CLEANTOAD Malware Overview

Operational (OP) | Cyber Espionage (CE)

February 01, 2018 11:05:00 AM, 18-00001944, Version: 1

DESCRIPTION

CLEANTTOAD is a disruption tool that deletes file system artifacts, including those related to BLINDTOAD, and runs after a date obtained from a configuration file. The malware injects shellcode into notepad.exe and overwrites and deletes files, modifies registry keys, deletes services, and clears Windows event logs.

FIREEYE DETECTION NAMES

FE_APT_HackTool_Win_CLEANTOD_1

ROLE

Disruption Tool

5950 Berkshire Lane, Suite 1600 Dallas, TX 75225