

A complex network visualization in shades of blue and teal, showing interconnected nodes and lines, resembling a globe or a data network. Some nodes are labeled with numbers like 5013, 2789, 3659, and 4617.

Renseignement sur les menaces

Bulletin du mois de septembre 2023

Sommaire

1. SYNTHÈSE	3
2. VULNÉRABILITÉS	4
2.1. ANDROID - CVE-2023-35674 (Exploitée)	4
2.1.1. Risque	4
2.1.2. Type de vulnérabilité	4
2.1.3. Criticité	4
2.1.4. Composants vulnérables	4
2.1.5. Recommandations	5
2.1.6. Preuve de concept	5
2.2. ACROBAT CVE-2023-26369 (Exploitée)	6
2.2.1. Risques	6
2.2.2. Type de vulnérabilité	6
2.2.3. Criticité	6
2.2.4. Composants vulnérables	6
2.2.5. Recommandations	7
2.2.6. Preuve de concept	7
2.3. MITSUBISHI MELSEC ELECTRIC CVE-2023-1424	8
2.3.1. Risques	8
2.3.2. Types de vulnérabilités	8
2.3.3. Criticité	8
2.3.4. Composants vulnérables	8
2.3.5. Recommandations	9
2.3.6. Mitigation	10
2.3.7. Preuve de concept	10
2.4. ACRONIS CVE-2023-41746	11
2.4.1. Risque	11
2.4.2. Type de vulnérabilité	11
2.4.3. Criticité	11
2.4.4. Composants vulnérables	11
2.4.5. Recommandations	11
2.4.6. Preuve de concept	11
2.5. GITLAB EE CVE-2023-5009	12
2.5.1. Risques	12
2.5.2. Type de vulnérabilité	12
2.5.3. Criticité	12
2.5.4. Composants vulnérables	12
2.5.5. Recommandations	12
2.5.6. Preuve de concept	12
3. AKIRA	13
3.1. Le rançongiciel AKIRA	13
3.2. Le groupe d'attaquants AKIRA	13
3.3. Campagne du groupe ciblant les accès VPN Cisco	16
3.4. Matrice MITRE ATT&CK	17
3.5. IOCs	18
3.6. Règles de détection YARA	19
4. STORM-0324 : LE PHISHING VIA MICROSOFT TEAMS	21

4.1. Historique	21
4.2. Nouveau MOA	22
4.3. Conclusion	23
4.4. Recommandations.....	23
4.5. Indicateurs de compromission JSS Loader	24
5. RÉFÉRENCES	25

1. Synthèse

Ce mois-ci, le CERT aDvens vous propose **cinq** vulnérabilités présentant un intérêt, en complément de celles déjà publiées.

Au travers de deux articles, les analystes du CERT dressent un portrait du récent groupe rançongiciel **AKIRA** ainsi que l'utilisation de campagne de phishing par le groupe cybercriminel **Storm-0324**, via l'application Teams; application collaborative largement déployées au sein des entreprises.

2. Vulnérabilités

Ce mois-ci, le CERT aDvens met en exergue **cinq** vulnérabilités affectant des technologies (IT/OT) 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.



Le CERT aDvens recommande de tester les mesures de contournement proposées dans un environnement dédié avant leur déploiement en production afin de prévenir tout effet de bord.

2.1. ANDROID - CVE-2023-35674 (Exploitée)



Annoncée dans le [bulletin de sécurité](#) du 5 septembre 2023, la [CVE-2023-35674](#) est une vulnérabilité importante qui affecte le système d'exploitation mobile *Android*.

Un défaut dans la configuration de ce système permet d'exécuter une tâche en arrière-plan.

L'exploitation de cette faille permet à un attaquant local, en utilisant des requêtes forgées, d'élever ses privilèges sur le système.



Cette vulnérabilité est exploitée.

2.1.1. Risque

- Élévation de privilèges

2.1.2. Type de vulnérabilité

- **CWE-371** : State Issues

2.1.3. Criticité

Vecteur d'attaque	Local	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. Composants vulnérables

Android Open Source Project (AOSP)

- Version 11
- Version 12
- Version 12L
- Version 13

2.1.5. Recommandations

- Appliquer la mise à jour du 5 septembre 2023.
- Des informations complémentaires sont disponibles sur le [site de l'éditeur](#).

2.1.6. Preuve de concept

Aucune preuve de concept n'est disponible en sources ouvertes.

2.2. ACROBAT CVE-2023-26369 (Exploitée)



Le 12 septembre 2023, *Adobe* publie le bulletin de sécurité [APSB23-34](#) dans lequel est mentionné la [CVE-2023-26369](#) : une vulnérabilité critique qui affecte la solution logicielle *Acrobat*.

Une gestion incorrecte du traitement des données lors de la lecture d'un document PDF a été identifiée. Des chercheurs ont découvert qu'il est possible d'écrire du code au-delà de l'espace alloué.

Un attaquant distant peut exploiter cette vulnérabilité de la manière suivante : il dissimule une charge utile dans un document PDF et incite l'utilisateur à le consulter. Lorsque le document est ouvert, le traitement des données génère un débordement de mémoire tampon et permet à la charge utile d'être exécutée sur le système.



Cette vulnérabilité est exploitée.



Une interaction avec l'utilisateur est nécessaire.



Le code arbitraire est exécuté avec les privilèges de l'utilisateur ayant consulté le document malveillant.

2.2.1. Risques

- Exécution de code arbitraire
- Déni de service

2.2.2. Type de vulnérabilité

- **CWE-787** : Out-of-bounds write

2.2.3. Criticité

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

2.2.4. Composants vulnérables

- *Acrobat DC*, versions 23.003.20284 et antérieures
- *Acrobat Reader DC*, versions 23.003.20284 et antérieures
- *Acrobat 2020*, versions 20.005.30516 (Mac) et antérieures
- *Acrobat 2020*, versions 20.005.30514 (Windows) et antérieures
- *Acrobat Reader 2020*, versions 20.005.30516 (Mac) et antérieures
- *Acrobat Reader 2020*, versions 20.005.30514 (Windows) et antérieures

2.2.5. Recommandations

Application de la mise à jour

- *Acrobat DC* : appliquer la mise à jour vers la version 23.006.20320
- *Acrobat Reader DC* : appliquer la mise à jour vers la version 23.006.20320
- *Acrobat 2020* : appliquer la mise à jour vers la version 20.005.30524
- *Acrobat Reader 2020* : appliquer la mise à jour vers la version 20.005.30524

Application manuelle de la mise à jour

- Bien que la solution logicielle *Acrobat* soit automatiquement mise à jour, il est possible d'appliquer les correctifs manuellement en accédant au menu "**Aide**" et en sélectionnant "**Vérifier la mise à jour**".

Ressources additionnelles

- Des informations complémentaires sont disponibles sur le [site de l'éditeur](#).
- Concernant *Acrobat DC*, *Adobe* recommande de consulter [la page des questions fréquemment posées](#).
- Concernant *Acrobat Reader DC*, *Adobe* recommande de consulter [la page des questions fréquemment posées](#).

2.2.6. Preuve de concept

Aucune preuve de concept n'est disponible en sources ouvertes.

2.3. MITSUBISHI MELSEC ELECTRIC CVE-2023-1424



Découverte par le chercheur en sécurité Matt Wiseman de l'équipe *Talos Intelligence Group* de *Cisco*, la [CVE-2023-1424](#) est une vulnérabilité critique qui affecte plusieurs produits de la série *MELSEC IQ-F / IQ-R*.

Le chercheur a identifié un défaut de type débordement de mémoire tampon.

L'exploitation de cette vulnérabilité permet à un attaquant distant, en envoyant des paquets forgés, de provoquer un déni de service ou d'exécuter du code arbitraire sur le système.



L'exécution de code arbitraire est considérée comme complexe. En effet, celle-ci requiert que l'attaquant ait une connaissance de la structure interne des produits ciblés.



Une compromission nécessitera la réinitialisation des systèmes.

2.3.1. Risques

- Exécution de code arbitraire
- Déni de service

2.3.2. Types de vulnérabilités

- **CWE-119** : Improper Restriction of Operations within the Bounds of a Memory Buffer
- **CWE-120** : Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

2.3.3. Criticité

Vecteur d'attaque	Réseau	Portée	Changée
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

2.3.4. Composants vulnérables

Série MELSEC IQ-F

Produits : FX5U-xMy/z x=32, 64, 80, y=T, R, z=ES, DS, ESS, DSS

- Numéro de série : 17X⁰⁰⁰⁰ ou ultérieures.
- Versions : de 1.220 à 1.281.

Produits : FX5UC-xMy/z x=32, 64, 96, y=T, z=D, DSS

- Numéro de série : 17X⁰⁰⁰⁰ ou ultérieures.
- Versions : de 1.220 à 1.281.

Produits : FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-T

- Versions : de 1.220 à 1.281.

Série MELSEC iQ-R

Produits : R00/01/02CPU

- Versions : 35 et antérieures.

Produits : R04/08/16/32/120(EN)CPU

- Versions : de 12 à 68.

Produits : R08/16/32/120SFCPU

- Versions : 26 et ultérieures.

Produits : R08/16/32/120PCPU

- Versions : de 3 à 37.

2.3.5. Recommandations

Correctifs

Pour la série MELSEC iQ-F

Produits : FX5U-xMy/z x=32, 64, 80, y=T, R, z=ES, DS, ESS, DSS

- Numéro de série : 17X^{oooo} ou antérieure.
- Appliquer la mise à jour vers la version 1.290 ou ultérieures.

Produits : FX5UC-xMy/z x=32, 64, 96, y=T, z=D, DSS

- Numéro de série : 17X^{oooo} ou antérieure.
- Appliquer la mise à jour vers la version 1.290 ou ultérieures.

Produits : FX5UC-32MT/DS-TS, FX5UC-32MT/DSS-TS, FX5UC-32MR/DS-TS

- Appliquer la mise à jour vers la version 1.290 ou ultérieures.

Pour la série MELSEC iQ-R

Produits : R00/01/02CPU

- Appliquer la mise à jour vers la version 36 ou ultérieures.

Produits : R04/08/16/32/120(EN)CPU

- Appliquer la mise à jour vers la version 69 ou ultérieures.

Produits : R08/16/32/120PCPU

- Appliquer la mise à jour vers la version 38 ou ultérieures.

Ressources additionnelles

L'éditeur Mitsubishi

- Des informations complémentaires sont disponibles sur le [site de l'éditeur](#).

L'agence CISA recommande les ressources additionnelles suivantes

- Document [control systems security recommended practices](#)
- Document [Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies](#)
- Document [ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies](#)

2.3.6. Mitigation

- Utiliser les produits vulnérables au sein d'un réseau local ;
- Utiliser un pare-feu ou un réseau privé virtuel (VPN) pour restreindre les accès au réseau local ;
- Appliquer un filtrage des adresses IP ;
- Restreinte l'accès physique aux produits vulnérables ;

Pour les fonctions de filtrage des adresses IP, des informations complémentaires sont disponibles dans les deux documentations ci-dessous

- " *12.1 IP Filter Function* " : Manuel d'utilisateur [MELSEC iQ-F FX5 \(Ethernet Communication\)](#)
- " *1.13 Security* " - " *IP filter* " : Manuel d'utilisateur [MELSEC iQ-R Ethernet \(Application\)](#)

2.3.7. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.4. ACRONIS CVE-2023-41746



Annoncée le 31 août 2023 dans le bulletin de sécurité [SEC-5810](#), la [CVE-2023-41746](#) est une vulnérabilité critique qui affecte *Acronis Cloud Manager* pour Windows.

Le contrôle des données saisies par l'utilisateur n'est pas réalisé de manière correcte.

En utilisant des requêtes malveillantes, un attaquant authentifié peut exécuter du code arbitraire sur le système.

2.4.1. Risque

- Exécution de code arbitraire

2.4.2. Type de vulnérabilité

- CWE-20 : Improper Input Validation

2.4.3. Criticité

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

2.4.4. Composants vulnérables

- *Acronis Cloud Manager* (Windows), build antérieure à 6.2.23089.203

2.4.5. Recommandations

- Appliquer la mise à jour *Acronis Cloud Manager* (Windows) vers la version 6.2.23089.203 ou ultérieure.
- Des informations complémentaires sont disponibles sur le [site de l'éditeur](#).

2.4.6. Preuve de concept

Aucune preuve de concept n'est disponible en sources ouvertes.

2.5. GITLAB EE CVE-2023-5009



Découverte par le chercheur en sécurité joaxcar d'*HackerOne*, la [CVE-2023-5009](#) est une vulnérabilité critique qui affecte l'*édition entreprise (EE)* de *Gitlab*.

Le chercheur a identifié une gestion inappropriée des privilèges dans l'application. Un attaquant peut ainsi exploiter les politiques de scan de sécurité planifiées pour exécuter un pipeline en usurpant un utilisateur.

Les risques de cette cyberattaque sont multiples. En effet, l'attaquant peut porter atteinte à la confidentialité des données. Par exemple, ce dernier peut récupérer des données d'identification ou le code source d'un projet. Par ailleurs, du code arbitraire peut aussi être exécuté par l'attaquant sur l'instance *Gitlab* vulnérable.

2.5.1. Risques

- Contournement de la politique de sécurité
- Exécution de code arbitraire
- Atteinte à la confidentialité des données

2.5.2. Type de vulnérabilité

- **CWE-269** : Improper Privilege Management

2.5.3. Criticité

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	Aucun

2.5.4. Composants vulnérables

Gitlab Enterprise Edition (EE)

- Versions 13.12 et antérieures à 16.2.7
- Versions 16.3 et antérieures à 16.3.4

2.5.5. Recommandations

- Appliquer la mise à jour de *GitLab EE* vers la version 16.2.7, 16.3.4 et ultérieures.
- Des informations complémentaires sont disponibles sur le [site de l'éditeur](#).

2.5.6. Preuve de concept

Aucune preuve de concept n'est disponible en sources ouvertes.

3. AKIRA

Le 12 septembre 2023, l'organisme de santé HC3 des États-Unis (Health Sector Cybersecurity Coordination Center) a publié un rapport d'alerte sur le tout nouveau groupe d'attaquants **AKIRA**. Remarqué au mois de mars de cette année, le groupe revendiquait alors déjà 16 victimes compromises. Actuellement, **AKIRA** aurait fait une soixantaine de victimes, dont 45 uniquement aux États-Unis, avec des demandes de rançon importantes allant de 200 000 à 4 millions de dollars US. Les secteurs les plus ciblés sont l'industrie, la finance, la santé et l'immobilier.

3.1. Le rançongiciel AKIRA

Ce groupe ne doit pas être confondu avec un autre rançongiciel également nommé **Akira**, actif depuis 2017, qui n'est pas lié à ce nouveau groupe d'attaquants éponymes.

Le nouveau venu possède deux variants :

- Le variant **Windows** est un binaire de 64 bits développé en C++ et délivre une clef symétrique chiffrée avec le chiffrement RSA-4096,
- Le variant **Linux** cible les serveurs **VMware ESXi** et utilise la bibliothèque Crypto++.

Le groupe procède à son accès initial avec des identifiants valides compromis, possiblement achetés sur le Dark Web. Toutefois, d'autres vecteurs de compromissions (courriels d'hameçonnage, sites Web malveillants ou chevaux de Troie) ne sont pas à exclure.

Une fois déployé, le malware supprime les *Shadow Copies* avec la commande suivante via **PowerShell** :

```
powershell.exe -Command "Get-WmiObject Win32_Shadowcopy | Remove-WmiObject"
```

Une fois le chiffrement lancé, celui-ci va épargner les fichiers contenus dans les dossiers `winnt`, `temp`, `thumb`, `Recycle Bin`, `System Volume Information`, `Boot`, `ProgramData`, `Windows` et `Trend Micro`. De même, les fichiers avec les extensions suivantes sont exclus du chiffrement : `.exe`, `.lnk`, `.dll`, `.msi` et `.sys` et `akira_readme.txt`. Tout le reste est chiffré avec l'extension `.akira`.

Le malware utilise l'API **Windows Restart Manager** pour fermer tous les processus actifs ou services qui maintiendraient un fichier ouvert. Le rançongiciel effectue un *dump* mémoire du LSASS, effectué avec **Mimikatz**, puis continue à se latéraliser.

Akira est le premier groupe à utiliser **RustDesk**, un outil d'accès à distance *open-source*, pour naviguer sur les réseaux de ses victimes. **RustDesk** étant un outil légitime, cet accès furtif ne déclenche aucune alarme sur les réseaux compromis. Par ailleurs, les attaquants activent l'accès RDP sur les serveurs, et inhibent les dispositifs de sécurité en désactivant **Windows Defender** et le pare-feu **Windows**.

3.2. Le groupe d'attaquants AKIRA

Les chercheurs en sécurité pointent aujourd'hui des similarités fortes entre **Akira** et le groupe **Conti** (ex-**Ryuk**).

Les modèles de portefeuilles de cryptomonnaies sont les mêmes que ceux utilisés précédemment par les opérateurs dirigeants de **Conti**. De plus, les échantillons de code source dans les malwares des deux groupes montrent de fortes similitudes, comme l'algorithme de chiffrement **ChaCha2008**, ou les répertoires exclus du chiffrement, comme `winnt` et `Trend Micro`.

Pour rappel, le groupe **Conti** avait prêté allégeance à la Russie suite à l'offensive en Ukraine début 2022. En représailles, le groupe a subi une fuite de données significative en février 2022, exfiltrée par l'un de ses propres membres. Le groupe s'est par la suite fragmenté entre soutiens à la Russie ou à l'Ukraine. Toutes ces concordances laissent à penser que le groupe **Akira** tire son origine de l'éclatement de **Conti**, dont il est une émanation.

A ce titre, la note de rançon est rédigée en anglais mais comporte des fautes de grammaire :

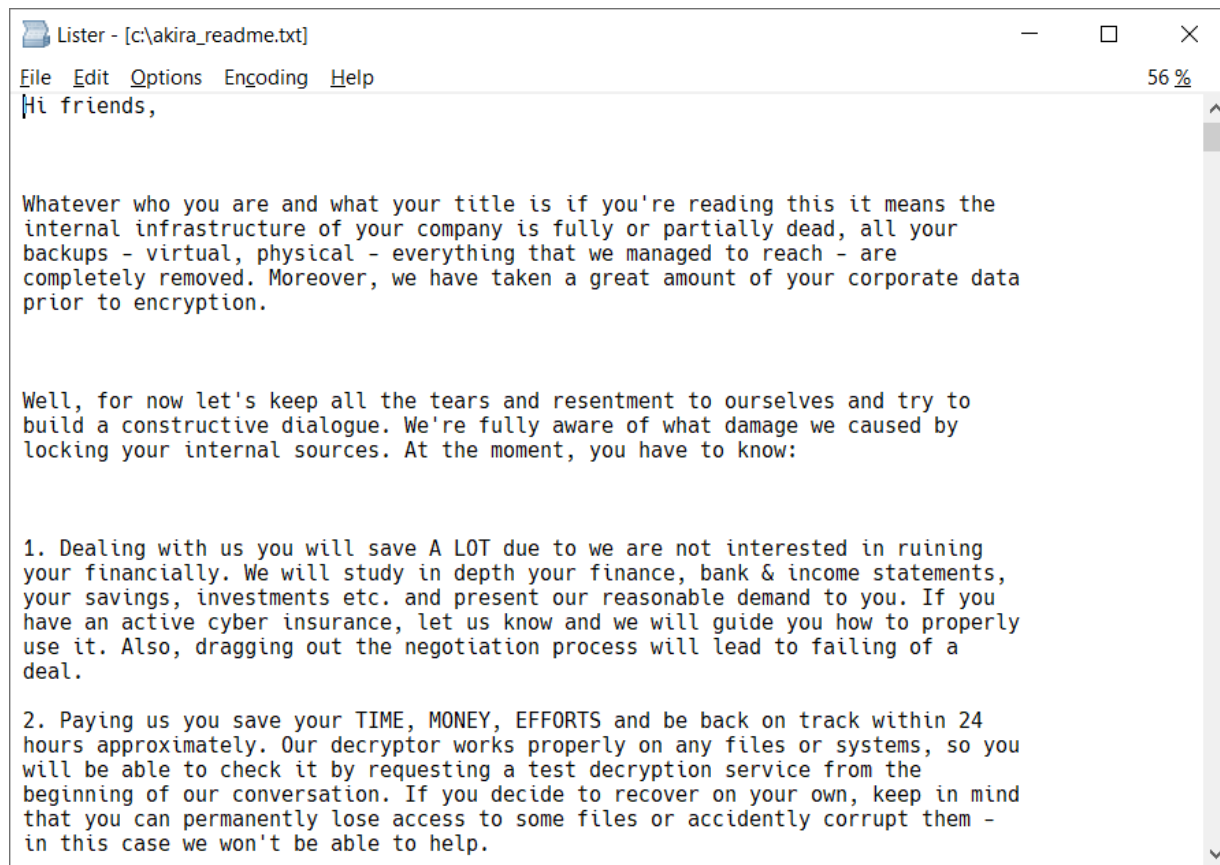


Figure 1. Note de rançon d'AKIRA (source : Bleeping Computer).

La demande de rançon invite à se rendre sur le site Web en *.onion* d'AKIRA pour négocier avec le groupe via un mot de passe unique. De plus, cette note de rançon propose aussi à la victime un prétendu audit de sécurité complet de son système, pour l'informer des failles exploitées.

Akira se distingue également avec l'habillage de son site Internet, conçu comme un site des années 80, dans lequel les visiteurs peuvent naviguer en exécutant des commandes :

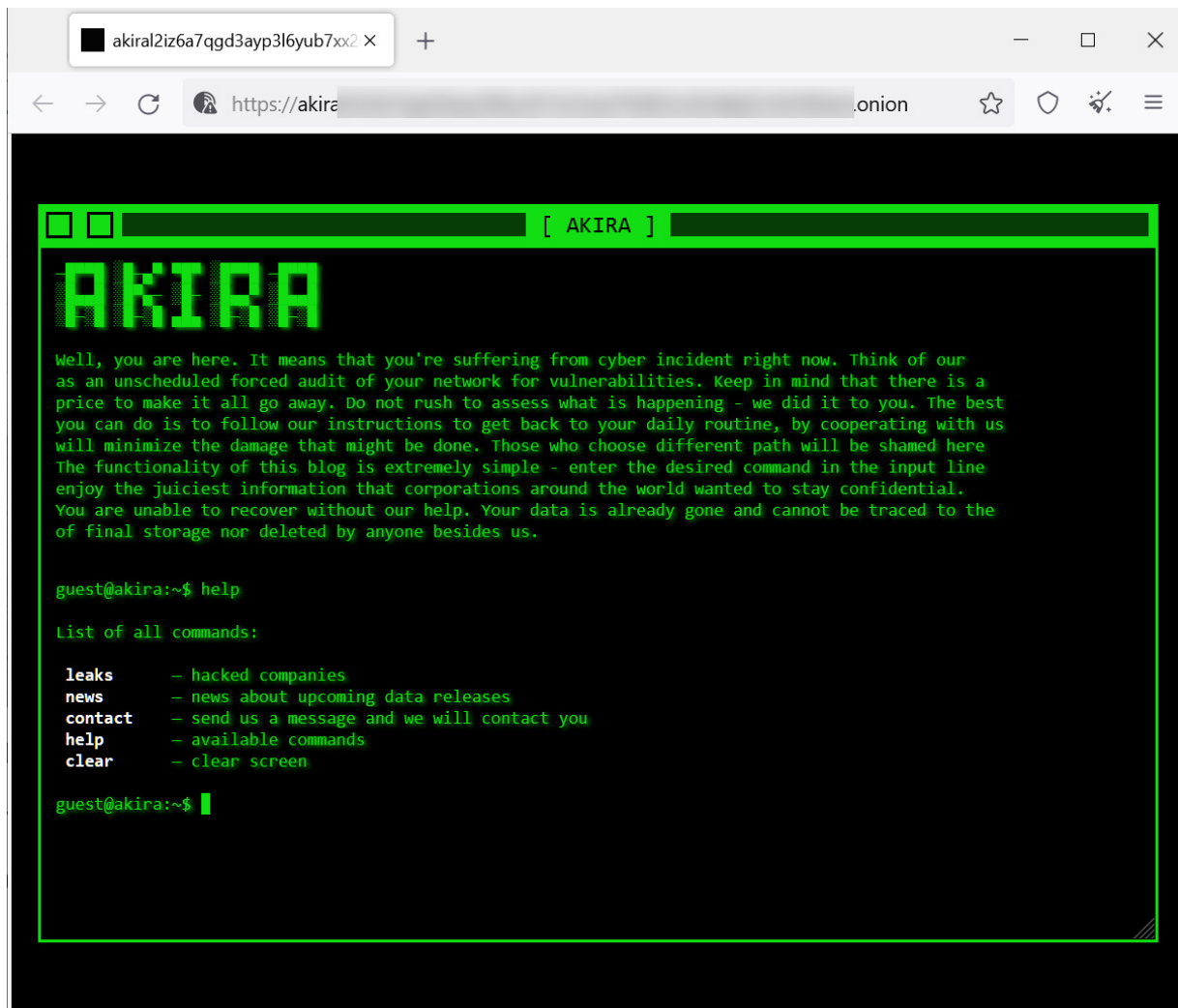


Figure 2. Site vitrine d'AKIRA (source : Bleeping Computer).

Le groupe suit maintenant la tendance de ses homologues et pratique la triple extorsion :

- Chiffrement du système d'information de la cible,
- Exfiltration et publication d'une partie des données,
- Prise de contact avec clients et partenaires de la victime pour les informer de l'attaque.

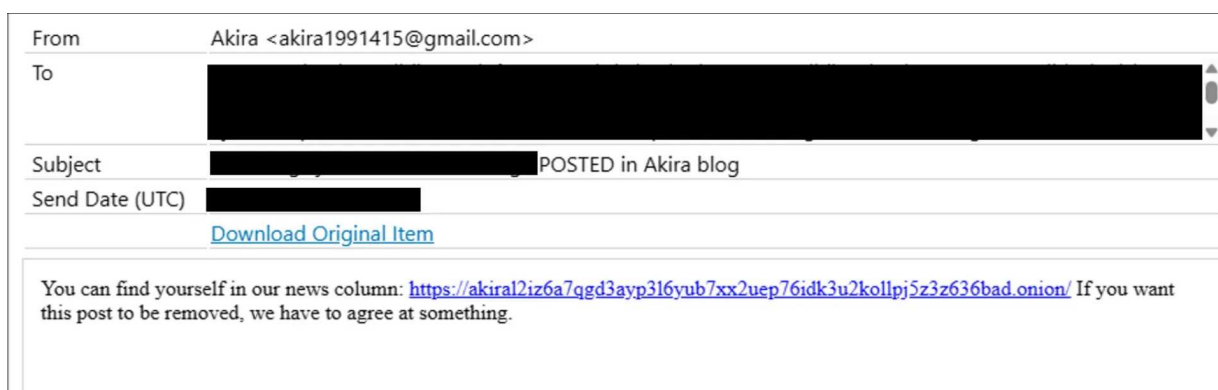


Figure 3. Prise de contact avec l'adresse akira1991415@gmail[.]com (source : TrueSec).

On peut noter que malgré sa doctrine de triple extorsion, Akira innove encore en proposant une double tarification. En effet, la victime peut choisir :

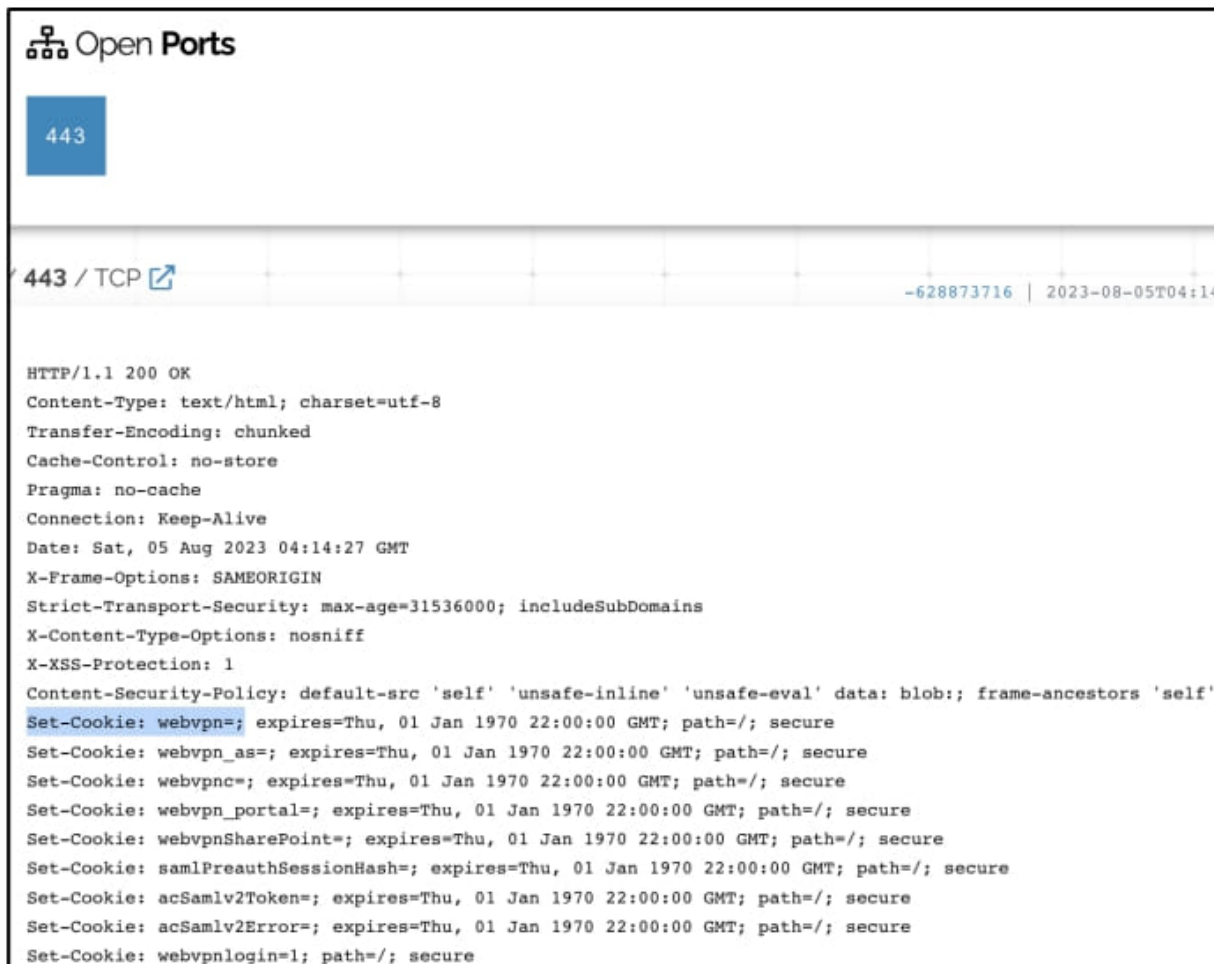
- Soit de payer la rançon pour lever le chiffrement,
- Soit de payer un tarif moindre pour retirer l'accès à ses données exfiltrées et rendues publiques.

3.3. Campagne du groupe ciblant les accès VPN Cisco

Dans une campagne de mai 2023, le groupe a exploité la vulnérabilité [CVE-2023-20269](#) pour cibler spécifiquement les VPN Cisco d'organisations qui n'ont pas mis en place l'authentification multifacteurs (MFA).

Le groupe s'est servi de comptes Cisco valides et compromis pour s'infiltrer dans les réseaux sans déployer de portes dérobées ou de mécanismes de persistance. A ce stade, on ignore encore si ces identifiants Cisco ont été obtenus par force brute ou achetés.

L'éditeur Cisco a confirmé le 24 août 2023 que ses passerelles VPN avaient bien été utilisées comme vecteurs de compromission. Cette approche, observée dans 8 différentes attaques, indique une stratégie d'attaque de la part du groupe Akira.



```
Open Ports  
443  
443 / TCP -628873716 | 2023-08-05T04:14  
HTTP/1.1 200 OK  
Content-Type: text/html; charset=utf-8  
Transfer-Encoding: chunked  
Cache-Control: no-store  
Pragma: no-cache  
Connection: Keep-Alive  
Date: Sat, 05 Aug 2023 04:14:27 GMT  
X-Frame-Options: SAMEORIGIN  
Strict-Transport-Security: max-age=31536000; includeSubDomains  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1  
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval' data: blob;; frame-ancestors 'self'  
Set-Cookie: webvpn=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: webvpn_as=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: webvpnc=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: webvpn_portal=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: webvpnSharePoint=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: samlPreauthSessionHash=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: acSamlv2Token=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: acSamlv2Error=; expires=Thu, 01 Jan 1970 22:00:00 GMT; path=/; secure  
Set-Cookie: webvpnlogin=1; path=/; secure
```

Figure 4. Caractéristiques VPN Cisco observées dans les attaques (source : SentinelOne).

3.4. Matrice MITRE ATT&CK



Figure 5. Matrice Mitre Att&ck du groupe AKIRA.

3.5. IOCs

TLP	TYPE	VALEUR
TLP:CLEAR	SHA256	5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5
TLP:CLEAR	SHA256	3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
TLP:CLEAR	SHA256	678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
TLP:CLEAR	SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
TLP:CLEAR	SHA256	8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
TLP:CLEAR	SHA256	1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
TLP:CLEAR	SHA256	9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163
TLP:CLEAR	SHA256	d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959
TLP:CLEAR	SHA256	6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
TLP:CLEAR	SHA256	1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
TLP:CLEAR	Courriel	akira1991415[at]gmail[.]com

3.6. Règles de détection YARA

```
[TLP:CLEAR] win_akira_auto (20230715 | Detects win.akira.)

rule win_akira_auto {

  meta:
    author = "Felix Bilstein - yara-signator at cocacoding dot com"
    date = "2023-07-11"
    version = "1"
    description = "Detects win.akira."
    info = "autogenerated rule brought to you by yara-signator"
    tool = "yara-signator v0.6.0"
    signator_config = "callsandjumps;datarefs;binvalue"
    malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.akira"
    malpedia_rule_date = "20230705"
    malpedia_hash = "42d0574f4405bd7d2b154d321d345acb18834a41"
    malpedia_version = "20230715"
    malpedia_license = "CC BY-SA 4.0"
    malpedia_sharing = "TLP:WHITE"

  /* DISCLAIMER
  * The strings used in this rule have been automatically selected from the
  * disassembly of memory dumps and unpacked files, using YARA-Signator.
  * The code and documentation is published here:
  * https://github.com/fxb-cocacoding/yara-signator
  * As Malpedia is used as data source, please note that for a given
  * number of families, only single samples are documented.
  * This likely impacts the degree of generalization these rules will offer.
  * Take the described generation method also into consideration when you
  * apply the rules in your use cases and assign them confidence levels.
  */

  strings:
    $sequence_0 = { 4d3bca 7223 49893b 41c7430802000000 41c6431001 e9???????? b8ffffffff }
    // n = 7, score = 100
    // 4d3bca | mov | dword ptr [esp + 0x20], ebp
    // 7223 | inc | ecx
    // 49893b | sub | dh, bh
    // 41c7430802000000 | imul | ebp, edi
    // 41c6431001 | inc | eax
    // e9???????? | |
    // b8ffffffff | movsx | eax, dh

    $sequence_1 = { e8???????? 4c8bc0 488bd3 488d4c2440 e8???????? 488d154de80600 488d4c2440 }
    // n = 7, score = 100
    // e8???????? | |
    // 4c8bc0 | dec | eax
    // 488bd3 | sub | esp, ecx
    // 488d4c2440 | dec | eax
    // e8???????? | |
    // 488d154de80600 | lea | ebx, [esp + 0x50]
    // 488d4c2440 | dec | eax

    $sequence_2 = { 488d8597010000 4c8bc7 0f1f840000000000 49ffc0 6642833c4000 75f5 488d9597010000 }
    // n = 7, score = 100
    // 488d8597010000 | dec | eax
    // 4c8bc7 | mov | eax, dword ptr [ebp - 8]
    // 0f1f840000000000 | dec | eax
    // 49ffc0 | mov | ebx, dword ptr [eax + 0x88]
    // 6642833c4000 | dec | eax
    // 75f5 | mov | eax, dword ptr [ebp - 0x20]
    // 488d9597010000 | dec | eax

    $sequence_3 = { 742c 4c8bc6 488d15fbf80400 488bcf e8???????? 488d55c0 48837dd810 }
    // n = 7, score = 100
    // 742c | dec | eax
    // 4c8bc6 | mov | edi, eax
    // 488d15fbf80400 | jmp | 0x3c2
    // 488bcf | dec | ecx
    // e8???????? | |
    // 488d55c0 | mov | edi, ebp
    // 48837dd810 | dec | eax

    $sequence_4 = { 488bd9 488bc2 488d0d45550400 0f57c0 488d5308 48890b 488d4808 }
    // n = 7, score = 100
    // 488bd9 | mov | edi, dword ptr [edi + 8]
    // 488bc2 | dec | eax
    // 488d0d45550400 | test | edi, edi

```

```

// 0f57c0      | jne      0x4f
// 488d5308   | dec     eax
// 48890b     | mov     edi, dword ptr [ebp - 0x79]
// 488d4808   | dec     eax

$sequence_5 = { 488d542420 e8???????? 8bf8 85c0 750d f744243010000000 0f95c3 }
// n = 7, score = 100
// 488d542420   | test    edi, edi
// e8????????   |
// 8bf8         | jne     0x649
// 85c0         | mov     edx, dword ptr [esp + 0x3b8]
// 750d         | cmp     edx, 0x3b9aca00
// f744243010000000 | dec     eax
// 0f95c3       | lea    eax, [esp + 0x50]

$sequence_6 = { 488b842430010000 668910 4c892b e8???????? eb7a 0f1f00 488d4b28 }
// n = 7, score = 100
// 488b842430010000 | add     edx, ecx
// 668910          | dec     eax
// 4c892b          | sar     edx, 6
// e8????????     |
// eb7a           | dec     eax
// 0f1f00          | mov     eax, edx
// 488d4b28        | dec     eax

$sequence_7 = { 0f57c0 0f118580110000 0f57c9 660f7f8d90110000 488d85d9010000 4c8bc7 660f1f440000 }
// n = 7, score = 100
// 0f57c0         | mov     eax, edi
// 0f118580110000 | nop     dword ptr [eax + eax]
// 0f57c9         | dec     ecx
// 660f7f8d90110000 | inc     eax
// 488d85d9010000 | movups  xmmword ptr [ebp + 0xfc0], xmm0
// 4c8bc7         | xorps   xmm1, xmm1
// 660f1f440000   | movdqa xmmword ptr [ebp + 0xfd0], xmm1

$sequence_8 = { 4688840da5000000 49ffc1 4983f90a 72a1 0f57c0 0f1185c00c0000 0f57c9 }
// n = 7, score = 100
// 4688840da5000000 | cmp     ecx, dword ptr [eax]
// 49ffc1           | jne     0xd18
// 4983f90a        | dec     eax
// 72a1            | add     eax, 2
// 0f57c0          | dec     ecx
// 0f1185c00c0000 | sub     edx, esp
// 0f57c9          | jne     0xcc9

$sequence_9 = { 6666660f1f840000000000 420fb68c0d84000000 83e955 446bc11f b809040281 41f7e8 }
// n = 6, score = 100
// 6666660f1f840000000000 | dec     ecx
// 420fb68c0d84000000 | inc     eax
// 83e955           | inc     dx
// 446bc11f         | cmp     dword ptr [eax + eax*2], 0
// b809040281      | movdqa xmmword ptr [ebp + 0x1070], xmm1
// 41f7e8          | dec     eax

condition:
  7 of them and filesize < 1219584
}

```

4. Storm-0324 : le phishing via Microsoft Teams

Le 12 septembre 2023, l'équipe de Threat Hunting de Microsoft rend officiel un rapport sur un nouveau groupe cybercriminel nommé **Storm-0324** (alias **TA543** ou **Sagrid**). Ce groupe est connu pour être spécialisé dans la revente d'accès initiaux (access broker) obtenus au travers de courriels d'hameçonnage. L'objet du rapport de Microsoft se concentre sur un nouveau mode opératoire d'attaque opéré par ce groupe, le phishing via **Microsoft Teams**.

4.1. Historique

Les investigations sur **Storm-0324** confirment que cet acteur a permis, ces dernières années, le déploiement de plusieurs outils malveillants tels que les rançongiciels **Clop**, **Mazeet**, **REvil**, les malwares **JSSLoader** et **Trickbot** – ce dernier étant utilisé lors des premières phases d'attaque du rançongiciel **Sangria Tempest** (**FIN7**) – ou encore les chevaux de Troie **Gootkit** et **Dridex**. L'infostealer **Gozi** et le malware **Nymaim** figurent également dans l'arsenal de **Storm-0324**.

L'essentiel des accès initiaux permettant le déploiement de ces outils malveillant est obtenu via des opérations d'hameçonnages ciblées. **Storm-0324** s'appuie en effet sur des systèmes de distribution de trafic (TDS) tels que **BlackTDS** et **Keitaro** afin d'échapper à une éventuelle détection par des solutions de filtrage et de protection. Les contenus des mails d'hameçonnage sont généralement à caractère professionnel, invitant la victime à cliquer sur un lien redirigeant vers un supposé service de gestion de documents tels que **DocuSign** ou **Quickbooks**.



Figure 6. Mail de Phishing Storm-0324 - Source : Microsoft

Les victimes sont en fin de compte redirigées vers un serveur SharePoint hébergeant un fichier compressé malveillant au format Microsoft Office documents, Windows Script File (WSF), Epika ou VBScript, contenant un code JavaScript qui enclenche finalement le téléchargement de la charge utile sur le poste de la victime grâce à l'exploitation de la **CVE-2023-21715**.

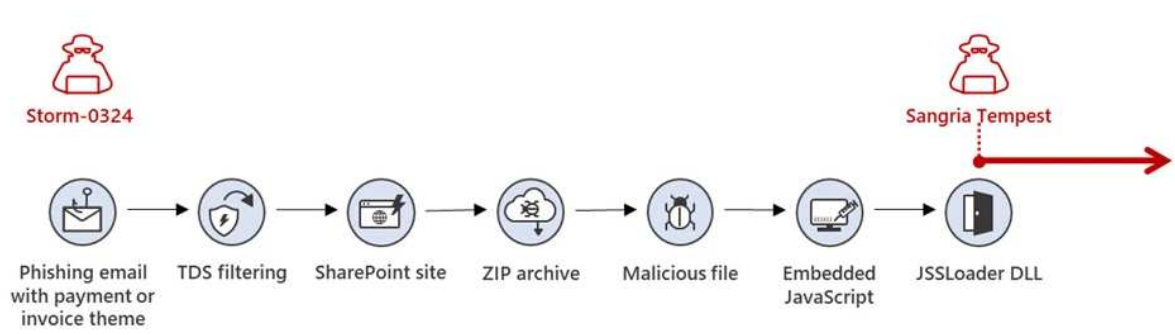


Figure 7. Chaîne d'infection JSSLoader par Storm-0324 - Source : Microsoft

Storm-0324 applique actuellement ce MOA pour l'implémentation du rançongiciel **Sangria Tempest** en déployant **JSSLoader** en charge utile. Il est à noter que certains emails de phishing peuvent être personnalisés avec l'ajout de codes ou de mot de passe « sécurisant » la redirection vers le document malveillant. Cet artifice permet non seulement de baisser la vigilance de la victime, mais également de bloquer l'analyse du document à dissimulé derrière le lien.

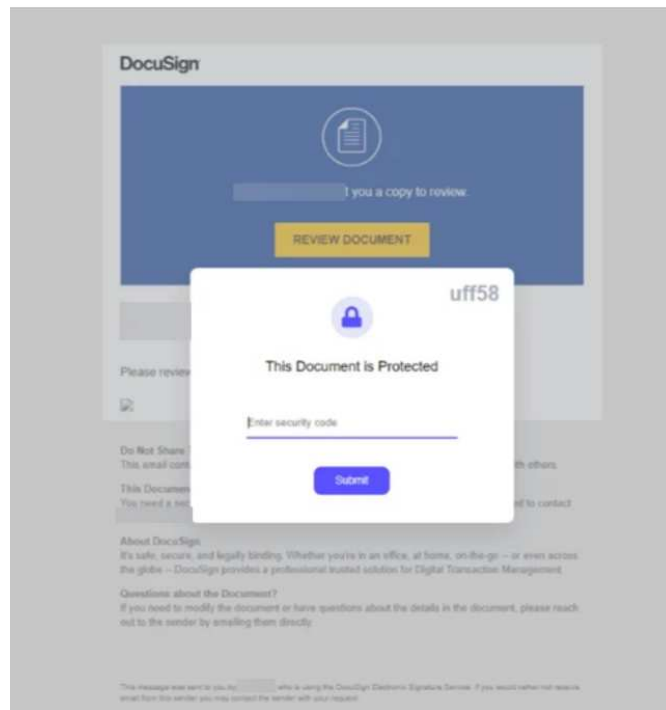


Figure 8. Demande d'authentification - Phishing - Source : Microsoft

4.2. Nouveau MOA

Les premières observations concernant ce nouveau MOA datent de juillet 2023. La chaîne d'infection précédemment exposée est modifiée : les liens de redirection menant à un fichier malveillant hébergé sur SharePoint sont désormais partagés sur Microsoft Teams. Cette évolution du mode opératoire s'accompagne de l'utilisation d'un nouvel outil Python nommé **TeamsPhisher**, permettant l'ajout de pièces jointes dans des messages destinés à des utilisateurs Teams dont les organisations autorisent les communications externes.

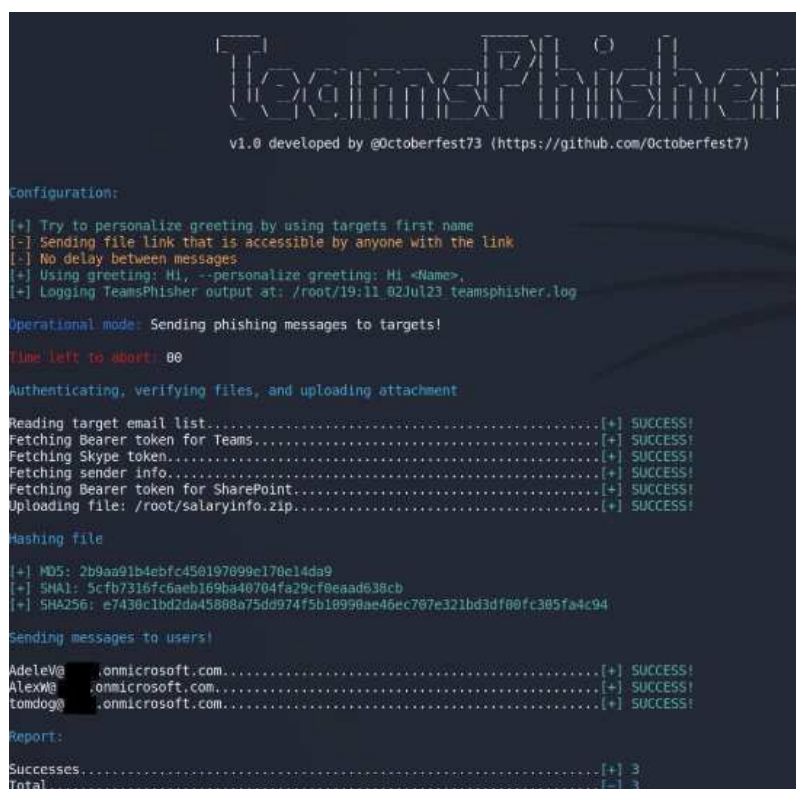


Figure 9. Console TeamsPhisher - source : Github

Devant l'emploi de cette nouvelle tactique, Microsoft a procédé à des mises à jour de sa solution Teams, notamment en soulignant

visuellement le fait qu'un utilisateur est extérieur à une organisation, en permettant le blocage d'utilisateurs dans des conversations en tête à tête ou encore en notifiant aux administrateurs la création de nouveaux domaines au sein de leurs réseaux.

4.3. Conclusion

Ce nouveau mode opératoire adopté par [Storm-0324](#) illustre une nouvelle fois l'adaptabilité des cybercriminels dans la course aux accès initiaux.

La détection de toute compromission par le groupe [Storm-0324](#) est d'autant plus importante que l'accès initial obtenu dans le système ciblé est ensuite proposé à la vente, multipliant ainsi la possibilité que celui-ci soit exploité par un groupe rançongiciel.

4.4. Recommandations

Face à ces tentatives d'hameçonnage par l'intermédiaire de Microsoft Teams, plusieurs recommandations peuvent être appliquées afin de diminuer cette menace :

- Paramétrage et, si possible, désactivation de l'accès externe dans Microsoft Teams.
- Mise en place de l'authentification multifacteur pour l'accès à Microsoft Teams.
- Renforcement de la sensibilisation des collaborateurs aux techniques d'hameçonnage et d'ingénierie sociale
- Blocage de l'exécution de contenus Javascript ou Bscript issus de téléchargements

Des recommandations supplémentaires sont disponibles sur le blog de Microsoft. Afin de se protéger contre cette nouvelle menace, l'équipe Microsoft met à disposition une requête permettant la détection de fichiers potentiellement partagés à l'aide de [TeamsPhisher](#).



La requête doit être modifiée avec le nom de domaine SharePoint personnel (« mysharepointname »)

```
let allowedSharepointDomain = pack_array(
'mysharepointname' //customize Sharepoint domain name and add more domains as needed for your query
);
//
let executable = pack_array(
'exe',
'dll',
'xll',
'msi',
'application'
);
let script = pack_array(
'ps1',
'py',
'vbs',
'bat'
);
let compressed = pack_array(
'rar',
'7z',
'zip',
'tar',
'gz'
);
//
let startTime = ago(1d);
let endTime = now();
DeviceFileEvents
| where Timestamp between (startTime..endTime)
| where ActionType =~ 'FileCreated'
| where InitiatingProcessFileName has 'teams.exe'
  or InitiatingProcessParentFileName has 'teams.exe'
| where InitiatingProcessFileName !has 'update.exe'
  and InitiatingProcessParentFileName !has 'update.exe'
| where FileOriginUrl has 'sharepoint'
  and FileOriginReferrerUrl has_any ('sharepoint', 'teams.microsoft')
| extend fileExt = tolower(tostring(split(FileName, '.') [-1]))
| where fileExt in (executable)
  or fileExt in (script)
  or fileExt in (compressed)
```



```
extend fileGroup = iff( fileExt in (executable),'executable','')
extend fileGroup = iff( fileExt in (script),'script',fileGroup)
extend fileGroup = iff( fileExt in (compressed),'compressed',fileGroup)
//
extend sharePoint_domain = toString(split(FileOriginUrl,'/')[2])
where not (sharePoint_domain has_any (allowedSharepointDomain))
project-reorder Timestamp, DeviceId, DeviceName, sharePoint_domain, FileName, FolderPath, SHA256,
FileOriginUrl, FileOriginReferrerUrl
```

4.5. Indicateurs de compromission JSS Loader

TLP	TYPE	VALEUR
TLP:CLEAR	SHA256	dd86898c784342fc11c42bea4c815cb536455ee709e7522fb64622d9171c465d
TLP:CLEAR	Domaine C2	bikweb[.]com
TLP:CLEAR	SHA256	a062a71a6268af048e474c80133f84494d06a34573c491725599fe62b25be044
TLP:CLEAR	Domaine C2	monusorge[.]com
TLP:CLEAR	SHA256	7a17ef218eebfdd4d3e70add616adcd5b78105becd6616c88b79b261d1a78fdf
TLP:CLEAR	Domaine C2	injuryless[.]com

5. Références

GOOGLE ANDROID CVE-2023-35674

- <https://exchange.xforce.ibmcloud.com/vulnerabilities/265268>
- <https://www.cybersecurity-help.cz/vdb/SB2023090551>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-35674>
- <https://source.android.com/docs/security/bulletin/2023-09-01?hl=fr>
- <https://vuldb.com/?id.239439>

ACROBAT CVE-2023-26369

- <https://exchange.xforce.ibmcloud.com/vulnerabilities/265786>
- <https://www.cybersecurity-help.cz/vdb/SB2023091235>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-26369>
- <https://helpx.adobe.com/security/products/acrobat/apsb23-34.html>

MITSUBISHI MELSEC ELECTRIC CVE-2023-1424

- <https://exchange.xforce.ibmcloud.com/vulnerabilities/256027>
- <https://www.cybersecurity-help.cz/vdb/SB2023052433>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-1424>
- https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-003_en.pdf
- https://www.talosintelligence.com/vulnerability_reports/TALOS-2023-1727
- <https://www.cisa.gov/news-events/ics-advisories/icsa-23-143-03>
- <https://www.mitsubishielectric.com/fa/download/index.html>
- <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices>
- https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- <https://www.cisa.gov/news-events/news/targeted-cyber-intrusion-detection-and-mitigation-strategies-update-b>

ACRONIS CVE-2023-41746

- <https://exchange.xforce.ibmcloud.com/vulnerabilities/264925>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-41746>
- <https://vuldb.com/fr/?id.238525>
- <https://security-advisory.acronis.com/advisories/SEC-5810>
- <https://security-advisory.acronis.com/updates/UPD-2303-79b2-e072>

GITLAB CVE-2023-5009

- <https://exchange.xforce.ibmcloud.com/vulnerabilities/266347>
- <https://nvd.nist.gov/vuln/detail/CVE-2023-5009>
- <https://www.cybersecurity-help.cz/vdb/SB2023092502>
- <https://theseckmaster.com/how-to-fix-cve-2023-5009-a-critical-vulnerability-in-gitlab-scan-execution-policies/>

AKIRA

- <https://www.hhs.gov/sites/default/files/akira-ransomware-sector-alert-ttpclear.pdf>
- <https://www.bleepingcomputer.com/news/security/meet-akira-a-new-ransomware-operation-targeting-the-enterprise/>
- <https://www.bleepingcomputer.com/news/security/linux-version-of-akira-ransomware-targets-vmware-esxi-servers/>
- <https://www.bleepingcomputer.com/news/security/akira-ransomware-targets-cisco-vpns-to-breach-organizations/>
- <https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication>
- <https://www.truesec.com/hub/blog/a-victim-of-akira-ransomware>
- <https://arcticwolf.com/resources/blog/conti-and-akira-chained-together/>
- <https://malpedia.caad.fkie.fraunhofer.de/details/win.akira>

Storm-0324 : le phishing via Microsoft Teams

- <https://www.microsoft.com/en-us/security/blog/2023/09/12/malware-distributor-storm-0324-facilitates-ransomware-access/>
- <https://www.bleepingcomputer.com/news/security/microsoft-notorious-fin7-hackers-return-in-clop-ransomware-attacks/>
- <https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#ELBRUS>
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715?ocid=magicti_ta_support