Trend Micro
Research

TREND MICRO

Inside the Halls of a Cybercrime Business

David Sancho and Mayra Rosario Fuentes

Contents

Published by
Trend Micro Research

Written by
David Sancho,
Mayra Rosario Fuentes

Size Matters: Are Criminal Corporations a Thing? Why Is This Important?

Criminal organizations, like any other human group, tend to become more complex as they grow larger. This complexity manifests as a group forms department-like groups with managers in charge, who report to others further up the hierarchy. We already know this from companies and their departmental subdivisions:

1. Cybercriminal groups often organize themselves like companies. More complex structures evolve as a group increases its revenue and membership.
2. Large criminal groups are very complex in the way they are organized, but there aren't many of them. Most of the landscape is made up of very small teams of criminals earning moderate revenues. These small groups are composed of a few members operating under a partnership model.
3. Larger criminal groups have corporate-like departments such as human resources (HR) and information technology (IT), among others. They might even have employee programs, like recognition of an exemplary employee of the month and performance reviews.
4. Large criminal organizations are distinct not only for their size; they also tend to be harder to manage, and they grapple with more political issues and have more poor performers to deal with. They contend with more trust issues, aside from managing overhead expenses that come with the size of their operations. Growing larger without addressing these issues negatively affects a criminal organization in the long run.

Introduction

Around the turn of the century, the security industry began to realize that most cyberattackers were organized in groups that clearly had criminal objectives: to earn money. This was a big leap from the earlier generation of disorganized malware writers who were much more focused on offensive research with destructive payloads. Also, by forming larger groups, these malicious actors can target organizations that would otherwise be impossible for an individual attacker to accomplish. This new wave of cybercriminals was in it exclusively for the money. Therefore, these new organizations evolved and became more complex.

More than 20 years later, the way these criminal groups are set up resembles modern corporations in many ways. This is not surprising given that any human social group always tends to become more complex as more layers of hierarchy are created as the group expands.

So how do modern cybercriminal groups compare to businesses in the way they are organized? This is precisely what we are going to explore in this paper. We will look at three differently sized criminal groups with cases taken from law enforcement arrests and insider information. Afterward, we will compare each of them to similarly sized, stereotypical, and legitimate companies and see what conclusions we can draw.

In this paper, we show estimates for the quarterly financial reports for typical criminal groups under small, medium, and large enterprise categories. These were not taken from real criminal organizations, as precise figures are naturally not disclosed, but are instead based on our observations and estimations. It's worth pointing out that by merely looking at these financial reports, one cannot prove any correlation between a group's output and its level of sophistication.

We have chosen three sample criminal groups, one for each size, from police arrests, closed cases, and from reliable inside sources. This has allowed us to compile revenue data and other information with extremely high visibility. We based our findings on older reliable data rather than newer estimations.

In addition, we focus on financially motivated cybercrime organizations, as opposed to those tied to nation states, which would more closely resemble the organizational structure of a government, a military department, or hacktivist groups that have very disorganized, unfocused, or chaotic organizational setups.

Defining the Size of a Criminal Business

The definition of an underground criminal business does not conform to the academic definition or to Gartner's definition of company size classifications like legitimate businesses do. Gartner defines a small business as an organization with fewer than 100 employees and generates an annual revenue of less than US$50 million. Medium-size businesses are defined as organizations with 100 to 999 employees, with more than US$50 million but less than US$1 billion in revenue.[1]

The definition of a legitimate company, however, cannot be applied to criminal organizations. If we did apply it, then all criminal groups would invariably be deemed as small.

Instead, for the purposes of this paper, we have set the definitions ourselves for ascertaining the size of a criminal group based on the number of employees and their hierarchical structure as observed from our studies of many criminal groups over time. We have not factored in the market impact, as some small groups might have a more significant impact in terms of the scope of infections or criminal customers, so they might not have large revenues. Nevertheless, it is worth noting that these are not rigid numbers in the same way that legitimate businesses do not always fit neatly into predefined categories.

With some degree of grayness, Figure 1 can be used as a guide for analysts to classify a criminal organization's size, while also considering other information available to them. As a good rule of thumb, a criminal organization's classification under a specific category means that it has passed all the three criteria set per category:

	Number of staff and affiliates	Annual revenue	Management layers
Small	1 – 5	Under US$500,000	1
Medium	6 – 49	Up to US$50 million	2
Large	50+	US$50 million+	3

Table 1: Guidelines for ascertaining criminal business size

Small criminal businesses in the underground are usually flat organizations: Either there are a few or even no management layers between the owner and the employees. Small criminal organizations are the most common business size in the cybercriminal underground. However, if they do become successful, they will generally evolve to become midsize or even large organizations. Because of the lack of regulation in the underground market, our analysis can only be anecdotal; however, we assume that like legitimate businesses, only a nominal percentage of small criminal groups progress to become a medium or large enterprise.

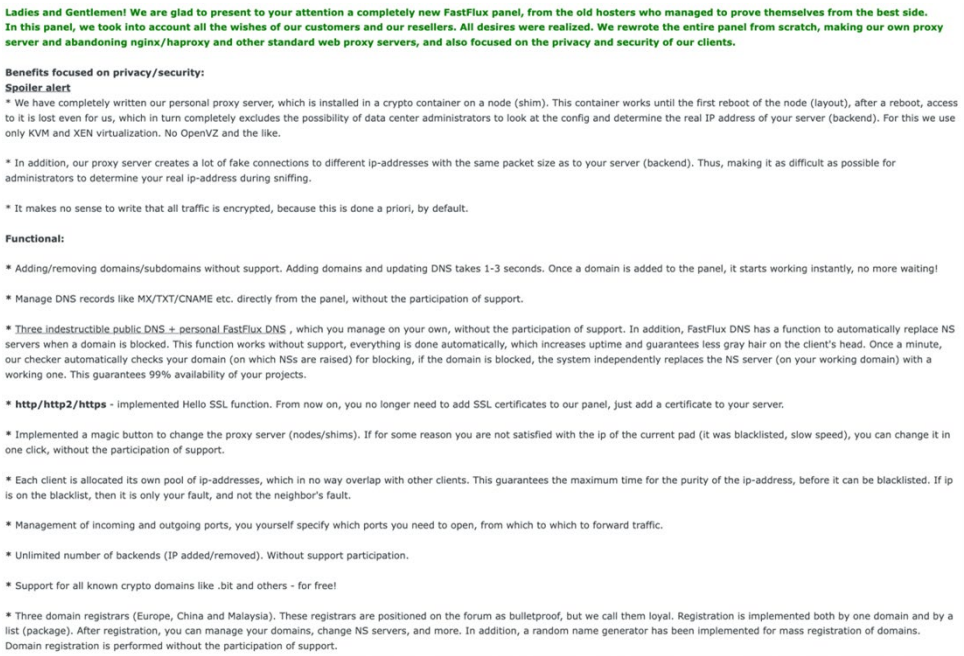
Like real-world businesses, small criminal gangs are founded by one or more entrepreneurs to create and market a unique product or service, but often these new business owners have not yet established their reputation among their peers. These types of small businesses are usually financed by their founders themselves to pay for developers of the malware code, servers, and other attendant fees.

Among legitimate businesses in the US, small-and medium-sized business enterprises make the vast majority at a staggering 99.9%, employ 47.1% of the private workforce, and drive about 44% of the economic activity.[2] In this paper, we have assumed that the landscape we see in the cybercrime market follows a similar distribution. Nevertheless, this has no bearing on our overall conclusion.

Small criminal groups usually consist of a team leader, a coder, a support role, and a network administrator. With such a lean workforce, each often fulfills multiple roles on top of the usual responsibilities such as advertising, recruiting, and money handling.

An example of a successful small business is Yalishanda. This is one of the most popular bulletproof hosting service providers in the underground community according to an analysis by Brian Krebs,[3] and is believed to be run by just two individuals.

Figure 1. Advertisement to recruit affiliates to form a botnet team



Ladies and Gentlemen! We are glad to present to your attention a completely new FastFlux panel, from the old hosters who managed to prove themselves from the best side. In this panel, we took into account all the wishes of our customers and our resellers. All desires were realized. We rewrote the entire panel from scratch, making our own proxy server and abandoning nginx/haproxy and other standard web proxy servers, and also focused on the privacy and security of our clients.

Benefits focused on privacy/security:
Spoiler alert
* We have completely written our personal proxy server, which is installed in a crypto container on a node (shim). This container works until the first reboot of the node (layout), after a reboot, access to it is lost even for us, which in turn completely excludes the possibility of data center administrators to look at the config and determine the real IP address of your server (backend). For this we use only KVM and XEN virtualization. No OpenVZ and the like.

* In addition, our proxy server creates a lot of fake connections to different ip-addresses with the same packet size as to your server (backend). Thus, making it as difficult as possible for administrators to determine your real ip-address during sniffing.

* It makes no sense to write that all traffic is encrypted, because this is done a priori, by default.

Functional:

* Adding/removing domains/subdomains without support. Adding domains and updating DNS takes 1-3 seconds. Once a domain is added to the panel, it starts working instantly, no more waiting!

* Manage DNS records like MX/TXT/CNAME etc. directly from the panel, without the participation of support.

* Three indestructible public DNS + personal FastFlux DNS , which you manage on your own, without the participation of support. In addition, FastFlux DNS has a function to automatically replace NS servers when a domain is blocked. This function works without support, everything is done automatically, which increases uptime and guarantees less gray hair on the client's head. Once a minute, our checker automatically checks your domain (on which NSs are raised) for blocking, if the domain is blocked, the system independently replaces the NS server (on your working domain) with a working one. This guarantees 99% availability of your projects.

* **http/http2/https** - implemented Hello SSL function. From now on, you no longer need to add SSL certificates to our panel, just add a certificate to your server.

* Implemented a magic button to change the proxy server (nodes/shims). If for some reason you are not satisfied with the ip of the current pad (it was blacklisted, slow speed), you can change it in one click, without the participation of support.

* Each client is allocated its own pool of ip-addresses, which in no way overlap with other clients. This guarantees the maximum time for the purity of the ip-address, before it can be blacklisted. If ip is on the blacklist, then it is only your fault, and not the neighbor's fault.

* Management of incoming and outgoing ports, you yourself specify which ports you need to open, from which to which to forward traffic.

* Unlimited number of backends (IP added/removed). Without support participation.

* Support for all known crypto domains like .bit and others - for free!

* Three domain registrars (Europe, China and Malaysia). These registrars are positioned on the forum as bulletproof, but we call them loyal. Registration is implemented both by one domain and by a list (package). After registration, you can manage your domains, change NS servers, and more. In addition, a random name generator has been implemented for mass registration of domains. Domain registration is performed without the participation of support.

Figure 2. Advertisement for bulletproof hosting services for Yalishanda

Midsize criminal businesses have a more hierarchical structure, such as those commonly found in legitimate businesses. They usually have a pyramid-style organization chart describing the authority within the organization with one person at the top who is in charge of the overall company.

An example of a midsize criminal business is the GozNym group. In May 2019, 10 people were charged from this group. According to the indictment, the team consisted of a leader, a developer, crypters, an account takeover specialist, a cashier, a technical administrator, a primary assistant, a "cash-out" or "drop master," an administrator of a bulletproof hosting service, and spammers.[4]

Figure 3. Organizational structure of GozNym as investigated by Europol

Source: Europol[5]

Large criminal businesses have highly hierarchical structures followed by increasingly larger numbers of lower management and supervisors. Large criminal organizations are a lot more structured than their medium-size counterparts. Successful large businesses demonstrate effective partnerships with others, exhibit leadership, and implement operational security (OPSEC). Large criminal organizations are more capable of competing with other cybercrime actors than small businesses and might operate one or more physical facilities. They also tend to hire more employees and generate sizable revenue.

We consider large criminal organizations as employing over 50 people. Usually, people in charge have been on the criminal underground for a long time and have a good reputation. These criminal organizations might have "business support" departments such as HR and accounting, but they lack the sort of formal qualifications like having business degrees commonly enforced in legitimate businesses. They hire multiple developers, administrators, and penetration testers. Some underground organizations have also been known to hire contractors instead of full-time employees for short-term projects.

Large criminal organizations sometimes form partnerships with other criminal teams. An example is Evil Corp, the Russian-based cybercriminal organization responsible for the development and distribution of the Dridex malware. Not only did Evil Corp regularly work with external affiliates, but they also relied on a network of money mules who are involved in transferring stolen funds obtained from victims' bank accounts to accounts controlled by members of Evil Corp.[6] This organization had also worked previously with other ransomware groups like LockBit.[7]

It is worth pointing out that cybercriminal groups manage their operations remotely. By virtue of this anonymity, these groups miss out on a lot of the social bonds and structure that hold legitimate teams and companies together, and this can ultimately lead to their fragmentation. There are limited water-cooler chats, no Christmas parties, no birthday cakes in the canteen, no seeing colleagues' family pictures on their desk. This lack of physical social interaction is one of their weak points.

Small Criminal Business

Overview

We have chosen Scan4You as our small business group example that did well in the underground. Scan4You was in operation from 2012 to 2017 and was once one of the largest Counter Antivirus (Counter AV or CAV) services in the criminal underground. Cybercriminals use Counter AV as a tool to evade antimalware detection, implemented by appointing crypters or programs that can disguise malicious programs from security software.[8] While things have changed since 2017 for small criminal groups, the overall setup has remained very similar.

The Scan4You business structure consisted of two employees and at least five resellers. There was no defined leader. Scan4You offered 100,000 scans per month for US$30 and US$0.15 for a single scan. Payment methods used at the time included Paypal, WebMoney, and bitcoin. There is also circumstantial evidence that Scan4You's operators might have been involved with banking malware. In the Trend Micro report titled "The Rise and Fall of Scan4You,"[9] we estimated that in 2013, Scan4You earned around US$15,000 per month.

Scan4You was run by Ruslans Bondars (aka BOrland) and Jurijs Martisevs (aka Garrik). Bondars was the administrator and maintained the technical infrastructure and the company's website. Martisevs served as an administrator and provided customer support typically via email, ICQ, Jabber, and Skype.

Scan4You had at least 30,000 registered user accounts.[10] Bondars had a day job as a software developer in a large company. Running a CAV service is a lot of work, especially when you have a day job, too. Additionally, to help them sell the CAV service, they set up a reselling partnership program by means of an application programming interface (API). Some of the resellers such as file2scan, refund.me, and indetectables provided scanning services to local non-English markets, like Spanish or German markets.

CAV Service
CAV Service
NoDistribute
nodetect.com
Indetectables
roboservice
RazorScanner
file2scan
Refud.me

Figure 4. Scan4You reseller partial list

Scan4You has all the hallmarks of a small criminal group as shown on Table 2.

1 layer of hierarchical structure	✓
2 employees, 5 Affiliates	✓
Estimated annual revenues of US$180,000	✓

Table 2. Key attributes of a small cybercrime business that Scan4You had

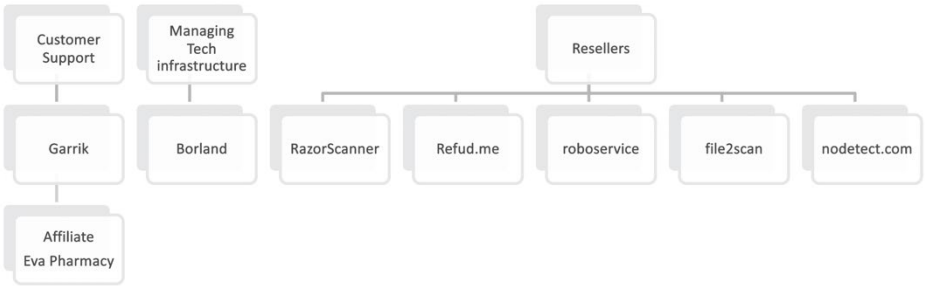


Figure 5. Scan4You's business organization chart

Estimated Quarterly Income of a Small Business Like Scan4You

In this section, we provide a mockup of an income statement that would approximate what one would have looked like in the first quarter of 2013. This does not represent the real income statement of Scan4You but only a prototype that a fictitious small-size criminal group would have had. As mentioned, this report does not aim to be one-hundred percent accurate, as that is not possible given the limitations of public data. Instead, we intend to give an idea of what a criminal business of this size would be like.

At that time, Scan4You was making around US$15,000 a month. The price for 100,000 scans was US$30 per month, while a single scan cost $0.15. As you can see, this is a very simple business. On one side is a simple revenue stream, while on the other side are wages and hosting costs with the difference representing the group's net profit.

Quarterly Income Statement Q1 January- March 2013	**2013** current year
Revenue	
Gross sales [1]	$44,955
Net Sales	**$44,955**
Operating Expenses	
Estimated Wages [2]	$12,000
Aproximate Servers/VPN Cost [3]	$2,000
Estimated cost of VM (40 machines) [4]	$1,440
Other Expenses	-
Total Operating Expenses	$15,440.00
Net Profit	**$29,514.92**

Figure 6. Estimated income of a fictitious small-size underground criminal group

Hypothesis

We used the following information as the basis for estimating the income of small criminal groups as shown on Figure 6:

1. US$1,500 to US$2,000 as the average IT salary in Russia
2. Using leaked Conti chat conversations as a source, where gang members mentioned estimates ranging from US$3,000 to US$4,000 every month
3. Using Azure's pricing for virtual machines as source,[11] estimating US$12 a month per 40 machines to represent a modern equivalent to virtual machines (VMs) or server costs at the time

A Day in the Life of an Employee

A day in the life of Bondars would likely start by reporting to his day job as a software developer at an internet company that provides products and services in the travel, finance, entertainment, and technology sectors in 50 countries. Bondars kept a LinkedIn professional profile (see Figure 7). Bondars apparently traveled on occasion for work. There is evidence of him attending a party in New York with coworkers (see Figure 8).

According to Glassdoor, as of 2022, a software developer like Bondars based in Latvia would make around €2,743 per month (US$2,938.45 as of this writing). Bondars's 2015 job as a software developer would have consisted of programming in Python and Go. Docker and Kubernetes would be needed for his job as well.[12] After working all day in an office, Bondars would likely have gone back home to work on the Scan4You servers and host the site for the service itself. The rest of the evening would have consisted of Bondars responding to help desk tickets and advertising on underground forums.

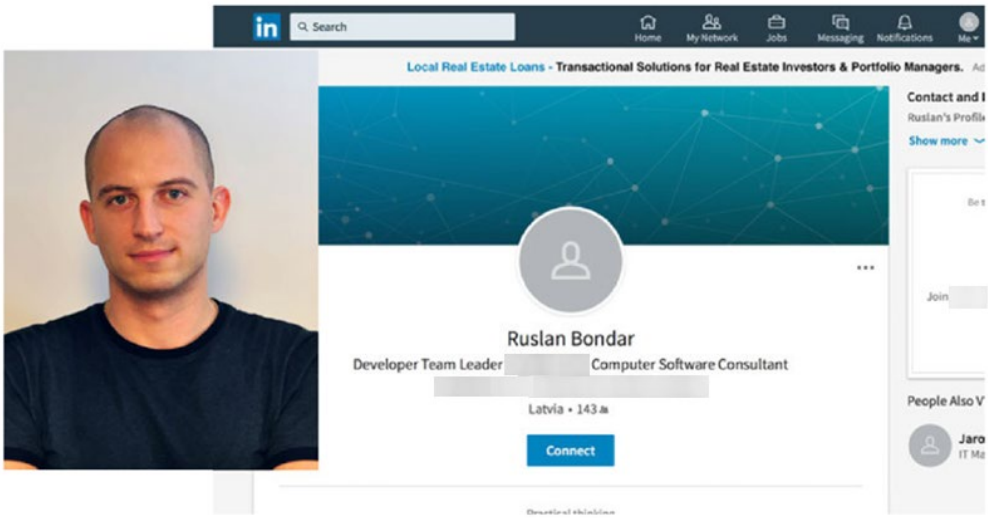


Figure 7. Ruslan Bondars' LinkedIn profile

Figure 8. Bondars at a party in New York

Figure 9. Estimated monthly salary for a software developer in Latvia in 2022 for a software company based on previous employees' inputs on Glassdoor.com

Key Takeaways:

- Small criminal groups have few members and no hierarchy (no reporting lines; normally they are just partners).
- Often, their members have a day job on top of their role in the group.
- Annual revenue is moderate.

Midsize Criminal Group

Overview

A midsize company is larger than a small business but not big enough to be considered a large business. We consider medium businesses to have between six and 49 employees and to make up to US$50 million yearly.

We have selected MaxiDed as an example of a midsize criminal group. MaxiDed started off as a small hosting provider with no mention of allowing illicit activities (although "Ded" is common underground slang for "Dedicated Servers" used in cybercrime). In 2011, they changed to a bulletproof hosting provider and were harboring child abuse material, command-and-control (C&C) servers for distributed denial-of-service (DDoS) botnets, cyberespionage, malvertising, and spam.

This group began in 2008 and its operations ended when the Dutch police seized its servers in 2018.[13] Thai police arrested a 29-year-old Moldavian man who allegedly owned MaxiDed at a holiday resort in Thailand in 2018. The Bulgarian police also arrested another suspect, a 37-year-old Moldavian national who was purportedly a server administrator of MaxiDed.[14]

MaxiDed was led by at least five administrators. Its business plan started out by offering merchants' server packages that allowed abuse. MaxiDed took a fixed 20% fee from each sale between a merchant and a customer. Customers neither saw the merchants' identities nor knew that an offer came from a separate entity. All they knew was that they had a contract with MaxiDed. MaxiDed also charged customers for performing additional administrative tasks, like reinstalling servers after a takedown by the upstream provider.

The administrators also operated a file-sharing platform called DepFile that hosted Child Sexual Abuse Imagery (CSAI) content. DepFile profits were much higher than those of MaxiDed. DepFile ran on servers that were part of the MaxiDed infrastructure and took off faster than MaxiDed.

Table 3 shows that MaxiDed had all the essential attributes of a midsize criminal group:

Two layers of hierarchical structure	✔
More than 6 employees, numerous affiliates	✔
US$925,000 estimated annual revenue	✔

Table 3. MaxiDed had all the key attributes of a midsize cybercrime business.

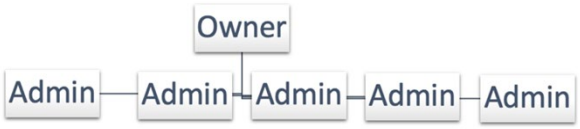


Figure 10. MaxiDed's organizational chart

Estimated Annual Income of a Midsize Business Like MaxiDed in 2013

We recreated what an income statement would have looked like for MaxiDed in 2013 (see Figure 11). This is an approximation only to illustrate common costs and revenues for a midsize criminal operation and not an actual statement from MaxiDed.

The total amount of revenues from 2011 to May 2018 was US$3.4 million.[15] The total profit made in seven years was US$679,741, not including wages, office space, or equipment. Meanwhile, DepFile was a more profitable side business. It made US$13 million in revenues and approximately, a profit of US$4.4 million for five years of operation. MaxiDed was more valuable to its owners as it was a cheap way to acquire bulletproof servers for their side business than its own business model.[16]

2013 Annual Income Statement	2013 current year
Revenue	
Gross sales (MaxiDed) 1	458,028
Net Sales	**$458,028**
Cost and Other deductions	
nonpaying customers 2	$57,143
Cost for Depfile 3	$248,307
Total Debts	$305,450
Gross Profit (Loss)	**$152,578**
Operating Expenses	
Cost for MaxiDed 4	$179,761.00
Wages 5	$60,000.00
Other Expenses	-
Total Operating Expenses	$239,761.00
Operating Profit (Loss)	**-$87,182.86**
	-
Other Income- DepFile gross sales 6	$334,540.00
Net Profit	**$247,357.14**

Figure 11. Estimated annual income for MaxiDed in 2013

Hypothesis

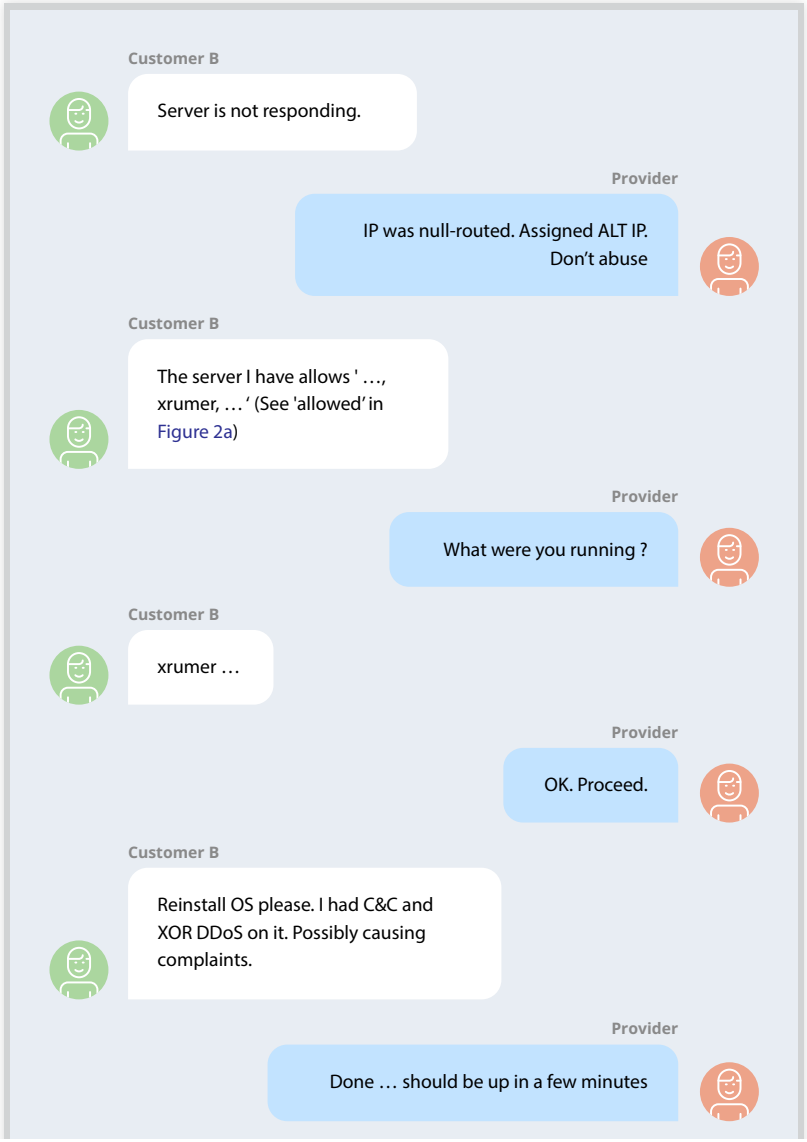
We based our hypothesis for recreating the approximated income statement on the following information:

1. We used the exact amount mentioned in the research of Noroozian, Koenders, and van Veldhuizen.[17]
2. A MaxiDed account accumulated US$400,000 in debt in the seven years that MaxiDed operated.[18]
3. The revenue-sharing scheme between MaxiDed and its merchants was 20%/80% in favor of MaxiDed, while the merchants would receive US$1.6 million.[19]
4. We estimated wages at US$1,000 per employee per month.

A Day in the Life of an Employee

A day in the life of a MaxiDed administrator would have been very busy and at times, stressful. This person would have been working full-time for MaxiDed and would not have had a day job. The administrator's day starts with an eight-hour shift. The first shift of the day would have been the busiest since people from all over the world wake up and get to work before the administrator logs in or even has their first cup of coffee. Clients overseas are already doing business and could be working on overnight issues from clients. Running your own web-hosting provider from home would consist of spending time dealing with customers and handling payments. Most of the shift would consist of going through the support ticket requests queue and new server orders. Customer services were operated through a live-chat service on MaxiDed's website using ICQ, Jabber, and Skype for communications.

The administrator would also need to spend time advertising on cybercriminal forums and responding to any questions about the company's services. At first, the administrator would have dedicated the majority of their shift running MaxiDed services, but once DepFile took over, the administrator would have needed to spend more time making sure DepFile servers were running while handling both MaxiDed and DepFile customer support tickets. Based on online reviews, administrators had many customer service complaints to handle.[20]



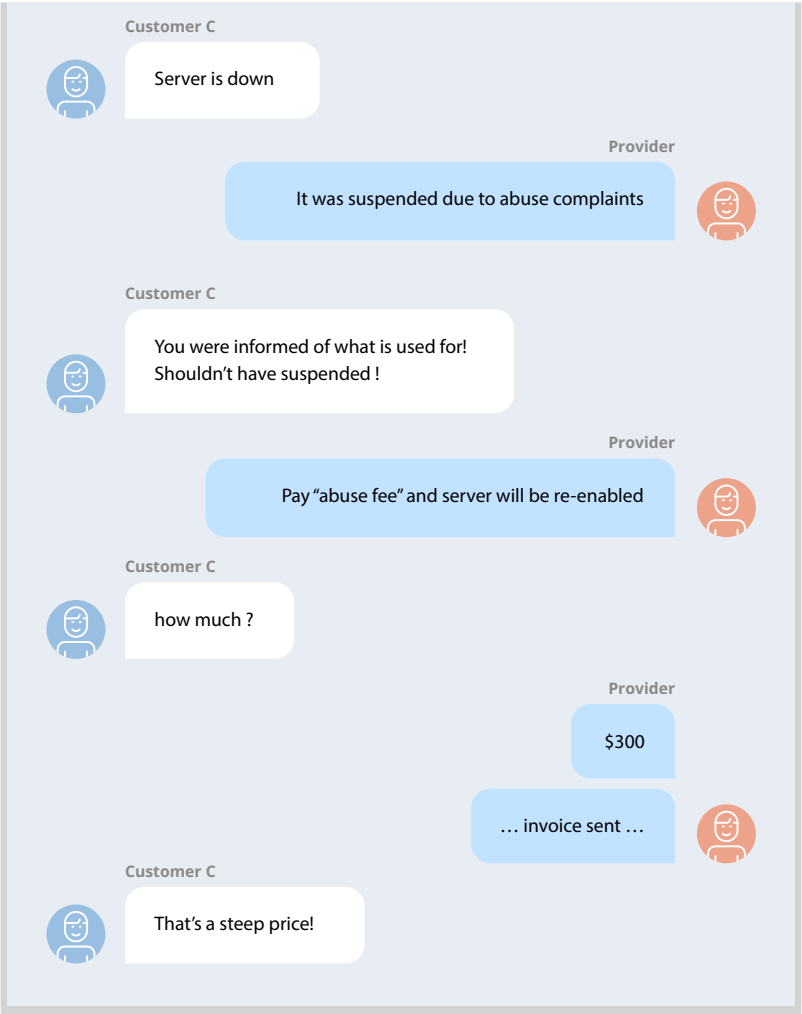


Figure 12. Sample conversation between a MaxiDed customer and an administrator

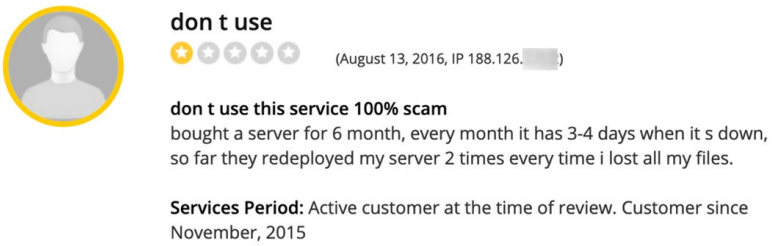


Figure 13. A snippet of a customer review of MaxiDed's services

Key Takeaways:

- Medium-size criminal groups have basic functional groups and reporting lines.
- The annual revenue justifies members working full-time for the group.

Large Criminal Organization

Overview

Larger criminal organizations are unique not only for their size. Beset with a more complex social structure, they tend to be harder to manage as they contend with more politics, more poor performers, trust issues, and the management of overhead costs that come with the consequent complexities. Growing larger without addressing those issues leaves a negative impact on a criminal organization.

We have chosen the Conti criminal group based in regions in the former USSR to illustrate a large cybercrime enterprise. After the huge data leak of the group's internal chat logs in late February 2022,[21] the security community was able to learn a lot about the inner workings of Conti. This includes the number of employees, some of its organizational structure, and other very interesting data. This makes Conti the perfect example to showcase the inner workings of a large cybercrime organization.

Conti is a criminal group that used to develop and deploy ransomware. This group's attacks were first seen during the first half of 2020. Over the span of only a few months, the criminals behind Conti established themselves as one of the most aggressive ransomware actors in existence. In August 2020, the US Department of State offered a US$10-million reward for information on the group's leaders.[22]

After the Ukraine-Russia conflict that started in February 2022, Conti publicly declared support for Russia,[23] although it quickly backpedaled and watered down their affiliation. This prompted a pro-Ukrainian researcher who had gained access to Conti's internal messaging server to publicly release all its internal communications.[24]

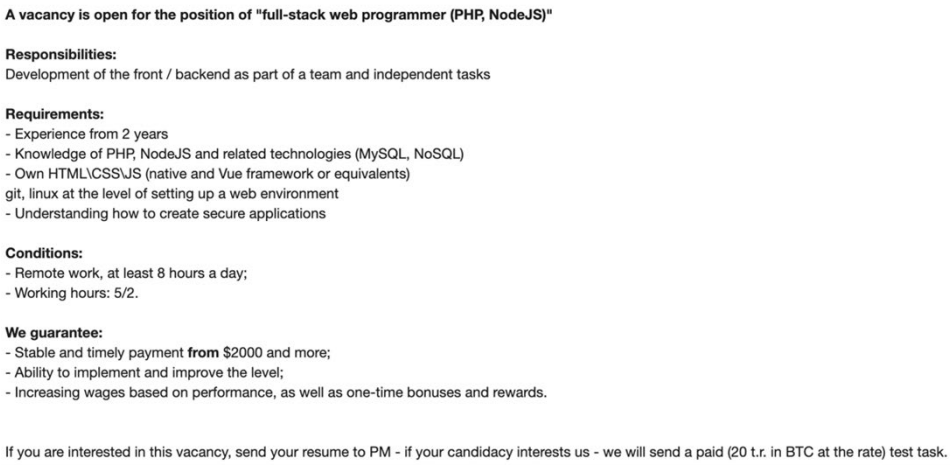
The leaked internal messages showed a multitude of interesting angles of the Conti business as well as the personal dimension of the people involved. We will outline only the most relevant parts to assess the size and scope of the operators behind this ransomware group:

- Payroll was mentioned to be around US$165,000 per month. This included only regular workers, not external collaborators. The number of people being paid in the bitcoin fund was around 60. The total number of employees was around 350 people.[25]
- Conti had an HR department consisting of the HR manager and six HR specialists. The group used regular recruitment websites to hire new employees. It set up performance bonuses for "salespeople" involved in successful ransom collections. It also offered retention bonuses for employees who threatened to leave after finding out the nature of the business. Curiously, the group also had an "employee-of-the-month" program as an additional performance incentive.
- Employees were offered weekends off. They also followed federal holidays observed in the US.
- Developers made around US$2,000 per month. This is roughly the same as the Russian average for this job type, if not slightly higher.
- Conti had two physical offices, which cost them US$26,000 per month in rent.
- Conti has previously acquired the source code of other criminal projects like TrickBot and Emotet. As such, the Conti management had kept the TrickBot coders as a separate development group under its "product" portfolio.[26]

The aforementioned facts extracted from the leaked conversations paint a picture of the Conti organization as closely resembling a large, legitimate business. These criminals seem to have managed to build a complex organization with many layers of management and internal rules and regulations that mimicked that of a legitimate corporation.

The number of employees on its payroll suggests that this was a fairly large team compared to standard cybercriminal organizations. The fact that it needed an HR department to manage employee affairs is very telling. The employee motivation programs the group put in place were also similar to what one would expect in a big company.

The revenue of Conti has been estimated to be at least US$150 million by the FBI[27] or US$180 million by Chainalysis.[28] These are accumulated values from the group's initial operation in early 2020 until May 2022, roughly a two-year span. This would yield an annual revenue of around US$75 million based on the FBI's estimation, and US$90 million based on Chainalysis' estimation. Note that both estimations are based on cryptocurrency payments that can be seen coming from known victims. The actual amount is probably much higher, considering the rest of the victims who haven't been made public.



A vacancy is open for the position of "full-stack web programmer (PHP, NodeJS)"

Responsibilities:
Development of the front / backend as part of a team and independent tasks

Requirements:
- Experience from 2 years
- Knowledge of PHP, NodeJS and related technologies (MySQL, NoSQL)
- Own HTML\CSS\JS (native and Vue framework or equivalents)
git, linux at the level of setting up a web environment
- Understanding how to create secure applications

Conditions:
- Remote work, at least 8 hours a day;
- Working hours: 5/2.

We guarantee:
- Stable and timely payment **from** $2000 and more;
- Ability to implement and improve the level;
- Increasing wages based on performance, as well as one-time bonuses and rewards.

If you are interested in this vacancy, send your resume to PM - if your candidacy interests us - we will send a paid (20 t.r. in BTC at the rate) test task.

Figure 14. Conti's job posting on XSS forum

Notably, the fact that Conti was acquiring external developers like TrickBot and keeping them under its own umbrella speaks volumes about the kind of thinking that was directing the group. Mergers and acquisitions are distinctive features of large, real-world corporations.

For all these reasons, we think it is very difficult for anybody to make the case that Conti is not a large cybercriminal organization. Conti embodies the hallmarks of a large criminal group.

More than two layers of hierarchical structure	✔
50+ employees	✔
US$75 million+ estimated annual revenue	✔

Table 4. Conti bears all the key attributes of a large cybercrime enterprise.

Estimated 2021 Annual Income for a Large Criminal Organization Like Conti

In Figure 15, we provide a recreated financial statement to show how one would look like for Conti based on the leaked chat conversations found a vx-underground[29] downloads page for 2021. This is not an actual income statement from Conti. The group has never released any such data publicly, so this is merely our own estimation of what the figures for one such group could be like. We have based the group's revenue of US$180 million on the analysis by Chainalysis for the payments it received in 2021.

Revenue	
Gross sales 1	$180,000,000
Less: Affliates Cut 2	$126,000,000
Less:	
Net Sales	**$54,000,000**
Cost of Goods Sold	
Negotiators 3	$1,800,000
Bonuses 4	$12,000
	-
Total Cost of Goods Sold	$1,812,000
Gross Profit (Loss)	**$52,188,000**
Operating Expenses	
Employee wages-Main Team 5	$1,169,364
Employee wages-New Team 6	$36,000
Employee Wages-Reverse Engineering Team 7	$280,164
Employee Wages-Research Team 8	$150,000
Employee wages-OSINT team 9	$108,000
Routers/Servers/Proxies 10	$36,000
Software-Cobalt Strike 11	$30,000
Third Party cut to obtain Cobalt Strike 12	$30,000
Rent/Lease 13	$312,000
Software Crunchbase 14	$5,000
Software ZoomInfo 15	$15,000
Exploit forum Cryptocurrency article contest 16	$10,000
	-
	-
Total Operating Expenses	$2,181,528
Operating Profit (Loss)	**$50,006,472**
Interest Income	-
Other Income-SQUID Cryptocurrency scam 17	$3,800,000
Profit (Loss) Before Taxes	**$53,806,472**
Less: Tax Expense	
Net Profit (Loss)	**$53,806,472**

Figure 15. Estimated annual income statement for Conti in 2021

Hypothesis

We used information from the following sources as basis for the assumptions we made to recreate the annual income statement prototype for Conti:

1. The 2022 Crypto Crime Report by Chainalysis[30]
2. Krebs on Security, Conti Ransomware Group Diaries, Part IV: Cryptocrime[31]
3. Chat logs: Employees of the month earn a bonus equal to half their salary, thus US$2,000 divided by two and multiplied by 12 months
4. Chat logs: US$97,447 per month for 52 employees
5. Chat logs: US$3,000 per month for three employees
6. Chat logs: US$23,347 per month for 16 people

7. Chat logs: US$12,500 per month for six people
8. Chat logs: US$9,000 per month for four people
9. Chat logs: US$3,000 to US$4,000 per month
10. Krebs on Security's Conti Ransomware Group Diaries, Part III: Weaponry[32]
11. Chat logs: US$26,000 a month
12. Crunchbase.com, which offers a service referred to as Pro, priced at US$49 per month. It also offers an enterprise version priced between US$5,000 and US$10,000 a year. We estimated that the malicious actors were using the low-bound US$5,000 enterprise version.[33]
13. Zoominfo.com's license fee, pegged at US$15,000 per year for its enterprise version[34]
14. Krebs on Security for Stern's idea about creating his own cryptocurrency scam for a cross-platform blockchain application.[35] Conti essentially outsourced the research and development for Stern's idea by launching a public contest to generate new ideas.
15. A BBC report[36] and Krebs on Security's Conti Ransomware Group Diaries, Part IV: Cryptocrime[37] for information on the US$3.8-million cryptocurrency scam

A Day in the Life of an Employee

As a regular developer for the group, a Conti employee would probably lead a life very similar to that of a corporate worker in a software company. This person works from home and spends their time typing out code and testing it remotely on a development environment set up by the IT department. On Fridays, they fill out a report detailing what they accomplished that week and they send it to their line manager. They have a rigid, predictable schedule and observe federal US holidays, even though they live in Russia.

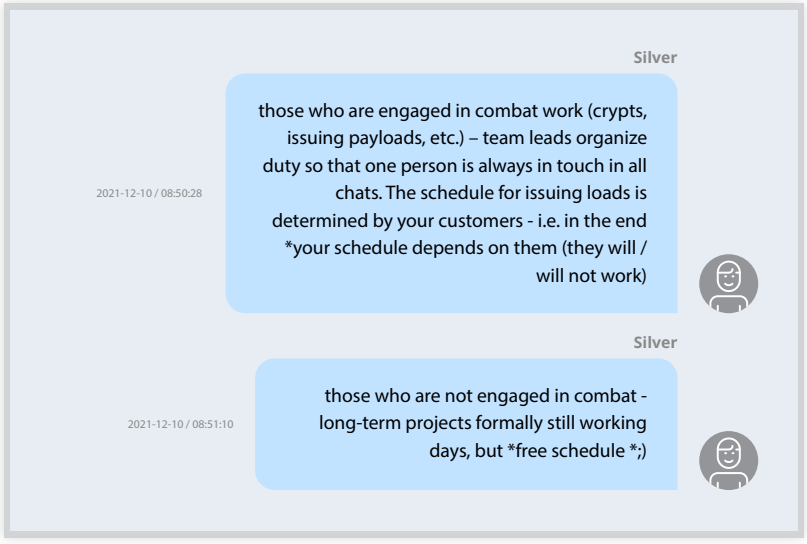


Figure 16. Excerpt from the leaked Conti chats, translated from Russian, showing its management informing employees of any work schedule changes, like US federal holidays or other events

Source: Check Point Research[38]

The developers communicate often with their direct manager, mostly through various chat applications, but sometimes also by video call. In these chats, the employee asks for direction and help on the projects they are currently working on. Every now and then, they also talk about productivity and performance and occasionally about salary increases.

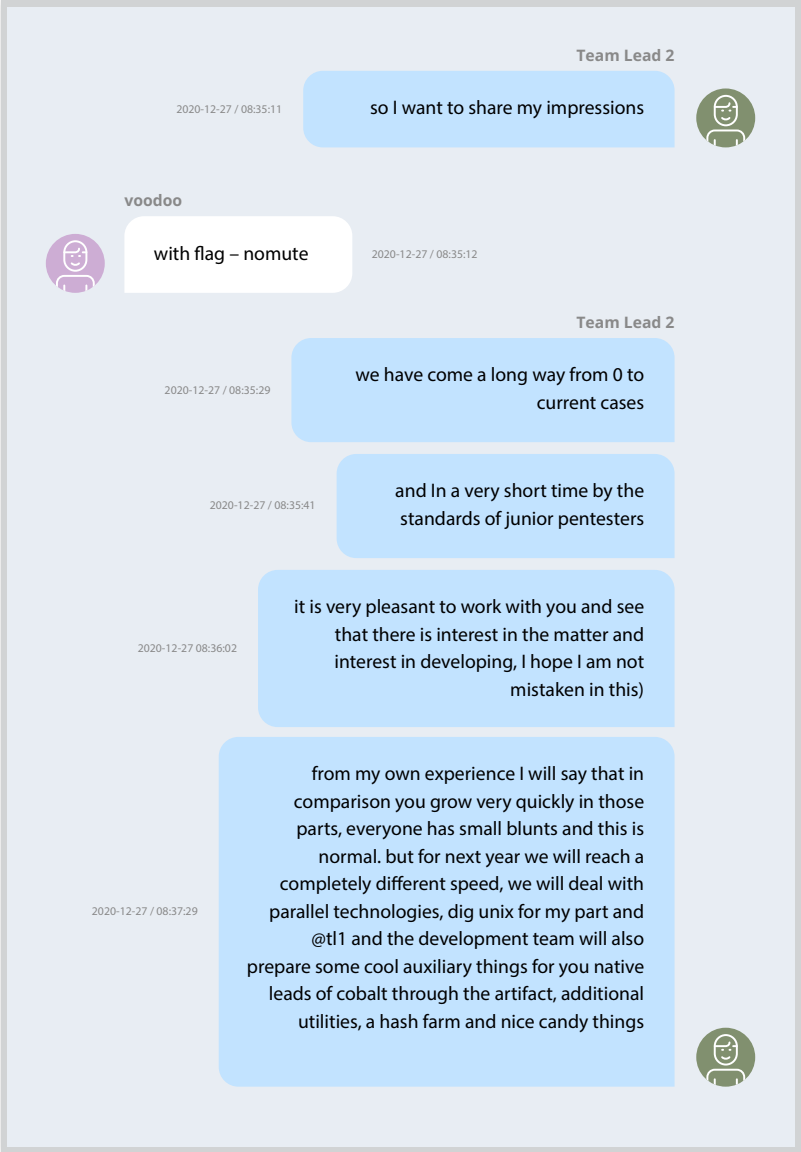


Figure 17. Excerpt of Conti's leaked chats mentioning a performance review between an employee and their direct line managers (translated from Russian)

Source: Check Point Research[39]

Like a normal remote worker, Conti employees occasionally open their hearts to one another by telling their colleagues their hopes and fears in the workplace.

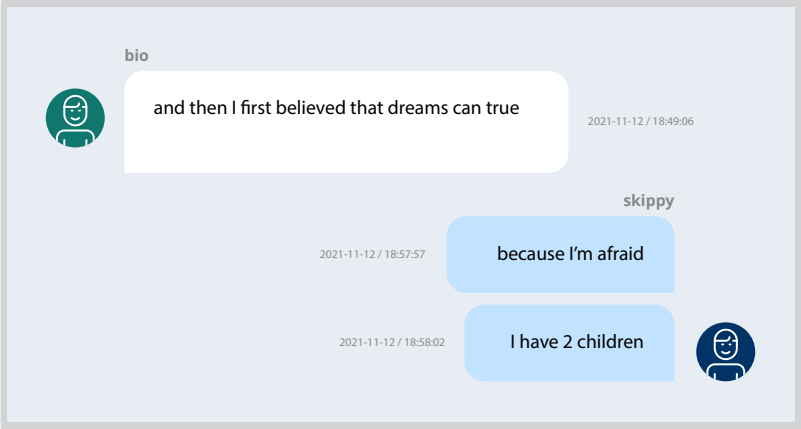


Figure 18. Excerpt of a leaked chat conversation between Conti employees, translated from Russian, commenting on and criticizing their personal situation in the workplace

Source: Check Point Research[40]

As aforementioned, the employer runs an "employee-of-the-month" program that rewards the highest performers with a significant money prize.

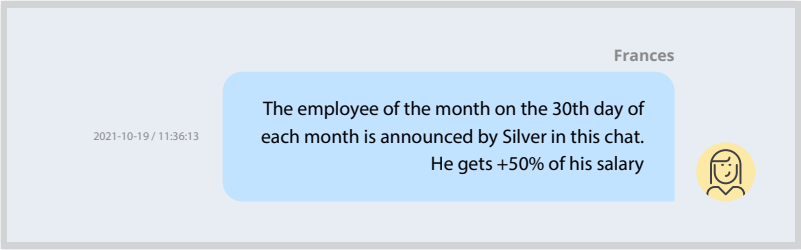


Figure 19. Excerpt, translated from Russian, taken from the leaked chats of Conti showing its announcement of its "employee-of-the-month" program

Source: Check Point Research[41]

In summary, a Conti employee's life is very similar to that of any salaried person that works for a corporation. Most of these employees work remotely, so water-cooler gossip takes place by chat. Direct managers have one-on-one talks with their direct levels regularly, and performance is monitored for each employee.

Key Takeaways:

- Large criminal groups are organized in functional departments, remarkably similar to any legitimate corporation.
- Reporting lines are highly hierarchical with middle management and upper management on top of the pyramid.
- Managers closely monitor employee performance and also encourage employee motivation.
- Annual revenue is high and on par with some legitimate companies.

The Advantages of Knowing the Size of Criminal Organizations for Investigators

In the previous three sections, we described how each of the small, medium, and large criminal groups differs from one another. This might seem like an academic distinction, but it's not. To a criminal investigator, there are practical implications of knowing what size a target criminal organization belongs to.

Investigators who suspect the size of their target criminal organization can have new potential data to look for in case of an infiltration:

- **Financial statements or financial plans.** The bigger the size, the more likely it is that the brains of the organization keep financial statements, possibly in the form of a spreadsheet. If there are complex business relations with partners or suppliers, the need to keep track of all these numbers is high. Financial projections and future plans are also a strong possibility.
- **List of employees.** The more members the group employs, the more likely that it keeps their salaries or commissions written somewhere, also probably in a spreadsheet. Being able to access the employee list (with or without salaries) can be crippling for the target organization.
- **Department-specific documentation.** Having access to tutorials or company manuals might enable an investigator to have a detailed overview of how things are done in each department. For malware development groups, penetration-testing guides and other group-specific tutorials might be important and can deepen the knowledge of the group and how their members behave. This can also be valuable for defenders in the security industry to counteract the group's tactics, techniques, and procedures (TTPs).
- **Cryptocurrency wallets.** Nowadays, paying salaries in cryptocurrency seems to be a common occurrence among criminal groups. This means that there has to be a list of each of member's wallet stored somewhere. Transactions to these wallets are likely to be much less obfuscated than incoming payments from victims. Finding such a list can be a great way to help piece together the real-life identities of the employees, especially if they are cashing out the money at regular cryptocurrency exchanges.
- **Organizational charts.** In more complex groups, there might be a written form of the organizational chart to describe the hierarchical structure of the group. Getting access to this data can be key to gaining a better understanding of the criminal organization and the key individuals to target with an in-depth investigation.
- **Merger and acquisition data.** In the case of a criminal group having acquired others, there might be documentation on the acquired group's organization or layout. This could be a very interesting finding. If the group is sharing infrastructure and information with partners, suppliers, or affiliates, perhaps getting access to that network infrastructure might be a new target for investigation.
- **Software licenses.** More organized departments would have some standardized software that their developers must use. Perhaps they also have a common messaging system to communicate with each other. There probably is a central repository that any employee can access to install the software, along with the respective licenses. Assuming that the licenses are not pirated, having access to them could allow an investigator to find out more about the organization by working with the software vendors. For example, there might be a new email address for the license, which could be used to pivot and access even more information.

- **Shared calendars.** If the group communicates through online meetings, there is a possibility that the members might be using shared calendars. If a researcher can access the group's email platform, perhaps the same researcher can also access the calendars of the gang's contacts, too, which can provide useful information on their time zones, countries, or other third parties they have business with.

It is worth mentioning that all this shared data might be kept in cloud storage systems such as Google Drive or Dropbox, or on shared cloud application systems such as Google Docs. Therefore, having access to a group member's credentials on any of those platforms can provide an investigator access to relevant information.

Knowing the management structure can give the investigator a baseline of the roles and number of people to look for. For instance, if you know there are 15 coders, the group is possibly large or perhaps medium; therefore, you can expect to find an HR person and a salesperson, among others. This can guide you to look for the right kind of people, instead of only focusing on the developers that you already know about.

Specifically for law enforcement, knowing the size of the targeted criminal organization can lead to prioritizing which groups to pursue over others to achieve maximum impact. Also, bear in mind that the larger the organization is, the less vulnerable it might be to arrests but the more prone to manipulation. Data-gathering techniques are vital. If there is something that the leaked Conti chats have taught us, it's that information disclosure can be far more powerful in crippling a group's operations than server takedowns. Once private information is leaked, the trust relationship between group members and between their external partners can be irreversibly eroded. At that point, reestablishing trust is much more difficult than changing IP addresses or switching to a new internet provider.

In summary, we have established how criminal groups have started behaving like corporations as they grow bigger. Large criminal enterprises are functionally like big companies, and midsize criminal organizations also share many of the characteristics of medium-size companies. A clever investigator can use this knowledge to their advantage.

Being aware of the size of a criminal group under investigation expands the kind of information that researchers can look for. Although this does not mean that the group will be easy to access, finding any of this internal data can still be pivotal and potentially destructive to the adversary's operations. If found, this information can be a powerful weapon for disabling or damaging the group more effectively than a technical takedown can ever do.

Endnotes

1 Gartner. (n.d.) *Gartner*. "Gartner glossary definition of small and midsize businesses." Accessed Feb. 1, 2023, at: Link.

2 Dixie Downing and Fernando Gracia. (July 2021). *The United States International Trade Commission*. "Demographic Makeup of SMEs in the United States and United Kingdom." Accessed on Feb. 1, 2023, at: Link.

3 Brian Krebs. (July 16, 2019). *Krebs on Security*. "Meet the World's Biggest 'Bulletproof' Hoster." Accessed on Feb. 1, 2023, at: Link.

4 United States Department of Justice Office of Public Affairs. (May 16, 2019). *United States Department of Justice Office of Public Affairs*. "GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation." Accessed on Feb. 1, 2023, at: Link.

5 Europol. (May 16, 2019). *Europol*. "GozNym Malware: Cybercriminal Network Dismantled in Criminal Operation." Accessed on Feb. 1, 2023, at: Link.

6 US Department of the Treasury. (Dec. 5, 2019). *US Department of the Treasury*. "Treasury Sanctions Evil Corp, the Russia-Based Criminal Group Behind Dridex Malware." Accessed on Feb. 1, 2023, at: Link.

7 Mandiant Intelligence. (June 2, 2022). *Mandiant Intelligence*. "To Hades and Back: UNC2165 shifts to LockBit to Evade Sanctions." Accessed on Feb. 1, 2023, at: Link.;

8 Trend Micro. (n.d.) *Trend Micro*. Definition of "Counter Antivirus." Accessed on Feb. 6, 2023 at: Link.

9 Trend Micro Research. (May 16, 2018). *Trend Micro*. "The Rise and Fall of Scan4You." Accessed on Feb. 1, 2023, at: Link.

10 US District Court, Aster District of Virginia. (June 30, 2017). *Document Cloud*. "Rusland Bondars and Jurijs Martisevs indictment." Accessed on Feb. 1, 2023, at: Link.

11 Azure. (n.d.). *Microsoft*. "Virtual Machines Series." Accessed on Feb. 1, 2023, at: Link.

12 Sarita Tomar. (n.d.) *Instahyre*. "Software Developer." Accessed on Feb. 1, 2023, at: Link.

13 Catalino Cimpanu. (May 16, 2018). *Bleeping Computer*. "Police Seize Servers of Bulletproof Provider Known for Hosting Malware Ops." Accessed on Feb. 1, 2023, at: Link.

14 Charlie Osborne. (May 17, 2018). *ZDNet*. "MaxiDed, Dead: Law Enforcement Closes Hosting Service Linked to Criminal Activity." Accessed on Feb. 1, 2023, at: Link.

15 Arman Noroozian, Jan Koenders, and Eelco van Veldhuizen (Aug. 14, 2019). *USENIX*. "Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting." Accessed on Feb. 1, 2022, at: Link.

16 Arman Noroozian, Jan Koenders, and Eelco van Veldhuizen (Aug. 14, 2019). *USENIX*. "Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting Abstract." Accessed on Feb. 1, 2023, at: Link.

17 Arman Noroozian, Jan Koenders, and Eelco van Veldhuizen (Aug. 14, 2019). *USENIX*. "Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting." Accessed on Feb. 1, 2022, at: Link.

18 Arman Noroozian, Jan Koenders, and Eelco van Veldhuizen (Aug. 14, 2019). *USENIX*. "Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting." Accessed on Feb. 1, 2022, at: Link.

19 Arman Noroozian, Jan Koenders, and Eelco van Veldhuizen (Aug. 14, 2019). USENIX. "Platforms in Everything: Analyzing Ground-Truth Data on the Anatomy and Economics of Bullet-Proof Hosting." Accessed on Feb. 1, 2022, at: Link.

20 HostSearch. (n.d.) *HostSearch*. "MaxiDed Reviews." Accessed on Feb. 1, 2023, at: Link.

21 Thomas Brewster. (Feb. 28, 2022) *Forbes*. "A Ransomware Crew Pledged Allegiance to Russia, Now Its Data Has Been Stolen." Accessed on Feb. 1, 2023, at: Link.

22 Ned Price. (May 6, 2022) *US State Department*. "Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice." Accessed on Feb. 1, 2023, at: Link.

23 AJ Vicens. (Feb. 25, 2022). *CyberScoop*. "Conti Ransomware Announces Support of Russia, Threatens Retaliatory Attacks." Accessed on Feb. 1, 2023, at: Link.

24 Zach Whittaker. (Feb. 28. 2022). *TechCrunch*. "Conti Ransomware Gang's Internal Chats Leaked Online After Declaring Support Russian Invasion." Accessed on Feb. 1, 2023, at: Link.

25 Monica Pitrelli (April 13, 2022). *CNBC.com*. "Leaked Documents show Notorious Ransomware Group Has an HR Department, Performance Reviews and an 'Employee of the Month.'" Accessed on Feb. 1, 2023, at: Link.

26 Intel471. (April 26, 2022). *Intel471*. "Conti and Emotet: A Constantly Destructive Duo." Accessed on Feb. 1, 2023, at: Link.

27 Ned Price. (May 6. 2022). *US State Department*. "Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice." Accessed on Feb. 1, 2023, at: Link.

28 Chainalysis. (February 2022). *Chainalysis*. "The Crypto Crime Report 2022." Accessed on Feb. 1, 2023, at: Link.

29 vx-underground. (n.d.) *vx-underground*. "Directory: Conti." Accessed on Feb. 1, 2023, at: Link.

30 Chainalysis. (February 2022). *Chainalysis*. "The Crypto Crime Report 2022." Accessed on Feb. 1, 2023, at: Link.

31 Brian Krebs. (March 7, 2022). *Krebs on Security*. "Conti Ransomware Group Diaries, Part IV: Cryptocrime." Accessed on Feb. 20, 2023, at: Link.

32 Brian Krebs. (March 4, 2022). *Krebs on Security*. "Conti Ransomware Group Diaries, Part III: Weaponsry." Accessed on Feb. 20, 2023, at: Link.

33 Crunchbase.com. (n.d.) *Crunchbase Pro*. "Our Products." Accessed on Feb. 20, 2023, at: Link.

34 ZoomInfo.com. (n.d.). *ZoomInfo Pricing*. "Who We Are & Why It Matters." Accessed on Feb. 20, 2023, at: Link.

35 Brian Krebs. (March 7, 2022). *Krebs on Security*. "Conti Ransomware Group Diaries, Part IV: Cryptocrime." Accessed on Feb. 20, 2023, at: Link.

36 BBC. (Nov. 2, 2021). *BBC News*. "Squid Game Crypto Token Collapses in Apparent Scam." Accessed on Feb. 20, 2023, at: Link.

37 Brian Krebs. (March 7, 2022). *Krebs on Security*. "Conti Ransomware Group Diaries, Part IV: Cryptocrime." Accessed on Feb. 20, 2023, at: Link.

38 Check Point Research. (March 10, 2022). *Check Point Research*. "Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Start-Up, Sort Of." Accessed on Feb. 1, 2023, at: Link.

39 Check Point Research. (March 10, 2022). *Check Point Research*. "Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Start-Up, Sort Of." Accessed on Feb. 1, 2023, at: Link.

40 Check Point Research. (March 10, 2022). *Check Point Research*. "Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Start-Up, Sort Of." Accessed on Feb. 1, 2023, at: Link.

41 Check Point Research. (March 10, 2022). *Check Point Research*. "Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Start-Up, Sort Of." Accessed on Feb. 1, 2023, at: Link.

For more information visit **trendmicro.com**