BREACHUNT

WWW.BREACHUNT.FR

OSSIR

12/12/2023

Présentation sur les stealers

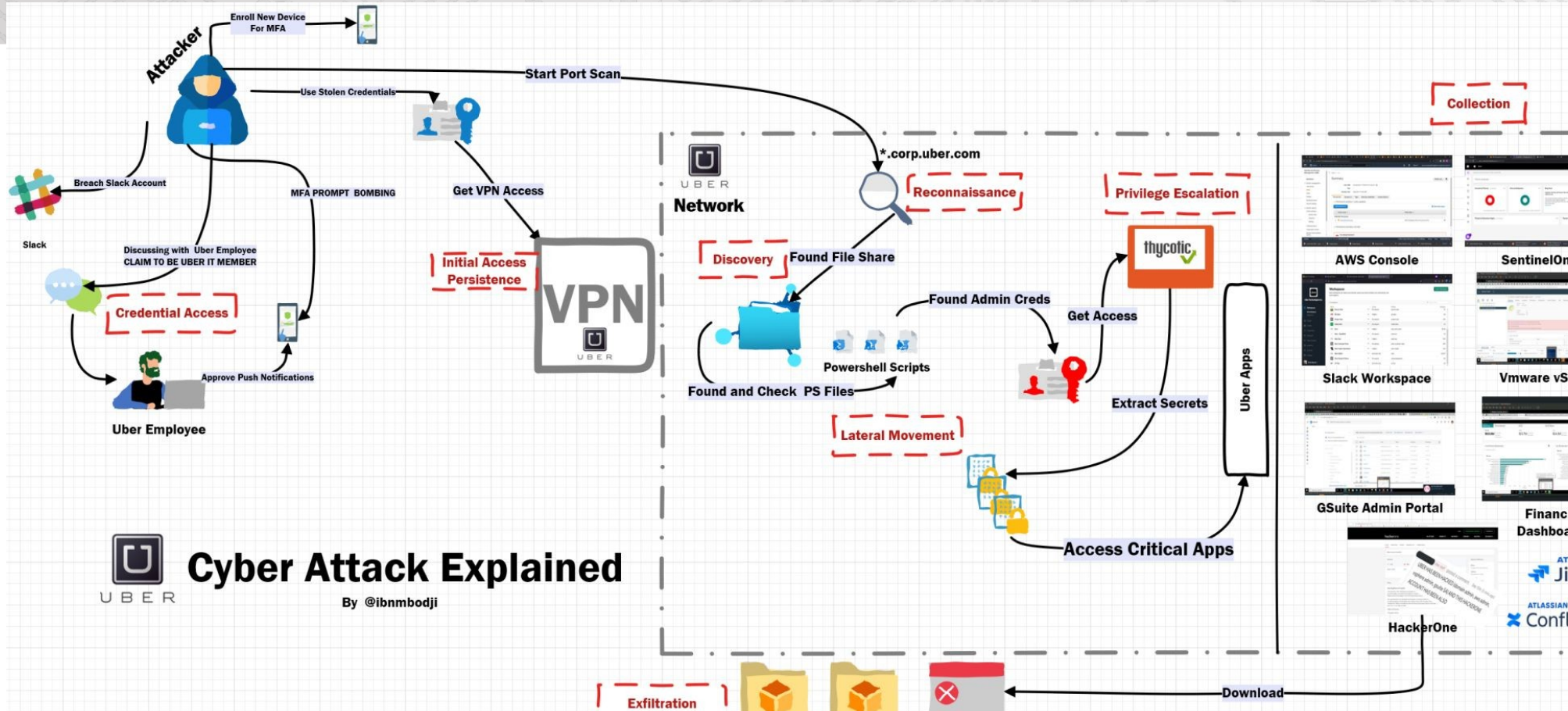
BREACHUNT

SOMMAIRE

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

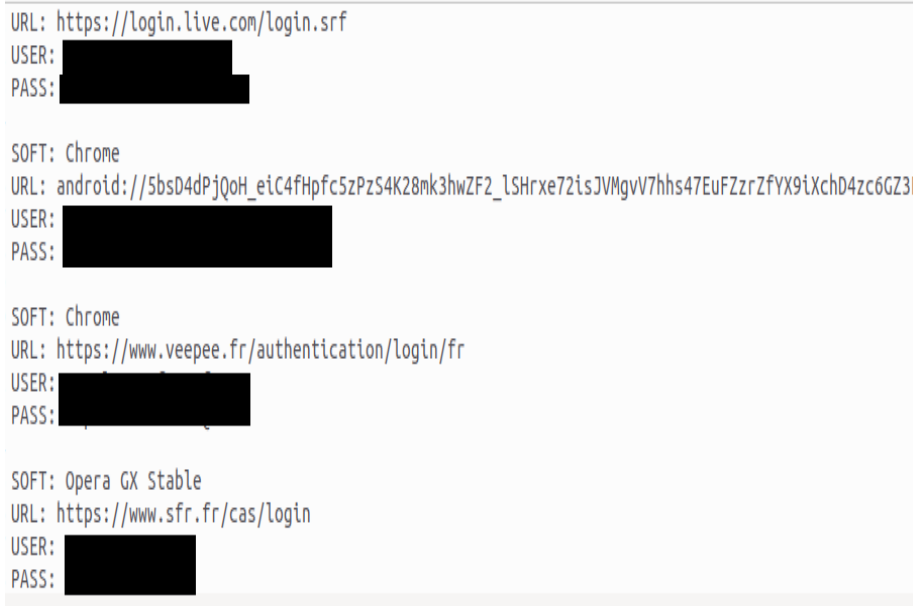
Terminologie du milieu

- 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 apercoivent 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...)
  - Credentiels FTP, token Discord ou Télegram
  - 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



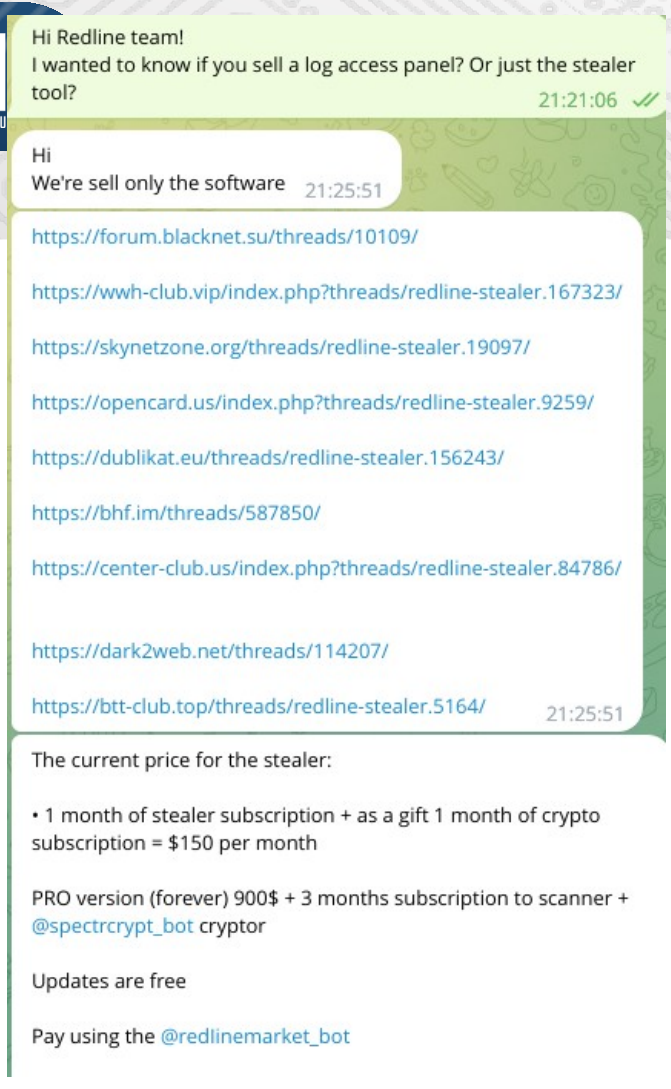
Les stealers - présentation générale

Des chiffres

- 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



Des chiffres

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

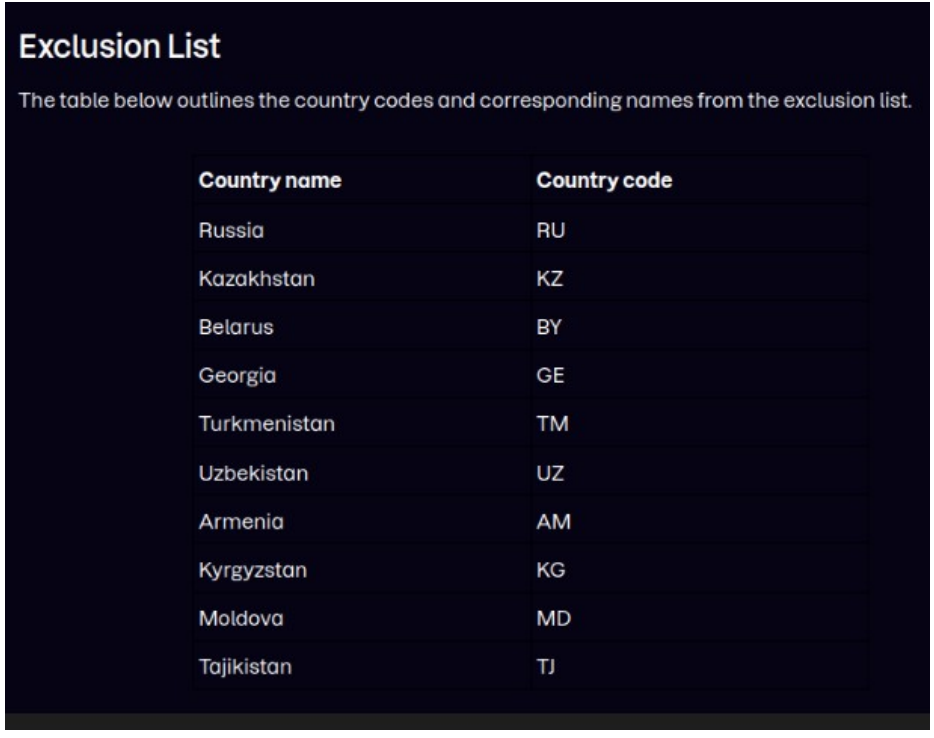
Prévention

- 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 credentiels 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…) !

Analyses

géopolitique

- Pays touchés principalement
  - Par ordre : Inde, Brésil, Indonésie, Pakistan, Turquie, Egypte, Vietnam, Mexique, Philippines, Thailande
  - 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 Certifica
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 Evasio
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
```

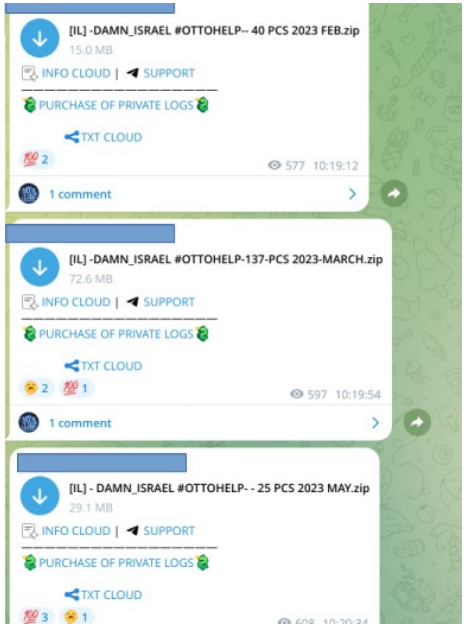
Technique de diffusion

- 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)

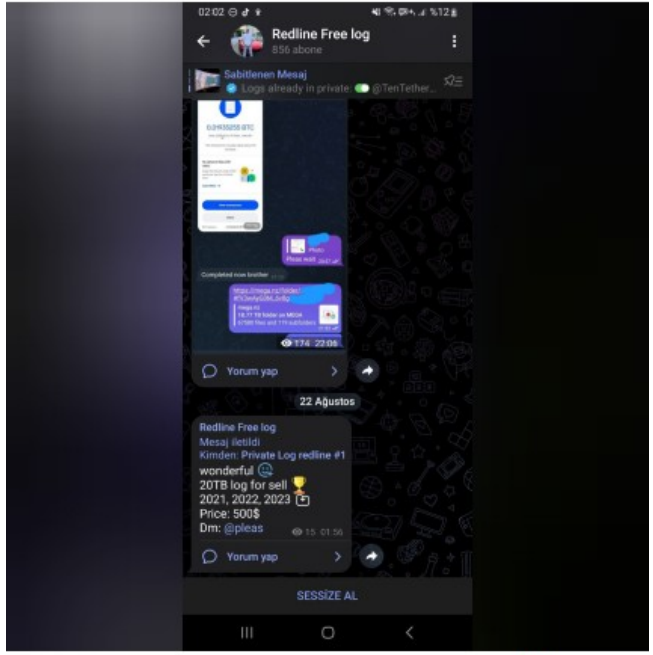
Analyse sociologique

Exemples

- Réaction à la guerre en Israel



Dénonciation des « clouds scams »

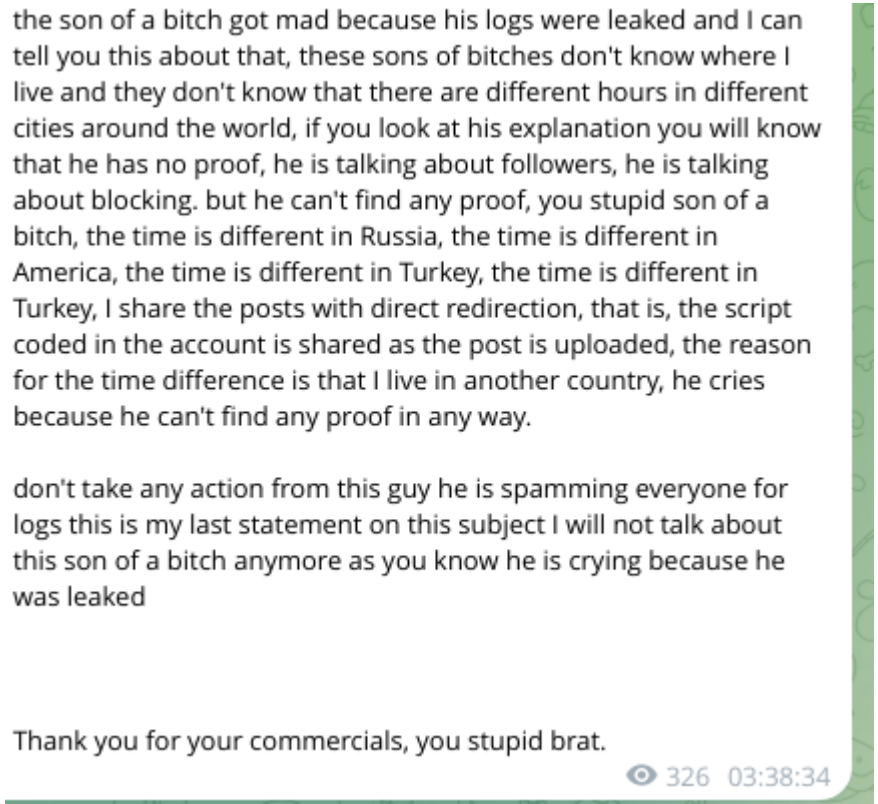


he is scammer dont buy the private logs public former 😂

Analyse sociologique

Exemples

- 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.

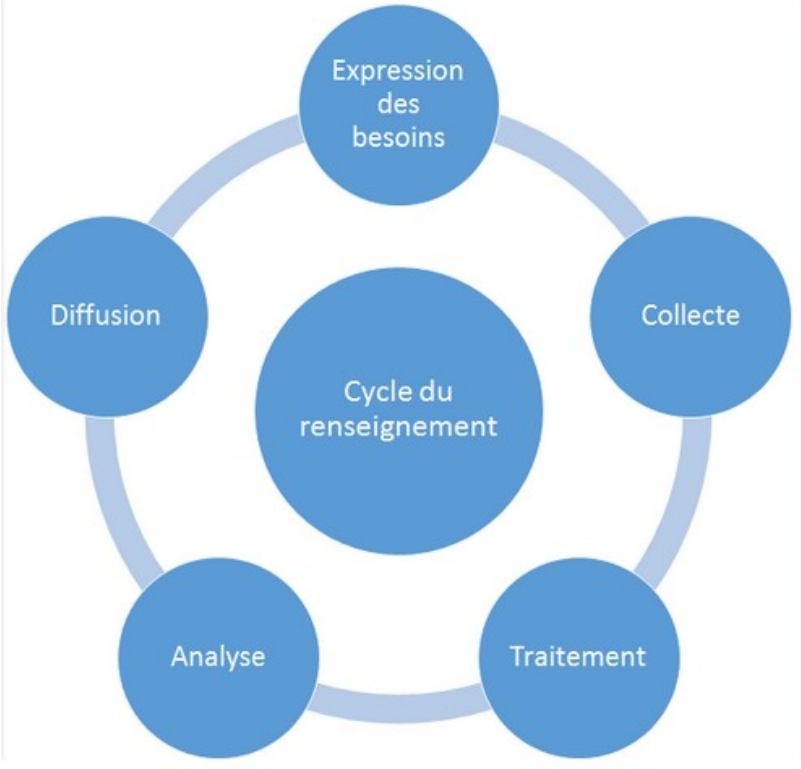
326 03:38:34

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 événement géo-politique

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 🏦

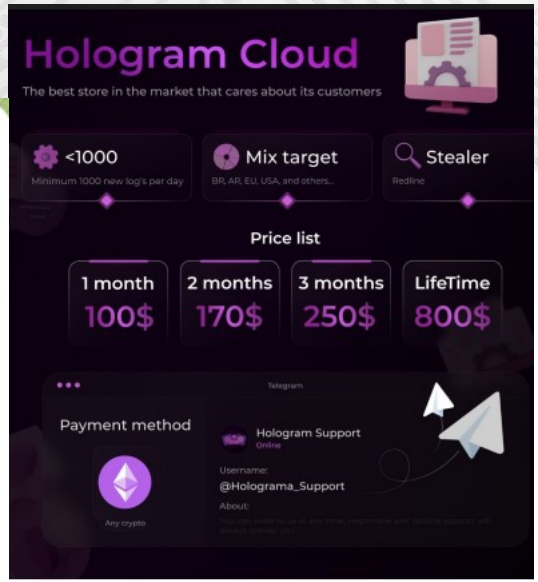
- BTC
- LTC
- BNB
- Smart Chain
- USDT (TRC20)
- BTC Banker Check

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

2. Buy by Admin - @daeftt 👨‍💼

1092 05:24:58

Leave a comment



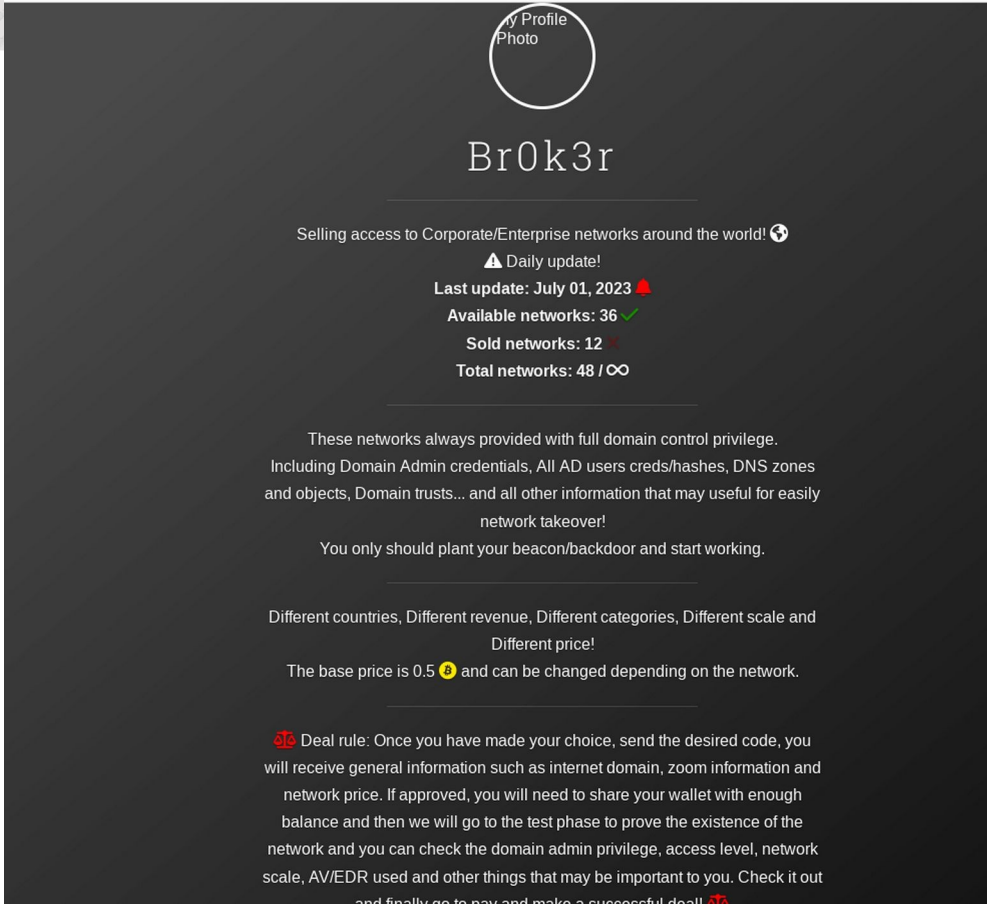
PRIVATE CLOUD LOGS
every day minimum 1.000 logs
BR, AR, EU, USA, CA, MIX Targeted
Work logs
Every day new fresh logs
Stealer RedLine

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/hologramacloud
TELEGRAM @Holograma_support
CHAT https://t.me/hologram_chat

Collecte

Forums

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



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

Méthodologie

Analyse

- Traitement automatisé des données bruts pour faire le tri
- Analyse manuelle / vérifications
  - fausses informations ?
  - faux positifs ?
  - Anciennes données ?
  - Capitalisation des résultats

- Exemple : **russian market**

Analyse juridique

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

BREACHUNT

WWW.BREACHUNT.FR

Questions ?