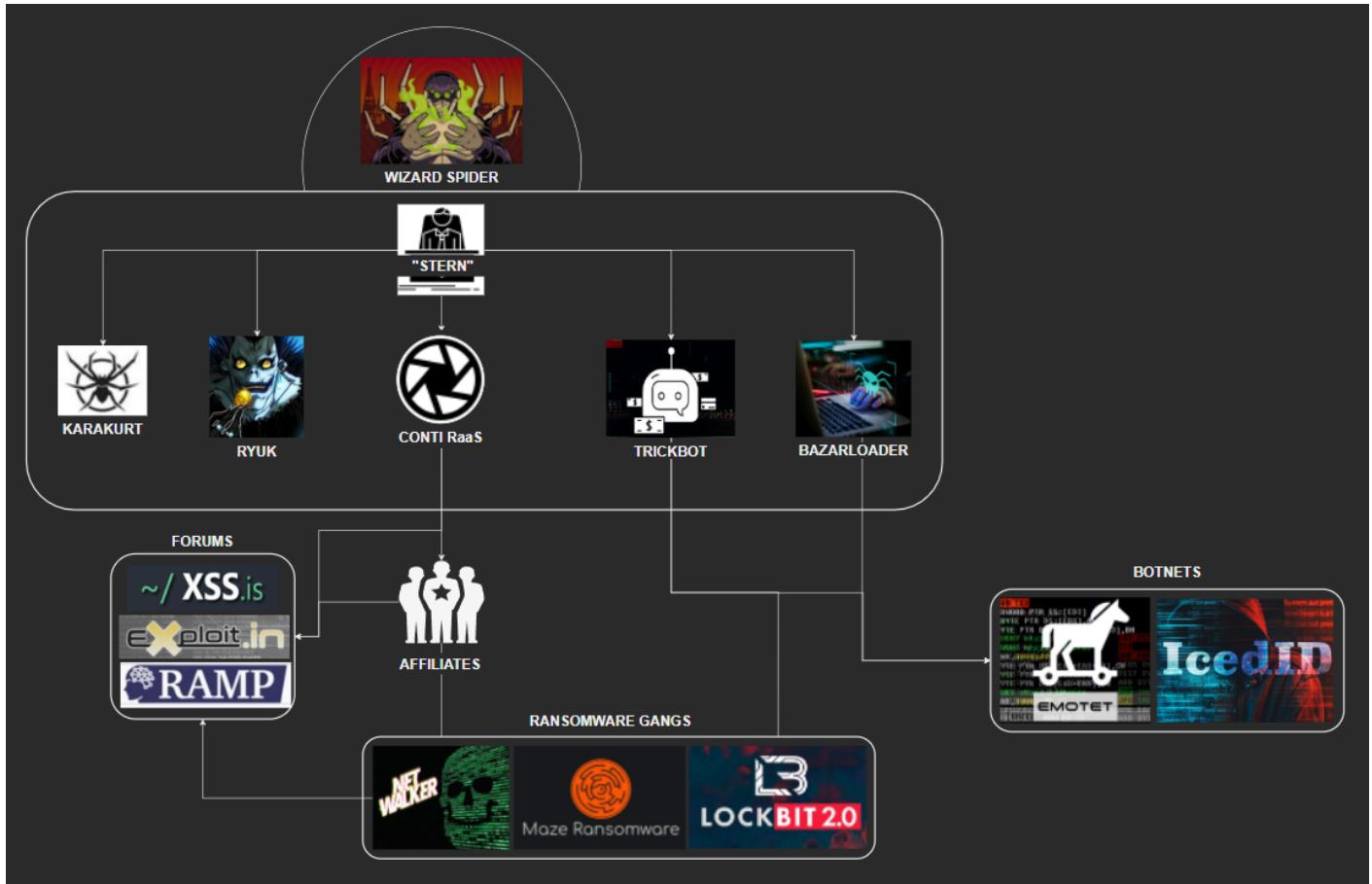


Lessons from the Conti Leaks

BushidoToken :: 4/17/2022



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:

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.

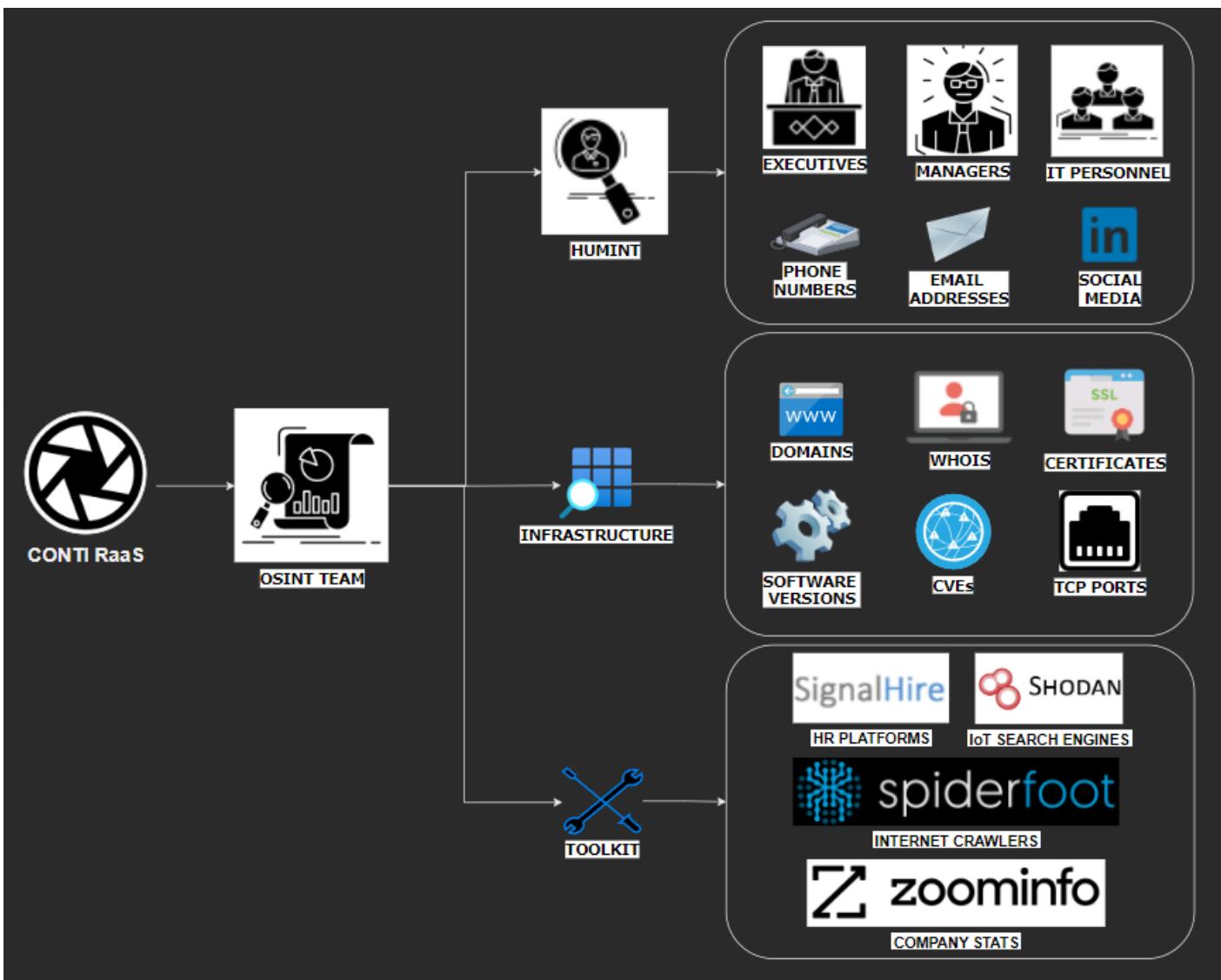


Fig. 1 - Overview of the Conti OSINT Team

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.

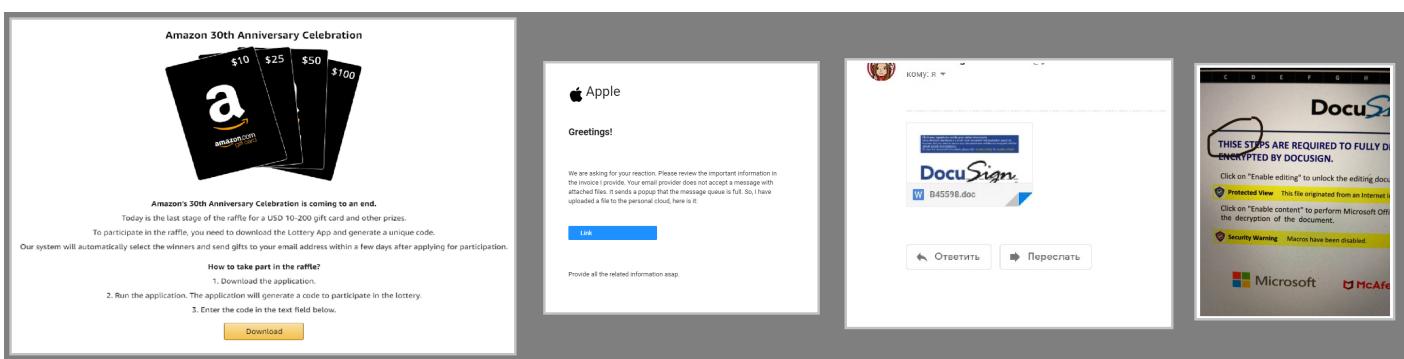


Fig. 2 - Example Phishing Email Templates used by Conti

All Campaigns

+ CREATE NEW CAMPAIGN

The dashboard displays four campaign entries:

- 20200919 Fall Edit Sale Transactional Reminder**: An Email campaign from Fri, Sep 18, 2020 at 10:13 AM to Sat, Sep 19, 2020 at 11:05 AM BST. Status: Finished.
- 20200921 Fall 2020 BD1 & BD2 Post Box - Qualtrics Personal Links Survey**: An Email campaign from Thu, Sep 17, 2020 at 10:20 PM to Fri, Sep 18, 2020 at 2:09 PM. Status: Finished.
- 20200918 Fall Charity Survey Suppression**: An Email campaign from Thu, Sep 17, 2020 at 5:11 PM to Fri, Sep 18, 2020 at 3:04 PM. Status: Finished.
- CS 20200917 FALL ADD-ONS W2 CBM-HO-001-DS REFUND/DAMAGED**: An Email campaign from Thu, Sep 17, 2020 at 5:09 PM to Thu, Sep 17, 2020 at 5:09 PM. Status: Ready.

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.

The image shows two windows side-by-side:

- Left Window (Win32 ENDPOINT ANTIVIRUS):** A threat was found in a file named "Preview (1).exe". The file was a WinRAR archive that tried to access a file. The threat was removed, and the file was deleted.
- Right Window (Windows Defender):** A scan was completed on 1 item, with no threats detected. Real-time protection is on, and virus and spyware definitions are up to date. The last scan was at 2:00 PM (Quick scan).

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 the homepage of ZEHost. At the top, there is a navigation bar with links for 'Servers', 'Domains', 'FAQ', and 'Contacts'. Below the navigation, a large blue banner features the text 'Try the best web hosting right now!' in white. To the left of this text, there is promotional information: 'FREE Domain Name for 1st Year', 'FREE SSL Certificate Included', '1-Click WordPress Install', and '24/7 Support'. A 'Get started' button is located at the bottom left of the banner. To the right of the text, there is a 3D illustration of three server racks connected to a cloud icon with an upward arrow, symbolizing data upload. Below the banner, the heading 'Our best plans:' is displayed in large blue text. Five service cards are listed below this heading:

VPS Hosting	Servers	WP Hosting	cPanel Hosting	GoGeek
Our managed VPS is built around the latest server technology with enterprise class SSD storage for awesome performance. Powered by Intel Xeon.	Fully managed & featuring Intel Xeon CPUs, SSD & next-gen firewall options designed for high performance applications.	Our managed WordPress Hosting is fast, secure and includes installation, free backup, and auto updates as part of our best packages.	High performance cPanel hosting built on our cloud infrastructure for optimal performance and reliability but at low cost.	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 switch 90-Days Money-Back
Starting at 21.08 USD per Month	Starting at 126 USD per Month	Starting at 0.25 USD per Month	Starting at 1.15 USD per Month	Starting at 13.99 USD per Month
More	More	More	More	More

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\покоторый сможет получить акк девелопера в майкрософт сторе\чтобы 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": "wfy76wigkpxqbe6.onion",
"channel": "general",
"from_user": "giovanni",
"attachment": "",
"body_ru": "Я по этому ману делал, вдруг поможет кому.\nhttps://www.bussink.net/ad-cs-exploit-via-petitpotam-from-0-to-domain-domain/",
"body_en": "I used this mana, maybe it will help someone.\nhttps://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

```

"timestamp": "2021-06-11T07:03:36.161991",
"server": "185.25.51.173",
"from_user": "mango@q3mcco35auwcstml.onion",
"to_user": "professor@q3mcco35auwcstml.onion",
"body_ru": "Добрый день. Есть 0-day эксплойт позволяющий привилегий для уязвимости типа Use-after-Free в драйвере WIDFRD.sys. Эксплойт реализован для Windows 10 x64 1607, 1703, 1709, 1803, 1809, 1903, 1909. Уязвимость есть и в 2804 и выше, но соответствующий код в драйвере был переписан, и падение ОС в BSOD происходит из-за срабатывания ложной уязвимости на размещении нулевого указателя. Есть некоторые нюансы по эксплуатации: не все системы могут быть уязвимы, так как есть зависимость от конфигурации оборудования. Эксплуатация происходит путем отключения SMEP (модификации CR4), модификации PTE/PML4 при необходимости и выполнения кода, осуществляющего замену токена целевому процессу на системный. Публичное обявление здесь, поскольку моим постоянным клиентам нужно не покупать, а я лично из тех, кто на форуме изложил желание купить, никто не отвечает. Цена - 60k, обсуждаема. Желающим могу написать и выдать уязвимость, которая при запуске на интересующий систему скрипт, ухмыла OS или нет. Первый контакт в ЛС, потом в jabber. \n\nhttps://filetransfer.io/data-package/cyCDTWGfLink\n\nПароль: bvdvivz2861rJVV1\n\nЧто происходит на видео:\n1. Запускается процесс wud.exe, эксплуатирующий уязвимость.\n2. wud.exe создает процесс cmd.exe и делает 5-секундовую паузу для проверки привилегий.\n3. Запускается созданной командой notepad.exe (экземпляр 1).\n4. Спустя некоторое время проверка привилегий и запускается notepad.exe (экземпляр 2).\n5. В Process Explorer-е проверка уровня cmd.exe и посмотрено 2 экземпляра notepad.exe. Видно, что экземпляр 1 запущен со средним IL, второй (когда права cmd.exe уже были повышенены) с SYSTEM.".
"body_en": "Good afternoon. There is a Use-after-Free vulnerability in the WIDFRD.sys driver. The exploit was implemented for Windows 10 x64 1607, 1703, 1709, 1803, 1809, 1903, 1909. The vulnerability exists in 2804 and later, but the corresponding code in the driver was rewritten, and the OS crashes into a BSOD before the target null pointer dereference vulnerability is triggered. There are some nuances in operation: not all systems may be vulnerable, as there is a dependence on the hardware configuration. Operation occurs by disabling SMEP (modification CR4), modifying PTE / PML4 if necessary, and executing code that replaces the token for the target process with the system one. I am publishing an ad here, because my regular customers do not need / did not fit, and in a personal message from those who expressed a desire to buy on the forum, no one answers. Price - 60k, negotiable. For those who wish, I can write and issue a utility that, when launched on the system of interest, will tell whether the OS is vulnerable or not. The first contact in the LAN, then in the jabber. I will add: The exploit is sold in one hand. Video of work: https://filetransfer.io/data-package/cyCDTWGfLink Password bvdvivz2861rJVV1 What happens in the video: 1. The wud.exe process is launched, exploiting the vulnerability. 2. wud.exe spawns a cmd.exe process and pauses for 5 seconds to check privileges. 3. I launch notepad.exe from the created console (instance 1). 4. After some time, I check the privileges and run notepad.exe (instance 2). 5. In Process Explorer I check the cmd.exe level and alternately 2 instances of notepad.exe. It can be seen that instance 1 is launched with medium IL, the second (when the rights of cmd.exe have already been elevated) with SYSTEM."
},

```

Fig. 9 - Conti member "mango" sharing the opportunity to buy a 0day privilege escalation exploit in the Windows WIDFRD.sys driver for "60k" in June 2021

```

"_source": {
  "timestamp": "2020-06-25T14:11:07.77127",
  "from_user": "revers@q3mcco35auwcstml.onion",
  "to_user": "stern@q3mcco35auwcstml.onion",
  "body_ru": "[07:32:37] <revers> спасибо @sashagrey за отчеты по группе тупла \n[07:33:09] <revers> работают они уже более 10 лет \n[07:34:34] <revers> методы заражения так же как и у нас но сколько я понимаю спам с документами содержащими уязвимости адбоя либо макросы \n[07:34:48] <revers> так же ион домены как и у нас \n[07:35:01] <revers> + еще добавлены схемы сплоев \n[07:35:23] <revers> и еще я обратил внимание на то что они снiff трафик и подменяют бинарь \n[07:35:34] <revers> скорее всего это делается митмом \n[07:38:05] <revers> векторы распространения по сети используют в основном такие же как и у нас \n[07:38:19] <revers> ищут уязвимые хосты под спloit ms17-10 \n[07:38:54] <revers> на сколько в отчетах написано икода из реверса их софта приступает крипапца из него делается вывод что парни русские \n[07:39:19] <revers> только я одного не понял зачем они заражают пк на территории ру и си \n[07:39:29] <revers> имен в группе много \n[07:43:34] <revers> и ее привлекают к правительстальным хакерам",
  "body_en": "[07:32:37]<revers> hello [07:32:55]<revers> I read the reports on the Turla group [07:33:09]<revers> they have been working for more than 10 years [07:34:34]<revers> infection methods are the same as ours, as far as I understand spam with documents containing adobe vulnerabilities or macros [07:34:48]<revers> just non domains like ours [07:35:01]<revers> + bundles of sploofs have been added [07:35:23]<revers> and I also noticed that they sniff traffic and replace binaries [07:35:34]<revers> most likely this is done by mitmo [07:38:05]<revers> propagation vectors over the network are used basically the same as ours [07:38:19]<revers> looking for vulnerable hosts for the ms17-10 exploit [07:38:54]<revers> how much is written in the reports, based on the reverse of their software, there is Cyrillic, from which it is concluded that the guys are Russian [07:39:19]<revers> only I didn't understand one thing why they infect PCs on the territory of ru and cis [07:39:29]<revers> the group has many names [07:43:34]<revers> and she is equated with government hackers"
},

```

Fig. 10 - Conti member "revers" shares that they read reports on the "Turla" group (a Russian cyber-espionage APT linked to the FSB)

A Cybercrime Empire

Researchers have stated that they believe Conti has up to 150+ members worldwide. If we do the math, each member is allegedly getting paid on average \$2,000 per month which equals around roughly \$300,000 per month in Conti "employee" salaries and roughly \$3,600,000 per year. This is a LOT for a cybercrime group. With this amount of purchasing-power, it is only natural Conti leadership began to wonder about acquisitions and starting their own forums, carding shops, and even [cryptocurrency platforms](#).

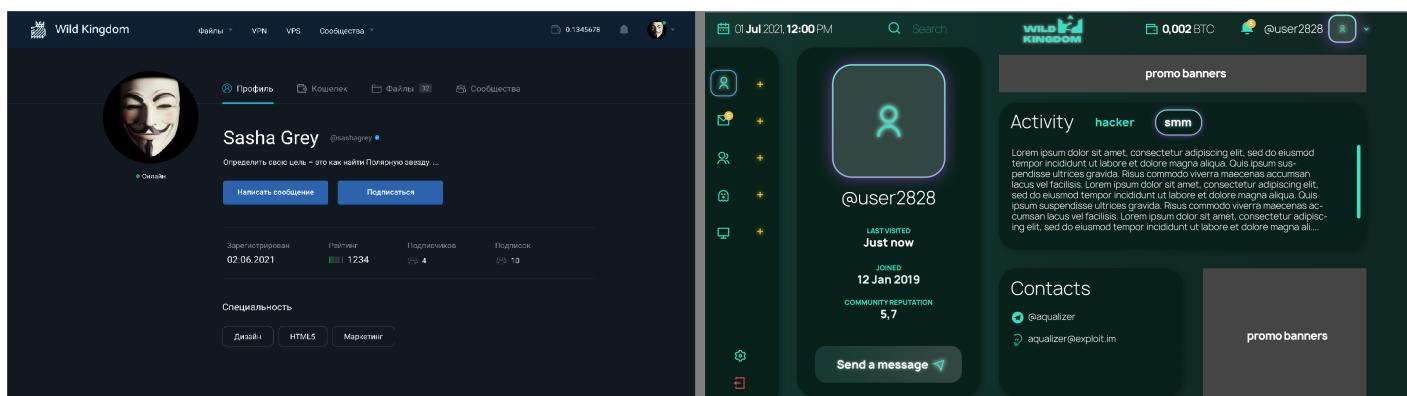


Fig. 11 - Conti members design what their new cybercrime forum might look like

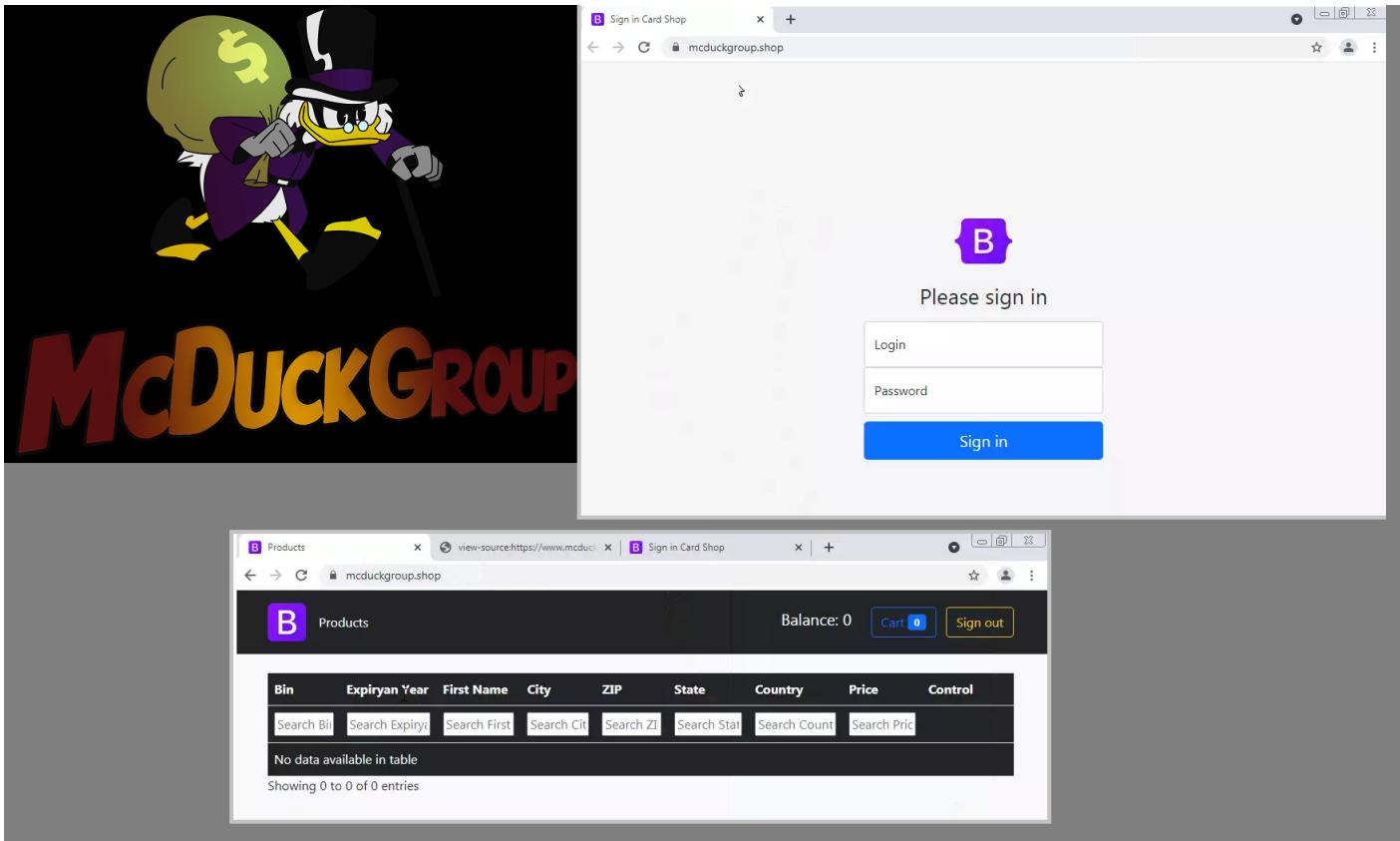


Fig. 12 - Logo of "McDuckGroup" shared to Conti Leaks

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, Diavol, 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": "xflemdsxjrjilw34dsxpvrxp5whnaut7hc5xejwuqs6eqrkt77bxkwid.onion",
"channel": "general",
"from_user": "rags",
"attachment": "",
"body_ru": "Парни криптовалюту походу запретить вплоть до уголовное преследования, а все благодаря кому? Revil поблагодарили этих людей что у них мозги хватило снимать деньги и все что отжали, складывать на складе у себя в квартире, а теперь нам еще головная боль как свои кровяные вывести в реал. Быstrykin посидел подумал, ну думает это delitants, а есть не delitants, и че там он похому боится преставлять. =)",
"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 that 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)

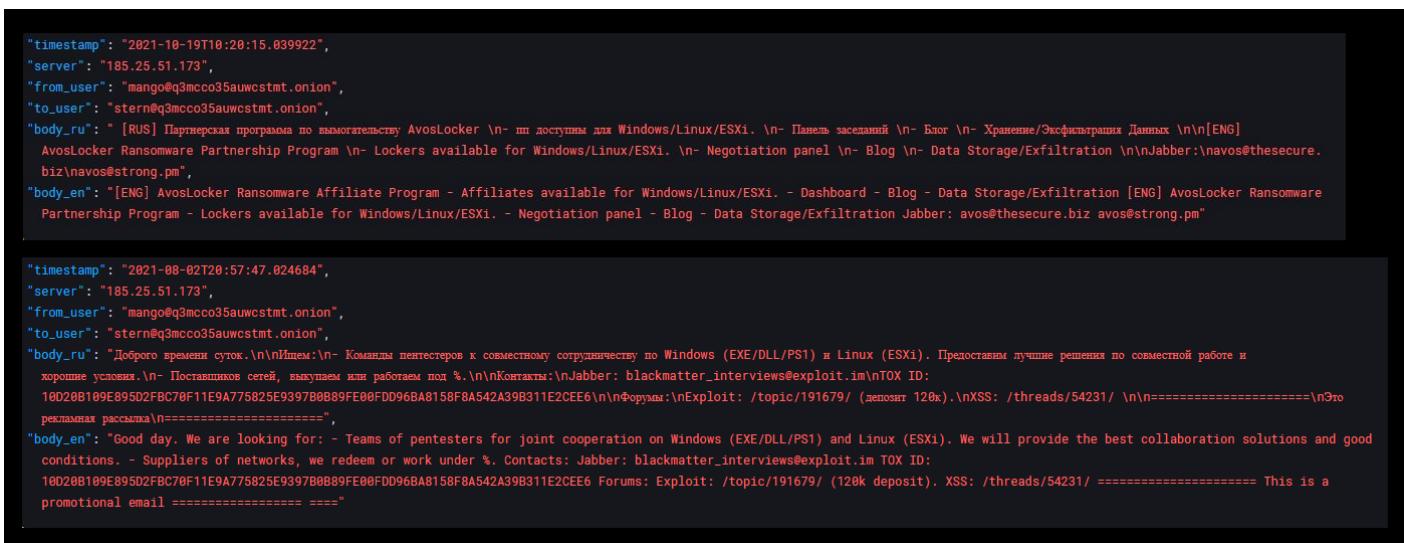


Fig. 16 - "mango" and "stern" shared adverts for AvosLocker and BlackMatter

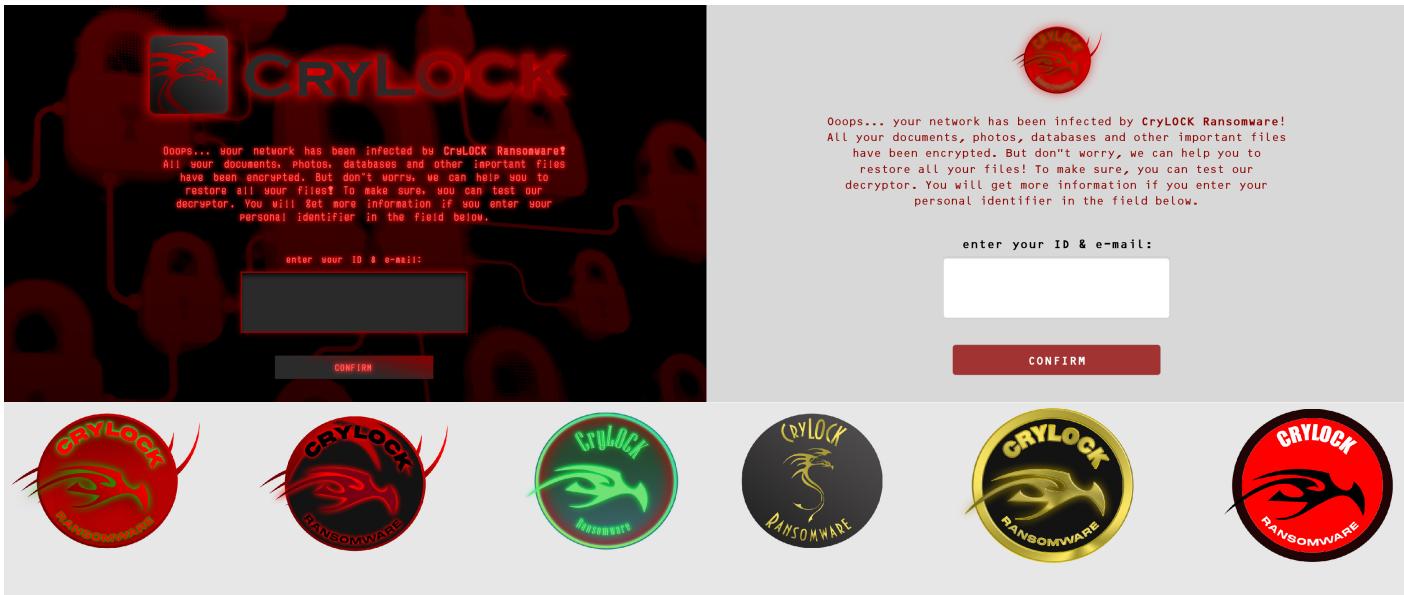


Fig. 17 - Logos and designs for CryLock ransomware shared to Conti server

```

#include "cryptor.h"
#include "mrph.h"
#include <comdef.h>
#include <Wbemidl.h>
#pragma comment(lib, "wbemuuid.lib")

STATIC CONST DWORD BufferSize = 5242880;
STATIC CONST BYTE g_ContiPattern[16] = { 0xab, 0xff, 0x63, 0xa1, 0x6f, 0xa2, 0x6e, 0xe, 0xa3, 0x74,
0x69, 0xbff, 0x4c, 0xdd, 0xff, 0xa1 };
STATIC process_killer::PPID_LIST g_WhitelistPids = NULL;

enum ENCRYPT_MODES {
    FULL_ENCRYPT = 0x24,
    PARTLY_ENCRYPT = 0x25,
    HEADER_ENCRYPT = 0x26
};

```

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.

The screenshot displays six victim profiles from the ContiNews darknet site:

- "BUHCK GRUPPE"**
Published 1%
3/3/2022 | 697 | READ MORE »
Link: <https://www.buhck.de>
Buhck GmbH & Co. KG
Südring 38
21465 Wentorf
Telefon: +49 (0)40/72 00 00 - 0
Telefax: +49 (0)40/72 00 00 - 44
E-Mail: info@buhck.de
Dafür steht die familiengeführte Buhck Gruppe mit ihren Standorten in der Metropolregion Hamburg als einer der großen Umweltdienstleister in Norddeutschland seit mehr als 115 Jahren. Von der Entsorgung und Verwertung von Müll und Abfall mit eigenem Containerdienst über den Handel mit Baustoffen aus dem Recycling und der Natur bis hin zum Rohr- und Kanalservice - unsere Unternehmen sind auf viele wichtige Bereiche der Umweltwirtschaft spezialisiert und ergänzen sich dabei ideal. Lernen Sie uns kennen!
- "GRUPPO ANGELANTONI"**
Published 4%
3/3/2022 | 53 | READ MORE »
Link: <https://www.angelantoni.com>
LOCALITA' CIMACOLLE
464 MASSA MARTANA
PERUGIA, 06056
Italy
ANGELANTONI GROUP:
CREATIVITY, EXPERIENCE, DESIGN.
From space simulation to the storage of human blood and plasma; from lithium battery testing to thin film deposition. Technology, creativity and design for improving product reliability, materials durability and process safety, since 1932.
- "SPORT VISION"**
Published 1%
3/3/2022 | 37 | READ MORE »
Link: <https://www.sportvision.rs>
Milentija Popovića 5v, Belgrade,
Central Serbia, Serbia
Sports inventory Serbian retailer. Has several offices in Bulgaria, Serbia, Romania, etc.
- "UNIVERSITY OF NEUCHÂTEL"**
Published 1%
3/3/2022 | 697 | READ MORE »
Link: <https://unine.ch>
University of Neuchâtel
Avenue du 1er-Mars 26
2000 Neuchâtel
Tel.: +41 32 718 10 00
contact@unine.ch
- "HOL-MAC CORP."**
Published 1%
3/3/2022 | 53 | READ MORE »
Link: <https://www.hol-mac.com>
P.O. Box 349
Bay Springs, MS 39422
Phone: 800-844-3019 / (601) 764-4121
Fax: (601) 764-4282
HolMac has over 50 years in steel
- "WARNING"**
Published 1%
3/3/2022 | 37 | READ MORE »
Link: [As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory](#)

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](#))

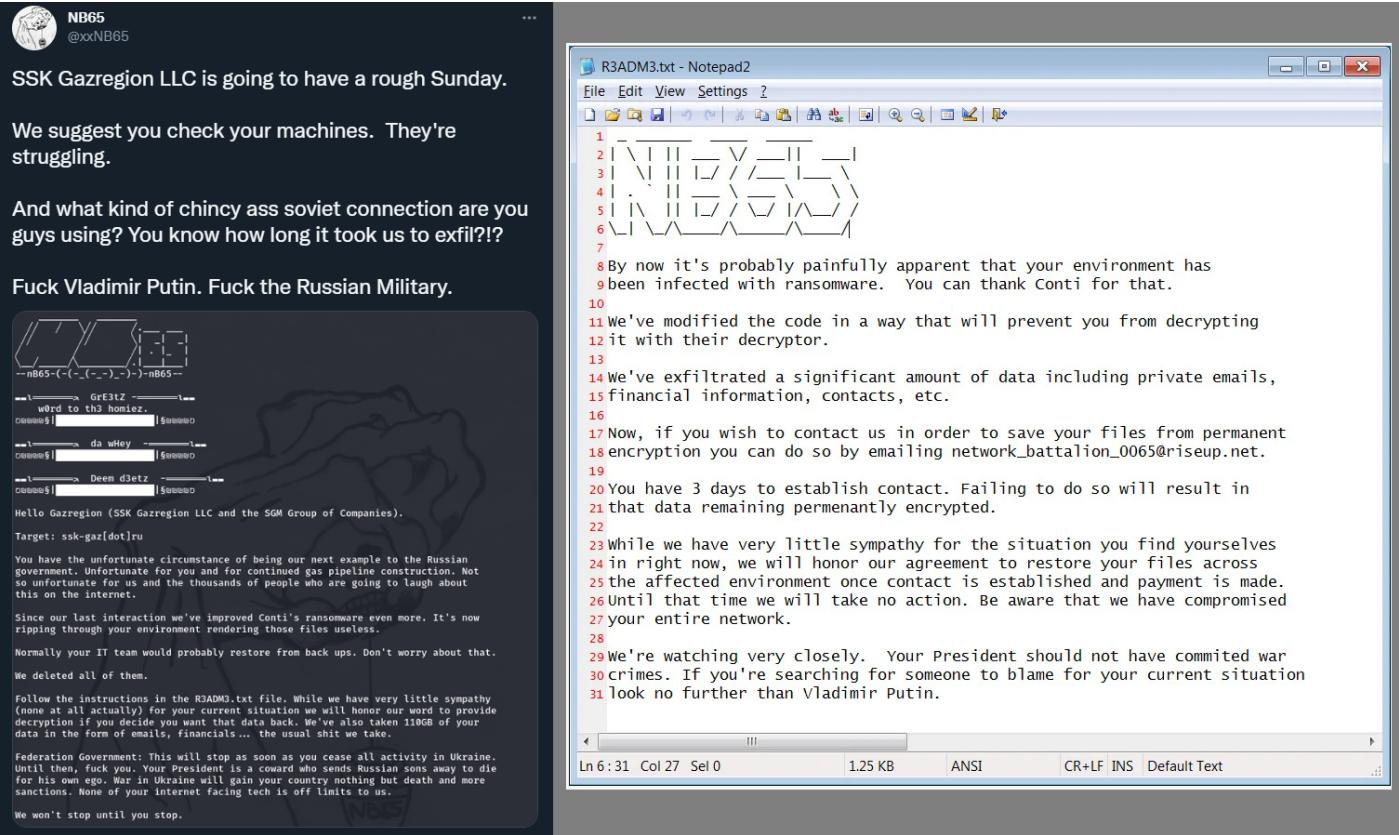


Fig. 20 - NB65 modified version of Conti v3 ransomware

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!