Hackers Corner
Target Intelligence

Background

At the beginning of May 2019, Cybersecurity firm AdvIntel published a blog[1] about a high-profile Russian hacking collective, Fxmsp, claiming to have breached three major anti-virus companies located in the United States. Following the publication both, Ars Technica[2] and Bleeping Computer[3] picked up the story and provided updates about this ongoing event.

Event

On May 9 the story broke that Fxmsp, a Russian hacking collective known to operate on a network of deep web forum was asking for $300,000 for the source code and network access to three major anti-virus companies. Yelisey Boguslavskiy, AdvIntel's director of security, told Bleeping Computers "The folders seem to contain information about the company's development documentation, artificial intelligence model, web security software, and antivirus software base code."

On May 11 researchers at HakDefNet[4] privately reported that Symantec, McAfee and TrendMicro were among those compromised and on May 13 Bleeping Computers provided a public update[5] when it received the unredacted communication logs from AdvIntel naming the three vendors.

The Tactics, Techniques and Procedures (TTP's) of Fxmsp have been tracked by many intel firms since 2017. In the past their offerings have checked out, but recently the group was banned for shady deals that involved reselling previously sold assets. In an update to the Ars Technica piece, AdvIntel said that Fxmsp went dark after a relationship was compromised in October 2018 with their proxy sellers. Here is an extracted conversation from the forum. This event forced the group to go silent on the forums and begin communicating strictly through Jabber.

In April 2019 Fxmsp returned advertising access to a network of a chain hotel's and the source code, plus access, to Symantec, McAfee and TrendMicro. This news generated by AdvIntel's blog resulted in pressure on the companies to respond with an official statement. In a quote given to Bleeping Computer, AdvIntel said: "AdvIntel works directly with Symantec to mitigate the risk. Even though Fxmsp collective claimed that the company is on the victim's list, they have not provided any sufficient evidence to support this allegation." An allegation that was passively proposed in AdvIntel's blog.

Threat Research and reporting is difficult but what is known about Fxmsp TTP's is that they typically target large corporations and sell that data through a network of proxy sellers on deep web forums, of which they have been known to resell sold network access and data to more than one buyer. Fxmsp TTP's include targeting Remote Desktop Protocol (RDP) and Active Directory (AD). They also claim to be developing a credential stealing botnet. In short, this is another case of an organized crime group targeting large corporations and service providers who maintain a large base of dependent users. Data stolen is quickly sold for profit and not leveraged for espionage like we see with Nation State actors. At the moment the legitimacy of the data for sale cannot be confirmed but this event does shed light on the importance of target/actor intelligence.

[1] https://www.advanced-intel.com/blog/top-tier-russian-hacking-collective-claims-breaches-of-three-major-anti-virus-companies

[2] https://arstechnica.com/information-technology/2019/05/hackers-breached-3-us-antivirus-companies-researchers-reveal/

[3] https://www.bleepingcomputer.com/news/security/hackers-selling-access-and-source-code-from-antivirus-companies/

[4] https://hakdefnet.org/

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

Hackers Corner
Target Intelligence

Corporate Insight

Target Intelligence is an important part of cyber threat research. The process allows us to study the components of a group to determine their vulnerabilities and relative importance in the threat landscape. This requires seeing past the packets and engaging the threat actors with covert and overt operations. While not all Intel will be actionable or accurate, it will allow you to see deeper and know more about your enemy.

Overt operations utilize a technique known as Open Source Intelligence or OSINT and involve the process of collecting data from publicly available sources while covert operations are more of a clandestine nature and leverage a technique called Human Intelligence or HUMINT. This requires personal contact and communication with your targets.

For example, in the recent event, we know that the Fxmsp went dark in October of 2018, but can we spot other associates? With this information and a few OSINT tools we can quickly begin to see who Fxmsp frequently communicates with. These accounts include g0rx, Lalartu and Nikoly. Group activity and commutations are seen echoed through several forums including LAMP and Club2Crd. On Club2Crd user Nikolay, while answering questions about a post, admitted to association with Fxmsp. His claimed association was quickly confirmed when the users' activity also dropped in October of 2018 with the disappearance of the group.

While the event has not provided actionable intelligence as of this moment, we can begin to see more of the landscape, where they operate and who is part of this group that is claiming to have targeted major anti-virus vendors. Even if the claim is proved to be false, we still gain insight into the group's relative importance through Target Intelligence.

Advice

If the reader takes anything away from the Fxmsp event, it's to exercise caution and patience when a hacking collective claims to have compromised your network. Verify the information and utilize threat sharing networks. These criminals will do anything and con anyone to draw attention to their sell in hopes it attracts a buyer.

Under Attack and in Need of Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.