PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS

Conti Ransomware Group In-Depth Analysis

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland   +41225481923   info@prodaft.com

Contents

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Reference Number	CH-2021100801
Prepared By	PTI Team
Investigation Date	25.09.2021 - 16.10.2021
Initial Report Date	16.10.2021
Last Update	18.11.2021

What's new ?

PRODAFT Threat Intelligence (PTI) Team has obtained valuable insights on the inner workings of the Conti ransomware group. The PTI team accessed Conti's infrastructure and identified the real IP addresses of the servers in question. This report provides unprecedented detail into the way the Conti ransomware gang works, how they select their targets, how many targets they've breached, and more.

Why does it matter ?

Ransomware attacks are increasing in severity and frequency, threatening major institutions and placing enormous strain on supply chains that are already stretched thin. Conti has shown itself to be a particularly ruthless group, indiscriminately targeting hospitals, emergency service providers, and police dispatchers. This report contains the latest and most accurate data available on one of the most dangerous ransomware groups in existence.

Conti also earned a reputation for not delivering decryption keys even after victims pay. However, simply telling companies not to pay isn't enough to solve the problem. Our mission is to equip executives, legal advisors, insurers and law enforcement agents with intelligence and unique insights that help them understand the threat, manage the risk more effectively, and find better practical solutions to deal with its consequences.

1 Introduction

Ransomware attacks work by encrypting the victim's business-critical data, rendering it inaccessible. After triggering the attack, cybercriminals will offer to sell a decryption key to the victim. If the victim doesn't comply, they simply have to accept the catastrophic loss of their most valuable data.

Some ransomware attacks use a two-pronged strategy. Attackers will demand a ransom payment for decrypting data, and threaten to publicly publish sensitive data if the ransom is not paid by a certain deadline. (*"Double Extortion"*).

Ransomware has been in use for decades, but it has surged in popularity among cybercriminals in recent years. Multiple factors contribute to this rise, including the development of cryptocurrency that enables near-anonymous payments, the widespread digitalization of sensitive data, and the release of sophisticated ransomware-as-a-service criminal business models. Ransomware losses are likely to exceed $20 billion by the end of 2021 [4].

Ransomware can be separated into two basic groups :

- Fully Automated Ransomware (FAR), and
- Semi-Automated Ransomware (SAR)

In FAR cases, ransomware generally infects the system via phishing emails or malicious web pages that contain the malicious payload. The malware contains the code to spread throughout the network, identify sensitive files, encrypt them, and display a ransom note for the victim. Threat actors who use FAR mostly focus on lightweight distribution channels that are easily automated – they tend to stay away from making direct contact with victims. FAR attacks do not typically succeed against enterprise-level organizations with a wide range of detection and prevention tools. Victims of FAR attacks tend to be more cautious about paying the ransom because the automated system doesn't instill a great degree of trust. In many cases, victims will ask to be transferred to a human representative, who will negotiate on behalf of the cybercrime organization.

SAR attacks can be more sophisticated since they rely on manual interaction between cybercriminals and their victims. In these cases, attackers may use zero-day exploits, or they may rely on known vulnerabilities that haven't yet been patched – even within hours of the patch release. Our team has observed SAR attackers buying RDP or VPN credentials directly from other hackers on underground markets. Upon successful entry, these attackers use common penetration testing tools for lateral movement within the victim's network. They then escalate their privileges, start encrypting, and trigger the ransomware attack.

Modern cybercrime organizations use a hierarchical workflow to monetize operations. The "X-as-a-Service" model has become popular among criminals since each step of an advanced attack kill chain requires different skills. This report will demonstrate how this business model works and provide in-depth insight about the illicit economy it perpetuates. These findings will help other researchers understand the working dynamics of other groups that operate in the ransomware industry.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

The group this report focuses on is called "Conti", which appears to be identical with the group known as "Wizard Spider". It is a criminal organization behind advanced ransomware technologies known as Ryuk and Hermes. We won't focus on sample analysis, as many reputable sources already offer this kind of technical information. Instead, this report is the first to presents findings regarding behind-the-scenes information on how the ransomware group operates.

Enterprise leaders, cybersecurity executives, and risk advisors can use this report's findings to better prepare their organizations against ransomware attacks. Proactive threat intelligence is key to identifying the factors that contribute to cybercrime trends and preventing threat actors from exploiting enterprise vulnerabilities.

Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing global fight against high-end threat actors and APTs.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

2 Executive Summary

2.1 Overview

Conti ransomware frequently makes headlines due to the high-profile organizations it often targets, as well as the high ransoms its negotiators demand. The PTI Team noticed a surge in Conti attacks and started analyzing the group in September 2021. Our team detected a vulnerability in the recovery servers that Conti uses, and leveraged that vulnerability to discover the real IP addresses of the hidden service hosting the group's recovery website. This report presents valuable data about the inner workings of the semi-automatic recovery service that Conti relies on to execute ransomware attacks. Threat intelligence data like this helps enterprise executives build resilient cybersecurity defenses and protect sensitive data from exfiltration.

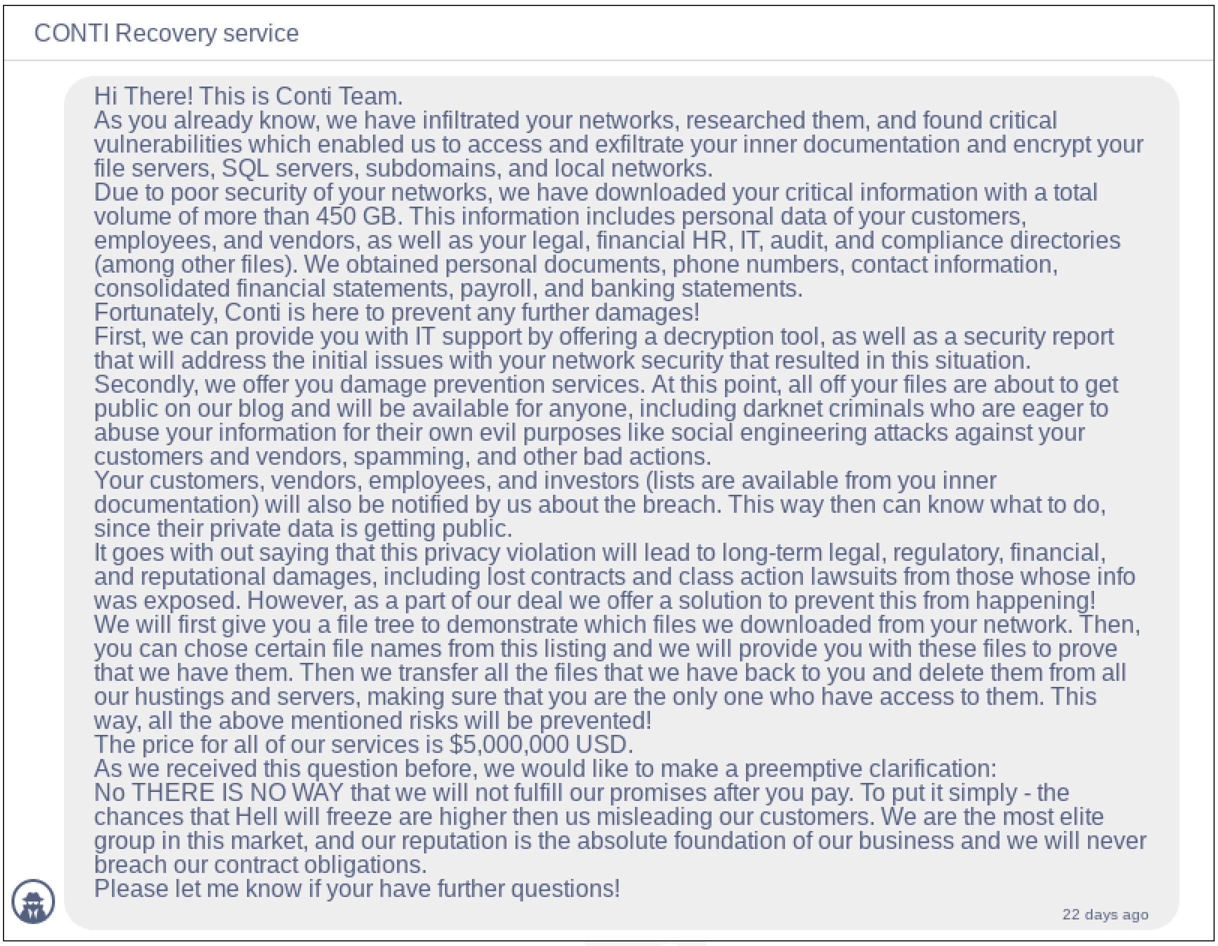
2.2 Conti Ransomware

Conti ransomware (a.k.a. Hermes, Ryuk[1], Wizard Spider[9]) is a malicious program that prevents users from accessing their data unless the victims pay a ransom. Conti automatically scans networks for valuable targets, spreads through the network, and encrypts every device and account it can find.

Unlike similar ransomware variants, Conti uses a ransomware-as-a-service (RaaS) business model. The ransomware developers sell or lease their ransomware technology to affiliates, who then use that technology to carry out attacks. This business model often includes a digital management panel. Conti customers – affiliate threat actors – use this management panel to create new ransomware samples, manage their victims, and collect data on their attacks. Our investigation showed that Conti threat actors also use extortion and victim shaming to coerce victims into paying ransoms.

> **Analyst Note :** Victim shaming is the use of tactical use of social pressure to push victim organizations into fulfilling ransom demands. They may threaten to release stolen confidential data, or to email business partners and draw attention to the ransomware attack.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.



CONTI Recovery service

Hi There! This is Conti Team.
As you already know, we have infiltrated your networks, researched them, and found critical vulnerabilities which enabled us to access and exfiltrate your inner documentation and encrypt your file servers, SQL servers, subdomains, and local networks.
Due to poor security of your networks, we have downloaded your critical information with a total volume of more than 450 GB. This information includes personal data of your customers, employees, and vendors, as well as your legal, financial HR, IT, audit, and compliance directories (among other files). We obtained personal documents, phone numbers, contact information, consolidated financial statements, payroll, and banking statements.
Fortunately, Conti is here to prevent any further damages!
First, we can provide you with IT support by offering a decryption tool, as well as a security report that will address the initial issues with your network security that resulted in this situation.
Secondly, we offer you damage prevention services. At this point, all off your files are about to get public on our blog and will be available for anyone, including darknet criminals who are eager to abuse your information for their own evil purposes like social engineering attacks against your customers and vendors, spamming, and other bad actions.
Your customers, vendors, employees, and investors (lists are available from you inner documentation) will also be notified by us about the breach. This way then can know what to do, since their private data is getting public.
It goes with out saying that this privacy violation will lead to long-term legal, regulatory, financial, and reputational damages, including lost contracts and class action lawsuits from those whose info was exposed. However, as a part of our deal we offer a solution to prevent this from happening!
We will first give you a file tree to demonstrate which files we downloaded from your network. Then, you can chose certain file names from this listing and we will provide you with these files to prove that we have them. Then we transfer all the files that we have back to you and delete them from all our hustings and servers, making sure that you are the only one who have access to them. This way, all the above mentioned risks will be prevented!
The price for all of our services is $5,000,000 USD.
As we received this question before, we would like to make a preemptive clarification:
No THERE IS NO WAY that we will not fulfill our promises after you pay. To put it simply - the chances that Hell will freeze are higher then us misleading our customers. We are the most elite group in this market, and our reputation is the absolute foundation of our business and we will never breach our contract obligations.
Please let me know if your have further questions!

22 days ago

Figure 1. **Conti threat actors using extortion**

2.3 The RaaS Business Model

RaaS owners employ multiple affiliates who are responsible for breaking into victims' networks and encrypting their files. These affiliates are selected mostly from forums, among highly-skilled hackers with backgrounds in penetration testing. People may also become affiliates if they have an established network for obtaining access to information from other cybercriminals. In both cases, RaaS owners require references from recognized cybercriminals before hiring affiliates.

The RaaS business model makes cybercriminal reputation essential to success. Most affiliates send a commission between 10-30% of each ransom payment they receive to the RaaS owners. The amount for the operators can also be automatically deducted from the collected ransom in certain cases. RaaS owners also often provide virtual machines, exploitation tools, and other technologies to support affiliates' attacks. Every affiliate has an access to a management panel where they can monitor and communicate with victims. An affiliate panel usually includes the following tools :

- A ransomware executable generator

- A separate ransomware decryption application
- A cryptocurrency payment gateway for victims
- A commission rate calculator
- Monitoring tools for victims and statistics
- Secure chat functionality for victim negotiation

These tools are designed with non-technical users in mind. Cybercriminals no longer need a great deal of technical expertise to run successful attack campaigns. Instead, they maximize profit using psychological tactics like extortion and victim shaming. Moreover, affiliates are expected to constantly attack and breach new targets. Whenever an affiliate becomes inactive for a long period of time, RaaS owners remove that affiliate's account, which has a negative impact on the affiliate's reputation.

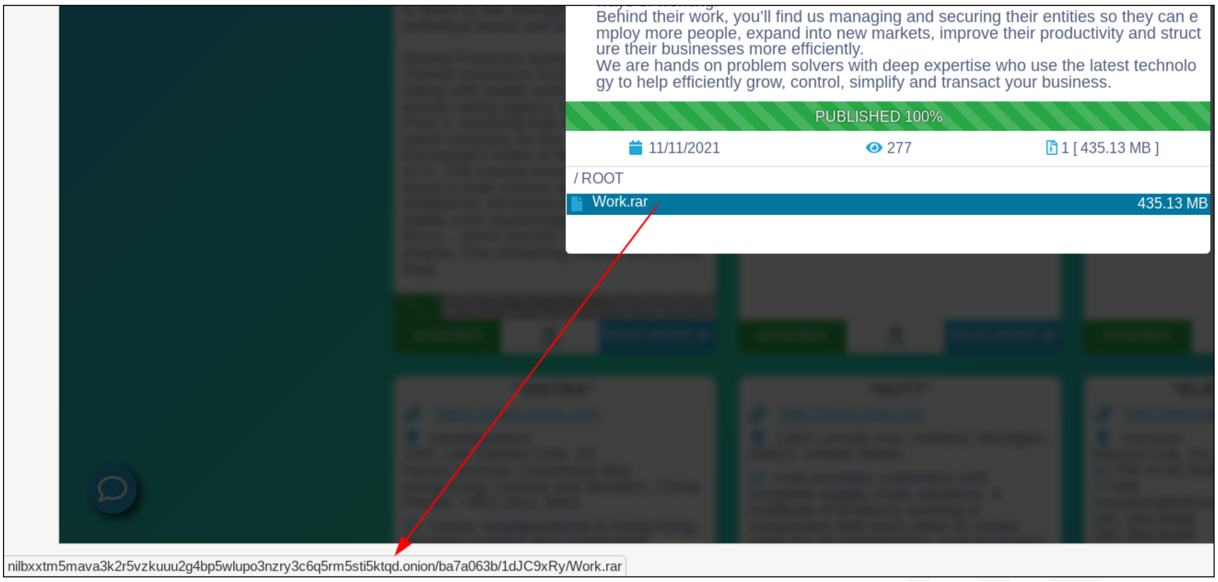
3 Technical Analysis

Our team obtained insider data on the Conti RaaS group and its platform, including information on its management panel and a step-by-step analysis of the Conti attack kill chain. This section contains intelligence about the threat responsible and their affiliates. It includes new, never-before-seen data on Conti's active management server and the group's techniques, tactics and procedures (TTP).

This is valuable information that enterprises and cybersecurity vendors can use to detect and mitigate Conti ransomware attacks. Organizations equipped with sophisticated threat intelligence capabilities can prepare for these attacks and proactively prevent devastating data breaches and ransomware attacks from occurring.

3.1 Conti's History

The first indications of a unique Conti ransomware group appeared in **October 2019**. The group did not establish its own website until early 2020 on the address **http://fylszpcqfel7joif.onion**. Since then, we've observed data belonging to **567** different companies have been shared on the Conti extortion site **https://continews.click** and **http://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion**. This number only represents victims whose names are shared on the extortion site or whose data is shared and subsequently deleted. In addition, Conti uses another TOR hidden service for serving the stolen victim data. As can be seen in the figure 2 data download links points to the domain **nilbxxtm5mava3k2r5vzkuuu2g4bp5wlupo3nzry3c6q5rm5sti5ktqd.onion** with a random path.



Behind their work, you'll find us managing and securing their entities so they can employ more people, expand into new markets, improve their productivity and structure their businesses more efficiently.
We are hands on problem solvers with deep expertise who use the latest technology to help efficiently grow, control, simplify and transact your business.

PUBLISHED 100%

11/11/2021 277 1 [435.13 MB]

/ ROOT

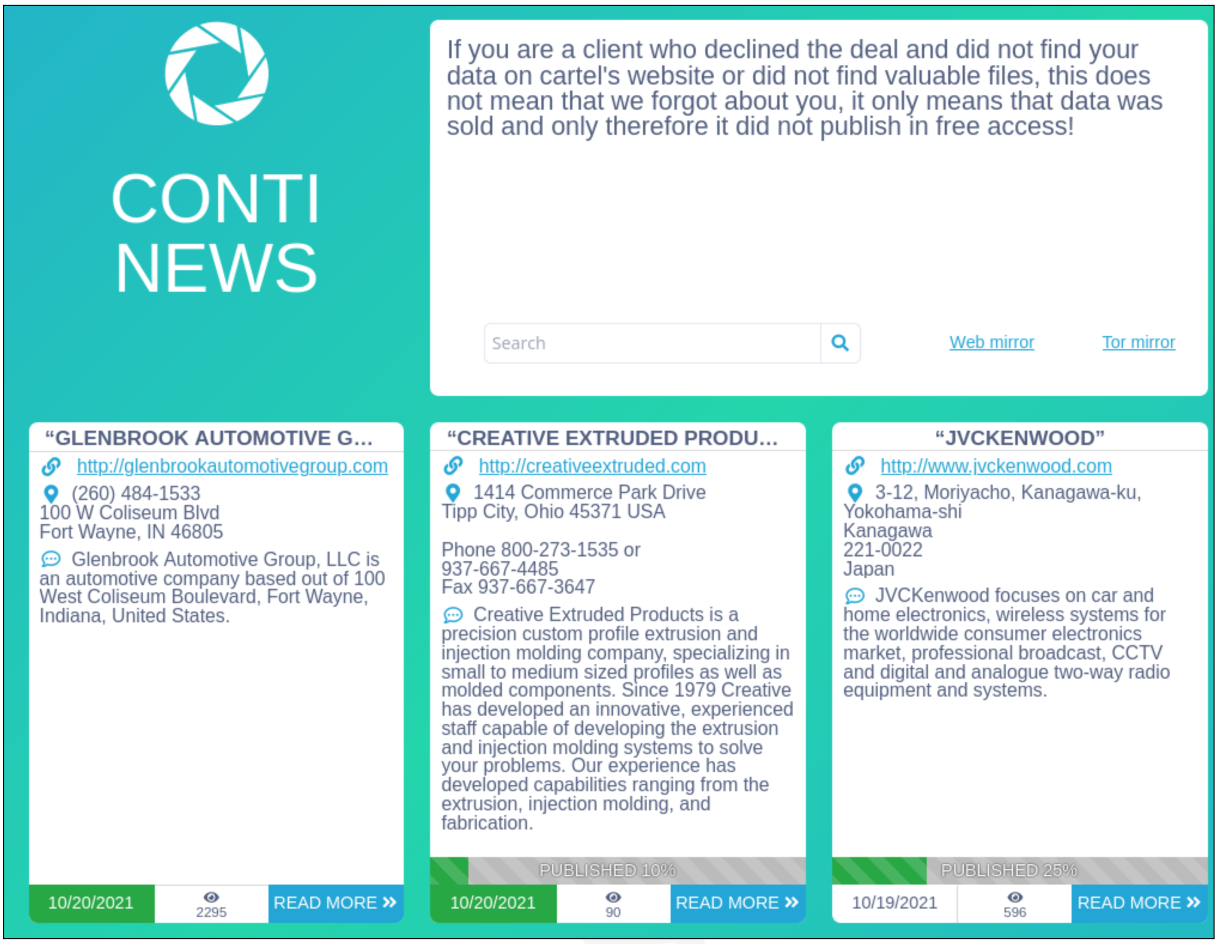
Work.rar 435.13 MB

nilbxxtm5mava3k2r5vzkuuu2g4bp5wlupo3nzry3c6q5rm5sti5ktqd.onion/ba7a063b/1dJC9xRy/Work.rar

Figure 2. **Conti's victim data download server**

Based on unofficial statistics, it appears that the number of companies affected by the Conti ransomware group is much higher than what we can see on just these websites. Expanding its scope of influence day by day, the Conti ransomware currently uses the RaaS affiliation model, enabling different threat actors to operate independently of one another. The Conti team is currently deploying a ransomware variant known as Conti v3.0 to victim systems, and development continues.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.



CONTI NEWS

If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

“GLENBROOK AUTOMOTIVE G...

http://glenbrookautomotivegroup.com

(260) 484-1533
100 W Coliseum Blvd
Fort Wayne, IN 46805

Glenbrook Automotive Group, LLC is an automotive company based out of 100 West Coliseum Boulevard, Fort Wayne, Indiana, United States.

10/20/2021 2295 READ MORE »

“CREATIVE EXTRUDED PRODU...

http://creativeextruded.com

1414 Commerce Park Drive
Tipp City, Ohio 45371 USA

Phone 800-273-1535 or
937-667-4485
Fax 937-667-3647

Creative Extruded Products is a precision custom profile extrusion and injection molding company, specializing in small to medium sized profiles as well as molded components. Since 1979 Creative has developed an innovative, experienced staff capable of developing the extrusion and injection molding systems to solve your problems. Our experience has developed capabilities ranging from the extrusion, injection molding, and fabrication.

PUBLISHED 10%

10/20/2021 90 READ MORE »

“JVCKENWOOD”

http://www.jvckenwood.com

3-12, Moriyacho, Kanagawa-ku,
Yokohama-shi
Kanagawa
221-0022
Japan

JVCKenwood focuses on car and home electronics, wireless systems for the worldwide consumer electronics market, professional broadcast, CCTV and digital and analogue two-way radio equipment and systems.

PUBLISHED 25%

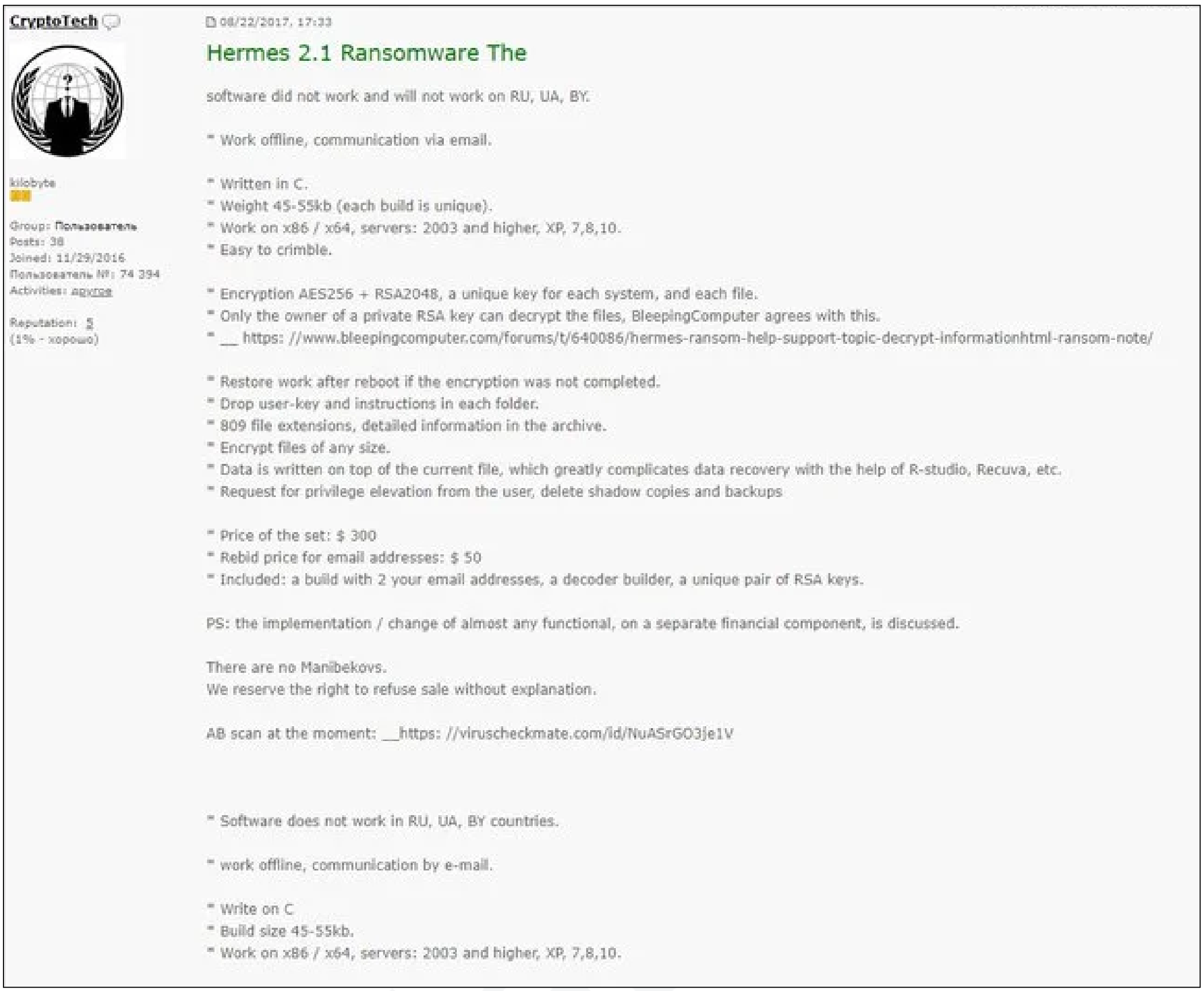
10/19/2021 596 READ MORE »

Figure 3. **Conti's extortion blog**

3.1.1 The Ryuk and Conti Connection

Based on an analysis made on ransomware samples and a comparison of bitcoin wallets used for receiving ransom payments, there is an undeniable connection between Conti and **Ryuk** ransomware teams. They may be the same team, or different teams that share members and resources with one another. The first examples of Ryuk were published on the **https://exploit.in/**, a well known underground cybercrime forum, under the name **Hermes** ransomware by a russian-speaking threat actor named **CryptoTech** in February 2017.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.



CryptoTech

kilobyte

Group: Пользователь
Posts: 38
Joined: 11/29/2016
Пользователь №: 74 394
Activities: другое

Reputation: 5
(1% - хорошо)

08/22/2017, 17:33

Hermes 2.1 Ransomware The

software did not work and will not work on RU, UA, BY.

" Work offline, communication via email.

" Written in C.
" Weight 45-55kb (each build is unique).
" Work on x86 / x64, servers: 2003 and higher, XP, 7,8,10.
" Easy to crimble.

" Encryption AES256 + RSA2048, a unique key for each system, and each file.
" Only the owner of a private RSA key can decrypt the files, BleepingComputer agrees with this.
" __ https: //www.bleepingcomputer.com/forums/t/640086/hermes-ransom-help-support-topic-decrypt-informationhtml-ransom-note/

" Restore work after reboot if the encryption was not completed.
" Drop user-key and instructions in each folder.
" 809 file extensions, detailed information in the archive.
" Encrypt files of any size.
" Data is written on top of the current file, which greatly complicates data recovery with the help of R-studio, Recuva, etc.
" Request for privilege elevation from the user, delete shadow copies and backups

" Price of the set: $ 300
" Rebid price for email addresses: $ 50
" Included: a build with 2 your email addresses, a decoder builder, a unique pair of RSA keys.

PS: the implementation / change of almost any functional, on a separate financial component, is discussed.

There are no Manibekovs.
We reserve the right to refuse sale without explanation.

AB scan at the moment: __https: //viruscheckmate.com/id/NuASrGO3je1V

" Software does not work in RU, UA, BY countries.

" work offline, communication by e-mail.

" Write on C
" Build size 45-55kb.
" Work on x86 / x64, servers: 2003 and higher, XP, 7,8,10.

Figure 4. CryptoTech's Hermes Share

Development of Hermes continued until version 2.1, which is released in August 2018. The threat actor replaced the name Hermes with "Ryuk" and begin advertising it for $300. Based on e-mail address data and similarities between forum submissions, it's overwhelmingly likely that the threat actor CryptoTech developed Ryuk.

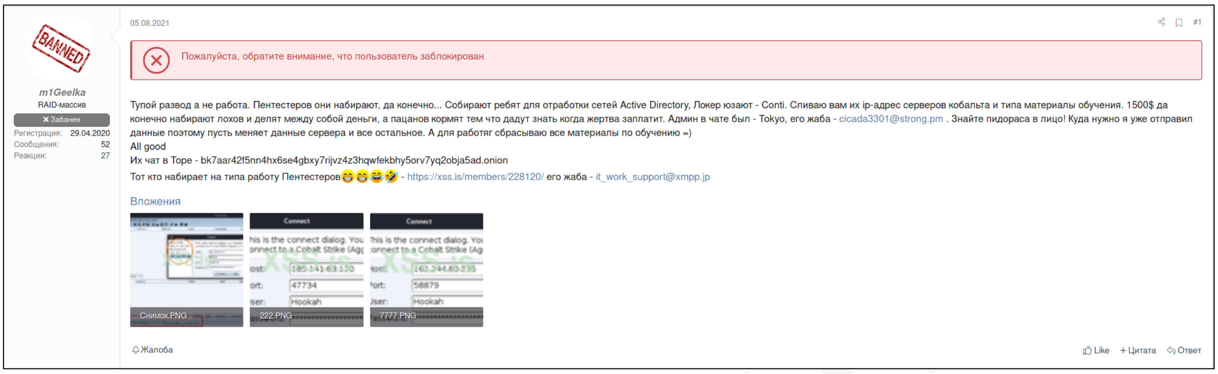
The Conti Ransomware can be understood as a continuation of Ryuk. The two ransomware tools share similarities in their libraries and the way they spread. They even share near perfect copy-pasted fragments of code. Both Conti and Ryuk rely on the same ransomware payload distributors : Trickbot, Emotet and BazarLoader. These are the software packages that do the work of actually delivering malicious ransomware files onto victim's networks.

At the beginning of 2021, ClearSkysec [3] analyzed bitcoin ransom transactions of Conti ransomware victims and revealed that they included a wallet address previously used by the Ryuk ransomware gang. This confirms the connection between Ryuk and Conti, which is now accepted as fact by the global threat intelligence community.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

3.1.2 Affiliate Leaks

The Conti group is currently working with an RaaS affiliate model and continues to recruit new members to the team. However, on **05.08.2021** the Conti team suffered a data leak which exposed internal documents, guides, training materials, and much more. This situation is common inside the cybercriminal industry, especially among organizations that use the affiliate business model. A user named **m1Geelka** shared information about the groups leader and his assistant in a thread on the on the *xss.is* cybercrime forum, claiming that the group treated him unfairly in regards to money.



m1Geelka
RAID-массив
✕ Забанен
Регистрация: 29.04.2020
Сообщения: 52
Реакции: 27

05.08.2021 #1

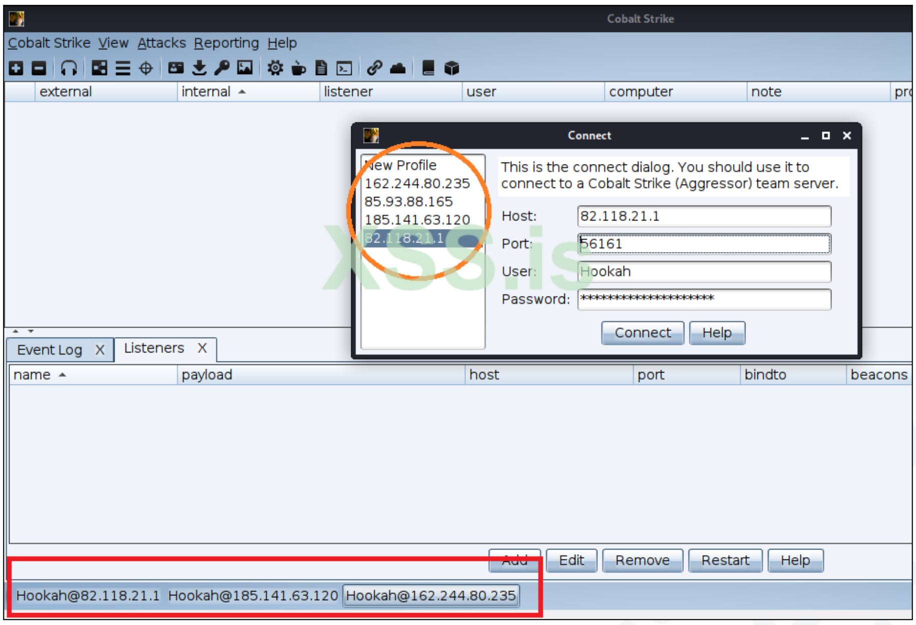
Пожалуйста, обратите внимание, что пользователь заблокирован

Тупой развод а не работа. Пентестеров они набирают, да конечно... Собирают ребят для отработки сетей Active Directory, Локер юзают - Conti. Сливаю вам их ip-адрес серверов кобальта и типа материалы обучения. 1500$ да конечно набирают лохов и делят между собой деньги, а пацанов кормят тем что дадут знать когда жертва заплатит. Админ в чате был - Tokyo, его жаба - cicada3301@strong.pm . Знайте пидораса в лицо! Куда нужно я уже отправил данные поэтому пусть меняет данные сервера и все остальное. А для работяг сбрасываю все материалы по обучению =)
All good
Их чат в Торе - bk7aar42f5nn4hx6se4gbxy7rijvz4z3hqwfekbhy5orv7yq2objа5ad.onion
Тот кто набирает на типа работу Пентестеров😁😁😂🤣 - https://xss.is/members/228120/ его жаба - it_work_support@xmpp.jp

Вложения

Figure 5. **Affiliate Leak Post**

Afterwards, m1Geelka uploaded a large cache of Conti group-related data, including training materials used by the affiliates, and shared the link to the group's **SendSpace** file-sharing site in the same post. This data contains a high volume of tactical information about Conti, and valuable intelligence about the operations of the threat actors responsible, such as images of the CobaltStrike servers that the Conti group actively uses.



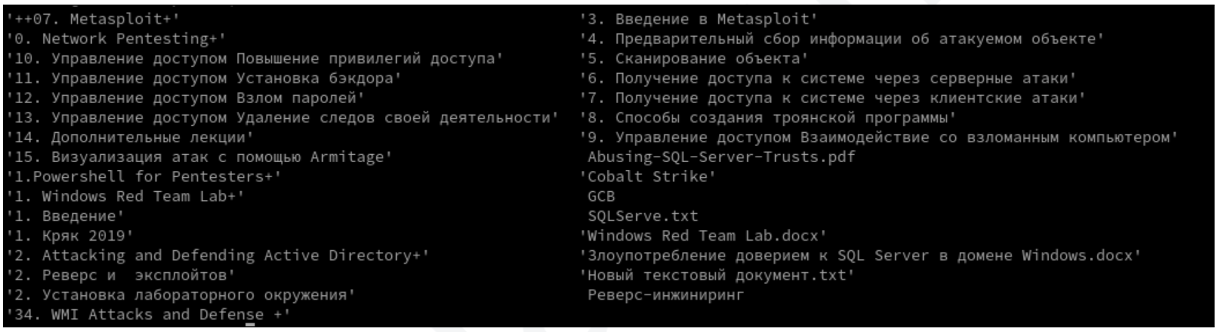
New Profile
162.244.80.235
85.93.88.165
185.141.63.120
82.118.21.1

This is the connect dialog. You should use it to connect to a Cobalt Strike (Aggressor) team server.

Host: 82.118.21.1
Port: 56161
User: Hookah
Password: ********************

Hookah@82.118.21.1 Hookah@185.141.63.120 Hookah@162.244.80.235

Figure 6. Cobaltstrike Servers Leak



```
'++07. Metasploit+'                                            '3. Введение в Metasploit'
'0. Network Pentesting+'                                       '4. Предварительный сбор информации об атакуемом объекте'
'10. Управление доступом Повышение привилегий доступа'         '5. Сканирование объекта'
'11. Управление доступом Установка бэкдора'                    '6. Получение доступа к системе через серверные атаки'
'12. Управление доступом Взлом паролей'                        '7. Получение доступа к системе через клиентские атаки'
'13. Управление доступом Удаление следов своей деятельности'   '8. Способы создания троянской программы'
'14. Дополнительные лекции'                                    '9. Управление доступом Взаимодействие со взломанным компьютером'
'15. Визуализация атак с помощью Armitage'                      Abusing-SQL-Server-Trusts.pdf
'1.Powershell for Pentesters+'                                 'Cobalt Strike'
'1. Windows Red Team Lab+'                                      GCB
'1. Введение'                                                   SQLServe.txt
'1. Кряк 2019'                                                 'Windows Red Team Lab.docx'
'2. Attacking and Defending Active Directory+'                 'Злоупотребление доверием к SQL Server в домене Windows.docx'
'2. Реверс и  эксплойтов'                                      'Новый текстовый документ.txt'
'2. Установка лабораторного окружения'                          Реверс-инжиниринг
'34. WMI Attacks and Defense +'
```

Figure 7. Conti Educational Materials for Affiliates

This list of topics was included inside the leaked training materials :

- How to build a Cobalt Strike executable
- An introduction to avoiding security products using compiler-based obfuscation techniques.
- A tutorial on using rclone to pull victim data to secure cloud storage accounts on MEGA.
- How to establish a remote connection to the victim's network and gain persistence using AnyDesk and Atera.
- How to connect to hacked networks with RDP using Ngrok secure tunnel.
- A guide to performing SMB brute-force attacks.
- A tutorial on operating system and anonymizing internet traffic via Tor network.
- A how-to on privilege escalation and gaining administrative rights inside a target network.

It's important to note that many of these technologies are readily available software products with legitimate commercial use cases, and that cybercriminals are abusing these technologies to attack victims :

- Cobalt Strike is a commercial, full-featured, remote access tool frequently used in cybersecurity event simulations.
- rclone is a command-line program that helps users manage cloud data storage using code.
- AnyDesk and Atera are commercial remote desktop applications that provide platform-independent remote access to personal computers and other devices.
- ngrok generates an interface where users can introspect all HTTP traffic running over specified tunnels in real-time.
- Tor is an open-source web browser designed for secure, anonymous communication.

3.2 The Conti Attack Kill Chain

Conti ransomware is constantly changing its attack pattern on a daily basis. It relies on up-to-date security exploits such as PrintNightmare[7] and FortiGate[10], which are known exploits with official patches available. However, many users still have not downloaded the appropriate patches and remain vulnerable.

- **PrintNightmare (CVE-2021-1675, CVE-2021-34527, and CVE-2021-36958)** works by escalating the Windows Print Spooler service permissions to executive privileged operations. An attacker can use this exploit to install programs ; view, change, or delete data ; or create new accounts with full user rights.
- **FortiGate firewall remote code execution (CVE-2018-13379 and CVE-2018-13374)** is a buffer underwrite vulnerability that impacts Fortigate VPN servers to gain access to enterprise networks.

Conti knows that many users don't update their security patches very frequently. Its affiliates count on users waiting for days or even weeks before downloading and running security patches. With a highly automated RaaS business model like the one Conti uses, it's possible for attackers to compromise unpatched systems mere hours after patches get released.

In the following sections, each step of the overall Conti attack kill chain will be explained, including every technique, tactic, and procedure that Conti affiliates use to attack their victims. Since Conti is a RaaS platform, every individual attack may use unique vectors and exhibit unique behaviour – there is no one-size-fits-all Conti ransomware attack variant.

3.2.1 Target Selection

Since the RaaS service model gives affiliates a great deal of flexibility over how they choose to operate, Conti affiliates use a wide range of target selection methods. These include :

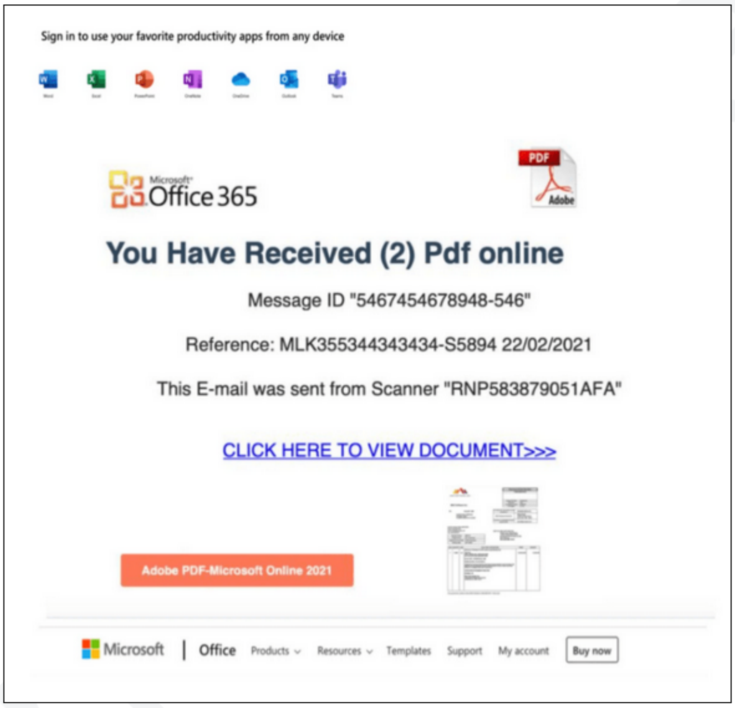
- Email phishing
- Mass vulnerability scanning
- High-end malware distribution software
- Credential stuffing
- Fake websites, impersonated phone calls, and similar social engineering tactics.

Of these target selection methods, email phishing is by far the most common. Another common method used by Conti affiliates is mass vulnerability scanning, which relies on automated bots checking publicly exposed networks for known vulnerabilities. We have also seen Conti affiliates using high-end Malware-as-a-Service technologies such as Trickbot, Emotet, and BazarLoader for distributing Conti ransomware.

3.2.2 Deployment and Execution

In the example our team analyzed for this report, the attack kill chain begins with a phishing campaign that installs the **BazarLoader** backdoor onto target systems.

Phishing campaigns often take advantage of Microsoft Office and Google Doc links, send via email. Attackers use these links to redirect victims to malicious sites where they download the BazarLoader[6] payload. At this point, the reconnaissance phase begins. The ransomware will try to discover all directories and network shares inside the victim's system and expand throughout.



Sign in to use your favorite productivity apps from any device

You Have Received (2) Pdf online

Message ID "5467454678948-546"

Reference: MLK355344343434-S5894 22/02/2021

This E-mail was sent from Scanner "RNP583879051AFA"

CLICK HERE TO VIEW DOCUMENT>>>

Figure 8. Bazarloader phishing page

Based on forensic investigations on multiple Conti victims, our Team observed that before launching Conti ransomware, attackers often try to identify mission-critical systems like domain controllers or backup servers. If they can find these systems early on, they can trigger the next phase of the attack faster.

Once discovery and reconnaissance is complete, the data exfiltration phase begins. Conti attackers evaluate the data inside the victim's system and decide whether it is important for the target company. If the data is important enough, attackers will start exfiltrating data to an anonymous account on the cloud-based anonymous file upload service called MEGA.

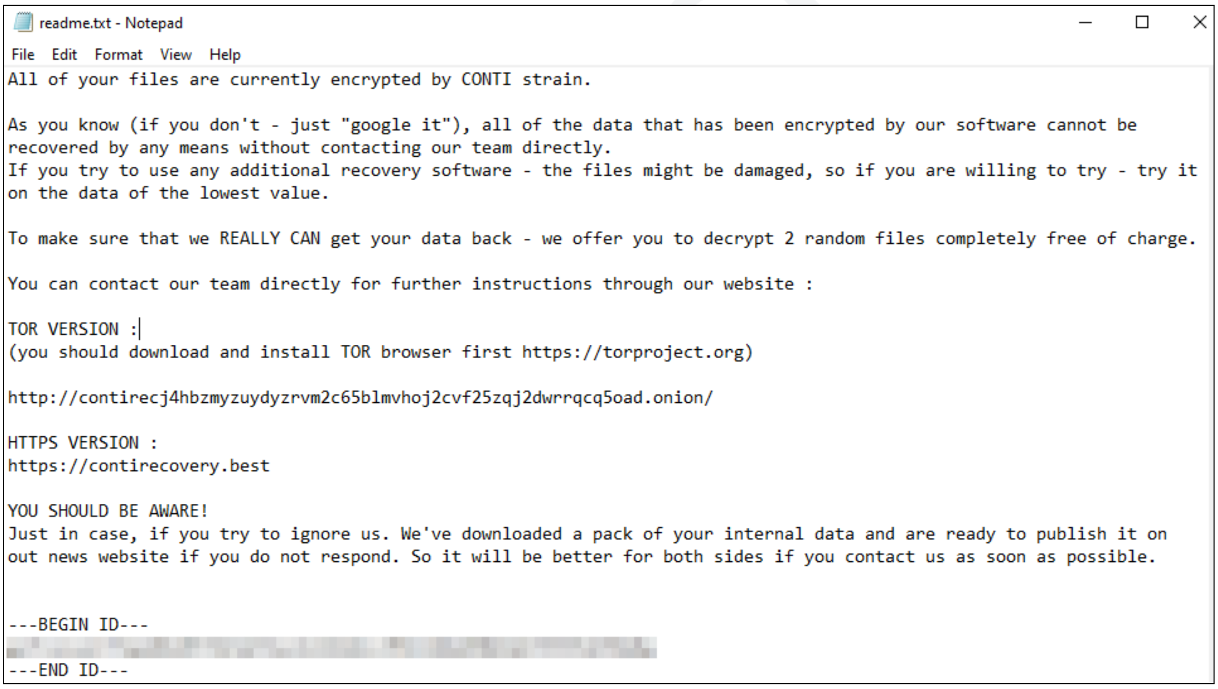
The tool attackers use to do this is called "rclone".

Once the first two stages are complete, Conti begins encrypting all files and backups in the target system, including accessible network devices. The Conti ransomware uses **ChaCha8** encryption with randomly generated keys for each file inside the target system. Every generated key is encrypted with a RSA-4096 public key and stored at a specific offset of each file. These keys are used to identify the victim, manage negotiation, and eventually generate decryption codes upon payment.

3.2.3 Demand and Negotiation

At the end of the ransomware execution phase, all important files of the victims are encrypted, backups are deleted and a **readme.txt** file containing the ransom note is dropped on the target system desktop. The Conti group uses two different ransom note formats.

The first ransom note directs victims to **https://contirecovery.best/** and **http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/** websites, which contain instructions for purchasing decryption keys from Conti affiliate attackers. The ransom note also contains instructions about installing the TOR browser in order to access the Conti group's hidden web service.

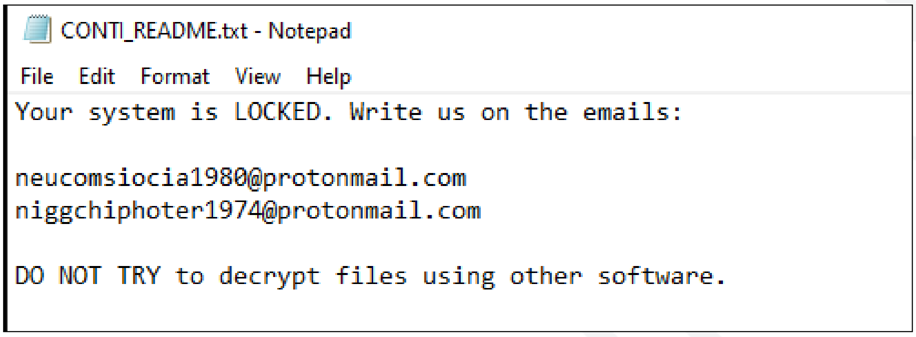


```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be
recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it
on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :
https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on
out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
[redacted]
---END ID---
```

Figure 9. **Conti ransom note inside the victim system**

There is a unique victim ID value at the end of this ransom note (readme.txt). It is the string enclosed with **—BEGIN ID—** and **—END ID—** delimiters. Victims are expected to upload their ransom note to the Conti's recovery service website. Once a victim uploads a valid ransom note, the website sends them to a chat page for negotiating with the affiliates. This type of ransom note format carries data leakage risks for companies. The victim IDs are hard-coded in the ransomware itself. This means that whenever malicious files are uploaded to any malware service, or the IDs get leaked, the chat becomes accessible to anyone.

The second ransom note includes one or two Protonmail accounts. Victims are expected to send their company information to those Protonmail mailboxes, which are operated by Conti affiliates. Victims are recognized by victim-specific Protonmails here, just like the victim IDs produced in the first example.

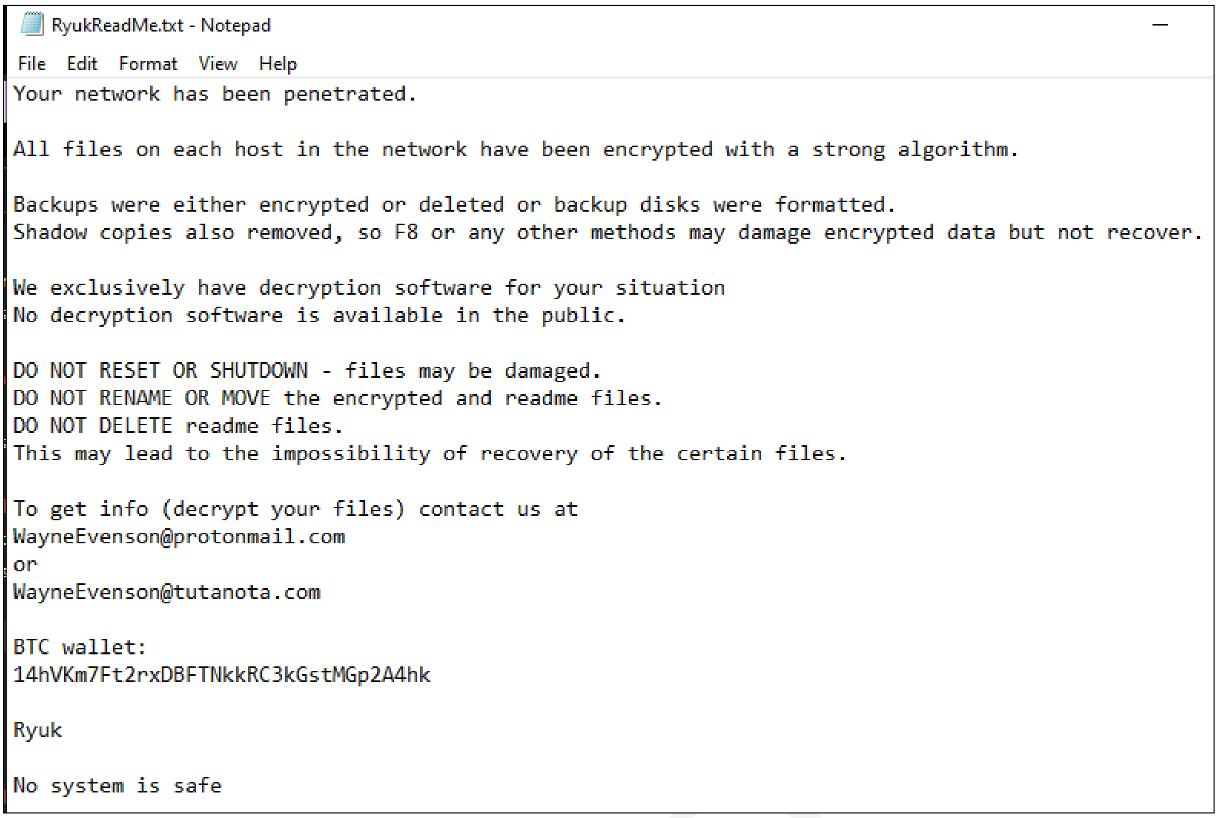


```
Your system is LOCKED. Write us on the emails:

neucomsiocia1980@protonmail.com
niggchiphoter1974@protonmail.com

DO NOT TRY to decrypt files using other software.
```

Figure 10. Conti ransom note with e-mails

As stated in 3.1, there are many similarities between Ryuk's ransomware and Conti's. This is particularly evident when comparing Conti and Ryuk ransom notes. Both ransoms use a similar structure. There are victim-specific e-mail addresses created with Protonmail and a BTC wallet in both examples[2].

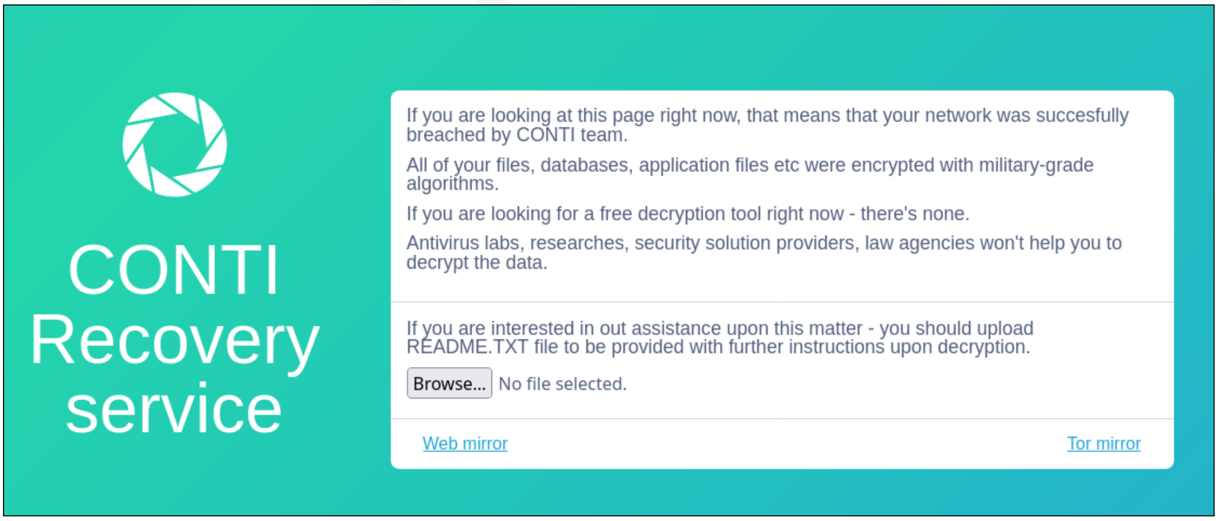
DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
WayneEvenson@protonmail.com
or
WayneEvenson@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk

No system is safe
```

Figure 11. **Ryuk ransom note**

Once the unique ID is uploaded to Conti's recovery system, it directs victims to a login page. On the login page, affiliates request the victim's names and e-mail addresses. Once they have this information, the web service provides a chat page with a standard greeting message (Figure 1).



CONTI Recovery service

If you are looking at this page right now, that means that your network was succesfully breached by CONTI team.

All of your files, databases, application files etc were encrypted with military-grade algorithms.

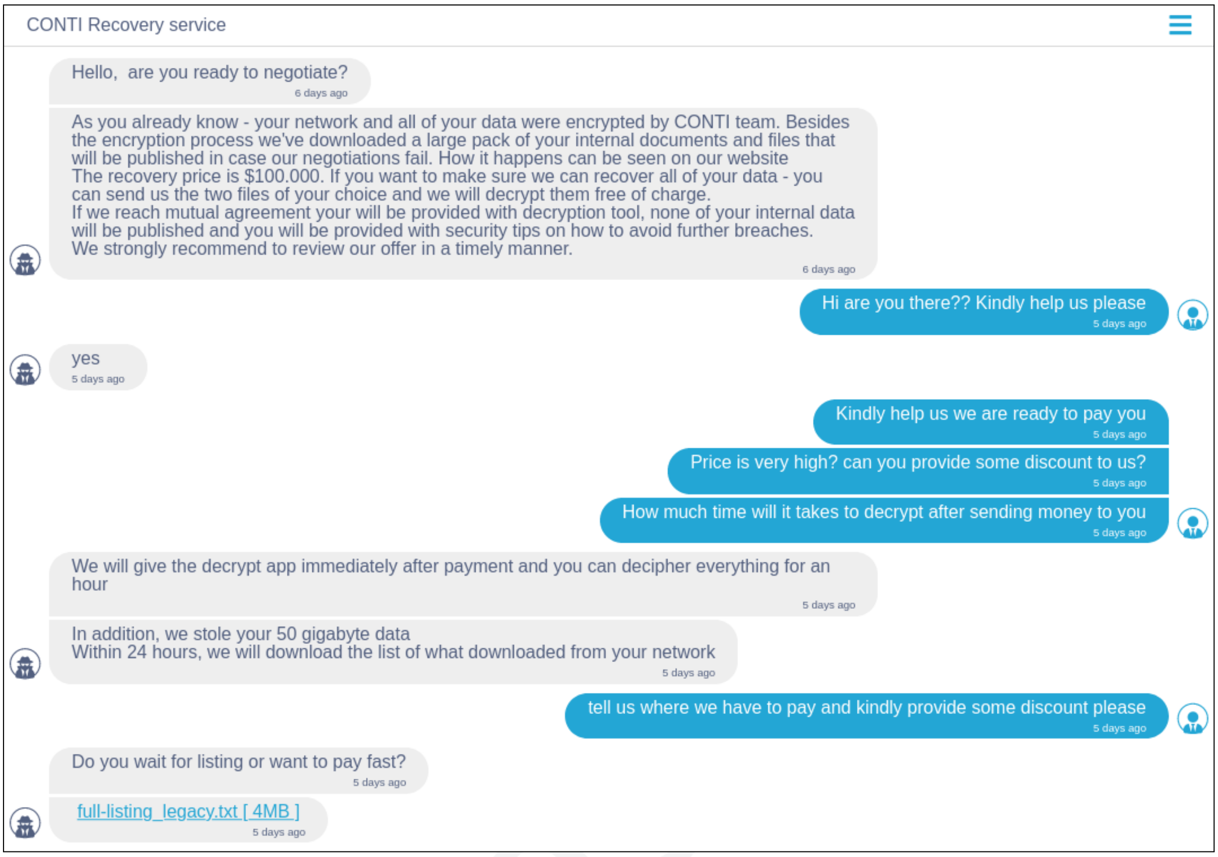
If you are looking for a free decryption tool right now - there's none.

Antivirus labs, researches, security solution providers, law agencies won't help you to decrypt the data.

If you are interested in out assistance upon this matter - you should upload README.TXT file to be provided with further instructions upon decryption.

Figure 12. **Conti main page**

At this stage, affiliates send the total captured file size and enumerated system information to the user. This proves that the data has indeed been compromised.



CONTI Recovery service

Hello, are you ready to negotiate?
6 days ago

As you already know - your network and all of your data were encrypted by CONTI team. Besides the encryption process we've downloaded a large pack of your internal documents and files that will be published in case our negotiations fail. How it happens can be seen on our website
The recovery price is $100.000. If you want to make sure we can recover all of your data - you can send us the two files of your choice and we will decrypt them free of charge.
If we reach mutual agreement your will be provided with decryption tool, none of your internal data will be published and you will be provided with security tips on how to avoid further breaches.
We strongly recommend to review our offer in a timely manner.
6 days ago

Hi are you there?? Kindly help us please
5 days ago

yes
5 days ago

Kindly help us we are ready to pay you
5 days ago

Price is very high? can you provide some discount to us?
5 days ago

How much time will it takes to decrypt after sending money to you
5 days ago

We will give the decrypt app immediately after payment and you can decipher everything for an hour
5 days ago

In addition, we stole your 50 gigabyte data
Within 24 hours, we will download the list of what downloaded from your network
5 days ago

tell us where we have to pay and kindly provide some discount please
5 days ago

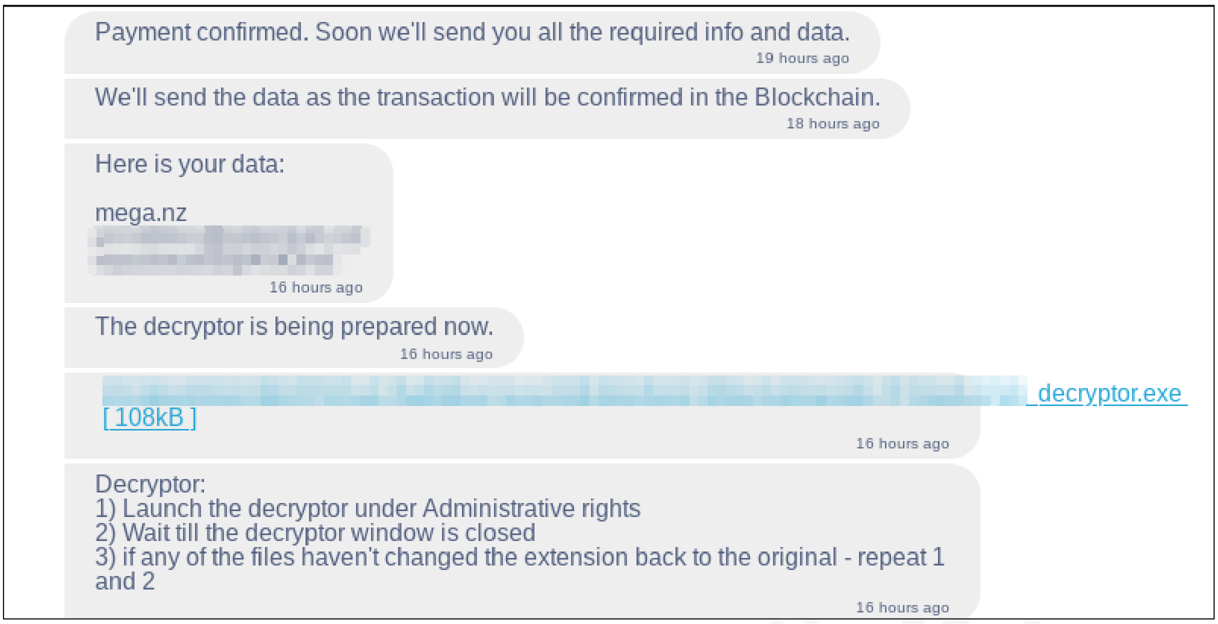
Do you wait for listing or want to pay fast?
5 days ago

full-listing_legacy.txt [4MB]
5 days ago

Figure 13. Victim system information messages

At this point, if the attacker and victim reach an agreement, the victim sends bitcoin to the designated address and the attacker produces a decryption key using the victim's ID. However, we have found evidence that some Conti affiliates simply take the money and disappear, refusing to provide the decryption key as promised. If the attacker sends the decryption key to the victim, the link includes a user manual 14 that shows how to use the decryption application. All information retrieved from the victim's systems is uploaded to a free file sharing site where it can be deleted, and that system data is shared with the victim.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.



Payment confirmed. Soon we'll send you all the required info and data.
19 hours ago

We'll send the data as the transaction will be confirmed in the Blockchain.
18 hours ago

Here is your data:

mega.nz
[redacted]
16 hours ago

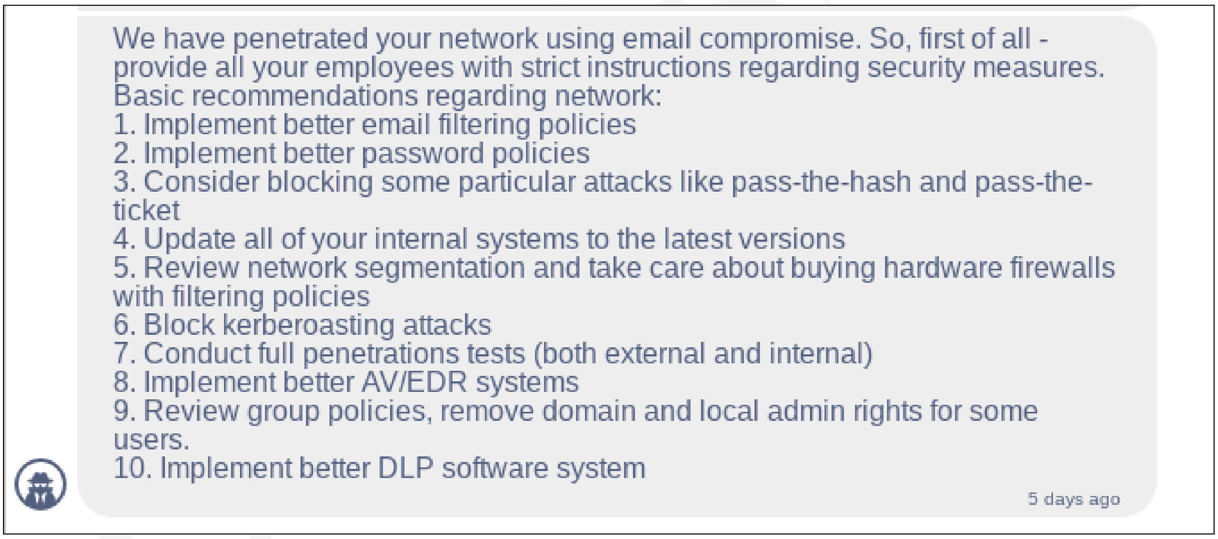
The decryptor is being prepared now.
16 hours ago

[redacted]_decryptor.exe [108kB]
16 hours ago

Decryptor:
1) Launch the decryptor under Administrative rights
2) Wait till the decryptor window is closed
3) if any of the files haven't changed the extension back to the original - repeat 1 and 2
16 hours ago

Figure 14. **Post-agreement messages**

Conti affiliates will also send recommendation messages 15 telling victims how to protect against future attacks.



We have penetrated your network using email compromise. So, first of all - provide all your employees with strict instructions regarding security measures.
Basic recommendations regarding network:
1. Implement better email filtering policies
2. Implement better password policies
3. Consider blocking some particular attacks like pass-the-hash and pass-the-ticket
4. Update all of your internal systems to the latest versions
5. Review network segmentation and take care about buying hardware firewalls with filtering policies
6. Block kerberoasting attacks
7. Conduct full penetrations tests (both external and internal)
8. Implement better AV/EDR systems
9. Review group policies, remove domain and local admin rights for some users.
10. Implement better DLP software system
5 days ago

Figure 15. **Recommendation message**

3.3 Management Panel

The PTI Team successfully gained access to several parts of Conti's RaaS infrastructure. This gave us cutting-edge insight into the way Conti manages its affiliates and ransomware technology.

We gained access to a victim landing page (recovery service) and an admin management panel hosted as a TOR hidden service on this address : **http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/**.

We located the subject management panel as well **/adminbdpm6p47p2ye3k5f.php**, which is mainly used for managing victims, affiliate accounts, and uploaded files.

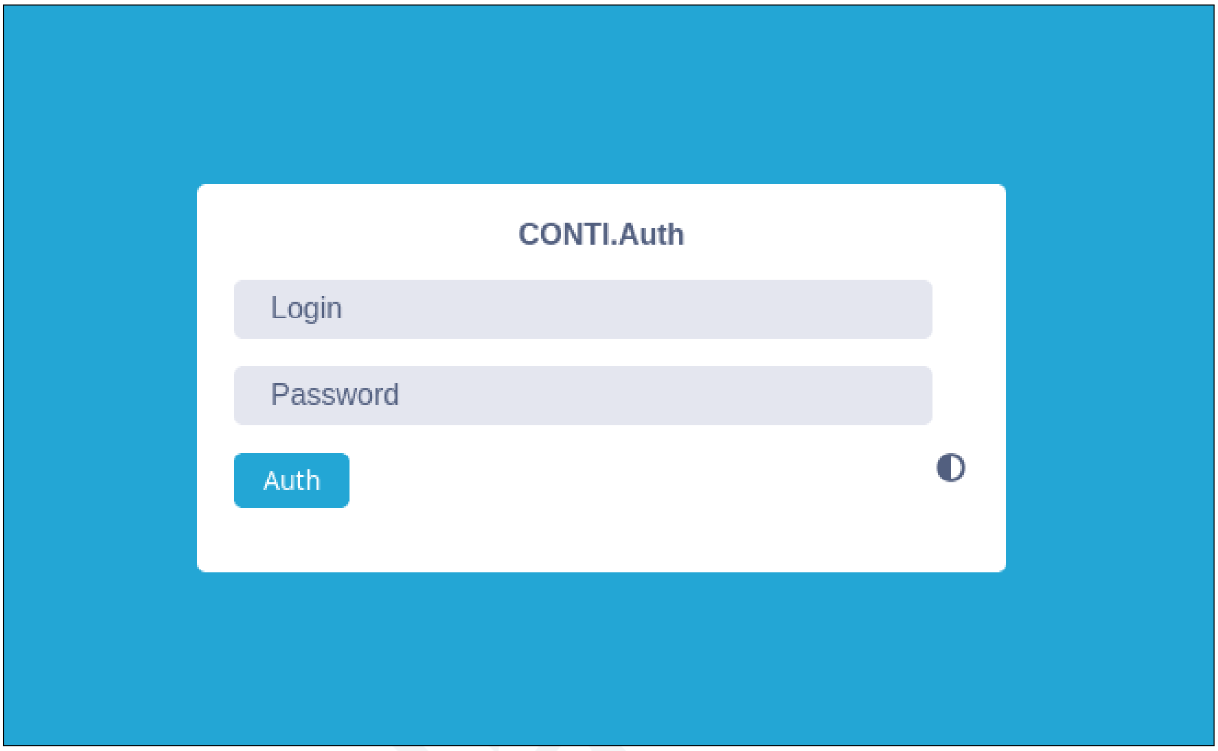
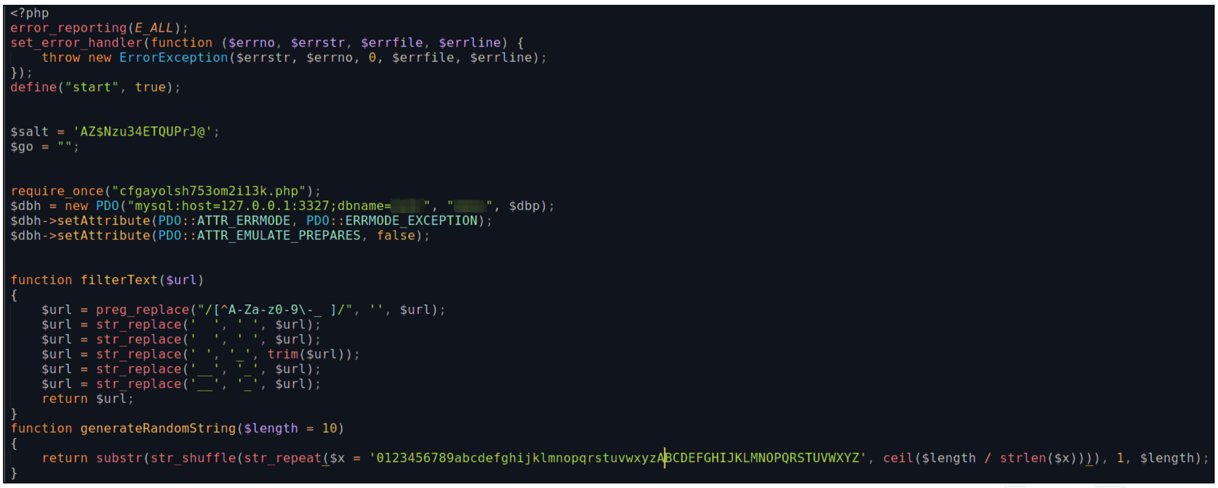


Figure 16. **Conti admin panel login page**

Our threat intelligence team was also able to access a hidden service that provided key information on the underlying technology stack Conti developers rely on. By analyzing the source code of Conti's recovery service and admin management panel, our team discovered a hidden service using dockerized MySql database bound to **127.0.0.1:3327**.

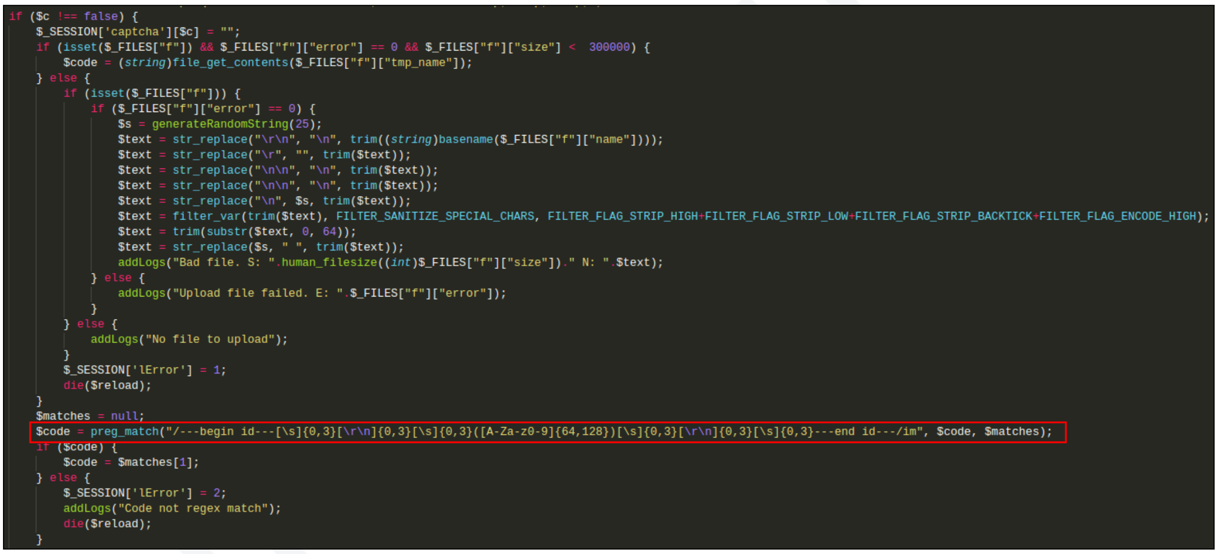
DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.



```php
<?php
error_reporting(E_ALL);
set_error_handler(function ($errno, $errstr, $errfile, $errline) {
    throw new ErrorException($errstr, $errno, 0, $errfile, $errline);
});
define("start", true);


$salt = 'AZ$Nzu34ETQUPrJ@';
$go = "";


require_once("cfgayolsh753om2i13k.php");
$dbh = new PDO("mysql:host=127.0.0.1:3327;dbname=[redacted]", "[redacted]", $dbp);
$dbh->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
$dbh->setAttribute(PDO::ATTR_EMULATE_PREPARES, false);


function filterText($url)
{
    $url = preg_replace("/[^A-Za-z0-9\-_ ]/", '', $url);
    $url = str_replace('  ', ' ', $url);
    $url = str_replace('  ', ' ', $url);
    $url = str_replace(' ', '_', trim($url));
    $url = str_replace('__', '_', $url);
    $url = str_replace('__', '_', $url);
    return $url;
}
function generateRandomString($length = 10)
{
    return substr(str_shuffle(str_repeat($x = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ', ceil($length / strlen($x)))), 1, $length);
}
```

Figure 17. **Conti admin panel source code**

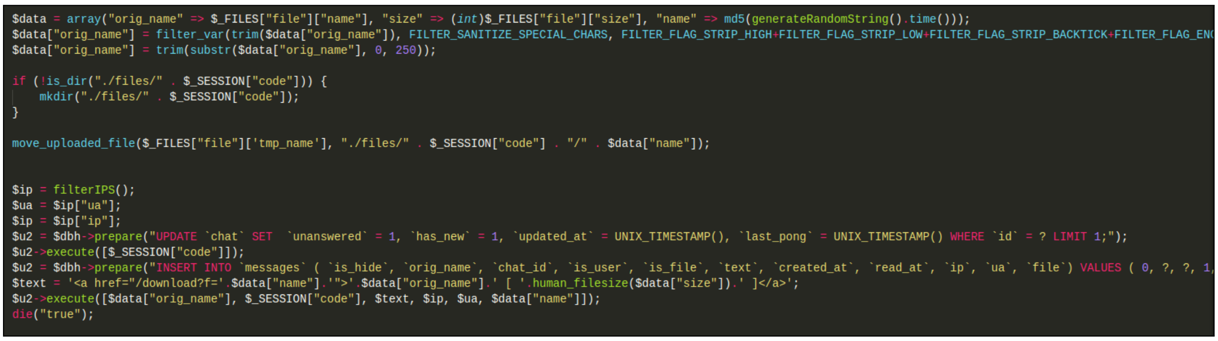
The victim recovery service panel contains a submit button, where victims are supposed to upload the readme.txt files created on their devices. We've highlighted the regex pattern that detects the victim-specific ID in the figure below,18.



```php
if ($c !== false) {
    $_SESSION['captcha'][$c] = "";
    if (isset($_FILES["f"]) && $_FILES["f"]["error"] == 0 && $_FILES["f"]["size"] <  300000) {
        $code = (string)file_get_contents($_FILES["f"]["tmp_name"]);
    } else {
        if (isset($_FILES["f"])) {
            if ($_FILES["f"]["error"] == 0) {
                $s = generateRandomString(25);
                $text = str_replace("\r\n", "\n", trim((string)basename($_FILES["f"]["name"])));
                $text = str_replace("\r", "", trim($text));
                $text = str_replace("\n\n", "\n", trim($text));
                $text = str_replace("\n\n", "\n", trim($text));
                $text = str_replace("\n", $s, trim($text));
                $text = filter_var(trim($text), FILTER_SANITIZE_SPECIAL_CHARS, FILTER_FLAG_STRIP_HIGH+FILTER_FLAG_STRIP_LOW+FILTER_FLAG_STRIP_BACKTICK+FILTER_FLAG_ENCODE_HIGH);
                $text = trim(substr($text, 0, 64));
                $text = str_replace($s, " ", trim($text));
                addLogs("Bad file. S: ".human_filesize((int)$_FILES["f"]["size"])." N: ".$text);
            } else {
                addLogs("Upload file failed. E: ".$_FILES["f"]["error"]);
            }
        } else {
            addLogs("No file to upload");
        }
        $_SESSION['lError'] = 1;
        die($reload);
    }
    $matches = null;
    $code = preg_match("/---begin id---[\s]{0,3}[\r\n]{0,3}[\s]{0,3}([A-Za-z0-9]{64,128})[\s]{0,3}[\r\n]{0,3}[\s]{0,3}---end id---/im", $code, $matches);
    if ($code) {
        $code = $matches[1];
    } else {
        $_SESSION['lError'] = 2;
        addLogs("Code not regex match");
        die($reload);
    }
```

Figure 18. **Recovery service readme.txt parser code**

As the following image shows 19, every uploaded file is stored under the /**files**/ directory, with a unique name and following format : **MD5(current_time+random_string)**, which prevents file name brute force attacks.



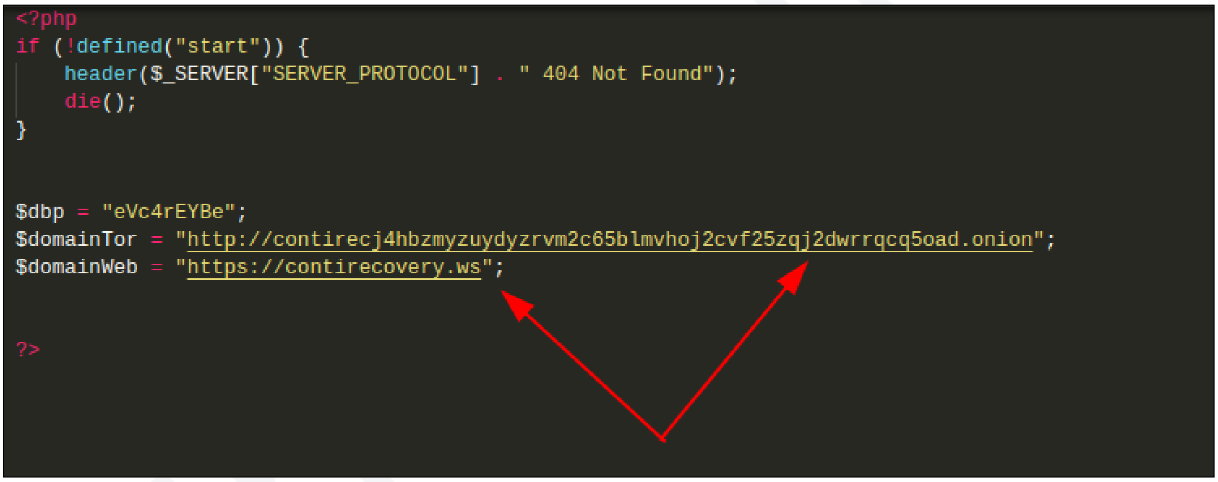
```
$data = array("orig_name" => $_FILES["file"]["name"], "size" => (int)$_FILES["file"]["size"], "name" => md5(generateRandomString().time()));
$data["orig_name"] = filter_var(trim($data["orig_name"]), FILTER_SANITIZE_SPECIAL_CHARS, FILTER_FLAG_STRIP_HIGH+FILTER_FLAG_STRIP_LOW+FILTER_FLAG_STRIP_BACKTICK+FILTER_FLAG_ENC
$data["orig_name"] = trim(substr($data["orig_name"], 0, 250));

if (!is_dir("./files/" . $_SESSION["code"])) {
    mkdir("./files/" . $_SESSION["code"]);
}

move_uploaded_file($_FILES["file"]['tmp_name'], "./files/" . $_SESSION["code"] . "/" . $data["name"]);


$ip = filterIPS();
$ua = $ip["ua"];
$ip = $ip["ip"];
$u2 = $dbh->prepare("UPDATE `chat` SET  `unanswered` = 1, `has_new` = 1, `updated_at` = UNIX_TIMESTAMP(), `last_pong` = UNIX_TIMESTAMP() WHERE `id` = ? LIMIT 1;");
$u2->execute([$_SESSION["code"]]);
$u2 = $dbh->prepare("INSERT INTO `messages` ( `is_hide`, `orig_name`, `chat_id`, `is_user`, `is_file`, `text`, `created_at`, `read_at`, `ip`, `ua`, `file`) VALUES ( 0, ?, ?, 1,
$text = '<a href="/download?f='.$data["name"].'">'.$data["orig_name"].' [ '.human_filesize($data["size"]).' ]</a>';
$u2->execute([$data["orig_name"], $_SESSION["code"], $text, $ip, $ua, $data["name"]]);
die("true");
```

Figure 19. **Uploaded content hiding**

3.4 De-Anonymization

One of the main objectives of our investigation was revealing the identity of the Conti affiliates, retailers, developers and servers. Our management panel analysis revealed a great deal of information regarding the servers that this group uses.

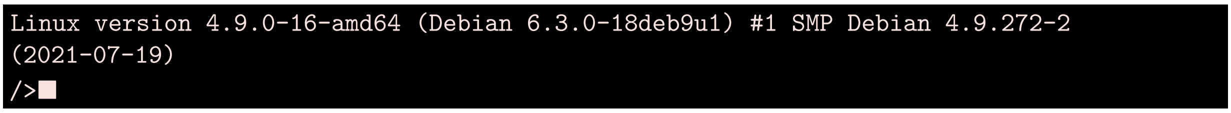
One of the most valuable pieces of threat intelligence we discovered is the the real IP address of Conti's TOR hidden service and **contirecovery.ws**, and **217.12.204.135**, on **Tuesday, 28 September 2021 21:30:03 UTC**.



```
<?php
if (!defined("start")) {
    header($_SERVER["SERVER_PROTOCOL"] . " 404 Not Found");
    die();
}


$dbp = "eVc4rEYBe";
$domainTor = "http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion";
$domainWeb = "https://contirecovery.ws";


?>
```

Figure 20. **Domain definitions inside the Conti recovery service source code.**

Additionaly, our team was able to identify the operating system details of the server hosting the TOR hidden service for Conti. The host is a Debian server with host name "dedic-cuprum-617836". We believe the numeric value at the end of the host name is an invoice number for the server, assigned by the hosting company **ITLDC**.



```
Linux version 4.9.0-16-amd64 (Debian 6.3.0-18deb9u1) #1 SMP Debian 4.9.272-2
(2021-07-19)
/>█
```

Console 1. OS Details of the Conti onion server (uname -a)

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

```
217.12.204.135 dedic-cuprum-617836.hosted-by-itldc.com dedic-cuprum-617836
/>█
```

Console 2. Hostname Details of the Conti onion server (/etc/hosts)

The captured IP address with the corresponding timestamp have been shared with law enforcement authorities for further legal action against the Conti group and its affiliates.

The next image shows the contents of **htpasswd** file of the subject host. The password hash can be used by other researchers in future Conti investigations.

```
user:$apr1$7F5MK3J3$/JX4zqKicgXi3hXS57OWZ/
/>█
```

Console 3. Htpasswd file of the Conti onion server

Throughout the analysis phase, our team constantly monitored network traffic entering and leaving Conti's recovery servers. This information will improve anti-ransomware software and lead to more effective filtering and blacklisting of Conti-related traffic. We found the following IP addresses communicating with the subject Conti server.

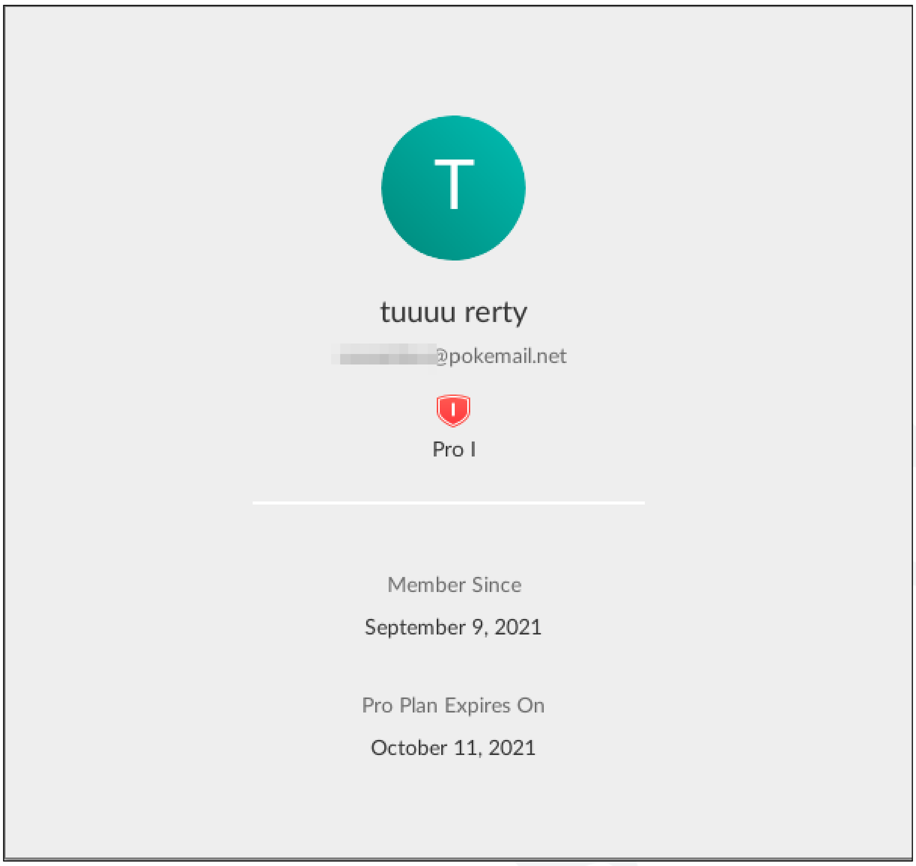
- 1.177.172.158
- 104.244.76.44
- 122.51.149.86
- 176.9.1.211
- 176.9.98.228
- 18.27.197.252
- 185.130.44.108
- 185.220.103.4
- 2.82.175.32
- 217.160.251.63
- 218.92.0.211
- 45.153.160.134
- 46.101.236.25
- 49.234.143.71
- 51.75.171.136
- 54.36.108.162
- 6.11.76.81
- 61.177.172.158
- 64.113.32.29
- 66.211.197.38

User	Connect With	Connected From	Login Date (GMT+3)	Login Activity
root	pts/0	89.163.249.244	Wed Nov 10 14:11 - gone	no logout
root	pts/0	107.189.31.241	Wed Nov 10 09:09 - 09:10	(00:01)
root	pts/0	185.220.103.5	Mon Oct 25 15:08 - 15:50	(00:42)
root	pts/0	192.42.116.25	Fri Oct 15 20:25 - 20:28	(00:03)
root	pts/0	18.27.197.252	Mon Oct 4 17:47 - 17:47	(00:00)
root	pts/0	45.153.160.134	Mon Sep 27 14:12 - 14:18	(00:05)
root	pts/0	185.220.103.4	Mon Sep 27 09:10 - 09:13	(00:03)
root	pts/0	185.130.44.108	Thu Sep 23 21:08 - 21:26	(00:18)
root	pts/3	104.244.76.44	Thu Sep 23 08:04 - 08:04	(00:00)
root	pts/2	104.244.76.44	Thu Sep 23 08:01 - 13:02	(05:01)
root	pts/0	64.113.32.29	Wed Sep 22 13:46 - 15:40	(1+01:54)
root	pts/0	54.36.108.162	Wed Sep 22 12:54 - 13:10	(00:16)

Table 1. Conti Hidden Server SSH Connections

By analyzing the IP addresses communicated with Conti servers, we discovered that most of the connections originate from TOR exit nodes. Two of the IP addresses **176.9.1.211:9001** and **217.160.251.63:29001** are constantly connected to the Conti server, which could indicate that these are TOR entry nodes used for Conti's hidden recovery service.

During this phase of the investigation, the PTI team discovered multiple victim chat sessions and captured login credentials for MEGA accounts used when extorting victims' data. Our team has revealed the connecting IP addresses, dates, the purchase method, and the software used for accessing the file sharing and upload service.



T

tuuuu rerty

[redacted]@pokemail.net

Pro I

Member Since

September 9, 2021

Pro Plan Expires On

October 11, 2021

Figure 21. **Mega account**

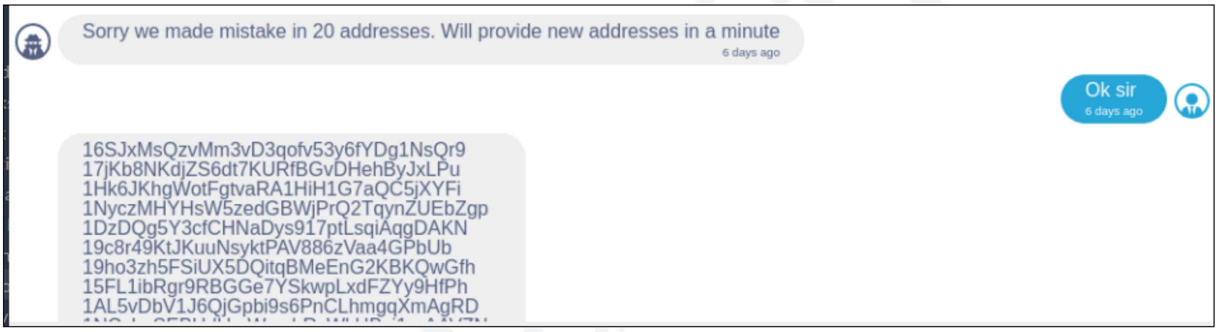
Analyzing the MEGA account in above image 21 revealed that the threat actor created the account using the TOR browser and made the purchase using Bitcoin. This transaction occurred while the ransomware attack against the victim was happening. Afterwards, this account was used with a variety of different operating systems before Conti attackers uploaded company data to this account using the rclone 3.2.2 tool.

Table 2 contains the login application, IP address, and access date for the MEGA account discovered by the PTI team.

Login App	IP Address	Access Date
MEGAsync-on-Linux	80.147.24.162	10/7/2021,06:03
Opera-on-Windows	198.98.60.19	10/6/2021,22:32
Opera-on-Windows	107.189.5.68	10/6/2021,20:54
MEGAsync-on-Windows	62.216.203.221	10/6/2021,19:02
MEGAsync-on-Windows	45.128.133.242	10/6/2021,18:38
MEGAsync-on-Windows	147.135.36.162	9/23/2021,07:02
Chrome-on-Windows	94.242.253.13	9/23/2021,07:02
Firefox-on-Windows	147.135.36.162	9/23/2021,06:53
MEGAsync-on-Windows	142.4.212.27	9/14/2021,15:45
rclone/v1.53.3	176.98.160.187	9/13/2021,14:54
rclone/v1.53.3	176.98.160.187	9/9/2021,14:35
Firefox-on-Windows	185.193.52.180	9/9/2021,12:47

Table 2. Conti Full List of Mega Account Information

Our analysis of victim chat logs revealed that several other Bitcoin wallet addresses were shared with some victims. The PTI Team is still conducting taint analysis on these wallet addresses to detect shared spending or laundering attempts.



Sorry we made mistake in 20 addresses. Will provide new addresses in a minute
6 days ago

Ok sir
6 days ago

16SJxMsQzvMm3vD3qofv53y6fYDg1NsQr9
17jKb8NKdjZS6dt7KURfBGvDHehByJxLPu
1Hk6JKhgWotFgtvaRA1HiH1G7aQC5jXYFi
1NyczMHYHsW5zedGBWjPrQ2TqynZUEbZgp
1DzDQg5Y3cfCHNaDys917ptLsqiAqgDAKN
19c8r49KtJKuuNsyktPAV886zVaa4GPbUb
19ho3zh5FSiUX5DQitqBMeEnG2KBKQwGfh
15FL1ibRgr9RBGGe7YSkwpLxdFZYy9HfPh
1AL5vDbV1J6QjGpbi9s6PnCLhmgqXmAgRD

Figure 22. Conti threat actor giving out additional wallet addresses

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

4 Statistics and Observations

The following graph (See Figure 23) displays changes in the number of Conti victims over a one-year period. The victim data were gathered from the Conti extortion blog (See Figure 3 [5]).

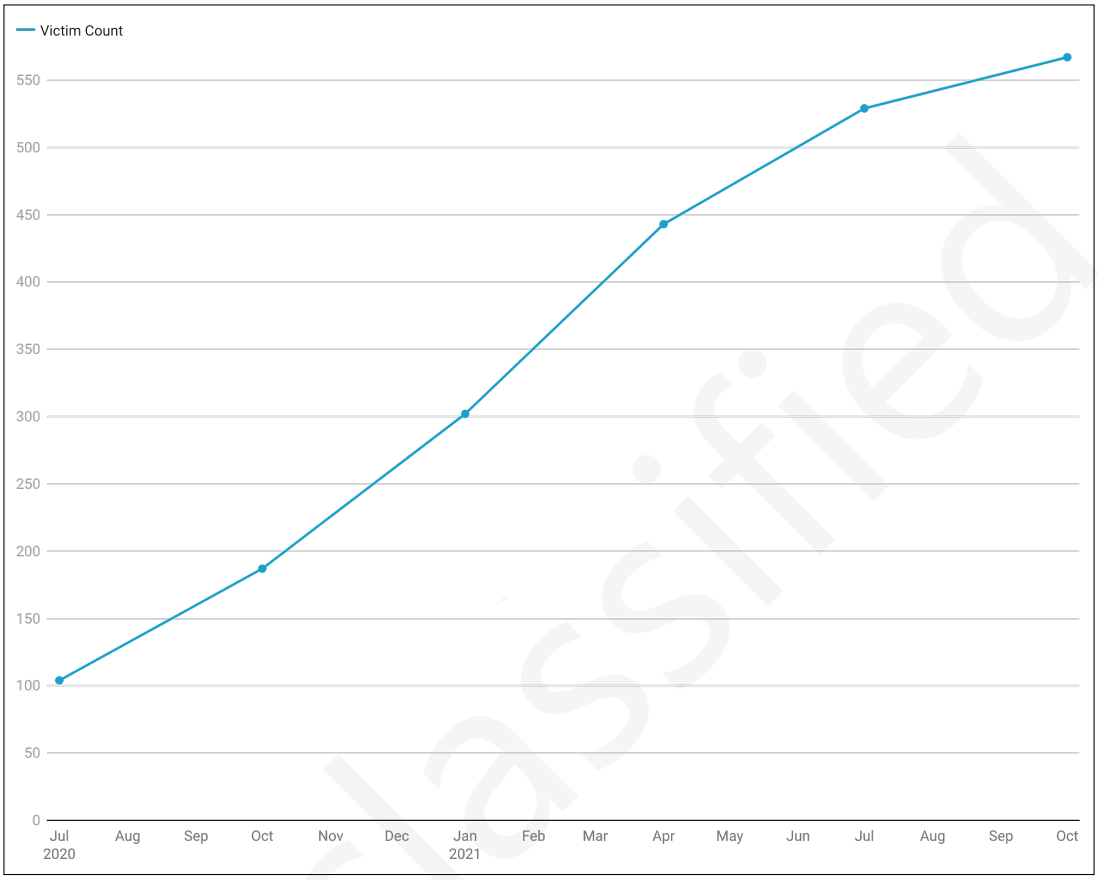


Figure 23. **Conti Victim Count**

It's clear to see that the number of victims has grown rapidly in the past year. The data contained in this report will help law enforcement authorities act against the Conti ransomware group and its affiliates, which should result in a drastic reduction in the number of victims in the near future. This report will inform ongoing investigations that could lead to the complete neutralization of Conti itself.

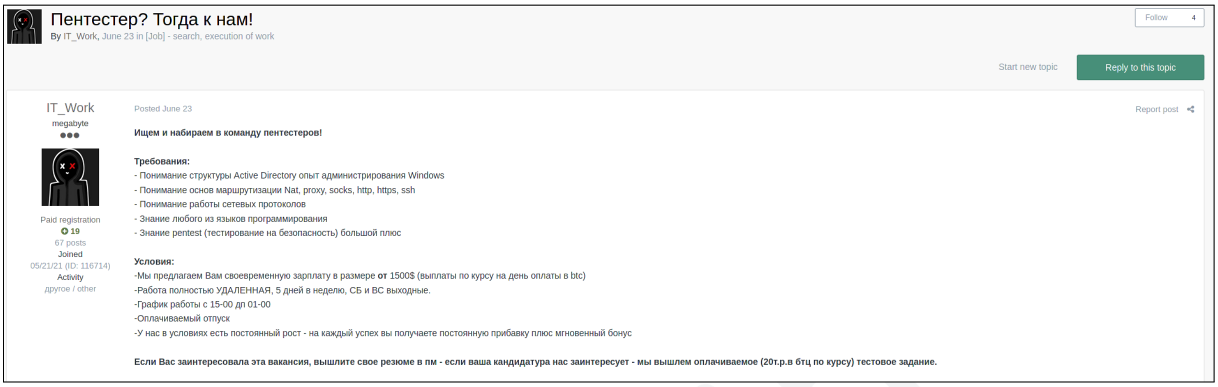
4.1 Known Recruiter Profiles

Ransomware groups hire affiliates from deep web and dark net forums, competing to attract new affiliates into their network. These recruiters generally create topics in well-known forums and discussion boards. In order to become an affiliate, one must have impressive skills, demonstrate motivation, and provide references from reputable cybercrime figures or

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

organizations.

Threat actors like the Conti team are both secretive and selective when it comes to recruiting. They recruit members only from experienced cybercrime organizations with high reputation, using private communication channels. The posts and forum topics of Conti recruiters often include penetration testing job ads and tooling projects. The following example shows a penetration test job announcement written by Conti recruiters.



Пентестер? Тогда к нам!
By IT_Work, June 23 in [Job] - search, execution of work

IT_Work
megabyte
Paid registration
19
67 posts
Joined
05/21/21 (ID: 116714)
Activity
другое / other

Posted June 23

Ищем и набираем в команду пентестеров!

Требования:
- Понимание структуры Active Directory опыт администрирования Windows
- Понимание основ маршрутизации Nat, proxy, socks, http, https, ssh
- Понимание работы сетевых протоколов
- Знание любого из языков программирования
- Знание pentest (тестирование на безопасность) большой плюс

Условия:
-Мы предлагаем Вам своевременную зарплату в размере **от** 1500$ (выплаты по курсу на день оплаты в btc)
-Работа полностью УДАЛЕННАЯ, 5 дней в неделю, СБ и ВС выходные.
-График работы с 15-00 дп 01-00
-Оплачиваемый отпуск
-У нас в условиях есть постоянный рост - на каждый успех вы получаете постоянную прибавку плюс мгновенный бонус

Если Вас заинтересовала эта вакансия, вышлите свое резюме в пм - если ваша кандидатура нас заинтересует - мы вышлем оплачиваемое (20т.р.в бтц по курсу) тестовое задание.

Figure 24. **Pentester call for application post**

The relevant post was shared by a Russian-speaking threat actor named **IT_Work** on the cybercriminal forum exploit.in. In the comments to the related post, IT_Work mentions that only those who can speak Russian can be included to the team. By combining the data gathered on the IT_Work profile and the Conti affiliate data leak 3.1.2 already mentions, the PTI team has gathered a list of threat actors identified as members of the Conti team :

- **Conti Admin**
  Nick : Tokyo
  Jabber : cicada3301@strong.pm
- **Assistant**
  Jabber : it_work_support@xmpp.jp
- **Recruiter**
  Nick : IT_Work
  Username : megabyte

This information will prove vital in helping enterprise cybersecurity teams and their vendors identify and mitigate security threats that originate from within the Conti cybercrime network.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

5 Money Flow

This section of the report is written by **Elliptic Ltd.** [8]. Elliptic is the leading provider of crypto compliance and blockchain analysis solutions globally.

5.1 Analysis of Conti ransom payments

113 bitcoin addresses were identified by Prodaft during this investigation. 100 of these addresses related to a single ransomware attack in which the victim requested to pay Conti in 100 separate transactions in order to hide the payment from tax and audit authorities. As a result, the addresses identified during this research are believed to be connected to 14 separate ransomware incidents. 50% of these attacks resulted in a payment to Conti.

Elliptic analysed the seven addresses to which ransom payments have been made. Conti operates as a Ransomware as a Service model. RaaS transactions characteristically split as the proceeds of each transaction is distributed between the ransomware operators and affiliates, with the exact percentage split differing between RaaS groups. In most instances, the affiliates are awarded the majority of the ransom payment, with the ransomware operators taking a smaller percentage. However, on 22 September 2021, the US Cybersecurity & Infrastructure Security Agency (CISA) issued an alert in which they described Conti's affiliate model as wage-based, as opposed to operating a traditional RaaS payment model.

5.1.1 Identification of consolidation cluster

Of the seven active addresses, four were found to send a percentage of their incoming funds, either directly or indirectly, to the same address cluster (hereafter referred to as "Conti consolidation cluster"). For three of these addresses, almost exactly 22.5% of the original incoming funds were sent to this cluster. As a result, it appears that this consolidation cluster may represent the operator portion of these ransomware payments.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

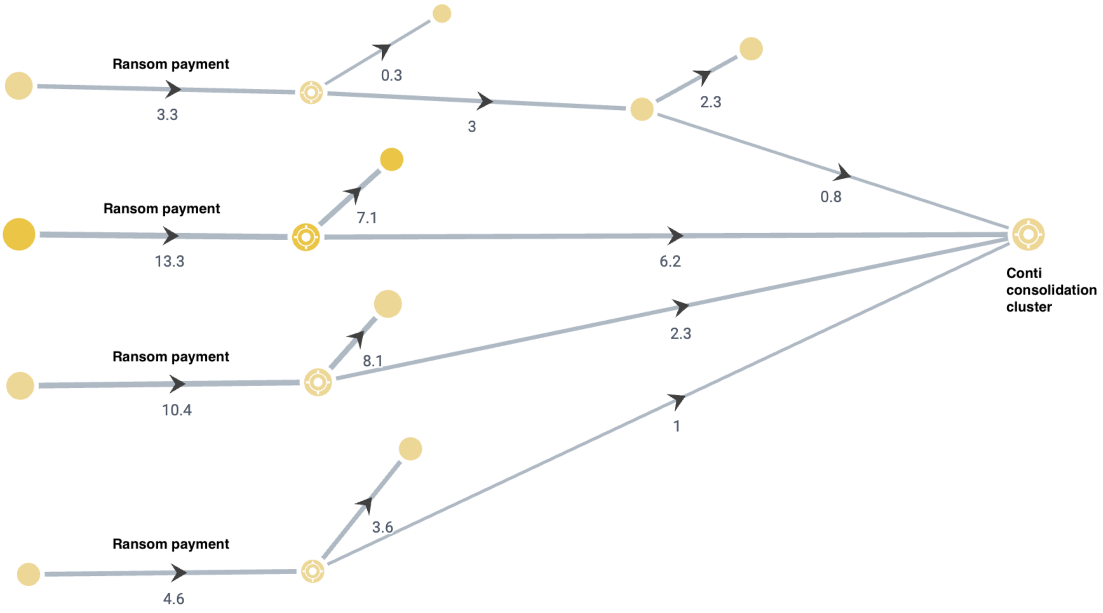


Figure 25. **Elliptic Forensics**

A further 31 incoming flows to this cluster were identified which appear to be ransomware payments. The majority of these send between 22-23% of their incoming funds either directly or indirectly to the Conti consolidation cluster. This common splitting pattern indicates that Conti affiliates may be awarded a percentage of the ransoms they successfully obtain, potentially contradicting CISA's assessment of Conti operating a wage-based affiliate payment model. Of interest, several further payments were identified in which the incoming funds originate from a split of a previous ransom payment, as demonstrated in the graph below. It is unclear whether this demonstrates an attempt to obfuscate the flow of funds, or a payment to the Conti operator for other services.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

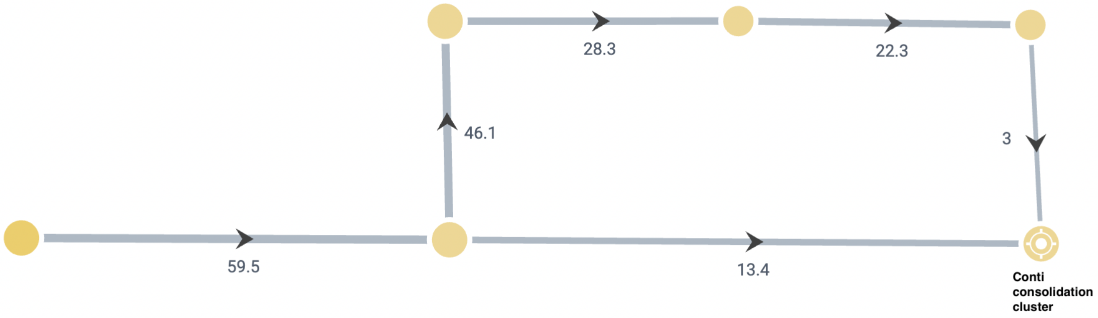


Figure 26. **Elliptic Forensics**

Researching the addresses identified by Prodaft and the incoming payments to the consolidation cluster indicates that since July 2021, Conti has received over 500 bitcoin in ransomware payments, valued at over $25.5 million, of which $6.2 million has been sent to the Conti consolidation cluster.

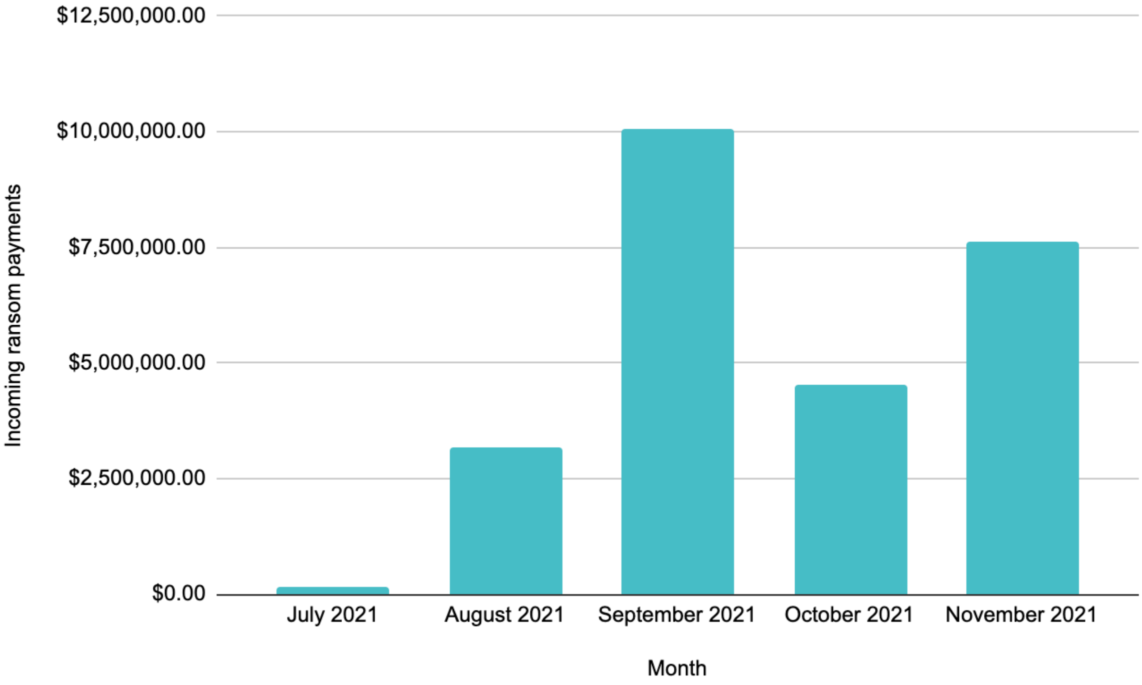


Figure 27. **Monthly ransom payments**

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

5.1.2 Destination of funds : Conti operator

The consolidation cluster, believed to be controlled by a Conti operator, was first active in December 2017 when it received one incoming payment of 1.8 bitcoin, which was later split and sent to a variety of prominent exchanges. After this time, the consolidation cluster was not active again until mid-2021. In August 2021, 0.07 bitcoin was sent from this cluster to a prominent exchange known to be used by ransomware groups. Aside from this, Conti have not attempted to cash out or exchange any of the bitcoin they have received into this cluster. Blockchain activity indicates that the remaining 123.06 bitcoin is currently held in an unhosted wallet.

5.1.3 Destination of funds : Conti affiliates

In addition to investigating the flow of funds into the consolidation cluster, Elliptic also investigated the ransomware proceeds which are believed to have been sent to Conti affiliates. One cluster was identified which has received payments from both Conti and DarkSide, which may indicate that an individual has worked as an affiliate for both of these groups.

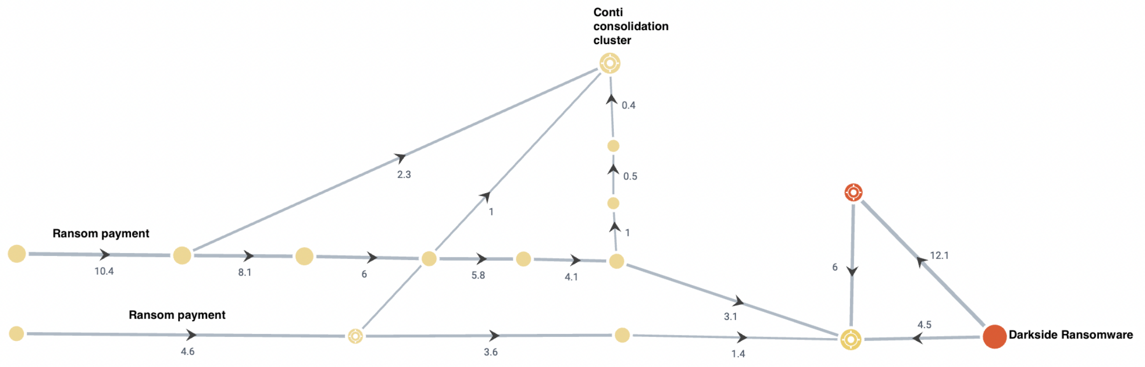


Figure 28. **Ransom payments over time**

Conti affiliates appear to conduct a sophisticated money laundering operation, avoiding obvious consolidation of funds. Due to the recent nature of some of these payments, some affiliate funds have not yet been moved. Despite this, Elliptic has identified affiliate funds being sent to a variety of services, including exchanges, coin swaps, privacy enhancing wallets including Wasabi, and the Russian-language darknet market Hydra.

5.1.4 Identification opportunities

This research indicates that identifying individuals associated with Conti through following the flow of funds is likely to be challenging, particularly given Conti's sophisticated money laundering techniques and use of services such as Wasabi wallet. Furthermore, whilst services including exchanges implement KYC policies, it is possible that groups such as Conti deposit and withdraw from these services in small amounts, which do not trigger KYC requirements. However, transaction screening tools can provide financial institutions and cryptocurrency exchanges with the ability to identify incoming transactions from illicit sources such as ransomware payments. Elliptic's clients, including financial institutions and cryptocurrency exchanges can be alerted to any client deposits which originate from addresses connected to Conti, by using our transaction and wallet screening solutions[1].

6 Conclusion

Bold, headline-making cyberattacks like the Colonial Pipeline attack in May 2021 showed the world how cybercriminals can deeply impact day-to-day life for millions of people. Enterprise executives and their risk advisors need in-depth threat intelligence in order to mitigate these threats while minimizing the damage they cause. The work of our PTI team is crucial towards understanding the cybercrime landscape and developing solutions that improve enterprise resilience against cyber threats and reduce risk exposure in the event of an attack.

In this report, we presented the inner workings of one of the most well-known ransomware groups in the world. However, the cybercrime industry moves rapidly. Many ongoing technological and cultural changes – like the widespread acceptance of cryptocurrency and the ongoing shift towards remote and hybrid work – will significantly impact how cyberattacks occur in the near future.

In order to tackle the complex challenge of disrupting cybercriminal organizations, public and private forces need to work collaboratively with one another to better understand and mitigate the wider legal and commercial impact of the threat. Our research sheds much-needed light on the inner workings of cybercriminal organizations, helping cybersecurity professionals, lawyers and insurance companies identify operatives and their external connections when investigating security incidents.

Enterprise leaders and cybersecurity executives who invest in threat intelligence services gain valuable insight into the unique risk profile of their organization. This kind of intelligence enables them to make comprehensive, data-based decisions about the overall exposure of their business e relative to real-world threat actor tactics and techniques.

If there is no choice but to negotiate, enterprises equipped with sophisticated threat intelligence capabilities like ours stand a far better chance of gaining the upper hand and preventing catastrophic damage to their brand, their users, and their stakeholders.

[1] https://www.elliptic.co/solutions/crypto-transaction-monitoring

Références

[1] CERTFR. *Hermes and Ryuk ransomware relation*. url : `https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-006.pdf`. (accessed : 10.11.2021).

[2] Checkpoint. *Ryuk ransomware notes*. url : `https://research.checkpoint.com/2018/ryuk-ransomware-targeted-campaign-break/`. (accessed : 10.11.2021).

[3] Clearskysec. *Clearskysec research : CONTI Modus Operandi and Bitcoin Tracking*. url : `https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf`. (accessed : 12.10.2021).

[4] Comparitech. *2018-2021 Ransomware statistics and facts*. url : `https://www.comparitech.com/antivirus/ransomware-statistics/`. (accessed : 25.03.2021).

[5] Conti. *Conti ransomware's extortion blog*. url : `https://continews.click/`. (accessed : 10.11.2021).

[6] Cybereason. *Bazarloader distrubition methods*. url : `https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware`. (accessed : 28.10.2021).

[7] Intel471. *Intel471 : Printnightmare usages in Conti ransomware*. url : `https://intel471.com/blog/ransomware-as-a-service-fivehands-printnightmare-babuk-conti`. (accessed : 28.10.2021).

[8] Elliptic Ltd. *AML Compliance Monitoring for Crypto Transactions*. url : `https://www.elliptic.co/solutions/crypto-transaction-monitoring`. (accessed : 12.11.2021).

[9] Malpedia. *Malpedia : Wizard Spidef References*. url : `https://malpedia.caad.fkie.fraunhofer.de/actor/wizard_spider`. (accessed : 28.10.2021).

[10] Sophos. *Fortigate firewall RCE usages in Conti ransomware*. url : `https://news.sophos.com/en-us/2021/02/16/conti-ransomware-attack-day-by-day/`. (accessed : 10.11.2021).

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Acknowledgement
We would like to thank *"Police Cantonale Vaudoise / Switzerland"* and our advisors for their valuable guidance and support throughout this research.

We also would like to thank Elliptic Ltd. (**www.elliptic.co**) for their invaluable contribution to this research by analyzing the money flow of one of the world's top ransomware gangs.

The public version of the report will be shared from our github page `https://www.github.com/prodaft`. The readers can find new samples, IOCs, and new versions of this report from our github page as we will constantly update our page based on new findings.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Historique

Version	Date	Auteur(s)	Modifications
1.0	16.10.2021	PTI Team	Initial DRAFT release
1.1	10.11.2021	PTI Team	Initial TLP:WHITE DRAFT
1.2	12.11.2021	PTI Team	Money Flow section added
1.3	15.11.2021	PTI Team	Typo fixes
1.4	17.11.2021	PTI Team	5.1 edited
1.5	18.11.2021	PTI Team	Intro and Conclusion edited
1.6	18.11.2021	PTI Team	Removed Hermes, Wizard Spider

PRODAFT was founded as a cyber threat intelligence company in 2012.

Aimed at creating a difference through expertise, the brand has significantly evolved thanks to its apposite technologies, all of which are developed in-house.

By looking at cyber threats from a realistic perspective, PRODAFT has always positioned itself as a "professionally unconventional" provider in its field, thanks to a suite of proprietary solutions.

PRODAFT continues to serve a range of global brands and critical industries via its threat intelligence, penetration testing and security research teams.

To ensure proactive nature of PRODAFT's solutions, our operational cycles are constantly reviewed and adapted to emerging challenges within cyber arena. Owing to this constant state of flux, PRODAFT is always prepared for the new realities and challenges of cyber security.

Our clients will never find themselves blindsided by any newly evolving cyber trend. Our commitment in this regard is the main reason behind PRODAFT's popularity among high-profile organizations.

Contact: info@prodaft.com
Address: Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.