Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant

By Ryan Sherstobitoff on Mar 08, 2018

Cryptocurrency, Hidden Cobra, Lazarus Group, Malware, Malware Analysis, Cheetah, Crackshot, and Bankshot Operation Blockbuster.

On February 23, the McAfee Advanced Threat Research team discovered that the Lazarus group (Hidden Cobra) continues to target financial institutions in Turkey with a new variant of the Bankshot implant. This campaign, which we have named Operation Blockbuster, is targeting the Turkish financial sector. Based on the code similarity, this malware is part of the Hidden Cobra campaign, which we have named Operation Cheetah and Operation Crackshot.

In this blog, we provide a technical analysis of the Hidden Cobra campaign and its use of Bankshot malware.

Hidden Cobra campaigns are known to be the Northern Korean cyber-espionage group. Hidden Cobra's campaigns have been active since at least 2009 and have been ongoing for at least the last two years. Hidden Cobra's campaigns have been known to target a variety of sectors.

Based on our analysis, Operation Blockbuster is a Trojan dropper and implant. The dropper is used to install a Bankshot implant. The Bankshot implant is a type of malware that allows the attacker to execute arbitrary commands on the victim's machine. The implant has capabilities to download and execute files, to upload files, and to delete files. The implant also has capabilities to enumerate and terminate processes, to enumerate and modify the registry, and to enumerate and modify the file system. The implant also has capabilities to enumerate and modify the network configuration and to enumerate network connections. The implant also supports a RAW protocol. In this blog we discuss Bankshot's capabilities in detail.

Dropper Analysis

The Trojan dropper is a Microsoft Windows Installer (MSI) file. The file is named Turkish-Airlines-Cancellation-Policy.msi. The file's SHA256 hash is:

- 2d7b0b7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d7d

The file has the capacity CD-R (650 MB).

The file's Universal Unique Identifier (UUID) is:

- {9E0A0A0A-0A0A-0A0A-0A0A-0A0A0A0A0A0A}

The file's Universal Unique Identifier (UUID) is:

- {9E0A0A0A-0A0A-0A0A-0A0A-0A0A0A0A0A0A}

The file's Universal Unique Identifier (UUID) is:

- {9E0A0A0A-0A0A-0A0A-0A0A-0A0A0A0A0A0A}

The following table lists the Bankshot implant's Portable Executable (PE) files:

SHA 1	Creation Date	Subject
2C9E7C0C0C0C0C0C0C0C0C0C0C0C0C0C0C0C0C	February 26, 2018	Microsoft Corporation
4ec7c2d57f0ee0f0f0f0f0f0f0f0f0f0f0f0f0	February 27, 2018	Microsoft Corporation
2dbdc0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0	February 27, 2018	Microsoft Corporation

Bankshot Malware Hashes

Dropper Analysis

The dropper's main executable is a Windows Installer Package with the filename Agreement.exe. The dropper's main executable is a Microsoft Installer Package. The dropper's main executable contains a Microsoft Installer Package. The dropper's main executable contains a Microsoft Installer Package. The dropper's main executable contains