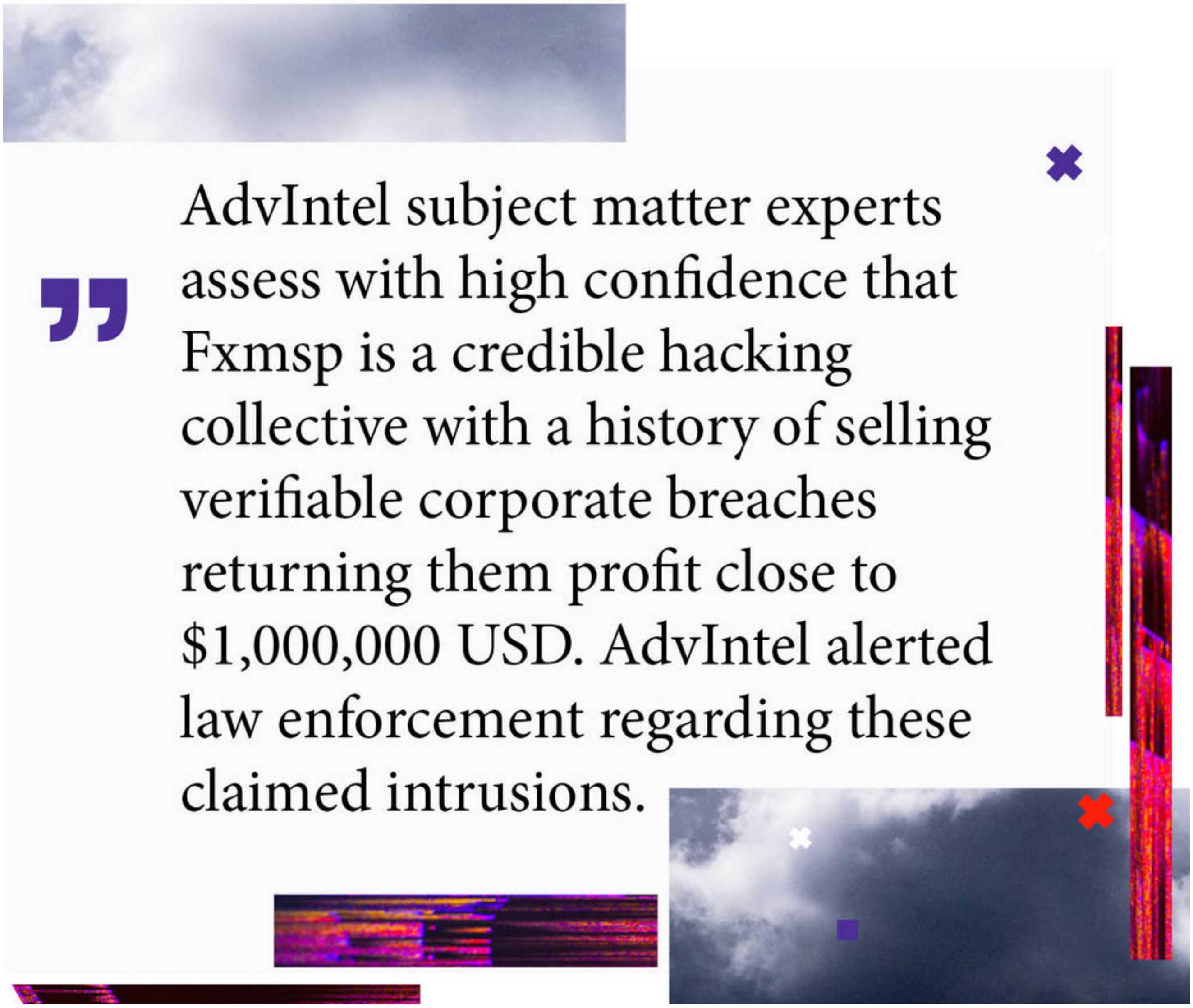
Top-Tier Russian Hacking Collective Claims Breaches of Three Major Anti-Virus Companies

advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies

AdvIntel May 9, 2019



” AdvIntel subject matter experts assess with high confidence that Fxmsp is a credible hacking collective with a history of selling verifiable corporate breaches returning them profit close to $1,000,000 USD. AdvIntel alerted law enforcement regarding these claimed intrusions.

- May 9, 2019
-
- 3 min read

Executive Summary

- "Fxmsp" is a high-profile Russian- and English-speaking hacking collective. They specialize in breaching highly secure protected networks to access private corporate and government information.

- They have a long-standing reputation for selling sensitive information from high-profile global government and corporate entities.
- In March 2019, Fxmsp stated they could provide exclusive information stolen from three top anti-virus companies located in the United States. They confirmed that they have exclusive source code related to the companies' software development. They are offering to sell it, and network access, for over $300,000 USD.
- AdvIntel subject matter experts assess with high confidence that Fxmsp is a credible hacking collective with a history of selling verifiable corporate breaches returning them profit close to $1,000,000 USD. AdvIntel alerted law enforcement regarding these claimed intrusions.

Background

Fxmsp is a hacking collective that has operated in various top-tier Russian- and English-speaking underground communities since 2017. They are known for targeting corporate and government networks worldwide.

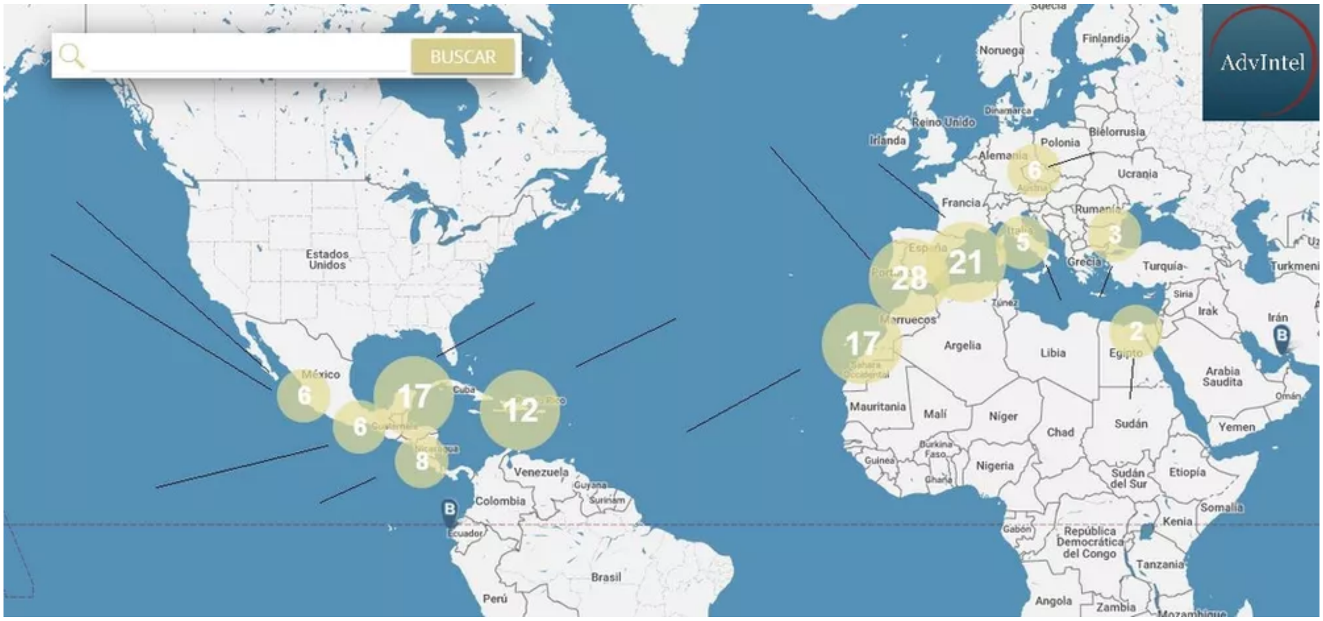


Image 1: Fxmsp offered access to one compromised hotel chain on April 5, 2018.

Tactics, Techniques & Procedures (TTPs)

Throughout 2017 and 2018, Fxmsp established a network of trusted proxy resellers to promote their breaches on the criminal underground. Some of the known Fxmsp TTPs included accessing network environments via externally available remote desktop protocol (RDP) servers and exposed active directory.

Most recently, the actor claimed to have developed a credential-stealing botnet capable of infecting high-profile targets in order to exfiltrate sensitive usernames and passwords. Fxmsp has claimed that developing this botnet and improving its capabilities for stealing information from secured systems is their main goal.

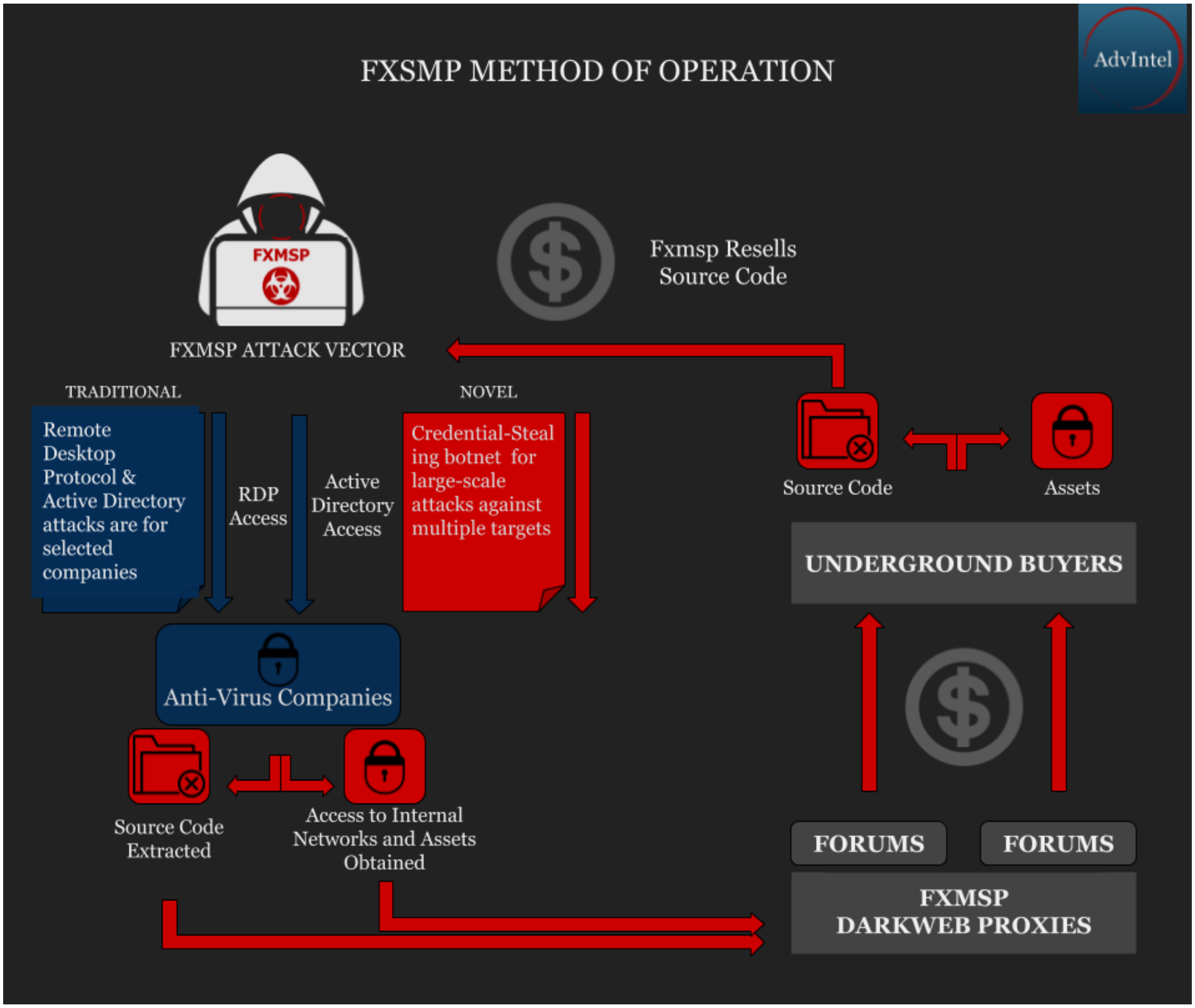
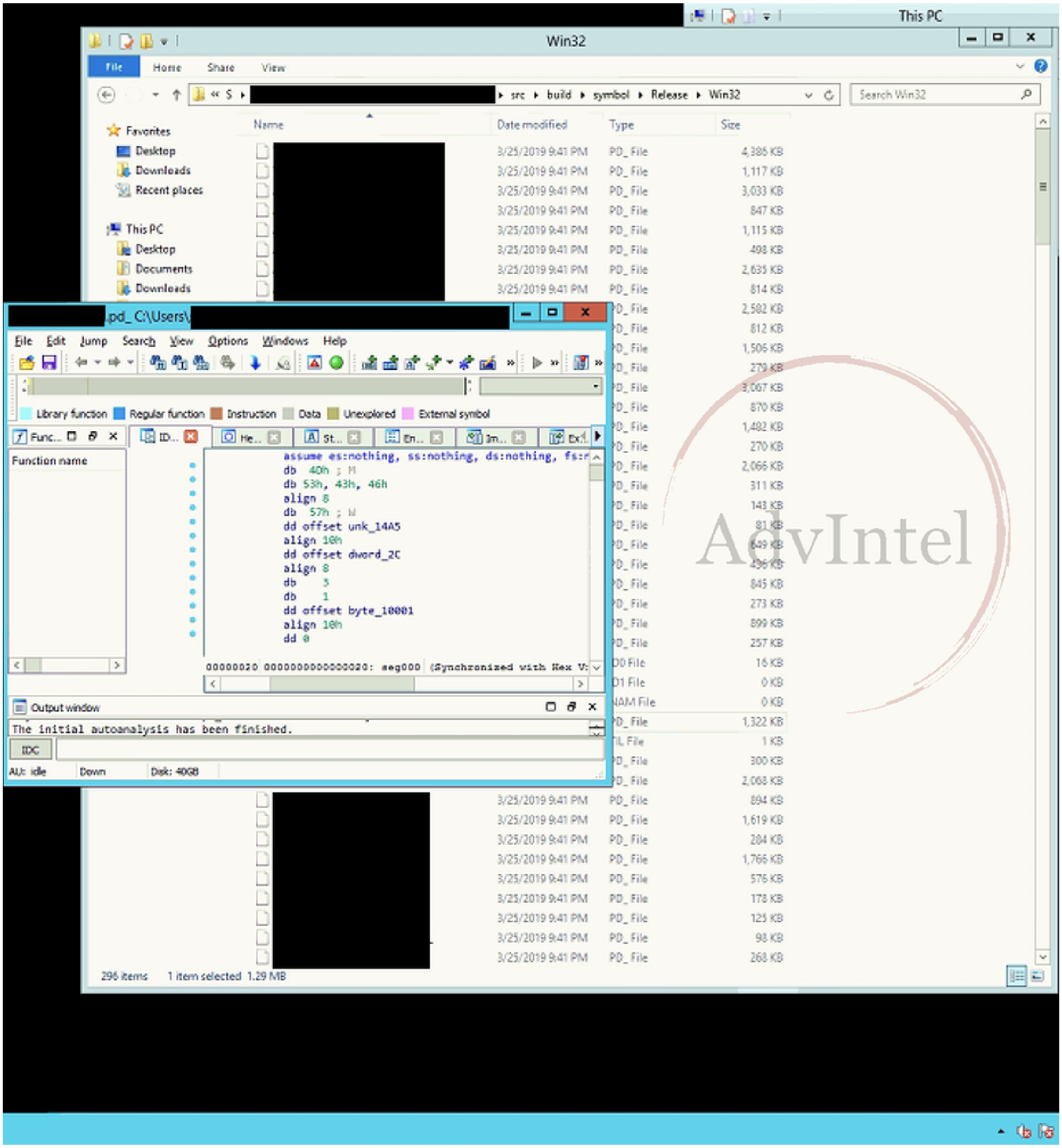

FXSMP METHOD OF OPERATION
AdvIntel
FXMSP
Fxmsp Resells Source Code
FXMSP ATTACK VECTOR
TRADITIONAL
NOVEL
Remote Desktop Protocol & Active Directory attacks are for selected companies
RDP Access
Active Directory Access
Credential-Stealing botnet for large-scale attacks against multiple targets
Source Code
Assets
UNDERGROUND BUYERS
Anti-Virus Companies
Source Code Extracted
Access to Internal Networks and Assets Obtained
FORUMS
FORUMS
FXMSP DARKWEB PROXIES

Image 2: AdvIntel research revealed sophisticated method of operation behind Fxmsp.

Fxmsp: Three Major Antivirus Company Breaches

On April 24, 2019, Fxmsp claimed to have secured access to three leading antivirus companies. According to the hacking collective, they worked tirelessly for the first quarter of 2019 to breach these companies and finally succeeded and obtained access to the companies' internal networks.

The collective extracted sensitive source code from antivirus software, AI, and security plugins belonging to the three companies. Fxmsp also commented on the capabilities of the different companies’ software and assessed their efficiency.



« $ › [redacted] › src › build › symbol › Release › Win32

Name	Date modified	Type	Size
[redacted]	3/25/2019 9:41 PM	PD_ File	4,386 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	1,117 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	3,033 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	847 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	1,115 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	498 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	2,635 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	814 KB
		D_ File	2,582 KB
		D_ File	812 KB
		D_ File	1,506 KB
		D_ File	279 KB
		D_ File	3,067 KB
		D_ File	870 KB
		D_ File	1,482 KB
		D_ File	270 KB
		D_ File	2,066 KB
		D_ File	311 KB
		D_ File	143 KB
		D_ File	81 KB
		D_ File	649 KB
		D_ File	436 KB
		D_ File	845 KB
		D_ File	273 KB
		D_ File	899 KB
		D_ File	257 KB
		D0 File	16 KB
		D1 File	0 KB
		AM File	0 KB
		D_ File	1,322 KB
		IL File	1 KB
		D_ File	300 KB
		D_ File	2,068 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	894 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	1,619 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	284 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	1,766 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	576 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	178 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	125 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	98 KB
[redacted]	3/25/2019 9:41 PM	PD_ File	268 KB

296 items   1 item selected 1.29 MB

[redacted].pd_ C:\Users\[redacted]

```
assume es:nothing, ss:nothing, ds:nothing, fs:r
db  40h ; M
db 53h, 43h, 46h
align 8
db  57h ; W
dd offset unk_14A5
align 10h
dd offset dword_2C
align 8
db    3
db    1
dd offset byte_10001
align 10h
dd 0
00000020 0000000000000020: seg000 (Synchronized with Hex V:
```

```
The initial autoanalysis has been finished.
```

AU: idle   Down   Disk: 40GB

Image 3: Fxmsp revealed the stolen source code stored in the debug information.

The collective provided a list of specific indicators through which it is possible to identify the company even when a seller is not disclosing its name. Fxmsp offered screenshots of folders purported to contain 30 terabytes of data, which they allegedly extracted from these networks. The folders seem to contain information about the company’s development documentation, artificial intelligence model, web security software, and antivirus software base code.

Motivation Behind Antivirus Company Breaches

Targeting antivirus companies appears to have been the primary goal of Fxmps' latest network intrusions. The actor claimed that antivirus breach research has been their main project over the last six months, which directly correlates with the six-month period during which they were silent on the underground forums where they normally post. This period started with their seeming disappearance in October 2018 and concluded with their return in April 2019.

Attribution Claims Behind Fxmsp Moniker

According to “ShadowRunTeam,” a high-profile Russian threat actor operating on Telegram, Fxmsp is reportedly a Moscow resident with the first name "Andrey" who started to engage in cybercrime activities in mid-2000 and specialized in social engineering.

Our subject matter experts assess with high confidence that Fxmsp is a credible hacking collective that has a history of selling verifiable corporate breaches returning them profit close to $1,000,000 USD. AdvIntel alerted US law enforcement regarding the purported intrusions.

Recommendations & Possible Mitigation

- Monitoring and reviewing the network perimeter for any externally-exposed Remote Desktop Protocol (RDP) servers and Active Directory (AD) might reduce exposure to the known two initial attack vectors.
- Employing robust patching and security hygiene, as well as monitoring for spearphishing email messages might assist with identifying early warnings linked to the Fxmsp's newer attack vector environment.
- Segregating and protecting sensitive source code development environments from access to the main network might thwart attempts to exfiltrate intellectual property from the network.