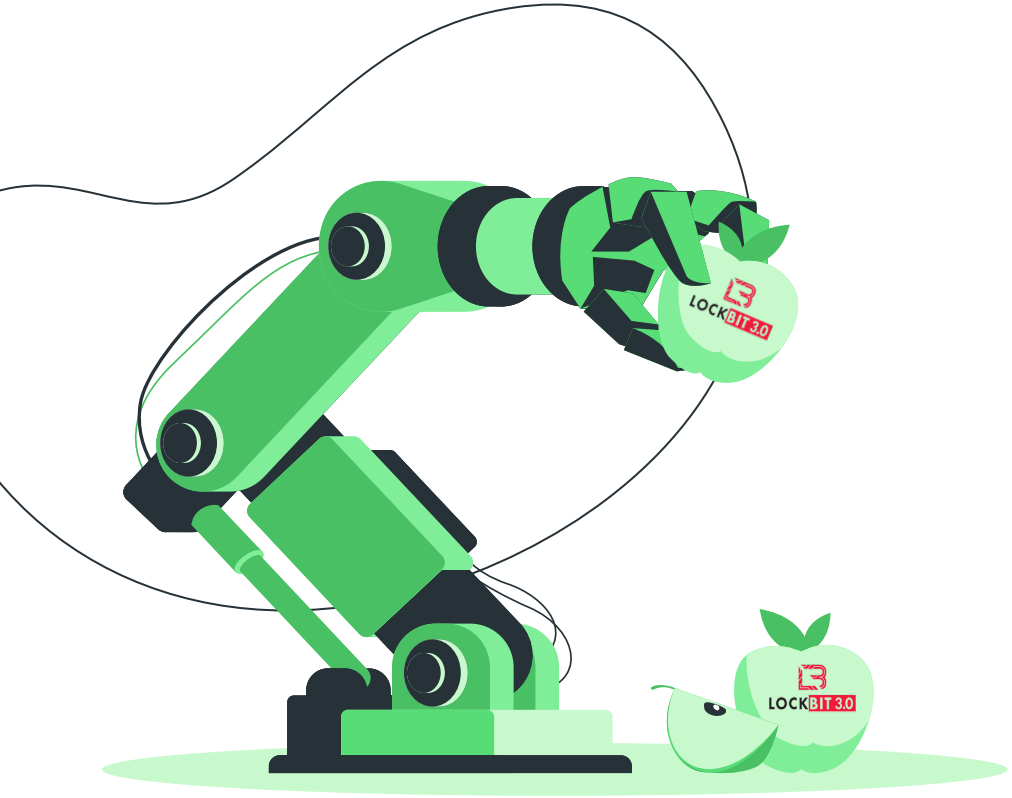


Lock A Bit of a Story

Par Shaym et Daeras

$~ whoarewe

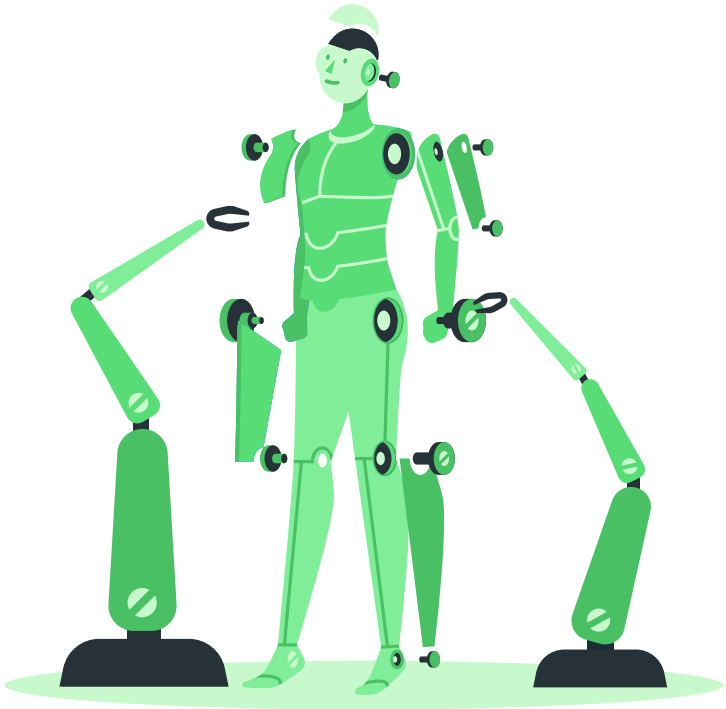
- **Daeras**
  - Membre d'Hack2G2

0xDaeras

- **Shaym**
  - Membre d'Hack2G2

0xShaym

Sommaire



Historique du groupe

ABCD ransomware

LOCKBIT 2.0

LOCKBIT 3.0

2019

Emergence du groupe sous le nom **ABCD**

2020

Lancement de son **programme d'affiliation** RaaS

Création d'un site dédié aux fuites de données

Stratégie de double extorsion

2021

Sortie de **LockBit 2.0**

Vol de 6To + Rançon de 50M$ sur **Accenture**

Changement de la méthode de chiffrement

2022-2023

Sortie de **LockBit 3.0** ou LockBit Black

Premier **bug bounty** dédié aux ransomwares

Leak du **code source**

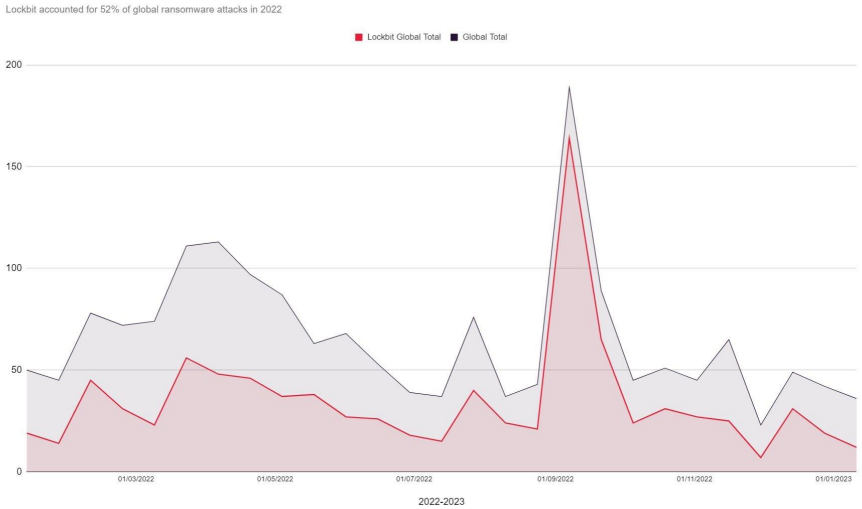
2024

Opération **Cronos**

Saisie de serveurs, **arrestation d'affiliés**

Mise en examen du **leader** du groupe

Historique du groupe

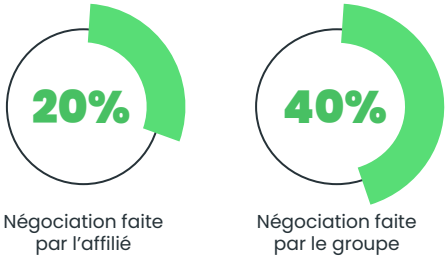


Graphique de JUMPSEC présentant la proportion d'attaques de Lockbit par rapport à toutes les attaques de ransomware

Modèle économique

Le RaaS

- Lockbit fournit le ransomware à des affiliés, qui mènent les attaques.
- La répartition des gains dépend de leur implication :



Blanchiement

- Utilisation d'exchangers chinois par transferts de petites sommes
- Investissement dans des business légitimes (restaurants ?)

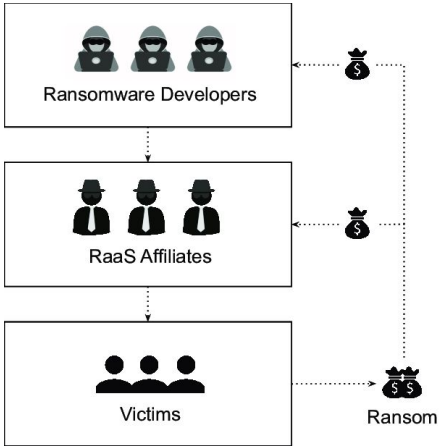
L'extorsion

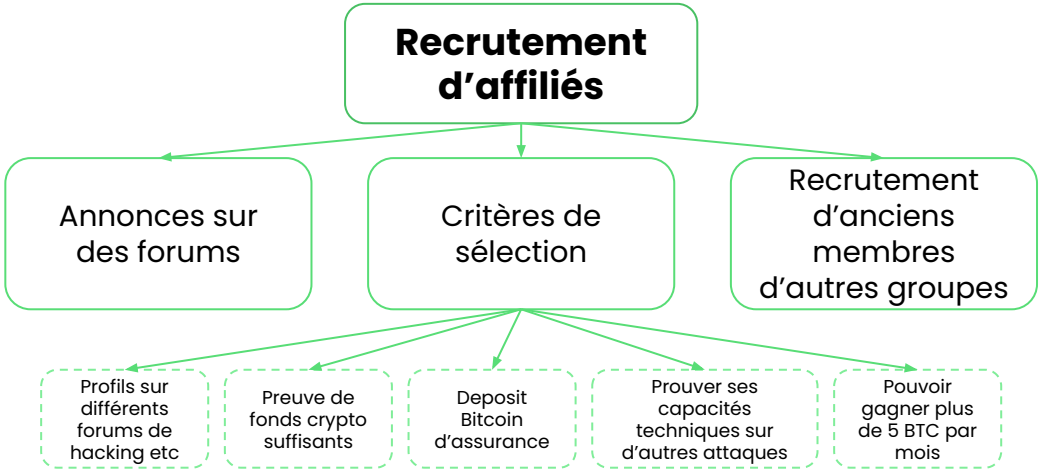
- Rançon pour déchiffrement des données
- Avec LockBit3.0, double extorsion : menace de leak des données en plus du chiffrement.
- Plusieurs options de rançon : repousser de 24h la deadline de rançon, connaître ou encore supprimer les données volées…

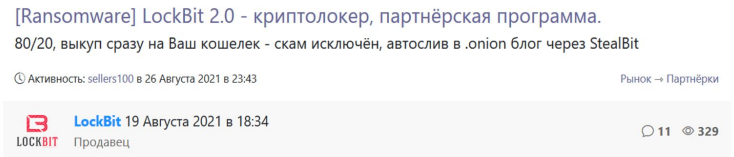
Marketing et réputation

- Réputation de fiabilité dans le milieu criminel
- Slogans accrocheurs "Make Ransomware Great Again"
- Logo reconnaissable

Fonctionnement RH et affiliation






[Ransomware] LockBit 2.0 - криптолокер, партнёрская программа.

80/20, выкуп сразу на Ваш кошелек - скам исключён, автослив в .onion блог через StealBit

Активность: sellers100 в 26 Августа 2021 в 23:43 — Рынок → Партнёрки

LockBit 19 Августа 2021 в 18:34 — Продавец — 11 — 329

LockBit promouvoit son programme affilié sur le forum RAMP, August 19, 2021

- Les affiliés ont le contrôle total des négociations et de la réception des rançons.
- Les paiements sont effectués directement sur l'adresse cryptocurrency de l'affilié.

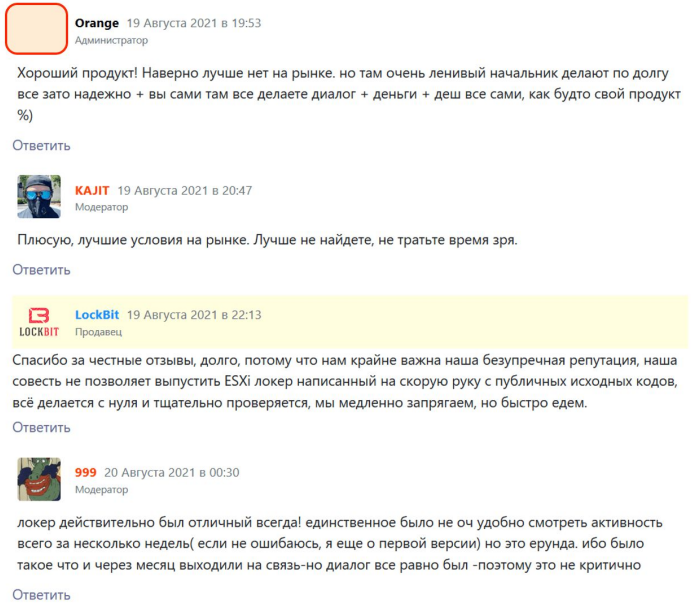
Fonctionnement RH et affiliation

Règles et procédures

- Recommandations sur les montants de rançon à demander en fonction du chiffre d'affaires de la victime
- Interdiction de proposer des remises supérieures à 50% du montant initial demandé
- Une flexibilité laissée aux affiliés pour fixer le montant final en fonction des dommages infligés

Culture d'entreprise

- Encourage la communication ouverte avec ses affiliés (sondage pour établir les nouvelles règles de négociation)



Orange 19 Августа 2021 в 19:53
Администратор

Хороший продукт! Наверно лучше нет на рынке. но там очень ленивый начальник делают по долгу все зато надежно + вы сами там все делаете диалог + деньги + деш все сами, как будто свой продукт %)

Ответить

KAJIT 19 Августа 2021 в 20:47
Модератор

Плюсую, лучшие условия на рынке. Лучше не найдете, не тратьте время зря.

Ответить

LockBit 19 Августа 2021 в 22:13
Продавец

Спасибо за честные отзывы, долго, потому что нам крайне важна наша безупречная репутация, наша совесть не позволяет выпустить ESXi локер написанный на скорую руку с публичных исходных кодов, всё делается с нуля и тщательно проверяется, мы медленно запрягаем, но быстро едем.

Ответить

999 20 Августа 2021 в 00:30
Модератор

локер действительно был отличный всегда! единственное было не оч удобно смотреть активность всего за несколько недель(если не ошибаюсь, я еще о первой версии) но это ерунда. ибо было такое что и через месяц выходили на связь-но диалог все равно был -поэтому это не критично

Ответить

Les administrateurs et modérateurs du forum RAMP discutent de la qualité de leur produit avec un représentant de LockBit et font l'éloge de ses caractéristiques et de sa grande qualité le 19 août 2021.

Bassterlord :

Graphic Designer to Ransomware affiliate

Profil de Bassterlord

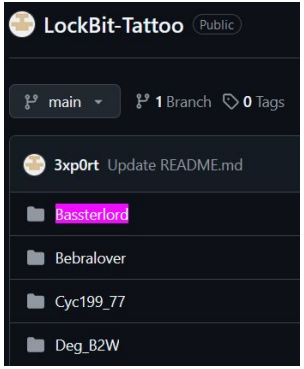
- **Nom :** Ivan Gennadievich Kondratyev
- **Age :** Homme de 27 ans
- **Lieux :** Louhansk, Ukraine
- **Alias connus :** Bassterlord, Fisheye,

  Buster, National Hazard Agency

ID	42241549
Alias	it11112
Name	Ivan
Surname	Kondratiev
Status	¯_(ツ)_/¯
Celebrity	No
Date of Birth	04/08/1996
Family status	not indicated
Floor	Man
About Me	
Languages	Russian, English
Music	Open the playlist
Movie	Who am I; Mr. Robot; Citizenfour. Snowden's truth; 5th Power

Trace de Bassterlord

- **Fuite de données Twitter :** sinner4iter@gmail.com ⟶ @It9111
- **Fuite 000webhost (2015) :** Bryanka, Louhansk, Ukraine
- **Profil Ok.ru :** Nom, date de naissance, école et adresse
- **Critique de clinique dentaire :** Recouper adresse et nom
- **Chaine youtube :** Vidéo de son tattoo LockBit



Bassterlord :

Graphic Designer to Ransomware affiliate

La genèse

- Mère hospitalisée
- Besoin d'argent
- Recherche d'opportunités sur les forums du Dark Web

Les débuts de Bassterlord

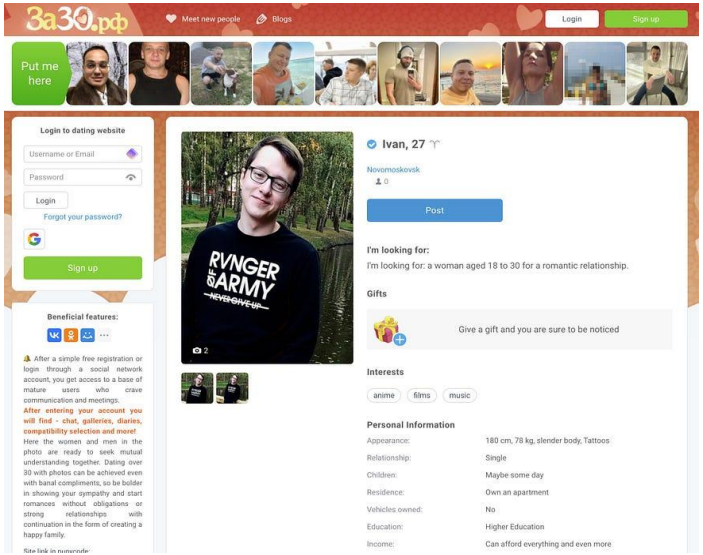
- Engagé comme scammer par **REvil**
- Mentorat par **Lalartu,** co-fondateur de **REvil**

Ses activités

- Graphic Designer de formation
- Écriture du manuel du parfait ransomware
    - Vol des droits d'auteur par PRODAFT
- Formation d'une équipe

La fin pour un affilié

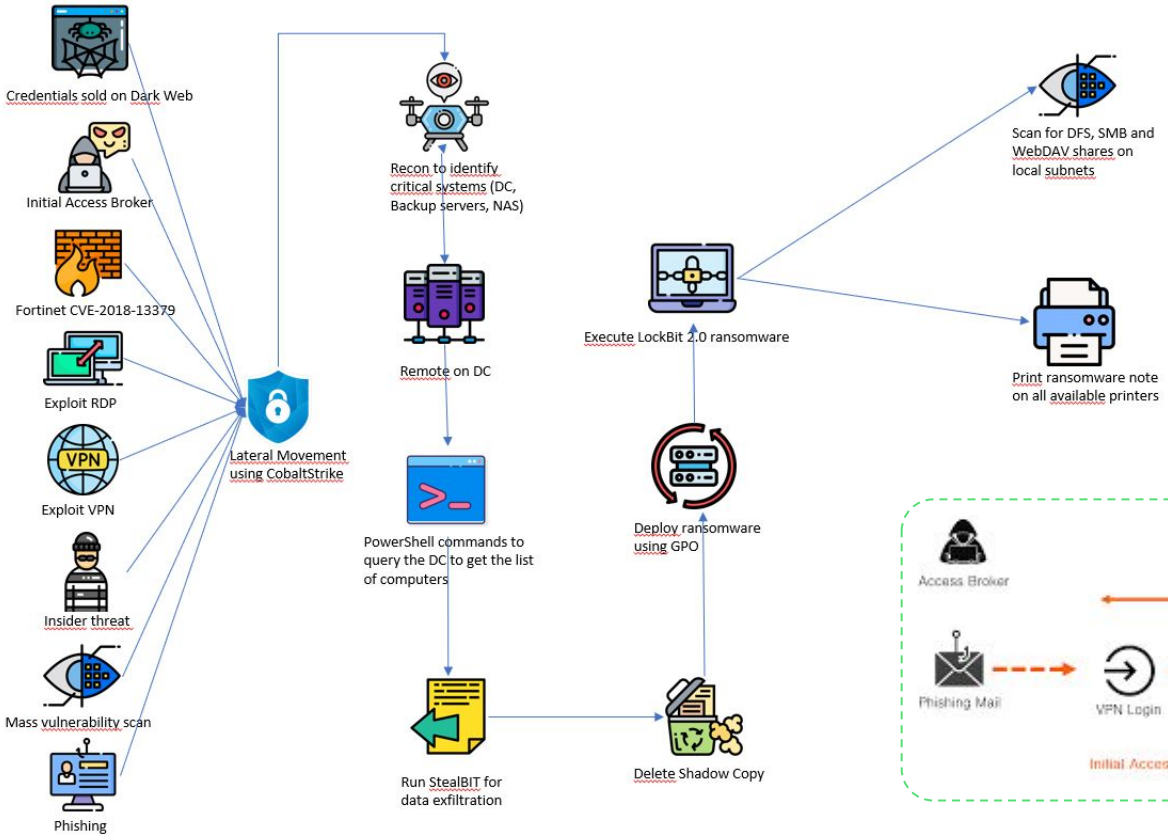
- Intensification des conflits en Ukraine
- Problèmes mentaux liés à l'insécurité global
- Contentieux avec d'autres membres de la communauté

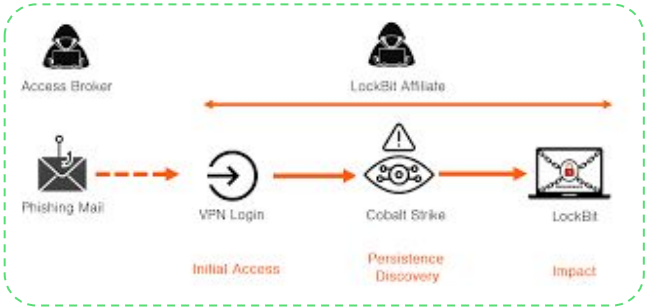


Leader

- **Pseudonymes :** putinkrab ,LockBitSupp, LockBit
- **Nom :** Dmitry Yuryevich Khoroshev (Дмитрий Юрьевич Хорошев)
- **Nationalité :** Russe
- **Chefs d’accusation :** 26, dont : fraude et extorsion au moyen d'ordinateurs, association de malfaiteurs en vue de commettre une fraude électronique, dommages intentionnels à un ordinateur protégé, extorsion liée à des informations obtenues illégalement à partir d'un ordinateur protégé et extorsion liée à des dommages intentionnels à un ordinateur protégé…

LockBit Killchain





Still a bit of data ?

Benchmark des stealers

- **Outil publique**
  - Rclone
  - Cloud publique (pcloud, mail.ru, mega.nz…)
- **Outil custom**
  - Ryuk Stealer
  - Exmatter
  - StealBit

Along with the encrypting system, you get access to the fastest stealer all over the world - StealBit automatically downloading all files of the attacked company to our updated blog.

Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	**83,46 MB/s**	**Yes**	**Yes**	**Yes**	**1M 59S**	**19M 58S**	**1D 9H 16M 57S**
Rclone pcloud.com free	4,82 MB/s	No	No	No	**34M 34S**	**5H 45M 46S**	**24D 18M 8S**
Rclone pcloud.com premium	4,38 MB/s	No	No	No	**38M 3S**	**6H 20M 31S**	**26D 10H 11M 45S**
Rclone mail.ru free	3,56 MB/s	No	No	No	**46M 48S**	**7H 48M 9S**	**32D 12H 16M 28S**
Rclone mega.nz free	2,01 MB/s	No	No	No	**1H 22M 55S**	**13H 48M 11S**	**57D 13H 58M 44s**
Rclone mega.nz PRO	1,01 MB/s	No	No	No	**2H 45M**	**1D 03H 30M 9S**	**114D 14H 16M 30S**
Rclone yandex.ru free	0,52 MB/s	No	No	No	**5H 20M 30S**	**2D 05H 25M 7S**	**222D 13H 52M 49S**

The LockBit group advertises StealBit (source: KELA, Twitter)

Still a bit of data ?

Caractéristiques de StealBit

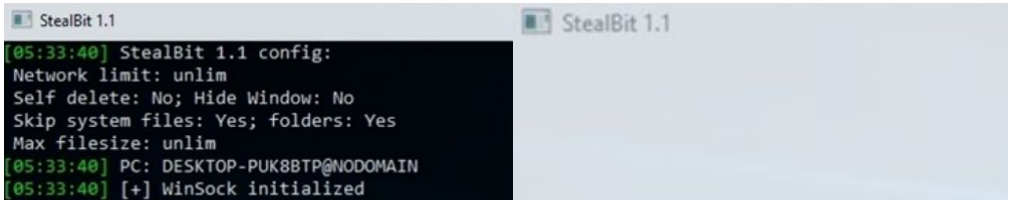
- Serveurs d'exfiltration aux Pays-Bas et aux États-Unis.
- Named pipe-based IPC et I/O Completion Ports pour une exfiltration efficace.
- Détection de débogueurs via NtGlobalFlag du PEB.

Évolution des versions

- Paramétrage limité
- Restriction d'exécution
- Nouveaux paramètres : -hide, -delete, -skipfiles …
- Ajout de l'auto-suppression
- Contrôle du taux d'exfiltration
- Suppression des restrictions géographiques

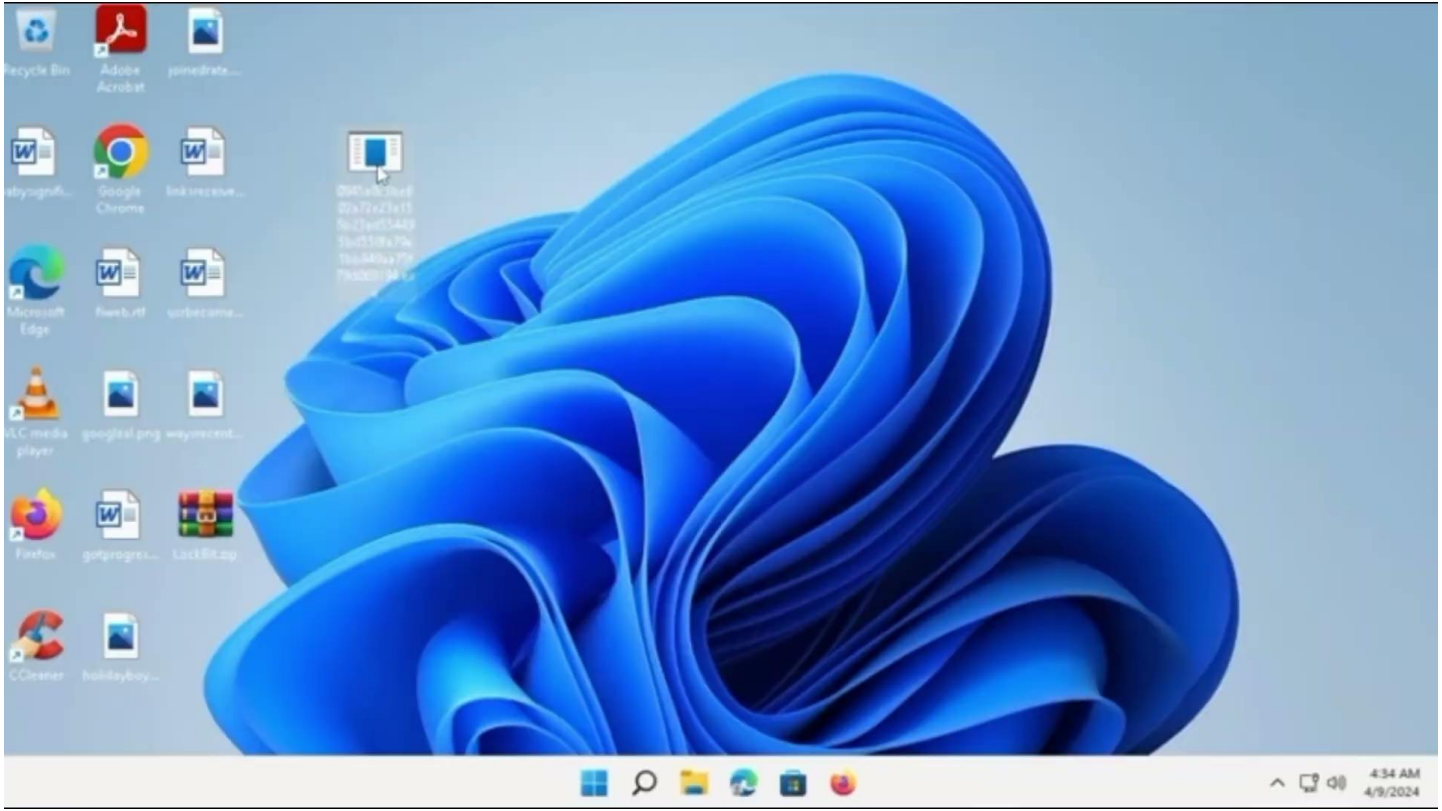
Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode
Stealer - StealBIT	83,46 MB/s	Yes	Yes
Rclone pcloud.com free	4,82 MB/s	No	No
Rclone pcloud.com premium	4,38 MB/s	No	No

LockBit claims that StealBit hides its presence on compromised systems (source: KELA, Twitter)



StealBit displays windows when the malware operator sets the parameter -hide to no or yes

Détonation de Lockbit Black



Analyse du ransomware

```
                    LAB_004c0030                                    XREF[1]:     004c0051(j)
004c0030 8a 94 34        MOV        DL,byte ptr [ESP + index*0x1 + gdiplus_dll[1]]
         ec 00 00 00
004c0037 8b 84 24        MOV        EAX,dword ptr [ESP + local_3a8]
         e8 00 00 00
004c003e 0f be c8        MOVSX      ECX,AL
004c0041 0f be c2        MOVSX      EAX,DL
004c0044 33 c8           XOR        ECX,EAX
004c0046 88 8c 34        MOV        byte ptr [ESP + index*0x1 + gdiplus_dll[1]],CL
         ec 00 00 00
004c004d 46              INC        index
004c004e 83 fe 0b        CMP        index,0xb
```

Code du binaire permettant de XOR la chaîne

- \MACHINE\Preferences\NetworkShares\NetworkShares.xml: **Permet de mettre en partage réseau tous les disques du serveur.**
- \MACHINE\Preferences\Services\Services.xml: **Arrête une liste de service trouvés précédemment.**
- \MACHINE\Preferences\Files\Files.xml: **Place le binaire sur le Bureau de tous les partages.**
- \MACHINE\Preferences\ScheduledTasks\ScheduledTasks.xml: **Kill tous les process de la liste trouvé précédemment.**
- \MACHINE\Registry.pol: **Contient des clés de registre.**
- \MACHINE\comment.cmtx

Configuration de la GPO

Chaque nom de DLL est encodé avec du code différent. La liste des DLL encodées est la suivante :

- `gdiplus.dll` - `ws2_32.dll` - `shell32.dll` - `advapi32.dll` - `user32.dll` - `ole32.dll` - `netapi32.dll` - `gpredit.dll` - `oleaut32.dll` - `shlwapi.dll` - `msvcrt.dll` - `activeds.dll` - `gdiplus.dll` - `mpr.dll` - `bcrypt.dll` - `crypt32.dll` - `iphlpapi.dll` - `wtsapi32.dll` - `win32u.dll` - `Comdlg32.dll` - `cryptbase.dll` - `ombase.dll` - `winspool.drv`

Résolution dynamique des DLL

```
if (isRegCreated != 0) {
  CryptoBoxKeypair(&GENERATED_PUBLIC_KEY,&GENERATED_PRIVATE_KEY);
  CryptoBoxEasy(SESSION_KEY,(uint)&GENERATED_PUBLIC_KEY,0x40,0,(uint)PUBLIC_KEY);
  MemFill(extraout_ECX_03,extraout_EDX_02,&GENERATED_PRIVATE_KEY,0xff,0x20);
  uVar5 = extraout_ECX_04;
  uVar6 = extraout_EDX_03;
  goto LAB_004a0b54;
}
```

Chiffrement avec bcrypt

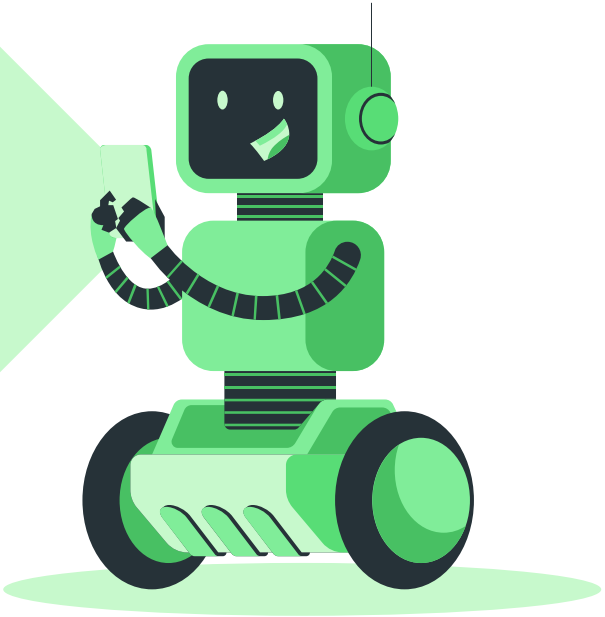
```
langue = (*GetSystemDefaultUILanguage)();
if (((((langue == 0x82c) || (langue == 0x42c)) ||
     ((langue == 0x42b || ((langue == 0x423 || (langue == 0x437)))))) || (langue == 0x43f)) ||
   (((((langue == 0x440 || (langue == 0x819)) || (langue == 0x419)) ||
     ((langue == 0x428 || (langue == 0x442)))) ||
    ((langue == 0x843 || ((langue == 0x443 || (langue == 0x422)))))))) {
```

- Azeri (Cyrillic) - Azeri (Latin) - Armenian (Armenia) - Belarusian - Georgian - Kazakh - Kyrgyz (Cyrillic) - Russian (Moldava) - Russian - Tajik - Turkmen - Uzbek (Cyrillic) - Uzbek (Latin) - Ukrainian

Vérification de la langue du système

Conclusion

En vrai il sont pas gentil mais dans l'ensemble ils sont Russe du coup bon y sont tranquilles :)



Sources

Programme affilié : https://www.linkedin.com/pulse/lockbit-affiliate-program-how-join-worlds-biggest-elena-koldobsky/
Importance par rapport aux autres groupes : https://www.jumpsec.com/uk-ransomware-trends-lessons-for-2023/
Historique du groupe : https://en.wikipedia.org/wiki/LockBit
Reverse d'un sample : https://www.adacis.net/blog/analyse-lockbit/
Business model : https://venturebeat.com/security/lockbit-3-0-and-the-ransomware-business-model/
Arrestations : https://www.justice.gov/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware
Programme affilié : https://blog.talosintelligence.com/ransomware-affiliate-model/
Rapport sur le groupe par la CISA : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
Rapport d'OSINT sur LockBitSupp : https://predictalab.medium.com/investigating-lockbits-leader-c5ec88899ad7
Rapport d'OSINT sur LockBitSupp : https://intel471.com/blog/alleged-lockbit-ransomware-gang-leader-named
Lockbit Horizon : https://analyst1.com/blog-negotiating-with-lockbit-uncovering-the-evolution-of-operations-and-newly-established-rules/
StealBit deep dive : https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
LockBit Tattoo : https://github.com/3xp0rt/LockBit-Tattoo