Arete
Incident Response

No One Is Immune to Cyberattacks

IF YOU BELIEVE YOUR ORGANIZATION HAS BEEN COMPROMISED, IMMEDIATELY CONTACT US AT ARETE911@ARETEIR.COM.

On December 8, 2020, the New York Times reported that FireEye (NASDAQ:FEYE) was hacked. Moments later, almost every major news outlet, security blogger, U.S. government agency, and security company released additional articles and opinions on the breaking news. It's not often one of our own gets hacked, but when it happens, it's a glaring reminder about the industry we serve and how the information we protect can be the target of bad actors.

Among the many follow-on news alerts, one issued from the United States Computer Emergency Readiness Team ("US-CERT") stood out. As an organization within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"), US-CERT offers a notification service that delivers timely information about cyberthreat actor activities, recent campaigns, and indicators of compromise for threat hunting. US-CERT issued its own advisory, announcing the theft of FireEye tools and providing links to FireEye blogs for more information.

Similar to the hack involving stolen offensive tools from the NSA in 2017, it appears that the bad actors have taken control of FireEye's red team tools, which according to US-CERT, can be used to take control of target systems. Unlike the stolen tools from the NSA, US-CERT goes on to report that FireEye's tools do not contain zero-day exploits.

FireEye issued a public statement addressing the attack while providing around 300 countermeasures to detect the tools in use. The article can be viewed here and the company's countermeasures can be found on GitHub. The rules, provided by FireEye, were developed for Snort, Yara, ClamAV, and HXIOC. Arete immediately incorporated dozens of signatures for the stolen FireEye tools into threat hunting rules to protect our clients in the event someone tries to use those tools against them.

RECOMMENDATIONS:

- Update all security products with countermeasures provided by FireEye.
- Implement Enterprise Detection and Response ("EDR") software enterprise wide.
- Update all antivirus definitions, operating system patches, and firmware patches.
- Promote awareness and implement employee training within your organization about cybersecurity and scrutinizing emails with attachments or links.
- Disable external access to Remote Desktop Protocol ("RDP") or restrict RDP access to make it accessible through VPN only.
- Disable SMBv1 on all devices.
- Implement multi-factor authentication (MFA) across the enterprise, prioritizing domain admin and other high privilege-level accounts.

Arete Incident Response has an elite global team of incident response experts with unparalleled capabilities to assist clients in preparing for and defending themselves against cyber-attacks, from incident response readiness assessments and breach response to post-incident remediation and ongoing hunting services. The Arete team has a 15-year track record of performance solving the most challenging US and international breaches in a multitude of industries. Our core skills include triage, digital forensics, malware reverse engineering, remediation, managed detection response and testifying expertise. Arete works with organizations of all sizes to provide highly customized advice specific to the company's industry.