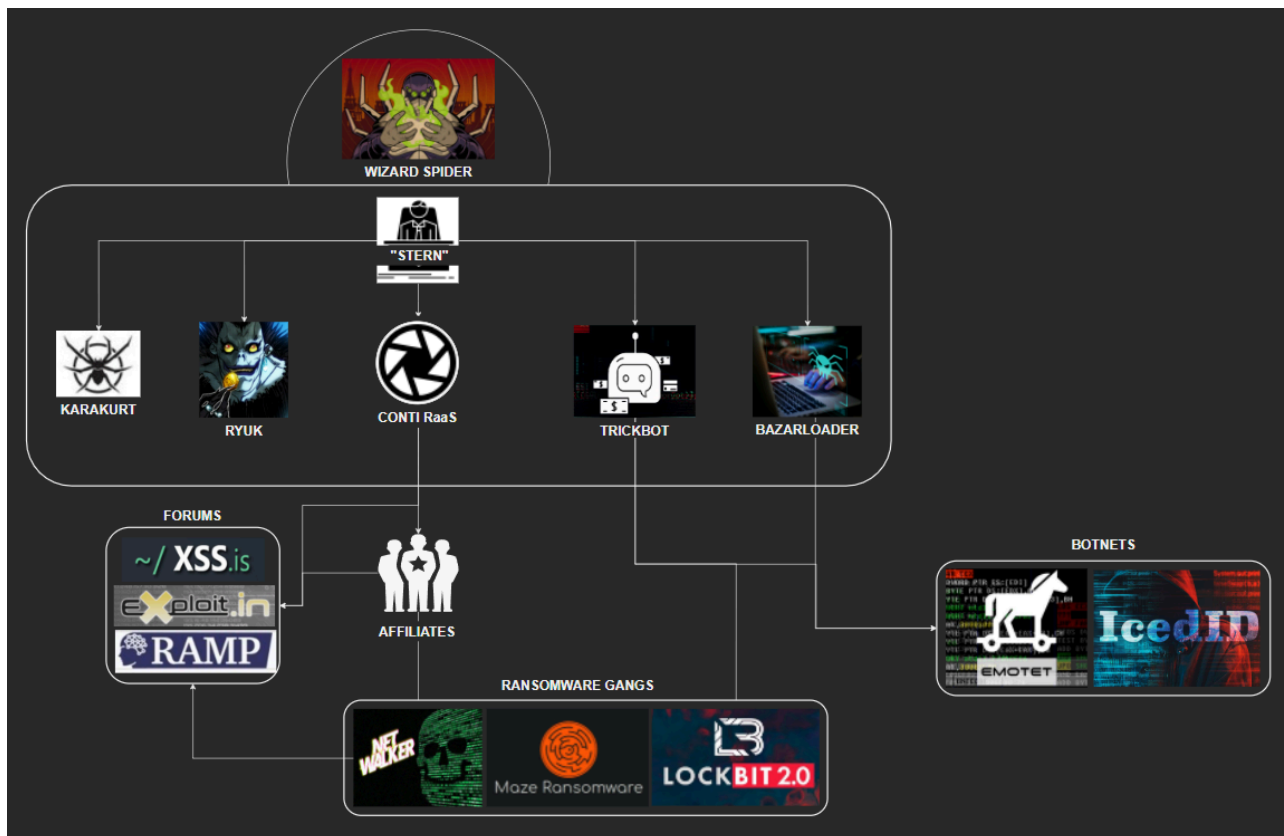


Lessons from the Conti Leaks

By BushidoToken

Published: 2022-04-17 · Archived: 2026-04-05 19:16:44 UTC



If you wanted to learn how an organized cybercriminal operation worked, look no further than the threat group known as Conti. The recent leaks of the group's chat logs have uncovered an unprecedented wealth of information and insights into how these veteran cybercriminals organize themselves.

Cyber Threat Intelligence (CTI) vendors and independent researchers have spent weeks poring over the Conti leaked chat logs and have uncovered dozens of very significant findings.

In this blog, I didn't want to duplicate what is already known (too much). I wanted to share some of the findings that I thought were the most interesting to me. To rapidly get up to speed on the Conti Leaks, I highly recommend other researchers to read the work in the following blogs:

- <https://www.trellix.com/en-gb/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html>
- <https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships>
- <https://intel471.com/blog/conti-leaks-ransomware-development>

- <https://intel471.com/blog/conti-leaks-cybercrime-fire-team>
- <https://arcticwolf.com/resources/blog/karakurt-web>
- https://research.checkpoint.com/wp-content/uploads/2022/03/map_index_v2.html
- <https://www.trmlabs.com/post/analysis-corroborates-suspected-ties-between-conti-and-ryuk-ransomware-groups-and-wizard-spider>
- <https://www.wired.co.uk/article/conti-ransomware-russia>
- https://ddanchev.blogspot.com/2022/02/exposing-conti-ransomware-gang-osint_28.html

I will also recommend to read what other researchers have tweeted about what they found in the Conti Leaks:

- Observable Tactics, Techniques, and Procedures (TTPs)
<https://twitter.com/TheDFIRReport/status/1498642505646149634>
- Cobalt Strike commands from RocketChat logs
<https://twitter.com/c3rb3ru5d3d53c/status/1499130574321197058>
- All CVEs discussed in the Conti chat server
<https://twitter.com/c3rb3ru5d3d53c/status/1499570311460753408>
- Proof Conti members are active on Twitter https://twitter.com/VK_Intel/status/1498761290709409792
- Conti member interviewed by local police https://twitter.com/VK_Intel/status/1498400616615395328
- Conti members acquire CarbonBlack and Sophos
<https://twitter.com/albertzsigovits/status/1498237945685422087>
- Conti's Exploit[.]in account <https://twitter.com/pancak3lullz/status/1499108972258906123>
- Conti's Bitcoin wallets <https://twitter.com/pancak3lullz/status/1498347648637624326>

With those out of the way, we can get to the meat of this blog. I cannot emphasize enough that these leaks are **gargantuan** and span years of the group's operations. I seem to find something new every time I take another look at them but now have enough for a blog of my own.

Reconnaissance

One major discovery in the Conti leaks is that multiple vendors have covered is the existence of an "OSINT Team" who gathers details on Conti's targets. This team uses multiple techniques, as well as commercial tools, to find every piece of information about a target that will support the end goal of domain-wide Conti ransomware deployment. This OSINT Team also may engage with the targets (HUMINT), posing as marketing or sales people, gathering details and information about managers, executives, and how the company operates for exploitation later.

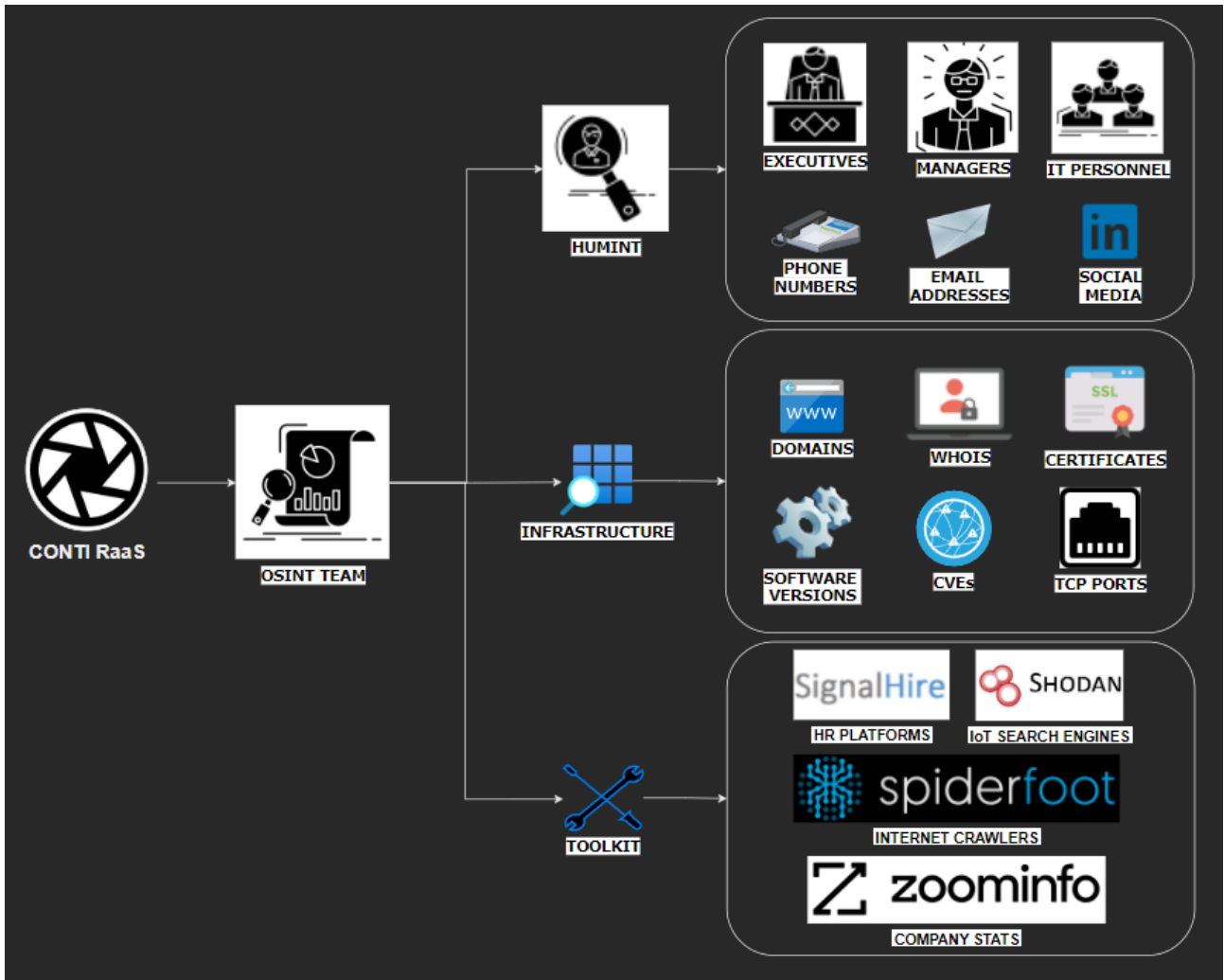


Fig. 1 - Overview of the Conti OSINT Team

Phishing

It is well-documented that Conti ransomware attacks often begin via a phishing email. The group has been launching widespread and targeted phishing campaigns for years using a [multitude of tactics](#). The Conti Leaks also shared some insights into how these phishing campaigns are orchestrated.

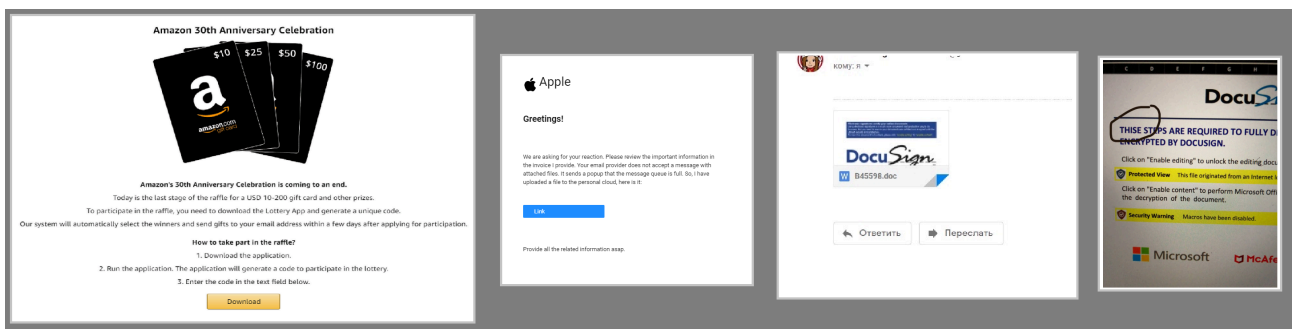


Fig. 2 - Example Phishing Email Templates used by Conti

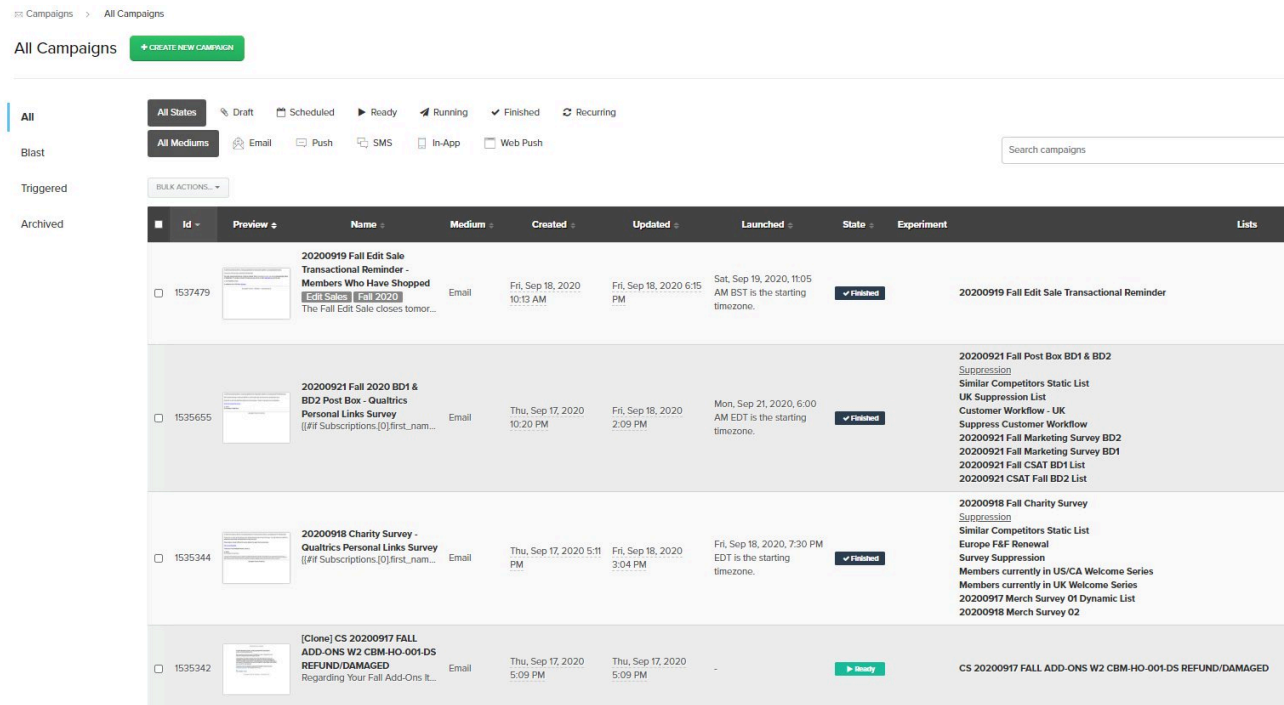


Fig. 3 - Iterable Email Marketing Dashboard shared in Conti Leaks in September 2020

Malware

The Conti Leaks revealed details on how a persistent cybercriminal operation develops its malware campaigns. The image below (see Fig. 4) highlights how the group works to test and develop its payloads against common detections systems used by its targets, such as ESET and Windows Defender.

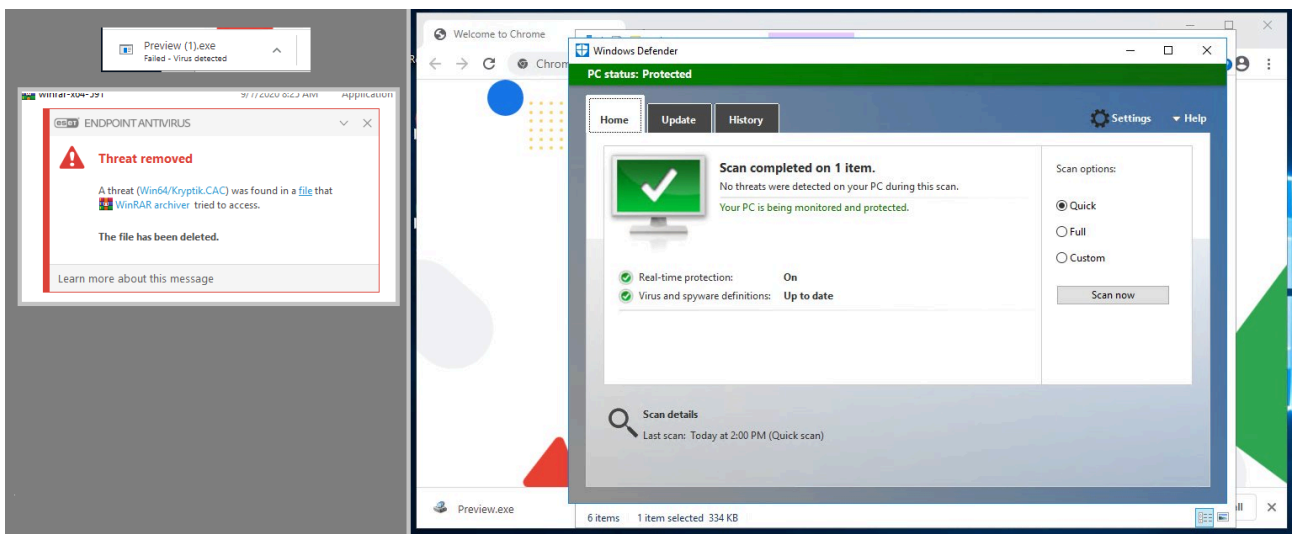


Fig. 4 - Conti members testing and making payloads fully undetectable (FUD)

Command and Control (C2)

Like any malware group, Conti needs server and hosting infrastructure to be able to launch its campaigns. This includes payload staging servers, proxy servers, C2 domains, Virtual Private Servers (VPS), and remote storage

for exfiltrated data.



The image shows a promotional banner for ZEHost with a blue and purple color scheme. The banner includes the ZEHost logo, navigation links for Servers, Domains, FAQ, and Contacts, and a main headline: "Try the best web hosting right now!". Below the headline, it lists benefits: "FREE Domain Name for 1st Year", "FREE SSL Certificate Included", "1-Click WordPress Install", and "24/7 Support". A "Get started" button is present. To the right is an illustration of server racks. Below the banner is a section titled "Our best plans:" featuring five pricing cards for different hosting services.

Plan Name	Starting Price (USD per Month)	Key Features
VPS Hosting	21.08	Managed VPS, latest server technology, enterprise class SSD storage, powered by Intel Xeon.
Servers	126	Fully managed, Intel Xeon CPU, SSD, next-gen firewall, high performance applications.
WP Hosting	0.25	Managed WordPress, fast, secure, includes installation, free backup, auto updates.
cPanel Hosting	1.15	High performance cPanel hosting, cloud infrastructure, optimal performance and reliability.
GoGeek	13.99	Unlimited websites, 40 GB web space, 100,000 visits monthly, unmetered traffic, free SSL, daily backup, free CDN, free email, managed WordPress, unlimited databases, 100% renewable energy, 90-day money-back.

Fig. 5 - Conti members discussed using ZEHost for hosting



Fig. 6 - Unknown botnet C2 panel shared by a Conti member

Tradecraft, Exploits, and 0days

What sets Conti apart from the rest of their peers in the cybercrime ecosystem is that members of this ransomware group are innovators and quick to leverage newly disclosed techniques. The Conti Leaks revealed multiple techniques used by Conti that had not been previously discussed publicly online.

```

"_source": {
  "timestamp": "2020-09-17T12:10:22.354394",
  "from_user": "target@q3mcco35auwcstmt.onion",
  "to_user": "bentley@q3mcco35auwcstmt.onion",
  "body_ru": "нам нужен разработчик\пктоый сможет получить акк девелопера в майкрософт сторе\пчтобы там внутри апрувить в сторе файлы",
  "body_en": "we need a developer who will be able to get a developer account in the microsoft store in order to approve files in the store inside"
},
    
```

Fig. 7 - Conti member "target" stating intentions in September 2020 to acquire a developer account in the Microsoft Store to approve their own files

```

"timestamp": "2021-08-03 14:43:24",
"server": "wfy76wigkpoqxbe6.onion",
"channel": "general",
"from_user": "giovanni",
"attachment": "",
"body_ru": "Я по этому ману делаю, вдруг поможет кому.\n`https://www.bussink.net/ad-cs-exploit-via-petitpotam-from-0-to-domain-domain/'",
"body_en": "I used this mana, maybe it will help someone.\n`https://www.bussink.net/ad-cs-exploit-via-petitpotam-from-0-to-domain-domain/'"
    
```

Fig. 8 - Conti member "giovanni" sharing a manual (aka "mana") for the PetitPotam exploit for Microsoft's NTLM authentication system in August 2021

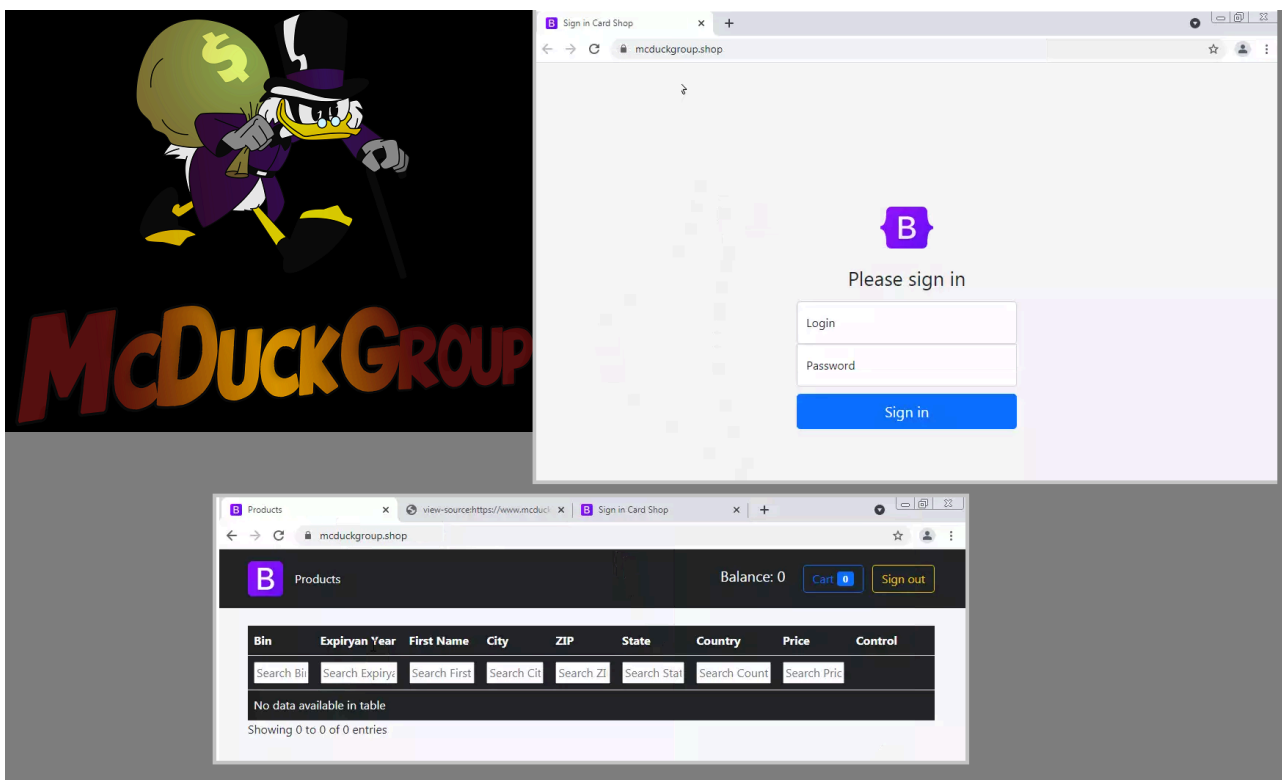


Fig. 12 - Logo of "McDuckGroup" shared to Conti Leaks

Researchers shared screenshots of all the links pasted into the Conti chats. One stood out to me: a logo with "McDuckGroup" and Scrooge McDuck. While some researchers I collaborate with theorized this was a ransomware rebrand, I managed to uncover it was the logo for a carding market currently under development. After Googling "McDuckGroup", a site called "mcduckgroup[.]shop" popped up as the first result. This is evidently a carding marketing due to the search bars for BIN numbers, Expiry dates, cardholder names, and addresses. Currently no data has been loaded onto the site.

Ransomware

A number of other ransomware groups are mentioned in the Conti Leaks. Trellix researchers highlighted how representatives of NetWalker, MAZE, and LockBit all have a presence in the Conti chat server. Ryuk, Diabol, REvil, AvosLocker, BlackMatter, and Crylock ransomware families are all also mentioned in the Conti Leaks.

```
<bomba777> did you see the news yesterday about the revil gang? [30.09.2020 11:15:30]
<bomba777> that they deposited lam bucks on the xss forum [30.09.2020 11:15:40]
<bomba777> people live :) [09/30/2020 11:16:00]
<gagarin66> yes, I saw the topic [09/30/2020 11:16:14]
<bomba777> here are the oligarchs.. [09/30/2020 11:16:24]
<gagarin66> well, I don't see a problem at all) [09/30/2020 11:16:27]
<gagarin66> yesterday here is 900k [09/30/2020 11:16:30]
<gagarin66> vylpata was) [09/30/2020 11:16:35]
<bomba777> by you? [30.09.2020 11:16:38]
<gagarin66> from maze [09/30/2020 11:16:38]
<gagarin66> yes [09/30/2020 11:16:44 AM]
<bomba777> fuck why am I the only poor one so far.. [30.09.2020 11:16:52]
<gagarin66> make bots"
```

Fig. 13 - "bomba777" and "gagarin66" (a MAZE affiliate) discuss REvil depositing 900k in Bitcoin to XSS[.]is

```
"timestamp": "2022-01-23 01:51:45",
"server": "xflemdsxjrjilw34dsxpvrpxp5whnaut7hc5xejwuqs6eqrkt77bxxwid.onion",
"channel": "general",
"from_user": "rags",
"attachment": "",
"body_ru": "Парни криптовалюте походу запретить вплоть до уголовного преследования, а все благодаря кому? REvil поблагодарим этих людей что у них мозгов хватило снимать деньги и все что  
отжали, складывать на складе у себя в квартире, а теперь нам еще головная боль как свои кровные вывести в реал. Быстрыкин посидел подумал, ну думает это делитанты, а есть не делитанты, и  
че там он походу боится представить. =)",
"body_en": "Guys, it's a campaign to ban cryptocurrency up to criminal prosecution, and all thanks to whom? REvil thank these people that they had the brains to withdraw money and put  
everything they squeezed out in a warehouse in their apartment, and now we still have a headache how to bring our hard-earned money into real life. Bystrykin sat and thought, well, he  
thinks these are delitants, but there are not delitants, and why is he afraid to imagine a campaign. =)"
}
```

Fig. 14 - "rags" discusses REvil arrests in January 2022 by Russian FSB, blaming them for the alleged crackdown on cryptocurrency in Russia

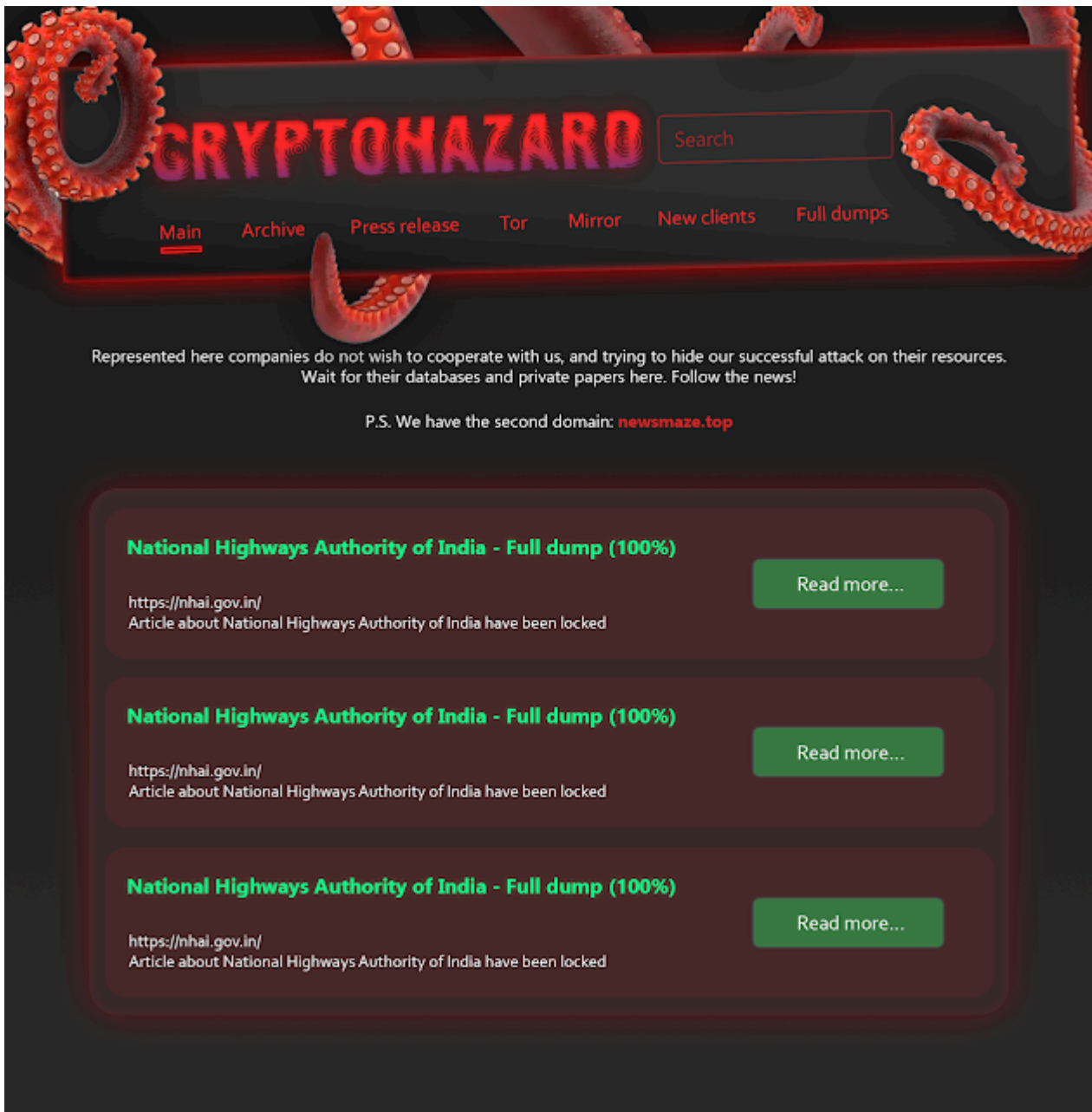


Fig. 15 - "CRYPTOHAZARD" leak site linked to MAZE ransomware (newsmaze[.]top)

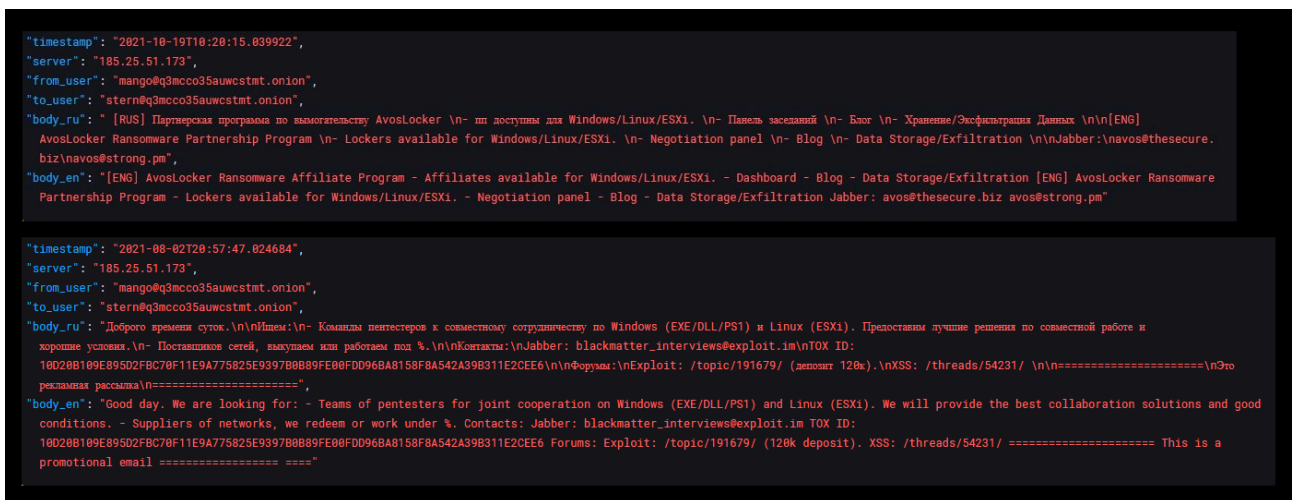


Fig. 16 - "mango" and "stern" shared adverts for AvosLocker and BlackMatter

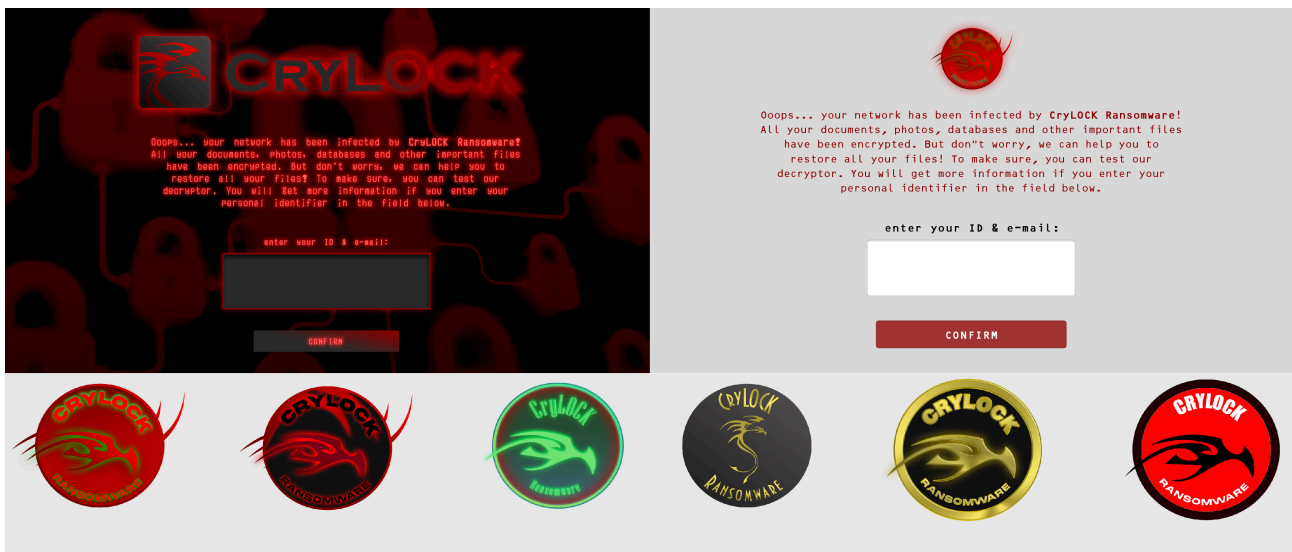


Fig. 17 - Logos and designs for CryLock ransomware shared to Conti server



Fig. 18 - Conti V3 Locker source code disclosed publicly by @contileaks Twitter account

Samples of Conti v3

- locker.exe e1b147aa2efa6849743f570a3aca8390faf4b90aed490a5682816dd9ef10e473
- locker_x86.dll fb737da1b74e8c84e6d8bd7f2d879603c27790e290c04a21e00fbde5ed86eee3
- cryptor.exe 5f3ae6e0d2e118ed31e7c38b652f4e59f5d5745398596c8b31248eda059778af

Closing Comments

The Conti Leaks have provided cybercrime researchers an unparalleled look into how Russian-speaking organized hacking groups operate. The leaks also supplement the Conti Playbook that was [leaked](#) by a disgruntled member in August 2021. As a community of cybersecurity researchers, we now know more about the Conti ransomware group than any other threat group in history.

For the Conti group itself, however, it appears to be business as usual (BAU). Less than one week after the Conti chats were leaked, new victims were uploaded to the ContiNews darknet site.



Fig. 19 - New victims added to ContiNews shortly after the Conti Leaks

BleepingComputer also [reported](#) on hacktivist groups, such as Network Battalion 65 (aka NB65), are leveraging a modified version of the leaked Conti v3 source code already. The group has targeted organizations in Russia for retribution over the invasion in Ukraine. (Sample available [here](#))

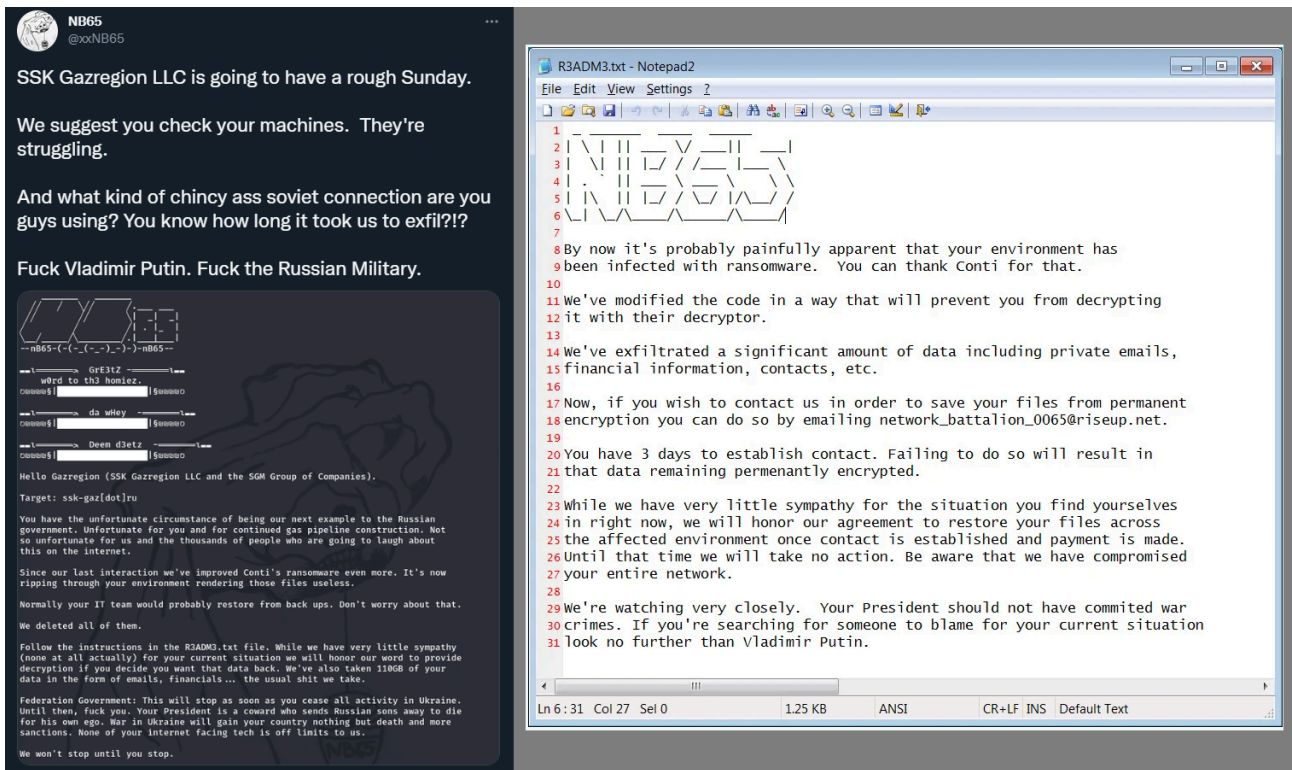


Fig. 20 - NB65 modified version of Conti v3 ransomware

Conti has seemingly recovered from the leaks and might be at the 'too big to fail' stage of operations. The Russian state is clearly fully aware of Conti's operations and allows them to operate with impunity. Researchers at Trellix highlighted the group's connections to the Russian state and how the intelligence services also benefit from Conti's coveted network access to high-profile organizations around the world.

Lastly, I hope you enjoyed the blog. There are still likely some secrets yet to be revealed in the Conti Leaks. I appreciate the help and resources shared by researchers online. S/O to Curated Intel, Trellix, Intel471, Secureworks, The DFIR Report, and researchers such as @vk_intel, @pancak3lullz, and @c3rb3ru5d3d53c, and many others!

Source: <https://blog.bushidotoken.net/2022/04/lessons-from-conti-leaks.html>