CONTI

De la genèse à la disparition d'une licorne du rançongiciel

Gérôme BILLOIS

@gbillois

Panocrim 23e édition - 26 janvier 2023

#Panocrim

CONTI – QU'ONT-ILS FAIT ?

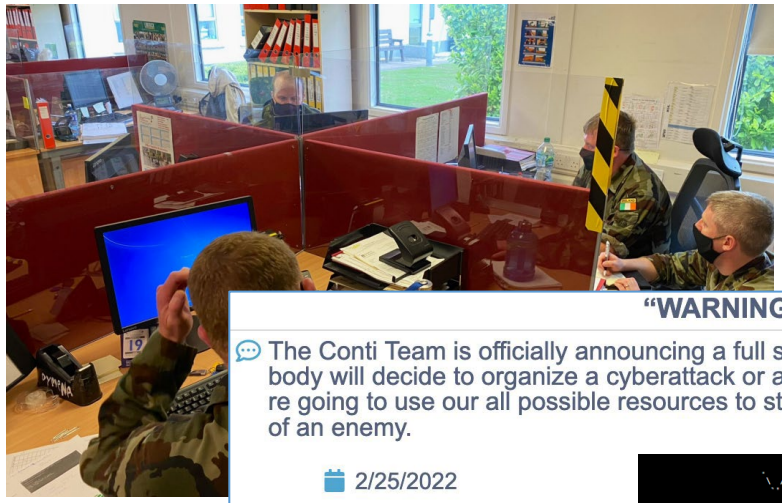
Février 2020 : Lancement

2020/2021 : Une carrière en fanfare

Février 2022 : Le conflit ukrainien et l'explosion

Avril 2022 : Le baroud d'honneur : le Costa Rica

Mai 2022 : Le simili démantèlement



"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022

Go Back

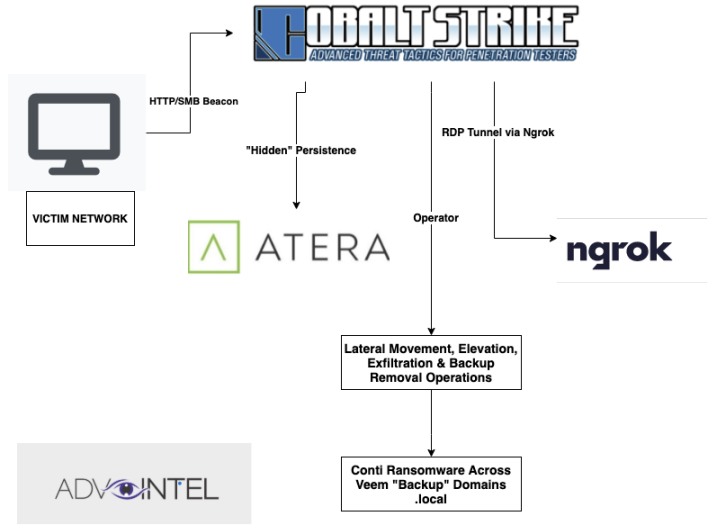
Directory: Conti/

File Name	File Size	Date
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1159600	2022-03-01 02:46:21
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Training Material Leak	0	1969-12-31 18:00:00

CONTI – COMMENT FONT-ILS?

Une approche classique sur l'attaque…

- Intrusion, escalade, exécution… avec des outils connus
- Evidemment de la double extorsion
- Une attention à l'effacement des sauvegardes

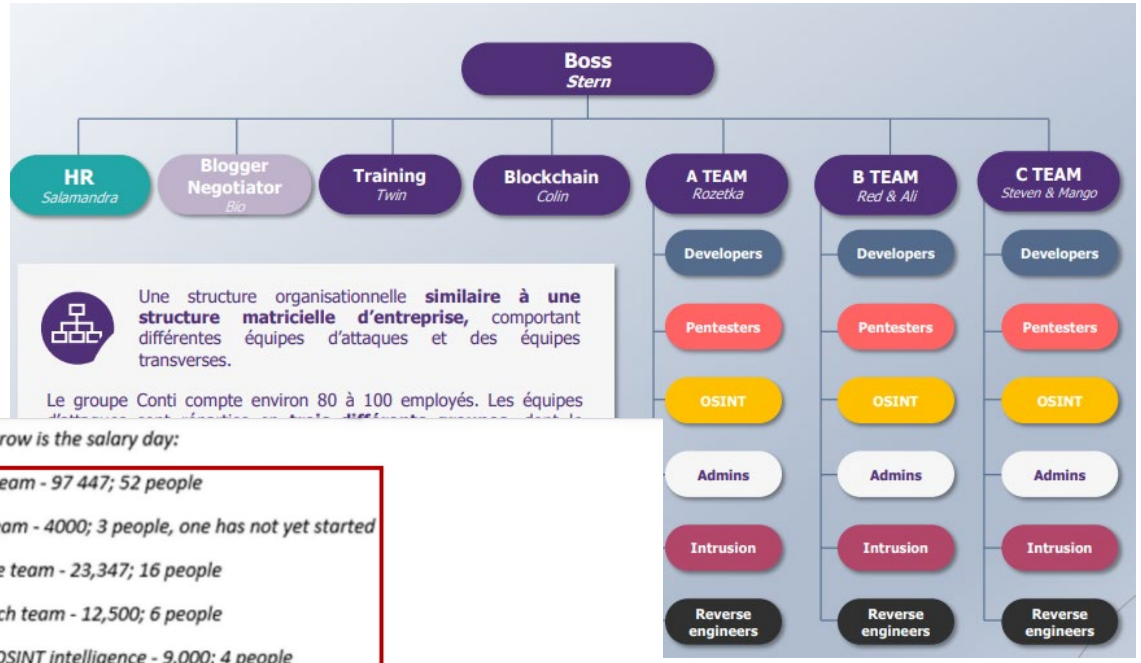


… avec une vrai professionnalisation

- Des locaux en Russie
- Des achats de licence d'outil (Cobalt Strike 60k$)
- Des abonnements pour des sites de recrutement (headhunter.ru, superjobs.ru…)
- L'embauche d'un journaliste pour mettre la pression sur les victimes
- L'emploi de personnes dédiées à créer des nouvelles versions toutes les 4 heures pour éviter les détections

CONTI – QUI SONT-ILS ?

- Un groupe de professionnels : entre 60 et 100 personnes ; des salaires moyens autour de 1800$
- Une organisation hiérarchique rodée avec une équipe de management, en lien (trouble) avec le gouvernement
- Des moyens importants : au moins 180M$ collectés en 2021



Si vous avez des informations sur les membres du groupe : 10M$ de récompenses offertes

CLUSIF
#Panocrim

SOURCES

- https://www.riskinsight-wavestone.com/2022/07/ransomware-immersion-au-sein-de-lancien-groupe-conti/
- https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/
- https://news.sophos.com/en-us/2021/02/16/what-to-expect-when-youve-been-hit-with-conti-ransomware/
- https://www.state.gov/reward-for-information-owners-operators-affiliates-of-the-conti-ransomware-as-a-service-raas/
- https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/
- https://cybersecurityworks.com/howdymanage/uploads/image/blogs/conti-aka-wizard-spider-ttps-mapped-from-vulnerability-associations-1.png
- https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love
- https://www.cyberkendra.com/2022/03/contis-ransomware-source-code-leaked.html
- https://techcrunch.com/2022/08/12/state-conti-ransomware-intelligence/
- https://www.breachquest.com/blog/conti-leaks-insight-into-a-ransomware-unicorn/
- https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks
- https://flashpoint.io/blog/history-of-conti-ransomware/#:~:text=The%20formation%20of%20Conti,-Led%20by%20Russia&text=By%20the%20end%20of%202020,Maze%E2%80%9D%20and%20%E2%80%9CEgregor.%E2%80%9D