

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

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: <https://intelligence.fireeye.com/reports/18-00001944>

© 2020, FireEye, Inc. All rights reserved.