Unauthorized Access of FireEye Red Team Tools

fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

Threat Research

FireEye

Dec 08, 2020

3 mins read

Threat Research

Overview

A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies —to significantly limit the ability of the bad actor to exploit the Red Team tools.

You can find a list of the countermeasures on the FireEye GitHub repository found HERE.

Red Team Tools and Techniques

A Red Team is a group of security professionals authorized and organized to mimic a potential adversary's attack or exploitation capabilities against an enterprise's security posture. Our Red Team's objective is to improve enterprise cyber security by demonstrating the impacts of successful attacks and by showing the defenders (i.e., the Blue Team) how to counter them in an operational environment. We have been performing Red Team assessments for customers around the world for over 15 years. In that time, we have built up a set of scripts, tools, scanners, and techniques to help improve our clients' security postures. Unfortunately, these tools were stolen by a highly sophisticated attacker.

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 our open-source virtual machine, CommandoVM.

Some of the tools are publicly available tools modified to evade basic security detection mechanisms. Other tools and frameworks were developed in-house for our Red Team.

No Zero-Day Exploits or Unknown Techniques

The Red Team tools stolen by the attacker did not contain zero-day exploits. The tools apply well-known and documented methods that are used by other red teams around the world. Although we do not believe that this theft will greatly advance the attacker's overall capabilities, FireEye is doing everything it can to prevent such a scenario.

It's important to note that FireEye has not seen these tools disseminated or used by any adversaries, and we will continue to monitor for any such activity along with our security partners.

Detections to Help the Community

To empower the community to detect these tools, we are publishing countermeasures to help organizations identify these tools if they appear in the wild. In response to the theft of our Red Team tools, we have released *hundreds* of countermeasures for publicly available technologies like OpenIOC, Yara, Snort, and ClamAV.

A list of the countermeasure is available on the FireEye GitHub repository found here. We are releasing detections and will continue to update the public repository with overlapping countermeasures for host, network, and file-based indicators as we develop new or refine existing detections. In addition, we are publishing a list of CVEs that need to be addressed to limit the effectiveness of the Red Team tools on the GitHub page.

FireEye Products Protect Customers Against These Tools

Teams across FireEye have worked to build the countermeasures to protect our customers and the broader community. We have incorporated these countermeasures into our products and shared these countermeasures with our partners, including the Department of Homeland Security, who have incorporated the countermeasures into their products to provide broad coverage for the community.

More information on the detection signatures available can be found in the GitHub repository.