne.

Deux autres adresses sont identifiées dans la souche virale :

```
hxxp://www[.]komico.or[.]kr/eng/sub3/index8.asp
hxxp://market[.]gumi.go[.]kr/m/sub1/sub5.asp
```

Les trois adresses URL sont codées en dure dans KoreanSpritz :

```
                    u_http://www.komico.or.kr_18011fd80             XREF[1]:     FUN_1800a63d0:1800a641f(*)
18011fd80 68 00 74      unicode     u"http://www.komico.or.kr"
          00 74 00
          70 00 3a ...

                    u_/eng/sub3/index8.asp_18011fdb0                XREF[1]:     FUN_1800a63d0:1800a644b(*)
18011fdb0 2f 00 65      unicode     u"/eng/sub3/index8.asp"
          00 6e 00
          67 00 2f ...
18011fdda 00            ??          00h
18011fddb 00            ??          00h
18011fddc 00            ??          00h
18011fddd 00            ??          00h
18011fdde 00            ??          00h
18011fddf 00            ??          00h

                    u_http://market.gumi.go.kr_18011fde0            XREF[1]:     FUN_1800a63d0:1800a6477(*)
18011fde0 68 00 74      unicode     u"http://market.gumi.go.kr"
          00 74 00
          70 00 3a ...
18011fe12 00            ??          00h
18011fe13 00            ??          00h
18011fe14 00            ??          00h
18011fe15 00            ??          00h
18011fe16 00            ??          00h
18011fe17 00            ??          00h

                    u_/m/sub1/sub5.asp_18011fe18                    XREF[1]:     FUN_1800a63d0:1800a64a3(*)
18011fe18 2f 00 6d      unicode     u"/m/sub1/sub5.asp"
          00 2f 00
          73 00 75 ...
18011fe3a 00            ??          00h
18011fe3b 00            ??          00h
18011fe3c 00            ??          00h
18011fe3d 00            ??          00h
18011fe3e 00            ??          00h
18011fe3f 00            ??          00h

                    u_https://www.airgreensystem.com_18011fe40      XREF[1]:     FUN_1800a63d0:1800a64cf(*)
18011fe40 68 00 74      unicode     u"https://www.airgreensystem.com"
          00 74 00
          70 00 73 ...
18011fe7e 00            ??          00h
18011fe7f 00            ??          00h

                    u_/DB_command/gallery/bbs_list.php_18011fe80    XREF[1]:     FUN_1800a63d0:1800a64fb(*)
18011fe80 2f 00 44      unicode     u"/DB_command/gallery/bbs_list.php"
          00 42 00
          5f 00 63 ...
```

Figure 8. Adresse codée en dures dans la souche virale.

3.5. PCONSNAP.DLL : un détail intéressant

Une recherche en source ouverte du mot-clé **PCONSNAP.DLL** révèle que ce dernier semble avoir été utilisé par l'APT Lazarus au cours de l'année 2022 à 2023.

Cet article de *Malpedia* indique que **PCONSNAP.DLL** aurait été utilisé dans le logiciel malveillant PostNapTea (alias SIGNBT)

PostNapTea aka SIGNBT is an HTTP(S) RAT that is written as a complex object-oriented project.

In 2022-2023, it was deployed against targets like a newspaper organization, agriculture-related entity or a software vendor. The initial access was usually achieved by exploiting vulnerabilities in widely-used software in South Korea.

It collects various information about the victim's computer, such as computer name, product name, OS details, system uptime, CPU information, system locale, time zone, network status, and malware configuration.

It stores its configuration in JSON format. It resolves the Windows APIs it requires during runtime, via the Fowler–Noll–Vo (FNV) hash function.

Its internal name in the version-information resource is usually ppcsnap.dll or pconsnap.dll, which loosely inspired its code name.

Figure 9. Source : Malpedia.

L'échantillon analysé sur Virus Total n'est pas signé et se présente comme Proper Console Snap de Microsoft. Il s'agit d'un point commun identifié avec PostNapTea.

Signature info

Signature Verification

⚠ File is not signed

File Version Information

Copyright	@ Microsoft Corporation. All rights reserved.
Product	Microsoft@Windows@Operating System
Description	Proper Console Snap
Original Name	pconsnap.dll
Internal Name	pconsnap.dll
File Version	10.0.22000.1

Figure 10. Source : Virus Total.

Ce détail renforce l'atribution de NukeSpeed - KoreanSpritz à l'APT Lazarus.

3.6. Famille NukeSpeed

Ci-dessous, quelques échantillons appartement à la famille NukeSpeed.

2019

- Échantillon : Album.app.zip (19.53 MB) *MAC*
- Nom de détection : trojan.nukesped/lazarus
- Date de création : inconnue
- Première analyse connue : 22 octobre 2019.
- SHA256 : d91c233b2f1177357387c29d92bd3f29fab7b90760e59a893a0f447ef2cb4715

2020

- Échantillon : D2DE01858417FA3B580B3A95857847D5 (164.00 KB) *Windows*
- Nom de détection : trojan.nukesped/zusy
- Date de création : 10 mai 2017
- Première analyse connue : 13 mai 2020
- SHA256 : aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6

2021

- Echantillon : production.dll (268.50 KB) *Windows*
- Nom de détection : trojan.nukesped/tigerrat
- Date de création : 13 octobre 1996
- Première analyse connue : 2 avril 2021
- SHA256 : 0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c

2023

- Échantillon : 861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d.iso (3.11 MB) *Windows*
- Nom de détection : Trojan/Win64.NukeSped
- Date de création : inconnue
- Première analyse connue : 12 mai 2023
- SHA256 : 861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d

2024

- Echantillon : pconsnap.dll ou AutoMapper.Net5.dll (71.04 MB) *Windows*
- Nom de détection : trojan.nukesped/mint
- Date de création : 28 mars 2024
- Première analyse connue : 25 juin 2024
- SHA256 : 4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74

3.7. Cluster NukeSpeed

La famille NukeSpeed est aussi connue pour être la base d'une autre famille de logiciels malveillants utilisés par l'APT Lazarus : ThreatNeedle, cette dernière émerge au cours de l'année 2019 et embarque des portes dérobées (ThreatNeedle-backdoor) ainsi que des logiciels de déploiement (ThreatNeedle-loader).

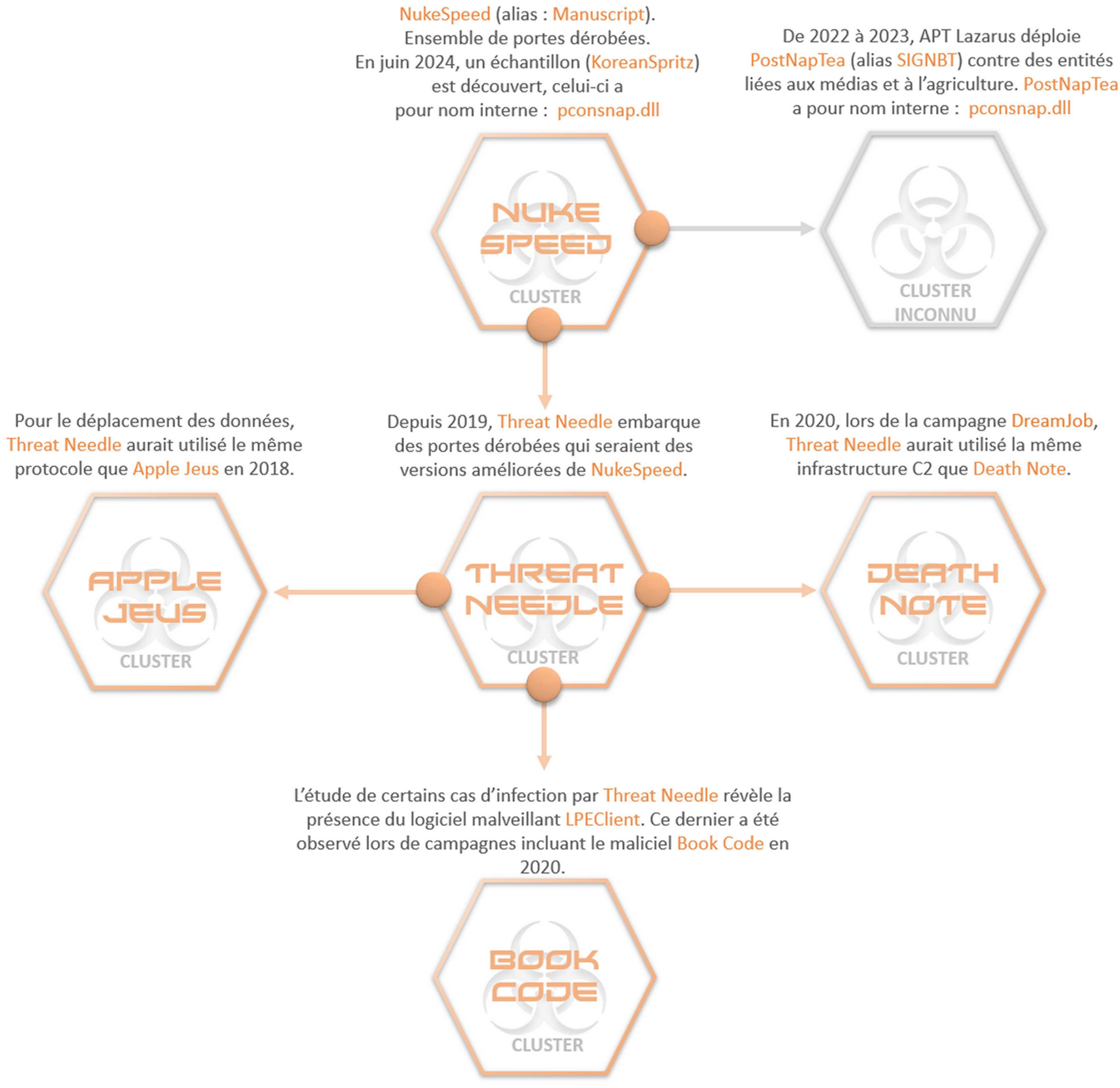


Figure 11. Principaux clusters (ensembles) proches de NukeSpeed.

3.8. APT Lazarus - Modèle diamant

L'APT Lazarus (alias Dark Seoul, Guardians of Peace, WHOIS Team, Diamond Sleet, Jade Sleet…) est une menace avancée et persistante d'origine nord-coréenne

Figure 12. Modèle diamant de l'APT Lazarus.

3.9. MITRE ATT&CK

RESOURCE DEVELOPMENT

T1587.001 Develop Capabilities: Malware.

EXECUTION

T1129 Shared Modules. T1059 Command and Scripting Interpreter.
T11569.002 System Services: Service Execution.

PERSISTENCE

T1574.002 DLL Side-loading. T1543 Create or Modify System Process.
T1134 Access Token Manipulation.

PRIVILEGE ESCALATION

T1055 Process Injection. T1548 Abuse Elevation Control Mechanism. T1574.002 DLL Side-loading.
T1134 Access Token Manipulation. T1134.004 Access Token Manipulation: Parent PID Spoofing.

DEFENSE EVASION

1055 Process Injection. T1548 Abuse Elevation Control Mechanism. T1574.002 DLL Side-loading. T1218.011 RunDLL32. T1497 Virtualization / Sandbox Evasion. T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion. T1134 Access Token Manipulation. T1134.004 Access Token Manipulation: Parent PID Spoofing. T1027.005 Obfuscated Files or Information. T1127 Trusted Developer Utilities Proxy Execution. . T1027 Obfuscated Files or Information: Software Packing. T1036.007 Masquerading: Double File Extension.

DISCOVERY

T1135 Network Share Discovery. T1082 System Information Discovery. T1518.001 Software Discovery: Security Software Discovery. T1518.016 System Network Configuration Discovery. T15049 System Network Connections Discovery. T1033 System Owner/User Discovery. T1007 System Service Discovery. T1124 System Time Discovery. T1016.001 System Network Configuration Discovery: Internet Connection Discovery. T1083 File and Directory Discovery. T1497 Virtualization / Sandbox Evasion. T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion. T1012 Query Registry.

COLLECTION

T1113 Screen Capture. T1005 Data from Local System (Parse credit card information + Get geographical location).

COMMAND AND CONTROL

T1071 Application Layer Protocol. T1573 Encrypted Channel. T1095 Non-Application Layer Protocol.

IMPACT

T1565 Data Manipulation. T1491 Defacement. T1489 Service Stop.

Figure 13. TTPS KOREANSPRITZ (APT LAZARUS)

3.10. IOCs

Nom de détection pour l'échantillon NukeSpeed - KoreanSpritz 2024 : TR/NukeSped.dggcy (Avira), Win64/NukeSped.KP trojan (Hybrid Analysis), Trojan:Win64/NukeSped.d298f49d (Alibaba), Trojan/Win.Lazardoor.R592967 (Ahnlab).

3.10.1. IOC NukeSpeed - KoreanSpritz 2024

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	SHA256	4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74	NukeSpeed-KoreanSpritz Backdoor
TLP:CLEAR	SHA1	2816b44de0065bee18ac963bcc3bf9b195499eeb	NukeSpeed-KoreanSpritz Backdoor
TLP:CLEAR	MD5	8fb5e72a31680189d9a529b49962a0b1	NukeSpeed-KoreanSpritz Backdoor
TLP:CLEAR	URL	hxxp://www[.]komico.or[.]kr/eng/sub3/index8.asp	URL potentiellement compromise
TLP:CLEAR	URL	hxxp://market[.]gumi.go[.]kr/m/sub1/sub5.asp	URL potentiellement compromise
TLP:CLEAR	URL	hxxps://www[.]airgreensystem[.]com/DB_command/gallery/bbs_list.php	URL potentiellement compromise (possible C2)

3.10.2. IOC NukeSpeed - anciens variants

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	Artéfact	Album.app.zip	NukeSpeed 2019
TLP:CLEAR	SHA256	d91c233b2f1177357387c29d92bd3f29fab7b90760e59a893a0f447ef2cb4715	NukeSpeed 2019
TLP:CLEAR	SHA1	5955837b6f888a733e05cbb444279d24f5313ac5	NukeSpeed 2019
TLP:CLEAR	MD5	a8096ddf8758a79fdf68753190c6216a	NukeSpeed 2019
TLP:CLEAR	Artéfact	D2DE01858417FA3B580B3A95857847D5	NukeSpeed 2020
TLP:CLEAR	SHA256	aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6	NukeSpeed 2020
TLP:CLEAR	SHA1	2c879a1d4b6334c59ac5f11c2038d273d334befe	NukeSpeed 2020
TLP:CLEAR	MD5	d2de01858417fa3b580b3a95857847d5	NukeSpeed 2020
TLP:CLEAR	IP	112(.)217.108.138	NukeSpeed 2020
TLP:CLEAR	Artéfact	production.dll	NukeSpeed 2021
TLP:CLEAR	SHA256	0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c	NukeSpeed 2021
TLP:CLEAR	SHA1	98d6417addec8607f1b62cc52123be76424befc0	NukeSpeed 2021
TLP:CLEAR	MD5	f4d46629ca15313b94992f3798718df7	NukeSpeed 2021
TLP:CLEAR	Artéfact	861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d.iso	NukeSpeed 2023
TLP:CLEAR	SHA256	861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d	NukeSpeed 2023
TLP:CLEAR	SHA1	d2f160bf01a1f7b863188c9b953c197f7b876c7a	NukeSpeed 2023
TLP:CLEAR	MD5	4e10c8d3d71136e870cf58c0e31db2bc	NukeSpeed 2023

3.11. YARA

3.11.1. YARA 1

YARA - aDvens

```
rule KOREANSPRITZ_Specific_strings {
meta:
author = "ADVENS CTI"
date = "3/07/2024"
source = "ADVENS"
status = "RELEASED"
sharing = "TLP:CLEAR"
malware = "NUKESPEED_variant_KOREANSPRITZ"
description = "Yara_rule_that_detects_KOREANSPRITZ_backdoor."
info = "KOREANSPRITZ_Backdoor"
Sample_SHA256 = "4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74"
Sample_SHA1 = "2816b44de0065bee18ac963bcc3bf9b195499eeb"
Sample_MD5 = "8fb5e72a31680189d9a529b49962a0b1"
//Vérification hexadécimale
strings:
$Hexa1 = { 56 18 48 8b c2 48 2b c1 }
$Hexa2 = { 48 89 85 58 01 00 00 48 }
$Hexa3 = { 48 89 5c 24 70 48 8d 54 }
$Hexa4 = { 49 ff c0 66 42 83 3c 40 }
$Hexa5 = { f6 ff 48 8d 85 28 07 00 }
$Hexa6 = { 48 63 c2 48 8d 4c 24 20 }
$Hexa7 = { 5c 0d 05 00 33 d2 38 45 }
$Hexa8 = { e8 7b 2d 00 00 cc cc cc }
//Vérification des fonctions
$Add1 = "GetDesktopWindow"
$Add2 = "DeleteFileW"
$Add3 = "CreateFileW"
$Add4 = "NetServerEnum"
$Add5 = "OpenInputDesktop"
$Add6 = "TerminateProcess"
condition:
filesize > 74490000 and filesize < 74500000 and all of ($Hexa*) and 3 of ($Add*)
}
```

3.11.2. YARA 2

YARA - FIleScan.IO

Source : https://www.filescan.io/uploads/667e6d880bf5978c0b1318c1/reports/2c045983-2ef5-4dc3-9f87-a68de8b27d23/overview

```
    rule autogen_peexe_FingerprintLolbinMasqueradeOverlayPackedRemote_4f9ef9f4
    {
    meta:
    author = "FileScan.IO Engine v1.1.0-6f9b172"
    date = "2024-06-28"
    sample = "4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74"
    score = 75
    tags = "fingerprint,lolbin,masquerade,overlay,packed,remote"
    isWeakRule = true
    strings:
    //IOC patterns
    $req0 = "http://market.gumi.go.kr"
    $req1 = "http://www.komico.or.kr"
    $req2 = "https://www.airgreensystem.com"
    //optional strings
    $opt0 = "!\"#$%&'()*+,-
./0123@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@"
    $opt1 = "ADVAPI32.dll"
    $opt2 = "AcquireSRWLockExclusive"
    $opt3 = "AreFileApisANSI"
    $opt4 = "CloseDesktop"
```

```
        $opt5 = "CreateFileA"
        $opt6 = "CreateFileMappingW"
        $opt7 = "CreateFileW"
        $opt8 = "CreateThread"
        $opt9 = "DecodePointer"
        $opt10 = "DeleteCriticalSection"
        $opt11 = "DeleteFileW"
        $opt12 = "DeleteIpNetEntry"
        $opt13 = "DeleteProcThreadAttributeList"
        $opt14 = "DeleteService"
        $opt15 = "EncodePointer"
        $opt16 = "EnterCriticalSection"
        $opt17 = "EnumDependentServicesW"
        $opt18 = "EnumDisplayDevicesW"
        $opt19 = "EnumServicesStatusExW"
        $opt20 = "EnumSystemLocalesEx"
        $opt21 = "EnumSystemLocalesW"
        $opt22 = "ExitProcess"
        $opt23 = "FileTimeToSystemTime"
        $opt24 = "FindFirstFileExW"
        $opt25 = "FindNextFileW"
        $opt26 = "FlushFileBuffers"
        $opt27 = "FreeEnvironmentStringsW"
        $opt28 = "FreeLibrary"
        $opt29 = "GetCommandLineA"
        $opt30 = "GetCommandLineW"
        $opt31 = "GetComputerNameA"
        $opt32 = "GetComputerNameW"
        $opt33 = "GetConsoleMode"
        $opt34 = "GetConsoleOutputCP"
        $opt35 = "GetCurrentProcess"
        $opt36 = "GetCurrentProcessId"
        $opt37 = "GetCurrentThreadId"
        $opt38 = "GetDateFormatW"
        $opt39 = "GetDesktopWindow"
        $opt40 = "GetEnvironmentStringsW"
        $opt41 = "GetFileAttributesExW"
        $opt42 = "GetFileInformationByHandle"
        $opt43 = "GetFileSize"
        $opt44 = "GetFileSizeEx"
        $opt45 = "GetFileType"
        $opt46 = "GetLastError"
        $opt47 = "GetLocalTime"
        $opt48 = "GetLocaleInfoW"
        $opt49 = "GetModuleFileNameW"
        $opt50 = "GetModuleHandleExW"
        $opt51 = "GetModuleHandleW"
        $opt52 = "GetProcAddress"
        $opt53 = "GetProcessHeap"
        $opt54 = "GetProcessId"
        $opt55 = "GetServiceDisplayNameW"
        $opt56 = "GetServiceKeyNameW"
        $opt57 = "GetStartupInfoW"
        $opt58 = "GetStdHandle"
        $opt59 = "GetStringTypeW"
        $opt60 = "GetSystemInfo"
        $opt61 = "GetSystemMetrics"
        $opt62 = "GetSystemTimeAsFileTime"
        $opt63 = "GetTickCount"
        $opt64 = "GetTickCount64"
        $opt65 = "GetTimeFormatW"
        $opt66 = "GetTimeZoneInformation"
        $opt67 = "GetUserDefaultLCID"
        $opt68 = "GetUserObjectInformationW"
        $opt69 = "GetWindowsDirectoryW"
        $opt70 = "GlobalAlloc"
        $opt71 = "GlobalFree"
        $opt72 = "GlobalLock"
        $opt73 = "GlobalUnlock"
        $opt74 = "HeapReAlloc"
        $opt75 = "IPHLPAPI.DLL"
        $opt76 = "InitializeCriticalSectionAndSpinCount"
        $opt77 = "InitializeCriticalSectionEx"
        $opt78 = "InitializeProcThreadAttributeList"
        $opt79 = "InitializeSListHead"
        $opt80 = "InterlockedFlushSList"
        $opt81 = "IsBadReadPtr"
        $opt82 = "IsDebuggerPresent"
        $opt83 = "IsProcessorFeaturePresent"
        $opt84 = "KERNEL32.dll"
        $opt85 = "LCMapStringW"
        $opt86 = "LeaveCriticalSection"
        $opt87 = "LoadLibraryA"
```

```
    $opt88 = "LoadLibraryExW"
    $opt89 = "LoadLibraryW"
    $opt90 = "LocalAlloc"
    $opt91 = "LocalReAlloc"
    $opt92 = "LockServiceDatabase"
    $opt93 = "LookupAccountSidW"
    $opt94 = "MapViewOfFile"
    $opt95 = "MoveFileExW"
    $opt96 = "NETAPI32.dll"
    $opt97 = "NetConnectionEnum"
    $opt98 = "NetServerEnum"
    $opt99 = "OLEAUT32.dll"
    $opt100 = "OpenDesktopW"
    $opt101 = "OpenInputDesktop"
    $opt102 = "OpenProcess"
    $opt103 = "OpenWindowStationW"
    $opt104 = "QueryPerformanceCounter"
    $opt105 = "QueryPerformanceFrequency"
    $opt106 = "QueryServiceStatus"
    $opt107 = "RaiseException"
    $opt108 = "ReadConsoleW"
    $opt109 = "ReleaseSRWLockExclusive"
    $opt110 = "RtlCaptureContext"
    $opt111 = "RtlLookupFunctionEntry"
    $opt112 = "RtlPcToFileHeader"
    $opt113 = "RtlVirtualUnwind"
    $opt114 = "SeDebugPrivilege"
    $opt115 = "SetEndOfFile"
    $opt116 = "SetEnvironmentVariableW"
    $opt117 = "SetFilePointer"
    $opt118 = "SetFilePointerEx"
    $opt119 = "SetLastError"
    $opt120 = "SetProcessWindowStation"
    $opt121 = "SetStdHandle"
    $opt122 = "SetThreadDesktop"
    $opt123 = "SetUnhandledExceptionFilter"
    $opt124 = "SleepConditionVariableSRW"
    $opt125 = "Status       Local     Remote                    Network"
    $opt126 = "SystemTimeToFileTime"
    $opt127 = "TerminateProcess"
    $opt128 = "TlsGetValue"
    $opt129 = "TlsSetValue"
    $opt130 = "USER32.dll"
    $opt131 = "UnhandledExceptionFilter"
    $opt132 = "UnmapViewOfFile"
    $opt133 = "UpdateProcThreadAttribute"
    $opt134 = "VirtualAlloc"
    $opt135 = "VirtualFree"
    $opt136 = "VirtualProtect"
    $opt137 = "WS2_32.dll"
    $opt138 = "WaitForSingleObject"
    $opt139 = "WakeAllConditionVariable"
    $opt140 = "WriteConsoleW"
    $opt141 = "connection reset"
    $opt142 = "gdiplus.dll"
    $opt143 = "mscoree.dll"
    $opt144 = "network reset"
    $opt145 = "read only file system"
    $opt146 = "shlwapi.dll"
    $opt147 = "stream timeout"
    condition:
    //require 50% of optional strings
    uint16(0) == 0x5A4D and filesize > 67045479 and filesize < 81944473 and all of ($req*) and 74 of ($opt*)
}
```

4. Groupes Hacktivistes : un tour d'horizon

Les évènements politiques survenus en 2023 et 2024 ont fait germer, au début de l'année 2024, une importante quantité de groupe hacktivistes. Si ce type de groupe existe déjà depuis de nombreuses années (Anonymous, Caliphate Cyber Army), le recours à des actions offensives cyber de la part d'individus civils est devenue une pièce intégrante des crises géopolitiques actuelles.

Un état des lieux des groupes hacktivistes au deuxième trimestre 2024 met en exergue des glissements qui se sont opérés au fil du temps. Ainsi, il est possible d'observer l'émergence de nouveaux acteurs majeurs et la disparition ou mise en veille de certains. À titre d'exemple, Anonymous Sudan et Killnet qui étaient omniprésents au début de la guerre en Ukraine ont laissé la place à de nouveaux acteurs tels que la « Holy League » ou NoName057.

De plus, la résonnance médiatique de la guerre menée par l'état israélien dans la bande de Gaza à la suite de l'attaque du 7 octobre 2023 a suscité au début de l'année 2024 la création de nombreux groupes hacktivistes propalestiniens venant de plusieurs pays et s'alliant à la manière d'une brigade ou légion internationale cyber.

Conformément à ces observations initiales, les groupes hacktivistes se scindent à l'heure actuelle en deux grandes familles calquées sur les deux principales problématiques géopolitiques de ce jour : le conflit israélo-palestinien et la guerre russo-ukrainienne.

4.1. Portraits d'hackteurs

4.1.1. NoName057(16)

Ce groupe hacktiviste est apparu en mars 2022 dans le cadre de la guerre en Ukraine. Il est actuellement le collectif le plus important et par ailleurs responsable de 36% de toutes les attaques DDOS contre l'Ukraine. Loin derrière lui vient Anonymous Russia, responsable de 17% de ces attaques.

Le collectif a réussi à attirer un contingent de volontaire important grâce à plusieurs points :

- une communication importante au travers de ses canaux Telegram,
- la création d'un canal spécifique pour les volontaires anglophones
- une simplification des démarches permettant aux volontaires d'être opérationnels rapidement au travers de tutoriel,
- la mise à disposition du kit logiciel *DDOSIA* et d'un support technique.

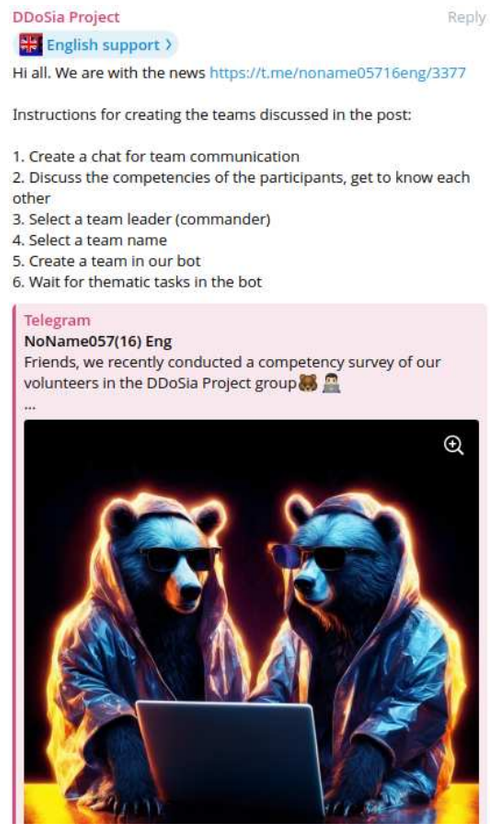


Figure 14. Tutoriel recrutement NoName057(16) - Telegram

Enfin, le collectif est connu pour rémunérer en cryptomonnaie ses volontaires les plus actifs.

4.1.2. Rippersec

Originaire de Malaisie, Rippersec est un exemple parfait de la mondialisation de l'hacktivisme propre au conflit israélo-palestinien. Dans l'esprit de ces groupes, le thème de la Oumma (communautés des croyants) est ainsi récurrent et les pousse naturellement à des alliances.

La motivation principale du groupe est de soutenir la cause palestinienne et de cibler des organisations ou gouvernements perçus comme favorables à Israël. Rippersec se distingue actuellement pour être en première ligne dans les attaques actuelles contre les sites français en réaction à l'arrestation de Pavel Durov au Bourget. Le groupe a ainsi mené des attaques DDOS contre le site de Police nationale.

Figure 15. Revendication RipperSec - Telegram

4.2. Alliances

Au fil du conflit ukrainien, des alliances se sont créées, notamment entre les groupes hacktivistes prorusses qui ont formé l'alliance Killnet, collectif qui a marqué les premières années de guerres. Un nouveau collectif s'est créé en mai 2024. Celui-ci a pour objectif d'attaquer les pays européens et membres de l'OTAN. Il regroupe une vingtaine de membres.

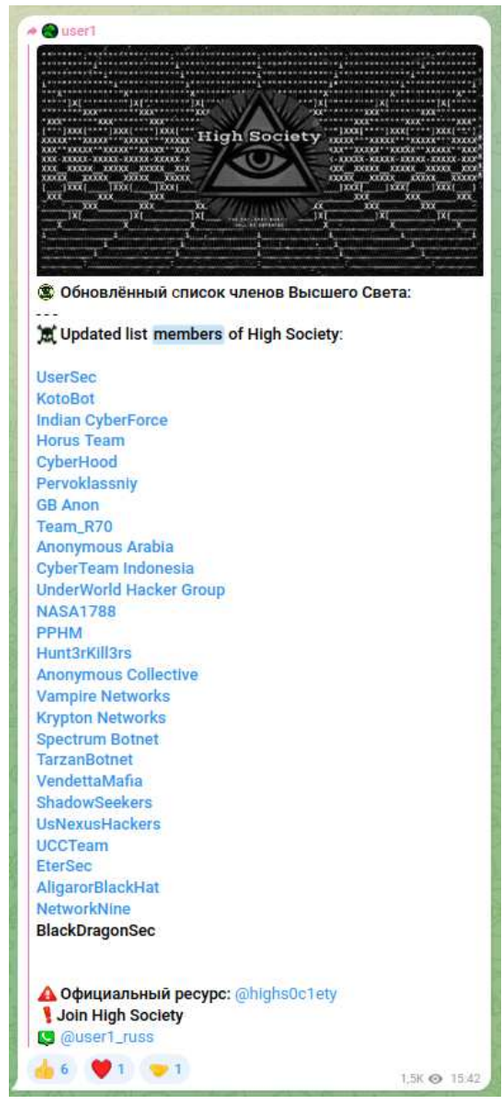


Figure 16. Membres de High Society - Telegram

Le 29 juin 2024, une nouvelle coalition de groupes hacktivistes pro-Palestine est créée regroupant 35 collectifs : *L'alliance du 7 Octobre*.

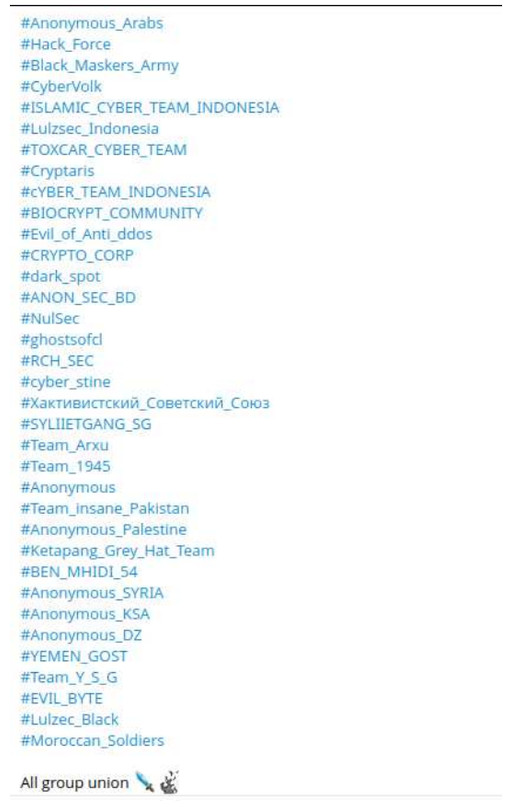


Figure 17. Membres de l'alliance du 7 octobre - Telegram

Le 22 juillet 2024, ces deux coalitions aux profils pourtant antagonistes dont les objectifs ont fini par se rapprocher décident de fusionner : la Holy League est ainsi créée. L'organisation revendique plus de 80 groupes, dont certains seraient secrètement dans l'alliance. 69 ont été officialisés et sont représentés dans le canal Telegram de l'alliance.

Figure 18. Annonce de la création de la Holy League - Telegram

la Holy League a également revendiqué des attaques contre la France en raison de l'arrestation de Pavel Durov, le hashtag #FreeDurov est à l'heure actuelle utilisé dans les revendication un grand nombre de groupe hacktivistes de sensibilités très diverses.

4.3. Techniques

4.3.1. DDOS & Defacement

Ces techniques de harcèlement sont largement utilisées, car elles réclament un niveau de connaissances techniques moindre. Le DDOS consiste à rendre un service inutilisable en l'inondant de requêtes visant à faire tomber ses serveurs tandis que le défacement vise à changer l'apparence d'un site afin notamment d'y afficher son propre message. La mise en oeuvre de ces techniques a surtout un impact symbolique et médiatique, but recherché par l'hacktivisme afin de se faire valoir et d'humilier l'adversaire.

Figure 19. Defacement de sites israeliens par ByteBlitz Team et Cyb3r Drag0nz - Telegram

4.3.2. Vol d'informations, doxing

Le doxing est la forme la plus violente d'hacktivisme avec la publication de données personnelles concernant une personne. Au début de l'invasion de la bande de Gaza et de la tentative de bombardement par l'Iran, une forte radicalisation a été observée dans plusieurs groupes hacktivistes avec un effacement de la frontière entre conflits physiques et cyber.

Dans ce cas de figure, l'action cyber sert de terrain de préparation à des opérations physiques, doxing en vue d'assassinat, appels à opération terroristes, vol de données sensibles pour des frappes, etc. Un stade a ainsi été franchi dans cette intensité avec des opérations hacktivistes devenant la brique cyber d'une guerre physique asymétrique.

Figure 20. Appel à renseignements sur personnel et infrastructures militaire ukrainiennes par NoName057(16) - Telegram

4.3.3. Campagnes de propagande ou désinformations

Le champ de la guerre psychologique fait partie de l'éventail des opérations menées par les hacktivistes mais s'éloigne quelque peu de leur cœur d'activités. Les actions psychologiques dans le champ cyber sont un sujet à part aux multiples ramifications. Les groupes cités précédemment peuvent cependant opérer des publications dans ce but afin de se mettre en avant ou de justifier leurs attaques.

Ainsi, le groupe Ghost of Palestine utilise ses canaux de diffusions afin de mener une guerre de propagande sur les actions militaires israéliennes, amplifiant les récits de résistance palestinienne ou mettre en avant les victimes de bombardement afin de remotiver l'opinion et justifier ses actions.

Figure 21. Vidéo de propagande anti israélienne publiée par Ghosts of Palestine

```
Traduction du post : "Quand ces missiles seront-ils lancés sur l'entité temporaire, ô Dieu, hâte-toi de
détruire les oppresseurs, notre Seigneur, et accepte que tu sois celui qui entend la supplication, et ton
Seigneur a dit : « Invoque-moi et je te répondrai » Ne sois pas arrogant au sujet du culte de la
supplication est très important, la façon des prophètes de parler avec Dieu, alors appelle-le par eux, et
évite ceux qui blasphèment ses noms, ils récompenseront ce qu'ils ont fait."
```

4.4. Outils

Pour mener à bien leurs attaques, les hacktivistes s'appuient sur des botnets. Certains exploitent plus spécifiquement Mirai. D'autres collectifs disposent de suffisamment d'adhérents et alliés pour composer leur parc sur la base de mise à disposition volontaire de machines. Ces réseaux utilisent alors des outils spécifiques pour coordonner leurs attaques.

4.4.1. DDOSIA

Le cœur du fonctionnement de NoName057 repose sur la distribution de l'outil DDOSIA. NoName057 recrute donc des volontaires via Telegram : une fois leur inscription au projet DDOSIA effectué, les nouveaux membres reçoivent au travers d'un bot un kit logiciel ainsi qu'un tutoriel destiné à l'installation de DDOSIA. Un canal de support en anglais est également disponible pour obtenir une assistance technique.

Développé en Python, DDoSia est capable de fonctionner sur plusieurs plateformes (Windows, Linux, macOS) et exploite la puissance de calcul des ordinateurs participants pour submerger les cibles de requêtes. Chaque machine est identifiée par un GUID unique (pour les environnements Windows extrait de la base de registres) et les données sont transmises de manière chiffrée, ce qui rend difficile la traçabilité des participants. L'outil se connecte à des serveurs de commande et de contrôle (C2) pour coordonner les attaques. Ces serveurs sont régulièrement changés afin d'éviter tout blocage.

4.4.2. MEGAMEDUSA

Le groupe RipperSec utilise le logiciel Megamedusa pour ses attaques DDOS, un outil développé en interne, disponible sur Github, MegaMedusa en est actuellement à sa version 3.2 .

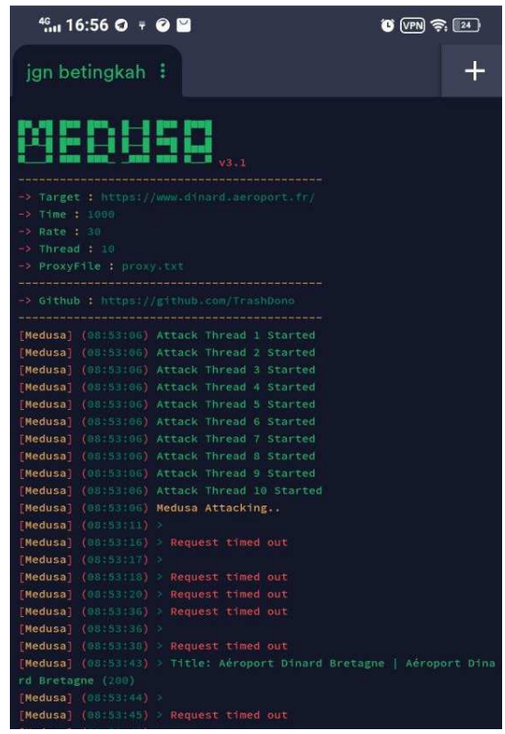


Figure 22. DDOS de l'aéroport de Dinard via MegaMedusa - Telegram

Le logiciel permet l'envoi massif de requêtes HTTP ou HTTPS et dispose de fonctionnalités permettant le contournement de CAPTCHAs ou de systèmes de protection tels que Cloudflare.

Figure 23. RipperSec propose MegaMedusa en accès libre- Telegram

L'outil semble être cependant limité et il semblerait que la version grand public soit bridée par rapport à l'outil utilisé en interne.

4.4.3. LOIC & HOIC

Low Orbit Ion Cannon (LOIC) et sa nouvelle version High Orbit Ion Cannon (HOIC) sont les outils DDoS open sources les plus répandus, souvent utilisés par des hacktivistes pour submerger un serveur de requêtes HTTP, UDP ou TCP. HOIC dispose d'une interface utilisateur le rendant accessible à des néophytes et peut accueillir des scripts personnalisés destinés à amplifier une attaque. HOIC est notamment utilisé par les groupes Anonymous, ainsi que par le collectif hacktiviste pro ukrainien HackYourMom.

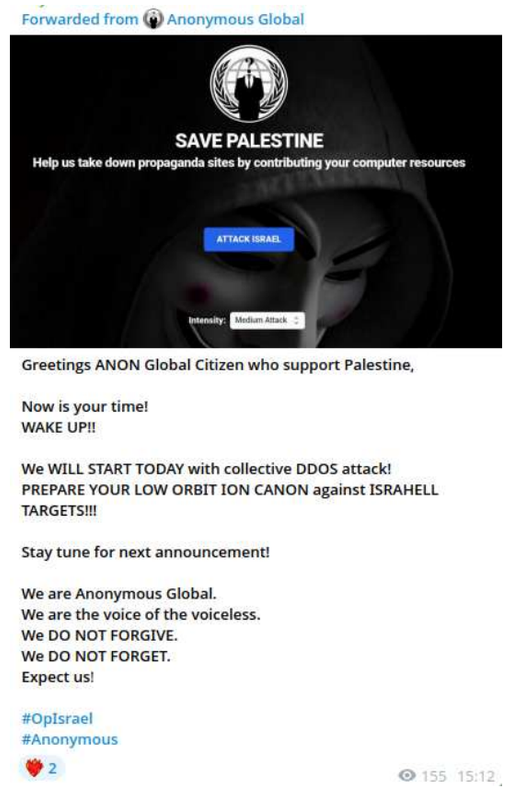


Figure 24. Message d'Anonymous Global revendiquant l'usage de LOIC- Telegram

D'autres outils sont également utilisés tels que Memcrashed, un outil permettant l'envoi de paquets UDP à des serveurs MemCached en utilisant l'API Shodan. Enfin, il convient de mentionner SlowLoris : un script permettant le DOS de serveur à partir d'une seule machine via un faible nombre de requêtes incomplètes empêchant la fermeture de connexions. Il s'agit du premier outil à avoir utilisé ce type d'attaque qui est maintenant largement utilisé par LOIC et HOIC.

Figure 25. Recommandations d'outils par le groupe propalestinien Team 1945 - Telegram

4.5. CONCLUSION

L'activité propre aux groupes hacktivistes est appelée à se développer, générant de nouvelles opportunités tels que le développement du DDOS as a service tel qu'il est pratiqué par Dark Storm Team ou le groupe Doubleface, membre de la Holy League.

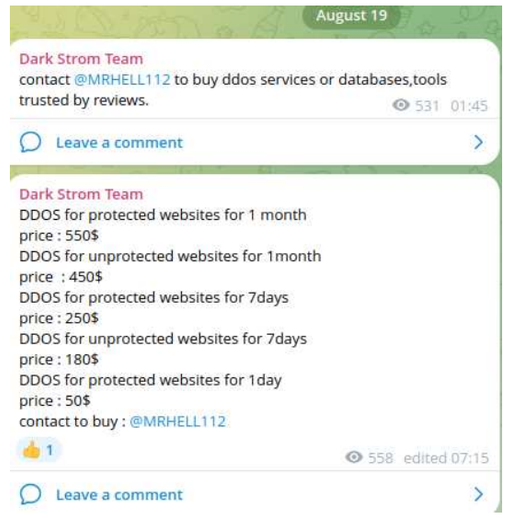


Figure 26. Pricing DDOS as a service - Telegram : Dark Storm Team

En fonction de l'évolution des conflits, une radicalisation peut être à craindre chez certains groupes ne souhaitant plus se limiter à des opérations symboliques. Ces activités sortent du cadre classique de l'hacktivisme pour rejoindre celui de la guérilla.

Ainsi, l'apparition de ces opérations cyber de faible envergure provenant de collectifs privés peut être comparée à l'avènement

des drones commerciaux FPV dans le conflit ukrainien : une nouvelle technique de combat asymétrique générée par une forme d'uberisation de la guerre.

5. Références

CVE-2024-28986

- https://nvd.nist.gov/vuln/detail/CVE-2024-28986
- https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28986
- https://www.cisa.gov/news-events/alerts/2024/08/15/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.helpnetsecurity.com/2024/08/15/cve-2024-28986/

CVE-2024-4885

- https://nvd.nist.gov/vuln/detail/CVE-2024-4885
- https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024
- https://summoning.team/blog/progress-whatsup-gold-rce-cve-2024-4885/
- https://x.com/Shadowserver/status/1821121075704647731
- https://thehackernews.com/2024/08/critical-security-flaw-in-whatsup-gold.html
- https://www.bleepingcomputer.com/news/security/critical-progress-whatsup-rce-flaw-now-under-active-exploitation/

CVE-2024-36971

- https://nvd.nist.gov/vuln/detail/CVE-2024-36971
- https://source.android.com/docs/security/bulletin/2024-08-01?hl=fr
- https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=92f1655aa2b2294d0b49925f3b875a634bd3b59e
- https://therecord.media/android-zero-day-google-fix-august-patch
- https://thehackernews.com/2024/08/google-patches-new-android-kernel.html

NUKESPEED - KOREANSPRITZ (APT LAZARUS)

- https://www.joesandbox.com/analysis/1464042/0/html
- https://bazaar.abuse.ch/sample/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/
- https://www.virustotal.com/gui/file/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/community
- https://cyber-fortress.com/docs/result/index.php?id=667e6dc27d0a7ff58bc74e3fwin10vpnfull_triage
- https://www.abuseipdb.com/check/211.47.74.11
- https://tria.ge/240628-jvzv4syeqb
- https://www.airgreensystem.com/index.html?menu=qlist1&dbname=oqbbs01
- https://www.google.com/maps/place/19-3+Jindeung-ro+19beon-gil,+Euijeongbu,+Gyeonggi-do,+Cor%C3%A9e+du+Sud/@37.7596224,127.028956,17z/data=!3m1!4b1!4m6!3m5!1s0x357cc12831a53295:0xdda7e5d50b75d3ed!8m2!3d37.7596224!4d127.0315309!16s%2Fg%2F11bz7d0dw2?hl=fr-FR&entry=ttu
- https://box.zero.camp/analysis/51384/summary/
- https://x.com/asdasd13asbz/status/1806561339604877609?t=RLQPn-uhVdUHo7DykjUrOg&s=19
- https://securelist.com/lazarus-threatneedle/100803/
- https://securelist.com/operation-applejeus/87553/
- https://threatpost.com/lazarus-targets-defense-threatneedle-malware/164321/
- https://malpedia.caad.fkie.fraunhofer.de/details/win.postnaptea

NUKESPEED (APT LAZARUS)

Variant 2019

- https://www.pcrisk.fr/guides-de-suppression/9478-nukesped-trojan-mac
- https://www.virustotal.com/gui/file/d91c233b2f1177357387c29d92bd3f29fab7b90760e59a893a0f447ef2cb4715/community

Variant 2020

- https://bazaar.abuse.ch/sample/aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6/
- https://www.virustotal.com/gui/file/aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6

Variant 2021

- https://bazaar.abuse.ch/sample/0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c/
- https://www.virustotal.com/gui/file/0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c/

Variant 2023

- https://bazaar.abuse.ch/sample/861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d/
- https://www.virustotal.com/gui/file/861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d/

Variant 2024 (KoreanSPritz)

- https://bazaar.abuse.ch/sample/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/
- https://www.virustotal.com/gui/file/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/

HACKTIVISME

- Sources principales : canaux et groupes Telegram

Profils

- https://socradar.io/dark-web-profile-noname05716/
- https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/rising-from-the-underground-hacktivism-in-2024

Outils

- https://www.radware.com/blog/uncategorized/2024/08/megamedusa-rippersec-public-web-ddos-attack-tool/?&web_view=true