FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community

fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

FireEye Stories Blog

December 08, 2020 | by Kevin Mandia
FireEye
tools
Red Team

FireEye is on the front lines defending companies and critical infrastructure globally from cyber threats. We witness the growing threat firsthand, and we know that cyber threats are always evolving. Recently, we were attacked by a highly sophisticated threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack. Our number one priority is working to strengthen the security of our customers and the broader community. We hope that by sharing the details of our investigation, the entire community will be better equipped to fight and defeat cyber attacks.

Based on my 25 years in cyber security and responding to incidents, I've concluded we are witnessing an attack by a nation with top-tier offensive capabilities. This attack is different from the tens of thousands of incidents we have responded to throughout the years. The

attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past.

We are actively investigating in coordination with the Federal Bureau of Investigation and other key partners, including Microsoft. Their initial analysis supports our conclusion that this was the work of a highly sophisticated state-sponsored attacker utilizing novel techniques.

During our investigation to date, we have found that the attacker targeted and accessed certain Red Team assessment tools that we use to test our customers' security. These tools mimic the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers. None of the tools contain zero-day exploits. Consistent with our goal to protect the community, we are proactively releasing methods and means to detect the use of our stolen Red Team tools.

We are not sure if the attacker intends to use our Red Team tools or to publicly disclose them. Nevertheless, out of an abundance of caution, we have developed more than 300 countermeasures for our customers, and the community at large, to use in order to minimize the potential impact of the theft of these tools.

We have seen no evidence to date that any attacker has used the stolen Red Team tools. We, as well as others in the security community, will continue to monitor for any such activity. At this time, we want to ensure that the entire security community is both aware and protected against the attempted use of these Red Team tools. Specifically, here is what we are doing:

- We have prepared countermeasures that can detect or block the use of our stolen Red Team tools.
- We have implemented countermeasures into our security products.
- We are sharing these countermeasures with our colleagues in the security community so that they can update their security tools.
- We are making the countermeasures publicly available in our blog post, "Unauthorized Access of FireEye Red Team Tools".
- We will continue to share and refine any additional mitigations for the Red Team tools as they become available, both publicly and directly with our security partners.

Consistent with a nation-state cyber-espionage effort, the attacker primarily sought information related to certain government customers. While the attacker was able to access some of our internal systems, at this point in our investigation, we have seen no evidence that the attacker exfiltrated data from our primary systems that store customer information from our incident response or consulting engagements, or the metadata collected by our products in our dynamic threat intelligence systems. If we discover that customer information was taken, we will contact them directly.

Over many years, we have identified, cataloged, and publicly disclosed the activities of many Advanced Persistent Threat (APT) groups, empowering the broader security community to detect and block new and emerging threats.

Every day, we innovate and adapt to protect our customers from threat actors who play outside the legal and ethical bounds of society. This event is no different. We're confident in the efficacy of our products and the processes we use to refine them. We have learned and continue to learn more about our adversaries as a result of this attack, and the greater security community will emerge from this incident better protected. We will never be deterred from doing what is right.

Forward Looking Statements

Certain statements contained in this blog post constitute "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. These forward-looking statements are based on our current beliefs, understanding and expectations and may relate to, among other things, statements regarding our current beliefs and understanding regarding the impact and scale of the disclosed event and our understanding of what occurred. Forward-looking statements are based on currently available information and our current beliefs, expectations and understanding, which may change as the investigation proceeds and more is learned, including what was targeted and accessed by the attacker. These statements are subject to future events, risks and uncertainties – many of which are beyond our control or are currently unknown to FireEye. These risks and uncertainties include but are not limited to our ongoing investigation, including the potential discovery of new information related to the incident.

Forward-looking statements speak only as of the date they are made, and while we intend to provide additional information regarding the attack, FireEye does not undertake to update these statements other than as required by law and specifically disclaims any duty to do so.

Previous Post
Next Post