S2W Intelligence Report_Form Book_20200722_web.pdf

Sida 2 av 9

2

‘FormBook Tracker’ unveiled on the Dark Web

Report ID : S2-CTI-20200034

Version: 1.0 (July. 21. 2020)

1. https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html

Figure 1: ‘FormBook Tracker’ site capture on the dark web

Executive Summary

S2W LAB has found ‘FormBook Tracker’ - the operation site of the malicious code ‘FormBook’ - on the dark web. The site contains information about 9,173 infected machines (as of 07/19) worldwide including affected machines’ OS, IP, date of Infection and last activity date etc. China, USA, and Turkey are top 3 countries which have the most infected machines based on the information from the site. All command and control (C&C, hereafter C2) servers are using hosting services from USA and Netherlands.

About FormBook1

FormBook is a data stealer and form grabber that has been advertised in various hacking forums since early 2016. The malware injects itself into various processes and installs function hooks to log keystrokes, steal clipboard contents, and extract data from HTTP sessions. The malware can also execute commands from a command and control (C2) server. The commands include instructing the malware to download and execute files, start processes, shutdown and reboot the system, and steal cookies and local passwords.

Source: https://drive.google.com/file/d/1oxINyIJfMtv_upJqRK9vLSchIBaU8wiU/view