Radware Cybersecurity Alert

The FireEye Hack: Insights Into Stolen Red Team Tools

Dec 14, 2020

The FireEye Hack

On December 1st, FireEye CEO Kevin Mandia announced that the company was hacked by what they believe was a sophisticated threat actor, one whose discipline, operational security and techniques lead them to believe it was a state-sponsored adversary.

What Was Stolen?

Consistent with a nation-state cyberespionage, the attacker sought information related to government customers. While the attacker was able to access some internal systems, at the moment of the announcement, there was no evidence of the attackers having exfiltrated confidential or sensitive data. FireEye did confirm that the attacker accessed and stole their red team assessment tools.

The stolen tools range from simple scripts used for automating reconnaissance to entire frameworks that are similar to publicly available technologies such as CobaltStrike and Metasploit. Many of the red team tools have already been released to the community and are already distributed in their open source virtual machine, CommandoVM.

The red team tools stolen by the attacker did not include zero-day exploits. The tools apply known and documented methods that are used by other red teams around the globe. Some of the tools are publicly available tools modified to evade basic security detection mechanisms. Other tools and frameworks were developed in-house by the FireEye red team. FireEye has published a collection of rules that provide countermeasures against the weaponized vulnerabilities used in their red team tools.

What Is A Red Team?

A cybersecurity red team is a group that helps organizations improve protection by acting as an opponent hacking group. Red teams perform vulnerability and penetration testing operations and develop in-house tooling or improve on publicly available tools to automate and improve efficiency.

Many organizations that work with sensitive information and are high value targets, such as Facebook, Netflix, Google, Amazon, etc., have their own red teams who continuously test and try to infiltrate their own organization. Organizations that do not have a resident red team can buy red team services from security organizations such as FireEye. There are many security vendors and consultancy organizations providing red team services.

If There Is A Red Team, There Is A Blue Team

The blue team is on the defensive side. Their job is to detect attacks as early as possible, assess the damage if attacks were successful, improve protection to prevent future attacks, and ensure adequate procedures for mitigation and improve incident response plans.

What Is The Impact Of FireEye Red Team Tools Being Stolen?

Based on the information disclosed in the announcement, the FireEye tools leverage only known vulnerabilities and tactics. It was explicitly mentioned that there are no zero-day exploits that were leaked through these tools. In consequence, Radware does not expect a global impact like we have witnessed from the Shadow Brokers leaks, the leaks that contained the EternalBlue exploit and were leveraged by WannaCry and NotPetya back in 2017.

That said, 300 red team tools that weaponize more than a dozen of the most popular vulnerabilities is concerning and the successful hack of a respected security organization such as FireEye demonstrates the difficulty of stopping determined and sophisticated attackers.

Whoever stole the tools have increased their offensive capability, but Radware does not expect a large fallout from this. While red teams are paid professionals, so are nation-state sponsored attackers and there is an expectation their capabilities are on par with red teams. However, tools are typically one of the indicators that can lead to attribution and when stolen tools are leveraged, it makes attribution of the attack much harder.

What Should Customers Do?

The stolen tools do not leverage unknown vulnerabilities or zero-day attacks, but they are still weaponized exploits that can be automated and leveraged to scale attacks. The stolen tools might have a higher degree of automation and integration compared to publicly available tools that were leveraged in the past.

Vulmon, a vulnerability search engine with vulnerability intelligence features, compiled a list of vulnerabilities based on the countermeasures published by FireEye (see below). Those vulnerabilities should be patched and mitigated as soon as possible if not already. Customers that were holding off on patching or upgrading certain systems should do so immediately.

What Is Radware Doing?

Many of the attack tools leverage well known and popular vulnerabilities, some of which were already mentioned on several occasions in publications and alerts by our threat intelligence team (see below). Countermeasures and signatures for most of the vulnerabilities are already available. Our cloud, application and network teams are reviewing the list of published rules and vulnerabilities and will publish additional updates, if necessary.

What To Expect From The Attacker(s)?

What will follow will mostly depend on the nature and tactics of the attacker. They might leverage the tools to automate their attacks and increase operations or they might leak the tools after leveraging them for highly visible hacks to create smokescreens and make attribution nearly impossible.

Vulnerabilities Leveraged By Stolen Tools

According to **Vulmon**, the list of vulnerabilities used by the stolen FireEye tools consists of:

- **CVE-2019-11510**: Pulse Secure Pulse Connect Secure unauthenticated path traversal
- **CVE-2020-1472**: Microsoft Active Directory privilege escalation vulnerability is also known as **Zerologon**
- **CVE-2018-13379**: Fortinet Fortigate SSL VPN unauthenticated path traversal
- **CVE-2018-15961**: Adobe ColdFusion remote code execution vulnerability
- **CVE-2019-0604**: Microsoft SharePoint remote code execution vulnerability
- **CVE-2019-0708**: Microsoft Windows Remote Desktop Services (RDS) remote code execution vulnerability also known as **BlueKeep**
- **CVE-2019-11580**: Atlassian Crowd remote code execution vulnerability
- **CVE-2019-19781**: Citrix Application Delivery Controller and Citrix Gateway remote code execution vulnerability
- **CVE-2020-10189** – RCE for Zoho ManageEngine Desktop Central remote code execution vulnerability
- **CVE-2014-1812**: Microsoft Windows local privilege escalation
- **CVE-2019-3398**: Atlassian Confluence authenticated remote code execution
- **CVE-2020-0688**: Microsoft Exchange remote code execution
- **CVE-2016-0167**: Local privilege escalation on older versions of Microsoft Windows
- **CVE-2017-11774**: Remote code execution in Microsoft Outlook via specially crafted URI (phishing) also known as Microsoft Outlook Security Feature Bypass Vulnerability
- **CVE-2018-8581**: Microsoft Exchange Server elevation of privilege vulnerability
- **CVE-2019-8394**: Zoho ManageEngine ServiceDesk Plus (SDP) unauthenticated file upload

References

- FireEye Announcement - **https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html**
- FireEye Red Team tool countermeasures - **https://github.com/fireeye/red_team_tool_countermeasures**
- Vulmon – Vulnerabilities Used by Stolen FireEye Tools - **https://blog.vulmon.com/vulmon/alerts/2020/07/21/vulnerabilities-used-by-stolen-fireeye-tools/**
- Radware Threat Advisory - Coronavirus: Security Recommendations For Remote Access Threats - **https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/coronavirus-remote-access-threats/**
- Radware Threat Advisory - Australian Cyberattacks - **https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/australian-cyberattacks/**
- FireEye, one of the world's largest security firms, discloses security breach - **https://www.zdnet.com/article/fireeye-one-of-the-worlds-largest-security-firms-discloses-security-breach/**

- FireEye Drops After Cybersecurity Company Says It Was Hacked - https://www.bloomberg.com/news/articles/2020-12-08/cybersecurity-firm-fireeye-says-it-was-targeted-by-hackers

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyberattacks 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.