CASE STUDY MANUFACTURING

# Detecting Crimeware with a Stolen Software Signing Certificate

### SECURITY CHALLENGE

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

### SOLUTION

Red Canary Managed Endpoint Detection & Response.

### 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.

### SNAPSHOT

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.

### CRIMEWARE: WHY IT'S DIFFICULT TO DETECT

Crimeware and ransomware authors are prolific and continue to rapidly deploy new and clever means of evading dynamic engines. 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.

### GOING BEYOND SIGNATURE-BASED DETECTION

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.

### DIGGING DEEPER

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.

red canary

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 The issuer, Thawte, was notified of the compromise and the signing certificate was revoked and replaced.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.

## MULTIFACETED BINARY ANALYSIS

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 |
| **Production Version:** | 6.0.310.5 |
| **Legal Copyright:** | Copywrite © 2012 |

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

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

## ABOUT RED CANARY:

Crimeware is just one of the many threats that Red Canary detects. The Managed Endpoint Detection and Response solution quickly and accurately identifies threats on customers' endpoints ranging from compromised credentials to lateral movement. Every threat is investigated by a Red Canary Analyst to remove false positives and provide the context required for remediation.

See how Red Canary can help defend your endpoints.

855.977.0686 | info@redcanary.com | www.redcanary.com