

FIREEYE LABS / FIREEYE THREAT INTELLIGENCE

# HIDING IN PLAIN SIGHT: FIREEYE AND MICROSOFT EXPOSE OBFUSCATION TACTIC

MAY 2015

REPORT

ireEye Threat Intelligence and the Microsoft Threat Intelligence Center investigated a command-and-control (CnC) obfuscation tactic used on Microsoft's TechNet, a web portal for IT professionals. TechNet's security was in no way compromised by this tactic, which is likely possible on other message boards and forums.

FireEye Threat Intelligence assesses that APT17, a China-based threat group, was behind the attempt. Other groups have used legitimate websites to host CnC IP address in the past. APT17 was embedding the encoded CnC IP address for the BLACKCOFFEE malware in legitimate Microsoft TechNet profiles pages and forum threads, a method some in the information security community call a "dead drop resolver." Encoding the IP address makes it more difficult to identify the true CnC address for network security professionals.

Few security companies have publicly discussed this tactic. After discovering the BLACKCOFFEE activity, the FireEye-Microsoft team encoded a sinkhole IP address into the profile pages and forum threads and locked the accounts to prevent the threat actors from making any changes. This collaborative approach allowed the team to observe the malware and its victims. Though the security community has not yet broadly discussed this technique, FireEye has observed other threat groups adopting these measures and expect this trend to continue on other community sites. Today, FireEye released Indicators of Compromise (IOCs) for BLACKCOFFEE and Microsoft released signatures for its anti-malware products.

Using Microsoft TechNet, a web portal for IT professionals, APT17 posted in forum threads and created profile pages to host encoded CnC IP addresses that would direct a variant of the BLACKCOFFEE backdoor to their CnC server.

## FIREEYE HAS OBSERVED THE CHINA-**BASED APT17 DISGUISING THEIR TRAFFIC**

APT17, also known as DeputyDog, is a Chinabased threat group that FireEye Intelligence has observed conducting network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. BLACKCOFFEE's functionality includes uploading and downloading files; creating a reverse shell; enumerating files and processes: renaming, moving, and deleting files; terminating processes; and expanding its functionality by adding new backdoor commands. FireEye has monitored APT17's use of BLACKCOFFEE variants since 2013 to masquerade malicious communication as normal web traffic by disguising the CnC communication as queries to web search engines.

### THREAT ACTORS' CnC: FROM OBVIOUSLY MALICIOUS TO THOUGHTFULLY OBFUSCATED

The use of BLACKCOFFEE demonstrates threat actors' evolving use of public websites to hide in plain sight. In the past, threat actors would modify easily compromised websites to host CnC commands and configuration, as observed in the China-based APT1's WEBCnC suite of backdoors. Now, threat actors are using well-known

Figure 1: The encoded IP address

websites-that they do not need to compromiseto host CnC IP addresses. They simply use the website for legitimate purposes, such as posting forum threads or creating profile pages.

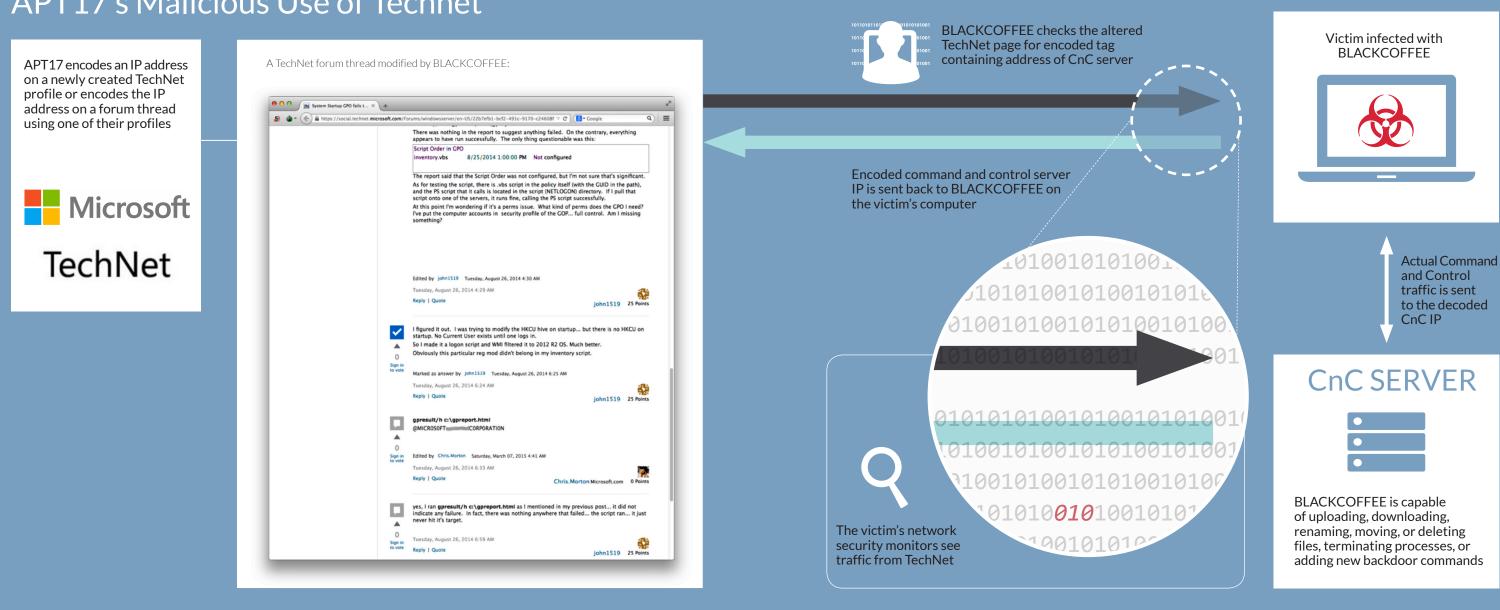
APT17 went further to obfuscate their CnC IP address and employed a multi-layered approach for the malware to finally beacon the true CnC IP. They used legitimate infrastructure—the ability to post or create comments on forums and profile pages-to embed a string that the malware would decode to find and communicate with the true CnC IP address. This additional obfuscation puts yet another layer between APT17 and the security professionals attempting to chase them down.

## HOW BLACKCOFFEE WORKS

This BLACKCOFFEE variant contains one or more URLs that link to the biography sections of attacker-created profiles as well as forum threads that contain comments from those same profiles. A URL is randomly selected and the malware searches at that location for an encoded IP address located between two tags, "@MICR0S0FT" and "CORPORATION".

#### @MICROSOFT<eight-character string with two characters per octet>CORPORATION

# APT17's Malicious Use of Technet



The malware then communicates directly with the retrieved and decoded IP address to receive commands and send stolen information. If the CnC server is discovered or shut down, the threat actors can update the encoded IP address on TechNet to maintain control of the victims' machines. BLACKCOFFEE supports an initial set of fifteen commands, including creating a reverse shell, uploading and downloading files, and enumerating files and processes. The attackers can also extend BLACKCOFFEE's functionality through additional commands sent as shellcode.

#### **IOCS/MD5S**

Indicators of compromise are available on Github at github.com/fireeye/iocs.

We have already observed threat actors adopting similar techniques and moving some CnC activity to legitimate websites that they do not need to compromise. In the same vein, some threat actors have already begun using social media sites such as Twitter and Facebook for malware distribution and CnC. APT17's tactic—using a dead drop resolver and embedding encoded IP addresses as opposed to displaying it in plain text-can delay detection, discourage IT staff from discovering the actual CnC IP address, and prevent discovery of the CnC IP via binary analysis. FireEye expects that threat groups are already using this technique, with their own unique variations, and others will adopt similar measures to hide in plain sight.

# **EXPECT MORE THREAT GROUPS TO EMPLOY LEGITIMATE** WEBSITES IN OPERATIONS

To download this or other FireEye Threat Intelligence reports, visit: https://www.fireeye.com/reports.html



FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com

© 2015 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. WP.HPS.EN-US.052015