Arete
Incident Response

NO ONE IS IMMUNE TO CYBERATTACKS

From Cyber Firm FireEye to the U.S. Treasury

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

Last week, the New York Times reported that FireEye (NASDAQ:FEYE), a cybersecurity software firm, was hacked and "red team" cyber-defense software code was stolen (see Arete article here). And just yesterday (December 13), the New York Times reported that the U.S. Department of the Treasury was hacked.

Unfortunately, both attacks appear to be related to Russian bad actors in a wide-ranging assault. Arete believes these attacks are part of a very serious, widespread hacking campaign that is impacting both commercial and government enterprises. This campaign is global in scale and not bound by industry, geolocation, political affiliation, or an enterprise's public or private management status.

FireEye was the first major company to acknowledge being compromised as part of this campaign; the U.S. Department of the Treasury was the latest impacted enterprise. This is real. This is serious. And we highly recommend that everyone takes action to mitigate the attack vectors.

The new hack of the U.S. Department of the Treasury involved a compromise of the SolarWinds Orion infrastructure, and on December 13, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released Emergency Directive 21-01, "Mitigate SolarWinds Orion Code Compromise."

The Emergency Directive states "SolarWinds Orion products (affected versions are 2019.4 through 2020.2.1 HF1) are currently being exploited by malicious actors. This tactic permits an attacker to gain access to network traffic management systems. Disconnecting affected devices is the only known mitigation measure currently available." Arete immediately incorporated the signatures for the SolarWinds attack into threat hunting tools and provided CISA guidance to our clients. Arete has continued to enhance our signatures and detection capabilities to protect our MDR and vCISO clients.

Please follow the recommendations below and, if you believe you have been compromised, reach out to Arete or another cybersecurity provider for assistance.

RECOMMENDATIONS

- Immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from your network.
- Block all inbound/outbound traffic to the SolarWinds servers at firewall.
- Reset passwords on all accounts with local/domain admin on the SolarWinds servers.
- Identify and remove all threat actor-controlled accounts and identified persistence mechanisms.
- Reference https://attack.mitre.org/techniques/T1558/003/ for specific recommendations to mitigate against kerberoasting.
- Reference https://cyber.dhs.gov/ed/21-01/ for additional guidance and recommendations.

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.