Detecting Crimeware with a Stolen Software Signing Certificate

Industry

Manufacturing

Security Challenge

An advanced attacker with a stolen software signing certificate can easily bypass perimeter defenses.

Solution

Red Canary's Managed Endpoint Threat Detection Service

Key Benefits

- *Extensive threat detection*. Red Canary records all endpoint activity and automatically hunts for threats – from malware to advanced multi-stage targeted attacks.
- *Community protection.* Once a threat is detected against one customer, the Red Canary Threat Detection Engine and SOC begins reviewing all customers' activity for the same or similar threats.

Summary

Red Canary protected a leading international materials manufacturer from a crimeware threat that used a stolen software signing certificate to sign a malicious binary masquerading as a Java update.

The Problem

One of the hallmark traits of crimeware is dynamic generation of both file names and payloads, making it uncommon to observe the same filename across multiple hosts.

The Solution

Red Canary is able to detect crimeware by looking for behaviors that are indicative of initial infection vectors, persistence mechanisms and remote access tools. Most often, this occurs with the introduction and execution of new binaries within a customer environment.

When an organization enlists Red Canary to protect its endpoints, they tap into a detection service that has observed malicious activity and crimeware in many different verticals and organizations – and thus Red Canary's extensive knowledge of tactics, techniques and procedures (TTPS), including filenames and command-and-control (C2) hostnames.

The Details

Red Canary detected an unsigned crimeware-related payload within a customer environment, notified the customer, and the threat was remediated.

Several weeks later, Red Canary detected a different binary of the same name on the manufacturing company's network. While not a novel situation, this binary had been signed.

The Details (cont.)

Despite being abnormally named, the binary had a Java icon and the file metadata was representative of Java 6 update 31. It appeared as follows in Carbon Black:

File Version Metadata	
File Description	Java(TM) Web Start Launcher
File Version	6.0.310.5
Original Filename	javaws.exe
Internal Name	Java(TM) Web Start Launcher
Company Name	Sun Microsystems, Inc.
Product Name	Java(TM) Platform SE 6 U31
Product Version	6.0.310.5
Legal Copyright	Copyright © 2012

However, the digital signature metadata did not compute. The binary was signed, but not by Sun Microsystems.

Digital Signature Metadata	
Result	Signed
Publisher	G
Signed Time	2014-09-23T19:54:00Z
Issuer	Thawte Code Signing CA - G2
Subject	G
Result Code	0x0

The Red Canary research team was able to evaluate the binary and immediately determined it to be a modified version of Qbot/Qakbot backdoor. The issuer, Thawte, was notified of the compromise and the signing certificate was revoked and replaced. The Red Canary manufacturing customer responded to the threat, protecting their network from malicious activity.

Interested in learning how Red Canary can help defend your endpoints? Contact us at info@redcanary.co to schedule a demo.