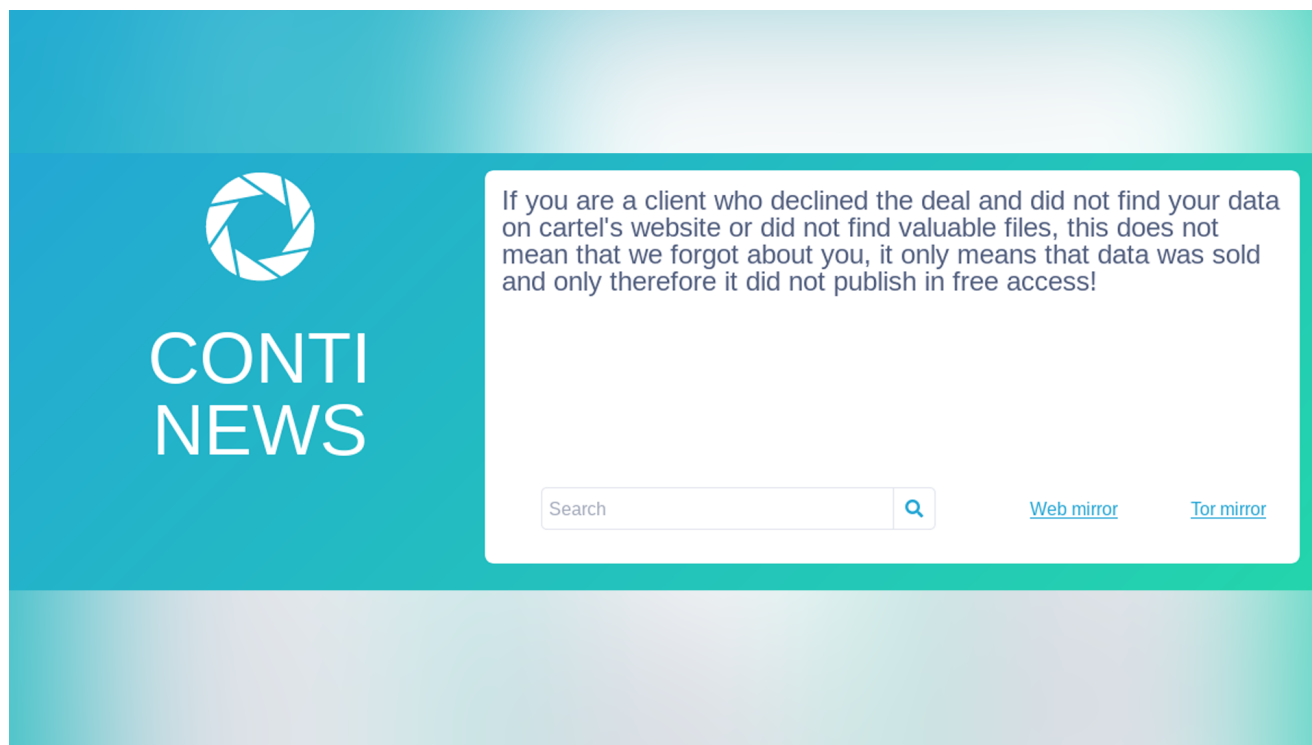


An insider insights into Conti operations – Part One

sekoia.io/en/an-insider-insights-into-conti-operations-part-one

August 17, 2021



This is the first of two blog posts, where we focus on the Conti ransomware group whose training material was recently leaked on a cybercrime forum. To provide some context to this analysis, we describe Conti's evolution and success since its origin. We then contextualize the leaks thanks to our observations on underground forums and analyze it in terms of threat intelligence. The second blog post will give some details on the techniques used by Conti operators and how to detect them.

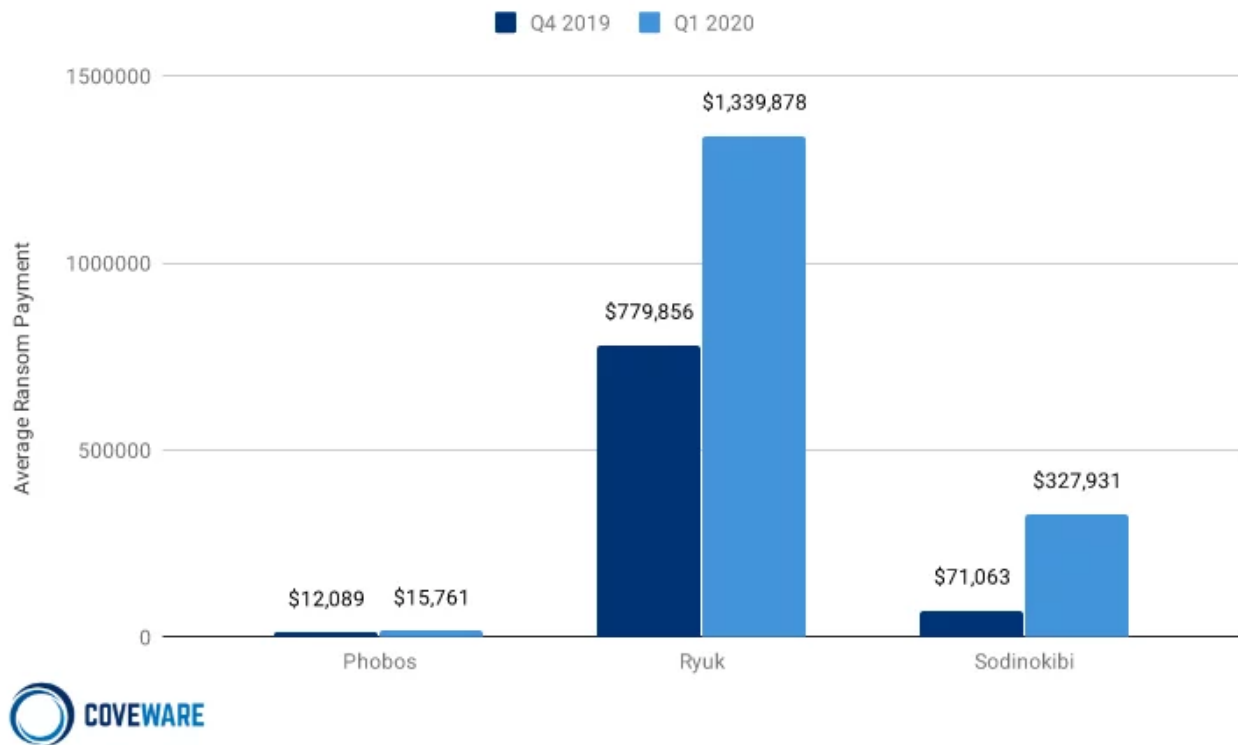
The origin of Conti ransomware

Conti and Ryuk were developed and operated by a group dubbed Wizard Spider by CrowdStrike (aka UNC1878, Grim Spider, Conti gang) and some affiliates. Wizard Spider started its activity in 2016 by conducting financial fraud campaigns using the TrickBot banking trojan¹. The link between Conti and Wizard Spider was confirmed by Clearsky, following a bitcoin transaction after a successful ransomware attack².

In August 2018, the actor previously using TrickBot started to use a new ransomware called Ryuk to target large organizations, asking for high ransom amounts. Wizard Spider seemed to follow the Big Game Hunting (BGH) trend started by BitPaymer's gang one year earlier³. Ryuk's activity made the project famous in the ransomware business. According to

Coveware, in Q1 2020, the average ransomware payment on behalf of the group was over \$1.3 million. During this period, we can note the attacks against major US companies such as Electronic Warfare Associates (EWA), a US Government contractor⁴.

Average Ransom Payment: Top 3 Ransomware Types



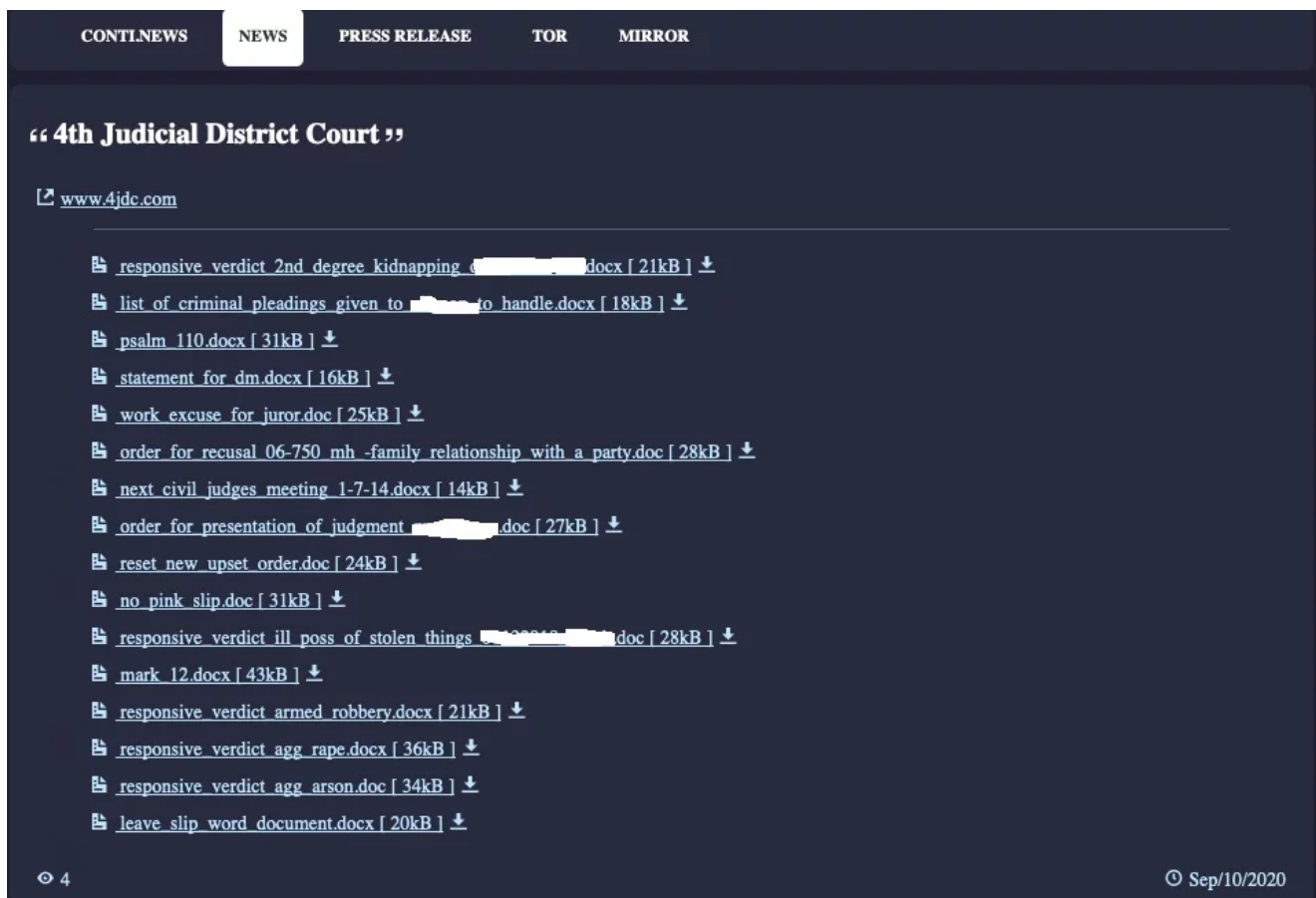
Average ransomware payment of Phobos, Ryuk & Sodinokibi in Q4 2019 and Q1 2020⁵

The group has constantly evolved its arsenal, reacting to attempts to block them. In 2020, they developed BazarLoader, which has a high level of obfuscation. They also regularly added known vulnerabilities such as Eternal Blue, Zerologon, and more recently, PrintNightmare to their arsenal.

Their loaders were often delivered through phishing email or credentials previously obtained from Emotet or IcedID activity. The affiliates probably used accesses sold by initial access brokers.

Conti appears in February 2020 as a Ryuk successor using the new data blackmailing technique⁶ (aka double extortion technique). They created a website to publish stolen data in case of non-payment of the ransom and to have a good-looking chat interface to communicate with victims and others. According to ransom notes SEKOIA studied, Ryuk operators used to communicate with victims through secure email services such as Protonmail or Tutanota.

Threatening to leak sensitive files is great to increase the pressure on companies and therefore increase the probability that the ransom will be paid and to increase its amount. Note that Wizard Spider seems to consider the file decryptor and the deletion of the stolen files as two different services.



The screenshot shows a website with a dark blue header and a white navigation bar. The navigation bar contains the following items: CONTI.NEWS, NEWS (highlighted), PRESS RELEASE, TOR, and MIRROR. Below the navigation bar, the page title is "4th Judicial District Court". Underneath the title, there is a link to "www.4jdc.com". The main content area is a list of document links, each preceded by a small icon of a document and followed by a download icon. The links are: responsive verdict 2nd degree kidnapping [redacted].docx [21kB] ↓, list of criminal pleadings given to [redacted] to handle.docx [18kB] ↓, psalm 110.docx [31kB] ↓, statement for dm.docx [16kB] ↓, work excuse for juror.doc [25kB] ↓, order for recusal 06-750 mh -family relationship with a party.doc [28kB] ↓, next civil judges meeting 1-7-14.docx [14kB] ↓, order for presentation of judgment [redacted].doc [27kB] ↓, reset new upset order.doc [24kB] ↓, no pink slip.doc [31kB] ↓, responsive verdict ill poss of stolen things [redacted].doc [28kB] ↓, mark 12.docx [43kB] ↓, responsive verdict armed robbery.docx [21kB] ↓, responsive verdict agg rape.docx [36kB] ↓, responsive verdict agg arson.doc [34kB] ↓, leave slip word document.docx [20kB] ↓. At the bottom left of the page, there is a small icon and the number "4". At the bottom right, there is a copyright symbol and the date "Sep/10/2020".

Old Conti leak website



CONTI NEWS

If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

[Web mirror](#)[Tor mirror](#)

"WELLIVER"

www.buildwelliver.com/
250 North Genesee Street
Montour Falls, New York 14865
P: (607) 535-5400
F: (607) 535-9145 For Bids F:
(607) 535-9254
(800) 376-3051

Welliver is a fifth generation, family owned company, supported by a team of construction professionals, project managers, and subcontractors who bring world-class expertise, safety, leadership, and accountability to every project.

We are builders who manage and managers who build. Welliver's name became synonymous with the construction industry more than a century ago. Since 1898, Welliver has earned the confidence of clients by providing construction management, pre-construction, general construction, and design/build services that meet the highest standards of quality.

We are a well-established, fifth-

"WEI"

www.wei.com/
Contact WEI
Phone
+1.603.893.0900 (Local)

+1.603.893.4442 (Fax)

Visit WEI
43 Northwestern Drive
Salem, NH 03079

You First, Every Step of the Way Partnering with industry leaders as well as smaller emerging technology companies has been a hallmark of the WEI way. Over the last 25 years, business priorities have changed as often as technology has, but WEI's commitment to customer service has remained consistently strong. Focusing on the unique challenges of individual organizations has guided WEI to a leadership position in the IT community. Hundreds of collaborations with the finest small, medium, and large companies in America have created a breadth of

"SAC WIRELESS INC"

www.sacw.com
Corporate Location
540 W Madison Street, 9th Floor
Chicago, IL 60661
info@sacw.com (312) 895-497
Melanie.Rivera@sacw.com (773) 991-9513
Cari.Shyiak@sacw.com (224) 775-4691
Wesley.Fain@sacw.com (630) 329-0158

SAC Wireless helps customers keep the world connected with our ideas, innovations and solutions. SAC offers a complete portfolio of self-performing services to support major network builds, 5G LTE upgrades and indoor/outdoor small cell and distributed antenna systems (DAS) deployments. The company's core business consists of fully integrated network solutions, specializing in site development, architectural and engineering design management, construction services and management, equipment installation, commissioning and integration, operations and maintenance.

New Conti leak website

([continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad\[.\]onion](http://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad[.]onion))

The double extortion technique used by Conti has apparently paid off: the group claims more than 150 successful attacks and \$20M of paid revenue by the end of 2020⁷. Based on our observations, Conti is the most prolific group since January 2021, with more than 300 publicly disclosed ransomware attacks this year.

This success is partly due to the efficiency of the group's tools. Indeed, in 2020, the Conti ransomware was one of the fastest to encrypt a computer by running 32 concurrent threads, using AES-256 keys bundled with a RSA-4096 public key. The encryption and data exfiltration speed has since been a marketing argument in the ransomware community and was greatly improved by other groups. One of the Conti ransomware specificities is that it can be used in command line to encrypt the local hard drive or network shares.

Encryption speed comparative table for some ransomware - 02.08.2021 (added BlackMatter)

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30 KB	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59 KB	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061 KB	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292 KB	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200 KB	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124 KB	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661 KB	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930 KB	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909 KB	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17 KB	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31 KB	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121 KB	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460 KB	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402 KB	79486

Comparative table created by LockBit 2.0 group (available on their website)

Another specificity that indicates a continuity between the activities of Ryuk and Conti is Ryuk's habit of demanding ransom payments proportional to the revenues of the targeted company that has continued with the Conti ransomware. Once their affiliates compromise a target, they send the operators a report containing information about the victim (name, website address, number of servers and endpoint locked, amount of stolen data, and target's revenue) to help during the ransom negotiation.

Conti's negotiators are experienced and patient. They use the anchor technique by setting a very high first price and negotiating it. They use a service-oriented rhetoric, calling the victim "customer" and themselves "support".

Unlike other ransomware gangs, Conti did not hold back from attacking the hospitals during the COVID-19 crisis⁸.

An internal discord at the origin of the Conti's training material leaks

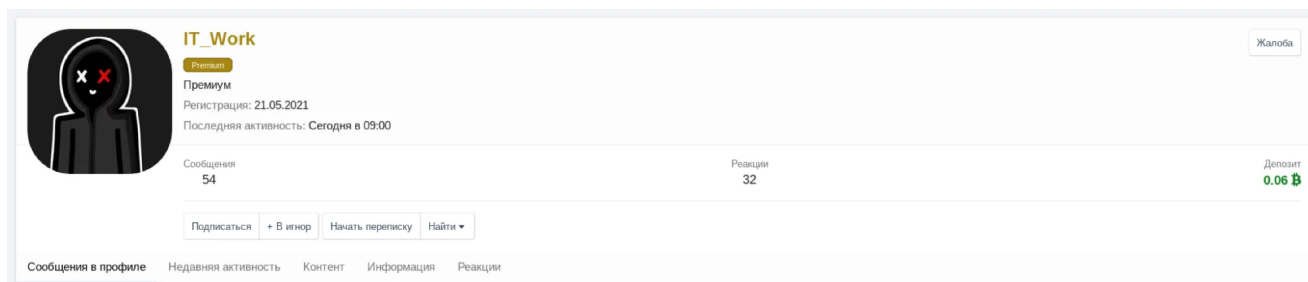
On August 5, 2021, a XSS cybercrime forum member known as "m1Geelka" leaked a Conti ransomware group's training material. The "manual" includes some insights on the modus operandi of one of the most successful ransomware cartels at the moment.

From our observations of the discussions between different actors, "m1Geelka" is *believed to be one of the Windows Administrators of the group. After allegedly working for Conti (or as he states, "I got in there to find out how they work")*, "m1Geelka" judged the remuneration formula to be unfair and decided to do justice to the group's "partners".

In fact, the cybercriminal community has repeatedly voiced that Conti's alleged remuneration was inadequate, given the qualifications they are looking for. Starting from \$1,500 and from \$2,000 for technical profiles, wages are, however, constantly being adjusted upwards, and accompanied by regular bonuses, all paid in BTC – the group states.

Even so, "m1Geelka" was promptly expelled from the Russian-speaking underground community. He has broken one unwritten rule that dictates the law in this medium: conflicts have to be solved through private arbitration processes.

This has also driven us to pay close attention to the most recent activity of a Conti representative on a forum where he was particularly active from June to August 2021. "IT_Work" is the online persona of a suspected threat actor who handled the group's expansion this summer.



The Conti's representative profile on XSS forum, banned since August 6, 2021

As commercial activities related to ransomware are now prohibited on this platform, no advertisements for the used software, nor any specifications about the targeted countries or industries were seen. Instead, we observed a massive recruitment campaign on the XSS


cybercriminal forum which is highly popular among ransomware operators seeking to create new partnerships.

“We are a small recruitment team” – “IT_Works” states. He announced “lots of vacancies” in June 2021, so candidates were encouraged to apply for job openings or to make spontaneous applications. “No formalization under the Labor Code” is stipulated, as to comfort some and prevent others.

There were over a dozen job openings on behalf of Conti spotted in less than two months, revealing a highly specialized and organized group structure. As commonly observed among ransomware groups originating from Russia or countries within the Commonwealth of Independent States (CIS), the communication is performed in Russian and the job listings are addressed to “Russian speakers only!”.

Вакансия "Бизнес-аналитик"

IT_Work · 11.06.2021



IT_Work
Премиум
Premium

Регистрация: 21.05.2021
Сообщения: 54
Реакции: 32
Депозит: 0.06 ₪

23.06.2021

Открыта позиция на вакансию "Бизнес-аналитик"

Необходимые навыки:

- Английский язык, владение деловым стилем (чтение); разговорный - большой плюс
- Знание специфики ведения бизнеса в США
- Аналитический склад ума, умение подмечать взаимосвязи, внимание к деталям
- Продвинутый пользователь ПК

Обязанности:

- Анализ B2B-рынков
- Анализ открытых данных гос.органов, финансовой отчетности компаний
- Ведение досье на ключевых игроков финансовых и промышленных рынков

Условия работы:

- Полная удаленка
- 40 часов в неделю, гибкий график
- Оплачиваемые отпуска, больничные
- Без оформления по ТК
- Стабильный оклад от 1500\$ в месяц + премии и бонусы

Пожалуйста, подавайте заявку на английском языке.
Расскажите о себе, о соответствующем опыте работы.

Жалоба

honda123

An example of a job listing posted by a Conti representative on June 11 on a Russian-speaking cybercriminal forum. Translated from Russian, the post reads:

“Vacancy for the position of Business Analysts. Required Skills: Business English (reading) required, conversational is a big plus; Knowledge of business particularities in the U.S.; Analytical skills, attention to detail; Advanced PC user. **Responsibilities:** Analysis of B2B markets; Analysis of companies’ financial statements, and other public data obtained from government institutions; Drawing up cases on key players on the financial and industrial markets [...]”

A close look at these messages allows us to draw up a rough picture of the Conti’s internal structure, which can be imaged as follows:



An overview of how the Conti Group is structured, based on statements recently made by its representatives on different cybercriminal forums

This is slightly out of the ordinary job offers that other ransomware groups publish (most often for pentester positions). Of particular curiosity is the position of Asterisk Administrator. Based on a July 2021 announcement by Conti, a dedicated Asterisk VoIP service was in development, probably to initiate phone conversations with the victims or the victim’s partners or employees, in order to put more pressure on them. Threat actors are particularly interested in the “Auto Redial” feature of the Asterisk framework to put the phone number on automatic dial repeatedly, until the called party picks up the phone.

The group is also looking for Web Designers with “*really creative ideas*” and UI/UX Designers “*to design layouts of websites and individual user interfaces of web applications*”.

To study potential victim’s activity or to analyze the already attacked ones, Business Analysts are wanted. They must be proficient in English and know the business particularities in the U.S., have good analytical skills and “*pay attention to detail*”. Business Analysts working for

Conti prospect the B2B market, collect and analyze companies' financial statements and other public data obtained from government institutions, and they are also drawing up cases on key players on the financial and industrial markets, according to "IT_Works".

What is also quite unique is the well-structured corporate approach Conti adopted: their "partners" have paid vacations and sick leaves. They usually have a 3pm-1am, Monday to Friday work schedule, remote only.

What do the Conti leaks tell us?

Following the first leak release, we decided to analyze its content and tried to assess how useful it could be in terms of threat intelligence and detection.

The archive, retrieved by vx-underground⁹, contains a majority of text files written in russian, a few archives, binaries, scripts, and softwares (e.g. Cobalt Strike 4.3, Router Scan), and what looks like an unstructured manual explaining to Conti affiliates how to operate.

```
3 # AV' 'Анонимность для параноиков.txt' 'Получение доступа к серверу с бекапами Shadow Protect SPX (StorageCraft).txt'
'3 # AV.7z' 'DAMP LSASS.txt' 'по отключению дефендера.txt'
ad_users.txt 'Если необходимо отсканировать всю сетку одним листом.txt' 'ПРСТАВЛЕНИЕ.txt'
'CS4_3_Clean ahsh4veaQu .7z' 'Закреп AnyDesk.txt' 'Рабочая станция на работу через Tor seb1b.txt'
'DAMP NTDS.txt' 'Заменяем sorted адфиндера.txt' 'Рабочий скрипт создания VPS сервера для тестирования на проникновение от А до Z.txt'
domains.txt 'КАК ДЕЛАТЬ ПИНГ (СЕТИ).txt' 'рклон
enhancement-chain.7z 'КАК ДЕЛАТЬ СОРТЕД СОБРАННОГО АД!!!!.txt' 'рклон.zip
Kerber-ATTACK.rar 'КАК И КАКУЮ ИНФУ КАЧАТЬ.txt' 'Сайт создание батникод.txt'
NetScan.txt 'КАК ПРЫГАТЬ ПО СЕССИЯМ С ПОМОЩЬЮ ПЕЙЛОАД.txt' 'Скринг для sorted .rar'
p.bat 'Личная безопасность.txt' 'СМЕ АВТОВРУТ.txt'
FENTEST SQL.txt 'ВНУАЛ.txt' 'СНЯТИЕ АД.rar'
FrxzfilePE.zip 'Мануал работа с AD DC.txt' 'Список IT форумов, много интересного.txt'
RDP_NGR0K.txt' 'Меняем RDP порт.txt' 'Установка метасплойн на плс.txt'
RMM_Client.exe 'ОТКЛЮЧЕНИЕ ДЕРЕНДЕРА ВРУЧНУЮ.txt' 'хантинг админов, прошу ознакомиться, очень полезно!.txt'
RouterScan.7z 'параметр запуска докера на линукс версиях.txt' 'Эксплуатация CVE-2020-1472 Zerologon в Cobalt Strike.txt'
RouterScan.txt 'ПЕРВОНАЧАЛЬНЫЕ ДЕЙСТВИЯ.txt' 'это установка армитажа. ставится поверх Metasploit'
'SQL DAMP.txt' 'ПОВЫШЕНИЯ ПРИВИЛЕГИЙ.txt'
'Аллиасы для мсф.rar' 'поднятие прав (дефолт).txt'
```

Archive content

A public quick English translation¹⁰ has been made available to organize the leak with three main attack steps: Increasing privileges and information collection, Uploading data and Lock. For each step, each manual provides one or more tools/techniques to reach the objective with a kind of best practices approach and a collection of the best tools to use.

There is no new tool or technique to discover, everything is quite old and renowned (e.g. Mimikatz) and should already be detected. Although they are up-to-date with the latest vulnerability and have a manual for "PrintNightmare" (CVE-2021-34527, that is still not fixed by a proper patch from Microsoft). Obviously they also try to use Microsoft built-in tools as much as possible to blend-in with legitimate activities in order to avoid detection (e.g. powershell, wmi).

Some recommendations are made in terms of operational security in the manual files translated as "Anonymity for the paranoid" and "Personal safety" (not available in the public English translation):

A couple of notes on posts about anonymity for the paranoid:

1. The task is not to hide (it still won't work), but to merge with the crowd. So by disabling webrtc, Javascript, Flash, etc. just attract more attention to yourself. You should NOT DISCONNECT, but CHANGE what allows you to be detected.
2. Concerning Kali and other operating systems for hackers. There is a group of people (Hackers) that needs to be tracked. Technically, this problem is difficult to solve. It's easier to play on human weakness (laziness) and gather everyone together by providing a properly advertised, convenient, ready-made and popular solution. I think the idea is clear. I advise you to use Debian or build something of your own.

I think everyone here works through a virtual machine. Therefore, I advise you to install the virtual machine on the encrypted volume using VeraCrypt.

1 download Veracrypt

2 you will need to allocate space on your disk for a file / or encrypt the entire disk at once

An important rule is that you will have to install the virtual machine again, because, unfortunately, when you encrypt your old working virtual machine, an insurmountable error will appear in the code and it will no longer start. This is not a big problem, because you can get all your files from the image of your old virtual machine via 7ZIP.

Because they are hunting for administrator accounts, they are also cautious about their reaction. In the following extract from the "Hunting admins, please read, very useful!" manual, a very explicit warning is made to dissuade an attacker to directly login to a computer session of an administrator:

Next is an IMPORTANT POINT.

First of all, beginners try to raise a session there and VERY OFTEN catch an alert. Alert at the admin = cutting out of the network, loss of time, nerves. Do not do this!

What we're going to do is poll it through the file system.

But at the same time they could go for a live brute force of accounts when required, and as noticed by other researchers¹¹, use the same example directory (*i.e.* "ProgramData") for all their command outputs which probably leads to a lot of copy/paste.

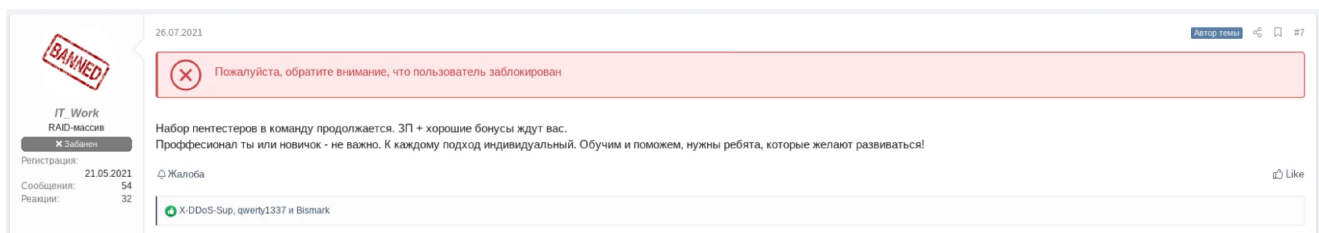
```
ad_users.txt
14:psinject 1884 x64 Invoke-UserHunter -Threads 20 -UserFile C:\ProgramData\list.txt >> C:\ProgramData\out.txt
```

"ProgramData" directory usage example

Their discovery, collection and exfiltration methods match a lot with other ransomware groups and most of the time the techniques described aim for efficiency more than stealthiness.

Overall the archive reveals an interesting insider look into some ransomware attack operations where the attackers look for the weakest points of defense. It also confirms that most of the techniques from these groups are known and give lots of detection opportunities. This should again remind us as defenders where to focus on.

The second leak¹² was not as useful: these are 27GBs of mainly tutorial video files from several sources (free or paying ones), teaching about penetration testing (e.g. Metasploit, Cobalt Strike, network) and reverse engineering. Some sources are in English while others are in Russian but none seem specific to Conti. Indeed, the content of this leak confirms that Conti recruiters are also looking for beginners who will then be trained by following these tutorials, as indicated on a cybercriminal forum:



Translated from Russian, the post reads: “Recruitment of pentesters continues. [...] Whether you’re a professional or a beginner, it doesn’t matter. We have an individual approach to everyone. We will teach and help, we need guys who want to progress in a long-term cooperation!”

Conclusion

Conti leaks are a great source of knowledge to find out more about how ransomware cartels operate overall. It gives good insights into how they handle their operations, how they are organized and the techniques being used in these operations. This will likely raise the interest of other threat actors who might enter the ransomware scene by embracing a modus operandi that, up until now at least, has worked very well.

In the second part of this blog series we will cover some techniques used by Conti in the first leak and the detection opportunities for each one. Read: [An insider insights into Conti operations – Part two](#) !