aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de mai

2024-06-06 | **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 présentant un intérêt, en complément de celles déjà publiées.

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

- le maliciel LATRODECTUS présentant des similitudes avec IcedID.
- le cryptominer KINSING pouvant être utilisé comme accès persistent sur des machines compromises.

2. Vulnérabilités

Ce mois-ci, le CERT aDvens met en exergue **trois** vulnérabilités affectant des technologies fréquemment utilisées au sein des entreprises.
Elles sont présentées par ordre de gravité (preuves de concept disponibles, exploitation …). L'application de leurs correctifs ou contournements est fortement recommandée.

2.1. CVE-2024-29212

Le 7 mai 2024, Veeam a publié un bulletin de sécurité concernant une vulnérabilité critique dans Veeam Service Provider Console et publié des correctifs appropriés. Ces derniers ont été encore affinés et le bulletin mis à jour le 28 mai 2024.

Une désérialisation non sécurisée dans le serveur Veeam Service Provider Console (VSPC) permet à un attaquant authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire.

2.1.1. Type de vulnérabilité

- CWE-502: Deserialization of Untrusted Data

2.1.2. Risque

- Exécution de code arbitraire

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

Vecteur d'attaque	Réseau	Portée	Changée
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

2.1.4. Produits impactés

- Veeam Service Provider Console versions 4, 5, 6, 7 et 8

2.1.5. Recommandations

- Mettre à jour Service Provider Console version 7.x vers la version 7.0.0.19551 ou ultérieure.
- Mettre à jour Service Provider Console version 8.x vers la version 8.0.0.19552 ou ultérieure.
- Les versions 4, 5 et 6 ne sont plus prises en charge.
- Des informations complémentaires sont disponibles dans le bulletin de Veeam.

2.1.6. Preuve de concept

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

2.2. CVE-2024-26289

Le 22 mai 2024, l'Agence de l'Union Européenne pour la Cybersécurité (ENISA) publie un bulletin d'alerte sur une vulnérabilité critique affectant plusieurs versions du logiciel PMB. PMB est un Système Intégré de Gestion de Bibliothèque (SIGB), avec une version gratuite. Cet outil est très répandu dans de nombreuses bibliothèques publiques, bibliothèques de recherches, écoles, centres de ressources ou de documentation dans des entreprises ou des associations.

Une désérialisation de données non sécurisée dans PMB 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. Produit impacté

- PMB :
  - Versions comprises entre 7.3.1 et 7.3.18 (exclue),
  - Versions comprises entre 7.4.1 et 7.4.9 (exclue),
  - Versions comprises entre 7.5.1 et 7.5.6-2 (exclue)

2.2.5. Recommandations

- Mettre à jour PMB vers la version 7.3.18, 7.4.9, 7.5.6-2, 7.5.7 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de l'ENISA.

2.2.6. Preuve de concept

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

2.3. CVE-2024-25641

Le 14 mai 2024, Cacti a publié un bulletin de sécurité afin de corriger la vulnérabilité CVE-2024-25641. Celui-ci contient également une preuve de concept.

Un défaut de gestion des caractères spéciaux dans la bibliothèque */lib/import.php* du composant *Package Import* de Cacti permet à un attaquant authentifié avec l'autorisation *Import Templates* d'exécuter du code PHP arbitraire sur le serveur web.

2.3.1. Type de vulnérabilité

- CWE-20: Improper Input Validation

2.3.2. Risque

- Exécution de code arbitraire

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

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

2.3.4. Produit impacté

- Cacti version 1.2.26 et versions antérieures

2.3.5. Recommandations

- Mettre à jour Cacti vers la version 1.2.27 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Cacti.

2.3.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

3. LATRODECTUS, le remplaçant de IcedID ?

3.1. Contexte

LATRODECTUS est un logiciel malveillant découvert pour la première fois en **2023** par les chercheurs de *Walmart* alors qu'ils investiguaient sur une campagne du logiciel IcedID.

Ils ont alors remarqué que l'empreinte (imphash) de l'échantillon étudié présentait un **chevauchement** avec un autre exécutable. Ce groupe utilise des **tactiques** et des **outils similaires** à ceux des campagnes IcedID historiques, ce qui suggère un **rapprochement entre ces opérateurs**.

LATRODECTUS se distingue par sa capacité à **évoluer** et à **adapter** ses méthodes, ce qui en fait une menace **persistante** et **sophistiquée**.

Le logiciel malveillant agit comme un ***loader***, installant des charges utiles supplémentaires. Il offre également des **fonctionnalités standards** après la compromission initiale, telle que la découverte des processus, l'énumération et la suppression des fichiers en cours d'exécution. Ce type de logiciel malveillant est souvent utilisé pour déployer des **rançongiciels**. Dans le cadre des campagnes de LATRODECTUS, cela n'a pas encore été observé.

La **victimologie** n'est pour le moment **pas établie**, des opérations de LATRODECTUS ont été observées sur **diverses organisations** sans qu'elles soient précisées.

Les opérateurs utilisent principalement des courriels de **phishing** pour distribuer LATRODECTUS. Ces campagnes sont **soigneusement conçues** pour contourner les mesures de sécurité traditionnelles, en utilisant des techniques telles que l'usurpation d'identité et des domaines ressemblant à des entités légitimes pour tromper les victimes. Les courriels peuvent contenir des **documents Word** ou **Excel** avec des macros qui, une fois activées, installent des logiciels malveillants sur l'ordinateur de la victime.

3.2. Attribution

Selon *ProofPoint*, ce logiciel malveillant a d'abord été remarqué lors de sa distribution par TA577, groupe cybercriminel déjà connu pour avoir distribué massivement le maliciel Qbot jusqu'en 2023. TA577 a utilisé LATRODECTUS dans au moins trois campagnes en novembre 2023 avant de revenir à Pikabot. Depuis la mi-janvier 2024, les chercheurs l'ont observé être utilisé presque exclusivement par TA578 dans des campagnes de menaces par e-mail. Cet acteur utilise généralement des formulaires de contact pour initier une conversation avec une cible. Dans une campagne observée le 15 décembre 2023, *Proofpoint* a constaté que TA578 distribuait LATRODECTUS via une infection DanaBot.

3.3. Dernières campagnes

Début mars 2024, les chercheurs d'*Elastic Security Labs* ont observé une **augmentation des campagnes** par courriels diffusant LATRODECTUS. Il est alors distribué via des campagnes de phishing utilisant des thèmes *Microsoft* et *Cloudflare* pour paraître légitime. Ces courriels contenaient des **pièces jointes PDF** ou des **URLs** intégrées, menant à un faux captcha *Cloudflare*. Une fois le captcha résolu, un **script JavaScript** est téléchargé. Ce fichier JavaScript, de taille inhabituelle, utilise la capacité de WMI à invoquer msiexec.exe et à installer un fichier MSI hébergée à distance sur un partage WEBDAV pour **déployer la DLL** TRUFOS.DLL correspondant à LATRODECTUS.

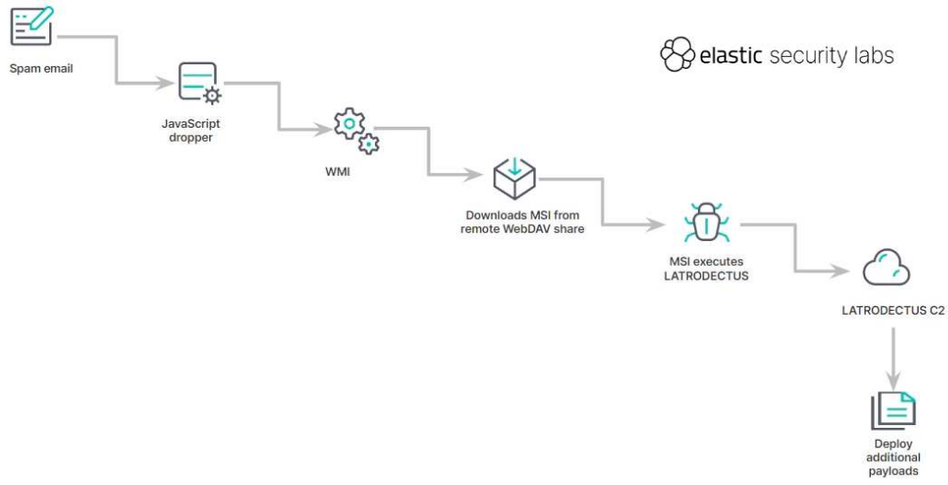
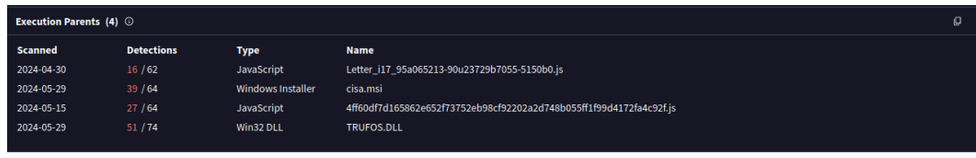


Figure 1. Chaine d'attaque LATRODECTUS

En effectuant des recherches sur le fichier malveillant analysé par *Elastic Security Labs*, il est possible de remonter le fil de cette campagne datant de mars 2024.



Execution Parents (4)

Scanned	Detections	Type	Name
2024-04-30	16 / 62	JavaScript	Letter_i17_95a065213-90u23729b7055-5150b0.js
2024-05-29	39 / 64	Windows Installer	cisa.msi
2024-05-15	27 / 64	JavaScript	4ff60df7d165862e652f73752eb98cf92202a2d748b055ff1f99d4172fa4c92f.js
2024-05-29	51 / 74	Win32 DLL	TRUFOS.DLL

Figure 2. VirusTotal TRUFOS.DLL

Le fichier TRUFOS.DLL a été exécuté par le fichier parent Letter_i17_95a065213-90u23729b7055-5150b0.js.

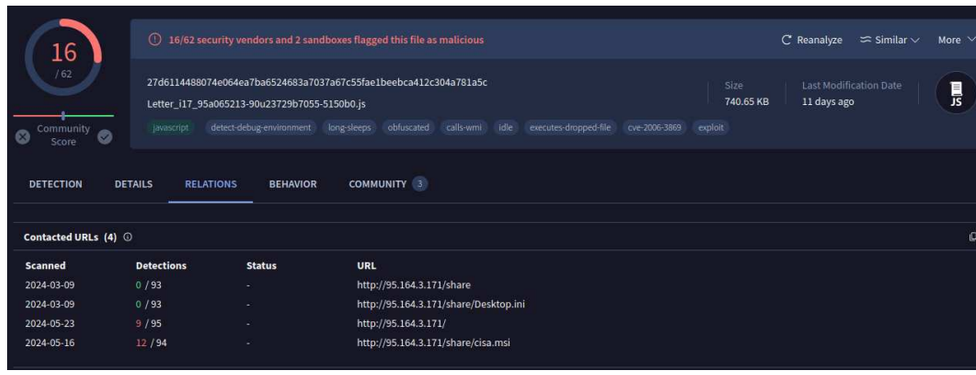
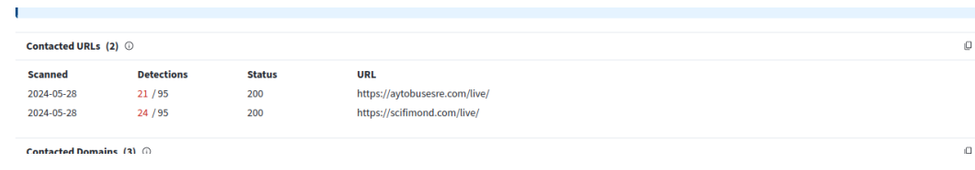


Figure 3. VirusTotal Letter_i17_95a065213-90u23729b7055-5150b0.js

Ce fichier malveillant, associé à LATRODECTUS, est également lié aux C2 hxxps://scifimond[.]com/live/ et hxxps://aytobusesre[.]com/live/.



Contacted URLs (2)

Scanned	Detections	Status	URL
2024-05-28	21 / 95	200	https://aytobusesre.com/live/
2024-05-28	24 / 95	200	https://scifimond.com/live/

Contacted Domains (3)

Figure 4. VirusTotal TRUFOS.DLL

3.4. L'infrastructure et les tactiques, techniques et procédures

Infrastructure

L'infrastructure des opérateurs de LATRODECTUS est **similaire** selon les différentes campagnes. Le groupe utilise des **domaines CloudFlare**, créés pour l'occasion comme C2. Les noms semble **générer aléatoirement**, avec des extensions différentes. Il existe toutefois un point commun à ces C2, la présence du **répertoire *"live"*** lors des diverses campagnes.

Ces domaines ne sont pas utilisés que pour une seule campagne, ils ont été vus sur **différentes périodes**. Le domaine hxxps://scifimond[.]com/live/ a été détecté la première fois le 4 mars 2024 et semble **actif** le 28 mai 2024.

Accès Initial

Les courriels de phishing, que ce soit à travers des pièces jointes malveillantes ou des liens spécifiquement forgés sont utilisés pour déployer le logiciel malveillant. Dans un premier temps, c'est un fichier Javascript (de taille inhabituelle) et contenant du texte aléatoire qui est installé sur la machine compromise.

Exécution

Le dropper JavaScript utilise WMI pour monter un partage WEBDAV et appelle msiexec pour installer un fichier MSI distant.

Une fois exécuté, il dépose la DLL LATRODECTUS et lance rundll32 pour la charger via le binaire Advanced Installer viewer.exe.

Évasion et défense

Rundll32 charge la DLL LATRODECTUS depuis AppData et commence l'injection de code. Lorsque celle-ci n'est pas chargée depuis AppData, elle se supprime tout en étant en cours d'exécution, puis redémarre à partir du nouveau chemin.

Afin d'éviter les *sandbox* ou les machines virtuelles qui peuvent avoir un nombre réduit de processus actifs, des vérifications sont utilisées pour combiner le nombre de processus en cours d'exécution avec la version du produit du système d'exploitation.

LATRODECTUS utilise les informations de fichier d'un composant de BitDefender (TRUFOS.SYS), se faisant passer pour celui-ci.

Persistance

Rundll32 va être utilisé pour créer des tâches planifiées, utilisant Windows Component Object Model (COM), pour établir de la persistance sur le système compromis.

Collection

Le logiciel malveillant utilise une liste de commandes Shell afin de collecter de l'information depuis le système compromis :

```
&ipconfig=
&systeminfo=
&domain_trusts=
&domain_trusts_all=
&net_view_all_domain=
&net_view_all=
&net_group=
&wmic=
&net_config_ws=
&net_wmic_av=
&whoami_group=
```

Commande et Contrôle

LATRODECTUS communique avec des serveurs de commande et de contrôle (C2) pour télécharger de nouvelles charges utiles.

Le logiciel malveillant chiffre ses requêtes, encodée en Base64, en utilisant RC4 et un mot de passe en dur "12345". La première requête POST via HTTPS inclut des informations sur la victime ainsi que des détails de configuration, enregistrant le système infecté.

3.5. IcedID et LATRODECTUS

3.5.1. Similarités techniques

Les deux groupes utilisent des **courriels de phishing** pour atteindre leurs victimes. Ces courriels sont souvent très **sophistiqués**, utilisant des techniques d'ingénierie sociale pour paraître légitimes et inciter les utilisateurs à ouvrir des pièces jointes ou cliquer sur des liens malveillants. Les documents attachés aux courriels, tels que les fichiers Word et Excel, contiennent des macros. Ces macros, une fois activées, téléchargent et exécutent des logiciels malveillants sur le système de la victime.

3.5.2. Infrastructures et outils partagés

Les deux groupes semblent **partager des infrastructures de C2** similaires. Cela inclut les serveurs utilisés pour contrôler les logiciels malveillants après leur installation sur les systèmes infectés. Cette infrastructure partagée suggère soit une collaboration directe entre les deux groupes, soit une utilisation commune de services criminels tiers.

Les analystes ont trouvé des **similitudes dans le code** des logiciels malveillants utilisés par LATRODECTUS et IcedID. Ces similitudes peuvent indiquer que LATRODECTUS utilise des variantes ou des versions modifiées des outils d'IcedID, ce qui est courant dans le milieu cybercriminel où le code malveillant est souvent échangé ou vendu entre groupes.

3.6. Conclusion

Il est possible que LATRODECTUS soit une **évolution** ou une **réorganisation des opérations** d'IcedID. Les groupes cybercriminels changent régulièrement de nom et de structure pour échapper aux autorités. LATRODECTUS pourrait donc être une **continuation des activités** d'IcedID sous un nouveau nom et avec quelques modifications pour améliorer leur efficacité et échapper à la détection. Toutefois, il semble que les capacités d'IcedID soient aujourd'hui, plus développées.

Une opération, nommée *EndGame* et menée par Europol est en cours afin d'entraver des services utilisés par les cybercriminels. Quatre logiciels malveillants, dont IcedID, sont concernés. À ce jour, quatre personnes ont été arrêtées et plus de 100 serveurs ont été mis hors ligne.

3.7. Règles de détection

```
rule Windows_Trojan_LATRODECTUS_841ff697 {
    meta:
        author = "Elastic Security"
        creation_date = "2024-03-13"
        last_modified = "2024-04-05"
        license = "Elastic License v2"
        os = "Windows"
        arch = "x86"
        threat_name = "Windows.Trojan.LATRODECTUS"
        reference_sample = "aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c"
    strings:
        $Str1 = { 48 83 EC 38 C6 44 24 20 73 C6 44 24 21 63 C6 44 24 22 75 C6 44 24 23 62 C6 44 24 24 }
        $crc32_loadlibrary = { 48 89 44 24 40 EB 02 EB 90 48 8B 4C 24 20 E8 ?? ?? FF FF 48 8B 44 24 40 48 81
C4 E8 02 00 00 C3 }
        $delete_self = { 44 24 68 BA 03 00 00 00 48 8B 4C 24 48 FF 15 ED D1 00 00 85 C0 75 14 48 8B 4C 24 50
E8 ?? ?? 00 00 B8 FF FF FF FF E9 A6 00 }
        $Str4 = { 89 44 24 44 EB 1F C7 44 24 20 00 00 00 00 45 33 C9 45 33 C0 33 D2 48 8B 4C 24 48 FF 15 7E
BB 00 00 89 44 24 44 83 7C 24 44 00 75 02 EB 11 48 8B 44 24 48 EB 0C 33 C0 85 C0 0F 85 10 FE FF FF 33 }
        $handler_check = { 83 BC 24 D8 01 00 00 12 74 36 83 BC 24 D8 01 00 00 0E 74 2C 83 BC 24 D8 01 00 00
0C 74 22 83 BC 24 D8 01 00 00 0D 74 18 83 BC 24 D8 01 00 00 0F 74 0E 83 BC 24 D8 01 00 00 04 0F 85 44 02 00
00 }
        $hwid_calc = { 48 89 4C 24 08 48 8B 44 24 08 69 00 0D 66 19 00 48 8B 4C 24 08 89 01 48 8B 44 24 08
8B 00 C3 }
        $string_decrypt = { 89 44 24 ?? 48 8B 44 24 ?? 0F B7 40 ?? 8B 4C 24 ?? 33 C8 8B C1 66 89 44 24 ?? 48
8B 44 24 ?? 48 83 C0 ?? 48 89 44 24 ?? 33 C0 66 89 44 24 ?? EB ?? }
        $campaign_fnv = { 48 03 C8 48 8B C1 48 39 44 24 08 73 1E 48 8B 44 24 08 0F BE 00 8B 0C 24 33 C8 8B
C1 89 04 24 69 04 24 93 01 00 01 89 04 24 EB BE }
    condition:
        2 of them
}
```

3.8. MITRE ATT&CK

RESOURCE DEVELOPMENT

T1583.001 Compromise Infrastructure: Domains T1587.001 Develop Capabilities: Malware

INITIAL ACCESS

T1566 Phishing T1566.001 Phishing: Spearphishing Attachment

EXECUTION

T1059.003 Command and Scripting Interpreter: Windows Command Shell T1047 Windows Management Instrumentation T1204 User Execution T1559.007 Command and Scripting Interpreter: JavaScript

PERSISTENCE

T1053.005 Scheduled Task/Job: Scheduled Task

PRIVILEGE ESCALATION

T1068 Exploitation for Privilege Escalation

DEFENSE EVASION

T1027 Obfuscated Filed or Information T1070.004 Indicator Removal: File Deletion T1036 Masquerading T1055 Process Injection T1218.007 System Binary Proxy Execution: Msiexec T1218.007 System Binary Proxy Execution: Rundll32

CREDENTIAL ACCESS

T1003 OS Credential Dumping

DISCOVERY

T1082 System Information Discovery

COLLECTION

T1005 Data from Local System

COMMAND AND CONTROL

T1105 Ingress Tool Transfer T1132 Data Encoding T1001 Data Obfuscation

EXFILTRATION

T1567 Exfiltration Over Web Service

Figure 5. TTPS LATRODECTUS

3.9. IOCs

TLP	TYPE	VALEUR	COMMENTAIRE	DATE
TLP:CLEAR	SHA256	db03a34684feab7475862080f59d4d99b32c74d3a152a53b257fd1a443e8ee77	LNK Payload	27 novembre 2023
TLP:CLEAR	SHA256	e99f3517a36a9f7a55335699cfb4d84d08b042d47146119156f7f3bab580b4d7	DLL Payload	27 novembre 2023
TLP:CLEAR	URL	hxxps://mazdakrichest[.]com/live/	Latrodectus C2	27 novembre 2023
TLP:CLEAR	URL	hxxps://riverhasus[.]com/live/	Latrodectus C2	27 novembre 2023
TLP:CLEAR	SHA256	bb525dc6b7a7ebefd040e01fd48d7d4e178f8d9e5dec9033078ced4e9aa4e241	JavaScript Payload	28 novembre 2023
TLP:CLEAR	SHA256	b97e093f2e0bf6dec8392618722dd6b4411088fe752bedece910d11fffe0288a2	DLL Payload	28 novembre 2023
TLP:CLEAR	URL	hxxp://162[.]55[.]217[.]30/gRMS/0[.]6395541546258323[.]dat	JavaScript Payload	28 novembre 2023
TLP:CLEAR	URL	hxxp://157[.]90[.]166[.]88/O3ZIYNW/0[.]7797109211833805[.]dat	JavaScript Payload	28 novembre 2023
TLP:CLEAR	URL	hxxp://128[.]140[.]36[.]37/cQtDlo/0[.]43650426987684443[.]dat	JavaScript Payload	28 novembre 2023
TLP:CLEAR	URL	hxxps://peermangoz[.]me/live/	Latrodectus C2	28 novembre 2023
TLP:CLEAR	URL	hxxps://aprettopizza[.]world/live/	Latrodectus C2	28 novembre 2023
TLP:CLEAR	URL	hxxps://nimeklroboti[.]info/live/	Latrodectus C2	28 novembre 2023
TLP:CLEAR	URL	hxxps://frotneels[.]shop/live/	Latrodectus C2	28 novembre 2023
TLP:CLEAR	SHA256	f9c69e79e7799df31d6516df70148d7832b121d330beebe52cff6606f0724c62	JavaScript Payload	28 novembre 2023
TLP:CLEAR	SHA256	d9471b038c44619739176381815bfa9a13b5ff77021007a4ede9b146ed2e04ec	DLL Payload	24 novembre 2023
TLP:CLEAR	URL	hxxps://hukosafaris[.]com/elearning/f/q/daas-area/chief/index[.]php	JavaScript Payload	24 novembre 2023
TLP:CLEAR	SHA256	d98cd810d568f338f16c4637e8a9cb01ff69ee1967f4cfc004de3f283d61ba81	DLL Payload	14 décembre 2023
TLP:CLEAR	SHA256	47d66c576393a4256d94f5ed1e77adc28426dea027f7a23e2dbf41b93b87bd78	EXE Payload	14 décembre 2023
TLP:CLEAR	IP	77[.]91[.]73[.]187:443	DanaBot C2	14 décembre 2023
TLP:CLEAR	IP	74[.]119[.]193[.]200:443	DanaBot C2	14 décembre 2023
TLP:CLEAR	URL	hxxps://arsimonopa[.]com/live	Latrodectus C2	14 décembre 2023
TLP:CLEAR	URL	hxxps://lemonimonakio[.]com/live	Latrodectus C2	14 décembre 2023
TLP:CLEAR	SHA256	bb525dc6b7a7ebefd040e01fd48d7d4e178f8d9e5dec9033078ced4e9aa4e241	JavaScript Payload	1 février 2024
TLP:CLEAR	SHA256	5d881d14d2336273e531b1b3d6f2d907539fe8489cbe80533280c9c72efa2273	DLL Payload	1 février 2024
TLP:CLEAR	URL	hxxp://superior-coin[.]com/ga/index[.]php	JavaScript Payload	1 février 2024
TLP:CLEAR	URL	hxxp://superior-coin[.]com/ga/m/6[.]dll	JavaScript Payload	1 février 2024
TLP:CLEAR	URL	hxxps://fluraresto[.]me/live/	Latrodectus C2	1 février 2024
TLP:CLEAR	URL	hxxps://mastralakkot[.]live/live/	Latrodectus C2	1 février 2024
TLP:CLEAR	URL	hxxps://postolwepok[.]tech/live/	Latrodectus Update	1 février 2024
TLP:CLEAR	URL	hxxps://trasenanoyr[.]best/live/	Latrodectus Update	1 février 2024
TLP:CLEAR	SHA256	10c129e2310342a55df5fa88331f338452835790a379d5230ee8de7d5f28ea1a	JavaScript Payload	5 février 2024

TLP	TYPE	VALEUR	COMMENTAIRE	DATE
TLP:CLEAR	SHA256	781c63cf4981fa6aff002188307b278fac9785ca66f0b6dfcf68adbe7512e491	MSI Payload	5 février 2024
TLP:CLEAR	SHA256	aa29a8af8d615b1dd9f52fd49d42563fbeafa35ff0ab1b4afc4cb2b2fa54a119	DLL Payload	5 février 2024
TLP:CLEAR	SHA256	0ac5030e2171914f43e0769cb10b602683ccc9da09369bcd4b80da6edb8be80e	JavaScript Payload	9 février 2024
TLP:CLEAR	SHA256	0e96cf6166b7cc279f99d6977ab0f45e9f47e827b8a24d6665ac4c29e18b5ce0	MSI Payload	9 février 2024
TLP:CLEAR	SHA256	77270e13d01b2318a3f27a9a477b8386f1a0ebc6d44a2c7e185cfbe55aac8017	DLL Payload	9 février 2024
TLP:CLEAR	URL	hxxps://miistoria[.]com/live	Latrodectus C2	9 février 2024
TLP:CLEAR	URL	hxxps://plwskoret[.]top/live	Latrodectus C2	9 février 2024
TLP:CLEAR	SHA256	e7ff6a7ac5bfb0bb29547d413591abc7628c7d5576a3b43f6d8e5d95769e553a	JavaScript Payload	13 février 2024
TLP:CLEAR	SHA256	dedbc21afc768d749405de535f9b415baaf96f7664ded55d54829a425fc61d7e	MSI Payload	13 février 2024
TLP:CLEAR	SHA256	378d220bc863a527c2bca204daba36f10358e058df49ef088f8b1045604d9d05	DLL Payload	13 février 2024
TLP:CLEAR	SHA256	edeacd49aff3cfea35d593e455f7caca35ac877ad6dc19054458d41021e0e13a	JavaScript Payload	20 février 2024
TLP:CLEAR	SHA256	9c27405cf926d36ed8e247c17e6743ac00912789efe0c530914d7495de1e21ec	MSI Payload	20 février 2024
TLP:CLEAR	SHA256	9a8847168fa869331faf08db71690f24e567c5cdf1f01cc5e2a8d08c93d282c9	DLL Payload	20 février 2024
TLP:CLEAR	URL	hxxp://178[.]23[.]190[.]199:80/share/gsm[.]msi	JavaScript WebDAV Payload	20 février 2024
TLP:CLEAR	URL	hxxps://sluitionsbad[.]tech/live/	Latrodectus C2	20 février 2024
TLP:CLEAR	URL	hxxps://grebiunti[.]top/live/	Latrodectus C2	20 février 2024
TLP:CLEAR	SHA256	856dfa74e0f3b5b7d6f79491a94560dbf3eacacc4a8d8a3238696fa38a4883ea	JavaScript Payload	23 février 2024
TLP:CLEAR	SHA256	88573297f17589963706d9da6ced7893eacbdc7d6bc43780e4c509b88ccd2aef	MSI Payload	23 février 2024
TLP:CLEAR	SHA256	97e08d1c7970c1c12284c4644e2321ce41e40cdaac941e451db4d334cb9c5492	DLL Payload	23 février 2024
TLP:CLEAR	URL	hxxp://5[.]252[.]21[.]207@80/share/escape[.]msi	JavaScript WebDAV Payload	23 février 2024
TLP:CLEAR	URL	hxxps://zumkoshapsret[.]com/live/	Latrodectus C2	23 février 2024
TLP:CLEAR	URL	hxxps://jertacco[.]com/live/	Latrodectus C2	23 février 2024
TLP:CLEAR	SHA256	60c4b6c230a40c80381ce283f64603cac08d3a69ceea91e257c17282f66ceddc	JavaScript Payload	27 février 2024
TLP:CLEAR	SHA256	88573297f17589963706d9da6ced7893eacbdc7d6bc43780e4c509b88ccd2aef	MSI Payload	27 février 2024
TLP:CLEAR	SHA256	97e08d1c7970c1c12284c4644e2321ce41e40cdaac941e451db4d334cb9c5492	DLL Payload	27 février 2024
TLP:CLEAR	URL	hxxp://5[.]252[.]21[.]207/share/escape[.]msi	JavaScript WebDAV	27 février 2024
TLP:CLEAR	SHA256	a189963ff252f547fddfc394c81f6e9d49eac403c32154eebe06f4cddb5a2a22	JavaScript Payload	4 mars 2024
TLP:CLEAR	SHA256	aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c	DLL Payload	4 mars 2024
TLP:CLEAR	URL	hxxp://95[.]164[.]3[.]171/share/cisa[.]msi	WebDAV Payload	4 mars 2024
TLP:CLEAR	URL	hxxps://scifimond[.]com/live/	Latrodectus C2	4 mars 2024

TLP	TYPE	VALEUR	COMMENTAIRE	DATE
TLP:CLEAR	URL	hxxps://aytobusesre[.]com/live/	Latrodectus C2	4 mars 2024
TLP:CLEAR	SHA256	4416b8c36cb9d7cc261ff6612e105463eb2ccd4681930ca8e277a6387cb98794	JavaScript Payload	7 mars 2024
TLP:CLEAR	SHA256	aee22a35cbdac3f16c3ed742c0b1bfe9739a13469cf43b36fb2c63565111028c	DLL Payload	7 mars 2024
TLP:CLEAR	URL	hxxps://popfealt[.]one/live/	Latrodectus Update	7 mars 2024
TLP:CLEAR	URL	hxxps://ginzbargatey[.]tech/live/	Latrodectus Update	7 mars 2024
TLP:CLEAR	URL	hxxps://minndarespo[.]icu/live/	Latrodectus Update	7 mars 2024
TLP:CLEAR	SHA256	090f2c5abb85a7b115dc25ae070153e4e958ae4e1bc2310226c05cd3e9429446	JavaScript Payload	11 mars 2024
TLP:CLEAR	SHA256	ee1e5b80a1d3d47c7703ea2b6b64ee96283ab3628ee4fa1fef6d35d1d9051e9f	MSI Payload	11 mars 2024
TLP:CLEAR	SHA256	3b63ea8b6f9b2aa847faa11f6cd3eb281abd9b9cceedb570713c4d78a47de567	DLL Payload	11 mars 2024
TLP:CLEAR	URL	hxxps://drifajizo[.]fun/live/	Latrodectus C2	11 mars 2024
TLP:CLEAR	URL	hxxps://scifimond[.]com/live/	Latrodectus C2	11 mars 2024
TLP:CLEAR	URL	hxxps://minndarespo[.]icu/live/	Latrodectus C2	11 mars 2024
TLP:CLEAR	SHA256	6904d382bc045eb9a4899a403a8ba8a417d9ccb764f6e0b462bc0232d3b7e7ea	JavaScript Payload	18 mars 2024
TLP:CLEAR	SHA256	71fb25cc4c05ce9dd94614ed781d85a50dccf69042521abc6782d48df85e6de9	DLL Payload	18 mars 2024
TLP:CLEAR	URL	hxxp://sokingscrosshotel[.]com/share/upd[.]msi	WebDAV Payload	18 mars 2024
TLP:CLEAR	URL	hxxps://titnovacrion[.]top/live/	Latrodectus C2	18 mars 2024

4. Kinsing Malware

Avec l'essor du Cloud, un nombre croissant de systèmes deviennent accessibles à tous, offrant ainsi aux cybercriminels de nouvelles ressources souvent insuffisamment protégées. Parmi les menaces courantes et sous-estimées se trouve le cryptominage. Ce type de logiciel malveillant exploite les ressources des systèmes pour générer des crypto-monnaies, tout en permettant à l'attaquant de maintenir un accès au système de la victime.

Kinsing, également connu sous le nom de h2Miner, constitue une menace active depuis cinq ans. Ce malware a été découvert en janvier 2020, bien que ses premières activités aient été observées en décembre 2019. Il est opéré par un groupe portant le même nom. Ce groupe cible principalement les infrastructures Cloud et les serveurs Linux pour déployer un rootkit ainsi qu'un mineur de cryptomonnaie. Quatre ans après sa découverte, le groupe continue de mener des campagnes réussies en conservant un mode opératoire quasiment inchangé.

4.1. Le malware

Kinsing est un logiciel développé en Go (Golang), se présentant sous la forme d'un fichier ELF et utilisé comme Remote Access Trojan (RAT) pour déployer un cryptomineur. Utilisé dans de multiples campagnes depuis 2019, principalement lors d'attaques opportunistes, ce malware permet aux cybercriminels de réaliser une primo-infection en exploitant principalement des vulnérabilités ou des mauvaises configurations dans des environnements Cloud.

Lors de la découverte de Kinsing en 2020, les opérateurs du malware ciblaient des API Docker mal configurées. Depuis, leur mode opératoire a évolué pour intégrer rapidement des scripts d'exploitation de vulnérabilités dès la publication de preuves de concept. Une liste (non exhaustive) des vulnérabilités exploitées est disponible en annexe.

Une fois la primo-infection obtenue, les attaquants téléchargent le malware Kinsing qui s'installe et établit une persistance sur le système. Ce malware inclut également un module nommé Masscan, qui lui permet de détecter les opportunités de latéralisation. Par la suite, Kinsing communique avec des serveurs C2 et installe un cryptomineur : XMrig. Ce dernier est un mineur open-source destiné à récupérer de la cryptomonnaie Monero. Le processus associé est souvent nommé *kdevtmpfsi*.

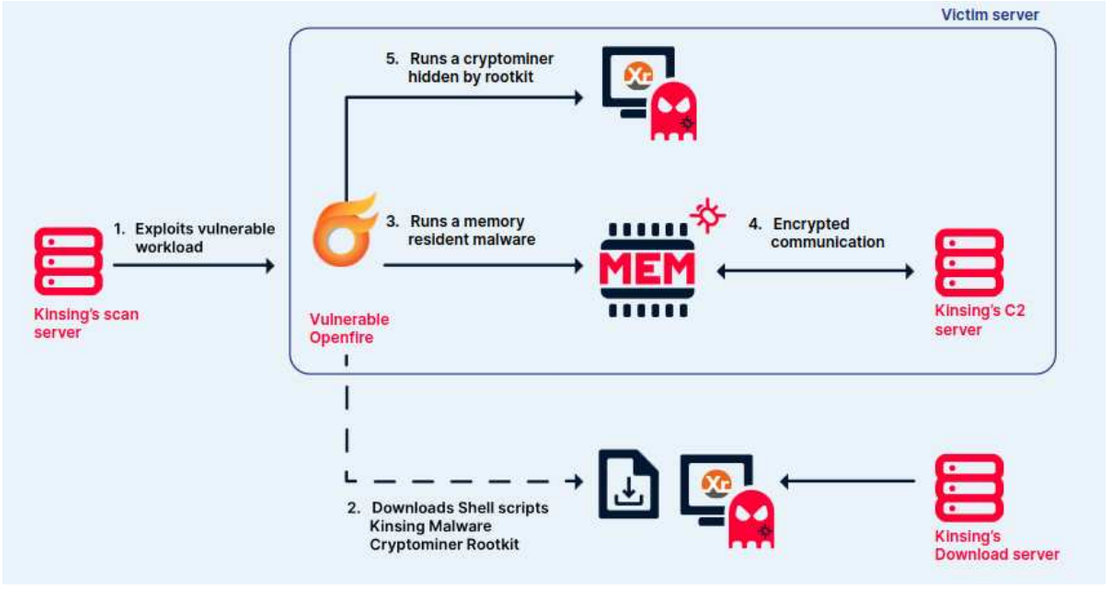


Figure 6. Campagne Openfire. Source : Aqua Nautilus

Dans le scénario présenté par les chercheurs d'Aqua Nautilus, les opérateurs exploitent la vulnérabilité CVE-2023-32315 dans Openfire pour obtenir l'accès initial.

4.2. Evasion de défense

Kinsing se distingue par ses méthodes d'évasion de défense, combinant des techniques courantes et des approches plus originales. Pour assurer l'efficacité de ces méthodes, plusieurs scripts d'installation de Kinsing et du malware lui-même existent, adaptés à l'architecture ciblée. Dans leur bulletin, les chercheurs en sécurité d'Aqua Nautilus identifient deux catégories de scripts d'installation : Type I et Type II.

- Les scripts Type I sont plus volumineux (environ 825 lignes) et cherchent essentiellement à éliminer d'autres implants malveillants "concurrents" (76% des lignes sont consacrées à cela). Ces fichiers pèsent environ 14 Mo.
- Les scripts Type II sont plus légers (environ 454 lignes) et se concentrent sur l'évasion de défense en installant un *rootkit* (un outil de persistence qui peut cacher son existence et celui d'autres logiciels). Ces fichiers pèsent environ 6 Mo.

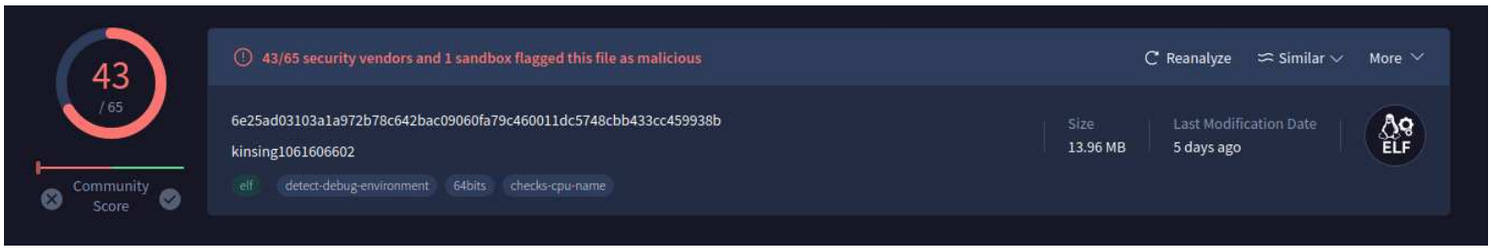


Figure 7. Script Type I

Figure 8. Script Type II

Suppression d'outils de défense

Lors de l'exécution de scripts Type I, certains outils de sécurité (tels que selinux, aegis, apparmor, etc.) sont arrêtés et supprimés. Le script désactive également les protections du parefeu *UFW* (via la commande *ufw disable*) et supprime les règles iptables (*iptables -f*).

Le script Type II, quant à lui, installe un *rootkit* dans le répertoire "*/etc/libsystem.so*".

Elimination d'autres malwares

Les deux types de scripts d'installation énumérent les processus présents dans le répertoire */proc* et mettent fin à certains processus spécifiques appartenant à des concurrents. Ces processus sont détectés grâce à une recherche par nom de processus, par certaines chaines de caractères ou d'adresses IP.

pkger

Un élément distinguant de Kinsing est la présence de l'entièreté de la pièce de théâtre *Hamlet* de Shakespeare dans certaines versions du malware. Les chercheurs de Cyberark ont trouvé l'origine de la présence de ce texte. La version 0.12.8 de l'outil opensource markbates/pkger disponible sur Github utilise ce texte et est intégré dans Kinsing.

Ce texte a pour objectif d'augmenter la taille du binaire et d'éviter la détection par des moteurs de scan statiques.

Les pages man

Dans des campagnes aussi récentes qu'avril 2024, Tenable a découvert Kinsing installé dans les pages de '*man*' de systèmes Linux. En effet, le malware s'est installé aux emplacements "*var/cache/man/zh_TW/cat8/*", "*/var/cache/man/cs/cat1/*" et "*/var/cache/man/cs/cat3/*". Ces emplacements sont utilisés, car ils ne sont pas souvent vérifiés pour la présence de malware.

4.3. Comparaison avec NSPPS

En 2021, Cyberark a mené une étude sur le malware Kinsing et a constaté de multiples similarités avec un autre malware nommé NSPPS.

NSPPS est un cheval de troie également développé en Go. Tout comme Kinsing, ce malware intègre l'outil Masscan. Pour l'utiliser, les deux contiennent un script bash nommé *firewire.sh* qui est exécuté par la fonction *main.masscan*. Les fichiers *firewire.sh* restent identiques mais les *main.masscan* diffèrent légèrement. Cyberark estime que cette différence est due à la compilation. Au moment de l'étude, ces fichiers n'étaient pas disponibles en sources ouvertes.

Une analyse du code montre que la structure utilisée est très similaire pour les deux malwares. La plus grande différence réside dans la fonctionnalité du cryptomineur présente uniquement dans Kinsing.

```
NSPPS
main.main()
{
healthChecker()
resultSender()

startSocks()
while (1):
    getTask()
    doTask()
    sleep()
}
```

```
Kinsing
main.main()
{
healthChecker()
resultSender()
minerRunningCheck()
startSocks()
while (1):
    getTask()
    doTask()
    sleep()
}
```

Figure 9. fonction main.main

```
main.doTask()
{
switch(task_name):
    case "scan":
        taskScan()
    case "update":
        updateTask()
    case "exec":
        execTask()
    case "exec_output":
        execTaskOut()
    case "masscan":
        masscan()
    case "socks":
        socks()
    case "backconnect":
        backconnect()
    case "request":
        makeClient()
        request()
    case "tcp":
        tcpTask()
    case "download_and_exec":
        downloadAndExecute()
    case "redis_brute":
        redisBrute()
}
```

```
main.doTask()
{
switch(task_name):
    case "scan":
        taskScan()
    case "update":
        updateTask()
    case "exec":
        startCmd()
    case "exec_output":
        execTaskOut()
    case "masscan":
        masscan()
    case "socks":
        socks()
    case "backconnect":
        backconnect()
    case "request":
        makeClient()
        runTaskWithHttp()
    case "tcp":
        runTask()
    case "download_and_exec":
        downloadAndExecute()
    case "redis_brute":
        redisBrute()
}
```

Figure 10. fonction main.doTask

Comparaison de code entre NSPPS (à gauche) et Kinsing (à droite). Source : Cyberark

Des chercheurs d'IronNet ont également découvert une clé *RC4* utilisé par NSPPS. Cette même clé était utilisée par Kinsing.

```
000000000088230E RC4_Key_Kinsing db 37h, 36h, 34h, 31h, 35h, 33h, 34h, 34h, 36h, 62h, 36h
000000000088230E                                        ; DATA XREF: .data:RC4_Key_off↓o
```

Figure N. 14: Kinsing RC4 key

```
00000000007B3F79 RC4_Key_NSPPS   db 37h, 36h, 34h, 31h, 35h, 33h, 34h, 34h, 36h, 62h, 36h
00000000007B3F79                                        ; DATA XREF: .data:RC4_Key_off↓o
```

Figure N. 15: NSPPS RC4 key

Figure 11. clé RC4. Source : CyberArk

La dernière étude portait sur les noms de fonctions. NSPPS contient 63 fonctions contre 59 pour Kinsing. Parmi celles-ci, 51 fonctions portent les mêmes noms, soit 84% des fonctions. Les 8 qui diffèrent dans Kinsing sont liées aux activités de cryptominage et les 12 de NSPPS sont liés aux activités de trojan.

Les similarités entre Kinsing et NSPPS donnent lieux à plusieurs hypothèses:

- Ces outils sont opérés par les mêmes opérateurs à des fins différentes.
- Un des deux outils provient d'une collaboration entre acteurs.
- Le premier malware a été récupéré et modifié par un acteur pour en faire son propre outil.

4.4. Conclusion

Bien que Kinsing ne soit pas récent, il demeure très efficace à l'encontre des environnements Cloud. Les opérateurs continuent de le maintenir et de le faire évoluer, notamment en améliorant ses performances et ses techniques d'évasion.

Le risque de cryptomineurs est souvent négligé mais ces logiciels permettent à des attaquants de maintenir des accès aux systèmes et peuvent provoquer des pertes financières aux entreprises victimes.

4.5. Annexes

4.5.1. Mitre Att&ck

DISCOVERY

T1595.002 Active Scanning: Vulnerability Scanning. T1087.001 Account Discovery: Local Account. T1083 File and Directory Discovery. T1057 Process Discovery. T1018 Remote System Discovery.

INITIAL ACCESS

T1190 Exploit Public-Facing Application. T1133 External Remote Services. T1078 Valid Accounts.

EXECUTION

T1059.004 Command & Scripting Interpréter: Unix Shell. T1106 Native API. T1204.002 User Execution: Malicious File. T1569.002 System Services: Service Stop. T1609 Container Administration Command.

PERSISTENCE

T1546.004 Event Triggered Execution: Unix Shell Configuration Modification. T1543.002 Create or Modify System Process: Systemd Service. T1053.005 Scheduled Task/Job: Scheduled Task. T1053.003 Scheduled Task/Job: Cron.

DEFENSE EVASION

T1222.002 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification. T1562.001/4 Impair Defenses: Disable or Modify Tools/System Firewall. T1070.004 Indicator Removal: File Deletion. T1027.002 Obfuscated Files or Information: Software Packing. T1140 Deobfuscate/Decode Files or Information. T1014 Rootkit.

DISCOVERY

T1595.002 Active Scanning: Vulnerability Scanning. T1087.001 Account Discovery: Local Account. T1083 File and Directory Discovery. T1057 Process Discovery. T1018 Remote System Discovery.

CREDENTIAL ACCESS

T1552.003 Unsecured Credentials: Bash History. T1552.004 Unsecured Credentials: Private Keys. T1110.001 Brute Force: Password Guessing.

COMMAND & CONTROL

T1071.001/2/4 Application Layer Protocol: Web Protocols/Proxy/DNS. T1105 Ingress Tool Transfer.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

IMPACT

T1496 Resource Hijacking. T1490 Inhibit System Recovery. T1485 Data Destruction.

Figure 12. Matrice Mitre Att&ck.

4.5.2. Detection

Regle YARA :

```
import "elf"
```

```
rule Kinsing_Malware
{
  meta:
    author = "Aluma Lavi, CyberArk"
    date = "22-01-2021"
    version = "1.0"
    hash = "d247687e9bdb8c4189ac54d10efd29aee12ca2af78b94a693113f382619a175b"
    description = "Kinsing/NSPPS malware"
  strings:
    $rc4_key = { 37 36 34 31 35 33 34 34 36 62 36 31 }
    $firewire = "./firewire -iL $INPUT --rate $RATE -p$PORT -oL $OUTPUT"
    $packa1 = "google/btree" ascii wide
    $packa2 = "kardianos/osext" ascii wide
    $packa3 = "kelseyhightower/envconfig" ascii wide
    $packa4 = "markbates/pkger" ascii wide
    $packa5 = "nu7hatch/gouuid" ascii wide
    $packa6 = "paulbellamy/ratecounter" ascii wide
    $packa7 = "peterbourgon/diskv" ascii wide
    $func1 = "main.RC4" ascii wide
    $func2 = "main.runTaskWithScan" ascii wide
    $func3 = "main.backconnect" ascii wide
    $func4 = "main.downloadAndExecute" ascii wide
    $func5 = "main.startCmd" ascii wide
    $func6 = "main.execTaskOut" ascii wide
    $func7 = "main.minerRunningCheck" ascii wide
  condition:
    (uint16(0) == 0x457F
    and not (elf.sections[0].size + elf.sections[1].size + elf.sections[2].size + elf.sections[3].size +
elf.sections[4].size + elf.sections[5].size + elf.sections[6].size + elf.sections[7].size > filesize))
    and ($rc4_key
    or $firewire
    or all of ($packa*)
    or 4 of ($func*)
    )
}
```

4.5.3. Indicateurs de Compromission

TLP	TYPE	VALUE	COMMENT	DATE
TLP:CLEAR	Sha256	0b0aa978c061628ec7cd611edeec3373d4742cbda533b07a2b3eb84a9dd2cb8a	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	0c811140be9f59d69da925a4e15eb630352fa8ad4f931730aec9ae80a624d584	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	2132d7bed60fda38adda28efdbbd2df2c9379fed5de2e68fc6801f5621b596b0	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	4b0138c12e3209d8f9250c591fcc825ee6bff5f57f87ed9c661df6d14500e993	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	4f4e69abb2e155a712df9b3d0387f9fb2d6db8f3a2c88d7bbe199251ec08683f	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	5059d67cd24eb4b0b4a174a072ceac6a47e14c3302da2c6581f81c39d8a076c6	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	511de8dd7f3cb4c5d88cd5a62150e6826cb2f825fa60607a201a8542524442e2	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	554c233d0e034b8bb3560b010f99f70598f0e419e77b9ce39d5df0dd3bc25728	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	655ee9ddd6956af8c040f3dce6b6c845680a621e463450b22d31c3a0907727e4	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	6814d22be80e1475e47e8103b11a0ec0daa3a9fdd5caa3a0558d13dc16c143d9	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	681f88d79c3ecab8683b39f8107b29258deb2d58fcea7b0c008bab76e18aa607	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	6e8c96f9e9a886fd6c51cce7f6c50d1368ca5b48a398cc1fedc63c1de1576c1e	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	7727a0b47b7fd56275fa3c1c4468db7fa201c788d1e56597c87deaff45aad634	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	7f9f8209dc619d686b32d408fed0beb3a802aa600ddceb5c8d2a9555cdb3b5e0	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	8c9b621ba8911350253efc15ab3c761b06f70f503096279f2a173c006a393ee1	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	98d3fd460e56eff5182d5abe2f1cd7f042ea24105d0e25ea5ec78fedc25bac7c	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	9fbb49edad10ad9d096b548e801c39c47b74190e8745f680d3e3bcd9b456aafc	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	a0363f3caad5feb8fc5c43e589117b8053cbf5bc82fc0034346ea3e3984e37e8	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	a5b010a5dd29d2f68ac9d5463eb8a29195f40f5103e1cc3353be2e9da6859dc6	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	b44dae9d1ce0ebec7a40e9aa49ac01e2c775fa9e354477a45b723c090b5a28f2	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	b70d14a7c069c2a88a8a55a6a2088aea184f84c0e110678e6a4afa2eb377649f	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	c44b63b1b53cbd9852c71de84ce8ad75f623935f235484547e9d94a7bdf8aa76	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	c9932ca45e952668238960dbba7f01ce699357bedc594495c0ace512706dd0ac	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	ccfda7239b2ac474e42ad324519f805171e7c69d37ad29265c0a8ba54096033d	source:Cyberark	3 september 2021

TLP	TYPE	VALUE	COMMENT	DATE
TLP:CLEAR	Sha256	d247687e9bdb8c4189ac54d10efd29aee12ca2af78b94a693113f382619a175b	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	db3b9622c81528ef2e7dbefb4e8e9c8c046b21ce2b021324739a195c966ae0b7	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	f2e7244e2a7d6b28b1040259855aeac956e56228c41808bccb8e37d87c164570	source:Cyberark	3 september 2021
TLP:CLEAR	Sha256	6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b	source:Lacework	12 december 2021
TLP:CLEAR	Sha256	c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	b9e79bb09995a9dd2f5a22dc2e59738696e2be2204ec92a2881fb3fa70e0160f	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	6fc94d8aecc538b1d099a429fb68ac20d7b6ae8b3c7795ae72dd2b7107690b8f	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	93fb80086c152179bfec7f19f5060758139828ef6938bac51ba8fbb673fc7b91	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	c6fbd6896d162a12d9c900056781eb82f44649945808b7b009646b5397bcf6bf	source:Sekoia	11 december 2023
TLP:CLEAR	Sha256	063f80c2c5accaecd8c9e6b6815ae80e372477f9df1113dafc72a2a0703aaa68	XMRig source:Tenable	16 may 2024

4.5.4. Liste des vulnérabilités exploitées

Produit	Identifiant CVE	Risque	Score CVSSv3
Citrix	CVE-2019-19781	Exécution de code arbitraire	9.8
Kibana	CVE-2019-7609	Exécution de code arbitraire	10
Oracle WebLogic	CVE-2020-14883	Compromission de serveur	7.2
SaltStack	CVE-2020-11651	Exécution de code arbitraire	9.8
SaltStack	CVE-2020-11652	Atteinte à la confidentialité	6.5
Liferay	CVE-2020-7961	Exécution de code arbitraire	9.8
WordPress File Manager	CVE-2020-25213	Exécution de code arbitraire	9.8
Apache HTTP Server	CVE-2021-41773	Exécution de code arbitraire	7.5
Log4j	CVE-2021-44228	Exécution de code arbitraire	10
Atlassian Confluence	CVE-2021-26084	Exécution de code arbitraire	9.8
Atlassian Confluence	CVE-2022-26134	Exécution de code arbitraire	9.8
WSO2	CVE-2022-29464	Exécution de code arbitraire	9.8
glibc	CVE-2023-4911	Exécution de code arbitraire	7.8
Apache ActiveMQ	CVE-2023-46604	Exécution de code arbitraire	9.8
Apache Openfire	CVE-2023-32315	Atteinte à la confidentialité	7.5

5. Références

CVEs

- https://nvd.nist.gov/vuln/detail/CVE-2024-29212
- https://www.veeam.com/kb4575
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0374/
- https://www.helpnetsecurity.com/2024/05/08/cve-2024-29212/
- https://nvd.nist.gov/vuln/detail/CVE-2024-25641
- https://github.com/Cacti/cacti/security/advisories/GHSA-7cmj-g5qc-pj88
- https://thehackernews.com/2024/05/critical-flaws-in-cacti-framework-could.html
- https://nvd.nist.gov/vuln/detail/CVE-2024-26289
- https://github.com/enisaeu/CNW/blob/main/advisories/2024/CNW-2024-A-12.md
- https://cert.be/en/advisory/warning-remote-code-inclusion-vulnerability-multiple-versions-pmb-library-software-patch

LATRODECTUS, le remplaçant de IcedID ?

- https://medium.com/walmartglobaltech/icedid-gets-loaded-af073b7b6d39
- https://www.elastic.co/security-labs/spring-cleaning-with-latrodectus
- https://www.proofpoint.com/us/blog/threat-insight/latrodectus-spider-bytes-ice
- https://github.com/pr0xylife/latrodectus/
- https://x.com/embee_research/status/1792826263738208343

Le malware Kinsing

- https://1665891.fs1.hubspotusercontent-na1.net/hubfs/1665891/Threat%20reports/AquaSecurity_Kinsing_Demystified_Technical_Guide.pdf
- https://www.cyberark.com/resources/threat-research-blog/kinsing-the-malware-with-two-faces
- https://redcanary.com/blog/threat-intelligence/kinsing-malware-citrix-saltstack/
- https://blog.sekoia.io/activemq-cve-2023-46604-exploited-by-kinsing-and-overview-of-this-threat/#h-iocs
- https://www.tenable.com/blog/kinsing-malware-hides-itself-as-a-manual-page-and-targets-cloud-servers
- https://www.trendmicro.com/vinfo/ph/security/news/virtualization-and-cloud/misconfigured-docker-daemon-api-ports-attacked-for-kinsing-malware-campaign
- https://sysdig.com/blog/cloud-defense-in-depth/
- https://www.ironnet.com/blog/malware-analysis-nspps-a-go-rat-backdoor