‘FormBook Tracker’ unveiled on the Dark Web

By S2W

Published: 2021-01-29 · Archived: 2026-04-06 00:55:00 UTC

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.

Press enter or click to view image in full size

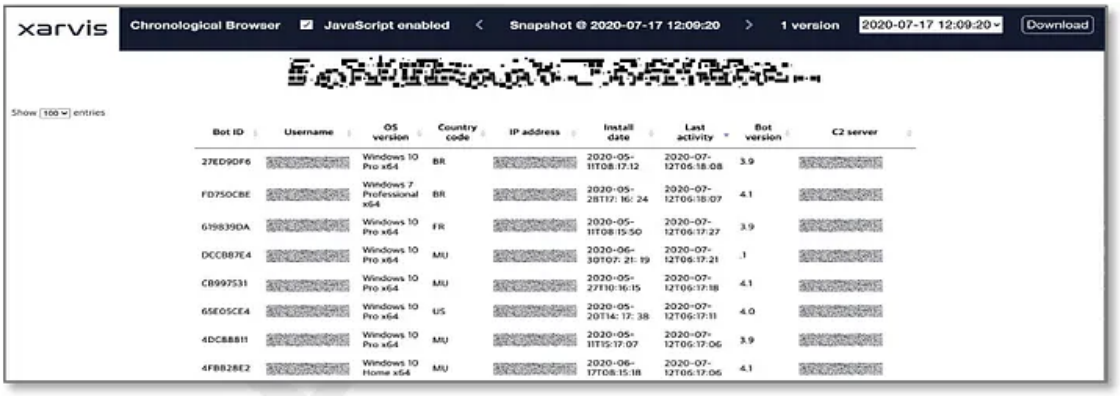


Figure 1: ‘FormBook Tracker’ site capture on the dark web

PDF Download : https://drive.google.com/file/d/1oxINyIJfMtv_upJqRK9vLSchIBaU8wiU

About FormBook

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.

Key Statistics for FormBook Infection in 2020

Press enter or click to view image in full size

Figure 2: Geographical mapping on infected machine

Geolocation of the infected machines were identified based on IP address. China (1,976), Turkey (647), USA (566), India (480), and Vietnam (344) are top 5 countries with number of infected machines.

Press enter or click to view image in full size

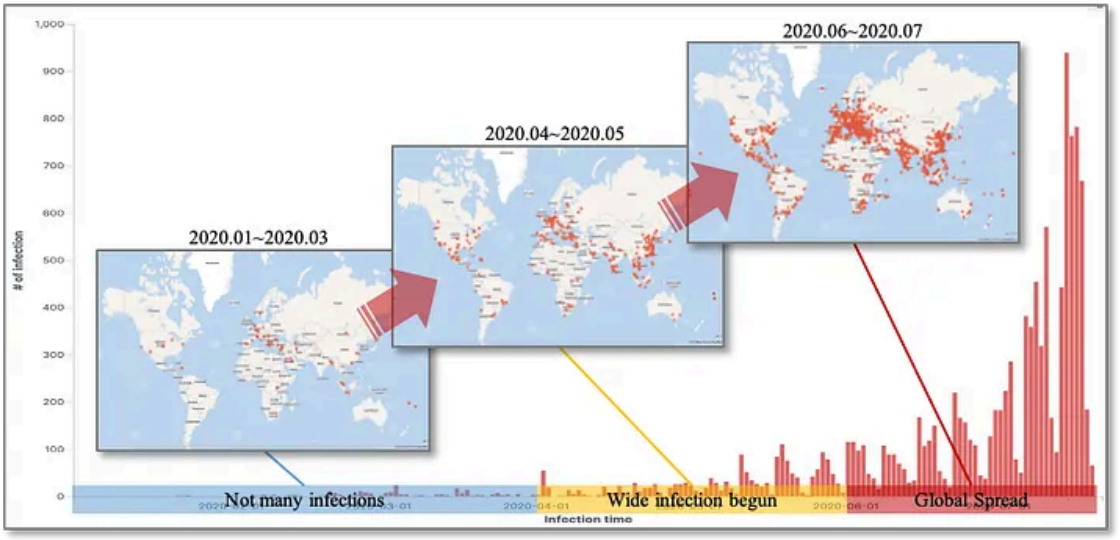


Figure 3: # of infected machine (unique IP address) by infection date (2020/01/01 to 2020/07/19)

The number of infected machines increased dramatically on July 2020. Not just number of infected machine, the spread of geographical region is mostly occurred in June ~ July period.

Press enter or click to view image in full size

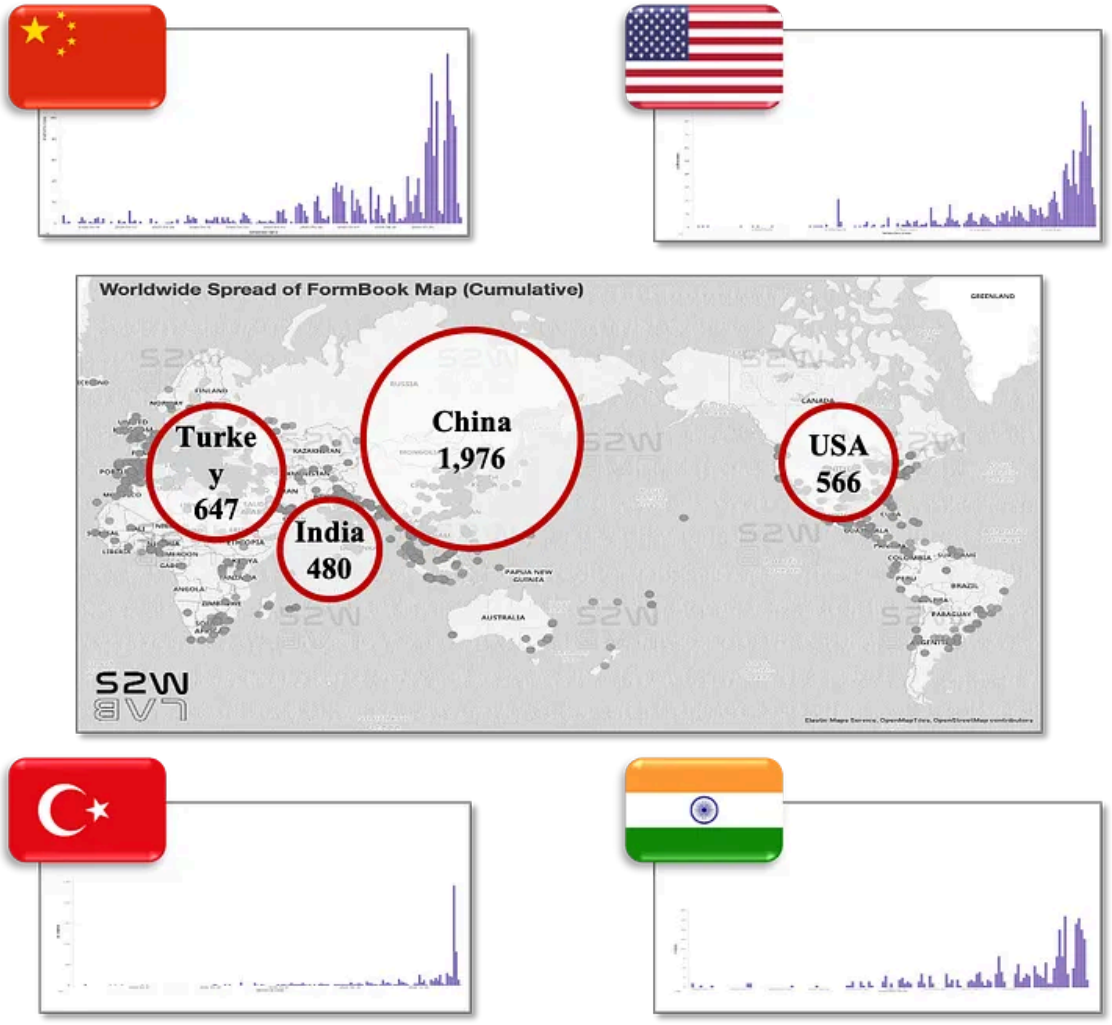


Figure 4: 2020 FormBook infection status for Top 4 countries

Press enter or click to view image in full size

Country	Total Infection (as of 07/19)	First Infection Date	Daily Infection Peak
China	1,976	2020/02/20	2020/07/14
Turkey	647	2019/11/27	2020/07/16
USA	566	2020/02/23	2020/07/14
India	480	2020/02/26	2020/07/10

Key Statistics for FormBook Infection in 2020 — South Korea

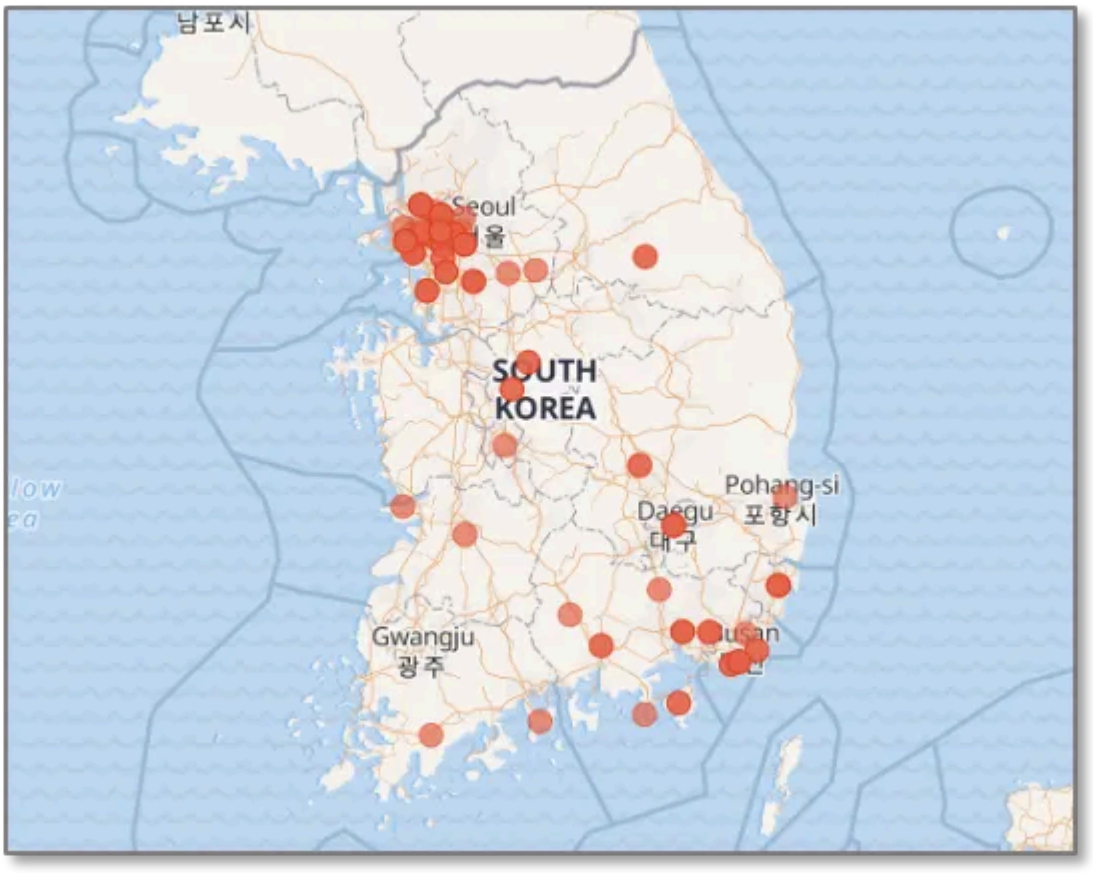


Figure 5: Geographical mapping on infected machine for South Korea

311 machines have been identified in South Korea. Most of infection in concentrated in metro area.

Press enter or click to view image in full size

Figure 6: # of infected machine (unique IP address) by infection date for South Korea (2020/04/27 to 2020/07/19)

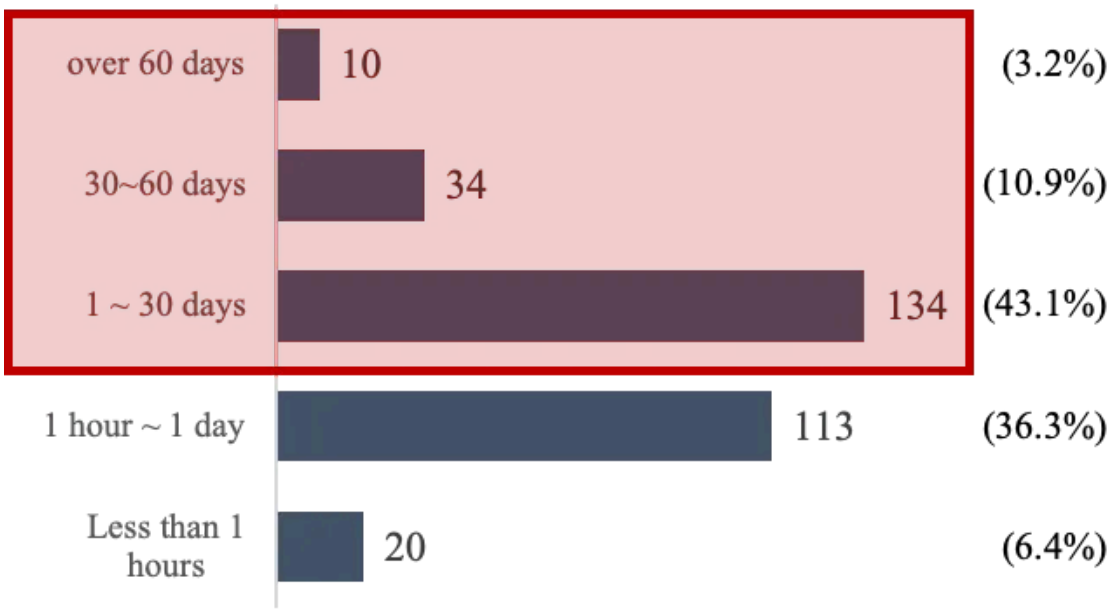
Infection of South Korea has started from April 27th. The infection speed drops on mid July; however, on July 14th, the number of daily infection suddenly hit its peak, and many infected machines were still alive after then.

Get S2W's stories in your inbox

Join Medium for free to get updates from this writer.

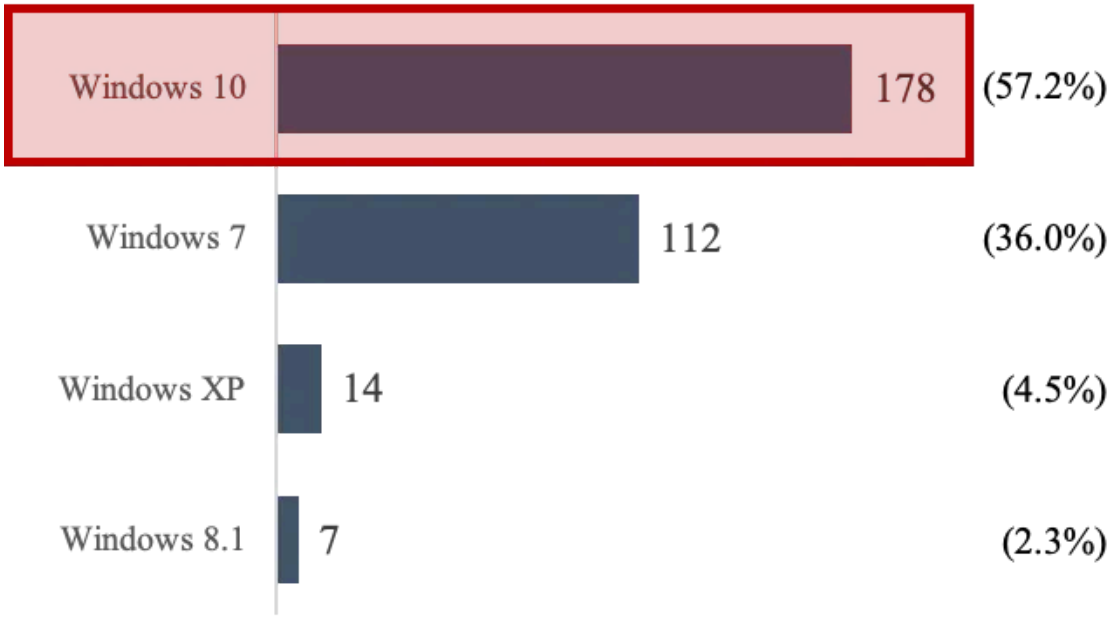
Remember me for faster sign in

In-depth analysis on infected machines from South Korea



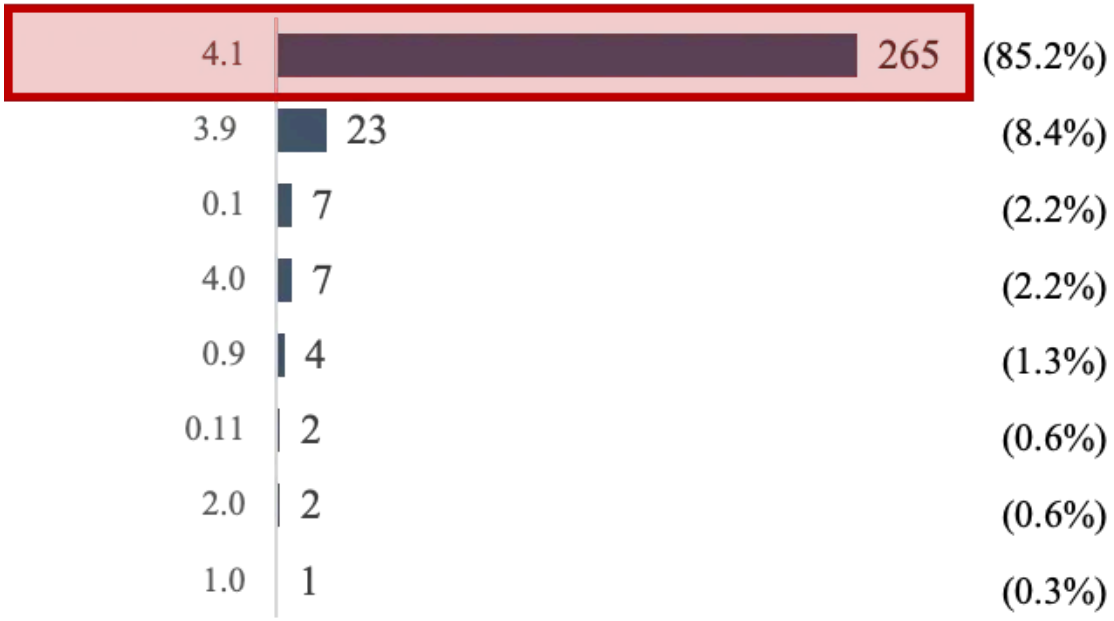
Bot Lifetime analysis (Total = 311)

In general, bot lifetimes are comparably long. 57.2% of infected machines' bot life-time is longer than 1 day. Only 20 out of 311 machines have less than an hour lifetime, which can be assumed as a 'Sandbox'.



Victim operating system (Total = 311)

Among the victims, Windows 10 is the most common operating system used. FormBook seems to target Windows OS and affect all versions including the most recent one.



Bot version (Total = 311)

FormBook version 4.1 is dominating the victim population which known to be the latest version and this might be the first report of its successful debut.

Key Findings

1. Operation FormBook is an ongoing threat campaign.

2. The operator behind the campaign has leveraged the dark web to monitor the compromised PCs and servers.

3. The operation has compromised at least 9,000 PCs/Servers worldwide, and at least 44 C2 servers has been operational.

4. A quick analysis on the operation site implicates that the potential secondary damage can be done as the life-time of communication between C2 and the compromised ones lasts more than a week.

5. Possible cases of malware communication,
5–1. A beacon lifetime of C2 and the target node is long that eventually compromised the node.
5–2. FormBook malware is preserved on the sandbox or in the same virtual machine image(identical SID) to monitor live C2 servers on purpose used by security team to counteract the malware.
5–3. Some of the victims appear to be the honeypots or relevant to security devices owned by business and public institutions.

Security advisory

It is recommended to the response team must update C2 domains and cut down the analyzing time/period that this type of operational page encourages attackers to advertise and capitalize their system to potential hackers/buyers by alluring them with those live information.

We will continue tracking ‘FormBook Tracker’ and report about new findings at www.s2wlab.com. Should you have any information that you think might be valuable to our research, please contact us at info@s2wlab.com.

Appendix — Identified C2 server list (updated on 2020–09–18)

artiyonq[.]com
becouf[.]com
chilogae[.]com
clickstrackings[.]com
discountsclicks[.]info
domaky[.]com
glamotd[.]com
funpexw[.]com
godhep[.]com
govaj[.]com
hearxy[.]com
howcuty[.]com
howndey[.]com
iskovlay[.]com
joomlas123[.]com
joomlas123[.]info
lodipytu[.]com
mafov[.]com
mansiobbok[.]info
mansiobok[.]com
mansiobok[.]info
nacemo[.]com
norjax[.]com
nyoxibwer[.]com
patlod[.]com
porcber[.]com
regular123[.]com
ranges-xx[.]com
regular8[.]info
regulars5[.]com
regulars6[.]com
regulars7[.]info
salomdy[.]com
sandrxy[.]com

slacktracks[.]com
spatren[.]com
stilonf[.]com
sudelt[.]com
sulicet[.]com
trancus[.]com
tromagy[.]com
ulxery[.]com
unlimitedgiveaways[.]xyz
utimake[.]com
vinoblay[.]com
worstig[.]com
writusp[.]com
yofdyk[.]com
masionlex[.]info
blindo[.]info

Press enter or click to view image in full size

About S2W LAB

S2W LAB is a big data intelligence company specialized in the **Dark Web and Crypto currencies.** The company captures a massive amount of data from various channels and conducts analysis with a unique AI based multi-domain analytic engine. **S2W LAB** offers a threat intelligence solution **‘S2-XARVIS’** and crypto currency Anti Money Laundering solution **‘S2-EYEZ’**
