

JUNE 2020
GROUP-IB.COM

|GROUP|IB|



Nickname:
Compromises co
and sells access
ms: more than 135
44
Per
ed damage: at lea
nickname: Fxms
omises compa
and sells access to the
Victims: more than 135
Per

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.

PROFILE

NICKNAME | **Fxmsp**

ACTIVITY | **COMPROMISES COMPANY NETWORKS AND SELLS ACCESS TO THEM**

VICTIMS | **MORE THAN 135 COMPANIES**

GEOGRAPHICAL SCOPE | **44 COUNTRIES**

PERIOD OF ACTIVITY | **3+ YEARS**

TOTAL EARNINGS | **AT LEAST \$1.5 MILLION**

TABLE OF CONTENTS

INTRODUCTION	4
KEY FINDINGS	5
EVOLUTION STAGES	5
VICTIM PORTFOLIO: GEOGRAPHICAL SCOPE AND INDUSTRIES	6
TIMELINE OF ACTIVITIES ON UNDERGROUND FORUMS	8
TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)	8
FIRST STEPS IN THE UNDERGROUND	10
EXPANSION OF ACTIVITY: PRESENCE ON NEW UNDERGROUND FORUMS	16
EXPLOIT[.]IN AND THE FIRST ADS FOR THE SALE OF ACCESS TO COMPROMISED NETWORKS	19
EPISODE I: COLLABORATION WITH LAMPEDUZA	27
EPISODE II: THE PHANTOM MENACE	35
THE FINAL STRAIGHT: END OF Fxmosp's OPERATIONS	36
Fxmosp's PRESUMED IDENTITY: DEANONYMIZATION STAGES	37
RECOMMENDATIONS	44
APPENDIX 1. LIST OF COMPANIES COMPROMISED BY Fxmosp TO WHICH HE AND HIS ACCOMPLICE SOLD ACCESS*	-

Register for a free product tour to test drive all the benefits of Group-IB Threat Intelligence, an advanced framework for attack attribution and protection against threat actors targeting your industry, country & company by contacting us through intelligence@group-ib.com

*The appendix is available in full version only.

INTRODUCTION

In October 2017, an advert was posted on one of the most popular Russian-speaking underground forums, exploit[.]in. The ad was for the sale of access to corporate networks belonging to various companies — a rare underground service at the time. For the first time, a user with an unusual nickname was offering access to all critically important network segments of compromised organizations and announced that a bank was among his victims, which back then was a unique lot.

Продаю доступы к корп сетям. Каскадный · [Стандартный] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

Fxmosp 1.10.2017, 17:35 Отправлено 2

Продаю доступы к различным корпоративным сетям...
 Доступы к серверам и их админкам... Логины всех админок внутри сети, к почтовым серверам, к базам итд...
 В каждой корп сети есть доступы к их порталам, базам данных, к активити директории итд...
 Списки пополняются постоянно...
 Примеры - банк в африке, ██████████, страховые компании крупные, итд...

мегабайт
 ■■■■

Группа: Пользователь
 Сообщений: 51
 Регистрация: 11.06.2017
 Пользователь №: 80 141
 Деятельность: другое

Репутация: 2
 - (0% - хорошо) +

Минимальная цена за доступ к сети 100 уе. (небольшие компании)
 Все остальные вопросы в личку....

Еще есть дедики стабильные - под
 Майнинг
 Брут
 Скан

Сообщение отредактировал Fxmosp - 2.10.2017, 13:35



Selling access to corporate networks	
Fxmosp	10/1/2017 17:35
megabyte ■■■■	I'm selling access to various corporate networks... Access to servers and their administration panels...Logins for all admin panels in the network, mail servers, databases, etc. For each corporate network, I have access to their portals, databases, Active Directory, etc. The list is being updated continuously... Examples: a bank in Africa, ██████████ major insurance companies, etc.
Group: User Messages: 51 Registration: 06/11/2017 Activity: Other Reputation: 2 - (0% - good) +	The minimum price for network access is \$100 (small companies) PM if you have any questions... I also have stable dedicated servers for Mining Brute-force Scanning
	The message was edited by Fxmosp on 10/02/2017, 13:35

Figure 1 - October 2017. Screenshot of the ad selling access to corporate networks*

The day of October 1, 2017 marked the “birthday” of **Fxmosp** as one of the most famous sellers of access to company networks on underground forums. But his name gained worldwide fame in May 2019, after it was reported that secure networks belonging to three leading antivirus software companies had been compromised. Fxmosp had gained access to fragments of the antivirus software source code, analytical modules, design documents, etc. The lot, according to media reports, was offered for \$300,000. Fxmosp wrote that he had carried out a targeted attack. In just over three years, Fxmosp went from being an ordinary user of a hacker forum who didn't know what to do with the companies to which he'd gained access and who was looking for like-minded individuals to one of

*Hereinafter screenshots from Russian-language underground forums will be provided together with a translation into English.

** <https://www.bleepingcomputer.com/news/security/fxmosp-chat-logs-reveal-the-hacked-antivirus-vendors-avs-respond/>

the major players of the Russian-speaking underground. Fxmsp soon acquired a loyal customer base and appointed a dedicated sales manager.

By the time that the scandalous news about the hacking of three antivirus vendors came to light, Fxmsp had ended all public activity. The most prolific seller of access remains at large, however, and poses a threat to companies in many industries, regardless of their location. In light of this, Group-IB Threat Intelligence experts decided to release this report, share its expanded version with international law enforcement agencies, and make our materials on Fxmsp's tools and tactics accessible to the general public.

KEY FINDINGS

EVOLUTION STAGES

Group-IB's Threat Intelligence specialists analyzed Fxmsp's activity in the Russian-speaking underground from the moment he registered on the first forum in September 2016 to late 2019, when he ceased all public activity. Fxmsp's activities involving the sale of access to corporate networks can be divided into three stages, which are described in the table below:



VICTIM PORTFOLIO: GEOGRAPHICAL SCOPE AND INDUSTRIES

In just over three years, Fxmsp managed to gain access to corporate networks of companies based in more than 44 countries. According to Group-IB Threat Intelligence specialists' estimates, Fxmsp is likely to have made at least 1.5 million dollars throughout his activity. This does not include the 20% of companies to which he offered access without naming the price and the sales he made through private messages.

Fxmsp did not focus on compromising a particular industry and targeted major banks and hotel chains as well as small websites belonging to schools.

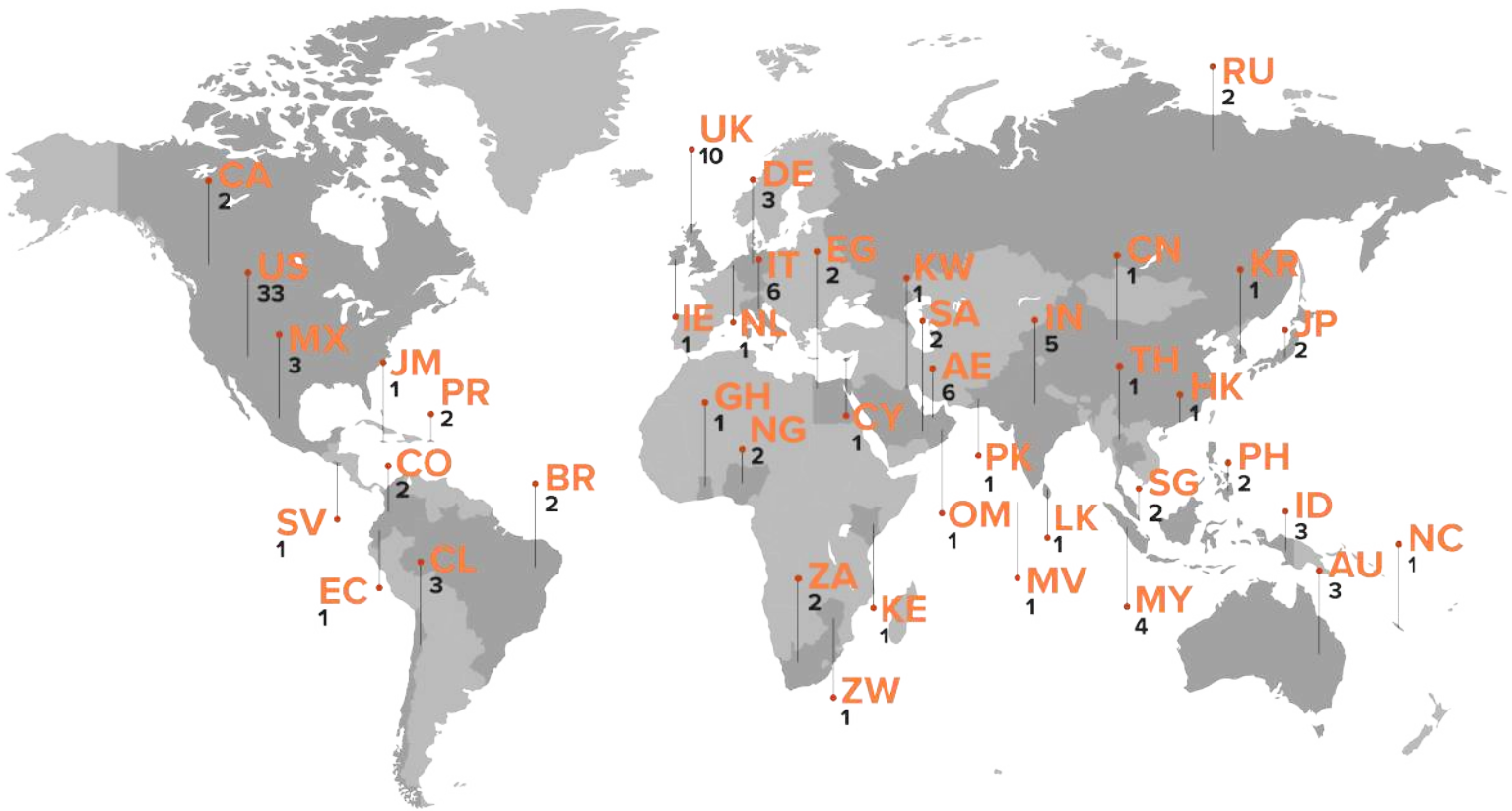


Figure 2 - Geographical distribution of Fxmsp's victims

*The map doesn't include international companies operating in different countries (5) and the companies access to which Fxmsp was selling without specifying their location (8).

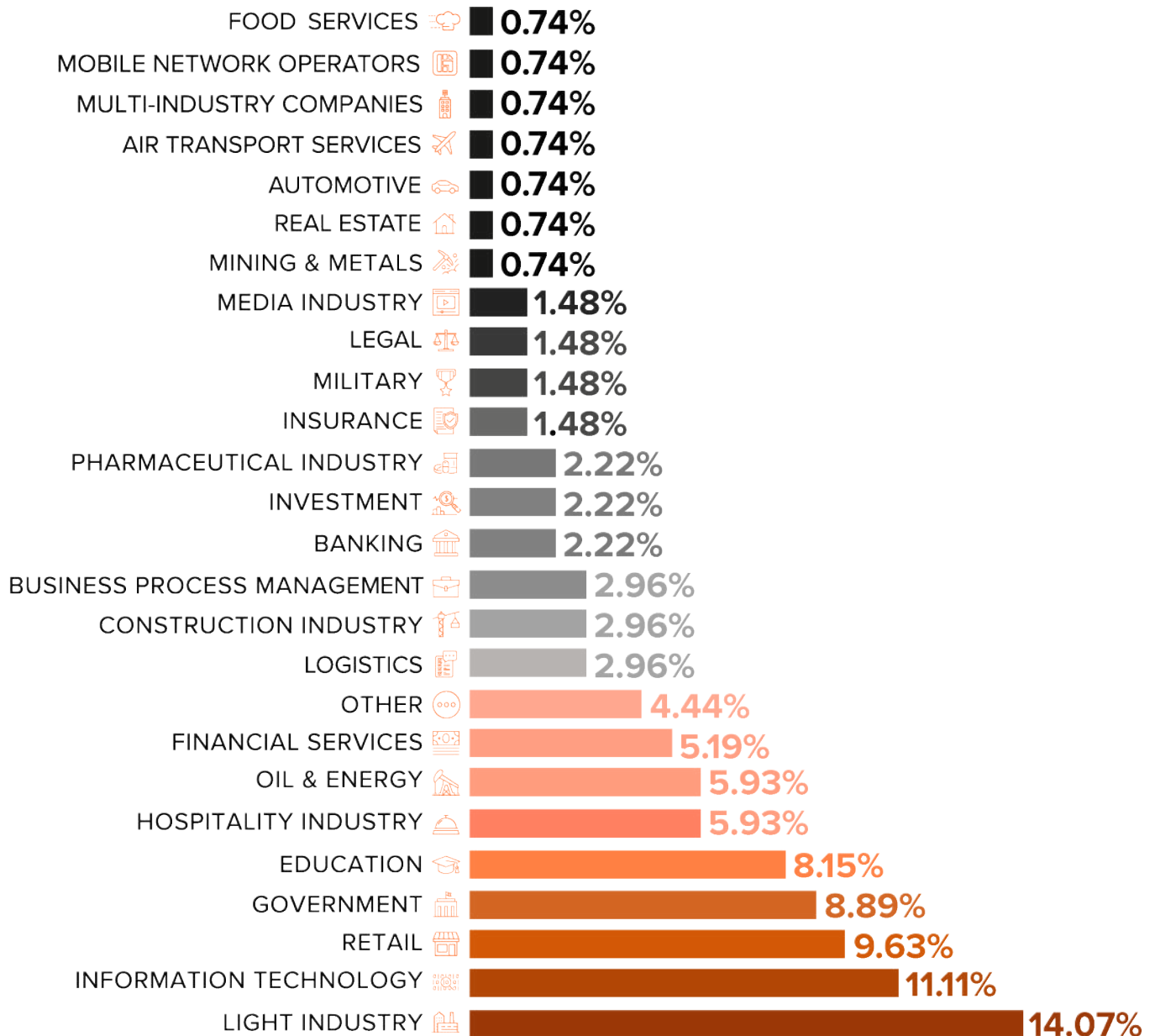


Figure 3 - Distribution of Fxmsp's victims by industry

As seen from Fig. 3, Fxmsp's victims were mainly companies in the light industry, i.e. focused on small production of consumer goods. His second most common targets were companies offering IT services. Retail businesses came third. Interestingly, around 9% of victim networks belonged to state-owned companies.

Four companies attacked by Fxmsp were included in the Fortune Global 500 ranking in 2019.

TIMELINE OF ACTIVITIES ON UNDERGROUND FORUMS

Fxmsp was most active from October 2017 to September 2019. In that time, he publicly advertised the sale of access to corporate networks belonging to 135 companies. The timeline of his posts on underground forums is shown below:

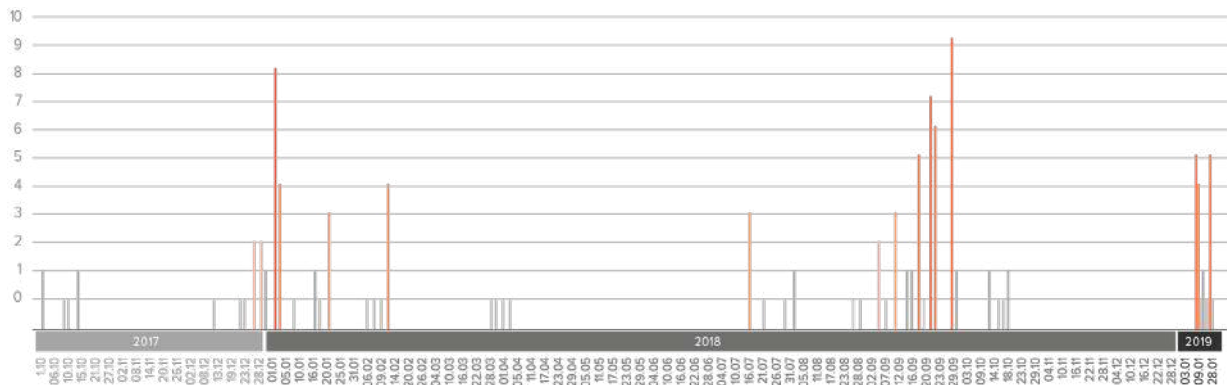


Figure 4 - Timeline of posts advertising the sale of accesses to compromised networks on underground forums

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

Unlike most cybercriminals, Fxmsp does not use spear-phishing, nor does he study his victims before the attacks. This fact indicates that his attacks are mass rather than targeted. Nevertheless, the threat actor successfully gains access to networks belonging to large companies. The main stages of Fxmsp's attacks are presented below:

- 1. Scanning of certain IP ranges.** Fxmsp uses a relatively common yet simple approach. He scans a range of IP addresses (within a city or a country) for certain open ports. Based on the cybercriminal's messages posted on underground forums, to do so he uses a popular software called **Masscan** as well as more advanced scanners. The main goal of IP addresses scanning is to identify open **RDP (remote desktop protocol)** ports, particularly 3389. The latter is used to provide remote access to Windows servers and workstations.
- 2. Attack preparation.** After scanning the range of IP addresses and identifying potential victims with open RDP ports, Fxmsp must reduce the amount of input data for brute-force attacks. To this end, he usually uses any programs with the name **RDP Recognizer**. On most remote Windows-based servers, the login screen can be seen together with a list of all accounts on the server. The application in question uses OCR (Optical Character Recognition) to recognize the login details of all accounts on the server. If login details are successfully recognized, the attacker needs only to brute-force passwords.
- 3. Brute-force attacks.** Next, the threat actor uses various programs to carry out brute-force attacks on the victim's server. Brute-force attacks are attempts to guess the RDP password by systematically sorting through all the possible options until the correct one is found. As part of the process, Fxmsp tries possible combinations of characters and searches dictionaries for commonly used or compromised passwords.

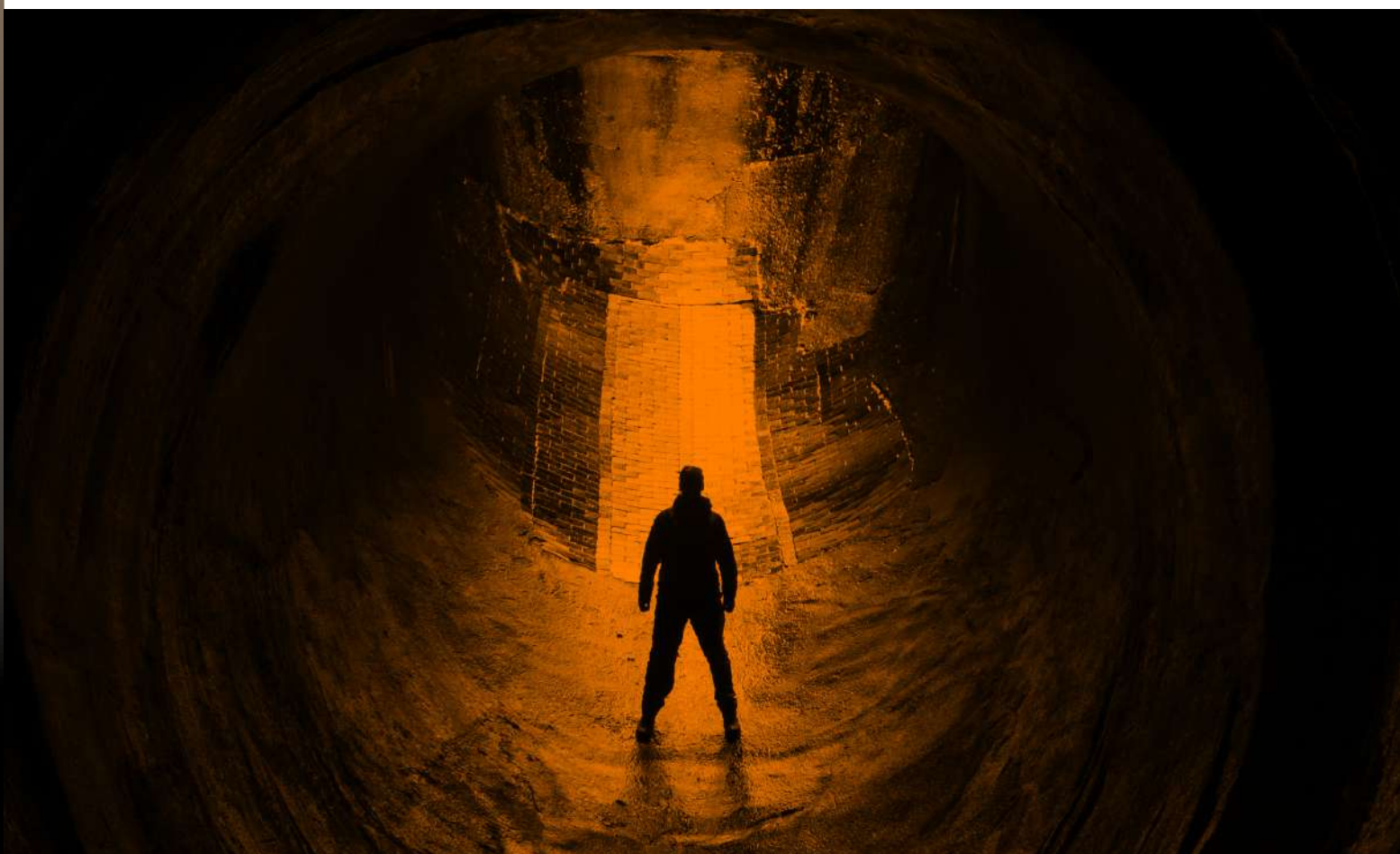
4. Persistence. After gaining access to the target device, Fxmsp usually disables the existing anti-virus software and firewall, then creates additional accounts. Next, he achieves persistence on the network. Given that in 2017 he was interested in working with Metasploit PRO, we can assume that he uses the **Meterpreter** payload on servers as a backdoor. Fxmsp himself noted in his posts that, when installing backdoors, he set a long interval for connections with C&C servers: once every 15 days.

5. Network reconnaissance. After ensuring persistence on an individual device, Fxmsp continues to explore the network. His next goal is to gain access to the domain controller. We can assume that he was looking for accounts with administrative privileges, which would make it easy to access data of interest. Fxmsp then harvests dumps of all the accounts and attempts to decrypt them. We know that he used **Windows Password Recovery** for decryption on at least one occasion. This tool automatically downloads user databases from SAM or ntds.dit and decrypts hashed passwords.

6. Compromise of backup servers. The cybercriminal's next step is to infect backups. As in the case of the original server, Fxmsp installs backdoors on backups with long intervals. This means that even if the victim notices suspicious activity in the system, they will most likely change passwords and perform a rollback to the backup, which has already been compromised.

7. Monetization. At the main stage of his activity, Fxmsp was selling accesses on underground forums, first on his own, then with the help of his accomplice, **Lampeduza**. At the earlier stages, he installed cryptocurrency mining malware on compromised servers.

Throughout Fxmsp's activity, Group-IB specialists monitored how his attacks evolved by analyzing dozens of his posts. These efforts helped determine the type of tools he used to compromise company networks and establish the exact number of victims and his presumed identity with a high degree of probability. The report ends with a list of **recommendations** to help companies protect against the types of attacks conducted by Fxmsp and similar cybercriminals.



FIRST STEPS IN THE UNDERGROUND

In September 2016, a user with the nickname **Fxmsp** first registered on a hacker forum that was popular at the time, fuckav[.]ru (hxxps://fuckav[.]ru/member.php?u=36898).

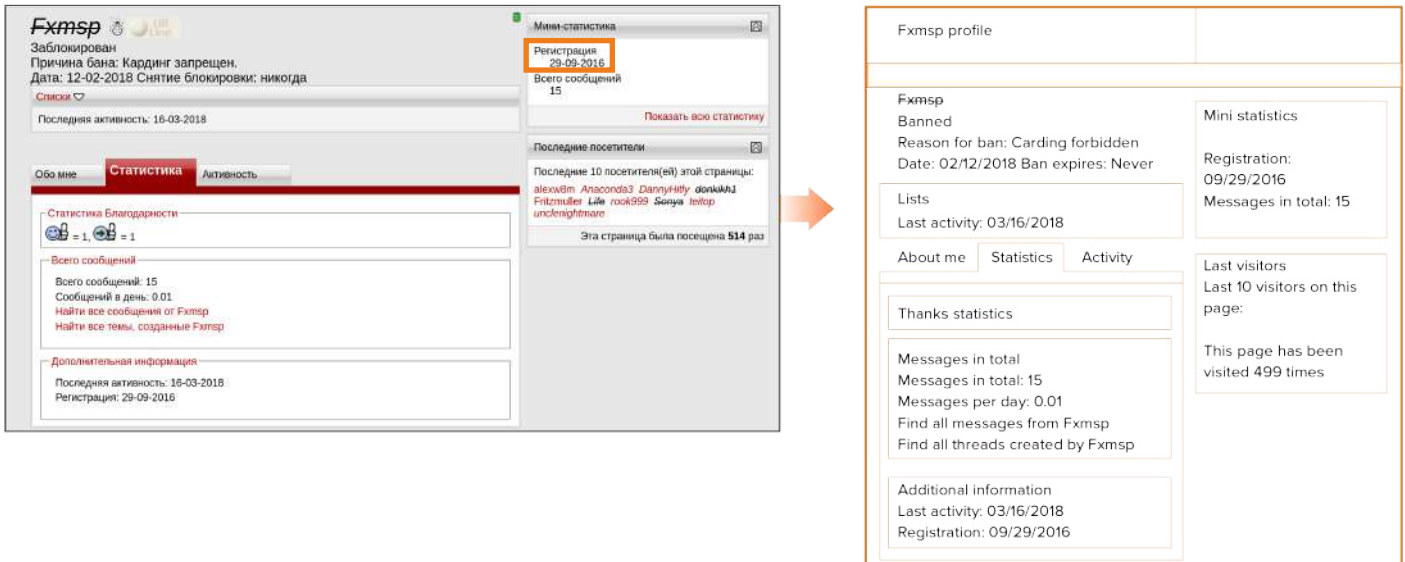


Figure 5 - Screenshot of Fxmisp's user account on fuckav[.]ru. Registration date: September 2016

According to [Group-IB's attribution-based Threat Intelligence](#), Fxmisp was rarely active in the first two months since joining the forum in September 2016, instead likely reading entries and occasionally leaving comments on posts made by other forum users in order to gain experience and find like-minded individuals.

It is highly likely that Fxmisp had already successfully hacked into many corporate networks by that point. He did not know how to monetize the access he had gained, however. He followed a relatively straight-line path. Instead of selling accesses, Fxmisp decided to use the resources belonging to compromised companies to mine cryptocurrency. On November 11, 2016, the cybercriminal wrote his first post about looking for self-propagating persistent cryptomining malware (hxxps://fuckav[.]ru/showthread.php?t=30798).



Figure 6 - November 2016. Screenshot of the post about looking for cryptomining malware

In answer to his question, Fxmsp received a rude reply from another user who was better known at the time, with the nickname **fred**, who told Fxmsp to get to the point instead of asking stupid questions. This is standard practice on underground forums. Individuals who frequent them are not keen on answering questions from newbies and teaching potential competitors.

Soon thereafter, Fxmsp started testing the infamous banking Trojan called Atmos, which was making the cyber rounds at the time.

Atmos is a version of malware called Citadel, which is based on the Trojan Zeus. The malware steals banking data through form grabbers and web injects (it supports Zeus injects). It also intercepts card data from GET and POST requests and has an ATS function. The Trojan has a VNC module, which provides a remote connection to the victim's computer. The Trojan also uses keyloggers/webloggers and a module for stealing files from the victim's device. Apart from that, the Trojan has many other additional functions. In June 2016, its source codes were shared in a public forum.

Usually when hackers take their first steps in the world of cybercrime, they do not think about the fact that they're leaving a digital trail that could lead to their identity being uncovered in the future. This is exactly what happened to Fxmsp. He included his Jabber account, `fxmsp@fuckav[.]ru`, in his contact information on the forum. Experienced users of underground forums never publish their contact details; they share them only through private messages.

Toward late November that year, Fxmsp published his last post before taking a long break. The post was about looking for self-propagating persistent malware for infecting networks.

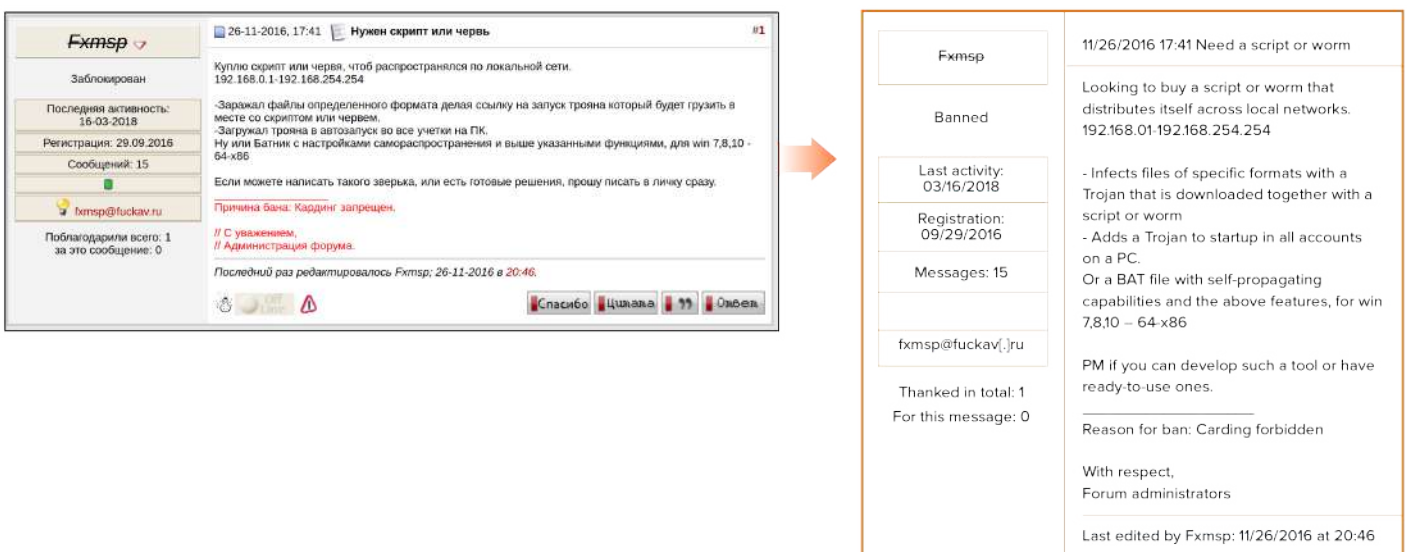


Figure 7 - November 2016. Screenshot of the post about looking for self-propagating malware

Nobody commented on Fxmsp's post, at which point he probably understood that it was pointless to look for cryptomining malware on public forums.

For the next six months, Fxmsp was not active on any forums. In all likelihood, he continued to attack corporate networks, however. The next posts shared by the user with the nickname Fxmsp did not appear until May 2017. In his newest post, Fxmsp explained that he had gained partial access to a large network that was divided into three administrative zones. He said he had managed to gain RDP access to a number of devices.

Fxmsp

Заблокирован

Последняя активность: 16-03-2018

Регистрация: 29.09.2016

Сообщений: 15

fxmsp@fuckav.ru

Поблагодарили всего: 1
за это сообщение: 0

11-05-2017, 07:48 Re: [БЕСПЛАТНО] Консультации от sweetMika7, задавай вопрос = получи ответ #185

Доброго дня!
Помогите разобраться с методом
Имеется более 6000 хороших серверов дедиков от крупного хостинг провайдера
900 из них 24 ядровые
У меня есть доступ к 20 серверам по RDP но всех их объединяют 3 административных логина
ArAdmin - нет доступа
ArAdministrator - нет доступа
Bradmin - нет доступа

Но есть и другие с разными паролями админки рдп на данных серверах - подобрать пароль не получается к первым трем админкам чтоб сразу получить доступ к 900 серверам

Доступ на 20 серверов имею, не помогло узнать пароль через кейлоггер, через всякие там рековори, подбор троянов на почту к данным админам (через кейлоггер узнал их почтовые адреса), перепробовал все что можно, перебрал более 1 500 000 паролей, но так и не могу найти данный пароль к

ArAdmin
ArAdministrator
Bradmin

Можно ли как то вытащить данные пароли от учетки этих трех админок из самой винды на сервере? Либо может есть какой то другой способ вытащить из них пароли? Буду очень благодарен за ранее!

Причина бана: Кардинг запрещен.

// С уважением,
// Администрация форума.

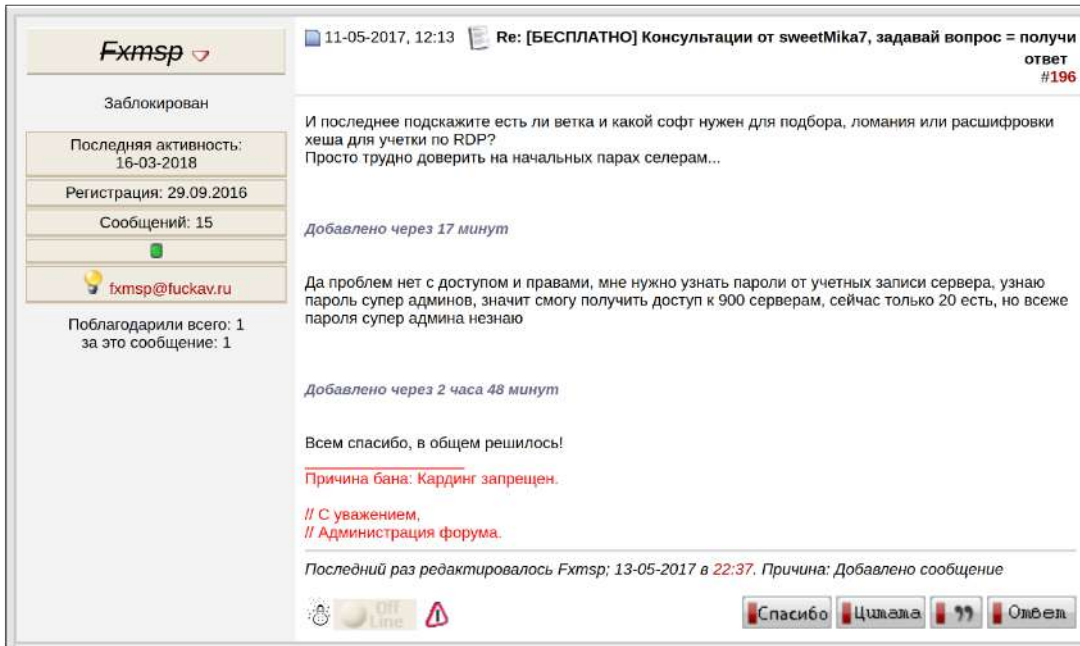


Fxmsp	05/11/2017 07:48 Re: [FREE] Consultations from sweetMika7, ask a question = receive an answer
Banned	Hello! Help me understand a technique There are 6,000+ good dedicated servers relating to a large hosting provider 900 of them have 24 cores I have access to 20 servers through RDP, but they all have 3 common admin logins ArAdmin – no access ArAdministrator – no access Bradmin – no access
Last activity: 03/16/2018	
Registration: 09/29/2016	
Messages: 15	But I also have other RDP administration panels with different passwords on the above servers. I need to find passwords for the first three administration panels to obtain access to 900 servers simultaneously
fxmsp@fuckav[.]ru	I have access to 20 servers; Keylogger did not help with getting the passwords. I attempted to use password recovery functions, sent infected emails to the administrators in question (the keylogger helped find their email addresses), tried everything I could, brute-forced over 1,500,000 passwords, but was unable to find the required passwords for
Thanked in total: 1 For this message: 0	ArAdmin ArAdministrator Bradmin
	Is it possible to retrieve these passwords from the Windows OS on the server? Or maybe there is another option to exfiltrate passwords? I will be grateful for any help!
	Reason for ban: Carding forbidden
	With respect, Forum administrators

Figure 8 - May 2017. Screenshot of the post about gaining partial access to a large network

Fxmsp understood that brute-force attacks on all 6,000 servers would be pointless, so he once again turned for help to the users of the underground forum. His main goal was to gain access to user accounts of domain administrators. In answer to his appeal, other users recommended going on exploit[.]in, where he could potentially find specialists with the skills to hack password hashes stored in SAM (Security Account Manager) databases.

It is interesting that on the very same day, May 11, 2017, five hours after his first post, Fxmsp announced that his problem had been solved.



Fxmsp	05/11/2017 12:13 Re: [FREE] Consultations from sweetMika7, ask a question = receive an answer
Banned	And lastly, is there a thread and what software is required to brute-force, crack or decrypt a hash for an account via RDP? It's just that it's hard to trust sellers in the beginning...
Last activity: 03/16/2018	Added after 17 minutes
Registration: 09/29/2016	I don't have any issues with access or privileges. I only need to know passwords for server accounts. If I obtain super admin passwords, I will gain access to 900 servers. For now, I have access to only 20 but I don't have the super admin passwords.
Messages: 15	Added after 2 hours 48 minutes
fxmsp@fuckav[.]ru	Thanks everyone. The problem has been solved!
Thanked in total: 1 For this message: 0	Reason for ban: Carding forbidden
	With respect,

Figure 9 - May 2017. Screenshot of the post about gaining partial access to a large network

Further research revealed that the post in question had been edited. Group-IB's attribution-based Threat Intelligence system makes it possible to monitor all posts on underground forums in real time and gain access to both original posts and all edit history. As such, it was possible to identify one of the tools used by the cybercriminal to conduct attacks on corporate networks: Windows Password Recovery. The latter automatically downloads user information from SAM databases or ntds.dit and decrypts hashed passwords. In Fxmsp's own words, he was able to decrypt the passwords for 90% of accounts thanks to the latest version of the program.

11.05.2017 15:13 (fuckav.ru)	[БЕСПЛАТНО] Консультации от sweetMika7, задай вопрос = получи ответ	Fxmsp	И последнее подскажите есть ли ветка и какой софт нужен для п одбора, ломания или расшифровки хеша для учетки по RDP? Просто трудно доверять на начальных парах селерам... Добавлено через 17 минут Да проблем нет с доступом и правами, мне нужно узнать пароли от учетных записи сервера, узнаю пароль супер админов, значит смогу получить доступ к 900 серверам, сейчас только 20 есть, но все же пароля супер админа незнаю Добавлено через 2 часа 48 минут Всем спасибо, в общем решилось все последней версией Windows Password Recovery, вытаскивает 90% акаунтов все что мне нужн о было я получил!!!!!!))))))
------------------------------------	---	-------	--



05/11/2017 15:13 (fuckav[,ru)	[FREE] Consultations from sweetMika7, ask a question = receive an answer	Fxmsp	And lastly, is there a thread and what software is required to brute-force, crack or decrypt a hash for an account via RDP? It's just that it's hard to trust sellers in the beginning... Added after 17 minutes I don't have any issues with access or privileges. I only need to know passwords for server accounts. If I obtain super admin passwords, I will gain access to 900 servers. For now, I have access to only 20 but I don't have the super admin passwords. Added after 2 hours 48 minutes Thanks everyone. The problem has been solved thanks to Windows Password Recovery. It retrieves passwords for 90% of accounts. I got everything I needed!!!!!!))))))
-------------------------------------	---	-------	---

Figure 10 - May 2017. Screenshot of the post describing how the hacker managed to obtain account passwords

In June 2017, the cybercriminal decided to try new ways of compromising networks and began working with a popular pentest software called Metasploit PRO. Fxmsp shared a post on the same forum saying that he was looking for people ready to help him with the malware or join his team on a permanent basis:

<p>Fxmsp </p> <p>Заблокирован</p> <p>Последняя активность: 16-03-2018</p> <p>Регистрация: 29.09.2016</p> <p>Сообщений: 15</p> <p></p> <p> fxmsp@fuckav.ru</p> <p>Поблагодарили всего: 1 за это сообщение: 0</p>		<p>01-06-2017, 18:38 Нужна помощь или платная консультация по Metasploit Pro #1</p> <p>Нужно помочь с Metasploit Pro под windows, немного обучить руководство пользования, это нужно для того чтоб понять стоит ли пользоваться данным ПО по отношению к серверам в сети, есть большая группа серверов на просторах сети , нужно получить доступ к данным серверам, платформа серверов windows 2008-2012 дата центр. Возможны и другие варианты использования другого эффективного ПО или методов с применением эксплойтов. Также если есть возможность то можно сотрудничать на постоянной основе, (платно) - постоянные консультации.</p> <p>Причина бана: Кардинг запрещен.</p> <p>// С уважением, // Администрация форума.</p> <p> </p>
--	--	--



<p>Fxmsp</p> <p>Banned</p> <p>Last activity: 03/16/2018</p> <p>Registration: 09/29/2016</p> <p>Messages: 15</p> <p>fxmsp@fuckav[,ru</p> <p>Thanked in total: 1 For this message: 0</p>	<p>06/01/2017 18:38 Need your help or paid consultation on Metasploit Pro</p> <p>I need help with Metasploit Pro for Windows, discuss its user manual. I need this to understand whether it's worth using this software for servers in the network. I need to gain access to these servers, Windows 2008-2012 server platform, data center. It is possible to use other effective software or techniques using exploits. Also, we could work together on a permanent basis (paid) – permanent consultations.</p> <p>Reason for ban: Carding forbidden</p> <p>With respect, Forum administrators</p>
--	---

Figure 11 - June 2017. Screenshot of the post about looking for help with Metasploit PRO

The cybercriminal's activity on even one underground forum helps understand his interests and goals. Group-IB specialists were able to recover the contact details that Fxmsp shared at the start of his activity:

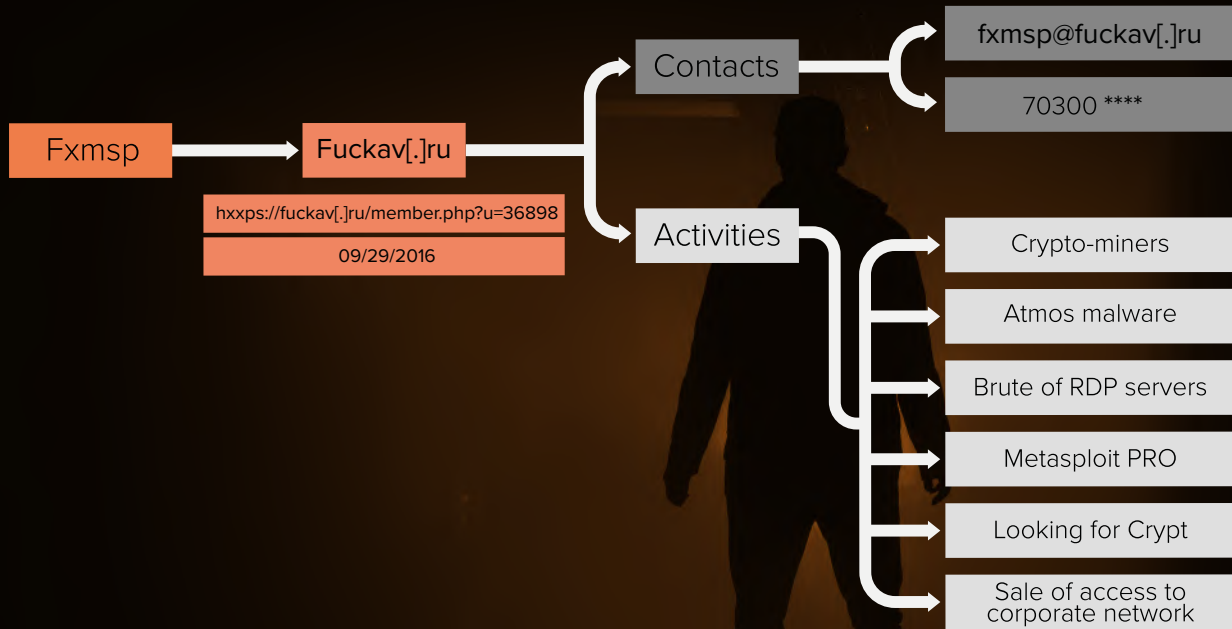
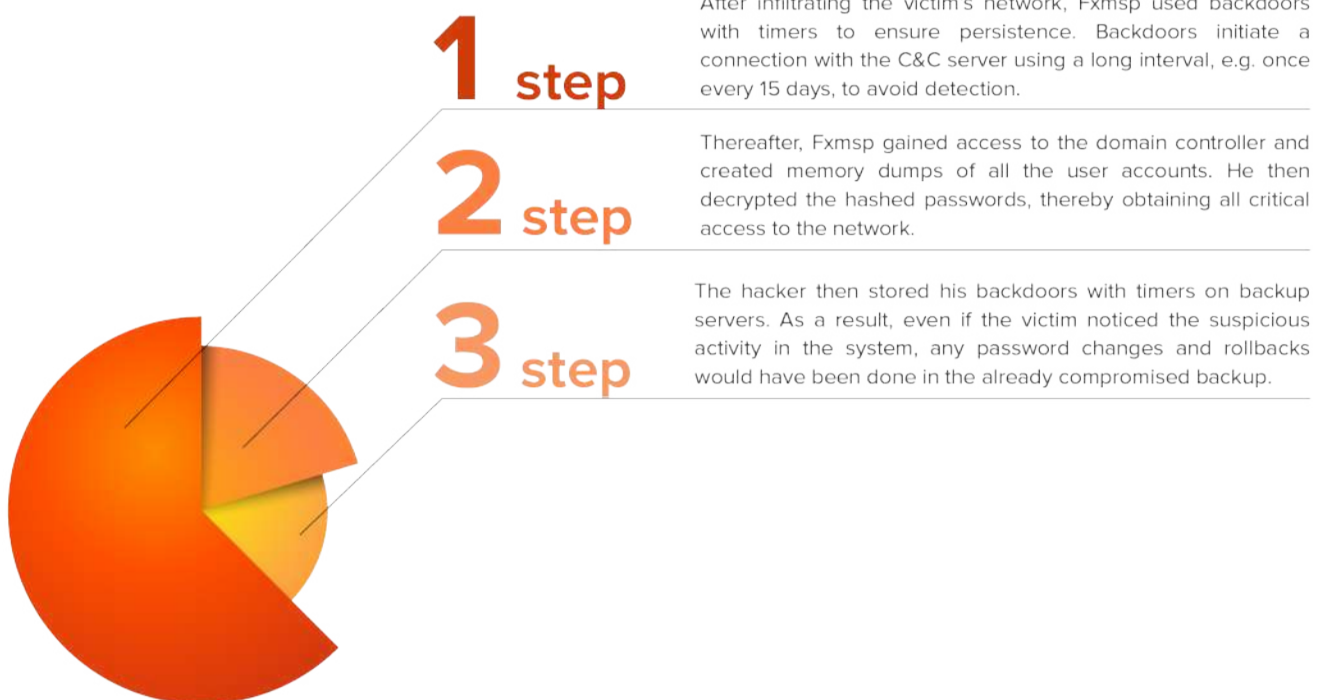


Figure 12 - Analysis of Fxmsp's hacker activity based on fuckav[.]ru forum data

While investigating Fxmsp's activity on fuckav[.]ru, Group-IB specialists identified the tools he used to achieve persistence in systems:



EXPANSION OF ACTIVITY: PRESENCE ON NEW UNDERGROUND FORUMS

In early June 2017, Fxmsp's activity on fuckav[.]ru slowed down. At the same time, Group-IB experts discovered that users with that very nickname were registering on other hacker platforms:

June 6

an account under the name Fxmsp appeared on the forum **proxy-base[.]com**

[https://proxy-base\[.\]com/members/fxmsp/](https://proxy-base[.]com/members/fxmsp/)

June 8

an account under the name Fxmsp was registered on the platform **lolzteam[.]net**

[https://lolzteam\[.\]net/members/125112/](https://lolzteam[.]net/members/125112/)

June 11

an account under the name Fxmsp was registered on the forum **exploit[.]in**

[https://forum.exploit\[.\]in/index.php?showuser=80141](https://forum.exploit[.]in/index.php?showuser=80141)

The image shows a user profile for 'Fxmsp' on an underground forum. The profile includes a header with the name 'Fxmsp', HTTP status, and status 'Dct, eltn!'. It also shows the last activity date and time: '14.02.2018 15:08'. A 'Мини-статистика' (Mini statistics) section displays registration date '06.06.2017' and total messages '3'. Below this is a section for 'Fxmsp' with a 'joined' date of 'Jun 8, 2017' and options to 'Find all threads by Fxmsp' and 'View accounts on market'. A 'Войдите, чтобы написать' (Log in to write) button is visible. At the bottom, there is a 'BANNED' status and a table of user statistics.

CONTENT COUNT	JOINED	MEMBER ID	LAST VISITED
64	June 11, 2017	80141	October 23, 2018

An arrow points from the profile to a 'Mini statistics' table:

Mini statistics	
Fxmsp offline	Registration
HTTP	06/06/2017
Status: Dct, eltn!	Messages in total:
	3
Last activity: 02/14/2018 15:08	Show all statistics

Figure 13 - June 2017. Fxmsp user account on other underground forums

The day after joining proxy-base[.]com, Fxmsp posted another message in which he wrote that he had managed to obtain access to a huge network of 1.5 million devices. By further scanning networks for unsecured RDP (remote desktop protocol) ports, Fxmsp found 230,000 devices with an open port 3389.

Fxmisp: The invisible god of networks

07.06.2017, 19:09
1 (детали)

Fxmisp
 HTTP
 Статус: Dct, elnt!

Регистрация: 06.06.2017
 Сообщений: 3
 Member ID: 36559

Репутация: 3
 Скавал(а) спасибо: 0
 Поблагодарили 1 раз в 1 сообщении

Помощь - 230 000 дедеков в локальной сети

Всем доброго!

Столкнулся с такой проблемой, или как сказать с вопросом, при brute дедеков наткнулся на локальную сеть в 1,500 000 мил ПС и 230 000 рдл в данной сети по порту 3389, вопрос брут в такой сети очень тнкий оказался - стандартными средствами не получается вытащить из локалки логины, всего 100 вытащил из 230 тыс. Хотел попробовать metasploit Pro - но понял это калец - 230 тыс проверить пару лет буду, а суть заключается в том, что я на данный момент не представляю чем и как взять и долбануть хотя бы 10 000 под майнинг в этой локальной сети, через различные эксплойты без автоматизации мне не справиться с таким объемом, ну а раз попал в такую сеть, то тснит попробовать все возможности.

Что успев узнать о данной локалке: все ПС тем 2012 сервер дата центр с процессорами CPU: Intel(R) Xeon(R) CPU E5-2673 v3-6

Ктонибудь может помочь? какими средствами, ПО, сортом, методом можно одолеть такую огромную локальную сеть?

Проверил 139-445 порты всего 2000 набралось, smb там мертвые. Странно что в основном там открыт порты для управления 3389, проверял другие порты все отключено кроме некоторых служб для управления SQL баз, я так понял они- пока даже не знаю кто они создают деки пачками в день по 500 штук под сервера каким то компаниям, на одну компанию 8-12 серверов, все деды в usa. Перебирать пароли не помогает 10 дедов из этой сети, перебрал по админу и администратору логику 25 000 паролей если не больше, полный ноль (9 дедов всего)... я понял что там нет логинов таких как Админ и Админист...

Что касемо уязвимостей то не представляю чем можно просканировать такую сеть на уязвимости за пару дней - там сервисы которые работают точно phpMyAdmin, JBoss, Oracle Web Application Testing Suite, ElasticSearch, MSSQL, Apache Tomcat, Oracle Weblogic итд.. Но ходить по одному и сканив уже зашло, на один сервер уходит до 15 минут для проверки на уязв... а как проверить 230 000?

Еще немного о серверах, в основном там 4 типа сервера 2, 4 ядра, 8 ядра, 16 ядра

2 - дают при нагрузке в 60% 80 H/s на валюте монеро
 4 - дают при нагрузке в 60% 180 H/s на валюте монеро
 8 - дают при нагрузке в 60% 320 H/s
 16 - дают при нагрузке в 60% 572 H/s

При анализе выборки из 3000 дедов у всех одинаковые параметры и делаю предположение что все они один и те же по качеству майнинга, выборку делал через каждые 500 дедов.

На просторах интернета я еще не встречал таких серверов с такими качествами по майнингу не у Китая, не у европы, не у индии итд и все в одном месте. Китай обычно дает 400 H/s только на 32 ядрах, европа на 24 ядрах 400 дает, а тут 8 ядери дают под 450 на 95% нагрузке. Попадались как то 32 ядерные в индии 4 сервера давали 800-1200 H/s. Готов к сотрудничеству, партнерству..... Только разобраться с данной сетью очень хочется страшно, как уже выше писал их объединяет несколько вещей: общая локальная сеть, все окна 2012 дата центры, 3-4 систем баз данных и еще пара мелочей. Если добыть хорошей эксплойт и автоматизировано внедрятся на сервера, то будет не подчитать выгоды. И само собой часть добытых средств пойдет на нужды сообщества и разработки и покупки софта.

На двух форумах просил консультации очень известных, кончилиось тем что мне сказали не кто не будет не помогать и объяснять итп - так как конкурентов не кто не хочет. Немного обидно было, ну да ладно, не там, может здесь кто дельный совет даст.

Помогите - поддержите ПЖ!

Последний раз редактировалось Fxmisp, 07.06.2017 в 19:17. Причина: Дополнение

ЦИТАТА

<p>06/07/2017 16:09</p> <p>Fxmisp offline</p> <p>HTTP</p> <p>Status: Dct, elnt!</p> <p>Registration: 06/06/2017</p> <p>Messages: 3</p> <p>Member ID: 36559</p> <p>Reputation: 3</p> <p>Said thank you: 0</p> <p>Was thanked 1 in 1 message</p>	<p>Re: Help - 230,000 dedicated servers in a local network</p> <p>Hello!</p> <p>I am facing the following problem, or should I say question: when brute-forcing dedicated servers, I found a local network made up of 1.5 million devices and found 230,000 RDP devices with an open port 3389. It's difficult to brute-force in such networks: I cannot obtain passwords using typical tools in a local network. I was able to retrieve only 100,000 out of 230,000. I was going to use Metasploit PRO, but I realized that it would take years to check 230,000 accounts. I need to hack at least 10,000 machines for cryptomining in the local network. I cannot do this by using exploits only, without automation. And since I'm already inside the network, I want to try everything I can.</p> <p>What I was able to find out about the local network: all PCs have a 2012 server data center with the following processor: CPU Intel(R) Xeon(R) CPU E5-2673 v3-6</p> <p>Can anybody help? What tools, software, techniques can help take on this local network?</p> <p>I checked ports 139-445 and only 2,000 are available. SMB access is blocked. It's strange that ports 3389 are open. I checked the other ports and they are disabled except for a few services for SQL database management. As I understand it, they (I don't yet know who they are) create 500 dedicated servers per day for some companies. 8-12 dedicated servers per company. All the dedicated servers are in the US.</p> <p>Brute-forcing doesn't help. I checked 10 dedicated servers from the network. I tried 25,000 or more passwords for Admin and Administrator accounts, there was no effect (a total of nine dedicated servers). I realized that there were no such accounts there.</p> <p>As for vulnerabilities, I don't understand how I can scan such a network for vulnerabilities in two days. The following services work: phpMyAdmin, JBoss, Oracle Web Application Testing Suite, ElasticSearch, MSSQL, Apache Tomcat, Apache Tomcat, Oracle Weblogic, etc. It takes up to 15 minutes to check one server for vulnerabilities... how am I supposed to check 230,000?</p> <p>A little more about the servers. In general, there are four types of servers there: 2, 4, 8, and 16 cores.</p> <p>2 cores - with a 60% load, gets to 80 H/s for Monero 4 cores - with a 60% load, gets to 180 H/s for Monero 8 cores - with a 60% load, gets to 320 H/s 16 cores - with a 60% load, gets to 572 H/s</p> <p>I analyzed a sample of 3,000 servers; all of them had the above parameters. Based on the results, I can conclude that they all demonstrate the same efficiency for cryptocurrency mining. I selected every 500th dedicated server.</p> <p>I haven't seen servers with such mining efficiency anywhere on the Internet - not in China, not in India or Europe. And yet here they are all in a single location. In China, servers give 400 H/s only with 32 cores, European ones give 400 H/s with 24 cores. Here, an 8-core server gives about 450 H/s with a 95% load. I once saw four 32-core processors in India that gave 800-1,200 H/s. I'm ready for a partnership, to work together... I just need to get to grips with this network. As I said, the servers have several things in common: a common local network, Windows 2012 data center, 3-4 database systems and some other stuff. If we get a good exploit and automate server infiltration, we can make a lot of money.</p> <p>Of course, some of this money will be spent for the community's needs, and to develop and buy software.</p> <p>I requested consultations on two popular forums. Nobody wanted to help or explain because they didn't want to help potential competitors. Shame. Maybe someone will give some solid advice here.</p> <p>Please help!</p> <p>Last edited by Fxmisp: 06/07/2017. Reason: Added information</p>
--	---

Figure 14 - June 2017. Screenshot of the post about looking for help accessing a large network

It is worth pointing out Fxmisp's confusion. Having gained access to a compromised company, he had no intention of selling that access or using sensitive information in the network for the purpose of reselling it. His only goal was mining the cryptocurrency Monero and he was planning on using the compromised organization's server capacities to do so.

Two users — with the nicknames **zunbah** and **Kibergyry** — expressed their willingness to help.

17

It is worth noting another post from the same thread: in November 2017, Fxmsp was asked whether the above-mentioned plan had been successful and he replied that, thanks to the DNS (Domain Name System), he had managed to find out who the servers in question belonged to. He had then started checking the networks for specific vulnerabilities, which had helped him gain access to some of the servers, while compromised passwords had helped him access the rest.



11/06/2017 10:04	
Fxmsp offline	Re: Help – 230,000 dedicated servers in a local network
HTTP	
Status: Dct , eltn!	The situation is ongoing. Thanks to the server DNS names, I managed to find out who these dedicated servers belonged to. I then checked a few servers for vulnerabilities and gained access to some of the servers. I retrieved all the passwords from them, which helped me access the remaining 1,000 servers.
Registration: 06/06/2017	To go further, I need information about large data centers.
Messages: 3	For example, it is possible to quietly hack into IBM or Microsoft (Microsoft would be better)
Member ID: 36559	
Reputation: 3	
Said thank you: 0	
Was thanked 1 in 1 message	

Figure 15 - November 2017. Screenshot of the post about the possibility of hacking into networks belonging to IBM and Microsoft

Having found the solution quickly and convinced of his own success, Fxmsp started boasting and talking about hacking into IBM and Microsoft.



EXPLOIT[.]IN AND THE FIRST ADS FOR THE SALE OF ACCESS TO COMPROMISED NETWORKS

As mentioned above, in June 2017, Fxmsp registered his main account on exploit[.]in, where he re-focused his activity and began selling access to compromised corporate networks.

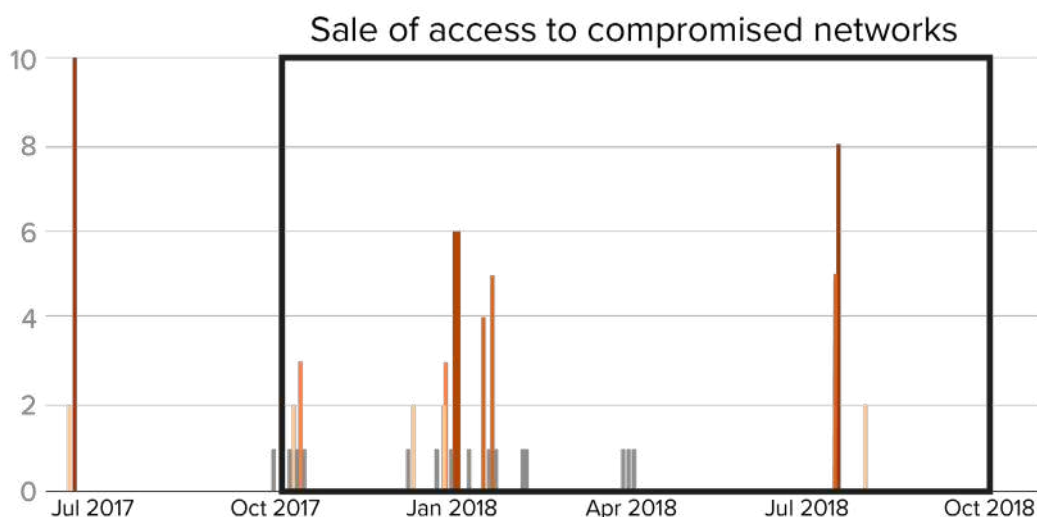


Figure 16 - Fxmsp's activity on exploit[.]in

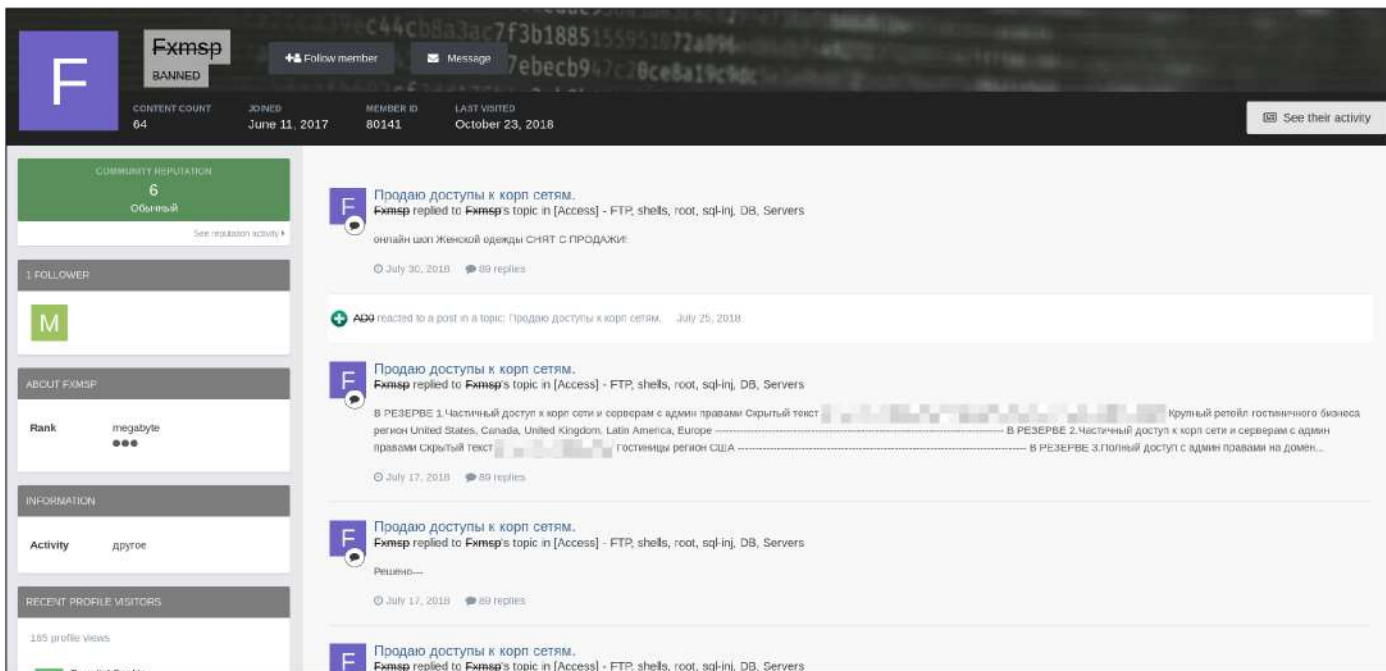


Figure 17 - October 2017. Screenshot of Fxmsp's account on exploit[.]in. The account was registered on June 11, 2017

It is highly likely that, initially, Fxmsp registered on the forum for other purposes. He was interested in only one question: is it possible to scan a large network linked to stock trading platforms for vulnerabilities. Other users advised him to send specific requests to ports and analyze the server's responses in order to identify devices with vulnerabilities.

Fxmsp: The invisible god of networks

Fxmsp
megabyte
●●●

Posted June 18, 2017 (edited) Report post

Доброго времени знающие и опытные спецы и форумчанины, у меня такая просьба к вам или вопрос?

Вот имеем мы сеть от 1.0.0.0-230.255.255.254.
В этой сети есть ПК, сервера, смартфоны... итд итп...

Вопрос заключается в 3х этапах.

1. Есть торговая платформа биржевых операций, у нее есть свой протокол обмена информации на 443 порту, между сервером и клиентом...

Я хочу провести так называемый массовый пентест на уязвимость, как самого протокола, так серверов, так и клиентов и получить совокупный отчет о состоянии данной торговой платформы и их клиентов. я новичок так сказать точно не программист, но есть небольшой опыт и большое стремление все это изучать с различных сторон.

Вопрос, возможно ли имея 100 серверов 1 гб каналами у себя, проанализировать весь интернет или хотя бы один город на использование торговой платформы на клиентских ПК, просто сканировать порт это не выход и смысла нет, но трудность у меня заключается в том что я не знаю как определить сам протокол в каком ввиде проводить анализ, допустим я дома получу сигнатуру через какой нибудь sniffер на предмет сигнатуры протокола, но как в сети интернет можно просканировать особый протокол? (Торговая платформа MT4, MT5 для биржевых операций)

Sniffерить весь интернет не реально думаю для меня, и даже город... Существуют ли методы или ПО для подобного анализа? Может кто то сможет посоветовать с чего начать?

Edited June 18, 2017 by Fxmsp



Fxmsp
megabyte

Posted June 18, 2017 (edited)

Hello, skilled and experienced specialists and forum users! I have a request or question for you.

Let's say we have a network 1.0.0.0-230.255.255.254
There are PCs, servers, smartphones and other devices within the network.

Banned

The question is three-fold:

1. There is a trading platform that has its data exchange protocol on port 443, between the server and the client...

I want to conduct a so-called massive penetration testing for vulnerabilities on the protocol, the server, and the client. As such, I want an accumulated report on the status of the trading platform and its clients. I'm a newcomer, not a programmer, but I have some experience and a great desire to study all this from different angles.

If I have 100 servers with 1-Gb channels, is it possible to analyze the entire Internet or at least one city as regards using the trading platform on clients' PCs. Scanning ports is not an option and there's no point to it. The difficulty is that I don't know how to determine the protocol or how to perform analysis. Let's say I get a signature using a sniffer, but how can I scan a given protocol on the Internet? (Trading platform MT4, MT5 for exchange operations).

Sniffing the entire Internet or even a city is not a realistic option for me...Are there methods or software that help perform such an analysis? Can anyone recommend where to start?

Figure 18 - June 2017. Screenshot of the post about help with scanning networks

After the last message about the subject from June 16, 2017, Fxmsp ceased his activity on forums for three months.

On October 1, 2017, Fxmsp published his first message about the sale of access to corporate networks. Initially, he tried to sell access to networks without naming the companies. The post also did not contain his contact details.

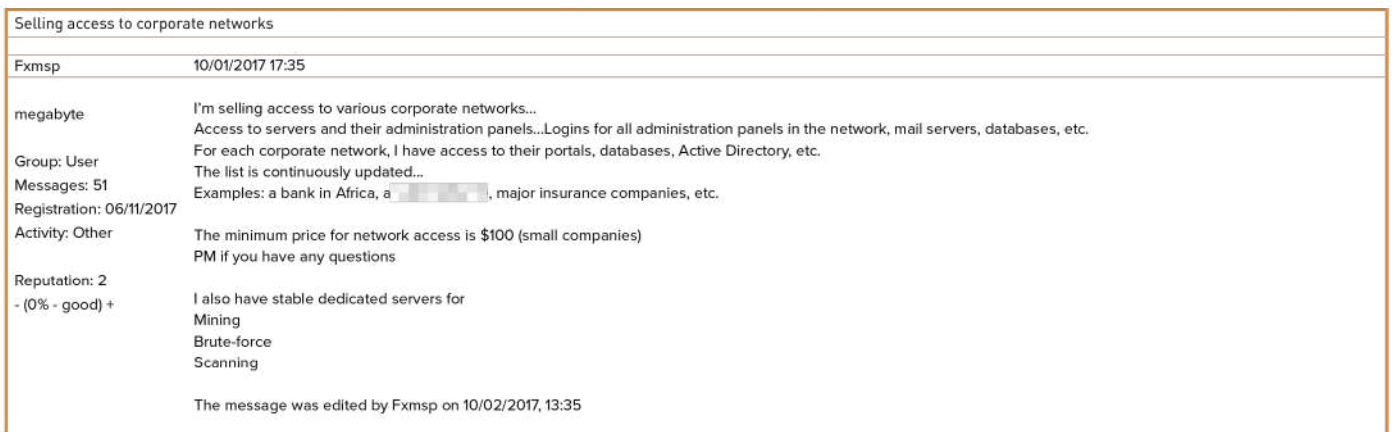
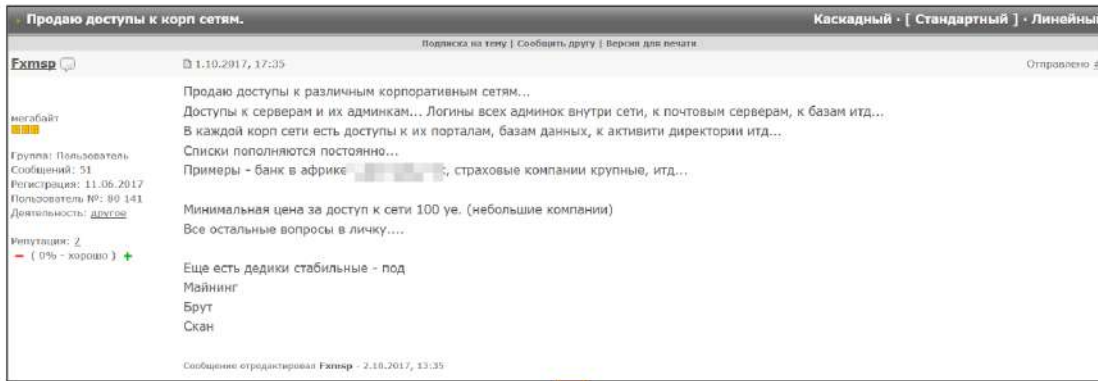


Figure 19 - October 2017. Screenshot of the ad for the sale of access to corporate networks (original version)

This message had been edited later. Fxmсп added his Jabber-account fxmsp541@exploit[.]im but, again, didn't include the names of compromised organizations.



Figure 20 - October 2017. Screenshot of the ad about the sale of access to corporate networks (edited version)

A week after posting the first ad, Fxmsp understood that it would be difficult to find buyers within the underground community without naming his victims. As such, he revealed the name of a bank. The hacker's first victim in the financial industry was a commercial bank in Nigeria.

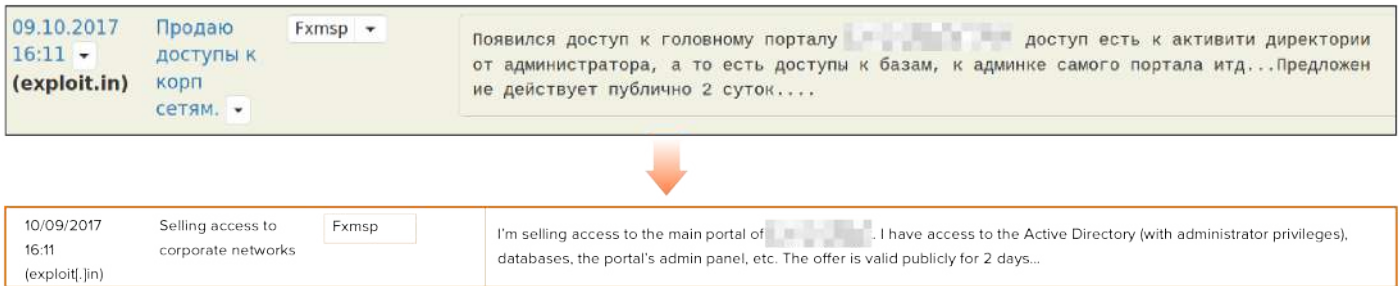


Figure 21 - October 2017. Screenshot of the ad about the sale of access to a Nigerian bank

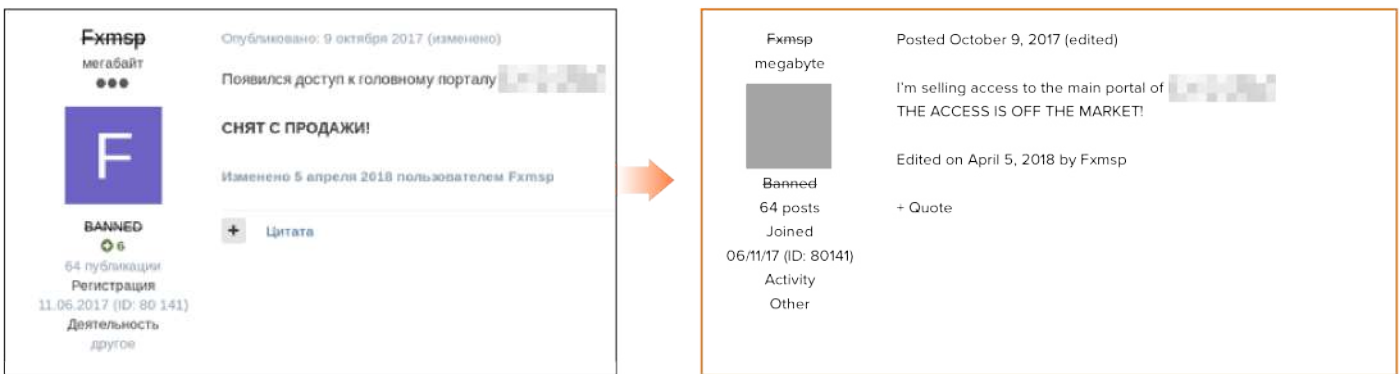


Figure 22 - October 2017. Screenshot of the ad about the sale of access to a Nigerian bank (edited version)

Fxmsp shared his another Jabber account, uwerty5411@exploit[.]im, for the first time on October 14, 2017.

Later, it was this information that helped establish his identity.

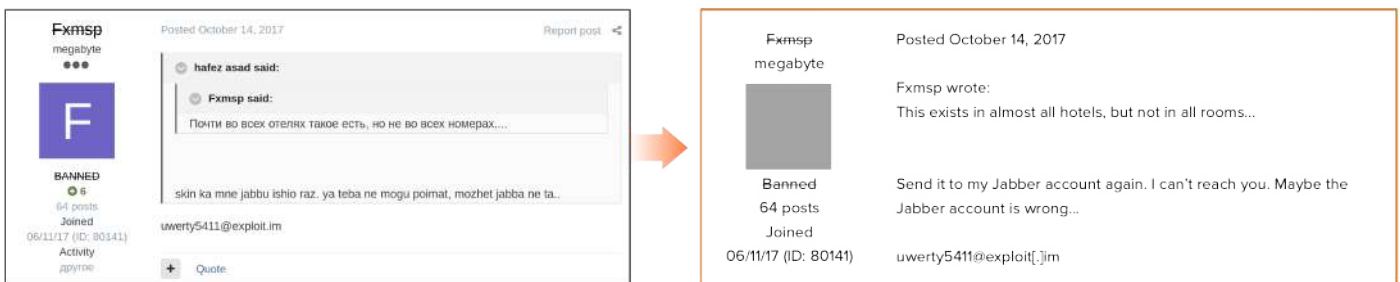


Figure 23 - October 2017. The first mention of Fxmsp's Jabber account on underground forums

On October 10, 2017, Fxmsp announced that he had gained access to the network belonging to a chain of luxury hotels with locations in the Dominican Republic, Cuba, Panama, the US, European and other countries. According to him, he was able to directly trace hotel guests and access the servers of the security services, the Active Directory, databases, and credit card control panels. The author offered access to 4-10 domain controllers, 600 servers, and 1,000 workstations. Administrator rights were included in the management of the domain controller and the Active Directory. Fxmsp also shared a map showing the hotel locations by country:



Figure 24 - One of the most high-profile cases: the sale of access to the network belonging to a chain of luxury hotels

On December 12, 2017, the author announced that he had gained access to an African bank with a capitalization of \$20 billion. According to him, the access offered comprehensive information about user accounts, passwords, databases, accounts, bank cards, bank accounts, and accounting records.

It should be noted that Fxmsp also tried to sell access in Russia: on December 30, 2017, Fxmsp published an ad for the sale of access through Radmin to an ATM and to the website of a customs office in two different Russian cities. A screenshot of this post can be found in Group-IB's attribution-based Threat Intelligence system:

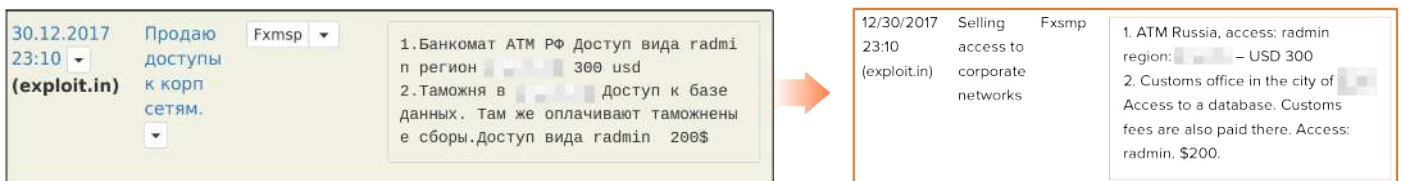


Figure 25 - December 2017. Screenshot of an ad for the sale of access to an ATM in Russia from Group-IB's internal system for monitoring darknet forums

On January 2, 2018, Fxmsp wrote that the access to the databases was no longer for sale, which usually means that the seller has found a buyer. However, shortly thereafter he edited the message and wrote that he did not work in CIS countries.

Fxmsp: The invisible god of networks

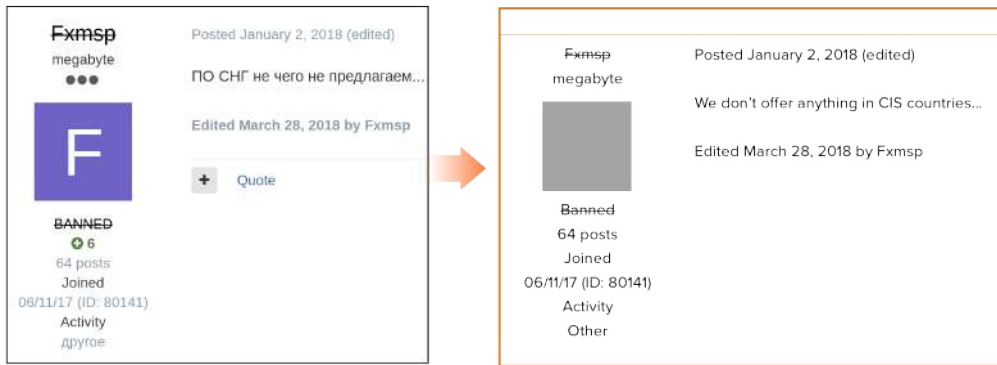


Figure 26 - Screenshot of the edited message in which the author announced that he did not work in CIS countries

Russian hackers have an unspoken rule about not working within Russia and CIS countries. This most likely stems from a fear of ending up behind bars. When you operate in other countries, any potential criminal investigation proceedings will take place in the victim country, which means that the chances of being caught and extradited are minimal, particularly if you choose to target countries that have weak diplomatic ties with Russia, or none at all.

Fxmsp was eventually banned from the forum for violating the rule of not working within Russia. The hacker learned his lesson. He deleted all offers linked to Russia and the ban was lifted.

On January 3, 2018, Fxmsp placed another ad for the sale of access to the network belonging to a company that builds and manages luxury hotels in the US. As before, he shared a map of where the compromised hotels were located:



Figure 27 - Another case involving compromised hotels' networks. Locations of compromised facilities

On January 17, 2018, the hacker shared exactly how many buyers he had at the time: 18. Fxmsp had been forced to show his hand in response to accusations from other users that he did not actually have the access he claimed.

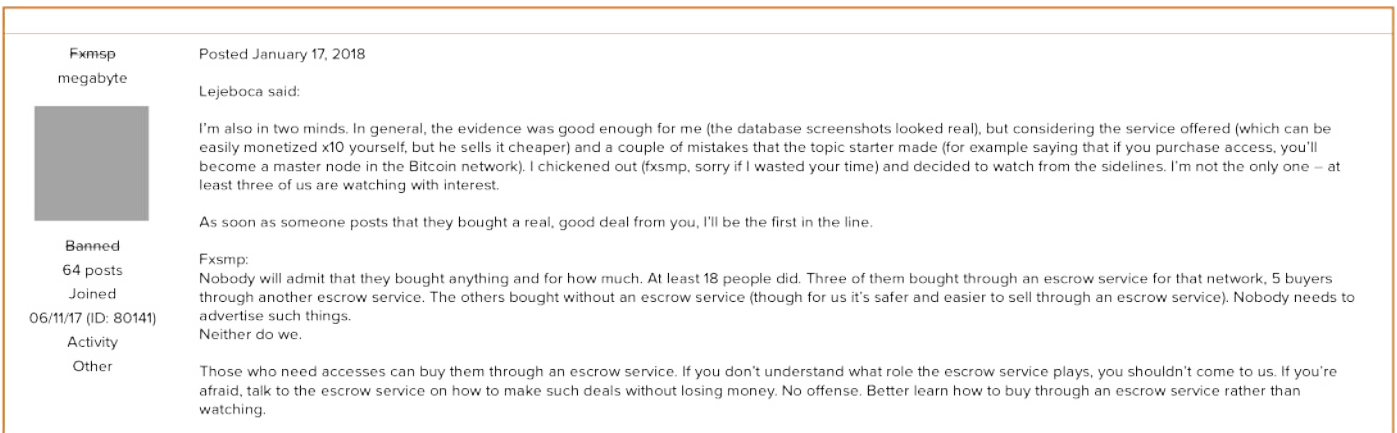
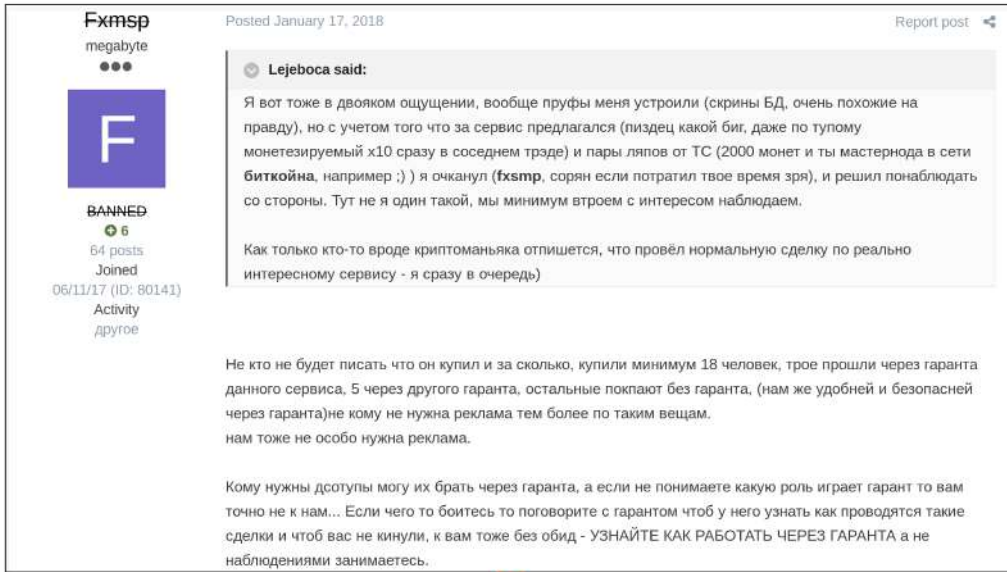


Figure 28 - Screenshot of the post in which Fxmsp shares the number of his current customers

On February 6, 2018, the author of the ad began selling access to the network of an Indian company and its subsidiaries. According to the post author, the company had direct access to its clients and the servers belonging to their partners, which included a few banks and mass media organizations. He named 8 companies, including 2 from the financial sector as examples of such partners and clients.

During the time that he was active on exploit[.]in, from early October 2017 to July 31, 2018, Fxmsp put access to 51 companies in 21 countries up for sale. The cybercriminal shared the price in only 30% of cases. By that time, after 9 months of activity, the minimum average price for all visible accesses that he advertised was \$268,000 (without including the sales he made through private messages).

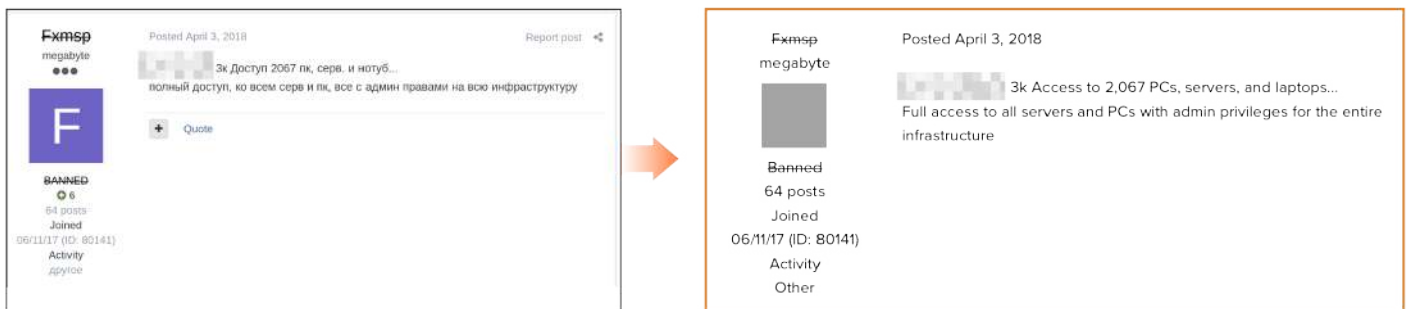
After publishing an ad for the sale of access to an Indonesian company in April 2018, Fxmsp ceased to be active on forums until mid-July, when he shared his additional Jabber account: fxsmp541@exploit[.]jim. In that same month, he published an ad for the sale of access to another five companies and ceased all activity, having appointed a user with the name **Lampeduza** already mentioned in this report as Fxmsp's sales manager.

EPISODE I: COLLABORATION WITH LAMPEDUZA

The user with the nickname **Lampeduza** registered on exploit[.]in on April 10, 2018 (hxxps://exploitingx4sjro[.]onion/profile/86842-lampeduza/). Lampeduza uses different pseudonyms on different underground platforms, which makes him difficult to track.

Nevertheless, Group-IB experts were able to identify Lampeduza's nicknames on other forums: **Antony Moricone, BigPetya, Fivelife, Nikolay, torter, andropov**, and **Gromyko**. Before Fxmsp and Lampeduza started working together, the latter sold bank card dumps (data stored on the card's magnetic strip) as well as login details and passwords to Facebook accounts. He also was interested in hacking into Snapchat accounts. The contact details that Lampeduza provided were in the form of a Jabber account: zeus11fe@exploit[.]im.

Group-IB researchers were able to make the connection between Lampeduza and Fxmsp because the two of them regularly published almost identical posts around the same time on different forums. For example, the image below shows them selling access to a few of the same companies:



Fxmsp
megabyte

Posted October 10, 2017 (edited) Report post

Есть доступ к группе Люкс отелей (Европа, доминикана, маями, куба, панама, и многое другое в основном курортные города, прямое отслеживание посетителей номеров, доступ к серверам службы безопасности видеокмеры (скрытые видео камеры в номерах) итд, весь трафик через днс сервера клиентов внутри номера итд), доступ к активти директория, к базе данных, к панели управления кредитными картами, отчеты итд итп...

Карта груп отелей по странам - Данный доступ состоит 4-10 доменов контролеров - более 600 серверов - и 1000 станций от бухгалтерии, до респешена...
Управление доменами и активти полное под админом...

Fxmsp
megabyte

Posted October 10, 2017 (edited)

I have access to a group of luxury hotels (Europe, the Dominican Republic, Miami, Cuba, Panama and much more, mainly resort towns), direct tracking of guests, access to security teams' servers, video cameras (hidden cameras in rooms), all traffic passing through DNS servers of clients in rooms, etc., access to Active Directory, databases, bank card control panels, reports, etc. Map of hotel groups by country. This access consists of 4-10 domain controllers, more than 600 servers, and 1,000 workstations belonging to various users ranging from accountants to receptionists ... Full control over domains and Active Directory with admin rights

BigPetya
Junior Member

Join Date: Jan 2018
Posts: 6
Reputation: 0 [+/-]

Есть доступ к группе Люкс отелей (Европа, доминикана, маями, куба, панама, и многое другое в основном курортные города, прямое отслеживание посетителей номеров, доступ к серверам службы безопасности видеокмеры (скрытые видео камеры в номерах) итд, весь трафик через днс сервера клиентов внутри номера итд), доступ к активти директория, к базе данных, к панели управления кредитными картами, отчеты итд итп...
Карта груп отелей по странам - Данный доступ состоит 4-10 доменов контролеров - более 600 серверов - и 1000 станций от бухгалтерии, до респешена...
Управление доменами и активти полное под админом...

BigPetya
Junior Member

Join Date: Jan 2018
Posts: 6
Reputation: 0 (+/-)

I have access to a group of luxury hotels (Europe, the Dominican Republic, Miami, Cuba, Panama and much more, mainly resort towns), direct tracking of guests, access to security teams' servers, video cameras (hidden cameras in rooms), all traffic passing through DNS servers of clients in rooms, etc., access to Active Directory, databases, bank card control panels, reports, etc. Map of hotel groups by country. This access consists of 4-10 domain controllers, more than 600 servers, and 1,000 workstations belonging to various users ranging from accountants to receptionists ... Full control over domains and Active Directory with admin rights ...

The fact that Fxmsp and Lampeduza were working together was first discovered in early 2018. On January 1, Lampeduza published a post about looking for work on the forum Omerta:

01-01-2018, 06:30 PM

Antony Moricone
Sgarrista

Join Date: Feb 2017
Posts: 143
Reputation: 1
Deposit: 0\$

RESUME

1. Bilingual (Russian&English)
2. Workaholic
3. Can prepare all typing-writing projects
4. LOYAL and Polite(will never lose your clients with me)
5. not young (experienced enough)
7. Not asking much wage(I am cheaper then others)

After that, in January 2018, Lampeduza began sharing posts on this forum and others about the sale of access to the very same companies that Fxmsp had mentioned earlier. Access to five companies that had not been mentioned on exploit[.]in was also put up for sale.

In late June 2018, Lampeduza once again posted that he was looking for work. This may have been due to the fact that neither Fxmsp nor Lampeduza advertised any access for sale between April and June 2018.

Lampeduza
megabyte

Posted June 28, 2018 Report post

Здравствуйте!

Ищу онлайн работу саппорта, администратора (неважно), любую работу где понабится мои знания.. Отличные знания английского, русского языков

- Если вам не хочется делать рутинную работу - ее сделаю я
- Опыт общения с техподдержкой (иностранные сайты), клиентами.
- Стрессоустойчив, порядочен и адекватен.
- При работе с деньгами предоставляю полную отчетность потраченных средств.
- Опыт работы в команде / в сапорте более 4х лет, в сети - более 9 ти.
- Обучаюсь быстро,
- При необходимости online 24/7

О себе:
занимаюсь деятельностью в интернете уже больше9 лет, опыт работы имеется во многих сферах, работа на постоянной основе приветствуется..

Оплата - договорная
Работа на постоянной основе - приветствуется..

Первый контакт В ЛС



Lampeduza
megabyte

Posted June 28, 2018

Hello!

I'm looking for an online job as a support agent or administrator (doesn't matter), any job where my skills will be useful. Excellent knowledge of English and Russian

- If you don't want to perform routine tasks, you can delegate them to me
- I have experience in communicating with tech support (foreign websites) and clients
- Able to work under pressure, honest, decent/
- When I work with money, I provide full reports on the funds spent.
- Experience in working in a team/tech support for more than 4 years. Working online over 9 years.
- Quick learner
- Online 24/7 if needed

About myself:
I have been working on the internet for over 9 years. I have experience in many areas. I would prefer a permanent job.

Pay – negotiable
Work on a permanent basis is welcome

First contact in PM

Figure 29 - Screenshot of Lampeduza's post about looking for work

In July 2018, Lampeduza and Fxmsp resumed cooperation. On July 16, 2018, a message appeared on an underground forum (en.wt1[.]la) about the sale of access to a corporate network belonging to a multinational retail franchise operator. By analyzing the brands involved, Group-IB specialists were able to determine the company in question. Fxmsp had advertised selling access to this company on exploit[.]in in February 2018. The message was published by a user with the nickname **Fivelife**, whose contact details showed the Jabber account zeusl1fe@exploit[.]im, which Lampeduza had shared on exploit[.]in.

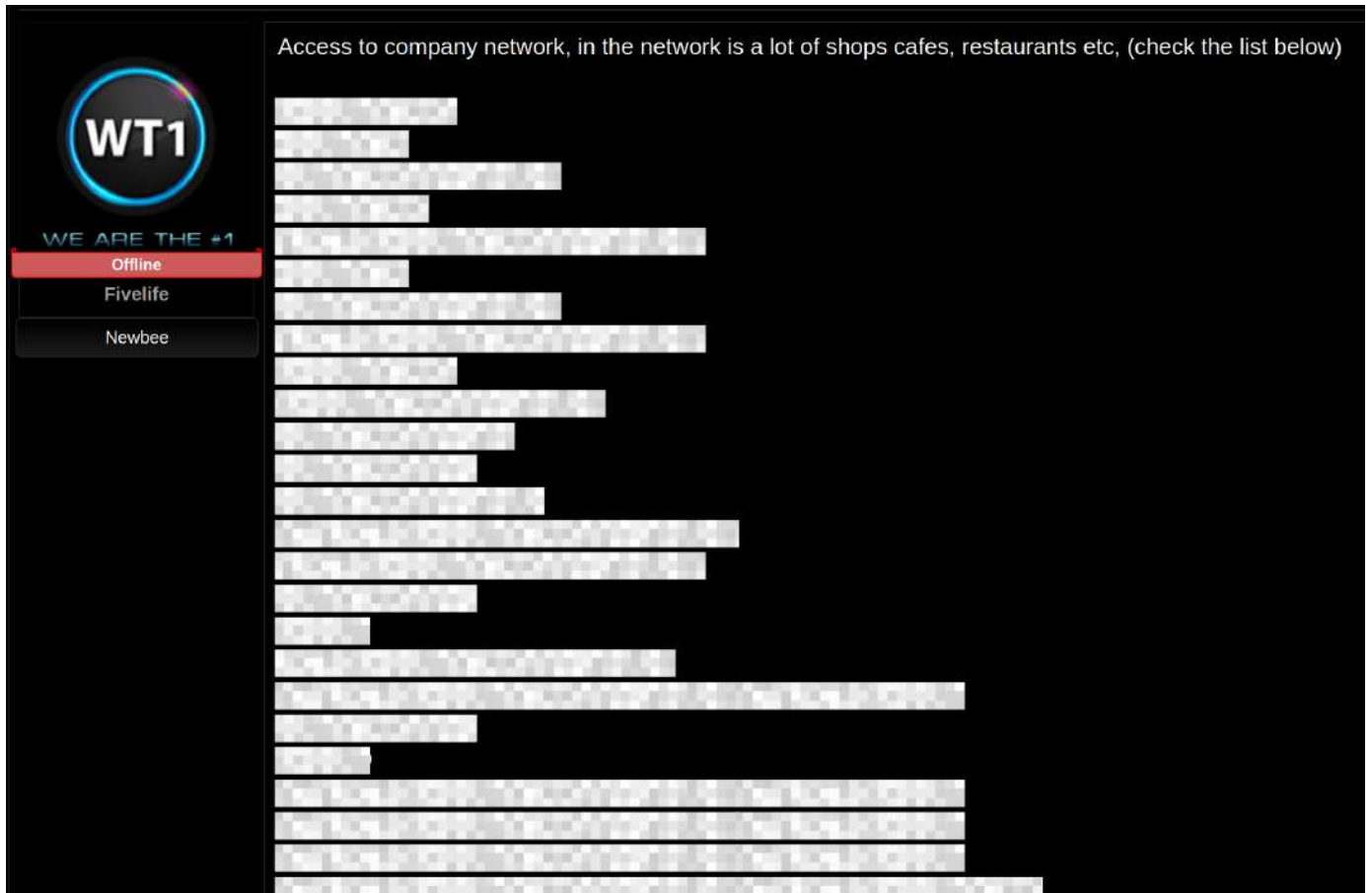


Figure 30 - Screenshot of the message with the list of accesses for sale on wt1[.]la

Moreover, Lampeduza relaunched sales on the forum Omerta under the nickname **Antony Moricone**. As of now, all his posts published on the forum contain the same text: “del” meaning they were deleted. Nevertheless, Group-IB’s attribution-based Threat Intelligence system was able to retrieve the original posts.



Figure 31 - July 2018. Lampeduza’s post about the sale of acceses on Omerta retrieved with the help of Group-IB’s attribution-based Threat Intelligence system

Fxmsp published the same post on exploit[.]in the same day:

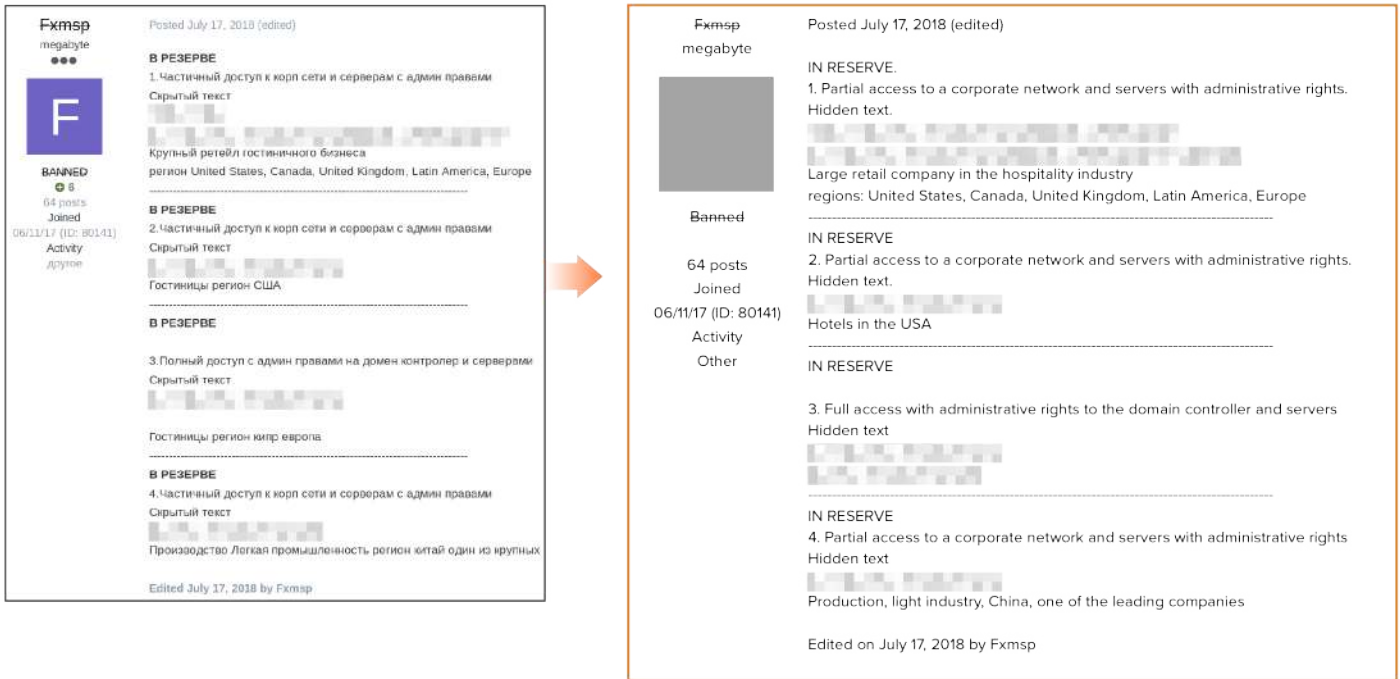


Figure 32- July 2018. Fxmsp's post about the sale of access on exploit[.]in

From late August 2018, Lampeduza ceased all earlier activity on forums and focused on selling access to corporate networks.

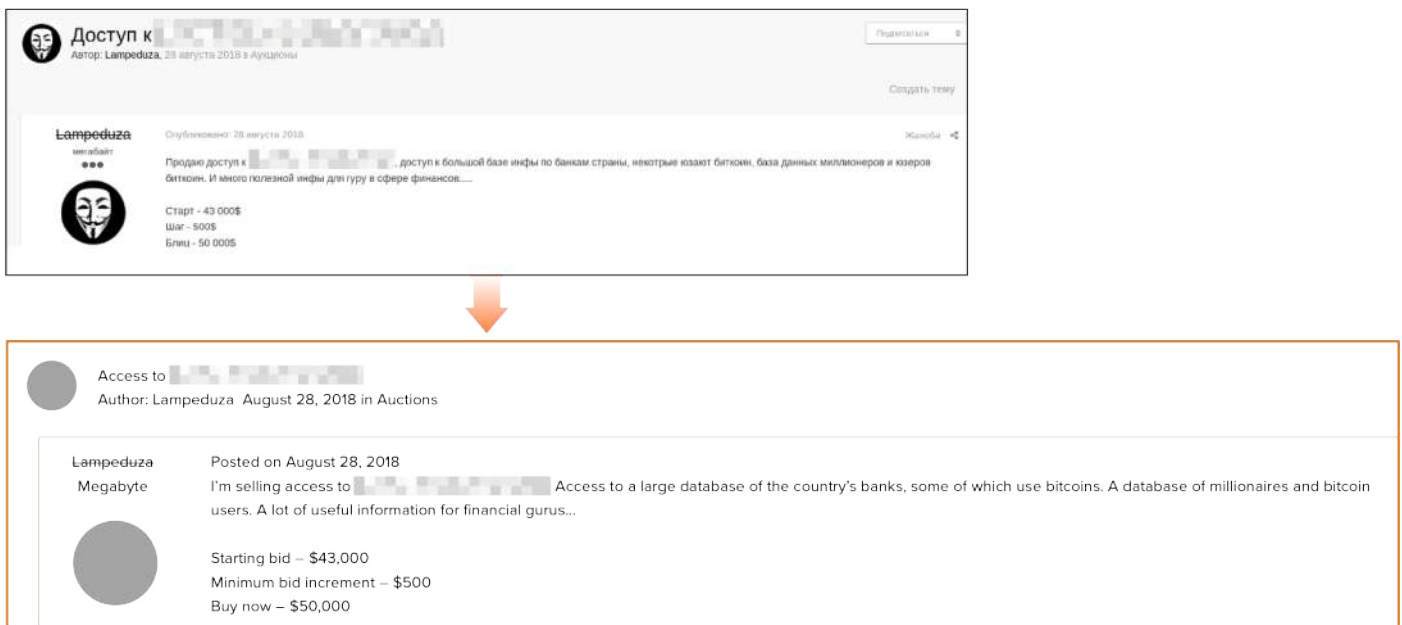


Figure 33 - August 2018. Lampeduza's offer of the sale of access to a government body in an African country

From September 20, 2018, Lampeduza started differentiating target audience and concealing the names of compromised companies from users who had made less than 50 posts:



Figure 34 - September 2018. Restrictions on viewing content

Nevertheless, Group-IB Threat Intelligence specialists were able to retrieve the information about compromised organizations:

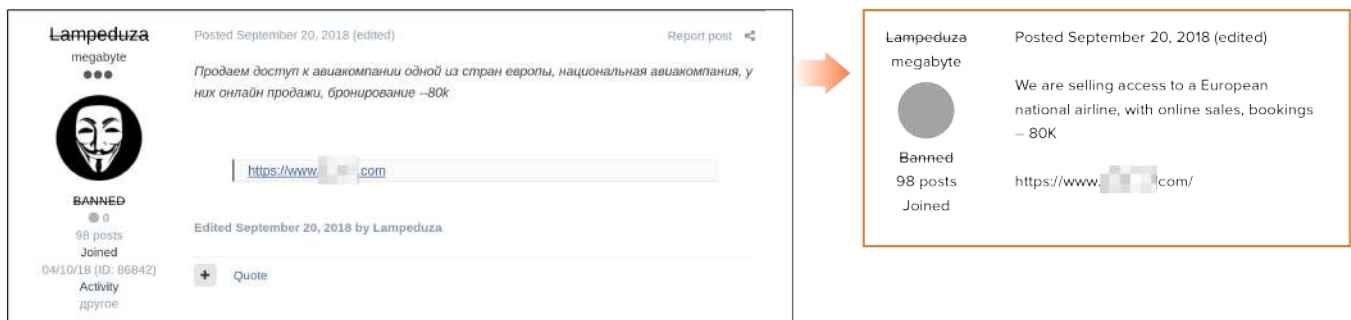


Figure 35 - Hidden information

On September 26, 2018, Lampeduza shared a post about the type of services he was providing and described in detail the advantages of having access to compromised networks. Promoting these services, Lampeduza wrote “[You will have access to the company’s] entire network ... You will become THE INVISIBLE GOD OF NETWORKS...”

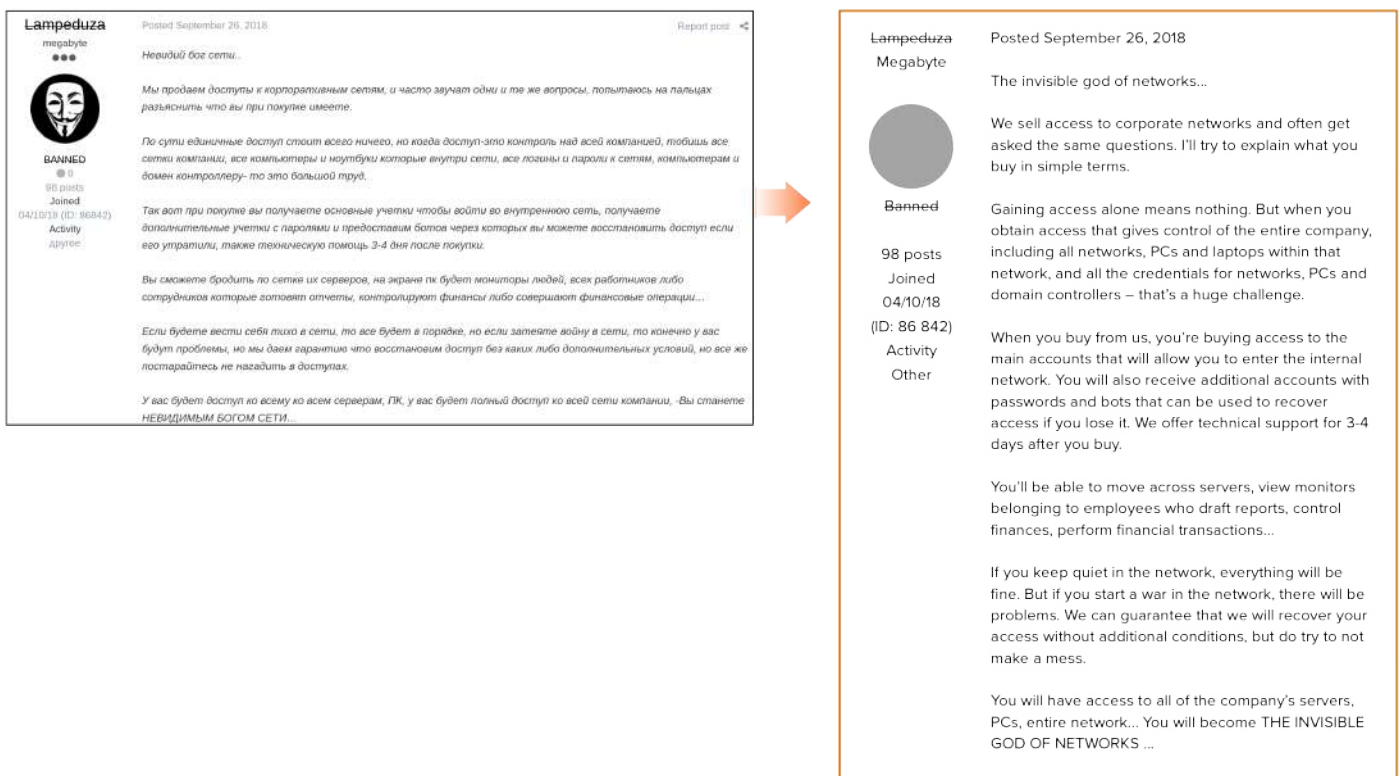


Figure 36 - September 2018. Screenshot of the post with a detailed description of how the co-conspirators sell access

In his message, Lampeduza noted that any access lost can be restored thanks to backdoors left in the network — a method also used by Fxmsp.

Lampeduza was mainly active from late August until November 2018, i.e. after being appointed as sales manager by Fxmsp, until he was banned from exploit[.]in. During this time, posts were shared on the forum advertising the sale of access to 62 new companies. The total price for all the access sold was \$1,100,800.

In late October 2018, Fxmsp and Lampeduza’s activity became threatened. It turned out that they were trying to sell access to the same network to several different buyers. This is prohibited on the forum without the buyer’s consent. As a result, a user with the name **g0rx** created a topic on the forum in which he described the situation. Such topics are used as a way to resolve disputes between underground community users when a buyer and seller enter into a conflict that requires the intervention of a third party, usually the forum administrator.

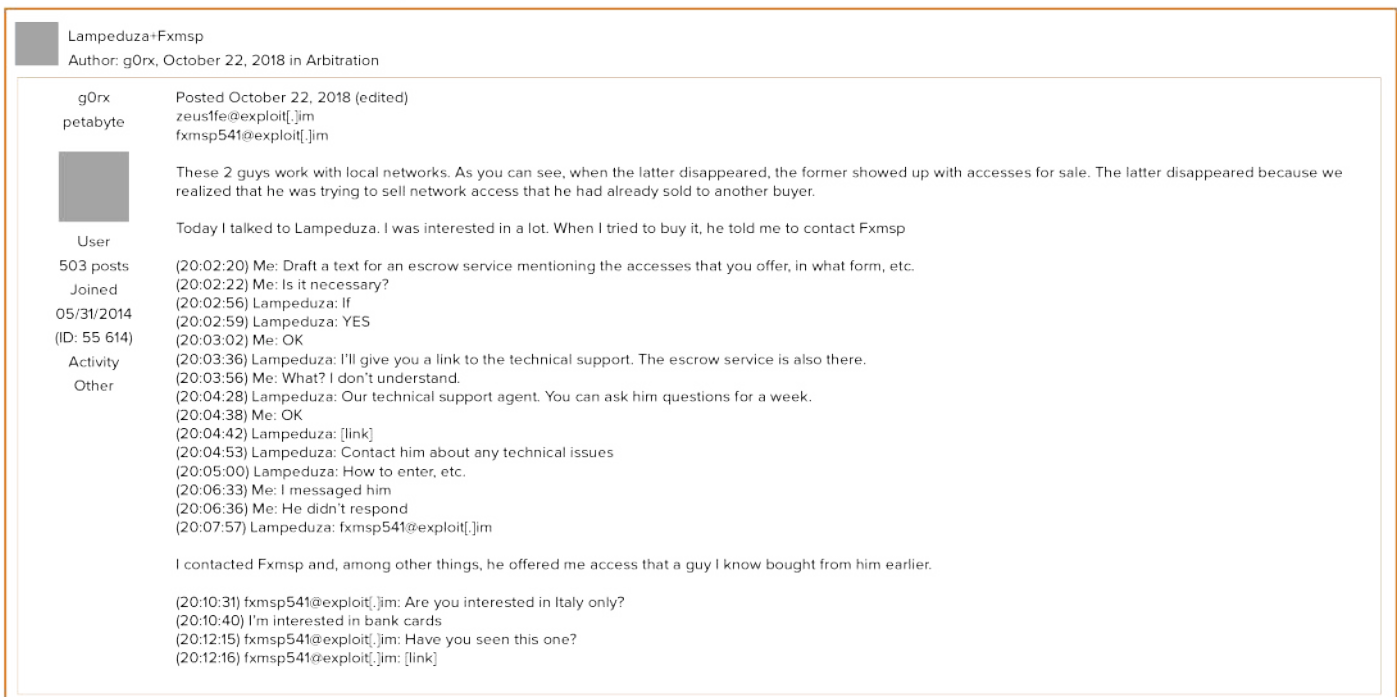
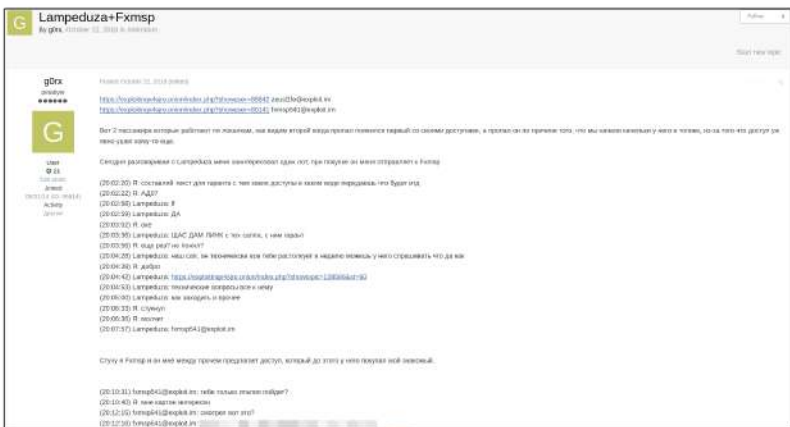


Figure 37 – Screenshot of the post about this cybercriminal group on an underground forum

The user g0rx wrote that someone he knew by the nickname of **mimikatz** had bought access to a corporate network from Fxmsp, but cryptominers were later discovered in it. As already mentioned in the “First steps in the underground” chapter, Fxmsp had indeed installed miners in compromised infrastructures at the start of his career. Moreover, Fxmsp also offered g0rx the opportunity to buy access to the same company.

In his defense, Lampeduza announced that he would cease working with Fxmsp and temporarily stop selling access to compromised networks. As a result on October 24, both users were banned from the main underground forum. The group suspended its activity on all other forums and allegedly focused on “private sales”, i.e. they started working only with a limited circle of trusted clients.

In mid-March 2019, the co-conspirators resumed their activity on forums. New messages about the sale of access appeared on several underground message boards. One of these ads is shown on the figure below.



Figure 38 – Screenshot of the new ad for the sale of access to corporate networks

It is also worth noting that on March 21, 2019, the user Antony Moricone posted an ad stating that he was selling access to corporate networks for the purpose of installing cryptocurrency miners within the company:

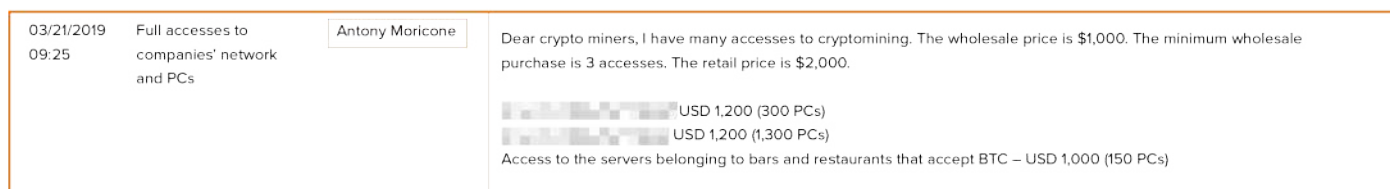
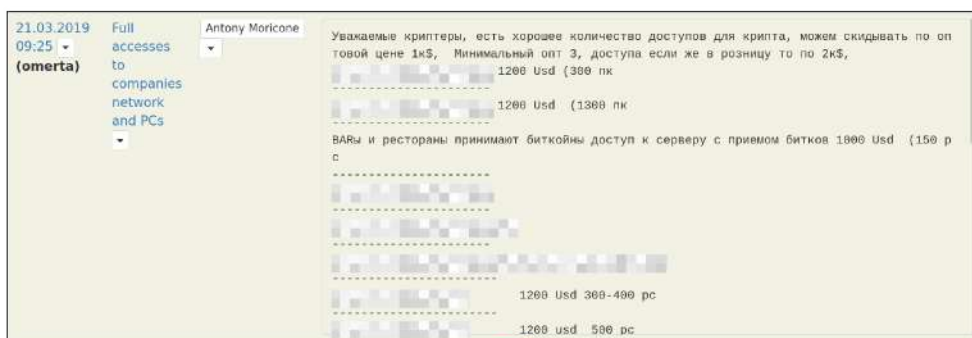


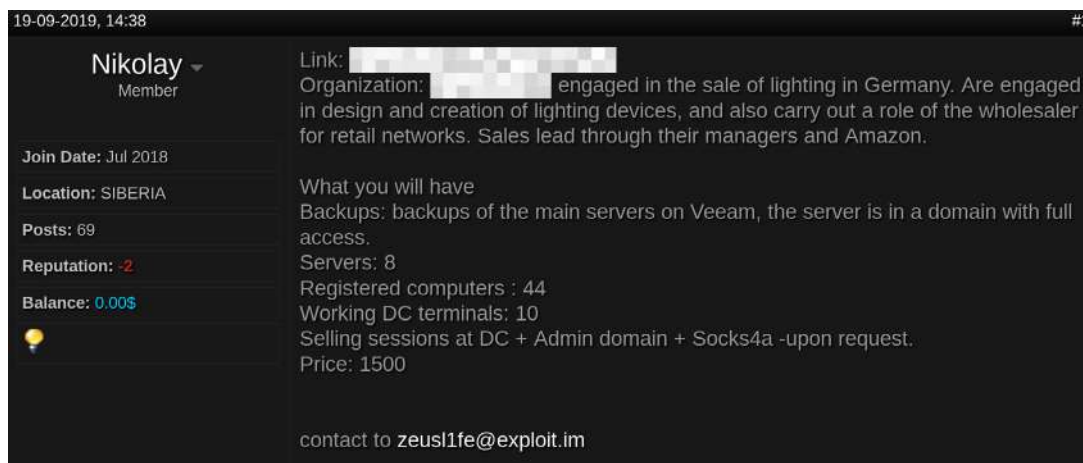
Figure 39 – Screenshot of the new ad selling access

Let us circle back to the beginning of this report: Fxmsp’s public activity culminated in April 2019. A company called AdvIntel reported to have received information from Fxmsp that he had compromised networks belonging to three major antivirus software vendors. According to the attacker, he had also exfiltrated the source codes of the antivirus agents, analytics modules, and security plug-ins for browsers from the compromised network. The price for the source code and network access was \$300,000. AdvIntel representatives stated that the attacker’s victims were McAfee, Symantec, and Trend Micro. Trend Micro then admitted that unauthorized access had been made to a single testing lab network by a third party, while the former two did not confirm the leak.

EPISODE II: THE PHANTOM MENACE

In May 2019, Lampeduza stated that he no longer worked with Fxmsp and had nothing to do with the leak of source codes belonging to the antivirus software companies. He also said that he had allegedly suspended their cooperation on underground forums due to the media paying more and more attention to Fxmsp. By that time, Lampeduza provided information about compromised companies to regular customers only. Thereafter, Lampeduza once again disappeared from forums for a while, but most likely continued selling accesses provided by Fxmsp through private messages.

Another public lot appeared several months later. On September 19, 2019, Lampeduza announced that he was ready to sell access to a new corporate network.



Screenshot 40 – September 2019. Screenshot of the new ad about selling access

It is difficult to assess how much money Fxmsp made in that time given that, in 2019, he publicly offered access to corporate networks belonging to only 22 companies. The total price for the services offered was \$124,100.

We can conclude that, despite being banned from exploit[.]in, the cybercriminal group continued its activity between May and September 2019. Moreover, despite his public claims Lampeduza most likely continued to sell access to corporate networks compromised by Fxmsp.



THE FINAL STRAIGHT: END OF Fxmsp's OPERATIONS

Lampeduza and Fxmsp officially stopped working together in December 2019. On December 3, 2019, Lampeduza, using one of his alternative nicknames, **Antony Moricone**, published a post on Omerta stating that he was looking for a job as an underground sales manager. It was the same post as the one he had published before he started working with Fxmsp:

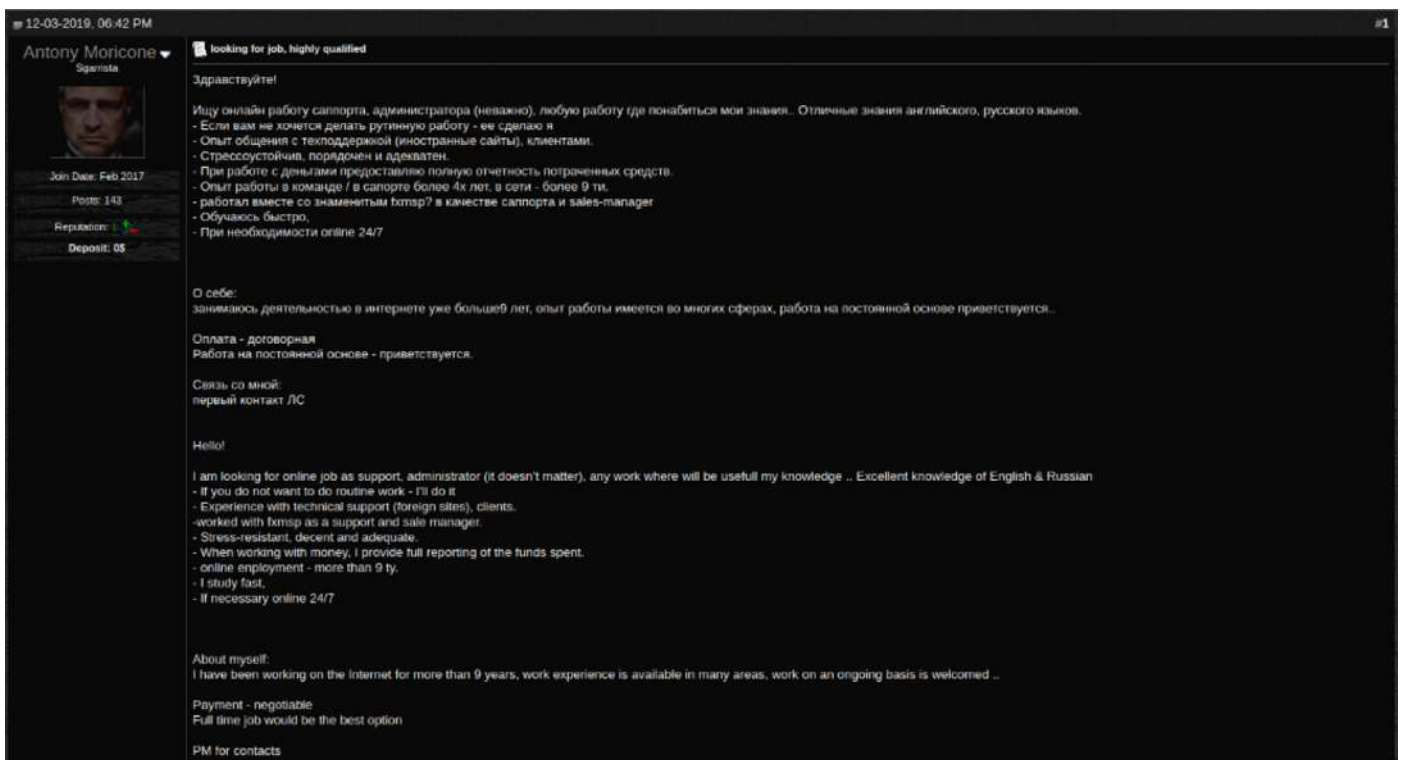


Figure 41 – March 2019. Screenshot of the Lampeduza's message about looking for a job

On December 17, 2019, Lampeduza confirmed to the forum users that Fxmsp had stopped his activity.

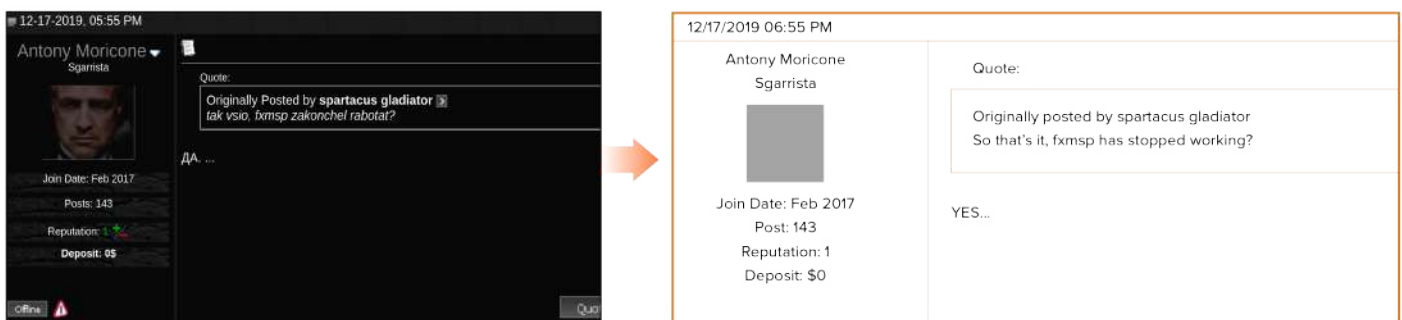


Figure 42 – December 2019. Lampeduza confirms that Fxmsp has stopped his activity

Fxmsp's PRESUMED IDENTITY: DEANONYMIZATION STAGES

Initially, Fxmsp used the Jabber account **uwerty5411@exploit[.]im** for communicating with other users. Group-IB specialists noticed that this account did not resemble his standard nickname and made a note of this pseudonym for the future. Most of the time, the threat actor used the unique nickname Fxmsp, which ultimately was the basis for establishing his true identity.

As the nickname is rare, Group-IB specialists were able to uncover his email account on the m^{***}.ru platform: **Fxmsp@m^{***}[.]ru**. The attacker has never mentioned this email on any forums, so it could have been a coincidence, but Group-IB decided to check whether this email address had been used to register any accounts on underground forums. As a result, Group-IB specialists uncovered overlaps with the attacker's accounts. The email had been used to register accounts on the following forums: proxy-base[.]com, lolzteam[.]net, exploit[.]in, and fuckav[.]ru.



Figure 43 - Correlation of m^{***}.ru account with Fxmsp's registration on forums

The address Fxmsp@m^{***}[.]ru was given as the backup email for the email account **fxmsp@b^{***}[.]ru**. The former was also linked to the latter; when linking, it was indicated that the nickname for the m^{***}.ru account begins with a capital letter. This detail is in fact crucial given that the attacker spelled his nickname with a capital letter on all forums.

As such, one more fact served as indirect confirmation that the original email was associated with the nickname that was used on underground forums.

Two Skype accounts are also linked to the email account Fxmsp@m^{***}[.]ru:

- **msgp^{***} (Mich^{***} Ko^{***})**
- **wcypr^{***} (An^{***} Ayt^{***})**

Moreover, the account Fxmsp@m^{***}[.]ru was used to register the domain gov360[.]info:



Figure 44 - Screenshot from Group-IB's system showing links between various accounts and a domain name registered using the account Fxmsp@m***[.]ru

In WHOIS data, the name “**andej a turchin**” appeared in the “Org” field:

Org	andej a turchin hosting telesystems jsc
Address	[REDACTED] [REDACTED]
City	almata moscow
Zipcode	050000 115093

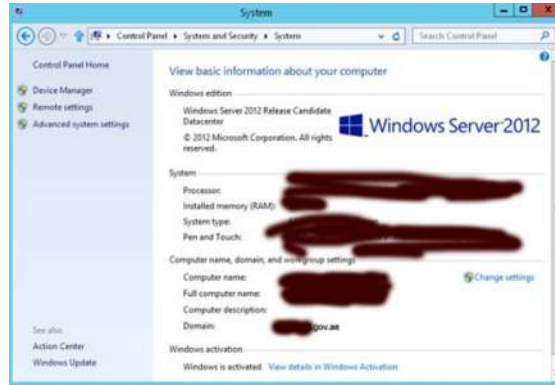
It is worth noting that in WHOIS data the email is also written with a capital letter:

```
Registrant Fax Ext:
Registrant Email: Fxmsp@m***.ru
```

The phone number **+7778316***** was also given. According to the operator's DEF code, the phone number belongs to the company Kcell/Activ in Kazakhstan.

Based on the attacker's Jabber account, Group-IB specialists found a similar account (i.e. similar activity was conducted using this account) registered on proxy-base[.]com (hxxp://proxy-base[.]com/members/uwert/). This fact was mentioned earlier in the report, but the reasoning behind why we believe that it also belongs to the attacker is explained below.

First, the account owner uses a nickname partially similar to the attacker's Jabber account. This factor alone is not proof in itself, however, because “uverty” is merely a common combination like qwerty with one letter changed. The second — much more important — factor is his activity on the forum. The user was interested in brute-force attacks on RDP servers. He asked the user with the nickname **Montano** (hxxp://proxy-base[.]com/members/montano/) for help. Later, it emerged that Montano had not been able to fulfill the task and instead created fake screenshots to confirm its supposed success; he inserted the domain name that Fxmsp had asked to attack in the screenshots. This is where the fun really begins. Messages exchanged between February 14 and 16, 2018 were published. A fake screenshot was also attached:



The top-level domain **gov[.ae]** appears on the screenshot. It is worth reiterating that a month earlier, Fxmsp had been selling access to compromised networks in the UAE.

During further research, based on the cybercriminal’s main Jabber account and his second detected account on proxy-base[.]com, Group-IB specialists checked the email uwert@m***[.]ru and discovered that it was used to register four domains:

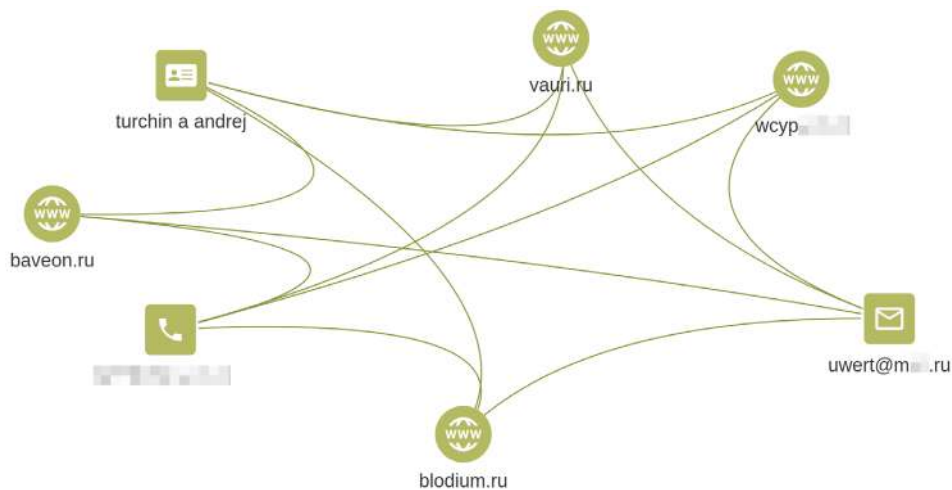


Figure 45 - Verification of connections between various accounts and identification of domains registered using uwert@m***[.]ru

As the figure shows, the domain name **wcyp***[.]ru** overlaps with the Skype username **wcyp*** (An*** Ayt***)**, which was registered using the email account Fxmsp@m***[.]ru.

The above-mentioned name “**turchin a andrej**” was used to register the account.

Status	registered, delegated, verified
Email	uwert@m[.]ru
Name	turchin a andrej

The month of birth provided in his Jabber account (uwerty5411@exploit[.]im) was **December**. The set of characters “**gdfsgfd**” was given as his name.

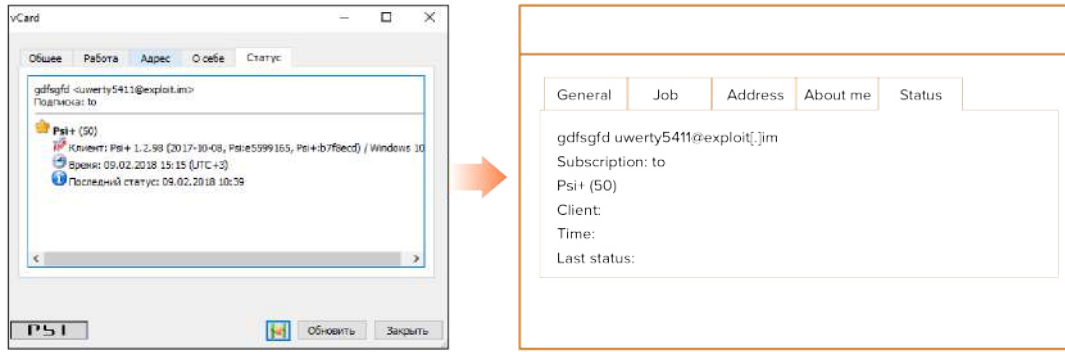
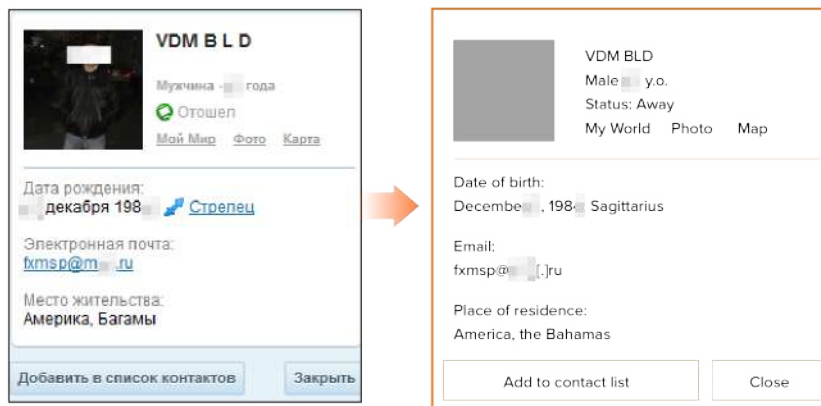
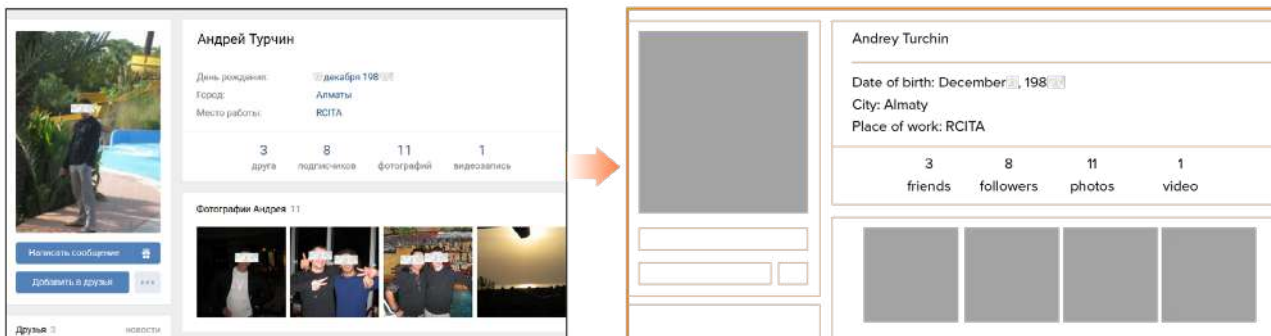


Figure 46 — Screenshot of information from the Jabber account uwerty5411@exploit[.]im

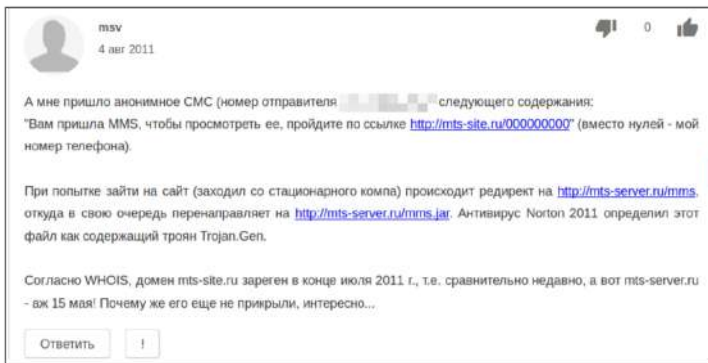
An analysis of the email address Fxmsp@m***[.]ru revealed that it was linked to an account in the Russian social network My World:



An account in the name of Andrey Turchin was discovered on the Russian social network VK.com (hxxps://vk[.]com/id***). The photo from this account matches the photo published on My World.



This account turned out to be linked to the email address uwert@m***[.]com.



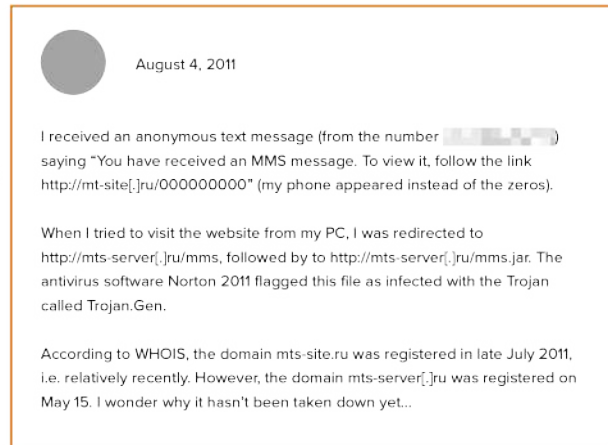
msv
4 авг 2011

А мне пришло анонимное СМС (номер отправителя [REDACTED] следующего содержания:
"Вам пришла MMS, чтобы посмотреть ее, пройдите по ссылке <http://mts-site.ru/000000000>" (вместо нулей - мой номер телефона).

При попытке зайти на сайт (заходил со стационарного компа) происходит редирект на <http://mts-server.ru/mms>, откуда в свою очередь перенаправляет на <http://mts-server.ru/mms.jar>. Антивирус Norton 2011 определил этот файл как содержащий троян Trojan.Gen.

Согласно WHOIS, домен mts-site.ru зарегистрирован в конце июля 2011 г., т.е. сравнительно недавно, а вот mts-server.ru - аж 15 мая! Почему же его еще не прикрыли, интересно...

Ответить



August 4, 2011

I received an anonymous text message (from the number [REDACTED]) saying "You have received an MMS message. To view it, follow the link [http://mt-site\[.\]ru/000000000](http://mt-site[.]ru/000000000)" (my phone appeared instead of the zeros).

When I tried to visit the website from my PC, I was redirected to [http://mts-server\[.\]ru/mms](http://mts-server[.]ru/mms), followed by to [http://mts-server\[.\]ru/mms.jar](http://mts-server[.]ru/mms.jar). The antivirus software Norton 2011 flagged this file as infected with the Trojan called Trojan.Gen.

According to WHOIS, the domain mts-site.ru was registered in late July 2011, i.e. relatively recently. However, the domain mts-server[.]ru was registered on May 15. I wonder why it hasn't been taken down yet...

Based on the information above, Andrey A. Turchin, born on December ***, **198*****, living in Almaty, Kazakhstan (according to social media profiles, domain registration data, and the phone number), is presumably the attacker who hides under the nickname "Fxmosp". The fact that he uses the same nicknames and the common interests related to exchange platforms both confirm this.



GROUP-IB'S PROFILE: Fxmsp

NAME | Andrey A. Turchin

ACTIVITY | Compromises company networks
and sells access to them

DOB | 12/***/198***

PLACE OF RESIDENCE | Almaty, Kazakhstan

USERNAMES | Fxmsp, uwert, vidi, bosslb

ICQ | 445436***
703004***

ACCOUNTS ON UNDERGROUND FORUMS | [https://lolzteam\[.\]net/members/125112/](https://lolzteam[.]net/members/125112/)
[http://proxy-base\[.\]com/members/fxmsp/](http://proxy-base[.]com/members/fxmsp/)
[http://proxy-base\[.\]com/members/uwert/](http://proxy-base[.]com/members/uwert/)
[https://forum.exploit\[.\]in/index.php?showuser=80141](https://forum.exploit[.]in/index.php?showuser=80141)
[https://fuckav\[.\]ru/member.php?u=36898](https://fuckav[.]ru/member.php?u=36898)

EMAIL ACCOUNTS | [fxmsp@m***\[.\]ru](mailto:fxmsp@m***[.]ru)
[uwert@m***\[.\]com](mailto:uwert@m***[.]com)
[uwert@m***\[.\]ru](mailto:uwert@m***[.]ru)
[boss@lb***\[.\]ru](mailto:boss@lb***[.]ru)

JABBER ACCOUNTS | [uwerty5411@exploit\[.\]im](jabber:uwerty5411@exploit[.]im)
[fxmsp541@exploit\[.\]im](jabber:fxmsp541@exploit[.]im)

RECOMMENDATIONS

At the time of writing, Fxmsp is no longer conducting public activities. It is uncertain, however, whether he is still breaking into company networks and selling access to them. Given the risk, we deem it essential to offer universal recommendations on how to prevent attacks that bear similarities to those conducted by Fxmsp.

As mentioned in the section “**Key findings. Tactics, techniques, and procedures**”, Fxmsp uses open RDP ports as the initial attack vector. We therefore recommend taking the following steps to protect against the types of incidents described in the report:

- 1. Change the default RDP port 3389.** Considering that attacks are usually not targeted, hackers often look for connections that use the default port. The port may be edited by changing it to any other.
- 2. Set up account lockout.** Given that attackers usually need a huge number of attempts to brute-force passwords and gain access to the RDP, make sure to enable account lockout policies by limiting the number of failed login attempts per user.
- 3. Check your logins and passwords in public leaks.** It is widely known that hackers use compromised data from various leaks to create dictionaries for brute-force attacks. Based on the leaked data, they create so-called combo lists (login and password pairs). As such, preventively checking leaks for your employees’ data significantly reduces the likelihood of an attack being successful.
- 4. Take preventive measures to detect leaked data offered for sale on underground forums.** To minimize the impact of data breaches, we recommend using Threat Intelligence systems that automatically monitor the darknet for compromised data related to a certain company. This type of solutions helps organizations take necessary steps to ensure data security and identify the source of the breach.
- 5. Install specialized software for detecting server anomalies.** Such programs help detect new accounts, traffic anomalies, and attempts to gain unauthorized access to any data.
- 6. Introduce IP address whitelisting.** We recommend that access to remote servers be limited to a specific list of IP addresses. If many employees work remotely, it is worth setting up a corporate VPN.
- 7. Ensure that the name of the last user who logged on is not displayed.** Ensure that the name of the last user who logged on is not displayed. To do this, change the group policy in the Active Directory (GPO_name**\ComputerConfiguration\Windows Settings\ Security Settings\Local Policies\Security Options**) and disable the parameter “Interactive logon: Do not display last user name.”

|GROUP|IB|

**Preventing
and investigating
cybercrime
since 2003.**

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

twitter.com/groupib_gib
blog.group-ib.com

+65 31 59 37 98
linkedin.com/company/group-ib