TALES FROM THE TRENCHES

Spearphishing Takeout

Technology alone does not fully protect against today’s sophisticated cyber attacks. FireEye Managed Defense (MD) analysts systematically hunt for evidence of activity from threat actors that continuously evolve and change their methods to try to establish a foothold in target environments while attempting to evade detection.

In a recent proactive hunting exercise, a Managed Defense analyst uncovered suspicious SSL activity that, after further review, was determined to have been generated as a result of a successful phishing attack from an unknown threat group.

After providing remediation recommendations to the customer, Managed Defense analysts initiated a Community Protection event to engage additional FireEye resources to collect new evidence across the FireEye ecosystem and bolster FireEye detections to ensure all of our customers were protected.

PROBLEM:
Suspicious SSL traffic evaded traditional detections.

HOW WE DID IT:
Uncovered via proactive hunting exercise.

HOW WE DID IT BETTER:
Frontline experience and home-grown tools used to collect and analyze data with limited visibility into customer environment.

RESULT:
Malicious activity mitigated, CPE event initiated, resulting in FireEye detections bolstered across products protecting entire customer base.
Spearphishing Takeout

**BUSINESS IMPACT**

The Managed Defense team systematically and proactively hunts for attacker activity that evades traditional security measures. This is the traditional cat-and-mouse attacker vs. security industry scenario.

In this case, analysts proactively uncovered suspicious SSL activity at one client, which turned out to be a successful phishing attack from an unknown threat group that had evaded the client’s traditional defenses.

This proactive hunting activity not only protected the client, it protected all FireEye customers as FireEye was able to bolster detections across the FireEye ecosystem to minimize risk for all of our customers.

**39%**
Advanced Threats Missed by Traditional Security Tools*  

**40%**
Organizations Using Hunting Proactively*  

---

* 2018 Threat Hunting Report
Spearphishing Takeout

FULL STORY

While proactively conducting hunting activities in a customer environment, a Managed Defense analyst noticed suspicious SSL traffic to a remote IP address and began to investigate further. Additional data was collected and analyzed to determine the suspicious SSL traffic was malicious.

The Managed Defense team determined that the suspicious network traffic was generated as a result of a successful phishing attack that resulted in the deployment of a previously unnamed malware, now known as DUOBEAN.

The Managed Defense team initiated a Community Protection event (CPE) to ensure all FireEye customers were aware of and protected against this newly discovered threat. Analysts reviewed data for all Managed Defense and FireEye product customers to look for similar activity.

The CPE led to analysts uncovering activity occurring at a Southeast Asian telecommunications corporation. The firm was targeted with more than two dozen emails that primarily contained themes on network strategy and a new VPN. All emails originated from the same sender address.

The archived attachments contained a mixture of benign decoys, malicious LNK files, and executables.

Further investigation of the activity confirmed that this additional activity was a new attacker method and warranted further investigation. FireEye was able to determine that this activity was being carried out by the same group of actors that leveraged QUASIFOUR malware against the telecommunications industry in Southeast Asia.

Analysts analyzed the campaign activity to identify the full scope and intent to ensure all FireEye customers were protected.

To summarize, all FireEye customers benefitted from the Managed Defense hunting activity at a single client, leading to the identification and eradication of compromise at multiple customers.

About DUOBEAN

DUOBEAN malware consists of a PE file without header, and a shellcode loader that is loaded into memory by a legitimate EXE and a malicious DLL via DLL side-loading. The PE payload, a plugin loader with little functionality of its own, is injected into a legitimate Windows process (e.g., msiexec.exe). It sends beacons to the configured command and control (C&C) address and expects to receive plugins to load directly into memory and commands to funnel to those plugins.

THREAT TYPE:
Previously Unknown

CAPABILITY:
"Trusted" stage 1 application which loads Stage 2 malware

MALWARE:
DUOBEAN