



B R E A C H H U N T

WWW.BREACHHUNT.FR



12/12/2023

Présentation sur les stealers



B R E A C H U N T

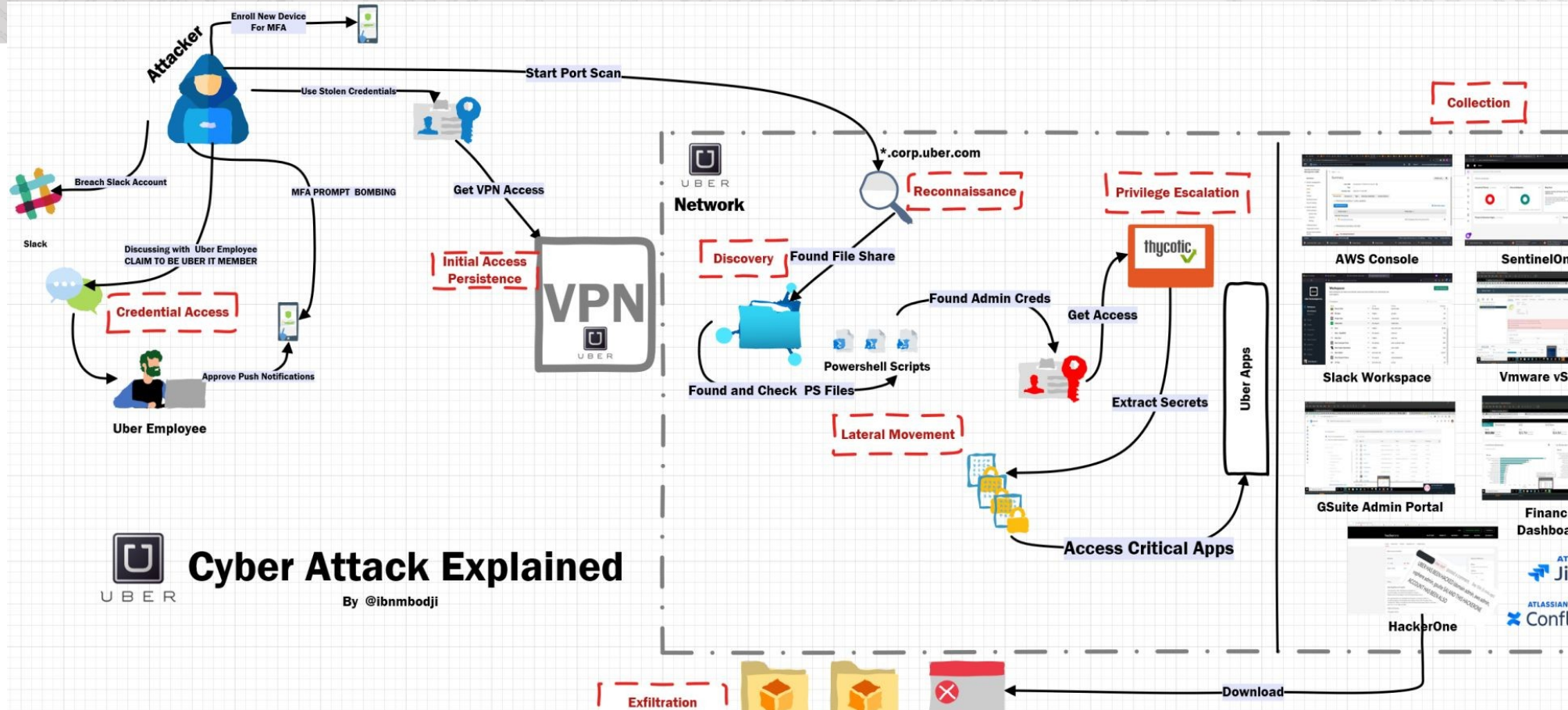
SOMMAIRE

- 1) Les stealers - présentation générale
 - A. Terminologie du milieu
 - B. Organisation
 - C. Quelques chiffres
 - D. Prévention
- 2) Analyses
 - E. Géopolitique
 - F. Technique
 - G. Sociologique
 - H. Juridiques
- 3) Le quotidien d'un analyste en CTI avec les stealers
 - I. Collecte
 - J. Analyse
 - K. Analyse juridique

C'est la ruée vers l'or, vendez des pelles

Dans les années 1800, des milliers d'Américains cherchaient de l'or en Californie. Mais les plus riches, ce n'étaient pas ceux qui en trouvaient...

Un des exemples les plus connus



Les stealers - présentation générale

Terminologie du milieu



- Les fabricants de malware revendent leurs outils (one shot ou abonnement)
- Les **clouds** les rachètent, les utilisent récupèrent et revendent les **logs**
- Ils diffusent le malware sur Windows et Mac via logiciels crackés, usurpations, fausses pubs...
- Une fois infectée les personnes ne s'en aperçoivent pas et voient leurs données collectées



Les stealers - présentation générale

Organisation



- Système économique: le MAAS: Malware As A Service
- Ce qui est récolté:
 - Passwords, cookies, formulaire et historique de tous les navigateurs (Opera jusqu' à tor browser...)
 - Crediens FTP, token Discord ou Telegram
 - Wallet Crypto
 - Liste de logiciels/processus, IP et config de la machine
 - Fichier au nom « juicy » (pdf, docx...)
 - Récemment : preuve de la collecte des accès à des coffres forts de mot de passe

URL: <https://login.live.com/login.srf>

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Chrome

URL: android://5bsD4dPjQoH_eiC4fHpfc5zPzS4K28mk3hwZF2_lSHrxe72isJVMgvV7hhs47EuFZrZfYX9iXchD4zc6GZ3

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Chrome

URL: <https://www.veepee.fr/authentication/login/fr>

USER: [REDACTED]

PASS: [REDACTED]

SOFT: Opera GX Stable

URL: <https://www.sfr.fr/cas/login>

USER: [REDACTED]

PASS: [REDACTED]

Les stealers - présentation générale

Des chiffres



BREACH

- 500 victimes = 300mo de données
- 80% des cyberattaques débutent par un infostealer (source: RecordedFuture)

Business model des attaquants (données moyennes)

- } Un log = 10 \$
- } Abonnement mensuel : 100-300\$
- } Abonnement à vie : 800 à 3000++\$
- } Filtres par pays, par site
- } Prix d'un VPN : 30-200\$ selon le sujet

Hi Redline team!

I wanted to know if you sell a log access panel? Or just the stealer tool?

21:21:06 ✓

Hi

We're sell only the software 21:25:51

<https://forum.blacknet.su/threads/10109/>

<https://www-club.vip/index.php?threads/redline-stealer.167323/>

<https://skynetzone.org/threads/redline-stealer.19097/>

<https://opencard.us/index.php?threads/redline-stealer.9259/>

<https://dublikat.eu/threads/redline-stealer.156243/>

<https://bhf.im/threads/587850/>

<https://center-club.us/index.php?threads/redline-stealer.84786/>

<https://dark2web.net/threads/114207/>

<https://btt-club.top/threads/redline-stealer.5164/>

21:25:51

The current price for the stealer:

• 1 month of stealer subscription + as a gift 1 month of crypto subscription = \$150 per month

PRO version (forever) 900\$ + 3 months subscription to scanner + @spectrcript_bot cryptor

Updates are free

Pay using the @redlinemarket_bot

Des chiffres



- Source : Recorded Future
- Quelques sources plus discrètes sur twitter qui semblent confirmer cet ordre de grandeur

18,895,360

COMPROMISED MACHINES

- Difficile car utilisation de scénario d'ingénierie sociale ou actions réalisées par l'humain pour l'infection
- La diffusion reste encore assez nébuleuse
- Sensibilisation des utilisateurs constante
- Interdire la sauvegarde des credentials dans le navigateur et l'export/import de session
- Monitorer les fuites de mot de passes (banlist de mdp, reset des utilisateurs compromis, réponse à incident parfois nécessaire)
- MFA everywhere (et encore...) !

- Pays touchés principalement
 - › Par ordre : Inde, Brésil, Indonésie, Pakistan, Turquie, Egypte, Vietnam, Mexique, Philippines, Thaïlande
 - › l'usage de logiciel cracké est davantage de mise dans ces pays
 - › **Mais fort impact sur la supplychain (et oui...la mondialisation...)**
- Provenance :
 - › pays russophones
- Les malwares ne s'exécutent souvent pas sur les claviers en cyrillique (pas d'infection sur RU, MN, BY etc....)
 - › Exemple : **Meduzza**

Exclusion List

The table below outlines the country codes and corresponding names from the exclusion list.

Country name	Country code
Russia	RU
Kazakhstan	KZ
Belarus	BY
Georgia	GE
Turkmenistan	TM
Uzbekistan	UZ
Armenia	AM
Kyrgyzstan	KG
Moldova	MD
Tajikistan	TJ

Exemple :

#1 – Redline – un système d'attaque complexe (source : alienvault.com)

ATT&CK IDS:

T1003 - OS Credential Dumping, T1036 - Masquerading, T1102 - Web Service, T1105 - Ingress Tool Transfer, T1119 - Automated Collection, T1137 - Office Application Startup, T1140 - Deobfuscate/Decode Files or Information, T1218 - Signed Binary Proxy Execution, T1566 - Phishing, T1059 - Command and Scripting Interpreter, T1204.002 - Malicious File, T1059.001 - PowerShell, T1204 - User Execution, T1059.003 - Windows Command Shell, T1047 - Windows Management Instrumentation, T1547 - Boot or Logon Autostart Execution, T1060 - Registry Run Keys / Startup Folder, T1055 - Process Injection, T1562.001 - Disable or Modify Tools, T1130 - Install Root Certificate, T1112 - Modify Registry, T1170 - Mshta, T1027 - Obfuscated Files or Information, T1055 - Process Injection, T1085 - Rundll32, T1553 - Subvert Trust Controls, T1497.003 - Time Based Evasion, T1497 - Virtualization/Sandbox Evasion, T1555 - Credentials from Password Stores, T1503 - Credentials from Web Browsers, T1081 - Credentials in Files, T1003 - OS Credential Dumping, T1539 - Steal Web Session Cookie, T1552 - Unsecured Credentials, T1087 - Account Discovery, T1217 - Browser Bookmark Discovery, T1083 - File and Directory Discovery, T1120 - Peripheral Device Discovery, T1057 - Process Discovery, T1012 - Query Registry, T1518 - Software Discovery, T1082 - System Information Discovery, T1016 - System Network Configuration Discovery, T1033 - System Owner/User Discovery, T1007 - System Service Discovery, T1124 - System Time Discovery, T1497.003 - Time Based Evasion, T1497 - Virtualization/Sandbox Evasion, T1560 - Archive Collected Data, T1119 - Automated Collection, T1005 - Data from Local System, T1114.001 - Local Email Collection, T1008 - Fallback Channels, T1095 - Non-Application Layer Protocol, T1571 - Non-Standard Port, T1102 - Web Service, T1048 - Exfiltration Over Alternative Protocol, T1041 - Exfiltration Over C2 Channel, T1011 - Exfiltration Over Other Network Medium, T1489 - Service Stop

Exemple :

#2 – Stealc – Offuscation et non persistence (source : sekoia.io)

```
cmd.exe /c timeout /t 5 & del /f /q "$STEALERPATH" & del  
"C:\ProgramData\*.dll" & exit
```

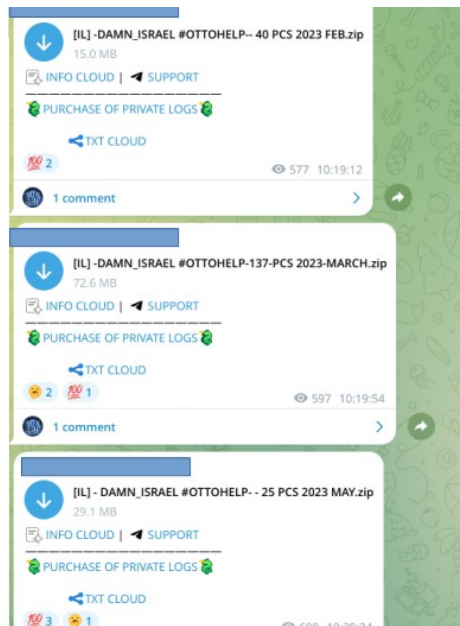

- Phishing, Exploits Kits, Sextorsion, vidéos youtube usurpées
- Usurpation de sites légitimes d'outils populaires (anydesk, fausses MAJ calendrier...)
- Diffusion via des logiciels contrefaits (Beware : alternativesto)

Analyse sociologique

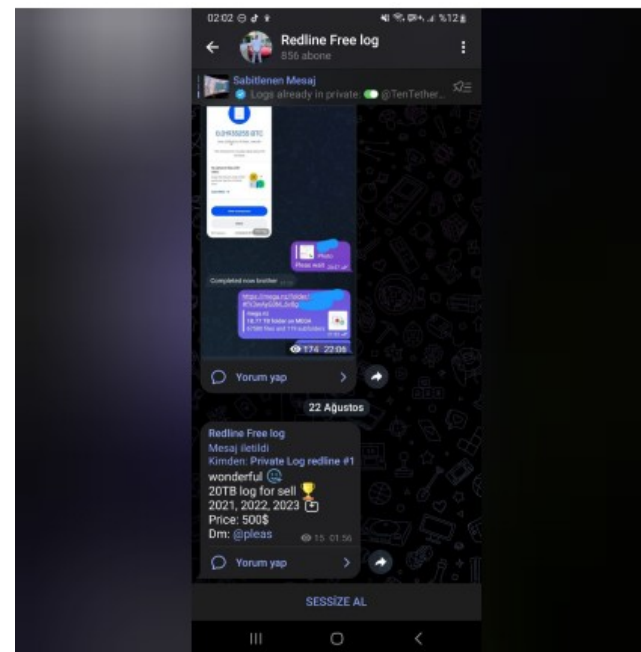
Exemples



- Réaction à la guerre en Israel



- Dénonciation des « clouds scams »



he is scammer dont buy the private logs public former 🤔

- Guerre inter-cloud

the son of a bitch got mad because his logs were leaked and I can tell you this about that, these sons of bitches don't know where I live and they don't know that there are different hours in different cities around the world, if you look at his explanation you will know that he has no proof, he is talking about followers, he is talking about blocking. but he can't find any proof, you stupid son of a bitch, the time is different in Russia, the time is different in America, the time is different in Turkey, the time is different in Turkey, I share the posts with direct redirection, that is, the script coded in the account is shared as the post is uploaded, the reason for the time difference is that I live in another country, he cries because he can't find any proof in any way.

don't take any action from this guy he is spamming everyone for logs this is my last statement on this subject I will not talk about this son of a bitch anymore as you know he is crying because he was leaked

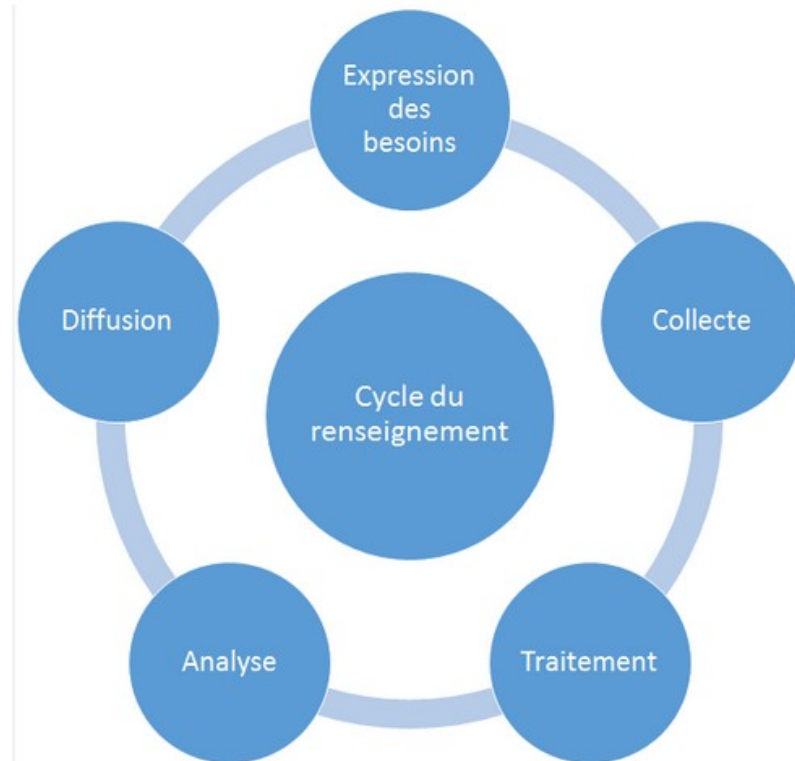
Thank you for your commercials, you stupid brat.

Quotidien d'un analyste en CTI

Collecte



- Veilles multiples
 - } Veille manuelle
 - } Veille automatique
 - } Interactions humaines (Humint)
- Chaque source à son avantage et ses inconvénient



Collecte Telegram



- On estime de 50 à 70 clouds
- Production de dizaines de Go de logs par jours
- Ecosystème sociologique: guerre, partenariat, dénonciation/doxxing et réaction aux événements géo-politiques

GODELESS CLOUD

PRIVATE CLOUD LOGS

★ OUR ADVANTAGES ★

- We use the Google Ads traffic source .
- In our logs you will find BA, COLD WALLETS, GAME ACC.
- We don't touch the LOGS before uploading to the private channel
- We can guarantee the quality of our logs.

⚡ PRICE LIST ⚡

- 💰 100\$ - WEEK
- 💰 230\$ - MONTH
- 💰 1500\$ - LIFETIME

💰 Payment methods 💰

- BTC
- LTC
- BNB
- Smart Chain
- USDT (TRC20)
- BTC Banker Check

1. Buy by BOT - @godeless_sell_bot 🤖 (early access)

2. Buy by Admin - @daeftt 🧑

👁 1092 05:24:58

🗨 Leave a comment

Hologram Cloud
The best store in the market that cares about its customers

⚙️ <1000
Minimum 1000 new log's per day

🎯 Mix target
BR, AR, EU, USA, and others...

🔍 Stealer
Redline

Price list

1 month	2 months	3 months	LifeTime
100\$	170\$	250\$	800\$

Payment method

Any crypto

Hologram Support
Online

Username:
@Holograma_Support

About:
We are a team of experts in the field of cyber security and we are looking for people who want to join our team.

👤 PRIVATE CLOUD LOGS 👤
🔍 every day minimum 1.000 logs
🌐 BR, AR, EU, USA, CA, MIX Targeted
📁 Work logs
🔄 Every day new fresh logs
🔍 Stealer RedLine

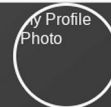
👤 PRICE LIST 👤

- 👤 Hologram Cloud 2 weeks - 70\$
- 👤 Hologram Cloud 1 month - 100\$
- 👤 Hologram Cloud 2 months - 170\$
- 👤 Hologram Cloud 3 months - 250\$
- 👤 Hologram Cloud Lifetime - 800\$

★ Payment methods

💎 Any crypt, BTC, ETH, USDT, LTC,
🔍 FREE CLOUD <https://t.me/hologramcloud>
📞 TELEGRAM @Holograma_support
💬 CHAT https://t.me/hologram_chat

- Présence active sur les forums notamment à accès restreint
- Possibilité d'interagir et de suivre les échanges
- Informations de première main



Br0k3r

Selling access to Corporate/Enterprise networks around the world! 🌐

⚠️ Daily update!

Last update: July 01, 2023 📅

Available networks: 36 ✓

Sold networks: 12 ✖️

Total networks: 48 / ∞

These networks always provided with full domain control privilege.
Including Domain Admin credentials, All AD users creds/hashes, DNS zones
and objects, Domain trusts... and all other information that may useful for easily
network takeover!

You only should plant your beacon/backdoor and start working.

Different countries, Different revenue, Different categories, Different scale and
Different price!

The base price is 0.5 💰 and can be changed depending on the network.

🔒 Deal rule: Once you have made your choice, send the desired code, you
will receive general information such as internet domain, zoom information and
network price. If approved, you will need to share your wallet with enough
balance and then we will go to the test phase to prove the existence of the
network and you can check the domain admin privilege, access level, network
scale, AV/EDR used and other things that may be important to you. Check it out
and finally go to pay and make a successful deal! 🤝

Collecte

Sources humaines



- Contact et échanges avec des acteurs du milieu Dark Web
- Tuyaux et analyse tendances
- Usage ponctuel selon situation
- Les contacts ont des avatars leur offrant des accès et contacts privilégiés



- Traitement automatisé des données bruts pour faire le tri
- Analyse manuelle / vérifications
 - } fausses informations ?
 - } faux positifs ?
 - } Anciennes données ?
 - } Capitalisation des résultats
- Exemple : **russian market**



- Problèmes identifiés : comment protège-t-on le client avec des données issues d'actions criminelles ainsi que les droits des détenteurs des données persos ?





B R E A C H H U N T

WWW.BREACHUNT.FR

Questions ?