Palo Alto Networks

Survol du rapport de réponse aux incidents Unit 42 - 2022

Unit 42

- Fondée en 2014, l'équipe de l'Unité 42 s'est rapidement imposée comme une organisation de renseignement sur les menaces (threat intelligence) de premier plan en apportant ses recherches et ses analyses au public.
- Le 42 de notre nom est un clin d'œil au « The Hitchhiker's Guide to the Galaxy » de Douglas Adams. Même si le nombre ne fournit pas les réponses à tous les questionnements sur les cybermenaces, c'est le travail de l'unité 42 de faire son mieux pour y répondre.
- Le volet de réponse aux incidents de sécurité a été renforcé par l'acquisition de Crypsis en 2021 (ajout de 140 experts en sécurité)
- Analyse de 500 milliards d'événements par jour avec plus de 85k clients

L'entreprise de réponse aux incidents préférée pour

70+

compagnies de cyber assurance

Expertise avancés avec

160+

Experts en réponse aux incidents

Notre équipe de réponse aux incidents répond à

1,300+

attaques par année

UNIT 42™

BY PALO ALTO NETWORKS

200+

chercheurs en cybermenaces

Réponse de classe mondiale aux violations de données avec

2,500+

clients mondialement

150+

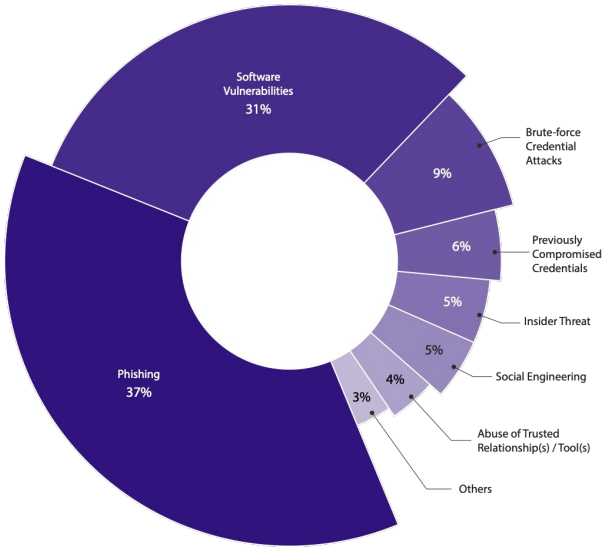
cabinets d'avocats internationaux appellent Unit 42 lorsque leurs clients soupçonnent qu'ils sont victimes d'un cybercrime

2022 Unit 42 Incident Response Report

- **Analyse de plus de 600 cas de réponse aux incidents de sécurité**
- **7 problèmes** qui ont contribués au succès
- **3 vecteurs d'attaque** principaux
- **6 catégories de CVE** les plus exploitées
- **6 recommandations** pour se préparer de manière proactive aux menaces futures
- **5 prévisions futures**

7 enjeux de sécurité les plus rencontrés

7 problèmes que les acteurs malveillants ne veulent pas qu'on règle



70%

Phishing and Software Vulnerabilities cause majority of Cyber Incidents

1 Multifactor authentication

In 50% of cases, organizations lacked multifactor authentication on key internet-facing systems such as corporate webmail, virtual private network (VPN) solutions and other remote access solutions.

2 EDR/XDR

In 44% of cases, organizations did not have an endpoint detection and response (EDR) or extended detection and response (XDR) security solution or it was not fully deployed on the initially impacted systems to detect and respond to malicious activities.

3 Patch management

In 28% of cases, having poor patch management procedures contributed to threat actor success. This refers to any time a non-zero-day vulnerability was exploited by a threat actor in any way and includes situations in which an exploit helped a threat actor at some point after initial access. It does not include cases when threat actors exploited a zero-day vulnerability to gain access.

4 Mitigations for brute-force attacks

In 13% of cases, organizations had no mitigations in place to ensure account lockout for brute-force credential attacks.

5 Security alerts

In 11% of cases, organizations failed to review/action security alerts.

6 Password security

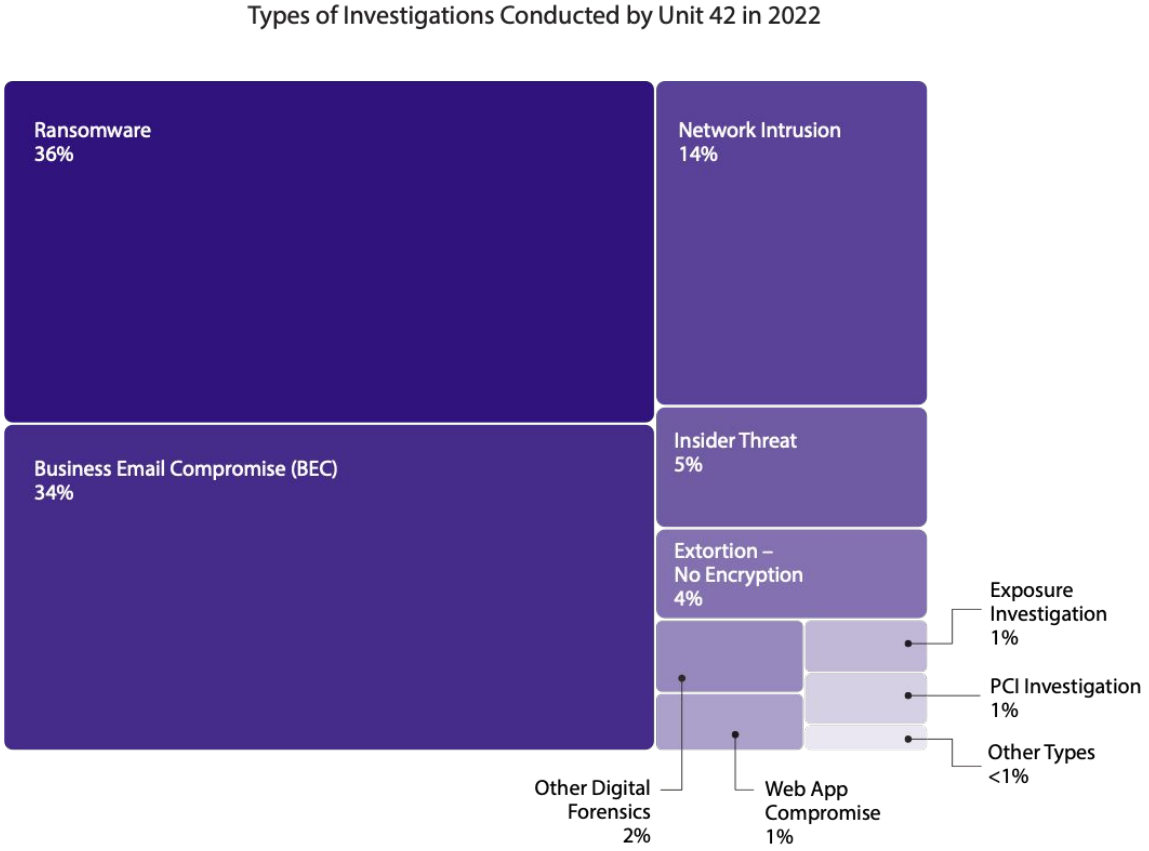
In 7% of cases, weak password security practices contributed to threat actors' ability to further their objectives (e.g., default password, blank or empty password, easily guessed or brute-forced password).

7 Misconfigurations

In 7% of cases, system misconfiguration was a contributing factor to the incident.

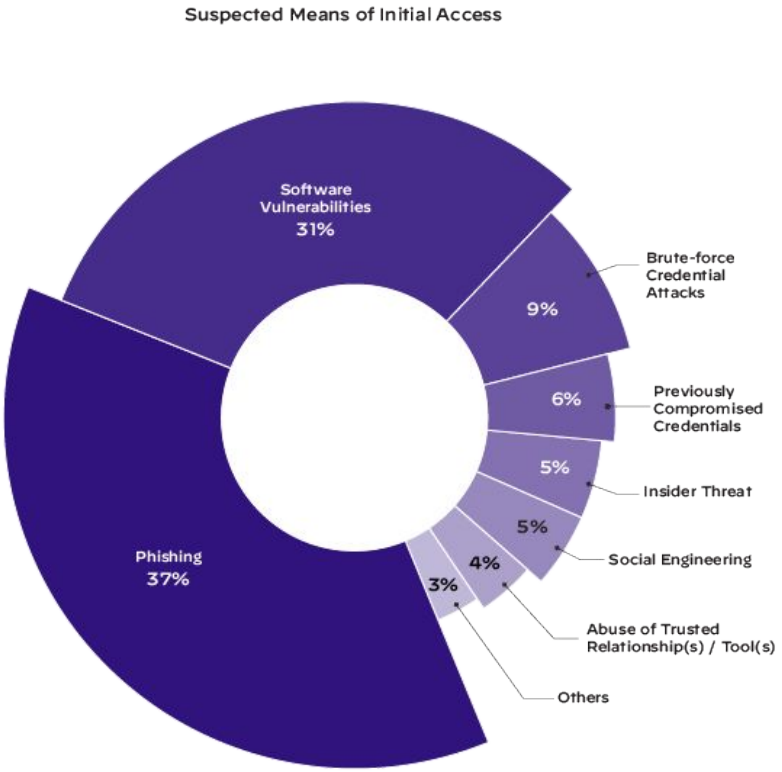
Principaux points à retenir : types d'incidents

Les rançongiciels & les compromissions via email corporatifs représentent **70%** des cas traités par Unit 42.



Principaux points à retenir : vecteurs d'attaque

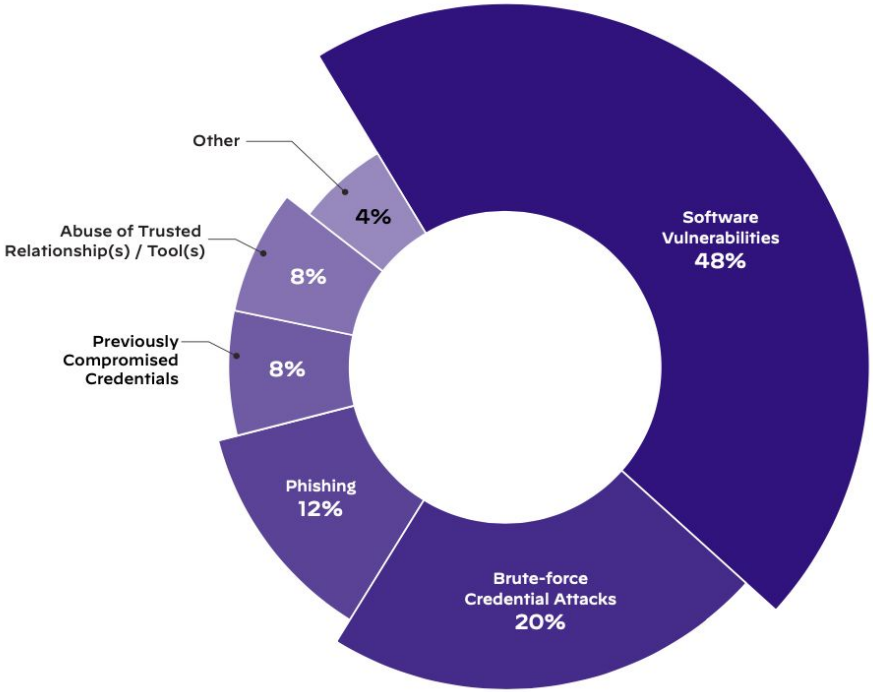
Les attaquants cherchent un moyen facile d'entrer.



3 vecteurs d'attaque représentent **77%** des vecteurs d'accès initiaux suspectés pour les incidents.

Principaux points à retenir : vecteurs d'attaque des rançongiciels

Techniques automatisées en grande majorité



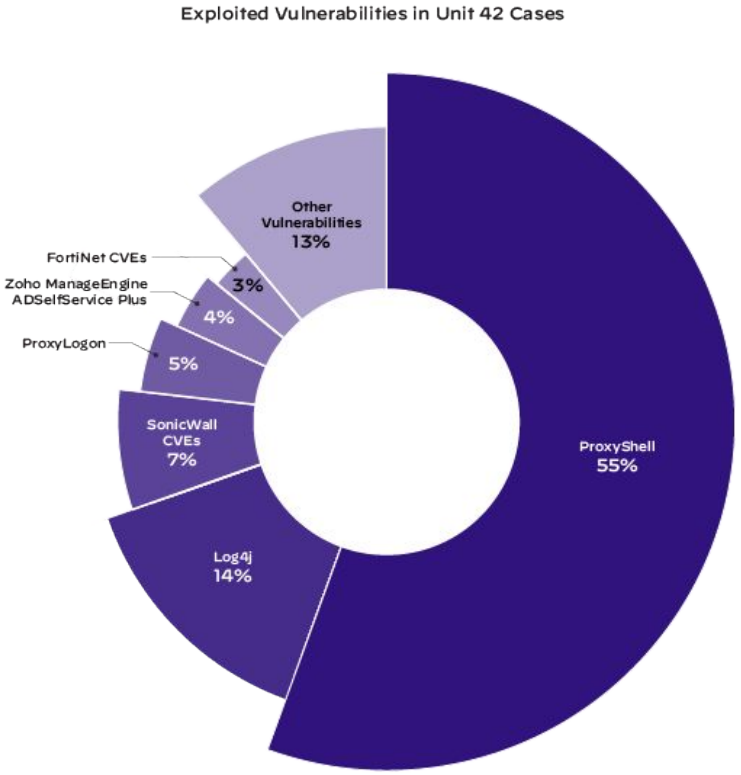
68% des incidents de rançongiciels ont été initiés avec soit ***des exploitations de vulnérabilités logicielles ou*** **des attaques par "bruteforce" de mots de passe**. Le "Ransomware-as-a-Service (Raas)" & les "exploit toolkits" rendent le travail très facile pour les pirates.

Remote Desktop Protocol (RDP) majoritairement exploité par les attaques à base d'informations d'authentification.

28 jours temps de séjour médian après l'accès initial

Principaux points à retenir : vulnérabilités exploitées

Quelques vulnérabilités clés sont devenues les préférées des attaquants.



6 catégories de CVE représentent **87 %** des vulnérabilités exploitées.

- *ProxyShell*
- *Log4j*
- *SonicWall*
- *ProxyLogon*
- *Zoho ManageEngine*
- *Fortinet*

6 points clés pour protéger votre organisation

1. Organiser des formations sur la prévention du phishing et la sécurité récurrente des employés et des sous-traitants.
2. Désactivez tout accès RDP externe direct à l'environnement.
3. Corrigez les systèmes exposés à Internet aussi rapidement que possible.
4. Implémentez l’authentification MFA avec des politiques de contrôle et de sécurité pour tous les utilisateurs.
5. Exigez que toutes les vérifications de paiement aient lieu en dehors des courriels.
6. Envisagez un service de détection des informations d'identification et des violations et/ou une gestion de la surface d'attaque.

5 prédictions futures

Où vont les acteurs malicieux dans l'avenir

Prédiction #1 : La fenêtre d'application des correctifs continuera de diminuer

Les attaquants utilisent de plus en plus les "Zero Day" très médiatisés, du genre dont vous entendez parler dans les actualités.

Le rapport 2022 sur gestion des menaces a révélé que les attaquants commencent à scanner les vulnérabilités à peine **15 minutes** après l'annonce d'un CVE.

Prédiction #2 : Les acteurs malicieux non qualifiés sont en augmentation

Même les acteurs malicieux qui semblent maîtriser les bases commencent à recourir à des versions plus simples d'attaques et à utiliser des "toolkits".

Même des attaquants non qualifiés pourraient causer des dommages à votre organisation s'ils sont capables de pénétrer dans vos systèmes.

Prédiction #3 : Les modifications apportées à la cryptomonnaie pourraient entraîner une augmentation des compromissions via courriels et Web

Une chose qui contribue actuellement à la nature lucrative des rançongiciels est la prévalence et l'anonymat relatif de la crypto-monnaie.

Les changements dans la disponibilité ou la stabilité de la crypto compromettent son utilité et peuvent inciter les acteurs malicieux à revenir aux méthodes classiques basées sur la monnaie.

Prédiction #4: Le climat économique difficile pourrait inciter davantage de personnes à tirer parti de la cybercriminalité

Si les conditions économiques mondiales se détériorent, davantage de personnes pourraient être incitées à s'essayer à la cybercriminalité.

Certains groupes sont connus pour proposer de l'argent à des employés qui sont prêts à remettre des informations d'identification ou à les aider à pénétrer dans leur entreprise.

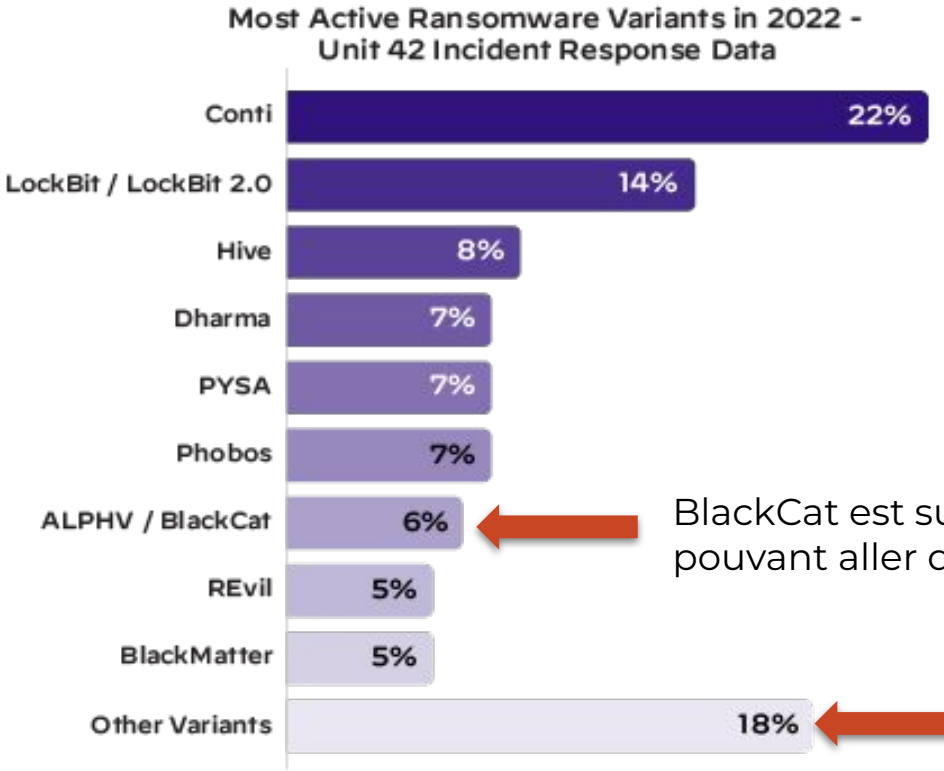
Prédiction #5: Les incidents à motivation politique peuvent augmenter

Alors que les questions politiques brûlantes s'intensifient dans le monde entier, nous pensons qu'il pourrait y avoir une augmentation du hacktivisme et de la cybercriminalité à motivation politique.

Les acteurs malicieux peuvent travailler avec des pays ou être payés par des groupes à motivation politique.

Groupes de rançongiciels les plus actifs

Unit 42 suit activement plus de 56 groupes qui opèrent des RaaS



A fermé boutique depuis le scandale Conti Leaks où leur chats interne ont fuitées (avril 2022)

BlackCat est suivi de près - ils offrent des commissions pouvant aller de 80 à 90 %

De nouveaux groupes continuent d'apparaître alors que les anciens groupes se dissoudent