GROUP-IB

HI-TECH CRIME TRENDS 2021/2022

ACCESS BROKERS

Access Brokers

Corporansom

Financial Sector Threats

Cyberwarfare

Scams and phishing

DISCLAIMER

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups 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 and 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.

HI-TECH CRIME TRENDS 2021/2022

Uninvited guests: the sale of access to corporate networks

PART 1

Analysis of dark web forums to understand the sale of access to compromised infrastructure

TABLE OF CONTENTS

GROUP-IB HI-TECH CRIME TRENDS REPORT

00

The Hi-Tech Crime Trends report analyzes cyberattacks, examines how the cybercrime industry functions, and forecasts upcoming changes in the threat landscape for various sectors of the global economy. Group-IB has published the report every year since 2012, integrating valuable data and key insights that the team has gained through over 70,000 hours of experience in responding to cybersecurity incidents worldwide.

The information provided in Hi-Tech Crime Trends enables businesses, NGOs, governments, and law enforcement agencies around the world to fight cybercrime and help potential victims. Intended for IT directors, heads of cybersecurity teams, SOC analysts, incident responders, and other security professionals, the Hi-Tech Crime Trends report serves as a practical guide for strategic and tactical planning.

With the use of unique tools for tracking threat-actor infrastructures and the careful analysis of globally-distributed specialists, Group-IB experts identify and confirm patterns of cyber threats each year. This information serves as a basis for forecasts, which have proven accurate every year since the first Hi-Tech Crime Trends report was published. These forecasts help companies around the world build effective cybersecurity strategies with relevant threats in mind.

The forecasts and recommendations contained in Hi-Tech Crime Trends are aimed at reducing financial losses and infrastructure downtime. They are also designed to help organizations take preventive measures to counteract targeted attacks, espionage, and cyber-terrorism operations.

Group-IB strongly believes that the continual exchange of data, combined with lasting partnerships between private companies and international law enforcement agencies, is the most effective way to combat cybercrime. Cybersecurity awareness helps preserve and protect digital spaces and freedom of communication. It is to these ends that the Hi-Tech Crime Trends report is published.

INTRODUCTION 01

Last year, Group-IB Threat Intelligence analysts provided a comprehensive picture of the shadow industry which sells access to corporate networks on dark-web forums. Such offers have increased in number year after year, but it is challenging to evaluate the overall underground market for selling access because such deals are usually kept secret. However, Group-IB's technology for analyzing underground platforms, which takes into account data that hackers have tried to delete or hide, enables the company's experts to study the market, exchange data with law enforcement officials, and estimate the industry's scale.

Over the past four years, one of the clearest trends on underground forums is the sharp increase in the number of offers to sell access to compromised corporate networks.

Access to a company's corporate network involves Citrix Gateway (later simply referred to as Citrix), VPN and RDP credentials; control panels; web shells; reverse shells; Cobalt Strike sessions; and more. Gaining initial access enables threat actors to penetrate the target company's network and obtain legitimate user or administrator rights.

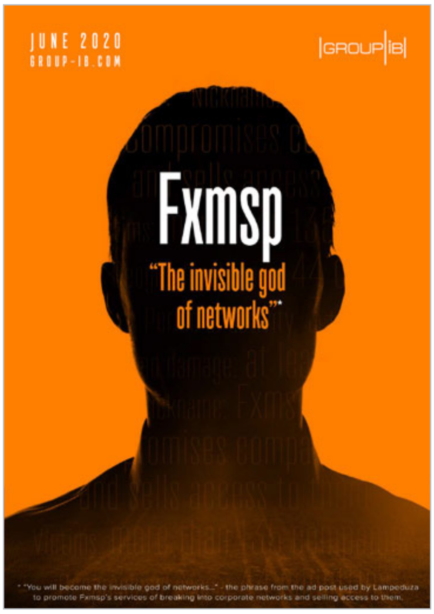
Group-IB experts have identified several factors contributing to the rapid growth of the initial access market.

One such factor is the emergence of Fxmsp, a hacker who first appeared on underground forums in 2017. Posts about selling access to corporate networks had appeared on dark-web resources before, but they had been rare and not streamlined. Fxmsp was the first to focus on gaining initial access for the purpose of selling it.

According to estimates by Group-IB Threat Intelligence specialists, Fxmsp's total revenue likely exceeded $1.5 million. Fxmsp did not focus on compromising a particular industry. The threat actor targeted major banks and hotel chains, but also websites belonging to schools. The hacker's success inspired other threat actors. The first and so far only analytical report about the hacker's tools and tactics, entitled **Fxmsp: "The invisible god of networks"**, is available on Group-IB's website.

Demand creates supply. The principle also applies to the sale of initial access to compromised networks. Beginning in 2019, there was a sharp increase in the number of ransomware attacks, the first stage of which is gaining access to a company's network. This fuelled demand for initial access and bolstered the rise of initial access markets. Initial access brokers (IABs) remove the need for threat groups carrying out ransomware attacks to put any effort in at this stage.

Fxmsp: "The invisible god of networks"


JUNE 2020
GROUP-IB.COM
GROUP-IB
Fxmsp
"The invisible god of networks"*
* "You will become the invisible god of networks..." - the phrase from the ad post used by Lampeduza to promote Fxmsp's services of breaking into corporate networks and selling access to them.

In the report **Ransomware Uncovered 2020—2021**, Group-IB experts noted that ransomware operators had set a record: between 2019 and 2020, they made at least $1 billion, making the year the most profitable for ransomware to date and thereby motivating such groups to continue their activities.

The third factor furthering the rise of initial access markets is the low threshold to enter the industry. A threat actor can gain access by using a type of malware called an information stealer, brute force, or by carrying out a targeted attack. The latter requires in-depth knowledge and skills, while the former two are available to low-skilled threat actors who cannot independently develop a profitable attack. In the case of information stealers, threat actors do not even need to think about how to deliver the malware to the target: the "results" of information stealer activity are sold on underground forums as archives containing various compromised credentials, both personal and corporate. Within that data, threat actors only need to find active accounts for corporate resources. The brute-force scenario does not require much knowledge, either: ready-made programs for brute-forcing passwords are publicly available. Attackers merely pick their victim.

The fact that tools for conducting full-fledged attacks against corporate networks are widely available means that underground actors can make money with almost no risk or effort. The market for initial access has been flooded with low-skilled threat actors who, despite their poor knowledge of the technical aspects involved, pose a threat to companies.

Such attackers (let us call them beginners) select their victims based on how simple it is to gain access to their network rather than on how popular they are, how big their business is, or how much money they make. This primitive way of choosing a target means that any company, regardless of its size or other characteristics that are important to highly skilled threat actors, is at risk of being compromised.

This explains why major companies are likely to be compromised even by low-skilled threat actors, which is now even more likely given how common remote work practices have become due to the COVID-19 pandemic.

Information that IABs provide about their targets sometimes helps **Group-IB Threat Intelligence** analysts identify victims even before access to their infrastructure is sold. This shortens incident detection time and, in some cases, prevents attacks from being developed further.

This report looks at key aspects of how and why the market for initial access to corporate networks has developed, provides a detailed analysis of the most active sellers' activity, and presents statistics on the most targeted countries and industries.

Ransomware Uncovered 2020—2021

KEY TRENDS 02

RANSOMWARE HAS GENERATED WORK FOR MANY HACKERS

Conti, LockBit, PYSA and REvil affiliate programs have been the most active.

MORE THAN 200 NEW BROKERS

Entered the market between H2 2020 and H1 2021.

THE LEADING COUNTRIES

With regard to the number of access offers are still the United States (30%), France (5%), and the United Kingdom (4%). Offers to sell access to companies in Australia (4%) and India (3%) have increased significantly.

THE TOP INDUSTRIES

In which initial access was put up for sale in 2020–2021 are manufacturing, education, financial services, healthcare, and trade.

A NEW TREND

Is emerging among IABs: in their posts, they have started including a short description of the victim company specifying its revenue, location, and industry. It is becoming increasingly rare for IABs to focus on technical aspects of vulnerable servers and databases.

1,099 ACCESS OFFERS

In total, were made between H2 2020 and H1 2021.

THE NUMBER OF SELLERS

Between H2 2020 and H1 2021 grew by **205%** compared to H2 2019–H1 2020.

THE NUMBER OF OFFERS

To sell access made between H2 2020 and H1 2021 grew by **204%** compared to the same period the previous year.

THE OVERALL MARKET SIZE

In the current period (H2 2020–H1 2021) is **$7,165,387**, which is 16% higher than in the previous period (H2 2019–H1 2020), when the market was **$6,189,388**.

THE PRIMARY METHOD

Of gaining access to corporate networks has remained the same for brokers: exploiting vulnerabilities in published applications and compromising accounts for remote access tools.

THE LEADERS IN ACCESS SALES

Have changed: five brokers make 35% of all the profit from access sale offers.

FORECASTS 03

THE NUMBER OF BROKERS

Will grow, while the average price for access will go down

INITIAL ACCESS BROKERS

May create their own platforms for auctioning off access.

RANSOMWARE

Will remain the main way to monetize access

CLOUD SINGLE SIGN-ON

May become a new entry point to networks, as more and more companies switch to this technology. Threat actors will gain access to applications and services accessible through cloud sign-on.

HOW THE MARKET DEVELOPED

04

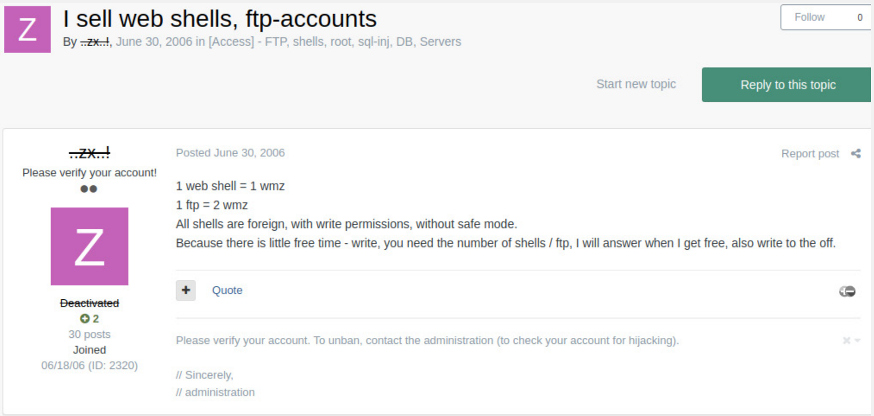
Authentication data has been sold on underground forums since they came into existence. One noteworthy example is CarderPlanet, which appeared in 2001.

At first, threat actors sold data that was easy to monetize, such as bank accounts, from which threat actors withdrew money to third-party accounts, and bank card data, which was used to make fraudulent transactions.

Over time, the type of information being exchanged on dark web markets changed from stolen financial data to other types of valuable information. This shift was largely the result of new security controls that made it more difficult to monetize the type of financial data previously exchanged on these underground forums.

Access to remote devices emerged on the black market in the early 2000s: threat actors would provide access to individual servers for a relatively small fee. This usually involved web shells on websites or FTP access.

Below, and throughout this report, we use historical data and screenshots stored by our platform, **Group-IB Threat Intelligence & Attribution**.



I sell web shells, ftp-accounts

By ~~..zx..!~~, June 30, 2006 in [Access] - FTP, shells, root, sql-inj, DB, Servers

~~..zx..!~~
Please verify your account!
~~Deactivated~~
2
30 posts
Joined
06/18/06 (ID: 2320)

Posted June 30, 2006

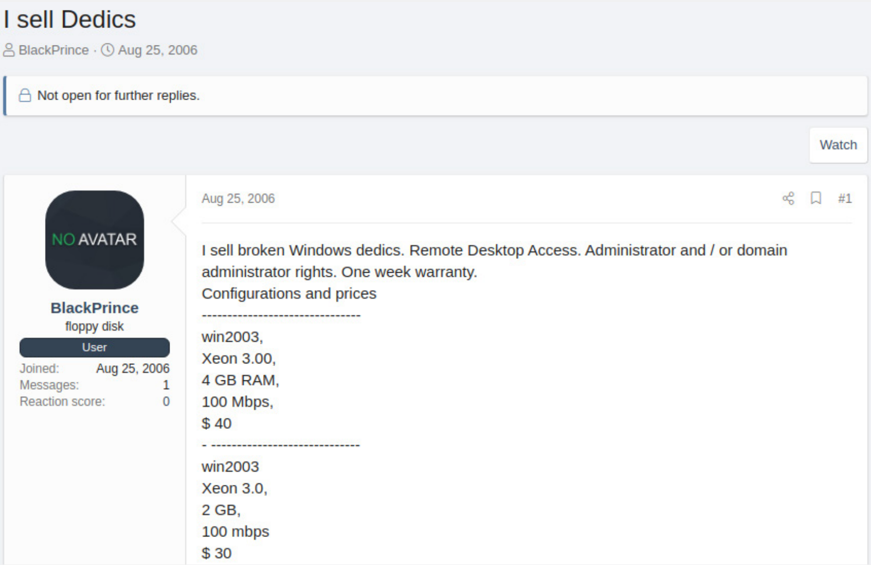
1 web shell = 1 wmz
1 ftp = 2 wmz
All shells are foreign, with write permissions, without safe mode.
Because there is little free time - write, you need the number of shells / ftp, I will answer when I get free, also write to the off.

Please verify your account. To unban, contact the administration (to check your account for hijacking).

// Sincerely,
// administration

Fig. 1. A post about selling web shells and FTP access

In the second half of the 2000s, offers to sell brute-forced remote access to dedicated servers emerged in various countries, and such access was mostly bought for the purposes of fraud.



I sell Dedics

BlackPrince · Aug 25, 2006

Not open for further replies.

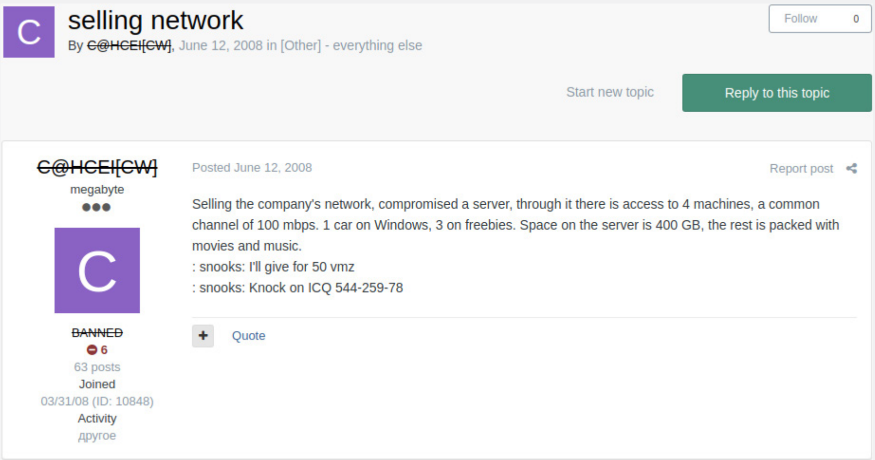
BlackPrince
floppy disk
User
Joined: Aug 25, 2006
Messages: 1
Reaction score: 0

Aug 25, 2006 #1

I sell broken Windows dedics. Remote Desktop Access. Administrator and / or domain administrator rights. One week warranty.
Configurations and prices
----
win2003,
Xeon 3.00,
4 GB RAM,
100 Mbps,
$ 40
- ------------------------------
win2003
Xeon 3.0,
2 GB,
100 mbps
$ 30

Fig. 2. A post about selling access to dedicated servers

At the time, it was typical for threat actors to not conduct any additional analysis after finding servers and gaining access to them; they did not realize that the compromised servers could belong to major companies and could therefore be monetized easily. At the time, the computing power of compromised servers, the memory available on them, and the bandwidth were the commodities most valuable to threat actors.



selling network

By ~~C@HCEI[CW]~~, June 12, 2008 in [Other] - everything else

~~C@HCEI[CW]~~
megabyte
~~BANNED~~
6
63 posts
Joined
03/31/08 (ID: 10848)
Activity
другое

Posted June 12, 2008

Selling the company's network, compromised a server, through it there is access to 4 machines, a common channel of 100 mbps. 1 car on Windows, 3 on freebies. Space on the server is 400 GB, the rest is packed with movies and music.
: snooks: I'll give for 50 vmz
: snooks: Knock on ICQ 544-259-78

Fig. 3. A post about selling access to a server, with the technical specifications mentioned

Much later, around the second half of the 2010s, threat actors took an interest in information stored on servers.

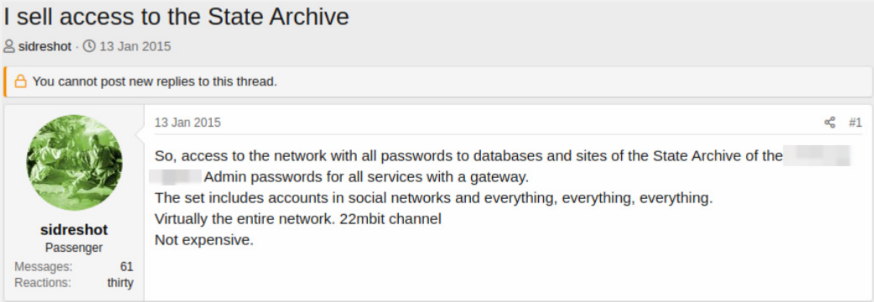
However, those who obtain such information might not necessarily know how to use it. This is true for situations where, instead of aiming to gain access to a specific object, a threat actor chooses a victim that can be hacked using a small skill set and basic knowledge about potential vulnerabilities.

Nevertheless, it was the shift in focus to information stored on servers that pushed threat actors to learn to whom their compromised devices belonged.

Interestingly, despite the same access mechanisms, descriptions in sales-related forum threads changed together with views on monetization. Between 2005 and 2014, the most common title was “Selling dedicated server.”

Since 2015, such posts are more often titled “Selling network access” or “Selling access to company.” Instead of focusing on the technical capabilities of the servers that they gain access to, threat actors now prioritize what information the servers contain and to whom the servers belong. This marked the emergence of the market for initial access.

However, in the early days of the access market, threat actors often struggled to think of a way to monetize the information they obtained.



I sell access to the State Archive

sidreshot · 13 Jan 2015

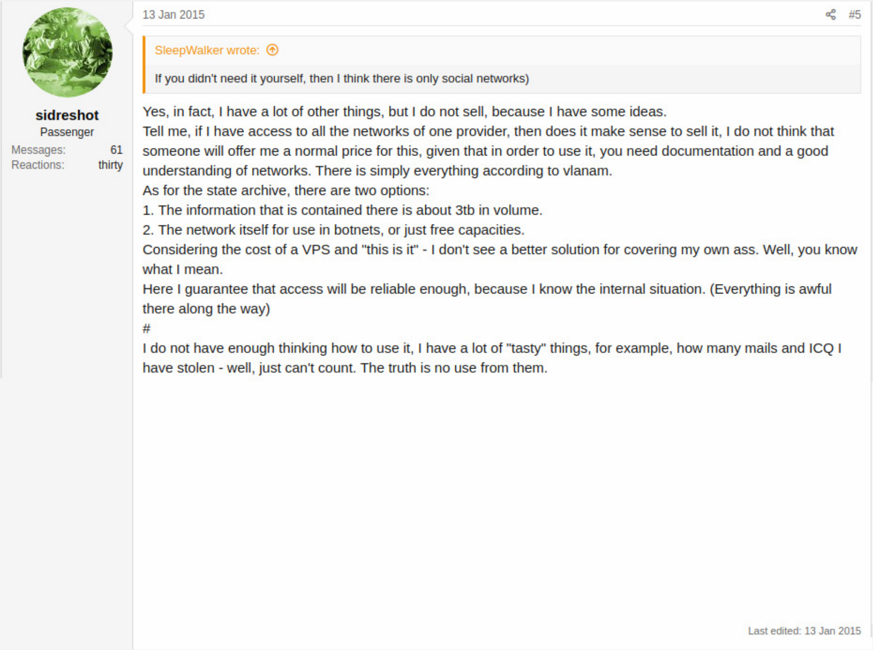
You cannot post new replies to this thread.

sidreshot
Passenger
Messages: 61
Reactions: thirty

13 Jan 2015 #1

So, access to the network with all passwords to databases and sites of the State Archive of the [redacted] Admin passwords for all services with a gateway.
The set includes accounts in social networks and everything, everything, everything.
Virtually the entire network. 22mbit channel
Not expensive.

Fig. 4. A post by the user sidreshot on the forum Rutor



sidreshot
Passenger
Messages: 61
Reactions: thirty

13 Jan 2015 #5

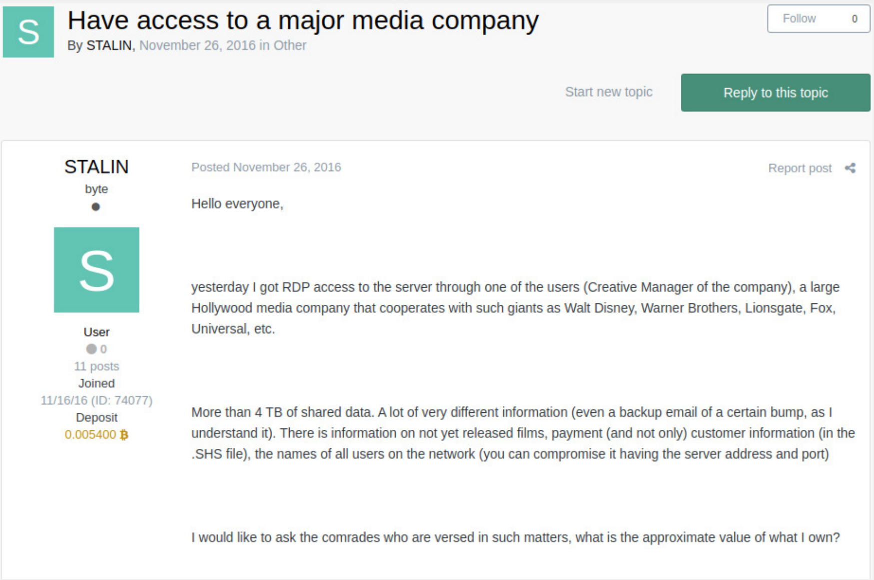
> SleepWalker wrote:
> If you didn't need it yourself, then I think there is only social networks)

Yes, in fact, I have a lot of other things, but I do not sell, because I have some ideas.
Tell me, if I have access to all the networks of one provider, then does it make sense to sell it, I do not think that someone will offer me a normal price for this, given that in order to use it, you need documentation and a good understanding of networks. There is simply everything according to vlanam.
As for the state archive, there are two options:
1. The information that is contained there is about 3tb in volume.
2. The network itself for use in botnets, or just free capacities.
Considering the cost of a VPS and "this is it" - I don't see a better solution for covering my own ass. Well, you know what I mean.
Here I guarantee that access will be reliable enough, because I know the internal situation. (Everything is awful there along the way)
#
I do not have enough thinking how to use it, I have a lot of "tasty" things, for example, how many mails and ICQ I have stolen - well, just can't count. The truth is no use from them.

Last edited: 13 Jan 2015

Fig. 5. A comment by a threat actor about searching for a way to monetize access

Unclear ideas about monetization in turn caused difficulties in deciding on the price of initial access. The example in Figure 6 shows, a threat actor is trying to find out an appropriate price from other forum users.



Have access to a major media company

By STALIN, November 26, 2016 in Other

STALIN
byte

User
0
11 posts
Joined
11/16/16 (ID: 74077)
Deposit
0.005400 ฿

Posted November 26, 2016

Hello everyone,

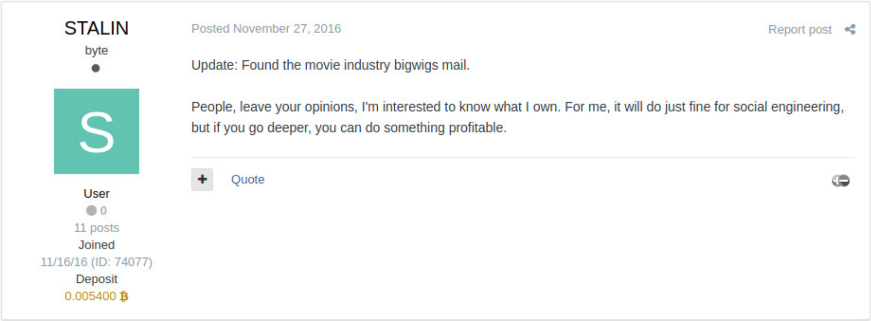
yesterday I got RDP access to the server through one of the users (Creative Manager of the company), a large Hollywood media company that cooperates with such giants as Walt Disney, Warner Brothers, Lionsgate, Fox, Universal, etc.

More than 4 TB of shared data. A lot of very different information (even a backup email of a certain bump, as I understand it). There is information on not yet released films, payment (and not only) customer information (in the .SHS file), the names of all users on the network (you can compromise it having the server address and port)

I would like to ask the comrades who are versed in such matters, what is the approximate value of what I own?

Fig. 6. A message by the user STALIN on the forum Exploit

One option that the threat actor (who had gained RDP access) came up with was an attack involving social engineering. Below is a post from 2016.



STALIN
byte

User
0
11 posts
Joined
11/16/16 (ID: 74077)
Deposit
0.005400 ฿

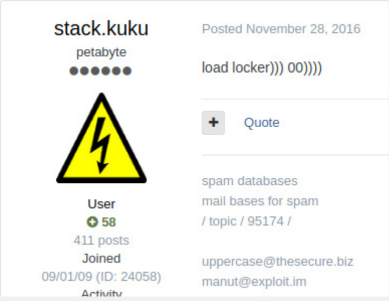
Posted November 27, 2016

Update: Found the movie industry bigwigs mail.

People, leave your opinions, I'm interested to know what I own. For me, it will do just fine for social engineering, but if you go deeper, you can do something profitable.

Fig. 7. A comment by the user STALIN on the forum Exploit

The ideas that emerged on underground forums back then have now become a reality. For instance, one forum user jokingly left a comment suggesting to upload ransomware to the target company's network. Clearly, at the time, no one realized that the alliance between IABs and ransomware operators would become one of the most dangerous and profitable relationships in the history of cybercrime.



stack.kuku
petabyte
●●●●●●

User
58
411 posts
Joined
09/01/09 (ID: 24058)
Activity

Posted November 28, 2016

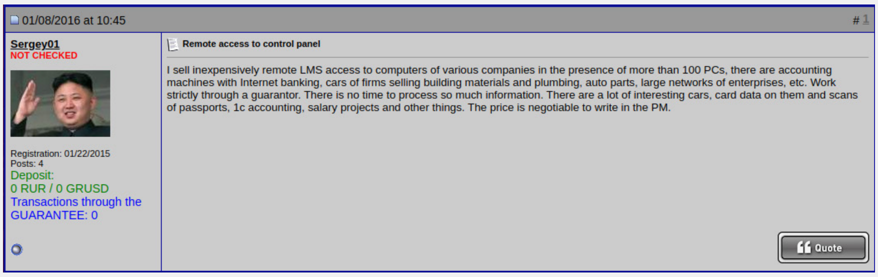
load locker))) 00))))

spam databases
mail bases for spam
/ topic / 95174 /

uppercase@thesecure.biz
manut@exploit.im

Fig. 8. A comment by the user stack.kuku on the forum Exploit

Although attempts to sell access to corporate networks were made, they were not streamlined. Offers for the sale of initial access were rare. As threads of this kind continued, threat actors came up with more ideas about how to monetize initial access, most of which were applicable to web shells that had been offered on forums from the beginning.



01/08/2016 at 10:45 # 1

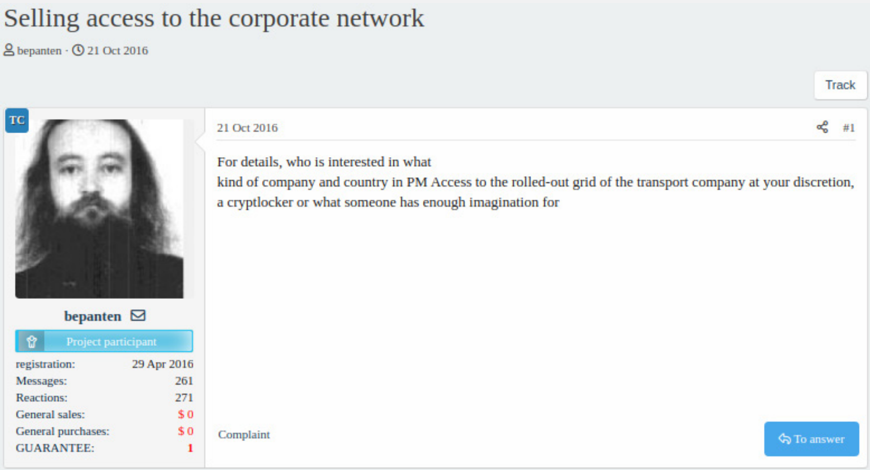
Sergey01
NOT CHECKED

Registration: 01/22/2015
Posts: 4
Deposit:
0 RUR / 0 GRUSD
Transactions through the
GUARANTEE: 0

Remote access to control panel

I sell inexpensively remote LMS access to computers of various companies in the presence of more than 100 PCs, there are accounting machines with Internet banking, cars of firms selling building materials and plumbing, auto parts, large networks of enterprises, etc. Work strictly through a guarantor. There is no time to process so much information. There are a lot of interesting cars, card data on them and scans of passports, 1c accounting, salary projects and other things. The price is negotiable to write in the PM.

Fig. 9. An offer to sell access in 2016



Selling access to the corporate network

bepanten · 21 Oct 2016

bepanten
Project participant

registration: 29 Apr 2016
Messages: 261
Reactions: 271
General sales: $ 0
General purchases: $ 0
GUARANTEE: 1

21 Oct 2016 #1

For details, who is interested in what
kind of company and country in PM Access to the rolled-out grid of the transport company at your discretion,
a cryptlocker or what someone has enough imagination for

Fig. 10. Another offer to sell access to a corporate network in 2016

In 2017, the situation changed as some threat actors began to focus exclusively on gaining and selling access to corporate networks. One of the most notorious hackers was **Fxmsp**, who pioneered the sale of initial access.

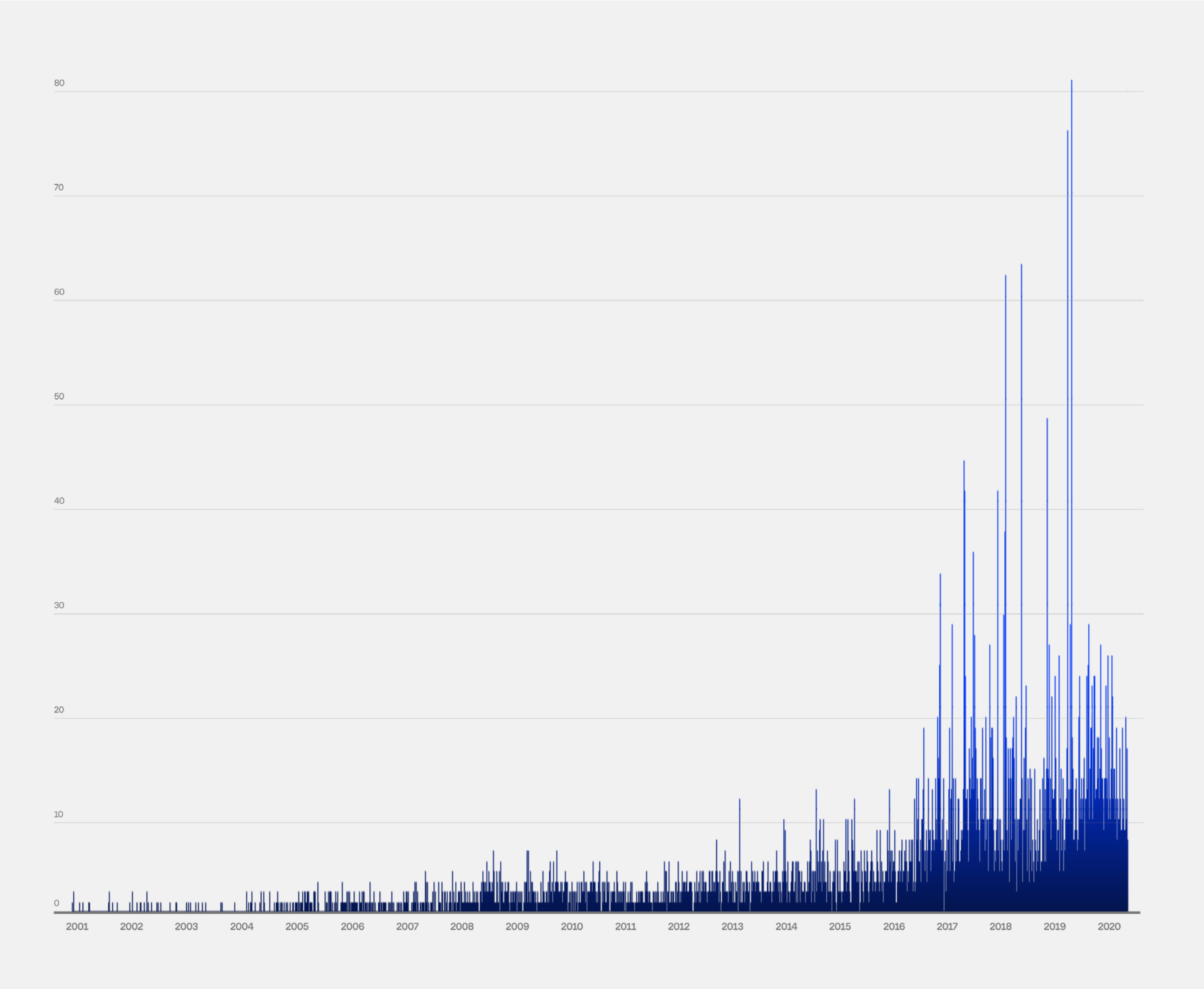
Fxmsp: "The invisible god of networks"

HOW FXMSP CHANGED THE ACCESS MARKET

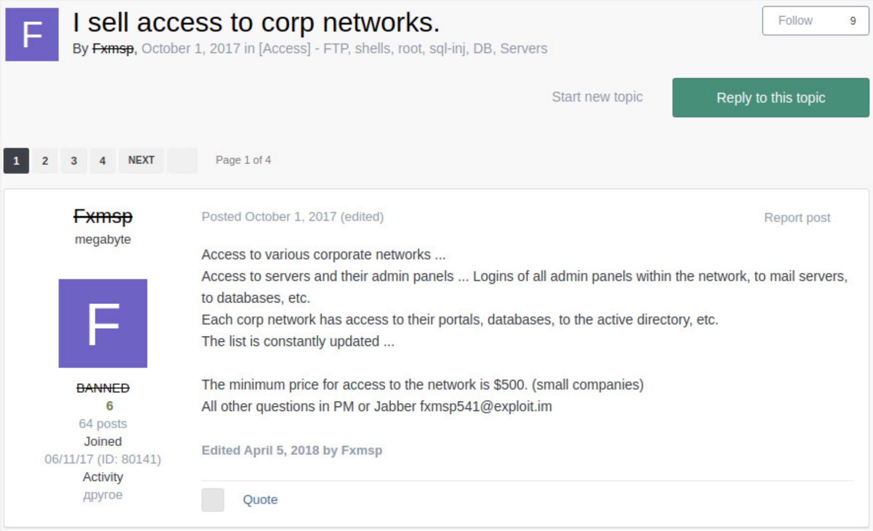
05

Before Fxmsp arrived on the scene, the number of access offers remained stable. Between 2015 and 2016, there were no more than ten ads. The figure stayed the same until October 2017, when the number of offers to sell access to corporate networks on underground forums began growing exponentially.

Fig. 11. Offers to sell access by year



In October 2017 an advert was posted on one of the most popular Russian-speaking underground forums, **Exploit**. The ad was for the sale of access to corporate networks belonging to various companies. For the first time, an individual with an unusual username was offering access to all the critically important network segments of compromised organizations and claimed that a bank was among the victims. Back then, this was entirely unprecedented.



I sell access to corp networks.

By ~~Fxmsp~~, October 1, 2017 in [Access] - FTP, shells, root, sql-inj, DB, Servers

~~Fxmsp~~
megabyte
~~BANNED~~
6
64 posts
Joined
06/11/17 (ID: 80141)
Activity
другое

Posted October 1, 2017 (edited)

Access to various corporate networks ...
Access to servers and their admin panels ... Logins of all admin panels within the network, to mail servers, to databases, etc.
Each corp network has access to their portals, databases, to the active directory, etc.
The list is constantly updated ...

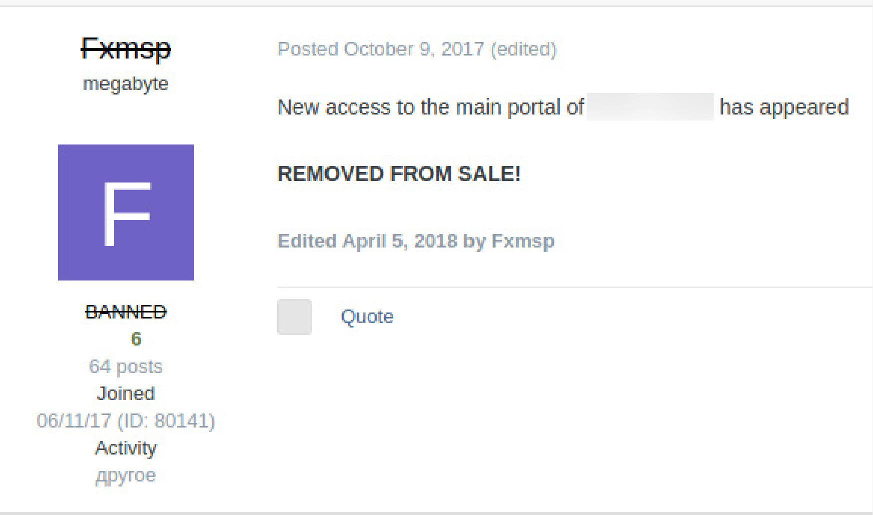
The minimum price for access to the network is $500. (small companies)
All other questions in PM or Jabber fxmsp541@exploit.im

Edited April 5, 2018 by Fxmsp

Fig. 12. Fxmsp's first post about selling access on the forum Exploit

From the start, Fxmsp realized that not understanding the victim reduces demand and, as a result, increases the time it takes to sell access.

A week after posting his first ad, which contained no specific details about the victims, Fxmsp left a message in which he named the company to which he was selling access. The year was 2017, and it can be called a watershed moment for the industry of selling unauthorized access to compromised corporate networks.



~~Fxmsp~~
megabyte
~~BANNED~~
6
64 posts
Joined
06/11/17 (ID: 80141)
Activity
другое

Posted October 9, 2017 (edited)

New access to the main portal of [redacted] has appeared

REMOVED FROM SALE!

Edited April 5, 2018 by Fxmsp

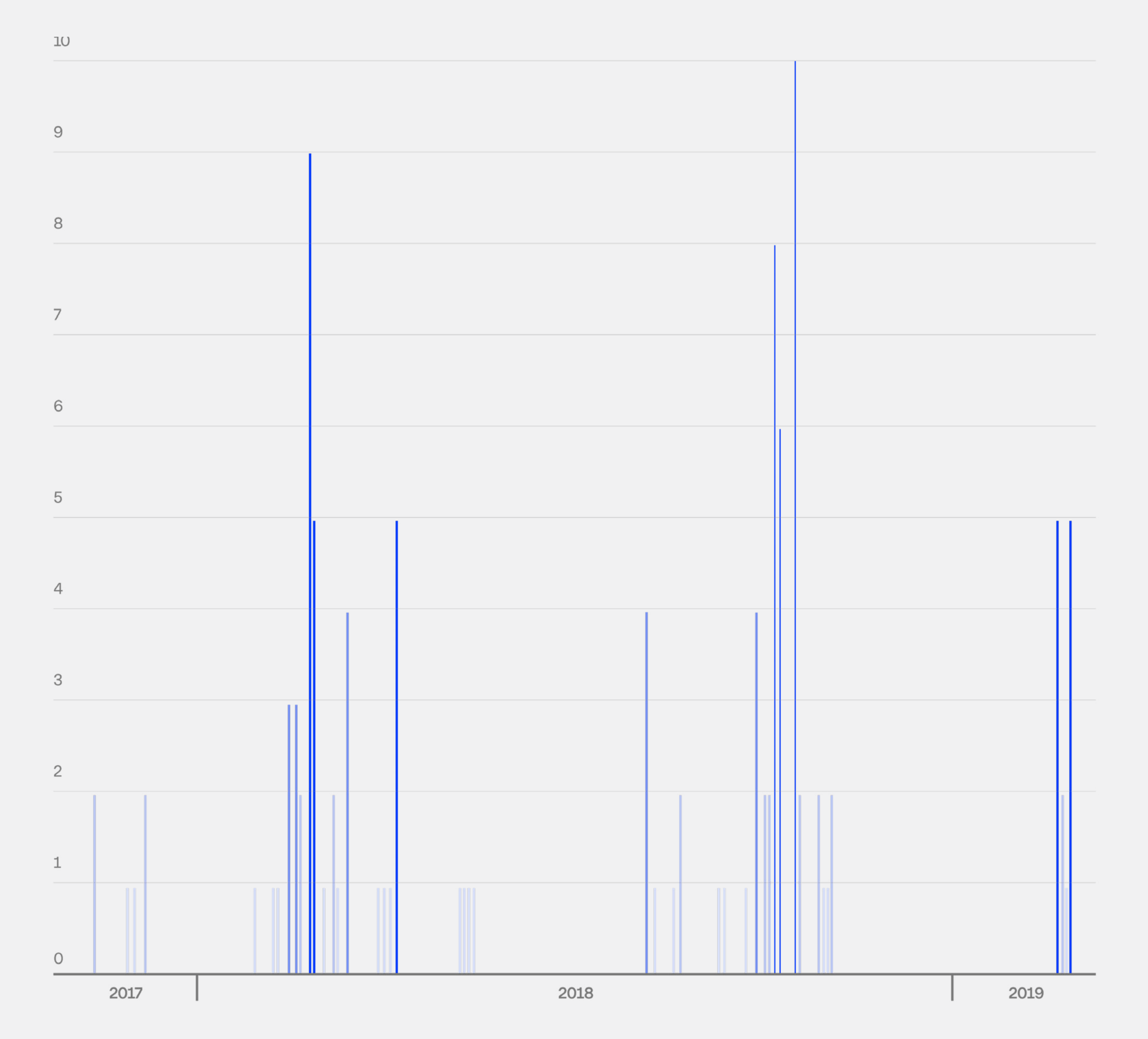
Fig. 13. Fxmsp's ad about selling access, with the victim's name specified

Throughout his activity, Fxmsp specified who his victims were.

Group-IB specialists analyzed Fxmsp's activity in the Russian-speaking underground from the moment he registered on the first forum in September 2016 until late 2019, when he ceased all public activity. More information is available in the report entitled **Fxmsp: "The invisible god of networks."**

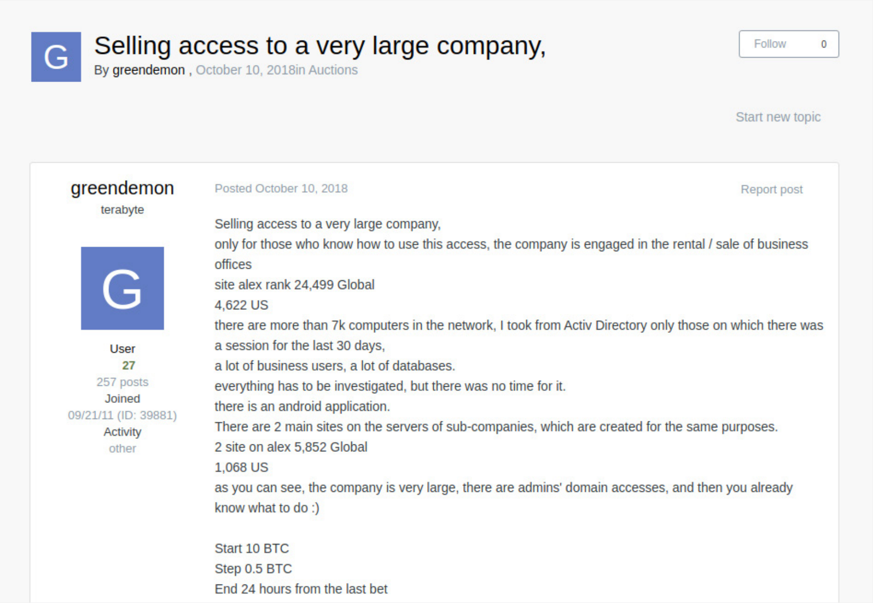
Throughout his activity, Fxmsp posted 135 ads about selling access to corporate networks, which made him at least $1.5 million. The figure below shows a timeline of Fxmsp's posts about selling unauthorized access to networks on underground forums.

Fig. 14. A timeline of Fxmsp's posts on underground forums



In late October 2018, Fxmsp's activity came under threat. It turned out that both Fxmsp and Lampeduza, the alias of Fxmsp's sales manager, tried to sell access to the same network to different buyers. On October 24 of that year, both users were banned from the main underground forum. The duo suspended its activity on all other forums and allegedly focused on "private sales," i.e., they worked only with a limited circle of trusted clients. Nevertheless, the threat actor's fruitful activity motivated numerous hackers to start a similar "business."

In 2018, other users started actively posting on Exploit about selling access to corporate networks.



Selling access to a very large company,

By greendemon , October 10, 2018in Auctions

greendemon
terabyte
User
27
257 posts
Joined
09/21/11 (ID: 39881)
Activity
other

Posted October 10, 2018

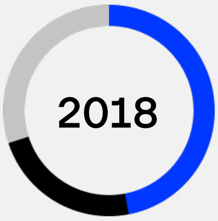
Selling access to a very large company,
only for those who know how to use this access, the company is engaged in the rental / sale of business offices
site alex rank 24,499 Global
4,622 US
there are more than 7k computers in the network, I took from Activ Directory only those on which there was a session for the last 30 days,
a lot of business users, a lot of databases.
everything has to be investigated, but there was no time for it.
there is an android application.
There are 2 main sites on the servers of sub-companies, which are created for the same purposes.
2 site on alex 5,852 Global
1,068 US
as you can see, the company is very large, there are admins' domain accesses, and then you already know what to do :)

Start 10 BTC
Step 0.5 BTC
End 24 hours from the last bet

Fig. 15. A post on Exploit from 2018 about selling access to a major company

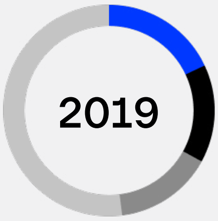
In 2018, Group-IB's Threat Intelligence & Attribution platform detected 141 threads about selling unauthorized access, 98 of which belonged to Fxmsp and his sales manager Lampeduza.

Statistics on threat actors who sold access to networks in 2018



Threat actor	%
Lampeduza	47
Fxmsp	23
BartSimpson	1
x999xx	1
Jendely	2
jabber	2
raf	2
Другие	22

Statistics on threat actors who sold access to networks in 2019



Threat actor	%
Lampeduza	18
Network	15
B.Wanted	15
toon1c3	2
streetskip	3
greendemon	3
nikolaruss	3
x999xx	4
SilvioBerlusconi	4
bc.monster	7
Другие	28

The two diagrams on the previous page show that in 2018 Fxmsp and Lampeduza were the absolute market leaders and left their competitors far behind, while 2019 saw the emergence of new threat actors who gained considerable market share, even surpassing the share of the market controlled by Fxmsp and Lampeduza.

Nevertheless, it was Fxmsp and Lampeduza who created the market for selling unauthorized access to corporate networks as we know it today. Fxmsp formed the concept of a specialized underground threat actor: a broker of initial access to corporate networks. He pioneered this activity and showed other threat actors how initial access could be monetized on the black market.

It is uncertain whether Fxmsp still operates.

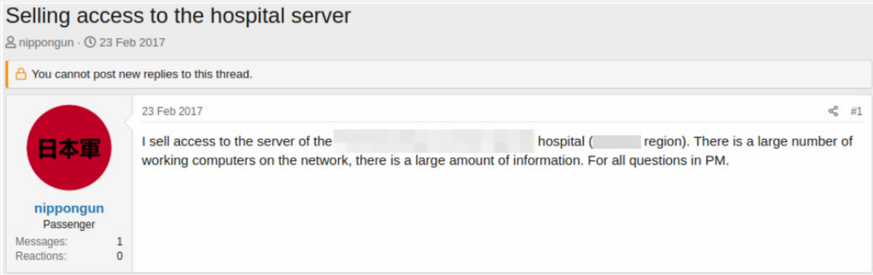
Group-IB's analysis of the threat actor's activity helped uncover the tools he used to compromise companies. For the first time, details about the hacker's identity were revealed in our report entitled **Fxmsp: "The invisible god of networks"** in which we also give recommendations on how to protect against such attacks.

Fxmsp: "The invisible god of networks"

IMPACT OF RANSOMWARE AS A SERVICE ON THE MARKET

06

IABs used to mention the number and characteristics of hosts in compromised networks and highlight the large volume of data available. As ransomware attacks became more popular, however, such details stopped attracting buyers. Below is a post about selling access at a time when the ransomware-as-a-service (RaaS) sales model was not as popular as it is today.



Selling access to the hospital server

nippongun · 23 Feb 2017

You cannot post new replies to this thread.

日本軍

nippongun
Passenger
Messages: 1
Reactions: 0

23 Feb 2017 #1

I sell access to the server of the [redacted] hospital ([redacted] region). There is a large number of working computers on the network, there is a large amount of information. For all questions in PM.

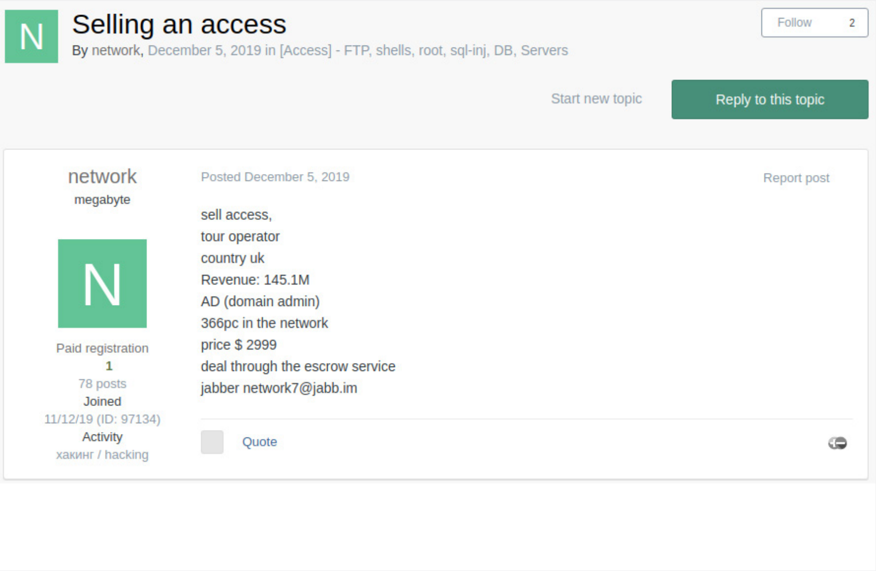
Fig. 16. A post by the user nippongun on the forum Rutor in 2017

After obtaining access, threat actors would look for information about their victim to determine a fair asking price. The price is influenced by the following characteristics of the target company:

- Revenue
- Brand awareness
- Industry
- Scale of business

The above details attract more attention and therefore make it easier to find a buyer and accelerate the sale.

Below is a thread about selling access published around the same time that the RaaS model was beginning to gain popularity.



Selling an access

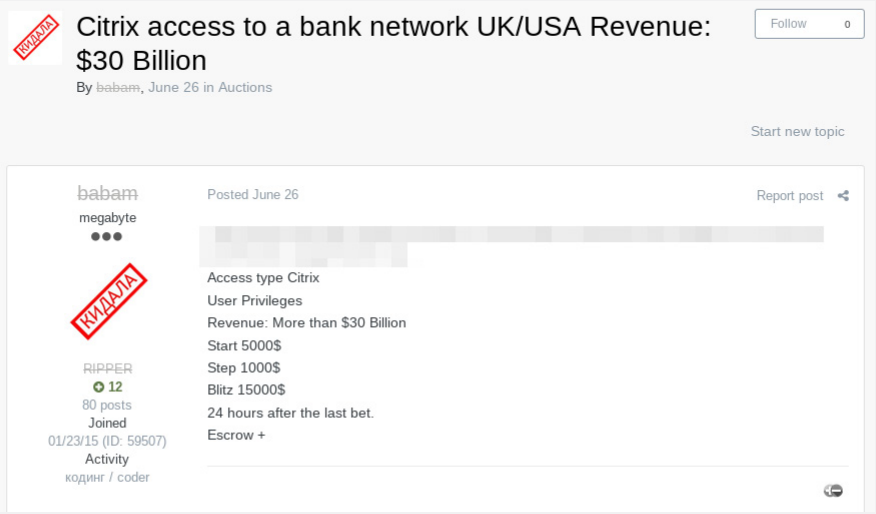
By network, December 5, 2019 in [Access] - FTP, shells, root, sql-inj, DB, Servers

sell access,
tour operator
country uk
Revenue: 145.1M
AD (domain admin)
366pc in the network
price $ 2999
deal through the escrow service
jabber network7@jabb.im

Fig. 17. A post by the user network in 2019

Information about a company's revenue is the decisive factor for threat groups who conduct ransomware attacks, as it helps them determine the ransom size.

Usually, access to networks belonging to companies with the highest revenues is particularly popular among buyers. In the example below, the user **babam** advertised access to the corporate network of a major bank with a revenue of over $30 billion.



Citrix access to a bank network UK/USA Revenue: $30 Billion

By ~~babam~~, June 26 in Auctions

[redacted]

Access type Citrix
User Privileges
Revenue: More than $30 Billion
Start 5000$
Step 1000$
Blitz 15000$
24 hours after the last bet.
Escrow +

Fig. 18. A post by the user babam about selling Citrix access to a major bank

A few hours after the post was published, an interested user wrote a message, after which the access was purchased.

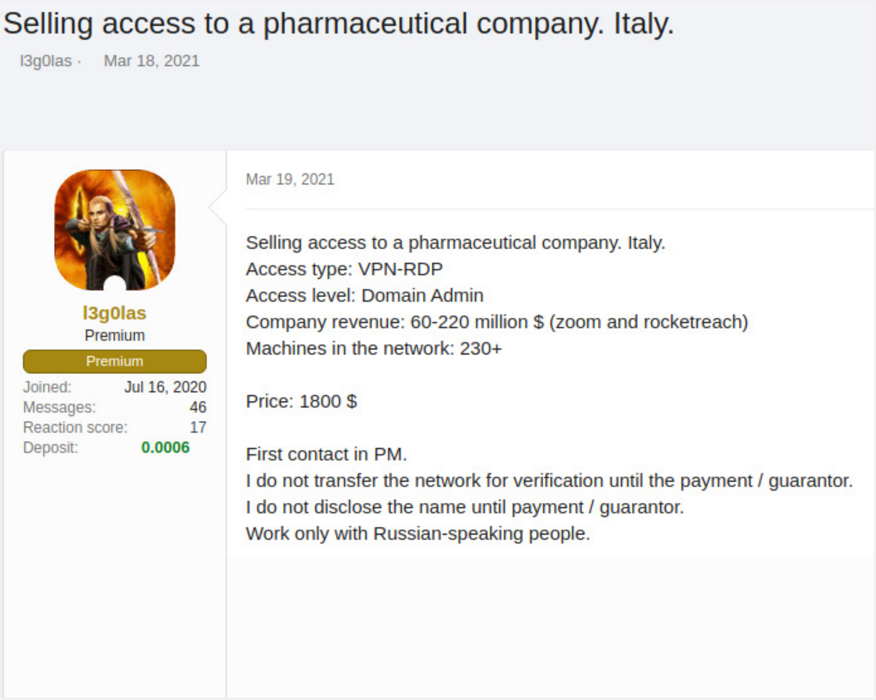
What types of access do ransomware operators buy?

A key criterion for choosing victims is their brand awareness. After infecting a company with ransomware, threat actors use blackmail them and threaten to disclose all the data in the corporate network if the company refuses to pay a ransom. The outcome jeopardizes the victim's reputation and, if the company is well known, the attack could completely halt the company's operations.

Characteristics such as industry and scale of business are also significant for threat actors who use RaaS. Such information helps them assess how well the target company is known and what its revenue is, which is why such details often appear in posts that advertise the sale of access. In addition, knowing the target company's industry helps attackers determine what type of data they could obtain, if they gain access.

Threat groups take the above factors into account when deciding whether it is worth carrying out an attack and whether it will satisfy their financial ambitions.

A key factor that affects the price and speed of the sale is the level of access: the higher it is, the more expensive the offer. Below is a thread about selling access to an Italian pharmaceutical company with administrator rights.



Selling access to a pharmaceutical company. Italy.

l3g0las · Mar 18, 2021

Mar 19, 2021

Selling access to a pharmaceutical company. Italy.
Access type: VPN-RDP
Access level: Domain Admin
Company revenue: 60-220 million $ (zoom and rocketreach)
Machines in the network: 230+

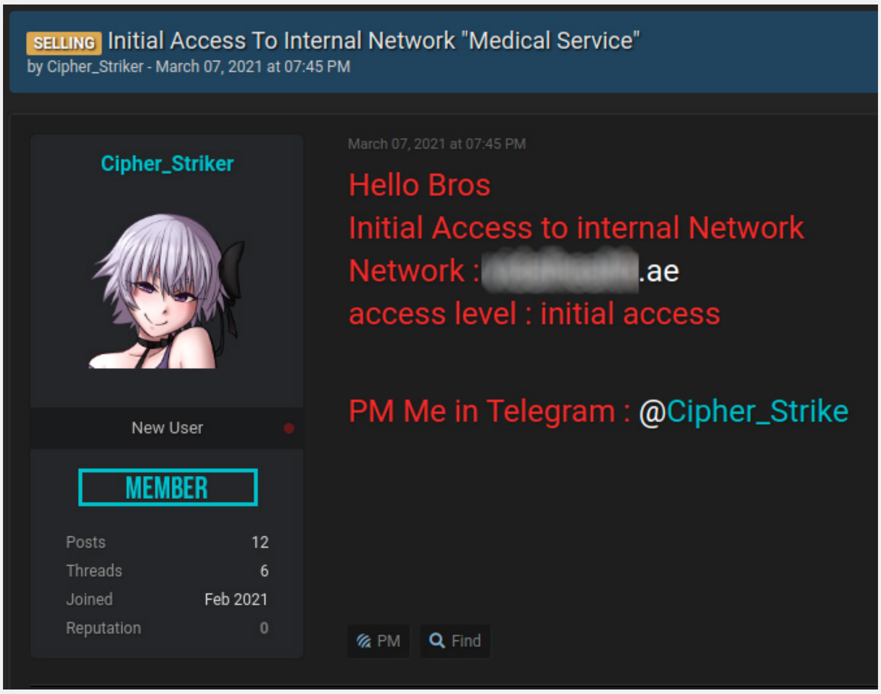
Price: 1800 $

First contact in PM.
I do not transfer the network for verification until the payment / guarantor.
I do not disclose the name until payment / guarantor.
Work only with Russian-speaking people.

Fig. 19. A post about selling access to an Italian pharmaceutical company

Access with domain administrator rights provides all existing privileges, so the purchasing threat actor gets access to all information in the network and can manage other accounts. For a threat actor planning to purchase access, the words "Domain Admin" in an ad mean that they will not struggle to steal information from the network in question or to launch malware, and the only thing standing between them and the target is the price of the access, which is likely to pay off.

Threat actors sometimes directly mention the company to which they are selling access. The screenshot below shows a thread about selling access to a healthcare organization in the United Arab Emirates (UAE).



Initial Access To Internal Network "Medical Service"
by Cipher_Striker - March 07, 2021 at 07:45 PM

Cipher_Striker
New User
MEMBER

Posts	12
Threads	6
Joined	Feb 2021
Reputation	0

March 07, 2021 at 07:45 PM

Hello Bros
Initial Access to internal Network
Network : [redacted].ae
access level : initial access

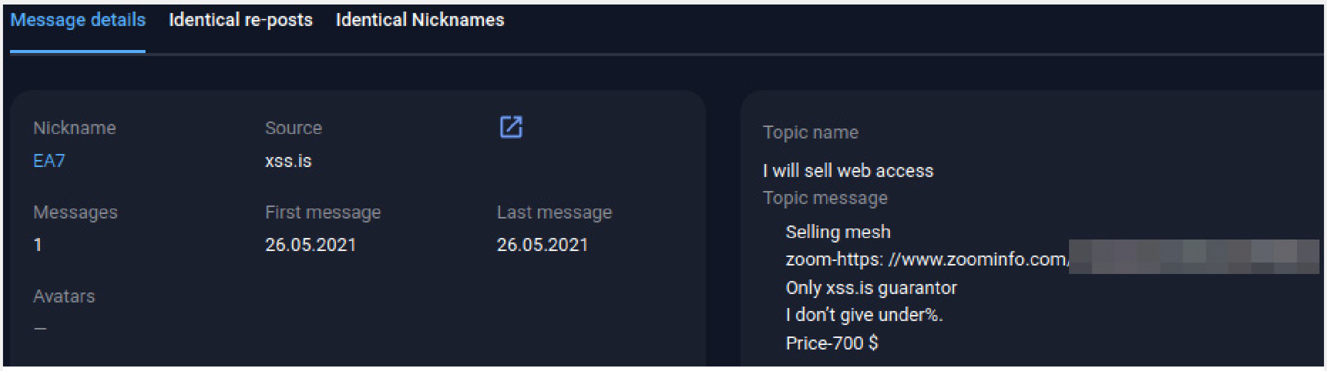
PM Me in Telegram : @Cipher_Strike

Fig. 20. A post about selling access to a healthcare organization in the UAE

However, this approach to publishing ads is risky for threat actors because security researchers are likely to notify the victim company, which will result in the access being closed. For this reason, most sellers prefer giving key information about the compromised company (annual revenue, type of access, country, and industry) without mentioning its name.

In some cases, IABs take descriptions from official websites or business databases.

In the example below, the seller included a link to the company's page on a website called Zoominfo. The thread is currently unavailable on the forum; the screenshot was saved by Group-IB's Threat Intelligence & Attribution platform.

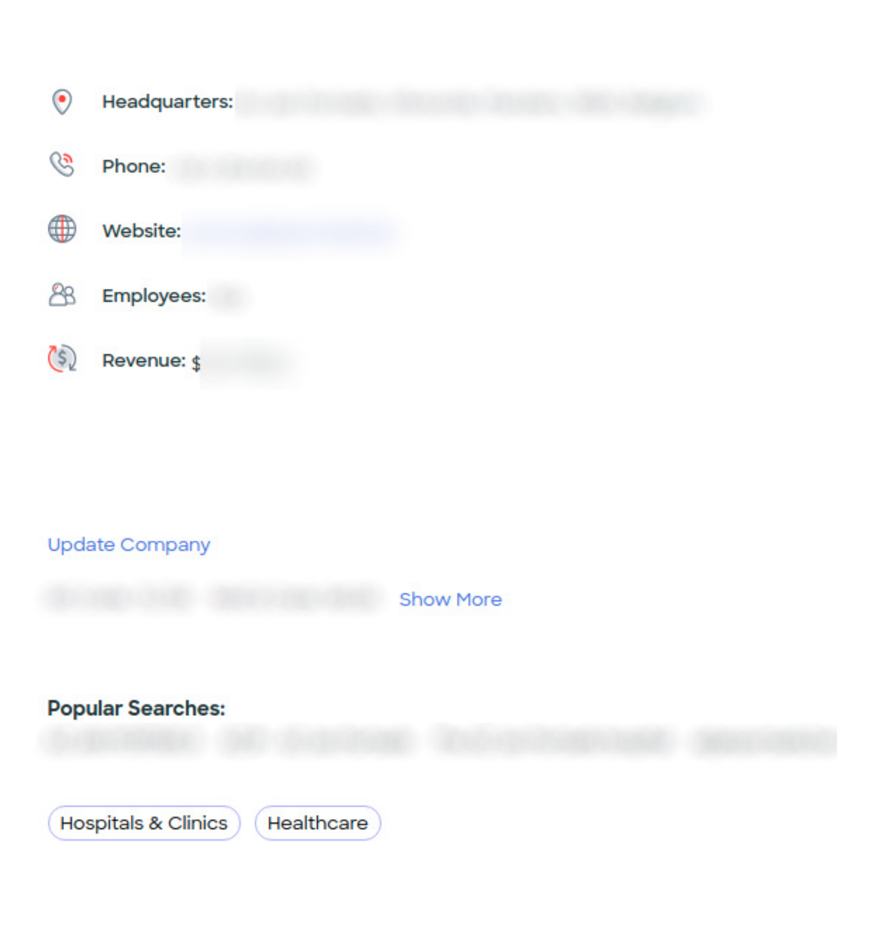


Nickname	Source	
EA7	xss.is	
Messages	First message	Last message
1	26.05.2021	26.05.2021
Avatars		
–		

Topic name
I will sell web access
Topic message
Selling mesh
zoom-https: //www.zoominfo.com/[redacted]
Only xss.is guarantor
I don't give under%.
Price-700 $

Fig. 21. A post about selling access to a Belgian healthcare organization

Zoominfo is a website that provides information about companies from its database. As shown in the screenshot below, the website includes characteristics that help decide whether or not to buy access.



Headquarters:

Phone:

Website:

Employees:

Revenue: $

Popular Searches:

Fig. 22. Information about a company on zoominfo.com

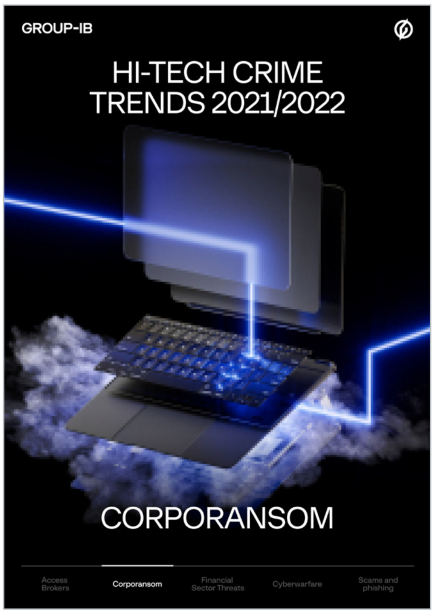
Since early 2020, the number of ransomware affiliate programs has increased significantly due to the pandemic, which has resulted in many companies having to change their infrastructure for employees to work remotely. Detailed information about the current ransomware trends can be found in the upcoming Group-IB report entitled **Corporansom**.

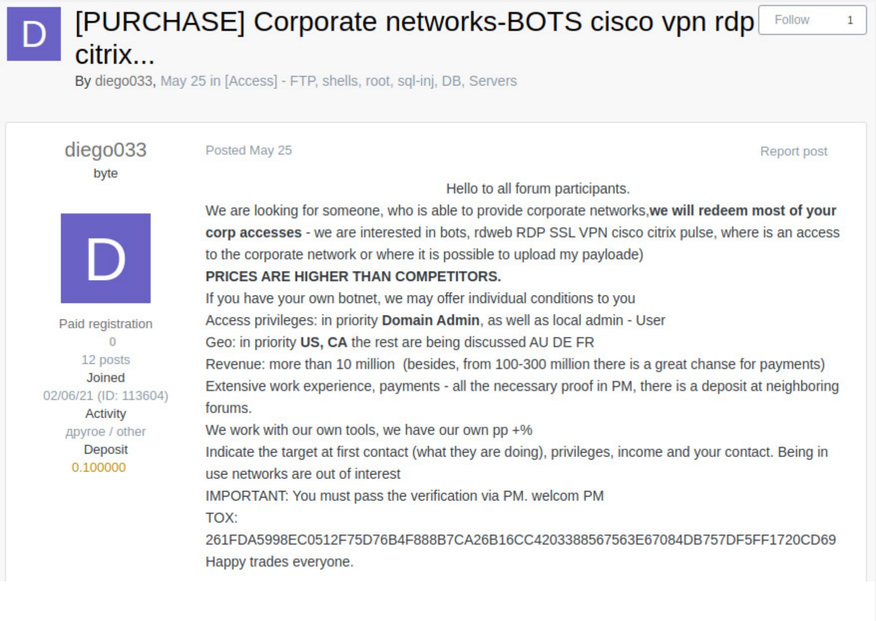
In many cases, deploying ransomware starts with establishing an RDP connection with a compromised server. Next, attackers move across the network to a domain controller. Publicly available RDP servers are the most common target for many ransomware operators, which in turn generates interest in sales of RDP access to corporate networks.

RDP access to servers is not the only entry point where ransomware operators apply brute force attacks. This method is also used against VPN services without multi-factor authentication.

As ransomware became more and more popular, the number of threat actors who sell access to corporate networks grew. This meant that ransomware operators and affiliate program participants no longer needed to search for vulnerabilities in infrastructures because they could simply purchase access to a network from a third party. Ads about buying access to networks became commonplace on underground forums.

Corporansom





D [PURCHASE] Corporate networks-BOTS cisco vpn rdp citrix...

By diego033, May 25 in [Access] - FTP, shells, root, sql-inj, DB, Servers

diego033
byte
D
Paid registration
0
12 posts
Joined
02/06/21 (ID: 113604)
Activity
другое / other
Deposit
0.100000

Posted May 25

Hello to all forum participants.

We are looking for someone, who is able to provide corporate networks,**we will redeem most of your corp accesses** - we are interested in bots, rdweb RDP SSL VPN cisco citrix pulse, where is an access to the corporate network or where it is possible to upload my payloade)

PRICES ARE HIGHER THAN COMPETITORS.

If you have your own botnet, we may offer individual conditions to you

Access privileges: in priority **Domain Admin**, as well as local admin - User

Geo: in priority **US, CA** the rest are being discussed AU DE FR

Revenue: more than 10 million (besides, from 100-300 million there is a great chanse for payments)

Extensive work experience, payments - all the necessary proof in PM, there is a deposit at neighboring forums.

We work with our own tools, we have our own pp +%

Indicate the target at first contact (what they are doing), privileges, income and your contact. Being in use networks are out of interest

IMPORTANT: You must pass the verification via PM. welcom PM

TOX:
261FDA5998EC0512F75D76B4F888B7CA26B16CC4203388567563E67084DB757DF5FF1720CD69

Happy trades everyone.

Fig. 23. A post about buying access on Exploit

The goal of ransomware operators is to extort ransoms in exchange for decrypting data. As such, in addition to encrypting data, their main goal is to destroy backup copies of critical information in order to ensure that victims cannot recover the data without paying the ransom. As a result, most ransomware can disable or delete system recovery features.

Many ransomware operators create dedicated leak sites (DLSs) where they periodically post compromised data as a way of intimidating their victims.

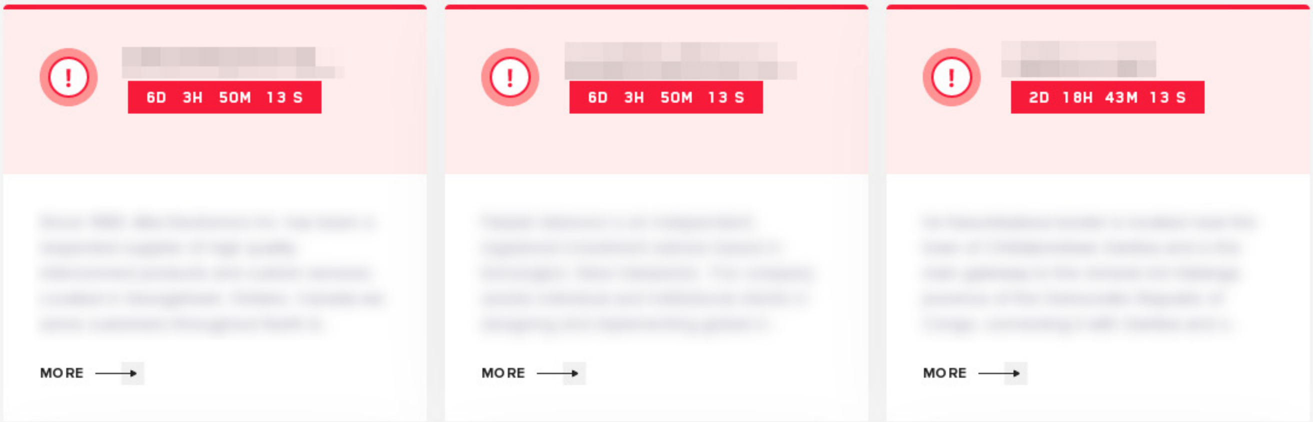


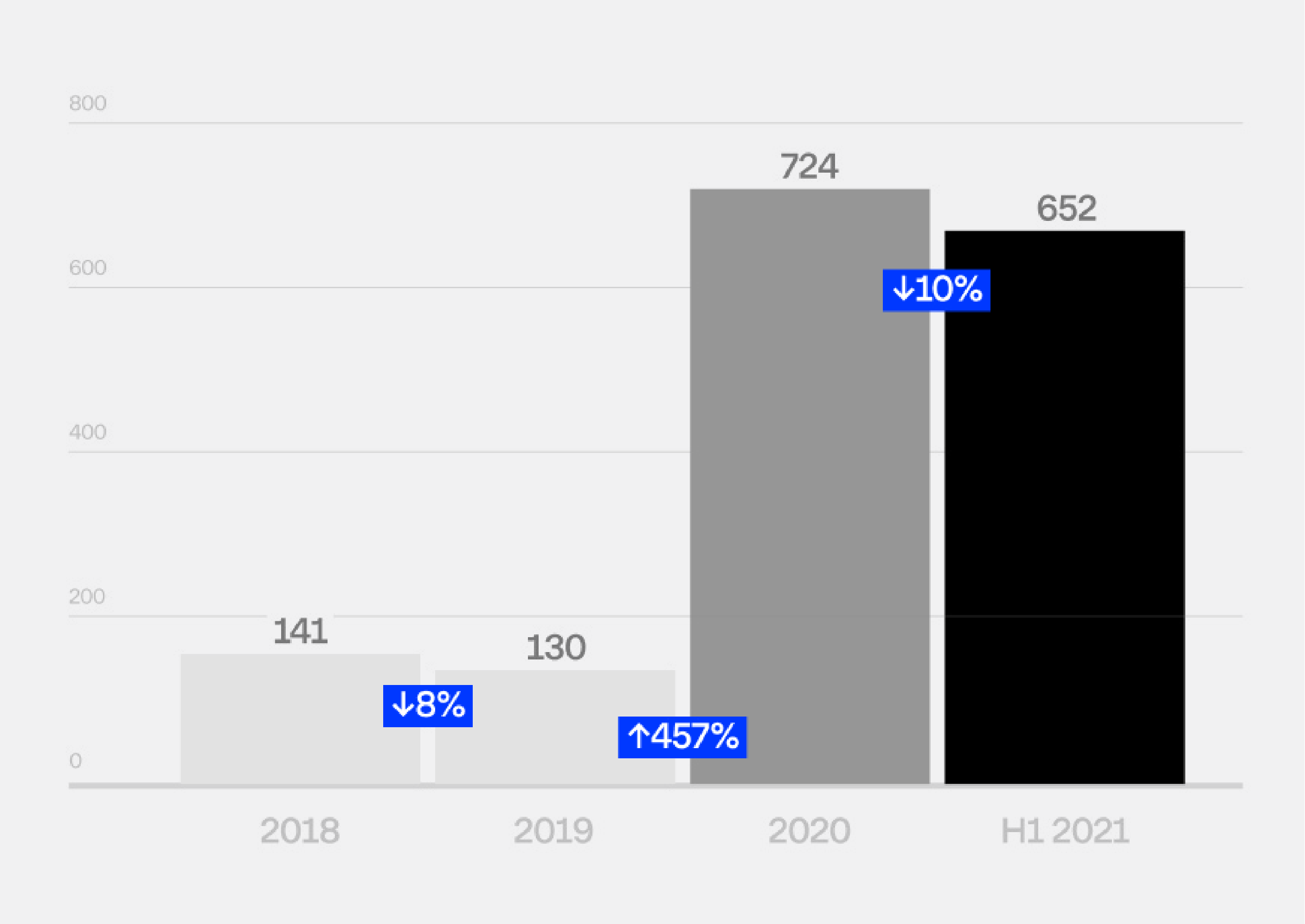
Fig. 24. A DLS of Lockbit ransomware operators

Since every group that operates ransomware can have several affiliates, threat actors who use the same ransomware can have different tactics, techniques and procedures. Group-IB conducted an in-depth analysis of ransomware and published a report called **Ransomware Uncovered 2020—2021** in March 2021. The report analyzes the main ransomware tactics and techniques and provides recommendations on how to prevent ransomware threats.

Affiliate programs have created demand for access to corporate networks, thereby motivating IABs to continue developing their activities.

A total of **1,647** offers to sell access were shared between early 2018 and mid-2021. Most (**1,099**) were made in the past year (H2 2020–H1 2021). Below are statistics for the number of access offers made since 2018.

Fig. 25. Graph of selling access

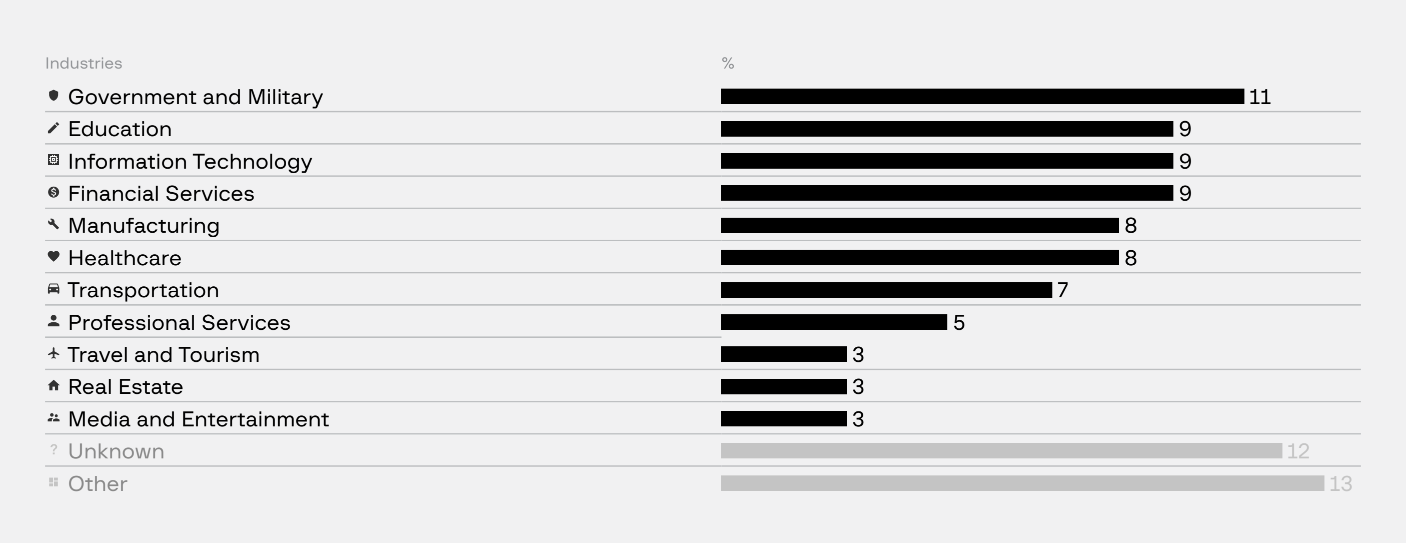


Fewer offers from Fxmsp and limited demand for initial access are two factors that slightly reduced sales in 2019 **(130 access offers)** compared to 2018 **(141 access offers)**. A year later, however, the number of access offers soared 5.5-fold **(724 access offers in 2020)**. The first half of 2021 saw slightly fewer offers on forums: **652**.

This section analyzes the market for initial access to corporate networks discovered on underground forums in the past two years.

Since the market emerged, virtually no major industry has been spared from having initial access sold on the black market.

The diagram below shows statistics for industries where unauthorized access was sold between the second half of 2019 and the first half of 2020.



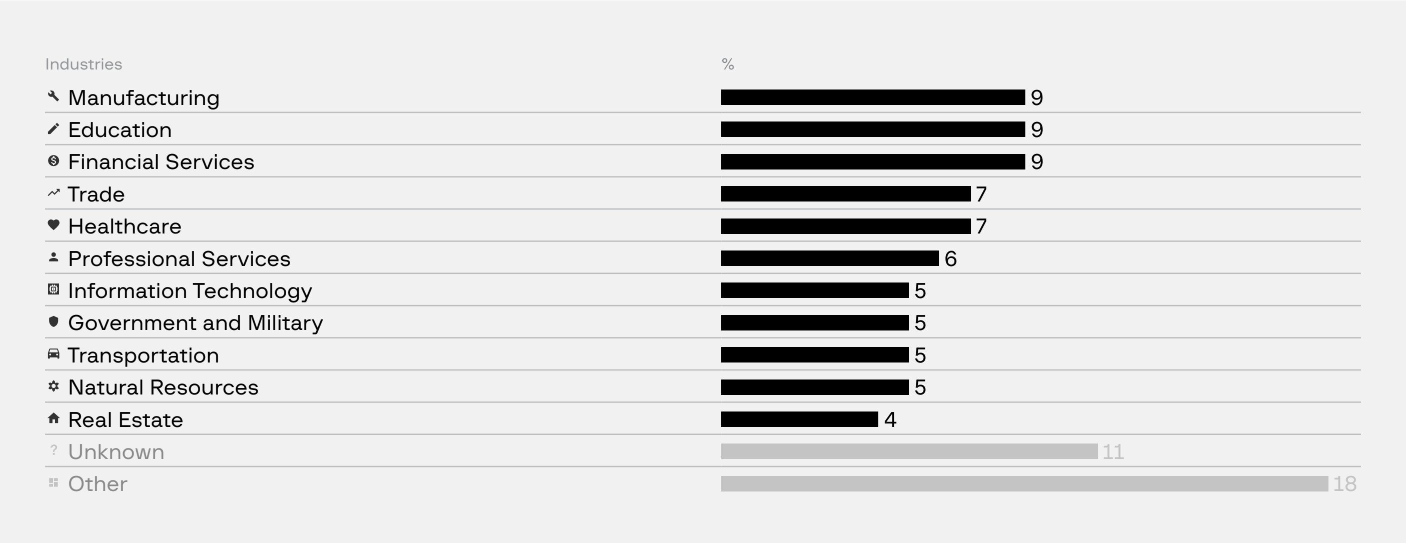
IABs share as little information as possible in their ads in order to generate interest among buyers and to avoid revealing identifying information about their victims. Often, they only publish information about a company's revenue and location. Industries are usually not specified or they are described in a way that reveals only whether the company is government-related or commercial. For this reason, 12% are in the “Unknown” category.

A similar figure applies to the “Other” category, which represents the total number of offers to sell access to companies from industries not shown in the diagram, with each accounting for no more than 2% of the total number of access offers between H2 2019 and H1 2020. These industries include charities as well as sports and gaming organizations.

Throughout this time, a total of **362 offers to sell access** were made, with government and military services comprising the industries with the most activity.

A year later, the situation changed markedly: the overall number of access offers between the second half of 2020 and the first half of 2021 amounted to **1,099,** which is nearly **three times more than during the previous period**.

Below are statistics for industries for which access offers were made between the second half of 2020 and the first half of 2021.



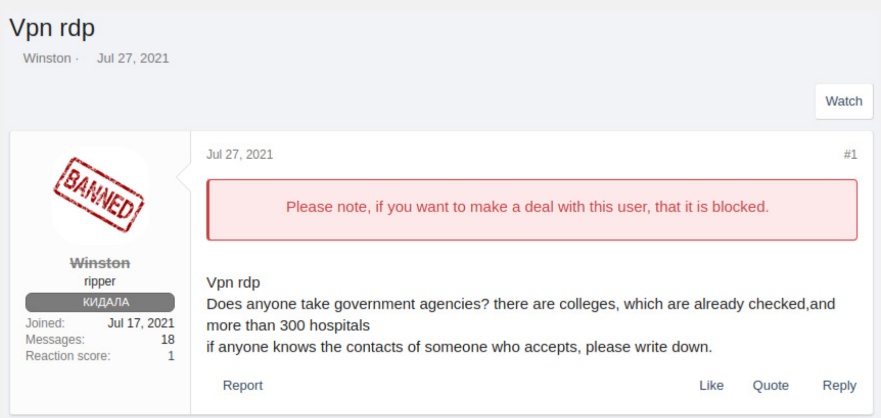
Manufacturing, **education**, and **financial services** are the leaders in the sale of unauthorized access. These three industries pushed the government and military sectors to fourth place. Due to an increase in the overall number of access offers, a decrease in a given industry's percentage does not mean that the total number of access offers related to it dropped. On the contrary, their number also increased.

The fact that the number of affected industries has expanded significantly shows that threat actors did not initially realize the full spectrum of potential victims. A year ago companies from 20 industries were affected. Now, the number is 35.

The situation also changed for attacked countries. The diagram below shows statistics for countries where the companies to which access was sold between H2 2019 and H1 2020 were registered.

Countries	%
US	33
France	5
UK	5
Italy	4
Canada	3
Australia	2
China	2
Other	23
Unknown	23

The United States ranked first, with the most companies attacked. However, a considerable percentage of access offers at the time could not be attributed to a specific country. A large percentage of access offers for which the victim's location is unknown, due to criminals publishing ads containing limited information. Below is an example of such an ad.



Vpn rdp

Winston · Jul 27, 2021

~~Winston~~
ripper
КИДАЛА
Joined: Jul 17, 2021
Messages: 18
Reaction score: 1

Jul 27, 2021 #1

Please note, if you want to make a deal with this user, that it is blocked.

Vpn rdp
Does anyone take government agencies? there are colleges, which are already checked,and more than 300 hospitals
if anyone knows the contacts of someone who accepts, please write down.

Fig. 26. A post about selling access to various organizations

It is difficult to include information from such offers in statistics, but we can assume that the victims in question are small, low-income organizations, considering that initial access to large organizations is usually sold separately and for a higher price.

Below are similar statistics for H2 2020 – H1 2021.

Countries	%
US	30
France	5
UK	4
Australia	4
Italy	3
India	3
Canada	3
Other	30
Unknown	18

The following year, the United States kept its leading position. Although its share has decreased, the overall increase in the total number of access offers does not point to a positive trend for the United States and other countries.

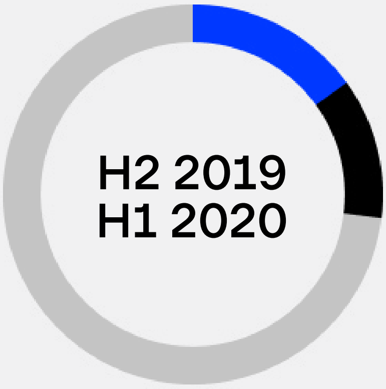
Notably, offers of access to companies in India have become some of the bestselling lots, surpassing China by several positions.

The number of countries in which unauthorized access can be gained has also increased: **68 countries** were attacked during H2 2020 – H1 2021 compared to just **42 countries** a year earlier.

There are also more cybercriminals actively selling access to corporate networks. Between **H2 2019** and **H1 2020**, Group-IB specialists identified **86 sellers**, and over the last year (H2 2020 – H1 2021) the number has grown to **262**, which is 3 times more than in the previous period. Among these, 229 are new brokers.

The diagram below shows statistics on cybercriminals who published ads for the sale of unauthorized access from the second half of 2019 to the first half of 2020.

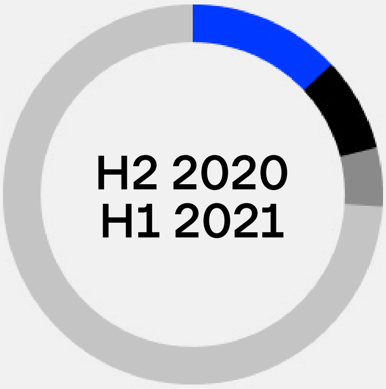
Threat actor	%
network	15
nanash	12
SHERIFF	6
Streetskip	5
B.Wanted	4
bc.monster	4
wazawaka (AKA m1x)	4
cryzaa	3
ellis.J.douglas	3
vasyldn	3
TrueFighter	2
Lannister	2
Other	37



During this period, the market leaders were sellers with the usernames **network** and **Nanash**, who were responsible for more than a quarter of all access offers.

Below are statistics for the current reporting period, between H2 2020 and H1 2021. The number of cybercriminals making single offers on the access market has increased significantly, which means there are more cybercriminals who want to earn extra money from this type of crime.

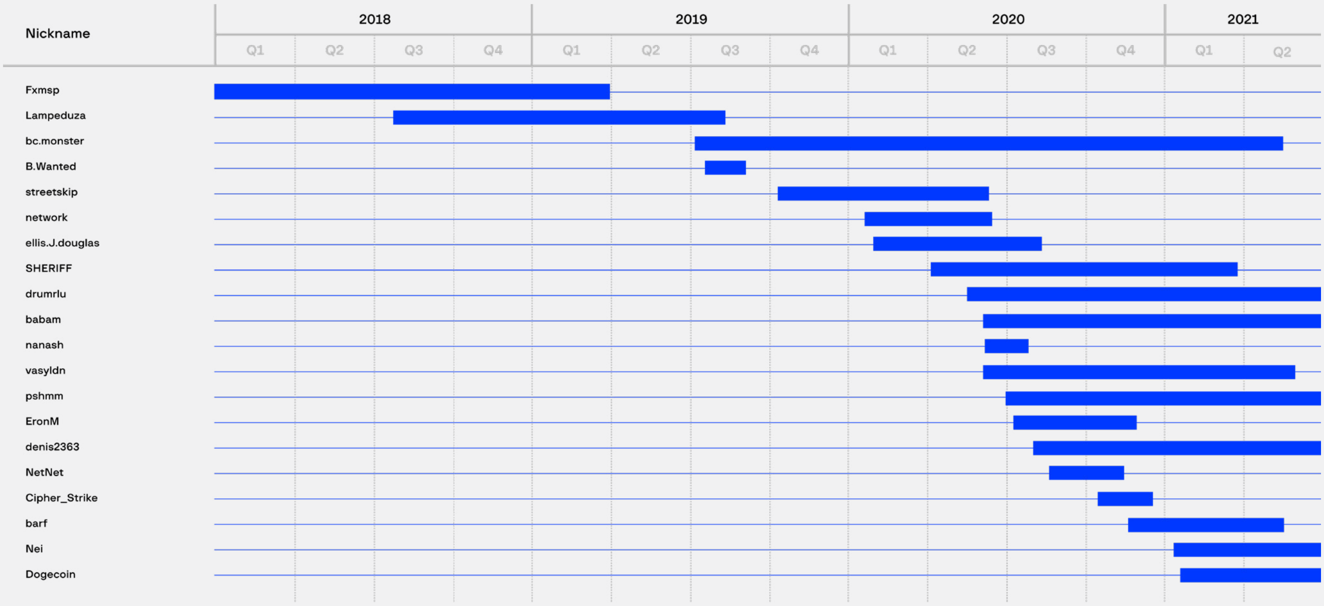
Threat actor	%
barf	13
pshmm	8
nei	5
vasyldn	4
DogeCoin	4
drumrlu	4
babam	3
denis2363	3
NetNet	2
EronM	2
Other	52



Only one criminal remained among the leaders in terms of access sales for two years in a row: an individual with the username **vasyldn**.

Between H2 2019 and H1 2020, **network** placed 54 access ads, which made him the leader among sellers. A year later **barf** took their place with 145 offers.

The diagram below shows the activity timeline of the main IABs from 2018 to the first half of 2021.



Size of the market for selling access to compromised networks

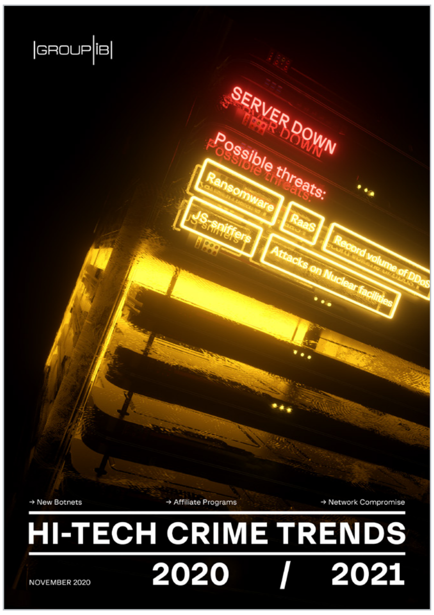
H2 2018 — H1 2019	H2 2019 — H1 2020	H2 2020 — H1 2021
$1,609,930	$6,189,388	$7,165,387
GLOBALLY	GLOBALLY	GLOBALLY

In last year's **Hi-Tech Crime Trends 2020/2021** report, which is available on Group-IB's website, Group-IB Threat Intelligence analysts estimated the total size of the market for selling access to corporate networks sold on dark web forums. The specialists concluded that the market size was increasing from year to year, but that "the peak of sales occurred in 2020." During that reporting period (H2 2020 – H1 2021), the number of offers on the market exceeded the peak of the previous period by almost three-fold. Group-IB specialists estimated the total market size in the current period at **$7,165,387**, which is 16% more than in the previous period (H2 2019 – H1 2020), when the market size was **$6,189,388**.

Group-IB experts also analyzed regional statistics. It is important to reiterate that we were unable to attribute some companies to specific countries, which is why the actual number of victims in each region may differ.

As can be seen below, the largest market share was estimated for instances of access to companies based in **APAC** countries. Between H2 2020 and H1 2021, the total cost of access was **$3,307,210**, which is almost six times more than in the previous year. The largest number of access offers in APAC countries during the above period was in **Australia (36%)**, followed by **India (23%)** and **China (14%)**.

Hi-Tech Crime Trends 2020/2021



H2 2020 — H1 2021 MARKET VOLUME APAC

$3,307,210

Countries	Number of accesses, %
Australia	36
India	23
China	14
Thailand	8
Singapore	4
Japan	4
Malaysia	2
Philipines	2
Taiwan	2
South Korea	2
Other	3

H2 2019 — H1 2020 MARKET VOLUME APAC

$453,497

H2 2018 — H1 2019 MARKET VOLUME APAC

$223,050

Countries in the Americas ranked second in terms of access market size, which accounted for **$1,377,552**, just under half as much as in H2 2019 - H1 2020, when the market amounted to more than **$3 million**. The United States ranked first among American countries, accounting for **76%** of all offers.

H2 2020 — H1 2021 MARKET VOLUME

AMERICAS

$1,377,552

Countries	Number of accesses, %
US	76
Canada	7
Brazil	6
Mexico	3
Argentina	2
Colombia	2
Other	4

H2 2019 — H1 2020 MARKET VOLUME
AMERICAS

$3,300,601

H2 2018 — H1 2019 MARKET VOLUME
AMERICAS

$647,400

For **European countries**, the peak occurred in the previous period and amounted to **$753,598**, which is 25% more than between H2 2020 and H1 2021 (**$590,095)**. The leading positions in this region are occupied by **France** and **Great Britain**, which gained **20%** and **18%** of the total, respectively. **Italy** ranked third **(13%)**, and each of the remaining countries account for no more than 10% of the total number of access offers.

H2 2020 — H1 2021 MARKET VOLUME

EUROPE

$590,095

Countries	Number of accesses, %
France	20
UK	18
Italy	13
Spain	10
Germany	9
Netherlands	5
Portugal	4
Switzerland	3
Belgium	3
Sweden	3
Other	12

H2 2019 — H1 2020 MARKET VOLUME
EUROPE

$753,598

H2 2018 — H1 2019 MARKET VOLUME
EUROPE

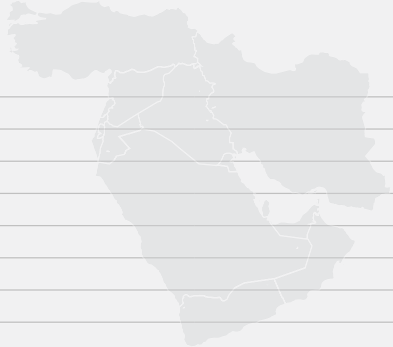
$408,700

As for **the Middle East**, in contrast to Europe, the market increased by 1.5 times as compared to the previous reporting period. The undisputed leader in this region is **the UAE**, with **24%** of the total number of access offers. Next are **Turkey** and **Israel**, each with **14%** and **13%** respectively and finally **Saudi Arabia** and **Iran** with **12%** a piece of all access ads in the region.

H2 2020 — H1 2021 MARKET VOLUME

MIDDLE EAST

$247,836



Countries	Number of accesses, %
UAE	24
Israel	14
Turkey	13
Saudi Arabia	12
Iran	12
Kuwait	11
Egypt	5
Qatar	5
Other	4

H2 2019 — H1 2020 MARKET VOLUME
MIDDLE EAST

$180,538

H2 2018 — H1 2019 MARKET VOLUME
MIDDLE EAST

$101,100

Among **African** countries, we observed less interest in access offers. Compared to the previous year, the market fell to **$120,290**. Between H2 2020 and H1 2021, two countries held the leading position in this region: **South Africa** and **Egypt**, whose shares in sum accounted for almost **50%** each of the total number of access sales in Africa. In addition to that, **23%** were ads in which the location was indicated as Africa, but the country was not explicitly stated. The share of each remaining country was no more than **6%**.

H2 2020 — H1 2021 MARKET VOLUME

AFRICA

$120,290

Countries	Number of accesses, %
South Africa	24
Egypt	23
Africa	20
Algeria	6
Nigeria	6
Sierra Leone	6
Libya	6
Other	23

H2 2019 — H1 2020 MARKET VOLUME
AFRICA

$135,188

H2 2018 — H1 2019 MARKET VOLUME
AFRICA

$167,500

In **CIS countries (the Commonwealth of Independent States)**, the market peak occurred in H2 2019 – H1 2020 and amounted to **$142,058**, while in H2 2020 – H1 2021 the market size was almost three times less **($48,239)**. In the most recent period, Russia held the main access market share at **76%**. It is noteworthy that almost all of the brokers identified are Russian-speaking and that they tend to refrain from attacking organizations in the CIS region, which makes it the least often attacked of the regions discussed.

H2 2020 — H1 2021 MARKET VOLUME CIS

$48,239

Countries	Number of accesses, %
Russia	76
Azerbaijan	12
Armenia	12

H2 2019 — H1 2020 MARKET VOLUME CIS

$142,058

H2 2018 — H1 2019 MARKET VOLUME CIS

$8,250

Given that offers published on underground forums hide various information (including the cost of access to a particular company) more and more often, it has become difficult to estimate the total market size. In addition, many transactions are carried out privately. However, Group-IB's technologies for analyzing information on underground forums (including deleted entries and information hidden by cybercriminals) help measure the dynamics and scale of sales of such "goods" on the dark web.

MOST WANTED: THE TEN MOST ACTIVE SELLERS OF ACCESS CREDENTIALS

08

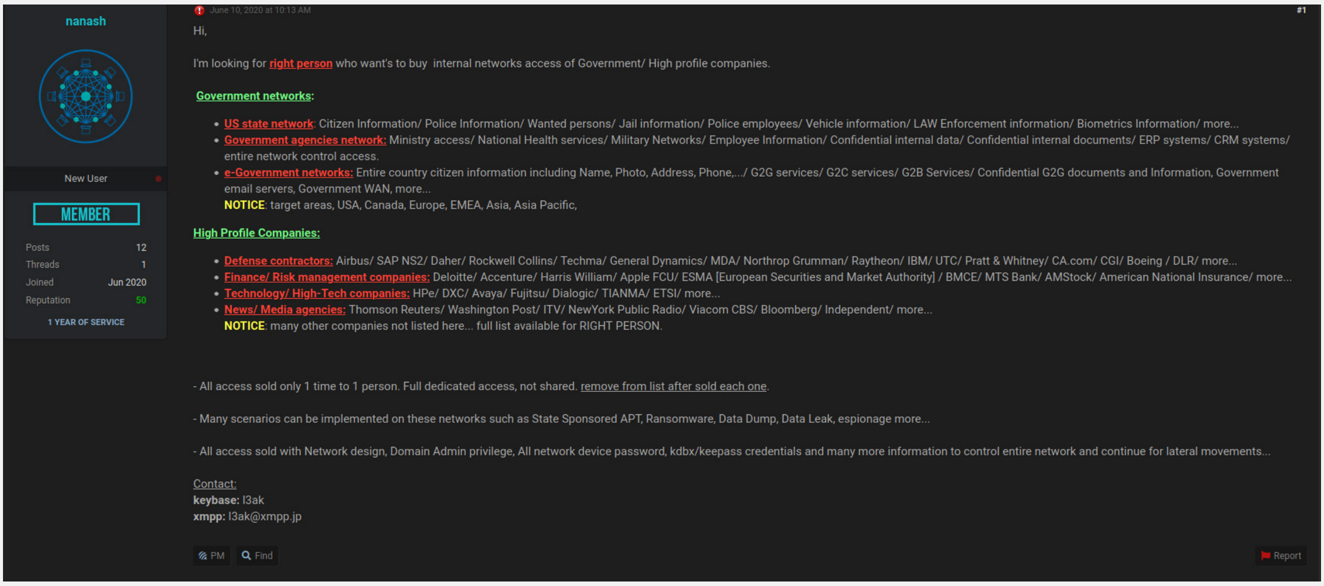
This section takes a close look at the ten sellers who offered the most initial access credentials for sale during the period under review.

Nanash

Active	**June 2020 — July 2020**
Number of victims	**40+ companies**
Attack geography	**11 countries**
Estimated earnings	**$5,000,000**

Nanash created an account on RaidForums, an underground forum, on June 10, 2020. That same day, Nanash started a for-sale thread offering access to corporate networks belonging to more than **40 companies** and government agencies worldwide. The account was last active in July 2020. In the subject line of their original message, Nanash included a short description of the companies and organizations to which they claimed to have access.

Fig. 27. Nanash's original Raidforums post



nanash

New User

MEMBER

Posts 12

Threads 1

Joined Jun 2020

Reputation 50

1 YEAR OF SERVICE

June 10, 2020 at 10:13 AM

#1

Hi,

I'm looking for right person who want's to buy internal networks access of Government/ High profile companies.

Government networks:

- US state network: Citizen Information/ Police Information/ Wanted persons/ Jail information/ Police employees/ Vehicle information/ LAW Enforcement information/ Biometrics Information/ more...
- Government agencies network: Ministry access/ National Health services/ Military Networks/ Employee Information/ Confidential internal data/ Confidential internal documents/ ERP systems/ CRM systems/ entire network control access.
- e-Government networks: Entire country citizen information including Name, Photo, Address, Phone,.../ G2G services/ G2C services/ G2B Services/ Confidential G2G documents and Information, Government email servers, Government WAN, more...
  NOTICE: target areas, USA, Canada, Europe, EMEA, Asia, Asia Pacific,

High Profile Companies:

- Defense contractors: Airbus/ SAP NS2/ Daher/ Rockwell Collins/ Techma/ General Dynamics/ MDA/ Northrop Grumman/ Raytheon/ IBM/ UTC/ Pratt & Whitney/ CA.com/ CGI/ Boeing / DLR/ more...
- Finance/ Risk management companies: Deloitte/ Accenture/ Harris William/ Apple FCU/ ESMA [European Securities and Market Authority] / BMCE/ MTS Bank/ AMStock/ American National Insurance/ more...
- Technology/ High-Tech companies: HPe/ DXC/ Avaya/ Fujitsu/ Dialogic/ TIANMA/ ETSI/ more...
- News/ Media agencies: Thomson Reuters/ Washington Post/ ITV/ NewYork Public Radio/ Viacom CBS/ Bloomberg/ Independent/ more...
  NOTICE: many other companies not listed here... full list available for RIGHT PERSON.

- All access sold only 1 time to 1 person. Full dedicated access, not shared. remove from list after sold each one.

- Many scenarios can be implemented on these networks such as State Sponsored APT, Ransomware, Data Dump, Data Leak, espionage more...

- All access sold with Network design, Domain Admin privilege, All network device password, kdbx/keepass credentials and many more information to control entire network and continue for lateral movements...

Contact:
keybase: l3ak
xmpp: l3ak@xmpp.jp

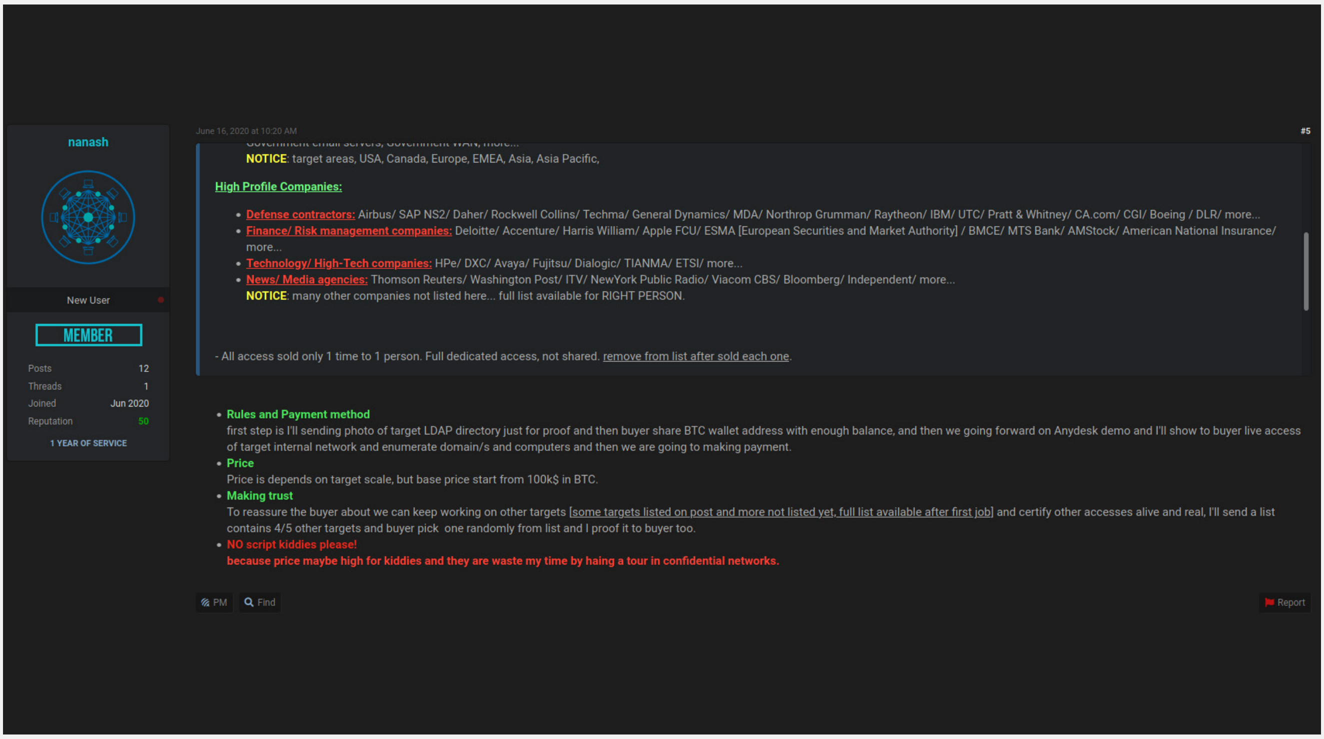
The criminal's message implied that they had access credentials for government agencies in **North America**, **Europe**, **the Middle East**, **Africa**, **and Asia Pacific**, but Nanash did not specify the names of most. In addition to government organizations, among their alleged victims Nanash listed private companies such as **Northrop Grumman**, **Airbus**, **Raytheon**, **Boeing**, **Deloitte**, **Accenture, HPE**, **Thomson Reuters,** and **The Washington Post**.

Nanash caused a mixed reaction from forum denizens: some expressed interest in the offerings, while others treated the newcomer with suspicion. However, Group-IB researchers discovered that the hacker had gained access to at least two companies, which was corroborated by the screenshots the criminal shared and by real-time LDAP preview logs.

After chatting with several forum members, Nanash quoted **11 BTC ($100,000)** for each set of access credentials. The criminal also insisted that they would sell access credentials to one buyer only, noting that they would share the full list of victims only with a trusted buyer. The hacker said that they expected the prospective buyer to pay 5 BTC upfront to "reserve the transaction," then pay the rest to get the full access data.

Based on the full list of access credentials for sale, and given the quoted price per set of access data, we estimate that the criminal could have potentially made at least **$5 million** from the sale.

Fig. 28. Nanash's comment about their price for access data



Government email servers, Government WAN, more...
NOTICE: target areas, USA, Canada, Europe, EMEA, Asia, Asia Pacific,

High Profile Companies:

- **Defense contractors:** Airbus/ SAP NS2/ Daher/ Rockwell Collins/ Techma/ General Dynamics/ MDA/ Northrop Grumman/ Raytheon/ IBM/ UTC/ Pratt & Whitney/ CA.com/ CGI/ Boeing / DLR/ more...
- **Finance/ Risk management companies:** Deloitte/ Accenture/ Harris William/ Apple FCU/ ESMA [European Securities and Market Authority] / BMCE/ MTS Bank/ AMStock/ American National Insurance/ more...
- **Technology/ High-Tech companies:** HPe/ DXC/ Avaya/ Fujitsu/ Dialogic/ TIANMA/ ETSI/ more...
- **News/ Media agencies:** Thomson Reuters/ Washington Post/ ITV/ NewYork Public Radio/ Viacom CBS/ Bloomberg/ Independent/ more...
NOTICE: many other companies not listed here... full list available for RIGHT PERSON.

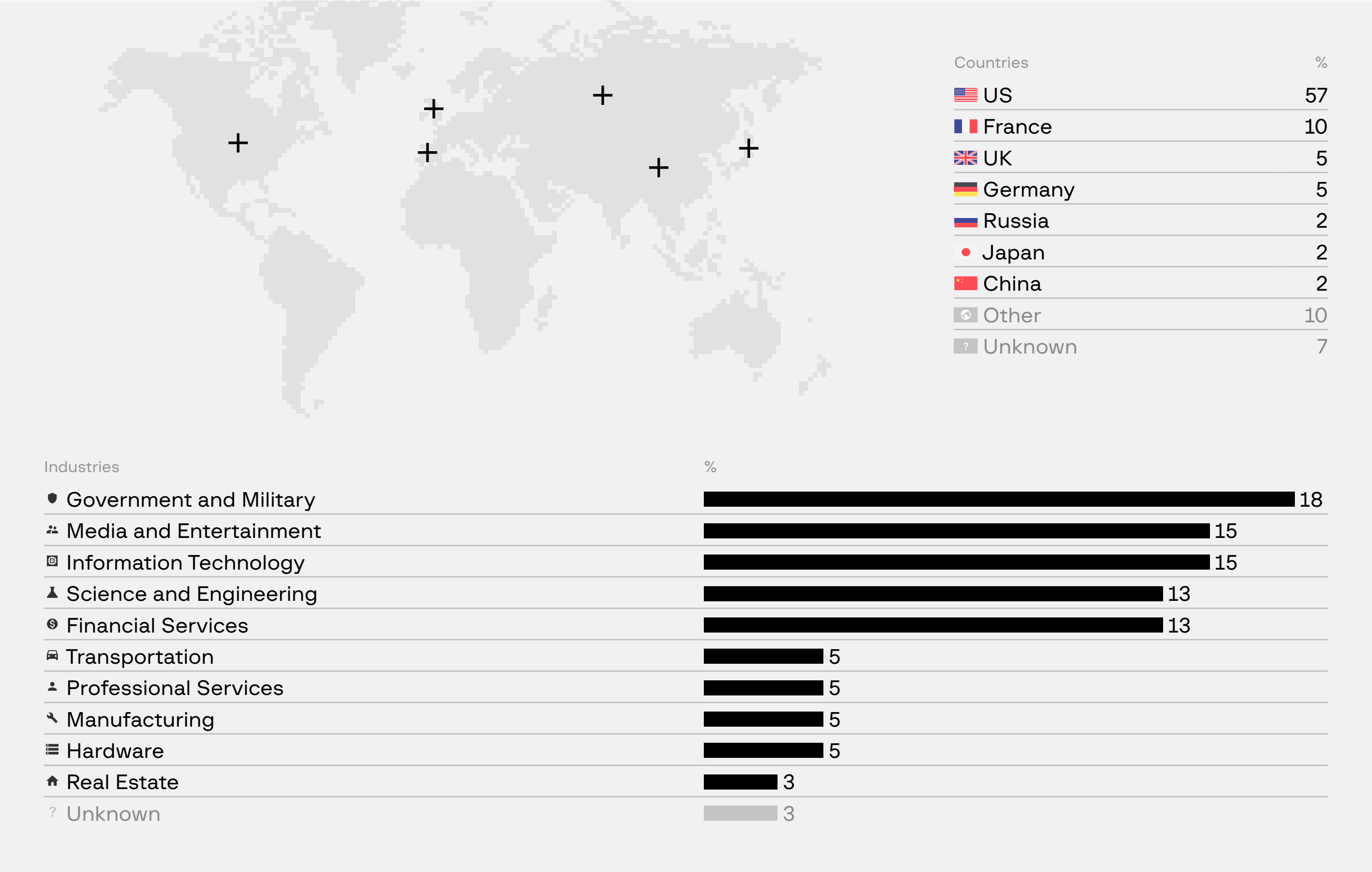
- All access sold only 1 time to 1 person. Full dedicated access, not shared. remove from list after sold each one.

- **Rules and Payment method**
first step is I'll sending photo of target LDAP directory just for proof and then buyer share BTC wallet address with enough balance, and then we going forward on Anydesk demo and I'll show to buyer live access of target internal network and enumerate domain/s and computers and then we are going to making payment.
- **Price**
Price is depends on target scale, but base price start from 100k$ in BTC.
- **Making trust**
To reassure the buyer about we can keep working on other targets [some targets listed on post and more not listed yet, full list available after first job] and certify other accesses alive and real, I'll send a list contains 4/5 other targets and buyer pick one randomly from list and I proof it to buyer too.
- **NO script kiddies please!**
because price maybe high for kiddies and they are waste my time by haing a tour in confidential networks.

What happened to Nanash after they posted their ad remains a mystery to this day. It is still unclear how many sets of access credentials they managed to sell, assuming that they actually had them in their possession. After this, the criminal disappeared from the forum.

A couple of months after Nanash was last seen on Raidforums, **ClearSkySec** researchers **published** a study on the Pay2Key ransomware campaign operated by the Iranian APT group best known as Fox Kitten. The researchers also connected a user known as **kharpedar** to Fox Kitten based on their posts on underground forums. ClearSkySec wrote in the report that kharpedar was selling access to many companies whose description seemed to match those that Nanash was offering for sale, expressing interest in Turkish organizations and showing no interest in the Indian government.

The diagram below presents the statistics relating to the home countries and industries of Nanash's victims.



Countries	%
US	57
France	10
UK	5
Germany	5
Russia	2
Japan	2
China	2
Other	10
Unknown	7

Industries	%
Government and Military	18
Media and Entertainment	15
Information Technology	15
Science and Engineering	13
Financial Services	13
Transportation	5
Professional Services	5
Manufacturing	5
Hardware	5
Real Estate	3
Unknown	3

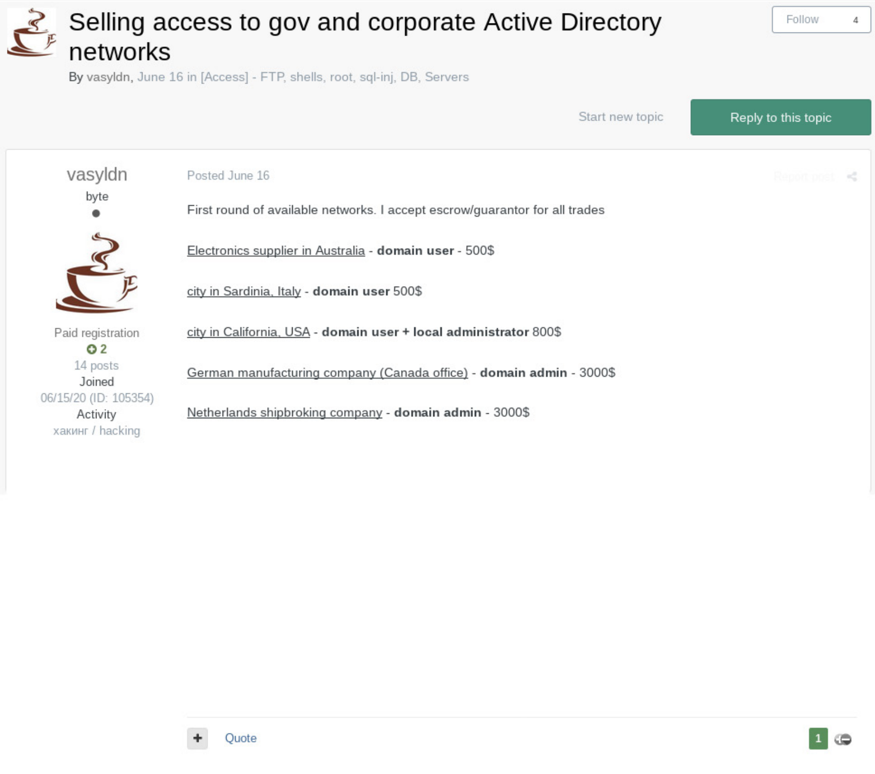
ATT&CK Matrix for Enterprise (Nanash)

TACTICS	TECHNIQUES	DETAILS
Discovery	Account Discovery: Domain Account (T1087.002)	The criminal provided an LDAP screenshot showing information about users of corporate network domains.
	Permission Groups Discovery: Domain Groups (T1069.002)	The criminal provided an LDAP screenshot showing information about corporate network domains.

Vasyldn

Active	**June 2020 — May 2021**
Number of victims	**50+ companies**
Attack geography	**14 countries**
Estimated earnings	**$360,000**

On June 15, 2020, a user named **vasyldn** created an account on the forum Exploit and immediately started a thread on selling access to Active Directory networks belonging to companies and government organizations, thereby starting their campaign to sell access to more than **50 organizations** across **14 countries**. Vasyldn was last seen posting on the forum in May 2021, and went silent after that.



Selling access to gov and corporate Active Directory networks

By vasyldn, June 16 in [Access] - FTP, shells, root, sql-inj, DB, Servers

vasyldn
byte
Paid registration
2
14 posts
Joined
06/15/20 (ID: 105354)
Activity
хакинг / hacking

Posted June 16

First round of available networks. I accept escrow/guarantor for all trades

Electronics supplier in Australia - **domain user** - 500$

city in Sardinia, Italy - **domain user** 500$

city in California, USA - **domain user + local administrator** 800$

German manufacturing company (Canada office) - **domain admin** - 3000$

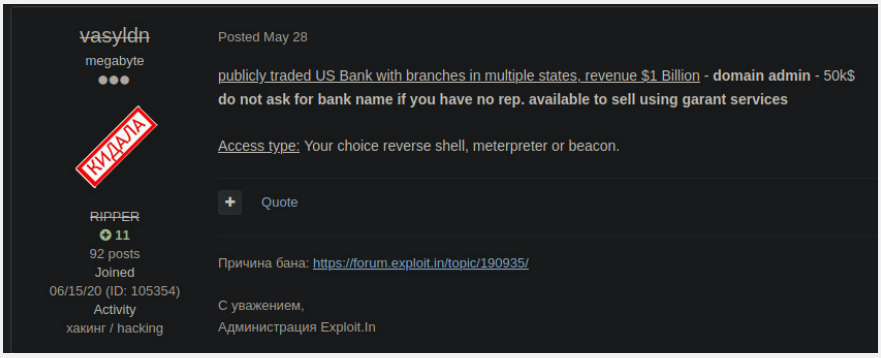
Netherlands shipbroking company - **domain admin** - 3000$

Fig. 29. Vasyldn's original post

In their first post, vasyldn advertised access to Active Directory networks belonging to five entities based in **the US**, **Italy**, **Canada**, **Australia**, and **the Netherlands**. The victims included an Australian electronics supplier, a Dutch ship broker, and a German manufacturing company, as well as infrastructure elements in unnamed cities in Sardinia and California.

Vasyldn actively promoted access credentials for sale until as late as October 2020. During this time the criminal compromised 23 companies, the access credentials for some of which were sold soon after the hacker posted the ads. After a six-month hiatus, vasyldn returned to selling access data. From March 2021, the criminal posted about 30 more ads.

Among others, the criminal's posts advertised data belonging to six companies based in different US states, including a major US bank with $1 billion in revenue.



~~vasyldn~~
megabyte
●●●

КИДАЛА

~~RIPPER~~
⊕ 11
92 posts
Joined
06/15/20 (ID: 105354)
Activity
хакинг / hacking

Posted May 28

publicly traded US Bank with branches in multiple states, revenue $1 Billion - **domain admin** - 50k$
do not ask for bank name if you have no rep. available to sell using garant services

Access type: Your choice reverse shell, meterpreter or beacon.

Причина бана: https://forum.exploit.in/topic/190935/

С уважением,
Администрация Exploit.In

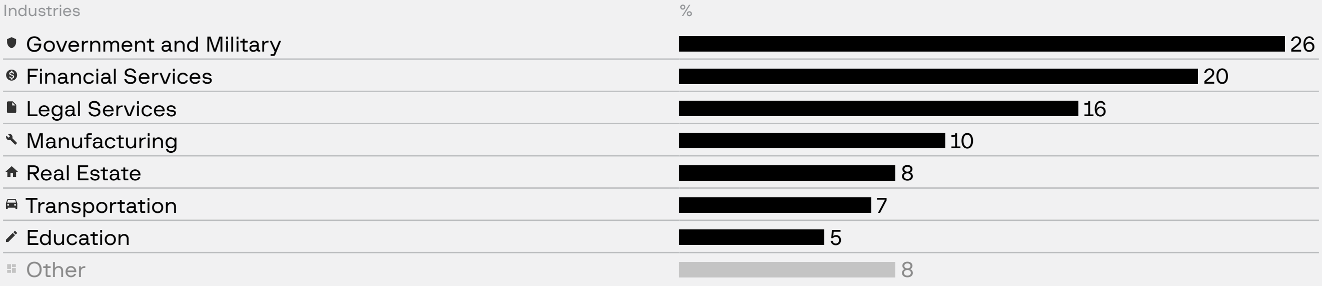
Fig. 30. Vasyldn's post advertising a bank's access data for sale

It is not entirely clear how vasyldn gained access to the corporate networks. What we do know is that the criminal used current domain admin account data to gain initial access.

An analysis of the hacker's activity revealed that vasyldn used Cobalt Strike to achieve persistence in networks, as well as alternative authentication methods (including pass-the-ticket and golden tickets) to move laterally across the network. In one of their posts, the attacker explicitly said that they had used ransomware within an unspecified network.

The chart below shows that vasyldn attacked companies mainly in the US, the UK, and Canada.

Countries	%
US	53
UK	10
Canada	7
Israel	7
Mexico	6
Italy	3
Switzerland	3
Other	12



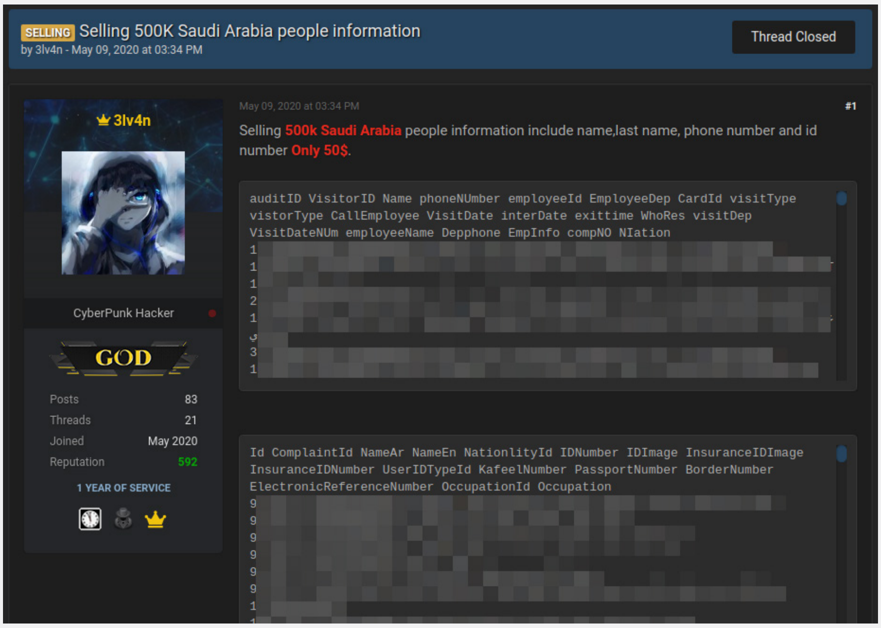
ATT&CK Matrix for Enterprise (vasyldn)

TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	The threat actor relied on RDP, VPN, and SSH to access corporate networks.
Execution	Command and Scripting Interpreter (T1059)	The threat actor indicated that they could provide access via Meterpreter and a reverse shell.
Credential access	Steal or Forge Kerberos Tickets: Golden Ticket (T1558.001)	The threat actor posted an ad claiming they were selling access with a Kerberos Golden Ticket (krbtgt) hash.
Discovery	Account Discovery (T1087)	The threat actor provided information about the number of hosts on the victim's network.
Command and Control	Ingress Tool Transfer (T1105)	The threat actor could have used Meterpreter or CSB to install a RAT on a victim's PC.
Impact	Data Encrypted for Impact (T1486)	The threat actor used encryption ransomware.

Drumrlu

Active	**May 2020 — present**
Number of victims	**50 companies**
Attack geography	**22 countries**
Estimated earnings	**$180,000**

Drumrlu, also known as **3lv4n**, is a database supplier and broker of initial access who is thought to be based in Turkey. Drumrlu was first seen on dark-web forums in May 2020. The threat actor started out by selling a database of private data relating to 500,000 Saudi nationals.



SELLING Selling 500K Saudi Arabia people information
by 3lv4n - May 09, 2020 at 03:34 PM

Thread Closed

3lv4n
CyberPunk Hacker
GOD

Posts	83
Threads	21
Joined	May 2020
Reputation	592

1 YEAR OF SERVICE

May 09, 2020 at 03:34 PM #1

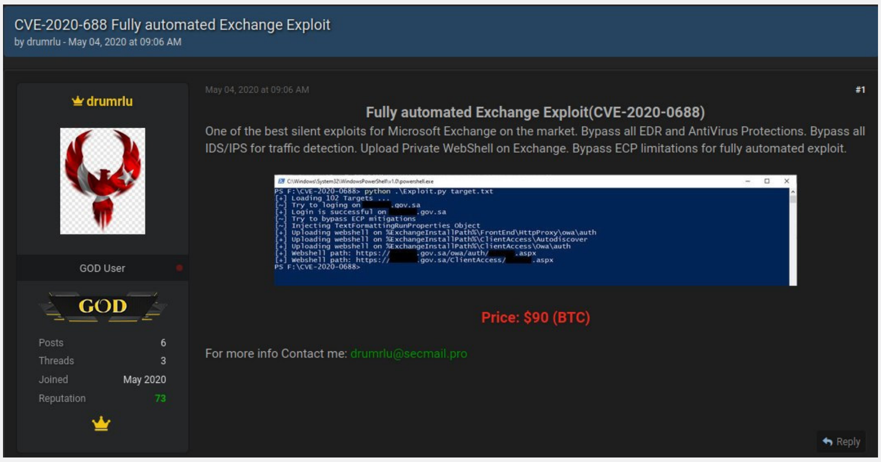
Selling 500k Saudi Arabia people information include name,last name, phone number and id number Only 50$.

```
auditID VisitorID Name phoneNUmber employeeId EmployeeDep CardId visitType
vistorType CallEmployee VisitDate interDate exittime WhoRes visitDep
VisitDateNUm employeeName Depphone EmpInfo compNO NIation
[redacted]
```

```
Id ComplaintId NameAr NameEn NationlityId IDNumber IDImage InsuranceIDImage
InsuranceIDNumber UserIDTypeId KafeelNumber PassportNumber BorderNumber
ElectronicReferenceNumber OccupationId Occupation
[redacted]
```

Fig. 31. Drumrlu's post advertising a database for sale

In addition to selling personal data, Drumrlu was seen on forums discussing vulnerabilities with other users. For example, Drumrlu suggested that someone should look into CVE-2018-14847, a critical WinBox vulnerability giving read and write access to random files due to a directory traversal vulnerability in the WinBox interface, which can be used to compromise an ISP. The threat actor also attempted to sell an exploit for the remote code execution vulnerability CVE-2020-0688 in Microsoft Exchange servers.



CVE-2020-688 Fully automated Exchange Exploit
by drumrlu - May 04, 2020 at 09:06 AM

drumrlu
GOD User
GOD

Posts	6
Threads	3
Joined	May 2020
Reputation	73

May 04, 2020 at 09:06 AM #1

Fully automated Exchange Exploit(CVE-2020-0688)

One of the best silent exploits for Microsoft Exchange on the market. Bypass all EDR and AntiVirus Protections. Bypass all IDS/IPS for traffic detection. Upload Private WebShell on Exchange. Bypass ECP limitations for fully automated exploit.

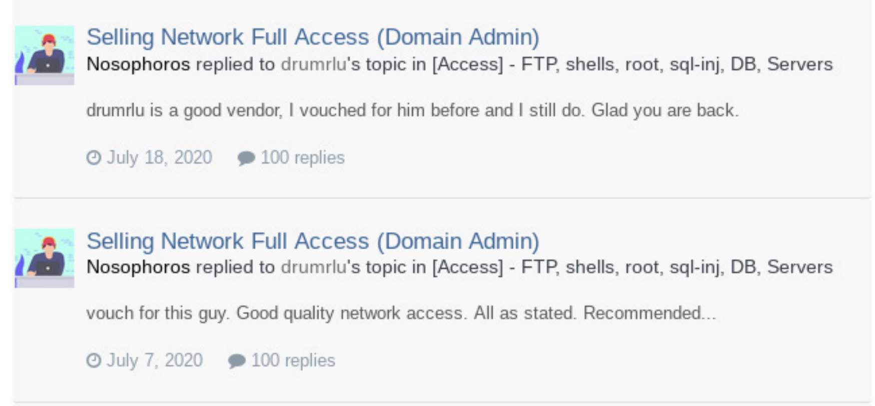
```
PS F:\CVE-2020-0688> python .\Exploit.py target.txt
[+] Loading 102 Targets ...
[~] Try to loging on [redacted].gov.sa
[+] Login is successful on [redacted].gov.sa
[~] Try to bypass ECP mitigations
[~] Injecting TextFormattingRunProperties Object
[+] Uploading webshell on %ExchangeInstallPath%\FrontEnd\HttpProxy\owa\auth
[+] Uploading webshell on %ExchangeInstallPath%\ClientAccess\Autodiscover
[+] Uploading webshell on %ExchangeInstallPath%\ClientAccess\Owa\auth
[+] Webshell path: https://[redacted].gov.sa/owa/auth/[redacted].aspx
[+] Webshell path: https://[redacted].gov.sa/ClientAccess/[redacted].aspx
PS F:\CVE-2020-0688>
```

Price: $90 (BTC)

For more info Contact me: drumrlu@secmail.pro

Fig. 32. Drumrlu's post offering an exploit for sale

Drumrlu has also likely worked with Nosophoros, the developer of Thanos. The two forum users have been seen praising each other's work on several occasions.



Selling Network Full Access (Domain Admin)
Nosophoros replied to drumrlu's topic in [Access] - FTP, shells, root, sql-inj, DB, Servers

drumrlu is a good vendor, I vouched for him before and I still do. Glad you are back.

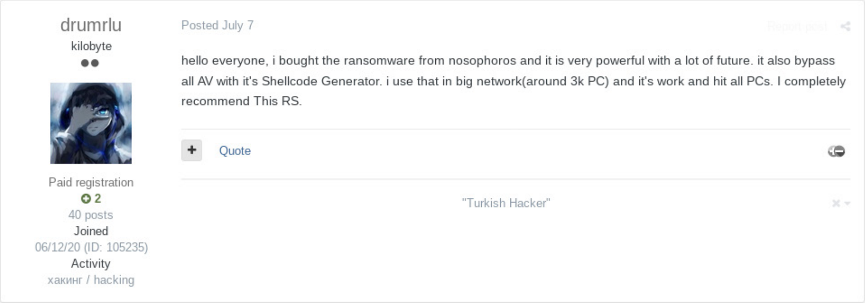
July 18, 2020 100 replies

Selling Network Full Access (Domain Admin)
Nosophoros replied to drumrlu's topic in [Access] - FTP, shells, root, sql-inj, DB, Servers

vouch for this guy. Good quality network access. All as stated. Recommended...

July 7, 2020 100 replies

Fig. 33. Comments by Nosophoros on working with Drumrlu



drumrlu
kilobyte
●●
Paid registration
2
40 posts
Joined
06/12/20 (ID: 105235)
Activity
хакинг / hacking

Posted July 7

hello everyone, i bought the ransomware from nosophoros and it is very powerful with a lot of future. it also bypass all AV with it's Shellcode Generator. i use that in big network(around 3k PC) and it's work and hit all PCs. I completely recommend This RS.

"Turkish Hacker"

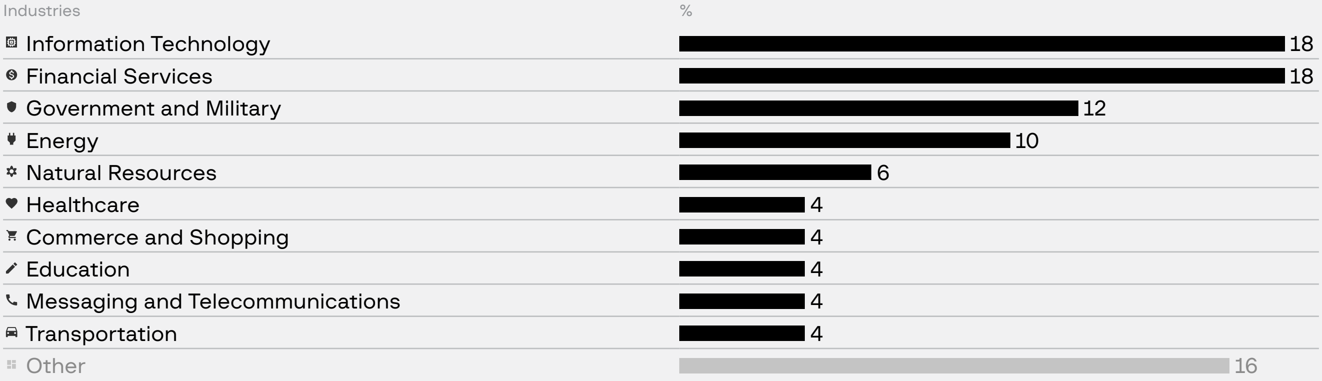
Fig. 34. Drumrlu's comment on working with Nosophoros

Drumrlu's use of ransomware is further corroborated by a team of researchers at **Intel 471**, who published a report stating that the hacker was presumably working for the Iranian government. According to the report, ransomware was deployed at several organizations a few months after the comment above was posted. Research findings indicate that the TTPs used by Drumrlu are similar to those used by MuddyWater, an APT group that works for the Iranian government.

Drumrlu obtains data using various methods. Group-IB has identified some of them based on the threat actor's posts, in which the criminal claims to have obtained data either by using malware or directly from the victim's network. In their earlier for-sale posts, Drumrlu mainly offered access to ESXi and AD servers. Based on Drumrlu's price quotes, the threat actor could have made approximately **$180,000**.

The chart below shows that most of Drumrlu's victims are based in the US, the UAE, and Saudi Arabia.

Countries	%
US	20
UAE	8
Saudi Arabia	8
Italy	6
Thailand	6
Jordan	4
India	4
Canada	4
Turkey	2
China	2
Unknown	12
Other	22



ATT&CK Matrix for Enterprise (drumrlu)

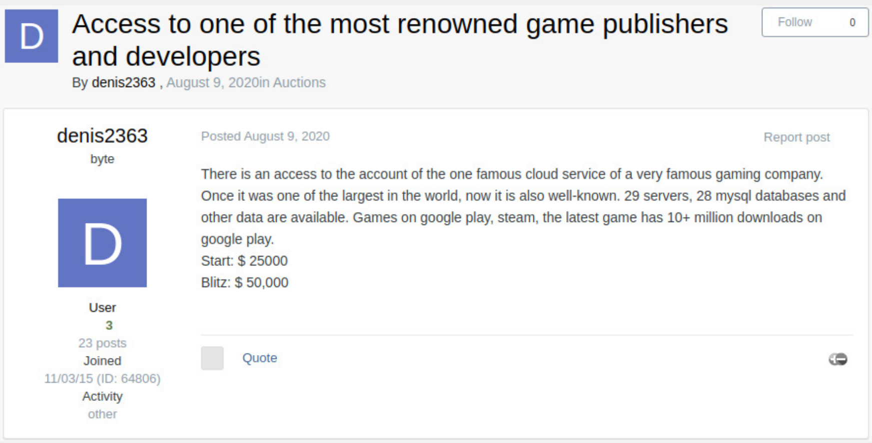
TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	The threat actor used VPN and Citrix accounts to access networks.
	Exploit Public-Facing Application (T1190)	The threat actor offered an exploit for the Microsoft Exchange vulnerability CVE-2020-0688.
Execution	Command and Scripting Interpreter: Visual Basic (T1059.005)	The threat actor used malicious Office document files with macros.
Persistence	Server Software Component: Web Shell (T1505.003)	The threat actor offered web shells for sale.
Credential Access	OS Credential Dumping: NTDS (T1003.003)	The threat actor advertised NTDS files for sale.
Discovery	Account Discovery: Domain Account (T1087.002)	The threat actor provided an LDAP screenshot showing information about users of corporate network domains.
Impact	Data Encrypted for Impact (T1486)	The threat actor posted a review about Thanos ransomware.

denis2363

Active	**August 2020 — present**
Number of victims	**50+ companies**
Attack geography	**4 countries**
Estimated earnings	**$160,000**

The individual who goes by **denis2363** started out on the forum Exploit on November 3, 2015, and continues to actively sell access data today.

On August 9, 2020, denis2363 posted their first ad offering access data for a game developer, setting the price at $25,000. Later that day, denis2363 lowered the price to **$5,000**, and on August 26 the threat actor left a comment in their for-sale thread claiming that the access data had been sold.



Access to one of the most renowned game publishers and developers

By denis2363 , August 9, 2020in Auctions

denis2363
byte

User
3
23 posts
Joined
11/03/15 (ID: 64806)
Activity
other

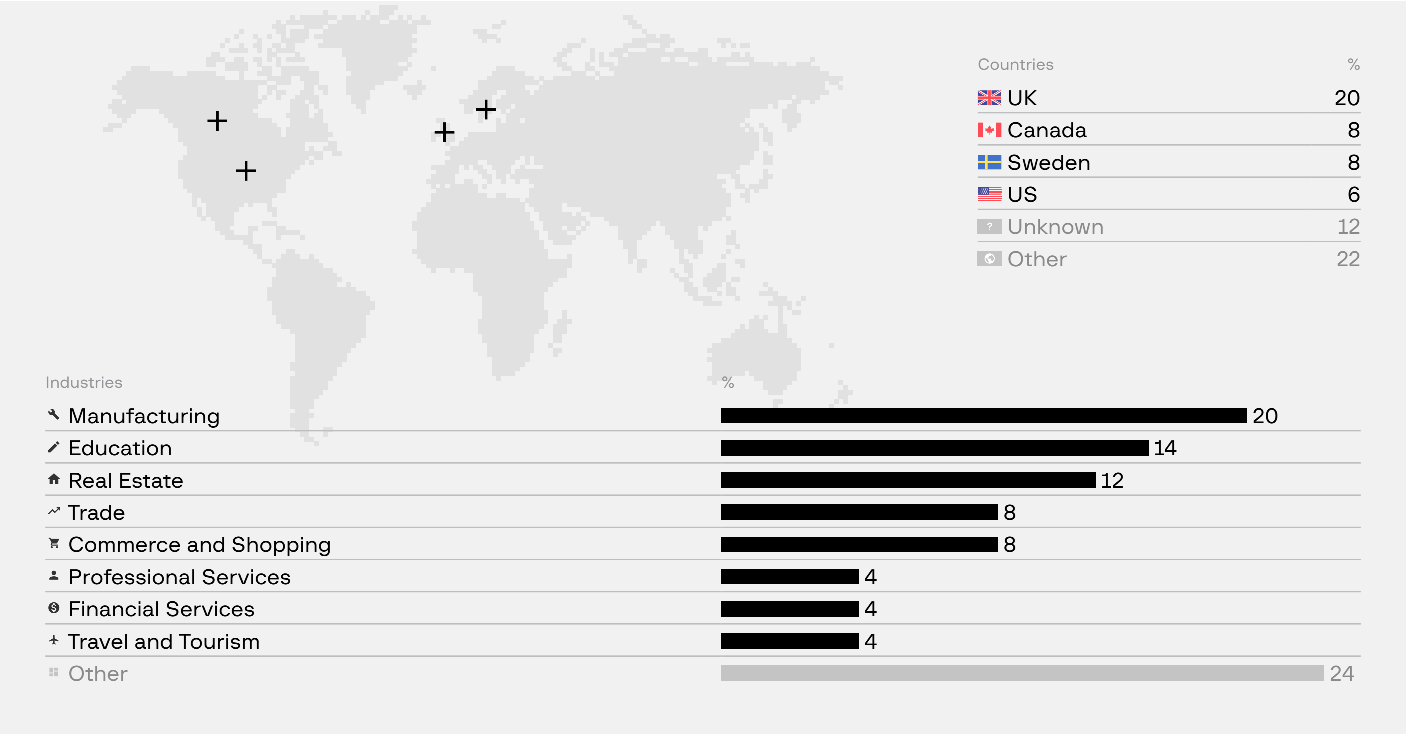
Posted August 9, 2020

There is an access to the account of the one famous cloud service of a very famous gaming company. Once it was one of the largest in the world, now it is also well-known. 29 servers, 28 mysql databases and other data are available. Games on google play, steam, the latest game has 10+ million downloads on google play.
Start: $ 25000
Blitz: $ 50,000

Fig. 35. A post by denis2363 offering access for sale

After analyzing denis2363's public activity, we concluded that they had exploited the BlueKeep, EternalBlue, and PrintNightmare vulnerabilities during some attacks. The threat actor identified vulnerable hosts by scanning open IP addresses and used **Shodan** to do so, among several other methods.

The threat actor has victims in many sectors, but most are in manufacturing, education, and real estate.



Countries	%
UK	20
Canada	8
Sweden	8
US	6
Unknown	12
Other	22

ATT&CK Matrix for Enterprise (denis2363)

TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning: Vulnerability Scanning (T1595.001)	The threat actor scanned IP addresses for signs of vulnerable services.
Initial Access	Exploit Public-Facing Application (T1190)	The threat actor exploited vulnerabilities in Citrix and FortiGate to gain access.
	External Remote Services (T1133)	The threat actor used VPN and Citrix accounts to access networks.
	Valid Accounts: Domain Accounts (T1078.002)	The threat actor used compromised domain accounts to access networks.
	Valid Accounts: Local Accounts (T1078.003)	The threat actor used compromised local accounts to access networks.
Persistence	Create Account: Local Account (T1136.001)	The threat actor mentioned creating a local admin account to achieve persistence in networks.
	Hijack Execution Flow: DLL Side-Loading (T1574.002)	The threat actor took advantage of DLL Side-Loading to exploit a vulnerability called PrintNightmare.

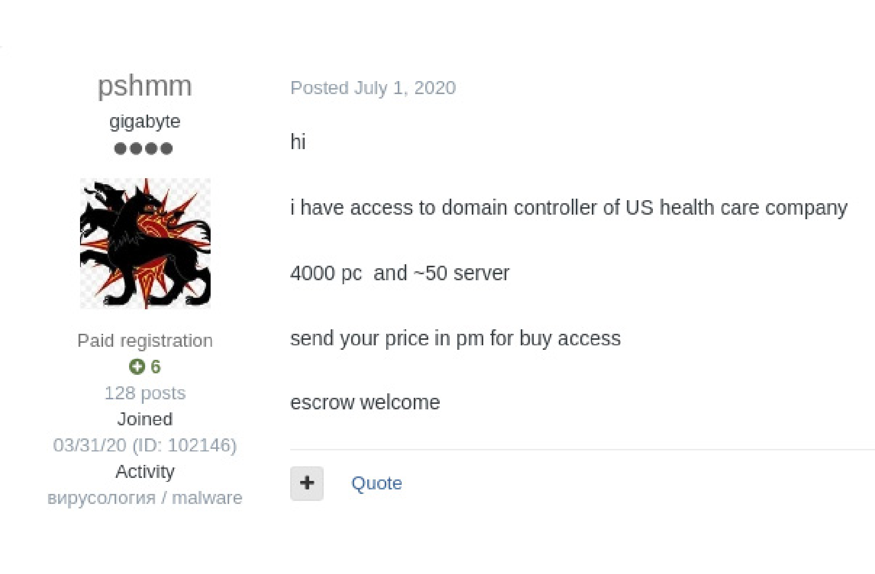
TACTICS	TECHNIQUES	DETAILS
Discovery	Network Share Discovery (T1135)	The threat actor used shared folders to exploit the vulnerability called PrintNightmare.
	Account Discovery (T1087)	The threat actor provided information about the number of hosts on the victim's network.
Lateral Movement	Exploitation of Remote Services (T1210)	The threat actor used the BlueKeep and EternalBlue vulnerabilities to move through networks.

Pshmm

Active	**July 2020 — present**
Number of victims	**85+ companies**
Attack geography	**19 countries**
Estimated earnings	**$300,000**

An English-speaking hacker using the alias **pshmm** was first seen on forums in early 2020 and was still active in October 2021.

Pshmm started their illegal activities by selling access to a US-based healthcare company's network domain controller.



pshmm
gigabyte
●●●●

Paid registration
6
128 posts
Joined
03/31/20 (ID: 102146)
Activity
вирусология / malware

Posted July 1, 2020

hi

i have access to domain controller of US health care company

4000 pc and ~50 server

send your price in pm for buy access

escrow welcome

Fig. 36. Pshmm's first post advertising network domain controller access for sale

The day after creating an Exploit forum account, pshmm started a dedicated thread that they later used to post ads about access data for sale. The threat actor sold data belonging to more than 85 companies in 19 different industries across 19 countries.

Although pshmm started out by selling access to network domain controllers that they had presumably infiltrated via RDP, the threat actor also claimed to have gained access to compromised networks by using corporate remote monitoring and management (RMM) software.

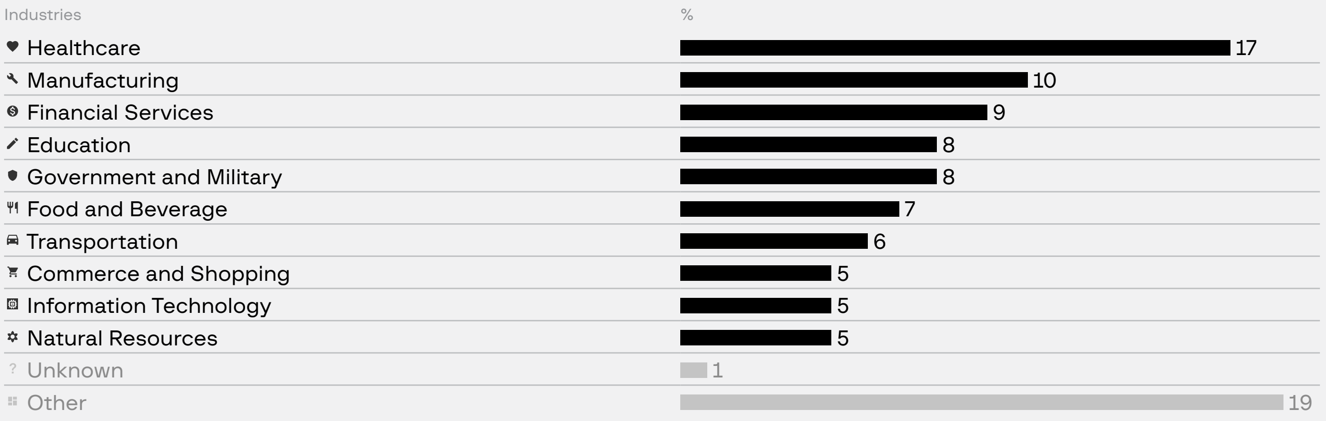
We know that pshmm used Zoho ManageEngine Desktop Central (software for centralized control over PCs and mobile devices on local networks) as a network access point. The software enables users (usually IT professionals) to perform remote operations such as deploying third-party software, configuring and setting policies, and— most importantly— launching custom scripts.

In January 2020, an RCE vulnerability was identified in Desktop Central but it remained unpatched for two months. The vulnerability enabled attackers to execute a series of commands of their choice with SYSTEM privileges without the need for authentication. Security researchers noted that this vulnerability was actively exploited, even after the official patch was released in March 2020. It is highly likely that pshmm exploited it.

As can be seen from the figure below, pshmm, like many other IABs we have looked at, has focused on the United States, which account for 42% of all of their victims.

Based on how the threat actor's attacks are distributed by industry, it seems that pshmm was focused on the healthcare sector, including hospitals and healthcare organizations, followed by manufacturers and financial service companies. Pshmm seems not to have a clear sequence of action when attacking an organization. Judging by the threat actor's activity, they were not focused on a particular country or industry for mass attacks, instead targeting whoever they could to make profit.

Countries	%
US	42
Canada	7
Brazil	6
China	6
France	3
UK	3
Italy	3
India	3
Australia	3
Unknown	7
Other	17



As for profits, given the access price quotes in the threat actor's posts, they could potentially have earned more than $300,000. Based on updates announcing the sale of access to certain buyers, it is safe to assume that pshmm made around $65,000 in guaranteed proceeds from selling unauthorized access.

ATT&CK Matrix for Enterprise (pshmm)

TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning (T1595)	The threat actor scanned devices running public RDP services.
Initial access	External Remote Services (T1133)	The threat actor used RDP and VPN accounts to access networks.
	Valid Accounts: Domain Accounts (T1078.002)	The threat actor used compromised domain accounts to access networks.
	Valid Accounts: Local Accounts (T1078.003)	The threat actor used compromised local accounts to access networks.
Credential access	Brute Force (T1110)	The threat actor used the brute-force search technique to access RDP accounts.
Discovery	Remote System Discovery (T1018)	The threat actor scanned the target environments for network domain controllers and remote services.
	File and Directory Discovery (T1083)	The threat actor mentioned specific files on a victim's file server.
	Network Share Discovery (T1135)	The threat actor mentioned specific files on a victim's file server.
	Account Discovery (T1087)	The threat actor provided information on the number of hosts on the victim's network.
Collection	Email Collection: Remote Email Collection (T1114.002)	The threat actor sold access data, including for Exchange servers.
	Data from Network Shared Drive (T1039)	The threat actor sold data obtained from a file server.

SHERIFF

Active	**April 2020 — March 2021**
Number of victims	**30+ companies**
Attack geography	**5 countries**
Estimated earnings	**$837,800**

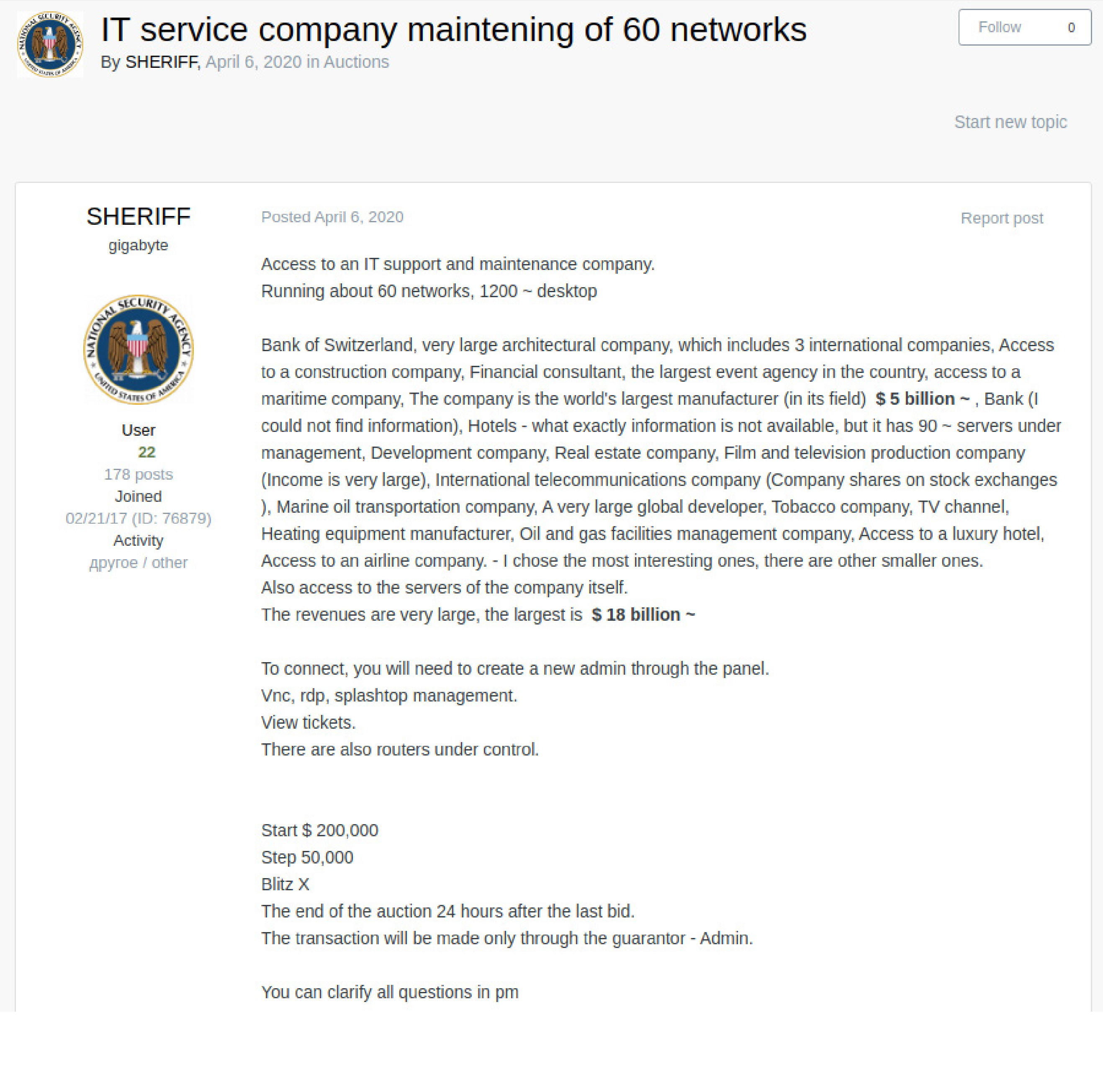
Another broker of initial access to corporate networks is an infamous Russian-speaking forum user known as **SHERIFF**, who focuses on financial service organizations. The broker first became active on the Exploit dark-web forum in 2017. SHERIFF was last seen on the forums as an active seller in March 2021.

The threat actor started out in the card theft business, selling data dumps of bank cards, databases and gift cards until 2019.

From early 2019, SHERIFF moved on to gaining access to vulnerable websites using tools such as the SIB service, X-MapAdmin, and OWASP ZAP. The hacker then started selling access to admin consoles and databases. Nearly all their victims were US-based online stores. Moreover, in 2020 the threat actor actively exploited RCE vulnerabilities linked to the Citrix RDP protocol.

In April 2020, SHERIFF advertised access to a major IT company (which may have been an MSP). The threat actor's post suggested that the company had customers in architecture, construction, financial consulting, and the maritime and aviation industries, as well as in several banks, with one based in Switzerland.

Fig. 37. SHERIFF's first post offering access for sale



IT service company maintening of 60 networks

By SHERIFF, April 6, 2020 in Auctions

SHERIFF
gigabyte

User
22
178 posts
Joined
02/21/17 (ID: 76879)
Activity
другое / other

Posted April 6, 2020

Access to an IT support and maintenance company.
Running about 60 networks, 1200 ~ desktop

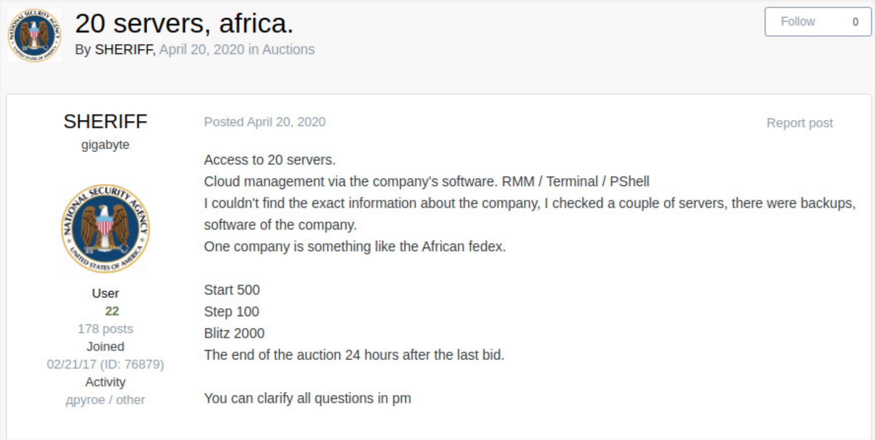
Bank of Switzerland, very large architectural company, which includes 3 international companies, Access to a construction company, Financial consultant, the largest event agency in the country, access to a maritime company, The company is the world's largest manufacturer (in its field) **$ 5 billion ~** , Bank (I could not find information), Hotels - what exactly information is not available, but it has 90 ~ servers under management, Development company, Real estate company, Film and television production company (Income is very large), International telecommunications company (Company shares on stock exchanges), Marine oil transportation company, A very large global developer, Tobacco company, TV channel, Heating equipment manufacturer, Oil and gas facilities management company, Access to a luxury hotel, Access to an airline company. - I chose the most interesting ones, there are other smaller ones.
Also access to the servers of the company itself.
The revenues are very large, the largest is **$ 18 billion ~**

To connect, you will need to create a new admin through the panel.
Vnc, rdp, splashtop management.
View tickets.
There are also routers under control.

Start $ 200,000
Step 50,000
Blitz X
The end of the auction 24 hours after the last bid.
The transaction will be made only through the guarantor - Admin.

You can clarify all questions in pm

In the same month, SHERIFF created another post offering 20 sets of access credentials to corporate servers. Since the description was similar to information in their earlier post, we have reason to believe that the hacker had gained access to the networks belonging to the IT company's clients. It is also unclear whether any of the access credentials were actually sold.



20 servers, africa.

By SHERIFF, April 20, 2020 in Auctions

SHERIFF
gigabyte

User
22
178 posts
Joined
02/21/17 (ID: 76879)
Activity
другое / other

Posted April 20, 2020

Access to 20 servers.
Cloud management via the company's software. RMM / Terminal / PShell
I couldn't find the exact information about the company, I checked a couple of servers, there were backups, software of the company.
One company is something like the African fedex.

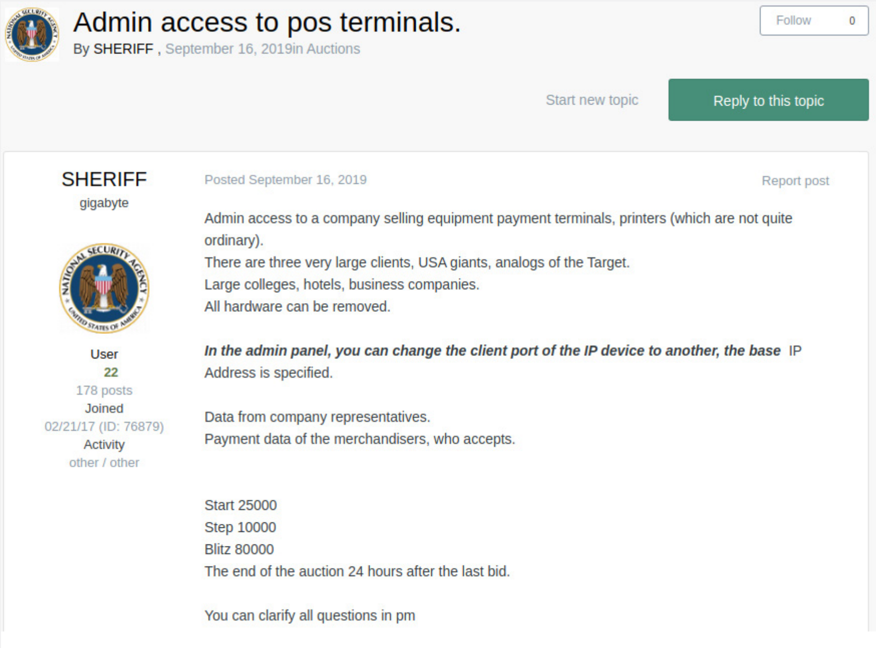
Start 500
Step 100
Blitz 2000
The end of the auction 24 hours after the last bid.

You can clarify all questions in pm

Fig. 38. SHERIFF's post advertising access to servers

In August 2019, SHERIFF started a topic on the forum asking other users to suggest ways to monetize data from an investment website that contained IBAN, BIC and SWIFT codes. The threat actor put the data up for sale two days later, asking for **$35,000**.

Further suggesting that SHERIFF focuses on the financial services industry, the threat actor's victims included a POS terminal manufacturer. According to a message from September 16, 2019, the manufacturer serves major US corporations, colleges, and hotels. Moreover, the message author said that hackers could change the customer IP port of payment processing terminals in the victim's admin console to intercept data.



Admin access to pos terminals.

By SHERIFF , September 16, 2019in Auctions

SHERIFF
gigabyte

User
22
178 posts
Joined
02/21/17 (ID: 76879)
Activity
other / other

Posted September 16, 2019

Admin access to a company selling equipment payment terminals, printers (which are not quite ordinary).
There are three very large clients, USA giants, analogs of the Target.
Large colleges, hotels, business companies.
All hardware can be removed.

In the admin panel, you can change the client port of the IP device to another, the base IP Address is specified.

Data from company representatives.
Payment data of the merchandisers, who accepts.

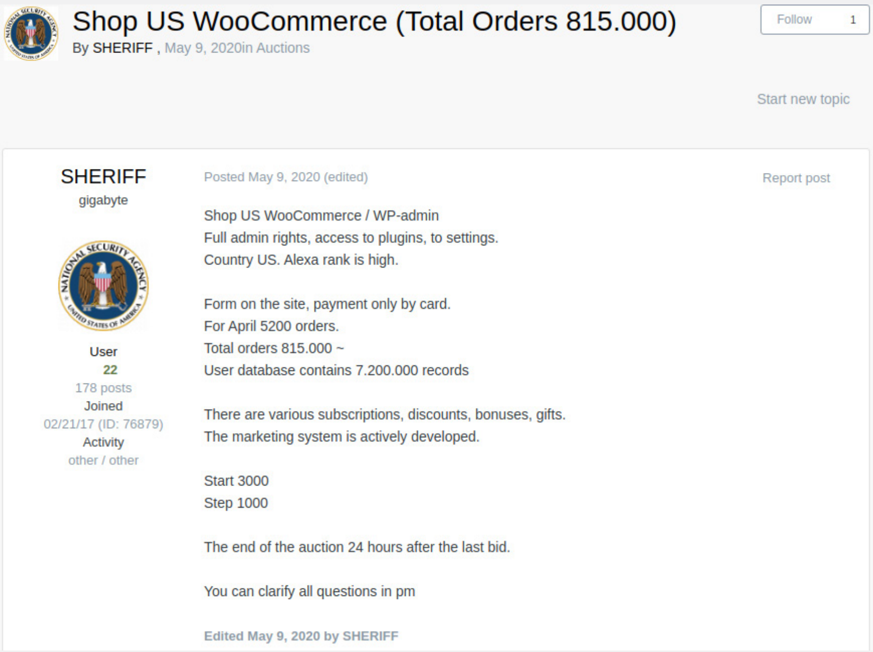
Start 25000
Step 10000
Blitz 80000
The end of the auction 24 hours after the last bid.

You can clarify all questions in pm

Fig. 39. SHERIFF's post about closing the sale of access

SHERIFF actively sought potential business partners and collaborators on underground forums. The threat actor also tried to purchase data (gathered by information stealers) from other participants at auctions. For example, SHERIFF attended an auction for selling "logs" of compromised data obtained using the AZORult stealer.

One of SHERIFF's most notable activities was their partnership with members of the hacker group **REvil**. The latter repeatedly purchased access data from SHERIFF, using **UNKN** and **unknown** as their aliases, which are known to belong to REvil members, who use similarly named ransomware in their cyberattacks.



Shop US WooCommerce (Total Orders 815.000)

By SHERIFF , May 9, 2020in Auctions

SHERIFF
gigabyte

User
22
178 posts
Joined
02/21/17 (ID: 76879)
Activity
other / other

Posted May 9, 2020 (edited)

Shop US WooCommerce / WP-admin
Full admin rights, access to plugins, to settings.
Country US. Alexa rank is high.

Form on the site, payment only by card.
For April 5200 orders.
Total orders 815.000 ~
User database contains 7.200.000 records

There are various subscriptions, discounts, bonuses, gifts.
The marketing system is actively developed.

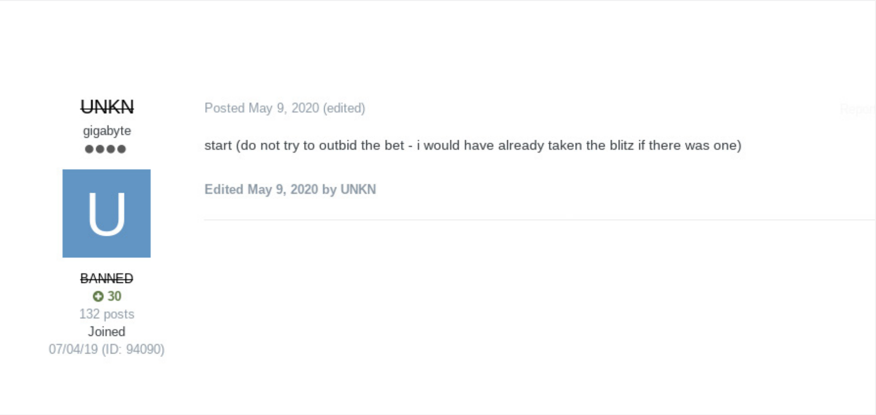
Start 3000
Step 1000

The end of the auction 24 hours after the last bid.

You can clarify all questions in pm

Edited May 9, 2020 by SHERIFF

Fig. 40. A screenshot of SHERIFF's thread on the Exploit forum



~~UNKN~~
gigabyte
●●●●

~~BANNED~~
30
132 posts
Joined
07/04/19 (ID: 94090)

Posted May 9, 2020 (edited)

start (do not try to outbid the bet - i would have already taken the blitz if there was one)

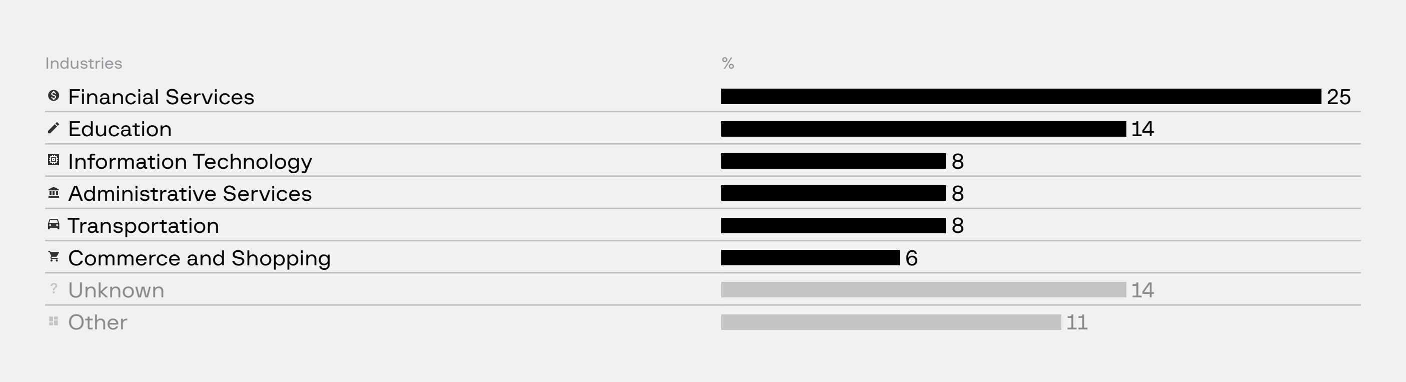
Edited May 9, 2020 by UNKN

Fig. 41. A comment by a REvil member in a thread started by SHERIFF

In 2020-2021, SHERIFF advertised 33 sets of access credentials for corporate networks. It is impossible to be absolutely certain how much the threat actor made from selling the data because most of the threads do not contain comments confirming the sale. Group-IB Threat Intelligence experts estimate that they could have made at least **$837,800**.

SHERIFF rarely specified what countries their victims were based in, so it is impossible to be sure which countries the threat actor attacked most often. From the information SHERIFF did provide in their posts, we can reasonably conclude that they focused on companies based in Asia and the US, with some victims based in Europe, Australia, and Canada.

The chart below breaks down SHERIFF's attacks by industry.



It is impossible to identify the countries SHERIFF focused on most often, as the threat actor never provided detailed information about the access data they were selling.

ATT&CK Matrix for Enterprise (SHERIFF)

TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning: Vulnerability Scanning (T1595.002)	The threat actor scanned websites for vulnerabilities (using X-MapAdmin).
Initial access	External Remote Services (T1133)	The threat actor sold Citrix and RDP access data.
	Valid Accounts (T1078)	The threat actor used compromised accounts to obtain access to remote services and websites.
Credential access	Brute Force (T1110)	The threat actor sold account access data obtained through brute-force attacks.
Discovery	Account Discovery (T1087)	The threat actor provided information on the number of hosts on the victim's network.
Command and Control	Remote Access Software (T1219)	The threat actor took advantage of hidden TeamViewer.

Nei (aka Rakuda)

Active	**March 2021 - present**
Number of victims	**55 companies**
Attack geography	**7 countries**
Estimated earnings	**$24,000 — $36,000**

Nei (aka **Rakuda** and **Asatru**) is a threat actor who focuses on selling VPN-RDP access data. Nei has been active on the forums Exploit and XSS since March 2021. The threat actor's most recent activity was in October 2021.

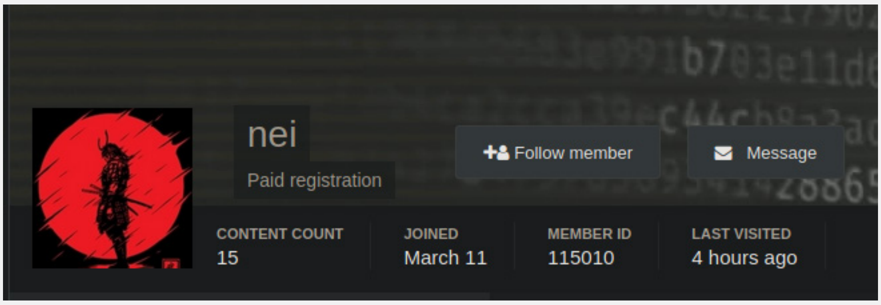
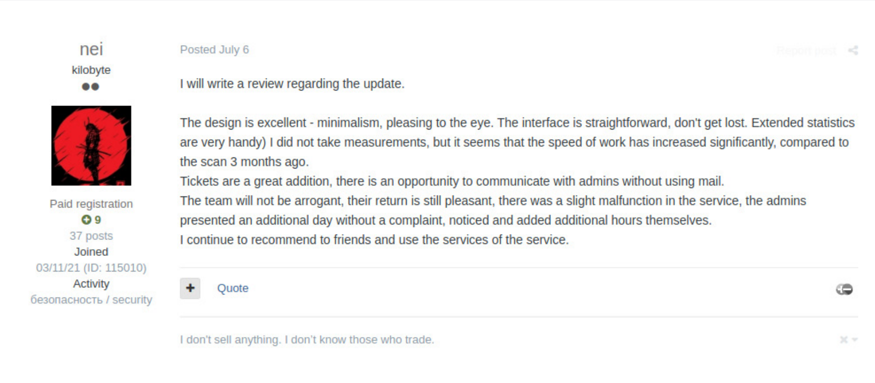


Fig. 42. Nei's profile on Exploit

In addition to selling access data on Exploit, Nei also actively takes part in discussions with other cybercriminals on XSS. For example, the threat actor left comments with tips on bypassing anti-fraud systems and attacking websites.

In published threads, Nei indicated that 42 of the 55 sets of access credentials they had put up for sale were sold. Although the threat actor's prices are lower than other brokers, Group-IB experts estimate that Nei's proceeds amount to between **$24,000 and $36,000**.

It is not 100% certain what methods Nei has used to gain access to corporate networks. What we do know is that they have used tools such as Masscan to identify large pools of new potential victims. This suggests that the threat actor actively searches for open RDP and VPN servers worldwide.



I will write a review regarding the update.

The design is excellent - minimalism, pleasing to the eye. The interface is straightforward, don't get lost. Extended statistics are very handy) I did not take measurements, but it seems that the speed of work has increased significantly, compared to the scan 3 months ago.
Tickets are a great addition, there is an opportunity to communicate with admins without using mail.
The team will not be arrogant, their return is still pleasant, there was a slight malfunction in the service, the admins presented an additional day without a complaint, noticed and added additional hours themselves.
I continue to recommend to friends and use the services of the service.

I don't sell anything. I don't know those who trade.

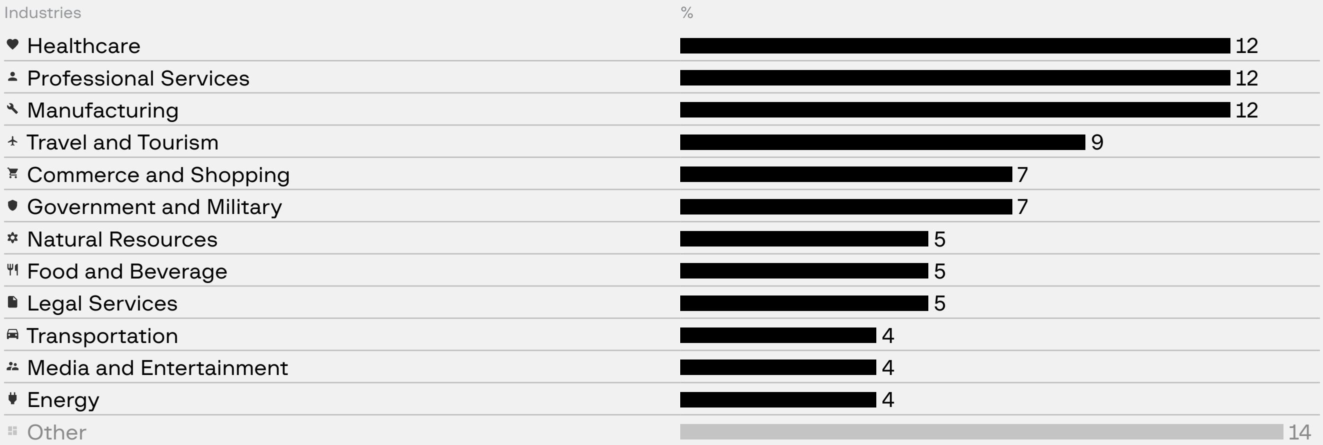
Fig. 43. Nei's comment in a thread discussing Masscan updates

After creating an account on XSS, Nei repeatedly expressed interest in new information stealer malware that was becoming available, including by taking part in discussions about Raccoon Stealer.

In the diagram below, Nei's attacks are broken down by industry. The threat actor focused on healthcare providers, service companies, and manufacturers. Another main category was "Other," which includes companies whose sectors have not been identified.

A breakdown of Nei's victims by country shows that the threat actor focused on companies based in the US and France, which account for half of their victims.

Countries	%
US	30
France	18
Spain	9
UK	9
Canada	5
Chile	5
Italy	5
Unknown	19



ATT&CK Matrix for Enterprise (Nei)

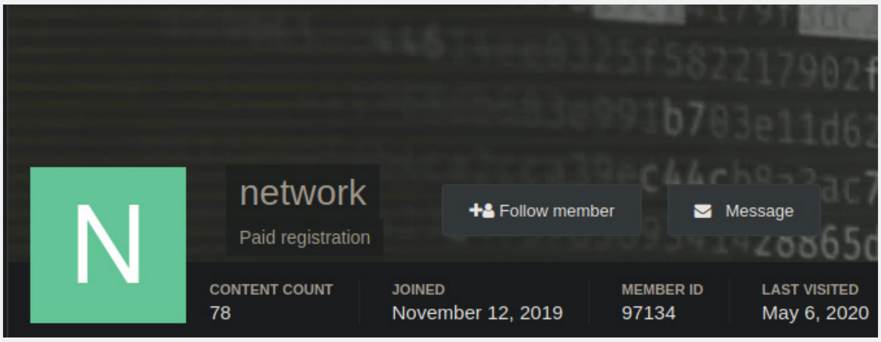
TACTICS	TECHNIQUES	DETAILS
Reconnaissance	Active Scanning: Scanning IP Blocks (T1595.001)	The threat actor used Masscan to search for open ports.
Initial access	Exploit Public-Facing Application (T1190)	The threat actor looked for vulnerabilities on WordPress websites.
	External Remote Services (T1133)	The threat actor used RDP and VPN to access corporate networks.
Execution	User Execution: Malicious File (T1204.002)	The threat actor relied on malware to obtain compromised user account data.

TACTICS	TECHNIQUES	DETAILS
Credential access	OS Credential Dumping (T1003)	The threat actor relied on malware to obtain compromised user account data.
Discovery	Account Discovery (T1087)	The threat actor provided information about the number of hosts on the victim's network.

network

Active	**November 2019 — May 2020**
Number of victims	**54 companies**
Attack geography	**17 countries**
Estimated earnings	**$400,000**

The user hiding behind the alias **network** was another IAB who was active on Exploit between November 2019 and May 2020.



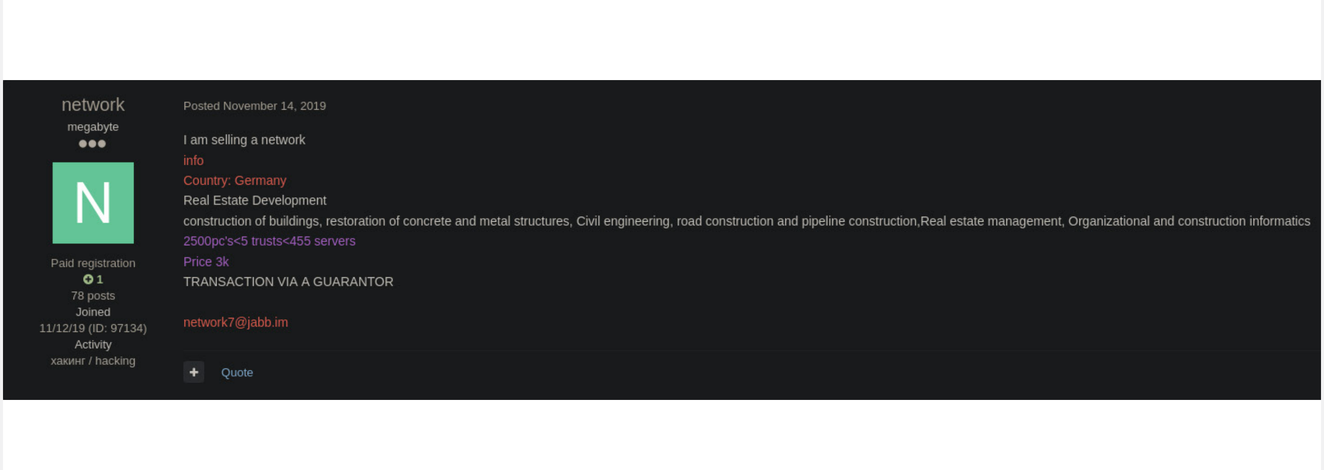
network
Paid registration

CONTENT COUNT	JOINED	MEMBER ID	LAST VISITED
78	November 12, 2019	97134	May 6, 2020

Fig. 44. Network's profile on Exploit

Network posted their first access ad just two days after creating their account, on November 14, 2019. The threat actor advertised access to a German real estate company for $3,000.

Fig. 45. Screenshot of network's first post offering access for sale



network
megabyte
●●●
Paid registration
1
78 posts
Joined
11/12/19 (ID: 97134)
Activity
хакинг / hacking

Posted November 14, 2019

I am selling a network
info
Country: Germany
Real Estate Development
construction of buildings, restoration of concrete and metal structures, Civil engineering, road construction and pipeline construction,Real estate management, Organizational and construction informatics
2500pc's<5 trusts<455 servers
Price 3k
TRANSACTION VIA A GUARANTOR

network7@jabb.im

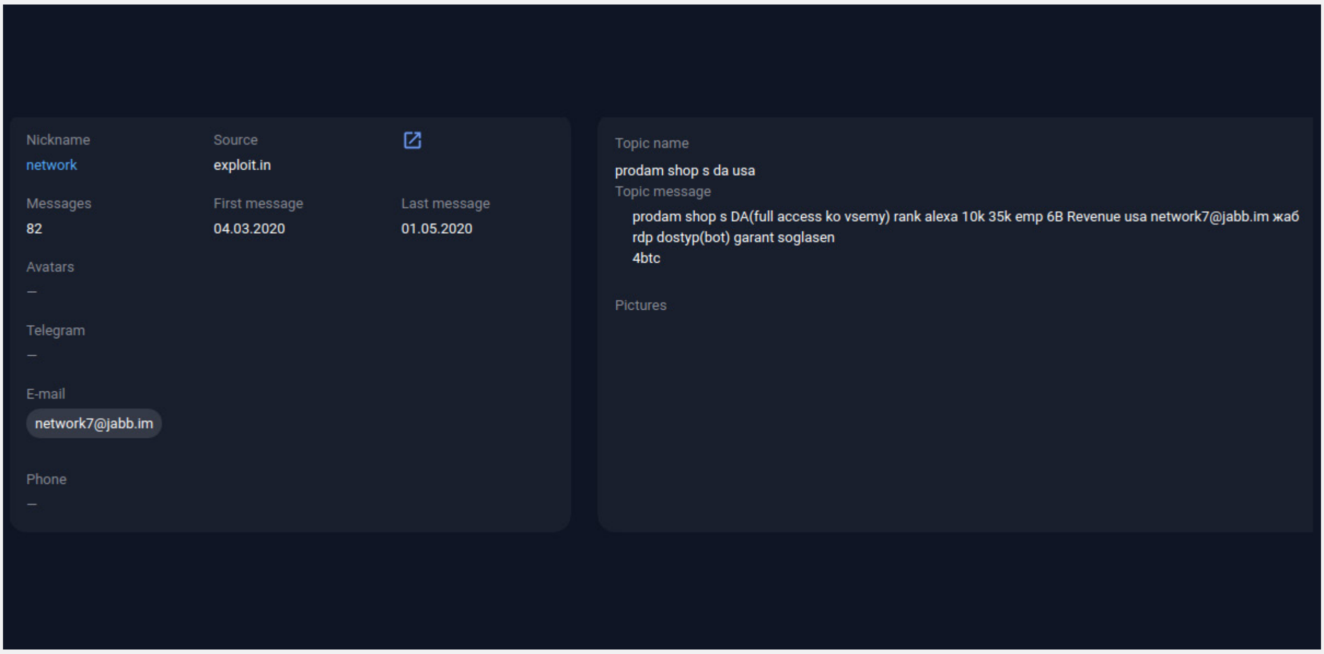
The IAB consistently posted ads in small batches of three to four per day. They usually sold two types of access: domain admin accounts and session access, which could indicate that the threat actor relied on Cobalt Strike or Armitage to obtain data.

After 12 months of nearly constant activity, network abruptly stopped posting on May 1. The threat actor's last sale involved access to a US online store with $6 billion in revenue. The post was later deleted from the forum.

Unlike other brokers, network did not indicate in their threads whether the access credentials had been sold or not; the threat actor deleted their forum posts from time to time. This could mean that access either was sold or became unavailable.

However, even though the author deleted their posts, the posts are still available through Group-IB Threat Intelligence & Attribution. Group-IB TI&A helps find out exactly how many sets of access credentials for corporate networks the threat actor put up for sale. Group-IB's system also made it possible to recover the message about the sale of access for the aforementioned US-based company. A screenshot of network's message is provided below.

Fig. 46. Network's message in Group-IB Threat Intelligence & Attribution



Nickname
network

Source
exploit.in

Messages
82

First message
04.03.2020

Last message
01.05.2020

Avatars
—

Telegram
—

E-mail
network7@jabb.im

Phone
—

Topic name
prodam shop s da usa

Topic message
prodam shop s DA(full access ko vsemy) rank alexa 10k 35k emp 6B Revenue usa network7@jabb.im жаб
rdp dostyp(bot) garant soglasen
4btc

Pictures

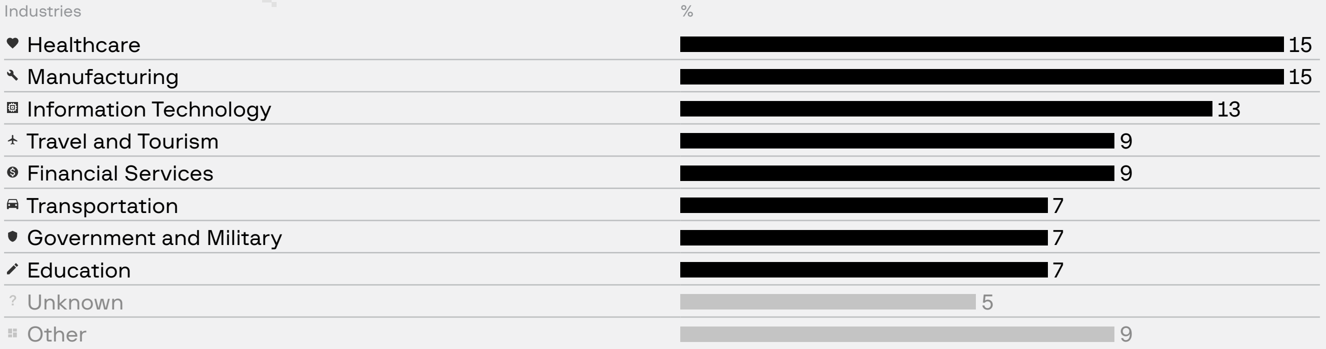
As noted above, network rarely announced when access had been sold, which makes their proceeds difficult to ascertain. Based solely on the price quotes, however, we can estimate that the overall value of the access credentials the threat actor put up for sale was more than **$400,000**.

Although network's career was brief (at least under that username), they managed to obtain access to more than 50 companies across 17 countries.

The figure below breaks down the threat actor's victims by country. Looking at the country data, we can conclude that network mainly targeted the United States, followed by the United Kingdom and the rest of Europe. Moreover, many sets of access credentials could not be definitively attributed to a country and were therefore included in the "Unknown" category. The category accounts for a significant share of their posts at 21%.

Network mainly targeted the following sectors: healthcare, manufacturing, software development, and travel and tourism.

Countries	%
US	34
Europe	21
UK	9
India	5
Americas	5
Unknown	24
Other	5



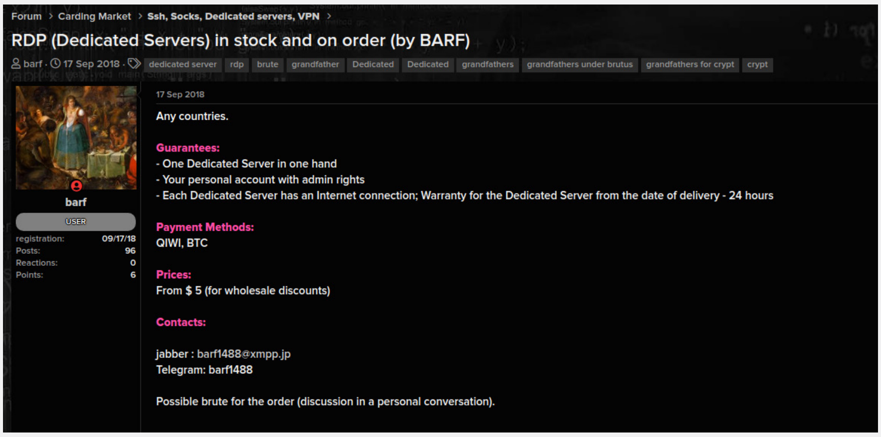
ATT&CK Matrix for Enterprise (Network)

TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	The threat actor used RDP accounts to access networks.
Discovery	Account Discovery (T1087)	The threat actor provided information about the number of hosts on the victim's network.

barf

Active	**December 2020 — May 2021**
Number of victims	**145 companies**
Attack geography	**9 countries**
Estimated earnings	**$49,000**

The user became active on underground forums in 2017 and continued posting until May 2021. From 2018, the hacker began posting ads selling RDP servers on other underground forums using **barf** as a username.



Forum > Carding Market > Ssh, Socks, Dedicated servers, VPN >

RDP (Dedicated Servers) in stock and on order (by BARF)

barf · 17 Sep 2018 · dedicated server rdp brute grandfather Dedicated Dedicated grandfathers grandfathers under brutus grandfathers for crypt crypt

barf
USER
registration: 09/17/18
Posts: 96
Reactions: 0
Points: 6

17 Sep 2018

Any countries.

Guarantees:
- One Dedicated Server in one hand
- Your personal account with admin rights
- Each Dedicated Server has an Internet connection; Warranty for the Dedicated Server from the date of delivery - 24 hours

Payment Methods:
QIWI, BTC

Prices:
From $ 5 (for wholesale discounts)

Contacts:

jabber : barf1488@xmpp.jp
Telegram: barf1488

Possible brute for the order (discussion in a personal conversation).

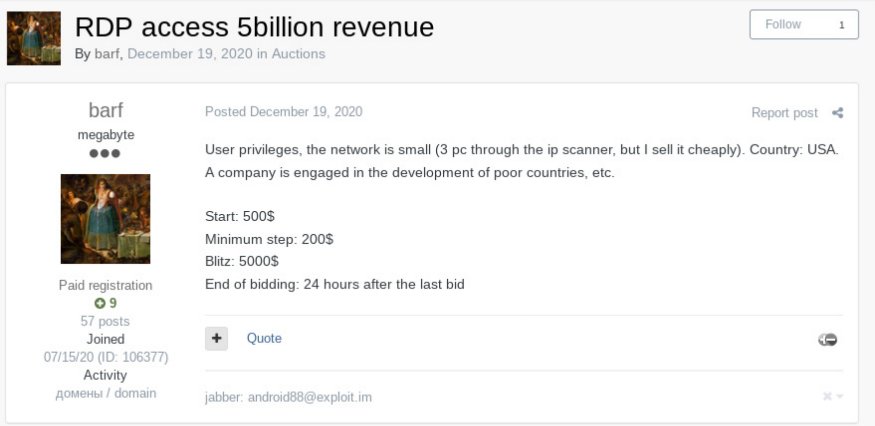
Fig. 47. One of barf's threads from 2018 selling dedicated servers

In January 2019, barf advertised a malware subscription for gaining SSH, RDP and VNC access through a brute-force attack created by z668, another threat actor active at the time. According to barf, they themselves had been using this specific malware for some time, but later changed their focus and thus stopped using the malware.

It is likely that barf switched to selling access credentials for corporate networks in July 2020, when they created an account on the popular underground forum Exploit. It was on this forum that the threat actor posted all their ads selling access credentials.

After creating an account, barf started a thread in which they said they were looking for a developer able to write software for brute-force RDP attacks that would check for access with admin permissions, the OS version, and other details.

The threat actor created their first thread selling network access on Exploit in December 2020. In their post, barf advertised access to a corporate network belonging to a US-based charity.



RDP access 5billion revenue
By barf, December 19, 2020 in Auctions

barf
megabyte
Paid registration
9
57 posts
Joined
07/15/20 (ID: 106377)
Activity
домены / domain

Posted December 19, 2020

User privileges, the network is small (3 pc through the ip scanner, but I sell it cheaply). Country: USA.
A company is engaged in the development of poor countries, etc.

Start: 500$
Minimum step: 200$
Blitz: 5000$
End of bidding: 24 hours after the last bid

jabber: android88@exploit.im

Fig. 48. Barf's first post about selling network access

Unlike most other IABs, barf's posts often included the first two octets of their victims' IP addresses, which suggests that the threat actor might have been using an IP scanner.

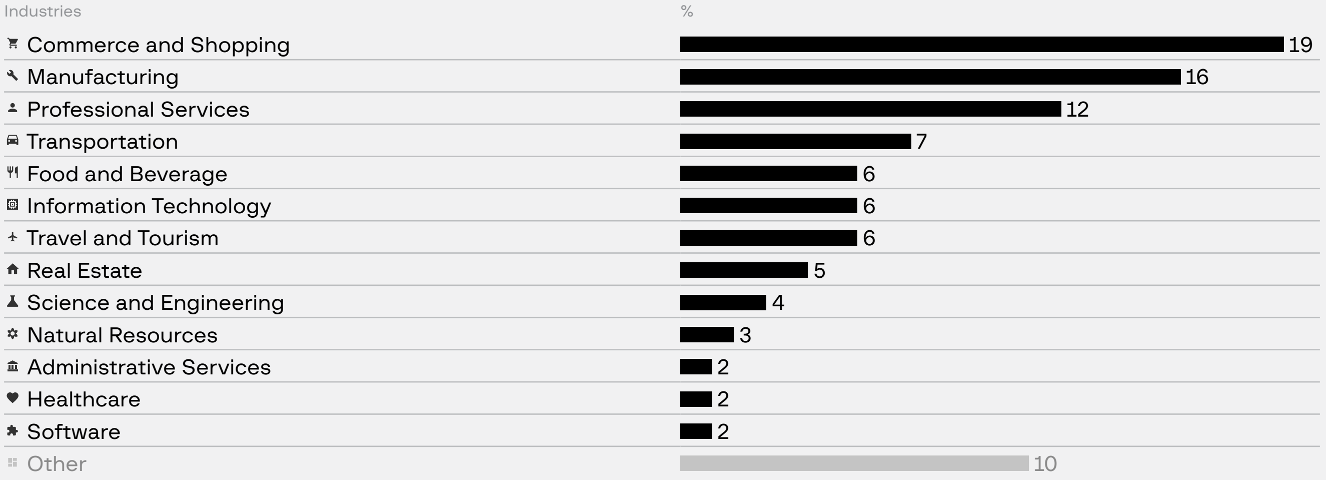
Based on their forum activity, barf seems to focus on selling access to corporate networks using RDP only.

In the period spanning H2 2020 and H1 2021, barf was one of the most active sellers of access to corporate networks.

Throughout their active phase, barf posted for-sale ads for 145 instances of RDP access on Exploit. The chart below shows that most of barf's victims are based in the US, followed by the UK and Australia. The "Other" category includes access credentials for companies based in other countries not shown in the chart. Each represents 2% or less of the total number of access offers made by barf.

The threat actor's main industry focus appears to be retailers, manufacturers, and service industry players. However, it would be difficult to claim that barf was interested in any specific industry, given the sheer volume of their for-sale posts.

Countries	%
US	22
UK	11
Australia	10
France	9
Brazil	7
Italy	7
Spain	6
Germany	3
Sweden	3
Other	22



Barf's lowest asking price was $10 and the highest was $5,000. We estimate that, throughout their active phase starting in December 2020, barf could have made approximately $49,000 by selling RDP access to corporate networks.

The table below shows the TTPs that barf presumably used.

ATT&CK Matrix for Enterprise (barf)

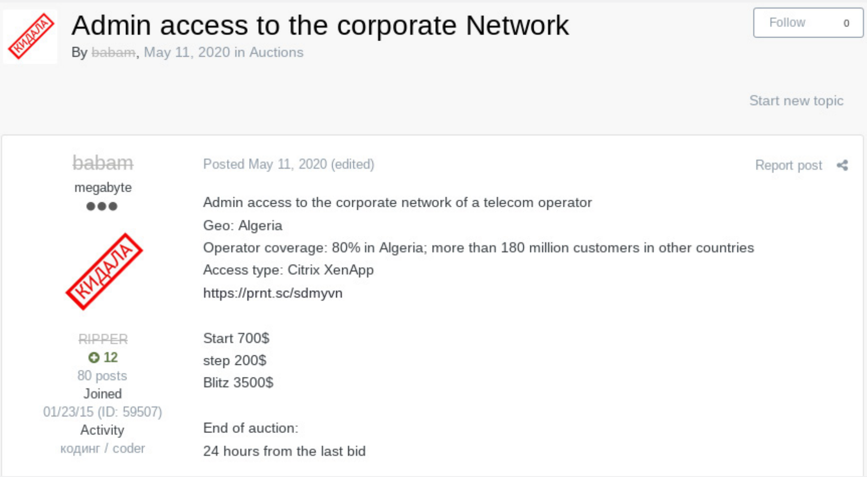
Tactics	Techniques	Details
Reconnaissance	Active Scanning (T1595)	The threat actor scanned devices running public RDP services.
Initial access	External Remote Services (T1133)	The threat actor used RDP accounts to access networks.
Credential access	Brute Force (T1110)	The threat actor used malware for a brute-force attack on RDP.
	Brute Force: Credential Stuffing (T1110.004)	The threat actor presumably took advantage of previously compromised user accounts for a brute-force attack to gain access to corporate networks.
Discovery	Network Service Scanning (T1046)	The threat actor obtained information about Drake Software installed on the victim's host.
	Account Discovery (T1087)	The threat actor provided information about the number of hosts on the victim's network.

babam

📅 Active	**May 2020 — September 2021**
👤 Number of victims	**37 companies**
🌐 Attack geography	**15 countries**
💼 Estimated earnings	**$25,000**

The hacker known as **babam** is one of the most well-known and prolific brokers of initial access to networks. The threat actor was first seen on Exploit on January 23, 2015. Their most recent activity was recorded on September 28, 2021, after which they were banned from the forum.

Although babam has been active on underground forums since 2015, their first offer to sell initial access to a corporate network was posted on May 11, 2020. The poster was selling Citrix XenApp access to an Algerian telecommunications company.



Admin access to the corporate Network

By ~~babam~~, May 11, 2020 in Auctions

~~babam~~
megabyte
~~RIPPER~~
12
80 posts
Joined
01/23/15 (ID: 59507)
Activity
кодинг / coder

Posted May 11, 2020 (edited)

Admin access to the corporate network of a telecom operator
Geo: Algeria
Operator coverage: 80% in Algeria; more than 180 million customers in other countries
Access type: Citrix XenApp
https://prnt.sc/sdmyvn

Start 700$
step 200$
Blitz 3500$

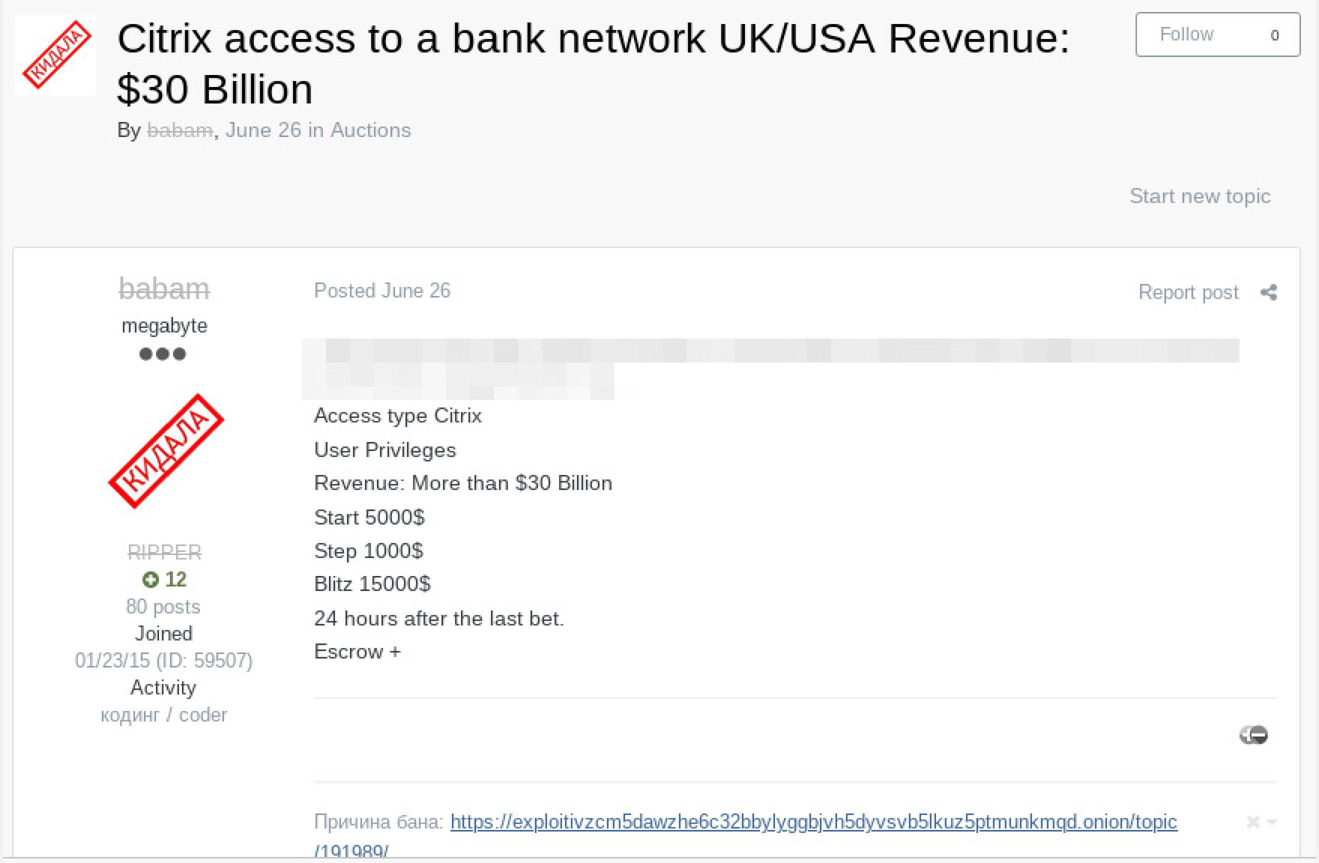
End of auction:
24 hours from the last bid

Fig. 49. babam's first post on Exploit selling initial access to a corporate network

In March 2021 the threat actor mentioned that they had used Mimikatz to extract data from a session dump.

On June 26, 2021, babam started a new topic on Exploit offering to sell Citrix access to a network belonging to a major bank with $30 billion in annual revenue. The user noted that the bank was based in the UK and the US.

Fig. 50. A post advertising Citrix access to a major bank's corporate network



КИДАЛА

Citrix access to a bank network UK/USA Revenue: $30 Billion

By ~~babam~~, June 26 in Auctions

~~babam~~
megabyte
●●●

КИДАЛА

~~RIPPER~~
12
80 posts
Joined
01/23/15 (ID: 59507)
Activity
кодинг / coder

Posted June 26

[redacted]

Access type Citrix
User Privileges
Revenue: More than $30 Billion
Start 5000$
Step 1000$
Blitz 15000$
24 hours after the last bet.
Escrow +

Причина бана: https://exploitivzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/topic/191989/

This victim was one of the largest entities to which babam had ever offered access. On June 28, 2021, the threat actor announced that the sale had been closed.

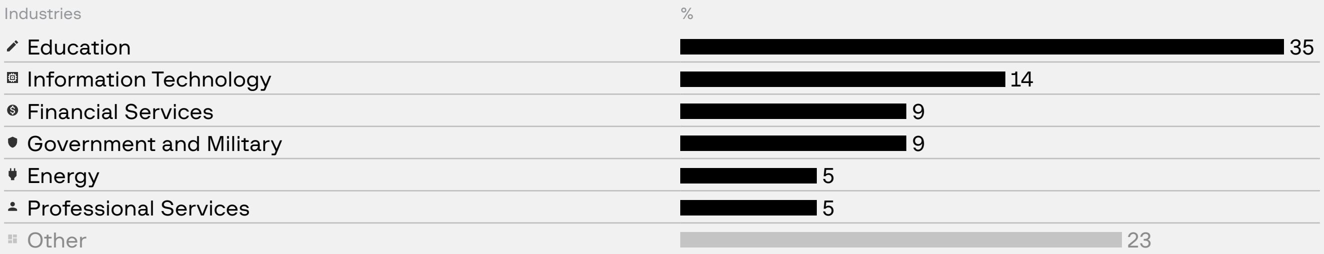
The hacker was most likely using an RDP brute-force tool created by z668, another forum user. Babam expressed their wish to purchase the tool in relevant threads in June 2017 and October 2020. As such, we assume that babam scanned vulnerable ports and brute-forced them using the RDP brute-force tool or a similar one.

Group-IB experts discovered that babam posted **37** ads on underground forums advertising initial access to corporate networks. We estimate the total value of the access offers at **$25,000** or more. They included Citrix, RD Web, RDP, VPN, and Cisco VPN access with both admin or user permissions.

Most of the threat actor's victims are based in the US, other parts of the Americas, and Europe. The chart below breaks down all the identified instances of access. The threat actor attacked victims in 18 countries.

Looking at the breakdown of their victims by industry, babam appears to have focused on education (which accounts for 35% of all the victims), followed by IT and financial services.

Countries	%
US	23
Spain	13
Canada	10
Australia	8
France	5
Netherlands	5
UK	6
Argentina	5
Other	26



ATT&CK Matrix for Enterprise (babam)

TACTICS	TECHNIQUES	DETAILS
Initial access	External Remote Services (T1133)	The threat actor used RDP, VPN, and Citrix accounts to access networks.
	Valid Accounts: Domain Accounts (T1078.002)	The threat actor used compromised domain accounts to access networks.
	Valid Accounts: Local Accounts (T1078.003)	The threat actor used compromised local accounts to access networks.
Credential access	OS Credential Dumping (T1003)	The threat actor used Mimikatz to extract data from a session dump.
	Brute Force (T1110)	The threat actor used malware to brute-force RDP.
Discovery	Account Discovery (T1087)	The threat actor provided information about the number of hosts on the victim's network.

SECURITY RECOMMENDATIONS

09

As the number of IABs has increased, so has the number of TTPs they use. Based on available information about TTPs, we recommend the following steps:

1. **Configure account access blocking.** To gain access, hackers often perform brute-force searches for account passwords. The number of authentication attempts in a brute-force attack is many orders of magnitude higher than the number of attempts by a user who makes a typo when entering the password. To prevent such attacks, set up account locking for a specified amount of time, which activates when the limit of unsuccessful authentication attempts is reached.
2. **Check public data leaks for sets of credentials.** Hackers often use compromised data from various leaks (so-called combo lists, i.e. sets of credentials) to put together dictionaries for brute-force attacks. As such, a preventative check for leaked user data makes a successful attack much less likely. Group-IB Threat Intelligence & Attribution makes it easy to run such checks.
3. **Take preventative measures to identify leaks advertised on the dark web.** To ensure a timely response to possible data leaks, Group-IB experts recommend using threat intelligence solutions to track any signs of corporate data appearing on the dark web, which helps take steps to secure data and identify the potential source of the leak.
4. **Install dedicated software to track and identify server anomalies.** Such software makes it easy to track traffic anomalies, new accounts being created, and attempts to gain unauthorized access to data.
5. **Allow whitelists for IP addresses.** Limit access to remote servers to a list of specific IP addresses. If any employees work remotely, configure a corporate VPN.
6. **Disable or block unused remote services**.
7. **Use multifactor authentication** for remote service accounts. This limits opportunities for using compromised credentials.
8. **Use unique strong passwords**.
9. **Utilize least privilege access principles** for service accounts, which restricts permissions to processes with potential vulnerabilities that hackers can take advantage of.
10. **Install software updates on a regular and timely basis** to eliminate any identified vulnerabilities.

11. **Analyze security and test for breach vulnerabilities** to identify network weaknesses and possible attack vectors.
12. **Take stock of the external network perimeter**, network firewall rules, and network address broadcasting rules to minimize the likelihood of making any services public by mistake.
13. **Ban internet access for any easily compromised devices** such as video surveillance equipment, smart home devices, office equipment (printers, scanners, multifunctional printers), and storage devices and media (such as SOHO-segment NAS servers).
14. **Do not allow external network perimeter access** to OS direct remote access services (such as RDP, SSH, VNC, and SMB/RPC).
15. **Limit network access** for specific tasks (e.g., contractors should get access only to servers that they need to carry out their work, rather than a whole network segment or the entire network).
16. **Add an “expires at”** field to user accounts and access privileges for situations when manually revoking remote access could fail.
17. **Identify signs of initial access**, gaining persistence, and progress across the network. Although most techniques used by attackers are primitive and can be detected even with an untrained eye, regular proactive threat hunting helps prevent and combat sophisticated attacks.
18. **Regularly scan the corporate infrastructure** to detect signs of compromised network access.
19. **Ban users from signing up to third-party services** using their corporate email address, as many people use the same password (or a version thereof) across multiple services. If a password is leaked from one service, hackers could attack the entire company.

Requirements for data security protection:

20. **Scan for signs of popular post-exploitation frameworks**.
21. **Scan for anomalous activity in legitimate software** installed within the organization, such as launching atypical processes; creating files; modifying the file system or registry, which is typical for persistence-gaining techniques; and so on.

ACCESS MARKET OUTLOOK

Over the past 12 months, the number of access offers on the market has tripled, while in dollar terms the market size has increased by only 14%. Group-IB Threat Intelligence experts believe that this situation is the result of a steep rise in the number of IABs (which has also tripled year after year), increasing competitive pressures. When a hacker lacks the skills to gain persistence in a network or when access is used improperly, access to that network may be lost. In such cases, threat actors may try to sell network access as quickly as possible and accept a price below the market value. To do so, hackers often reduce their price to a few hundred US dollars, which practically guarantees that they will close the sale. The trend is likely to reduce the price of access credentials in the future, which should make them an even more attractive commodity.

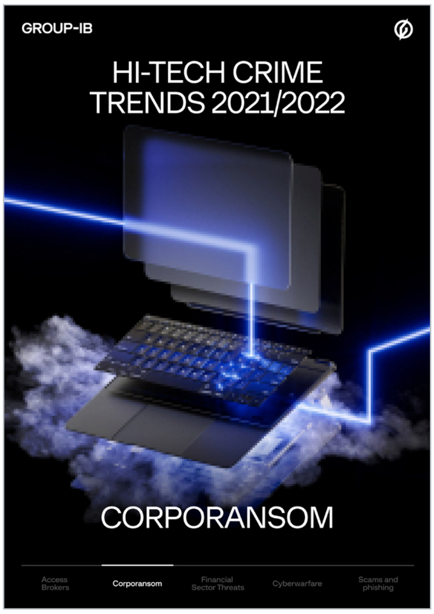
There seems to be a direct correlation between access value and the victim company's revenue: the higher the revenue, the higher the price, which makes large multinationals especially vulnerable to attacks. Unless steps are taken to secure a corporate network, it is probable that it will eventually become compromised, potentially causing substantial damage to the company's business.

The popularity of the access credentials market largely depends on the popularity of ransomware. Group-IB experts have concluded that many ransomware operators have been actively using (and are possibly still using) the services of popular IABs, thereby increasing demand for illicitly obtained access credentials on the dark web. According to the Group-IB report entitled **Corporansom**, the trend of ransomware being increasingly used should continue, resulting in a rising number of attacks on businesses worldwide.

RaaS is currently the main avenue for monetizing access to corporate networks. Increased demand for ransomware should also encourage new threat actors to enter the access market, which would further increase the overall number of IABs.

Robust growth in the initial access market gradually helped brokers reach a common understanding of their roles and a shared concept of their businesses. In turn, this mutual understanding helped determine initial access pricing and informed IABs how popular specific target countries were with the buyers. Hackers will likely remain most interested in obtaining access to companies based in the US, the Middle East, and the APAC region, while interest in the former Soviet Union and Africa should remain low or decline.

Corporansom



GROUP-IB

HI-TECH CRIME TRENDS 2021/2022

CORPORANSOM

Access Brokers | Corporansom | Financial Sector Threats | Cyberwarfare | Scams and phishing

Concealing certain data in their ads is how hackers have reacted to the efforts of threat researchers who warn companies that access to their network is for sale on the dark web. Given that the market has been active for years, the most influential IABs are likely to have regular clients to whom they can sell access credentials directly, thereby bypassing the forums. Hackers are also likely to create dedicated private dark-web resources for selling access credentials.

Our final forecast is the emergence of new access points to corporate networks. These could be new remote access and virtualization solutions, computer network building platforms, cloud services, or products already available on the market. All of them could have vulnerabilities enabling easy access from devices with older software missing essential updates, as was the case with Citrix, FortiGate, and Pulse Secure.

As an example, businesses are increasingly shifting to using SSO with cloud single sign on accounts, so it is reasonable to assume that it might become the new vector for attacks as hackers gain access to apps and services available through this solution.

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

Moscow
Amsterdam
Dubai
Singapore

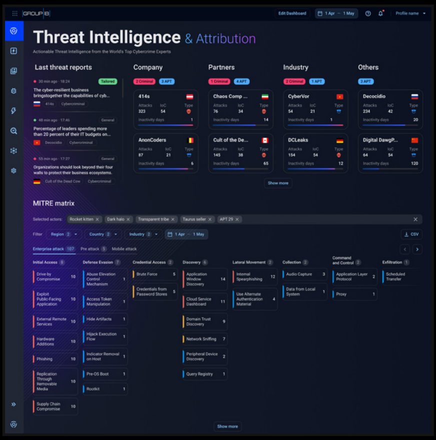
- Europe
- Russia
- Middle East
- Asia-Pacific

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.

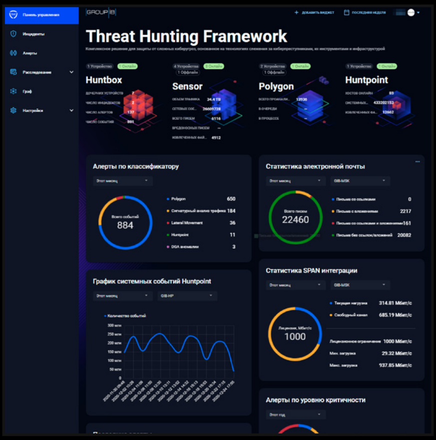
Group-IB's technologies are recognized by the world's leading research agencies

IDC · Gartner · Forrester · KuppingerCole Analysts · Frost & Sullivan



Threat Intelligence & Attribution

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

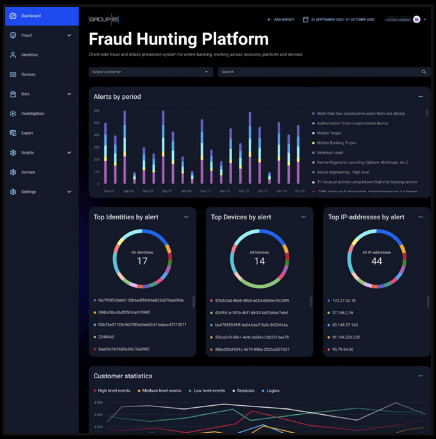


Threat Hunting Framework

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

18 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 +7 495 984 3364