China Chopper Malware Overview

Operational (OP) | Fusion (FS)

Cyber Espionage (CE)

April 18, 2017 04:02:00 PM, 16-00020834, Version: 2

OPERATING SYSTEM

DESCRIPTION

This is a simple code injection webshell that is capable of executing Microsoft .NET code within HTTP POST commands. This allows the shell to upload and download files, execute applications with web server account permissions, list directory contents, access Active Directory, access databases, and any other action allowed by the .NET runtime. This webshell is composed of at least two parts: a small bit of code on a server and a client that provides command and control (C&C). The webshell client, while not necessary, provides an easy-to-use front end and many commands necessary to conduct C&C of the compromised server. Because of the simplicity and variability of the contents of a malicious script, it is often not detected by anti-virus software. Rather, it must be detected via network traffic or manual detection on the victim computer using regular expressions (regexes).

FIREEYE DETECTION NAMES

Backdoor.APT.ChinaChopper

5950 Berkshire Lane, Suite 1600 Dallas, TX 75225