aDvens

Security for the greater good

Bulletin mensuel CTI

de Février

CERT aDvens
CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

SOMMAIRE

1. SYNTHÈSE

Ce mois-ci, le CERT aDvens vous propose un état des lieux des menaces émergentes et des vulnérabilités critiques à surveiller :

- trois vulnérabilités d'intérêt, dont deux exploitées,
- une présentation des campagnes du rançongiciel Termite, actif depuis avril 2024.

Autant de sujets essentiels pour anticiper les risques et renforcer votre posture de cybersécurité.

2. VULNÉRABILITÉS

2.1. SimpleHelp - CVE-2024-57727

Le 22 janvier 2025, les chercheurs en sécurité d'Arctic Wolf ont observé une campagne exploitant le logiciel SimpleHelp RMM comme vecteur d'accès initial. Cette attaque fait suite à la divulgation publique de plusieurs vulnérabilités dans SimpleHelp par Horizon3.

La CVE-2024-57727 est une vulnérabilité de traversée de répertoires qui permet à un attaquant non authentifié de télécharger des fichiers arbitraires depuis un serveur SimpleHelp vulnérable.

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	Aucun
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Aucun

2.1.4. Produits impactés

- SimpleHelp Server versions 5.5.x antérieures à 5.5.8
- SimpleHelp Server versions 5.4.x antérieures à 5.4.10
- SimpleHelp Server versions 5.3.x antérieures à 5.3.9

2.1.5. Recommandations

Mettre à jour SimpleHelp Server vers la version 5.5.8, 5.4.10, 5.3.9 ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin de SimpleHelp.

2.1.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.1.7. Indicateurs de Compromission

TLP	VALUE	COMMENT
TLP:CLEAR	385a826b9f7e72b870a92f1901d9d354	MD5
TLP:CLEAR	EC43ED845102760265ED6343EF1FCEF696588905	SHA-1
TLP:CLEAR	15f3e5b47894b953542d2fe2353786229da47af00c96dc1b41a8efe631364e49	SHA-256
TLP:CLEAR	d6828e30ab66774a91a96ae93be4ae4c	MD5
TLP:CLEAR	475c9302dc42b2751db9edcac3b74891	MD5
TLP:CLEAR	45.9.148[.]136	IP
TLP:CLEAR	45.9.149[.]112	IP
TLP:CLEAR	213.173.45[.]230	IP
TLP:CLEAR	194.76.227[.]171	IP

2.2. Trimble - CVE-2025-0994

Le 19 février 2025, Recorded Future a publié une analyse de la vulnérabilité CVE-2025-0994 affectant Trimble Cityworks, un logiciel de gestion d'actifs et de commandes de travail destiné aux administrations locales et aux services publics. Cette vulnérabilité de désérialisation permet à un attaquant authentifié d'exécuter du code à distance sur le serveur Microsoft Internet Information Services (IIS) ciblé.

L'exploitation de cette faille a été observée pour déployer des chargeurs personnalisés en Rust, capables de charger en mémoire des outils tels que VShell et Cobalt Strike.

2.2.1. Type de vulnérabilité

- CWE-502 : Deserialization of Untrusted Data

2.2.2. Risques

- Exécution de code arbitraire
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données
- Déni de service

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	Faible	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

2.2.4. Produits impactés

Trimble Cityworks versions antérieures à 15.8.9 Cityworks avec Office Companion versions antérieures à 23.10

2.2.5. Recommandations

Mettre à jour Trimble Cityworks vers la version 15.8.9 et Cityworks avec Office Companion vers la version 23.10.

Il est recommandé de vérifier et restreindre les permissions IIS.

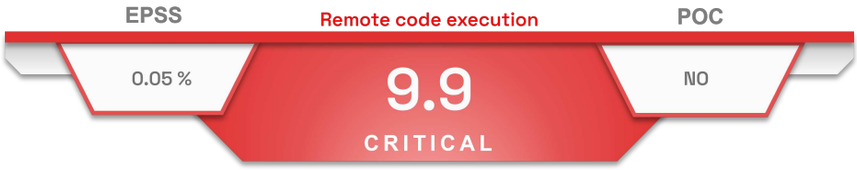
2.2.6. Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

2.2.7. Indicateurs de Compromission

TLP	VALUE	COMMENT
TLP:CLEAR	4b7561e27c87a1895446d7f2b83e2d9fcf71e6d6e8bc99d44818dc39a6ff99d5	SHA-256
TLP:CLEAR	4ffc33bdc8527a2e8cb87e49cdc16c3b1480dfc135e507d552f581a67d1850a9	SHA-256
TLP:CLEAR	8a6c735f3608719ec9f46d9c6c5fc196db8c97065957c218b98733a491edd899	SHA-256
TLP:CLEAR	883d849b94238c26c57c0595ccb95b8c356628887b9a3628bf56e726332af925	SHA-256
TLP:CLEAR	151a71c43e63db802d41d5d715aa98eb1b236e0a6441076a8d30fd93990416b4	SHA-256
TLP:CLEAR	1de72c03927bcd2810ce98205ff871ef1ebf4344fba187e126e50caa1e43250b	SHA-256
TLP:CLEAR	14a072113baa0a1e1e2b6044068c7bc972ae5e541a0aec06577b0d6663140079	SHA-256
TLP:CLEAR	04dc3a16e1e2b4924943805a1cea5e402c4f2304c717ea21fdf43274b8c34a84	SHA-256
TLP:CLEAR	f09b51b759dfe7de06fa724bd89592f5b8eae57053d5fb4891e40f24055103fb	SHA-256
TLP:CLEAR	C:\windows\temp\z1[.]exe	File path
TLP:CLEAR	C:\windows\temp\z2[.]exe	File path
TLP:CLEAR	C:\windows\temp\z44[.]exe	File path
TLP:CLEAR	C:\windows\temp\z55[.]exe	File path
TLP:CLEAR	C:\Windows\Temp\UDGEZR[.]exe	File path
TLP:CLEAR	C:\Windows\Temp\z55.exe_winpty\winpty-agent[.]exe	File path
TLP:CLEAR	C:\Windows\Temp\z55.exe_winpty\winpty[.]dll	File path
TLP:CLEAR	192.210.239[.]172:3219	IP:port
TLP:CLEAR	192.210.239[.]172:4219	IP:port
TLP:CLEAR	23.247.136[.]238	IP
TLP:CLEAR	31.59.70[.]13	IP
TLP:CLEAR	31.59.70[.]11	IP
TLP:CLEAR	149.112.117[.]49	IP
TLP:CLEAR	192.210.137[.]81	IP
TLP:CLEAR	192.210.183[.]118	IP
TLP:CLEAR	cdn.phototagx[.]com	Domain
TLP:CLEAR	ifode[.]xyz	Domain
TLP:CLEAR	https[:]//cdn.lgaircon[.]xyz[:]443/jquery-3.3.1.min.js	URI
TLP:CLEAR	https[:]//192.210.239[.]172/messages/73KWf-o0-s0hxVCDJp1sfAHRcgdm7	URI

2.3. Ivanti - CVE-2025-22467



Un défaut de contrôle de la mémoire dans Ivanti Connect Secure permet à un attaquant authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire.

2.3.1. Type de vulnérabilité

→ **CWE-121** : Stack-based Buffer Overflow

2.3.2. Risque

→ Exécution de code arbitraire

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

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

2.3.4. Produits impactés

Ivanti Connect Secure versions antérieures à 22.7R2.6

2.3.5. Recommandations

Mettre à jour Ivanti Connect Secure vers la version 22.7R2.6 ou ultérieure.

Des informations complémentaires sont disponibles dans le bulletin d'Ivanti.

2.3.6. Preuve de concept

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

3. TERMITE, LE NOUVEAU VENU

Le rançongiciel Termite apparaît comme l'un des derniers acteurs apparus sur l'échiquier de la menace cyber. Détecté fin 2024, il pourrait avoir été actif dès avril 2024. Le groupe utilise une variante du défunt rançongiciel Babuk disparu en 2021 à la suite d'une fuite interne au groupe. Certaines des caractéristiques de Termite, comme sa propension à s'attaquer à des cibles françaises ou francophones, son choix d'attaquer des structures de santé et sa volonté d'affichage de données personnelles et sensibles sur son site, méritent de s'y attarder.

3.1. Chronologie des attaques

Avril 2024 Début présumé de l'activité de Termite

Certaines analyses suggèrent que Termite pourrait être actif depuis le printemps 2024. Une des premières victimes potentielles, la branche française de Culligan, une entreprise de traitement et distribution d'eau, aurait été compromise autour de cette période, bien que la date exacte reste incertaine.

17 novembre 2024 : premières revendications de Termite

Termite entame sa première vague de montée en puissance et revendique cinq victimes sur son site vitrine (h**p://termiteuslbumdge2zmfmfcsrvmvsfe4gvyudc5j6cdnisnhtftvokid[.]onion).

Parmi elles, le Conseil scolaire Viamonde (Canada), l'association caritative Lebenshilfe Heinsberg (Allemagne), la compagnie pétrolière d'Oman ou encore Culligan sont mentionnés, suggérant que ces attaques ont eu lieu avant ou autour de cette période. Certaines de ces victimes ont été supprimées du portail depuis, laissant supposer le versement de rançons. Les premiers éléments techniques sont remontés : le groupe utilise un ransomware basé sur le code de Babuk.

Figure 1. Site vitrine - Termite

13 novembre 2024 : Département de La Réunion

Le Département de La Réunion confirme une cyberattaque, revendiquée par Termite le 20 novembre. L'attaque est contenue rapidement, mais entraîne une suspension temporaire des services numériques et des communications par e-mail. Une fuite de données est constatée, avec publication de données personnelles.

21 novembre 2024 : Attaque massive contre Blue Yonder

Termite revendique une attaque contre Blue Yonder, un éditeur de logiciels supply chain américain ayant notamment pour clients Starbucks, Morrisons, et Sainsbury's. Le groupe affirme avoir volé 680 Gb de données sensibles (e-mails, documents financiers, etc.). Coïncidence ou réellement proximité entre les deux groupes : le rançongiciel Cl0p a également ajouté Blue Yonder à la liste de ses victimes en janvier 2025 à l'issue de sa campagne d'exploitation des vulnérabilités CLEO.

30 novembre 2024 : Hôpital Communautaire de Watsonville (États-Unis)

Les employés doivent recourir à des dossiers papier, et l'incident dure près d'une semaine. 1er février 2025 : Attaque contre le CESI (France) Le CESI, un établissement éducatif français, est victime d'une cyberattaque revendiquée publiquement par Termite le 20 février 2025. L'incident nécessite une coupure d'accès à Internet et la mise en place d'une cellule de crise.

20 février 2025 : revendication de cyberattaque contre l'éditeur Ligentia (Royaume-Uni)

26 février 2025 : deuxième vague de montée en puissance

Termite revendique des cyberattaques contre la clinique de fertilité australienne Genea (en diffusant notamment des dossiers médicaux sensibles), l'entreprise Art & Co, les cabinet juridiques anglais RooksRider et National Legal Sevice, le cabinet londonien d'assureurs Belgravia Brokers et d'autres entreprises de la City telles que Heritage Venues, Nova Financial, et d'autres non revendiquées nommément.

L'analyse de l'évolution des attaques du groupe Termite permet de faire ressortir trois éléments essentiels :

- En premier lieu, il est aisé de s'apercevoir que le panel de victimes visées est extrêmement varié avec des entreprises privées (Culligan, Blue Yonder), des institutions publiques (Département de La Réunion), mais également des établissements éducatifs (CESI) ou des infrastructures de santé (Genea). Cette diversité suggère une stratégie de ciblage opportuniste plutôt qu'une spécialisation.
- Le deuxième aspect repose sur l'évolution par vague avec un rythme soutenu d'attaques, témoignant d'une forte ambition du groupe. Ces deux premiers points indiquent que le groupe semble être uniquement motivé financièrement et applique ces techniques dans le but d'obtenir des gains rapidement.
- Dernier point : le groupe ne s'est fixé aucune ligne rouge en termes de conduite pour parvenir à ses fins : des hôpitaux, cliniques et associations caritatives sont attaqués et des données sensibles de patients ou bénéficiaires sont diffusées comme preuves.

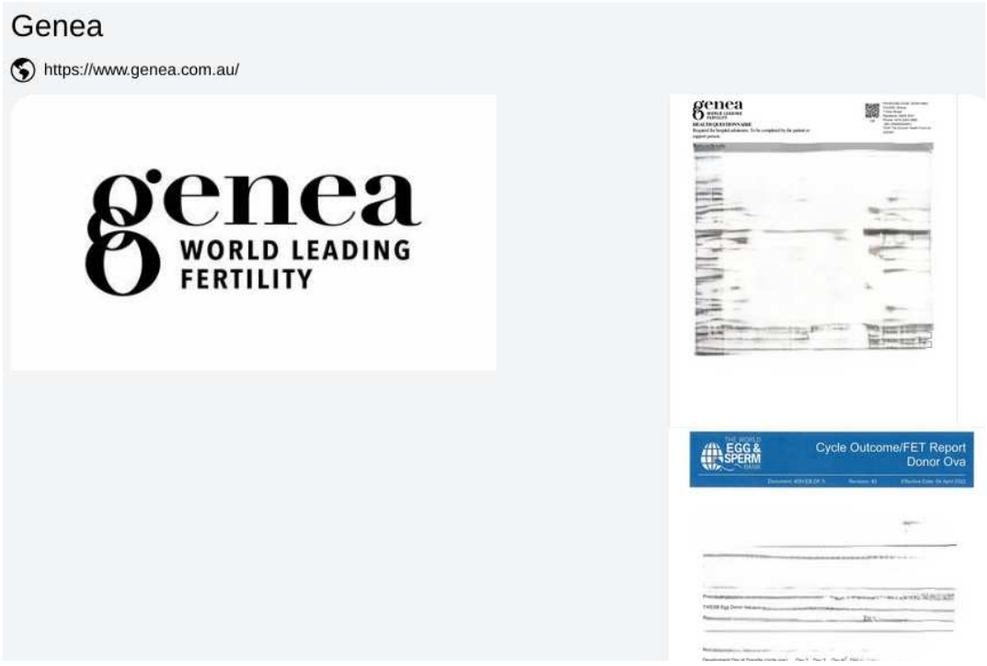


Figure 2. Revendication cyberattaque clinique de la fertilité Genea - Termite n'hésite pas à mettre en avant des données médicales sensibles

3.2. TTPs

Le cycle d'attaque de Termite se décompose en plusieurs étapes, chacune exploitant des techniques spécifiques :

1. **Accès Initial**

Les acteurs utilisent des techniques classiques (phishing ou utilisation de données de connexion dérobées) pour obtenir un accès initial. Dans certains cas, l'exploitation de vulnérabilités dans des solutions tierces est observée, comme l'exploitation de CLEO (*CVE-2024-50623*).

1. **Escalade de Privilèges**

Une fois l'accès obtenu par phishing ou exploitation de vulnérabilité, le malware énumère et arrête des services et processus liés à la sauvegarde ou des bases de données comme *sql.exe*, *oracle.exe*, etc. afin d'éviter toute interférence avec son chiffrement.

1. **Désactivation des Mécanismes de Récupération**

Le rançongiciel lance des commandes (via *vssadmin.exe* et *SHEmptyRecycleBinA*) pour supprimer les copies système et vider la corbeille, empêchant ainsi la restauration du système.

1. **Chiffrement des Données et Déploiement de la Note de Rançon**

Le variant de Babuk chiffre les fichiers de l'utilisateur, en excluant certains dossiers et extensions critiques afin de maintenir un minimum de fonctionnalité système. Il ajoute l'extension « .termite » aux fichiers chiffrés et dépose une note de rançon (nommée « *How To Restore Your Files.txt* ») qui dirige la victime vers un site .onion pour obtenir des instructions.

> **Marqueur de chiffrement** : L'ajout de la signature textuelle « *choung dong looks like hot dog* » à la fin des fichiers chiffrés constitue un identifiant unique de l'attaque. Il s'agit d'une fonctionnalité typique du rançongiciel Babuk.

1. **Double Extorsion et Exfiltration de Données**

En plus du chiffrement, Termite opère une double extorsion en menaçant de publier ou de vendre les données exfiltrées, comme les 680 Gb suite à l'attaque contre Blue Yonder.

1. **Propagation latérale**

Le rançongiciel utilise des API système, notamment *NetShareEnum()* et *GetDriveTypeW()*, afin de détecter et attaquer les partages réseau, facilitant ainsi sa propagation vers d'autres machines présentes dans celui-ci.

3.3. Vulnérabilités exploitées

Parmi les vulnérabilités exploitées par Termite, une en particulier est régulièrement mentionnée dans le cadre d'attaques ciblant des solutions tierces :

3.3.1. CVE-2024-50623

À l'instar de Cl0p, il apparaît que Termite a exploité la faille CLEO (*CVE-2024-50623*), une vulnérabilité d'exécution de code à distance affectant certaines versions des produits CLEO (LexiCom, VLTrader et Harmony, avant la version 5.8.0.21).

D'autres vecteurs (comme des campagnes de phishing ou l'exploitation d'autres vulnérabilités non spécifiées) pourraient également être utilisés pour faciliter l'accès initial.

3.4. Recommandations

- Mise à jour en continu des systèmes et applications.
- Renforcement des mesures de sécurité portant sur les partages réseau et les systèmes de sauvegarde.
- Formation des utilisateurs aux campagnes de phishing et est adoption des politiques de sécurité générale robustes (segmentation, surveillance, etc.).

3.5. Conclusion

Termite se positionne comme une menace montante dans le paysage des rançongiciels avec une intensification de ses opérations entre novembre et décembre 2024. En s'appuyant sur une variante du Babuk, le groupe exploite des techniques classiques (arrêt de services, suppression de sauvegardes locales) tout en intégrant des méthodes de double extorsion, ce qui accroît la pression sur les victimes.

La deuxième vague d'attaque de février 2025 illustre bien la montée en puissance de ce groupe qui sera l'un des acteurs à surveiller au long de cette année 2025.

3.6. Matrice Mitre ATT&CK

INITIAL ACCESS

T1566 Phishing. T1659 Content Injection. T1195.001 Supply Chain Compromise: Compromise Software Dependencies and Development Tools.

EXECUTION

T1204.002 User Execution.

PRIVILEGE ESCALATION

T1078 Valid Accounts.

DEFENSE EVASION

T1070.004 Indicator Removal: File Deletion.

DISCOVERY

T1083 File and Directory Discovery. T1135 Network Share Discovery.

LATERAL MOVEMENT

T1021 Remote Services.

COMMAND AND CONTROL

T1105 Ingress Tool Transfer.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

IMPACT

T1486 Data Encrypted for Impact. T1490 Inhibit System Recovery.

3.7. IOC

3.7.1. Indicateurs Termite

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	SHA256	f0ec54b9dc2e64c214e92b521933cee172283ff5c942cf84fae4ec5b03abab55	Variant BABUK
TLP:CLEAR	SHA256	30a8cf3e6863030c762b468bf48d679f3dd053a80793770443938fa18de89617	Variant BABUK
TLP:CLEAR	Text	choung dong looks like hot dog	Signature
TLP:CLEAR	IP	176.123.5.126	CLEO exploitation
TLP:CLEAR	IP	5.149.249.226	CLEO exploitation
TLP:CLEAR	IP	185.181.230.103	CLEO exploitation
TLP:CLEAR	IP	209.127.12.38	CLEO exploitation
TLP:CLEAR	IP	181.214.147.164	CLEO exploitation

4. RÉFÉRENCES

Termite, le nouveau venu

- Portail de revendications - Termite h**p://termiteuslbumdge2zmfmfcsrvmvsfe4gvyudc5j6cdnisnhtftvokid[.]onion/
- Echantillons Termite - Malware Bazaar https://bazaar.abuse.ch/browse/tag/Termite/
- Communiqué de presse cyberattaque BlueYonder https://blueyonder.com/customer-update
- Dark Web Profile: Termite Ransomware https://socradar.io/dark-web-profile-termite-ransomware/
- Echantillon Termite https://bazaar.abuse.ch/browse/tag/Termite/
- Inventaire attaques Termite https://www.ransomlook.io/group/termite
- Ransomware : que sait-on de Termite, qui a attaqué le département de la Réunion ? https://www.lemagit.fr/actualites/366616976/Ransomware-que-sait-on-de-Termite-qui-a-attaque-le-departement-de-la-Reunion
- Threat Advisory: Oh No Cleo! Cleo Software Actively Being Exploited in the Wild https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild
- A tecnical look at Termite ransomware https://cyble.com/blog/technical-look-at-termite-ransomware-blue-yonder/