AhnLab Cyber Threat Intelligence Report

TLP: AMBER

Threat Trend Report on Conti Ransomware

V1.0

AhnLab Security Emergency Response Center (ASEC)

May. 18, 2022

AhnLab

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-05-18	First release

Contents

Introduction......6

1) Attack Targets and Actual Cases......7

2) Affected Countries......8

3) Attack Method (Attack Vectors)......9

4) Major Tools......10

(1) Cobalt Strike......11

(2) PsExec......11

(3) Mimikatz......11

(4) Anydesk......11

(5) RDP (Remote Desktop Protocol)......11

Scale of Organization......12

Related Issues......13

1) Whistleblowing by an Insider......13

2) Server Infrastructure Exposed......14

3) Declaration of Full Support for the Russian Government......15

4) Source Code of Conti Ransomware Version 3 Leaked......16

5) Branching Out Into Cryptocurrency Platforms and Carding Markets......17

AhnLab Response Overview......19

Conclusion......20

IOC (Indicators Of Compromise)......21

File Hashes (MD5)......21

MITRE ATT&CK......21

References......23

⚠ CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Introduction

Conti Ransomware, known to have first made its appearance in May 2020, is said to be the sequel of Ryuk Ransomware. It is controlled by Wizard Spider, an APT group based in Russia (hereinafter referred to as Conti Group). They run Ransomware-as-a-Service (RaaS) and known to be behind not only Conti Ransomware but also Trickbot and BazarLoader.

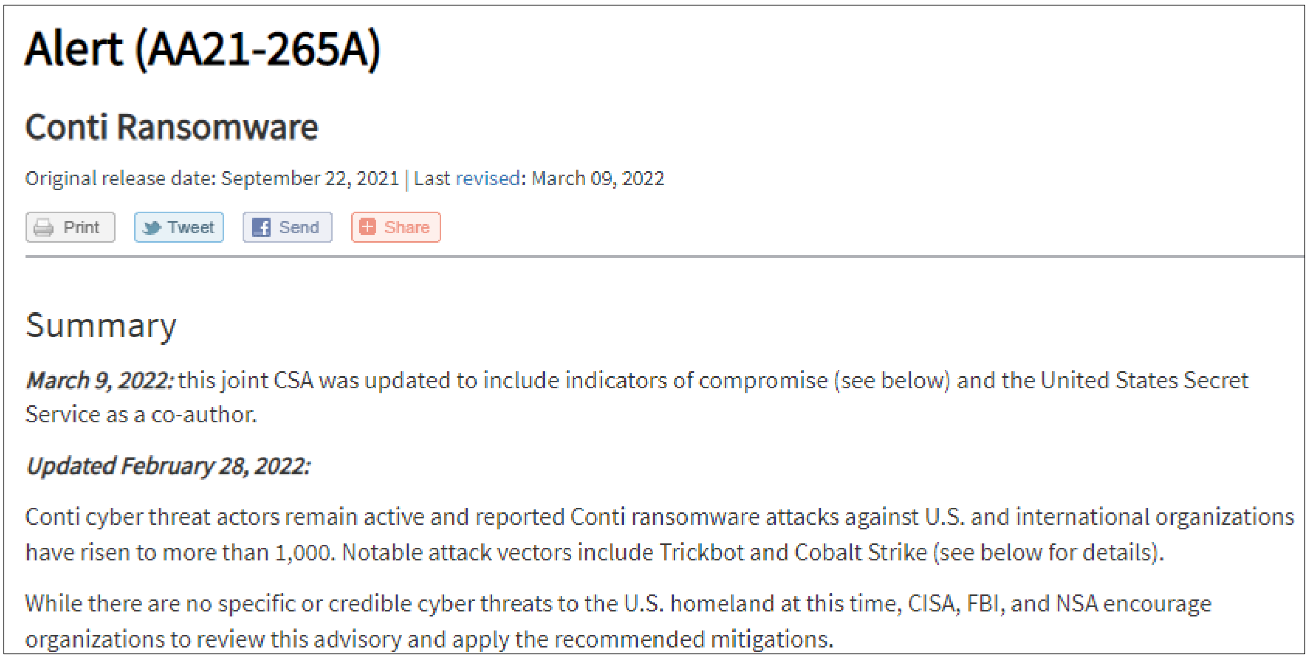
They also use a "double extortion" scheme where they steal and encrypt data and demand the victim pay a ransom for decryption, threatening to disclose said data on the leaked site if the ransom is not paid. Following the cease in activities of Sodinokibi (Revil) Ransomware, the activities of Conti have increased dramatically, as in the case of LockBit Ransomware.

Accordingly, the Cybersecurity and Infrastructure Security Agency (CISA) published a security advisory statement on Conti Ransomware on September 22nd, 2021.[1]

AhnLab had posted Conti Ransomware Analysis Report on May 28, 2021[2]. In this report, we covered the issue of internal data leakage and organizational scale of the Conti Group.

[1] https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

[2] https://atip.ahnlab.com/ti/contents/issue-report/malware-analysis?i=b5aa6ae8-c9d1-45b7-bf56-32007462d397



Alert (AA21-265A)

Conti Ransomware

Original release date: September 22, 2021 | Last revised: March 09, 2022

Summary

March 9, 2022: this joint CSA was updated to include indicators of compromise (see below) and the United States Secret Service as a co-author.

Updated February 28, 2022:

Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000. Notable attack vectors include Trickbot and Cobalt Strike (see below for details).

While there are no specific or credible cyber threats to the U.S. homeland at this time, CISA, FBI, and NSA encourage organizations to review this advisory and apply the recommended mitigations.

Figure 1. Security advisory statement published by CISA

1) Attack Targets and Actual Cases

Below are major cases of attacks collected through published analysis reports and information confirmed by AhnLab.

Date	Target	Details
May, 2021	HSE (Health Service Executive), the healthcare service in Ireland	System shut down with a request of a ransom of about $20,000,000[3]
May, 2021	Waikato Hospital in New Zealand	Hospital system infected[4]
2021.05	Overseas corporate body in Korea	Staff PC name and OS information leaked[5]
2021.10	JVCKenwood, a multinational electronics company in Japan	1.7 TB of data leaked with a request for a

[3] https://www.bleepingcomputer.com/news/security/irelands-health-services-hit-with-20-million-ransomware-demand/

[4] https://www.rnz.co.nz/news/national/442850/cyber-attack-at-waikato-hospitals-patients-anxiously-wait-for-updates

[5] https://news.sbs.co.kr/news/endPage.do?news_id=N1006325546

		ransom of about $7,000,000[6]
2022.01	Delta Electronics, Taiwan	Over 1,500 servers and 12,000 computers encrypted[7]
2022.05	The country of Costa Rica	672 GB of data leaked from government organizations[8]

Table 1. Major attack cases

The Delta Electronics attack case in Taiwan has also been covered in ASEC Notes on January 28th, 2022.[9]

Their targets are mainly medical and manufacturing industries, but also attacks various industries and organizations.

2) Affected Countries

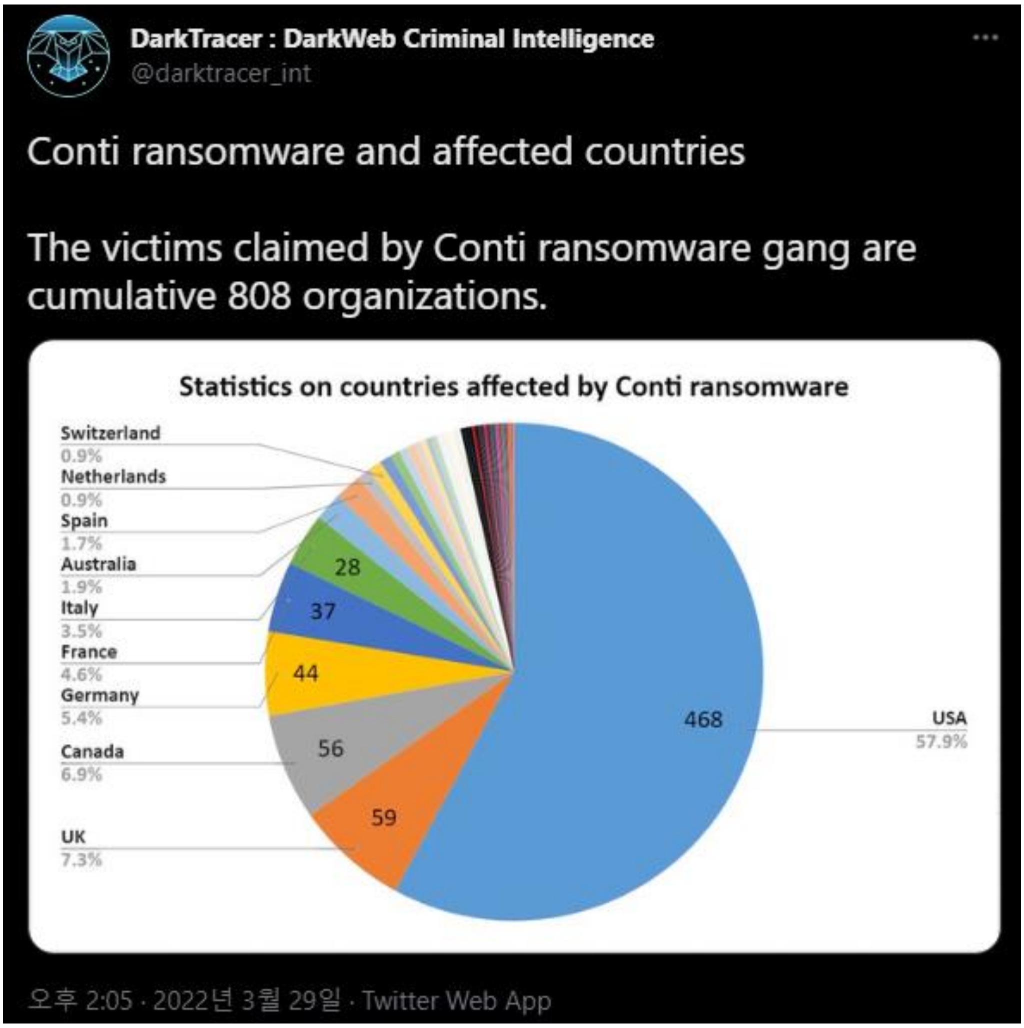
According to Darktracer, a cybersecurity AI firm, the US suffered the most damage from Conti Ransomware. It is said that the Conti Group attacked a total of 808 organizations (As of the tweeted date: March 29th, 2022).

[6] https://www.dailysecu.com/news/articleView.html?idxno=129644

[7] https://therecord.media/conti-ransomware-hits-apple-tesla-supplier/

[8] https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/

[9] https://atip.ahnlab.com/ti/contents/asec-notes?i=bafdea04-34b9-4ce4-bb0a-7ca5546a82d1



DarkTracer : DarkWeb Criminal Intelligence
@darktracer_int

Conti ransomware and affected countries

The victims claimed by Conti ransomware gang are cumulative 808 organizations.

오후 2:05 · 2022년 3월 29일 · Twitter Web App

Figure 2. Affected countries[10]

3) Attack Method (Attack Vectors)

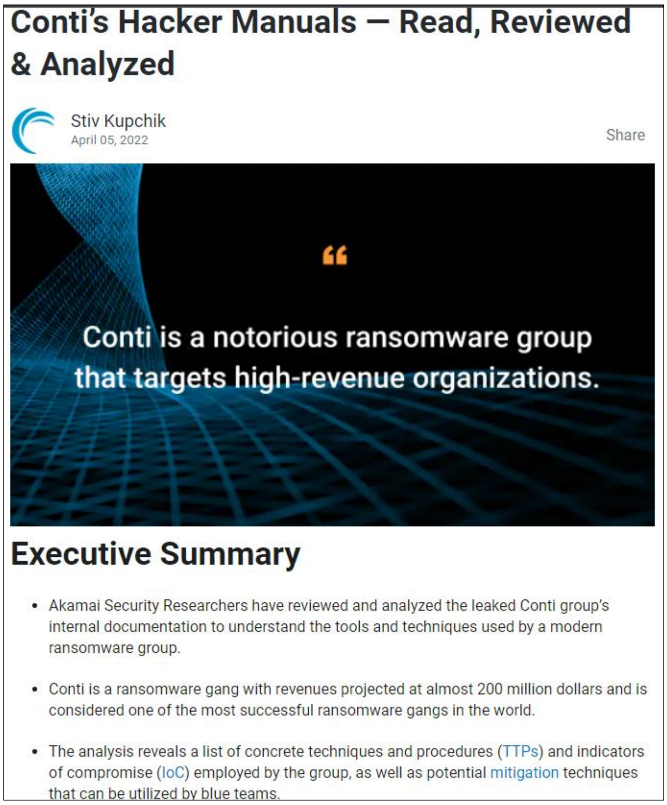
According to the security company Akamai, initial access methods mainly involved, but were not limited to, vulnerable firewalls, exposed RDP (Remote Desktop Protocol) services, and phishing emails.

[10] https://twitter.com/darktracer_int/status/1508671560890327043/photo/1

Websites such as Shodan provide network information and vulnerability information needed by threat actors for their attacks. This service could be used to select an attack target.

Mimikatz is used to gain PC account information, and Angry IP, a normal IP scanner tool, is used to identify accessible servers.

Rclone, an open-source tool that transmits data to a cloud storage and manages them, is then used to leak data, after which Conti Ransomware infection occurs in the end.



Conti's Hacker Manuals — Read, Reviewed & Analyzed

Stiv Kupchik
April 05, 2022

Share

“

Conti is a notorious ransomware group that targets high-revenue organizations.

Executive Summary

- Akamai Security Researchers have reviewed and analyzed the leaked Conti group's internal documentation to understand the tools and techniques used by a modern ransomware group.
- Conti is a ransomware gang with revenues projected at almost 200 million dollars and is considered one of the most successful ransomware gangs in the world.
- The analysis reveals a list of concrete techniques and procedures (TTPs) and indicators of compromise (IoC) employed by the group, as well as potential mitigation techniques that can be utilized by blue teams.

Figure 3. Analysis on the Conti Group[11]

4) Major Tools

The tools mainly used by the Conti Group are as follows.

[11] https://www.akamai.com/blog/security/conti-hacker-manual-reviewed

(1) Cobalt Strike

This was developed for the purpose of checking security vulnerabilities of corporate and organizational networks and systems. It supports various features for each stage of penetration tests. However, following the release of its cracked version, it is being abused by many threat actors to serve their malicious goals.

(2) PsExec

This is a utility tool that allows processes to be run by another system through a complete interaction of console applications without the need for manual installation of client software.

(3) Mimikatz

This is a Dump tool that allows its users to obtain account credentials of Windows PCs and information useful for network security testing. It is usually used to gain account credentials from PCs.

(4) Anydesk

This is a software that allows remote access to another PC. It also offers file transfer and VPN functionality beside the remote control.

(5) RDP (Remote Desktop Protocol)

This is a remote control protocol included by default in Windows PCs. This protocol is usually used for initial access.

Scale of Organization

Their paydays are on the 15th and 30th of each month, and they have a physical office. Their size is about that of a small or medium company, made up of about 150 people in HR and other departments (testers, analysts, coders).

Korean media have published their total personnel count as 350 because there were about 350 people in their group chat, but this is still an inference.[12]

Their work hours are from 10:00 to 18:00 Moscow time, for five days a week. The person with the nickname "Stern" is the general manager and director. The monthly wage of each member is $2,000 on, which means that the total amount of money spent on wages is about $300,000 monthly, or about $3,600,000 annually.

Also, they recruit employees from a legal headhunting website in Moscow called "headhunter".[13] They access this website through abnormal methods— presumably by hacking—and attempt to recruit members by contacting candidates via email.

These numbers were calculated through the analysis conducted by multiple security companies and researchers based on the operators' chat. Some content of the internal group chat will be covered in the section further on when discussing about the leakage of internal data.[14][15][16]

[12] https://www.sedaily.com/NewsView/265ZQIYPI7

[13] https://hh.ru/

[14] https://www.computing.es/seguridad/noticias/1132110002501/opera-grupo-de-ransomware-conti.1.html

[15] https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

[16] https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html

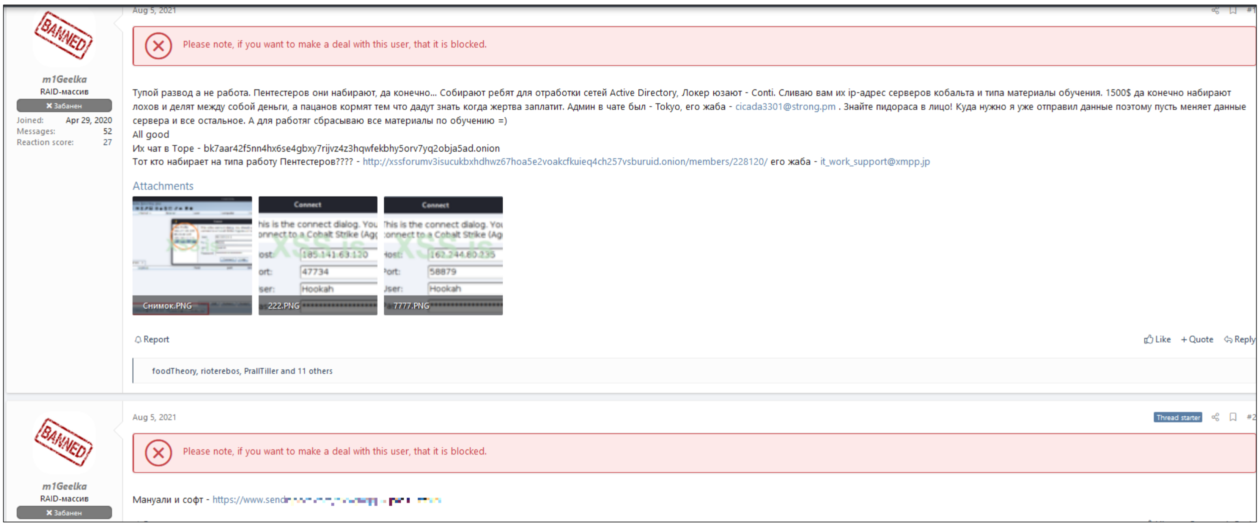
Related Issues

1) Whistleblowing by an Insider

On August 5th, 2021, a person deemed to be a client with much dissatisfaction against the Conti Group posted a whistleblowing post on a dark web in Russian.

It included the group's manuals related to member training, methods for internal access and propagation, and how to extract data before file encryption. It also included contents of the internal group chat.

The post also shared the IP address hosting the Cobalt Strike C2 server used by the Conti Group.



Please note, if you want to make a deal with this user, that it is blocked.

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 - bk7aar42f5nn4hx6se4gbxy7rijvz4z3hqwfekbhy5orv7yq2obja5ad.onion
Тот кто набирает на типа работу Пентестеров???? - http://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/members/228120/ его жаба - it_work_support@xmpp.jp

Attachments

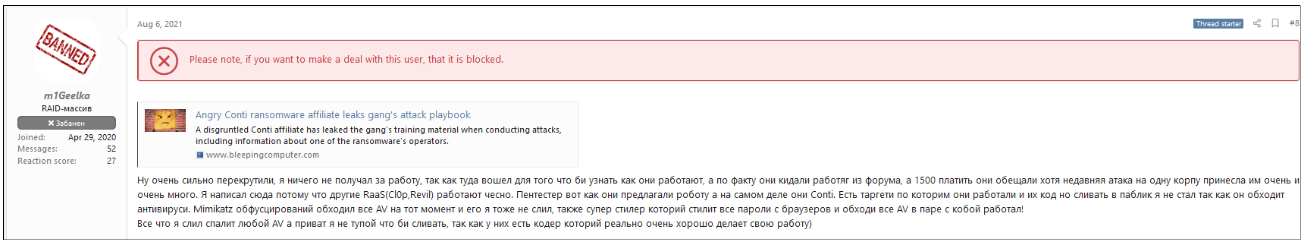
Please note, if you want to make a deal with this user, that it is blocked.

Мануали и софт - https://www.send[redacted]

Figure 4. Whistleblowing post

The message additionally included the reason for whistleblowing; it said that the Conti Group laid off hard-working people and were to pay them $1,500 which they did not follow through.

The post claims that not all data are disclosed, but only those that can be detected by AV products.



m1Geelka
RAID-массив
✖ Забанен

Joined:	Apr 29, 2020
Messages:	52
Reaction score:	27

Aug 6, 2021

Please note, if you want to make a deal with this user, that it is blocked.

Angry Conti ransomware affiliate leaks gang's attack playbook
A disgruntled Conti affiliate has leaked the gang's training material when conducting attacks, including information about one of the ransomware's operators.
www.bleepingcomputer.com

Ну очень сильно перекрутили, я ничего не получал за работу, так как туда вошел для того что би узнать как они работают, а по факту они кидали работяг из форума, а 1500 платить они обещали хотя недавняя атака на одну корпу принесла им очень и
очень много. Я написал сюда потому что другие RaaS(Cl0p,Revil) работают чесно. Пентестер вот как они предлагали роботу а на самом деле они Conti. Есть таргети по которим они работали и их код но сливать в паблик я не стал так как он обходит антивируси. Mimikatz обфусцированний обходил все AV на тот момент и его я тоже не слил, также супер стилер котоpий стилит все пароли с браузеров и обходи все AV в паре с кобой работал!
Все что я слил спалит любой AV а приват я не тупой что би сливать, так как у них есть кодер который реально очень хорошо делает свою работу)

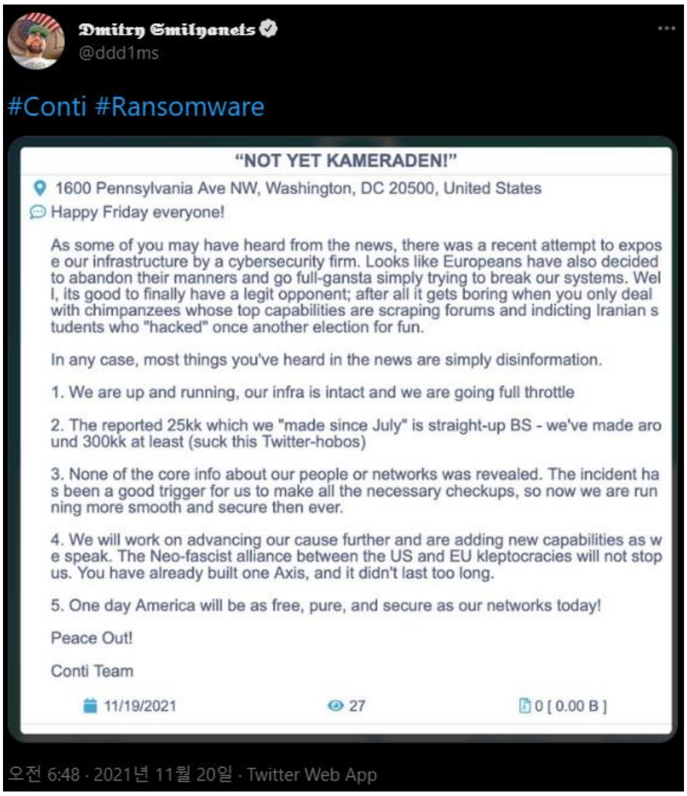
Figure 5. Reason behind the whistleblowing

2) Server Infrastructure Exposed

On November 18th, 2022, security company Prodaft uploaded a report on the Conti Group's infrastructure.[17]

This report included content about the actual IP of the hidden service that hosts the recovery website used by the Conti Group. One day after the post was uploaded (Nov 20), the Conti Group responded with the statement that these arguments are untrue, that their infrastructure is still well-functioning and is being used to its full capacity.

[17] https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis



Dmitry Smilyanets
@ddd1ms

#Conti #Ransomware

"NOT YET KAMERADEN!"

1600 Pennsylvania Ave NW, Washington, DC 20500, United States

Happy Friday everyone!

As some of you may have heard from the news, there was a recent attempt to expose our infrastructure by a cybersecurity firm. Looks like Europeans have also decided to abandon their manners and go full-gansta simply trying to break our systems. Well, its good to finally have a legit opponent; after all it gets boring when you only deal with chimpanzees whose top capabilities are scraping forums and indicting Iranian students who "hacked" once another election for fun.

In any case, most things you've heard in the news are simply disinformation.

1. We are up and running, our infra is intact and we are going full throttle

2. The reported 25kk which we "made since July" is straight-up BS - we've made around 300kk at least (suck this Twitter-hobos)

3. None of the core info about our people or networks was revealed. The incident has been a good trigger for us to make all the necessary checkups, so now we are running more smooth and secure then ever.

4. We will work on advancing our cause further and are adding new capabilities as we speak. The Neo-fascist alliance between the US and EU kleptocracies will not stop us. You have already built one Axis, and it didn't last too long.

5. One day America will be as free, pure, and secure as our networks today!

Peace Out!

Conti Team

11/19/2021 27 0 [0.00 B]

오전 6:48 · 2021년 11월 20일 · Twitter Web App

Figure 6. Rebuttal stating that the content of the report are untrue[18]

While the truthfulness of this statement cannot be ascertained, it is deemed that such a response was made for the purpose of client reassurance.

Also, while the post announced that the profits of the Conti Group totaled at least 25.5 million dollars, the group corrected it 300 million dollars.[19]

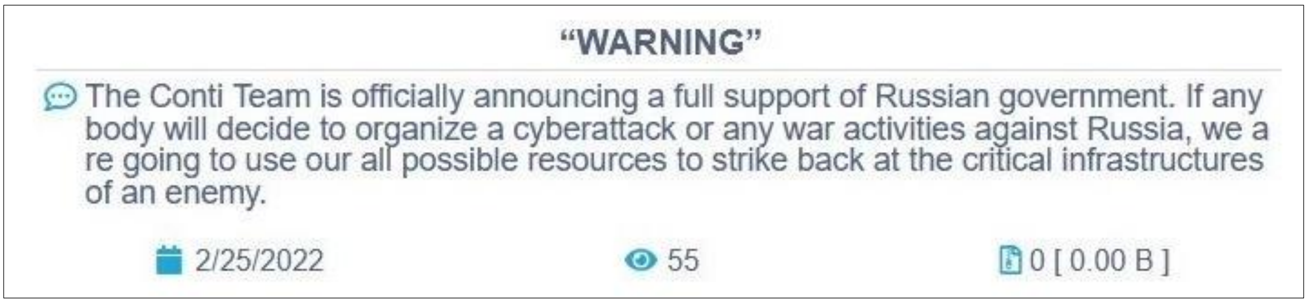
However, there is a possibility that the numbers from the Conti Group were inflated to advertise their profitability.

3) Declaration of Full Support for the Russian Government

On February 24th, 2022 the war between Russia and Ukraine broke out. On the next day, the Conti Group posted a message that they support the Russian government.

[18] https://twitter.com/ddd1ms/status/1461813586154635268

[19] https://therecord.media/conti-gang-has-made-at-least-25-5-million-since-july-2021/



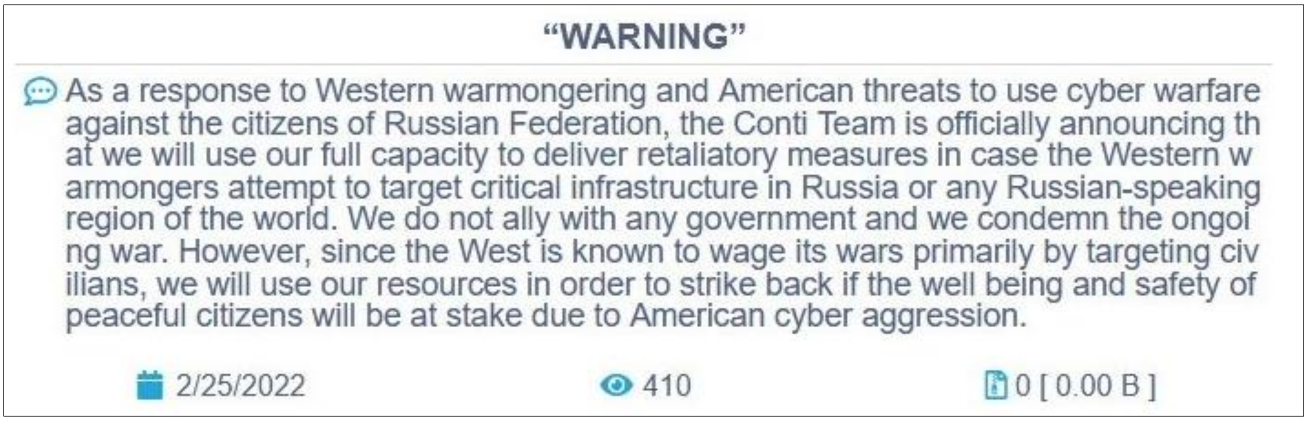
"WARNING"

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 55 0 [0.00 B]

Figure 7. Conti Group declaring their support for the Russian government

However, in a few hours, the message was edited to read that they would not form an alliance with any government and that they denounce the ongoing war. They are thought to have withdrawn their statement because of the possibility of losing customers due to negative sentiments to the original post, which could lead to a decline in their profit line.



"WARNING"

As a response to Western warmongering and American threats to use cyber warfare
against the citizens of Russian Federation, the Conti Team is officially announcing th
at we will use our full capacity to deliver retaliatory measures in case the Western w
armongers attempt to target critical infrastructure in Russia or any Russian-speaking
region of the world. We do not ally with any government and we condemn the ongoi
ng war. However, since the West is known to wage its wars primarily by targeting civ
ilians, we will use our resources in order to strike back if the well being and safety of
peaceful citizens will be at stake due to American cyber aggression.

2/25/2022 410 0 [0.00 B]

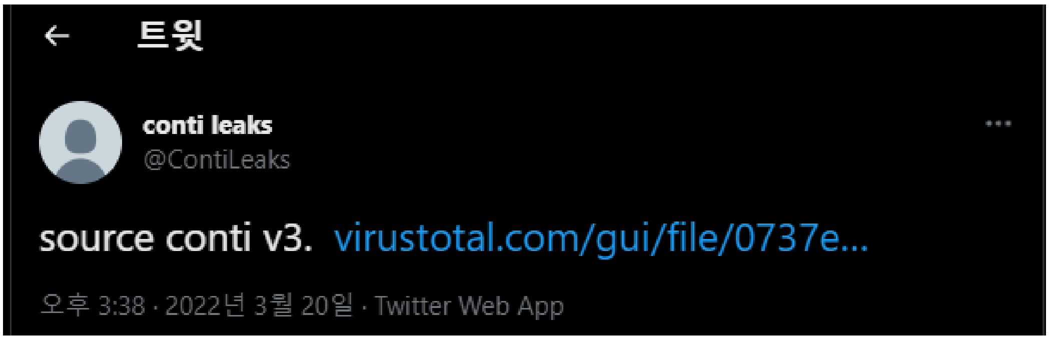
Figure 8. Withdrawing their supporting statement for the Russian government

4) Source Code of Conti Ransomware Version 3 Leaked

On March 20th, 2022, the source code of Conti Ransomware Version 3 was leaked by a Twitter user named "conti leaks".++++++++++++++

According to BleepingComputer, the hacking group known as "NB65" used this source to build the ransomware and attacked a Russian corporation, stealing their data.

They disclosed their motive to be the Russian invasion of Ukraine, and the ransomware in question is being detected by many antivirus companies as Conti Ransomware. However, it is built in a way that does not allow decryption with the decryption tool included in the leaked source. Also, the group announced that there is no way to decrypt files without contacting them.



← 트윗

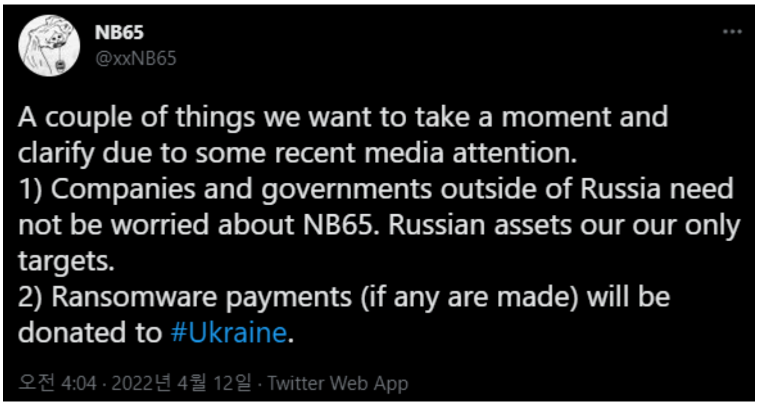
conti leaks
@ContiLeaks

source conti v3. virustotal.com/gui/file/0737e...

오후 3:38 · 2022년 3월 20일 · Twitter Web App

Figure 9 Source code leaked on Twitter[20]

Afterwards, on April 12th, 2022, NB65 proclaimed that they would not attack corporations or governments outside Russia and any decryption fees paid to them will be donated to Ukraine.



NB65
@xxNB65

A couple of things we want to take a moment and clarify due to some recent media attention.
1) Companies and governments outside of Russia need not be worried about NB65. Russian assets our our only targets.
2) Ransomware payments (if any are made) will be donated to #Ukraine.

오전 4:04 · 2022년 4월 12일 · Twitter Web App

Figure 10. Official statement by NB65[21]

5) Branching Out Into Cryptocurrency Platforms and Carding Markets

According to the acquired chat messages, it can be assumed that a cryptocurrency platform and a private forum, as well as a carding shop[22] is under development.

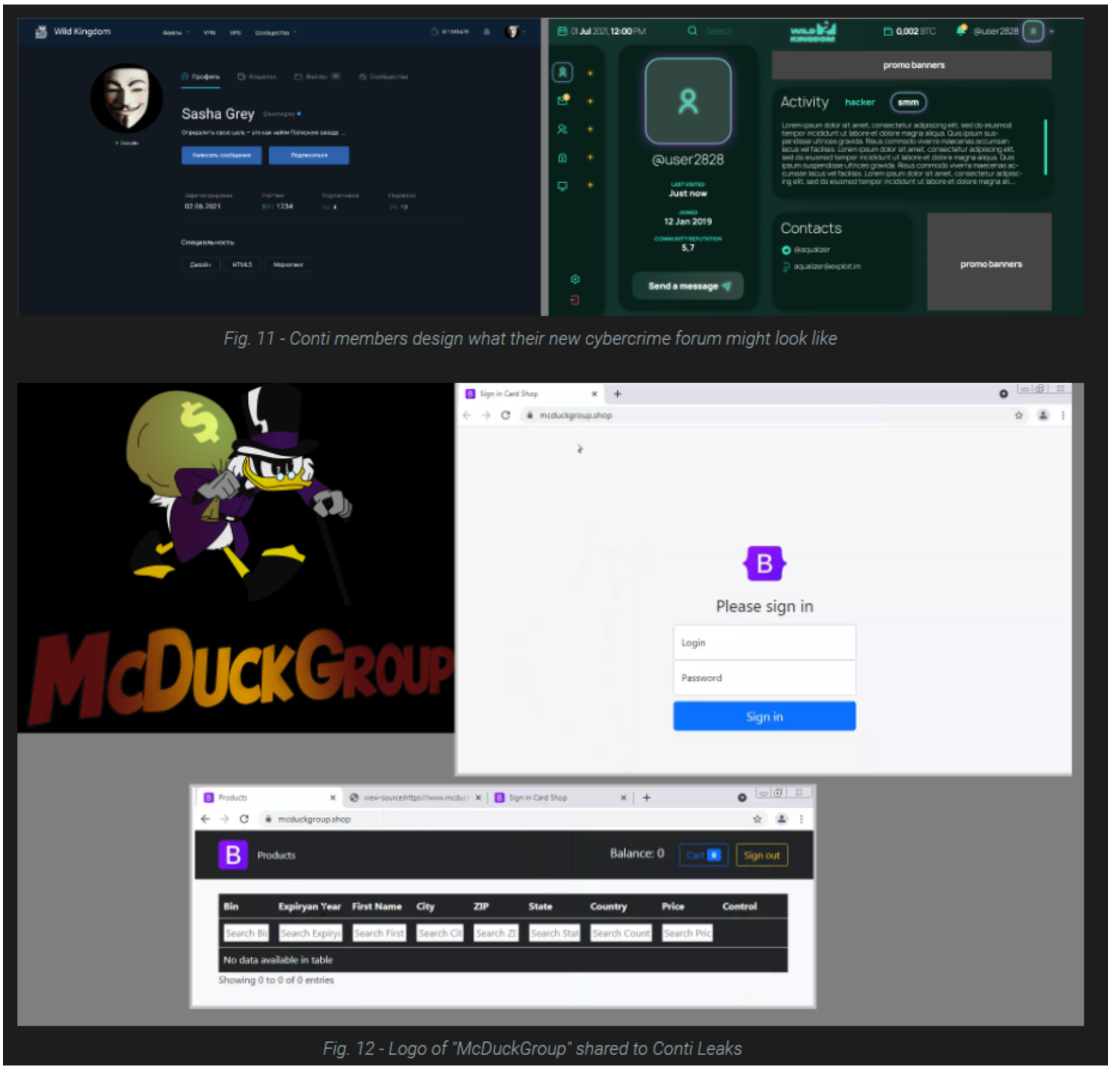
[20] https://twitter.com/ContiLeaks/status/1505433648023146499?cxt=HHwWhsC49af7r-QpAAAA

[21] https://twitter.com/xxNB65/status/1513593777759428624

[22] A market for selling and buying stolen credit card information

It is seen to be an attempt to branch out into a new market to reap higher profits and increase the size of their organization. The Conti Group steals data first before infecting target systems with ransomware.

When the carding shop development is complete, they may be able to generate income with decryption fees and produce additional income by selling the credit card information out of the stolen data to the carding shop.



Bin	Expiryan Year	First Name	City	ZIP	State	Country	Price	Control
Search Bi	Search Expiry	Search First	Search Ci	Search Zi	Search Sta	Search Count	Search Pric	
No data available in table								

Showing 0 to 0 of 0 entries

Fig. 11 - Conti members design what their new cybercrime forum might look like

Fig. 12 - Logo of "McDuckGroup" shared to Conti Leaks

Figure 11. Images found among the leaked chat messages[23]

[23] https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

AhnLab Response Overview

The aliases and the engine version information of AhnLab products are shown below. Even if the activities of this threat group have been identified recently, AhnLab products may have already diagnosed related malware in the past. While ASEC is tracking the activities of this threat group and responding to related malware, there can be variants that have not been identified and thus are not detected.

Ransomware/Win.Conti.R483081 (2022.04.11.03)
Ransomware/Win.CONTI.C4932859 (2022.01.26.03)
Ransomware/Win.Conti.R372647 (2021.05.24.02)
Ransomware/Linux.Conti (2022.05.17.02)
Trojan/Win32.ContiRansom.R358495 (2020.12.17.06)

Conclusion

The Conti Group’s activities have increased exponentially alongside LockBit Ransomware following the cessation of BlueCrab (Sodinokibi) Ransomware.

More shock descended upon the public as the group's internal chat messages and data were leaked, which revealed their attack tactics, target selection methods and the size of their organization.

We can see from this issue that threat actors are putting in much effort to choose and attack targets, and are increasing their size of organization by branching out into new markets.

Seeing from the fact that these attacks mostly begin from vulnerable firewalls, exposed RDP, and phishing emails, periodic inspection and antivirus scans are crucial to check for suspicious files and take appropriate measures. In addition, emails from unknown sources must always be approached with caution.

IOC (Indicators Of Compromise)

A portion of the following IOC quotes other analysis reports, and there are some cases that could not be verified because samples could not be obtained. Updates may occur without prior notice when new information is found.

File Hashes (MD5)

The MD5 of the related files are as follows. **However, sensitive samples may have been excluded.**

Delta Electronics, Taiwan (Windows)
7E18DD4A4B84F2F93EFF4790F16E8E8B

Version 2 (Windows)
B3D6BA0AA663F699283D25DDCB6561B9

Version 3 (Windows)
77078664b4bbfbe25be44004431c1a37

Conti Ransomware (From Group NB65, Windows)
F746EA39C0C5FF9D0A1F2D250170AD80

Conti Ransomware (Linux)
CFB6D21FFE7C4279F761F2351C0810EE

MITRE ATT&CK

The MITRE ATT&CK information on this security attack is as follows. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is the classification of tactics and techniques of the malicious behaviors presented by the threat actor. Relevant information can be found on https://attack.mitre.org/.

The MITRE ATT&CK ID corresponding to this threat group quotes from another analysis report and has additional details confirmed by AhnLab.

Tactic	ID	Description
Reconnaissance (TA0043)	T1589	Collect information from attack targets
Resource Development (TA0042)		
Initial Access (TA0001)	T1078	Initial approach with the collected credentials, transmit spear phishing emails with malware attachments, transmit spear phishing emails with malicious links
	T1566.001	
	T1566.002	
Execution (TA0002)	T1059.003	Execution command with cmd.exe, various Windows API used
	T1106	
Persistence (TA0003)	T1133	Secure initial access and persistence through an external remote service
Privilege Escalation (TA0004)	T1055.001	Inject DLL into another process for privilege escalation
Defense Evasion (TA0005)	T1027	Evade antivirus scan through string encryption
	T1140	
Credential Access (TA0006)	T1110	Attempt initial access by brute force, attempt to obtain network information, attempt to obtain process information,
	T1016	
	T1057	

	T1135	attempt to search the shared network folder
Discovery (TA0007)		
Lateral Movement (TA0008)	T1021.002	Attempt lateral movement through SMB, Attempt propagation through shared network drives
	T1080	
Collection (TA0009)		
Command and Control (TA0011)		
Exfiltration (TA0010)		
Impact (TA0040)	T1486	Encrypt files, Disable recovery by deleting volume shadow copies
	T1490	

Table 2. MITRE ATT&CK

References

[1] Disgruntled ransomware affiliate leaks the Conti gang's technical manuals
https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/

[2] Conti gang has made at least $25.5 million since July 2021
https://therecord.media/conti-gang-has-made-at-least-25-5-million-since-july-2021/

[3] Translated: Talos' insights from the recently leaked Conti ransomware playbook
https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html

[4] Alert (AA21-265A) Conti Ransomware
https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

[5] DarkTracer (Countries and corporations affected by Conti)
https://twitter.com/darktracer_int/status/1508671560890327043

[6] Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of
https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/

[7] NB65 Twitter
https://twitter.com/xxNB65/status/1513593777759428624

[8] Hackers use Conti's leaked ransomware to attack Russian companies
https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

[9] Conti's Hacker Manuals — Read, Reviewed & Analyzed
https://www.akamai.com/blog/security/conti

[10] Lessons from the Conti Leaks
https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html

[11] Conti Leaks: Examining the Panama Papers of Ransomware
https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html

[12] Costa Rica declares national emergency after Conti ransomware attacks
https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/

[13] Hacking Group Conti Chased by the **US** Exposed..."Divided Work Among 350 Specialists"
https://www.sedaily.com/NewsView/265ZQIYPI7

[14] [CONTI] Ransomware Group In-Depth Analysis
https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
www.ahnlab.com
www.asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab