FXMSP: The invisible god of networks[1]

One of the most infamous sellers of access to corporate networks

ROOT LEVEL RESOURCES

44
countries affected by the attacks

135
companies attacked

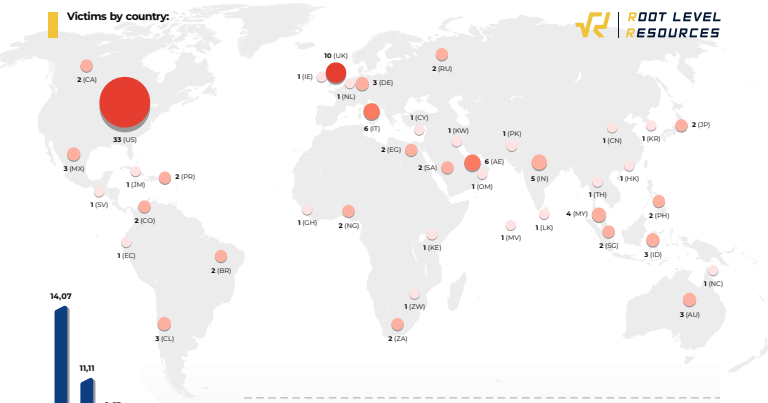
$1 500 000+
lower estimate of the sales revenue[2]

Более 3 лет
years of activity on underground forums

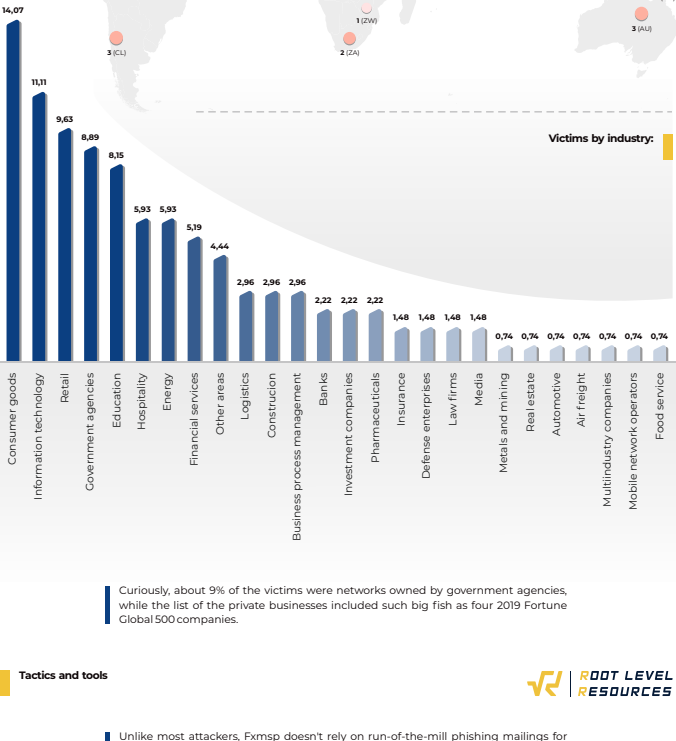
October 1, 2017 is Fxmsp's "birthday". On this day, the mastermind behind it for the first time offered for purchase access to all critical segments of the corporate networks he had broken into. According to the seller, one of the lots was a bank – a previously unheard-of precedent at the time.

But it was in May 2019 when the name Fxmsp became known all over the world, thanks to the news report about the hacker gaining access to the secure networks of three leading antivirus companies.[3] Fxmsp copied various code fragments of antivirus software, analytics modules, development documentation, etc. from the vendors' intranets. This lot was put up for $300,000. Fxmsp wrote that this was a planned operation. It took him just over three years to grow from an ordinary hacker forum user who had no clue about the ways to monetize his cracking skills into one of the main Russian hacking underground players, with his own pool of regular customers and even a sales manager.

Victims by country:



Victims by industry:



Curiously, about 9% of the victims were networks owned by government agencies, while the list of the private businesses included such big fish as four 2019 Fortune Global 500 companies.

Tactics and tools

ROOT LEVEL RESOURCES

Unlike most attackers, Fxmsp doesn't rely on run-of-the-mill phishing mailings for breaking into networks and doesn't do any research on the victim in advance, which means he prefers mass attacks over targeted strategy. The following outline lists the main stages of a typical Fxmsp raid and its movement through the network.

Scanning a specific range of IP addresses

This fairly simple and well-known approach involves scanning the IP addresses of a given city or country for certain open ports, using the popular Masscan software as well as more advanced scanners. At this stage, the perpetrator typically targets open RDP[4] ports, 3389 in particular. It is this port, used to provide remote access to MS Windows servers and workstations, that Fxmsp aims for.

Preparing an attack

After scanning the IP address range and identifying potential victim machines with open RDP ports, the attacker needs to reduce the amount of input data for a brute-force entry, using RDP Recognizer software. Most remote servers running Windows allow for viewing the authorization screen with a list of all accounts on the server. Via OCR, RDP Recognizer attempts to read the logins of all accounts on the server. If it succeeds, the attacker only needs to find the passwords using bruteforcing.

Bruteforce attack

At this stage, the perpetrator uses various programs to bruteforce their way into the victim's servers. This type of attack is essentially an attempt to arrive at the RDP password by trying all possible options until the correct one is found. Bruteforcing software may test either random character combinations or lists of popular and compromised passwords.

Ensuring persistence

Upon gaining access to the target machine, the attacker disables its antivirus software and firewall, then creates additional accounts for access. This is followed by further entrenchment in the network. Presumably, for this purpose Fxmsp uses the Meterpreter payload as a backdoor on the compromised servers. It's noteworthy that the interval of connections to CnC that Fxmsp specifies when installing the backdoors is quite long: once in 15 days.

Network reconnaissance

Having established a foothold on one machine, next the perpetrator sets their sights on accessing the domain controller. Presumably, Fxmsp seeks out accounts with administrative privileges, which offer easy access to valuable data. The attacker then extracts the dumps of all the accounts and attempts to decrypt them. One utility known to be used, among others, for this purpose is Windows Password Recovery, which allows for automated loading of user databases from SAM or ntds.dit and provides the function of decrypting hashed passwords.

Infecting backups

In the same manner as with the initial server, Fxmsp plants backdoors on backups at long intervals. Thus, even if the victim notices suspicious activity in the system, the likeliest outcome will be a change of passwords and a rollback to the already compromised backup.

Monetization

This main stage of Fxmsp's activity involves selling access to the compromised networks on underground forums. Initially he used to do it himself, and later enlisted the help of an accomplice known as Lampeduza. Early in his career he also installed cryptocurrency mining malware on the compromised servers.

So far, however, the most prolific network access seller remains at large, posing a threat to companies in a broad array of industries and across all geographical borders.

Incidents like those described above may be prevented by following these steps:

Identifying leaks put up for sale on underground forums

Threat Intelligence Platforms, which automatically monitor all appearances of company data across the darknet, enable users to promptly react to data leaks, identify potential leak channels, and ensure data security.

Configuring account blocking

As the perpetrator usually goes through a huge number of passwords by trial and error in order to access RDP, a temporary account blocking feature can be configured to turn on after a certain number of failed password entry attempts.

Checking public leaks for logins and passwords

Often, when compiling password dictionaries for bruteforcing, the attacker uses previously compromised data from various leaks known as combo lists.[5] Preventive checking of these lists for employee data can significantly lower the chances of success in case of a bruteforce attack.

Using anomalous activity detection software on the server

This software helps detect the appearance of new accounts, anomalous traffic patterns, and attempts of unauthorized access to any data.

Introducing white-listed IP addresses

It might be worthwhile to restrict remote server access to a specified list of IP addresses. If a number of employees work remotely, setting up a corporate VPN is a good option.

Disabling information output about the last authorized user on the server

This is accomplished by changing the group policy in Active Directory – setting the parameter 'Interactive logon: Do not display last user name' to 'disabled'.

Changing the default RDP port

Since the attacks are typically not targeted, the attacker must scan the default RDP ports. This setting can be changed to any other port.

1 – In 2018, in a post about selling access to compromised corporate networks, Lampeduza wrote, "You will have full access to the entire company network. You will become the invisible god of the network."

2 – Not including private sales nor about 20% of lots for the compromised company networks with unspecified prices

3 – https://www.bleepingcomputer.com/news/security/fxmsp-chat-logs-reveal-the-hacked-antivirus-vendors-avs-respond/

4 – Remote Desktop Protocol

5 – The login and password combination