Malware Masquerades as Privacy Tool

proofpoint.com/us/blog/threat-insight/malware-masquerades-privacy-tool

July 1, 2021

Blog
Threat Insight
Malware Masquerades as Privacy Tool

July 01, 2021 Selena Larson and Bryan Campbell

Key Findings

- Threat actors created a detailed, legitimate looking “Privacy Tools” website to trick victims into downloading malware.
- The Privacy Tools site purports to offer file protection via encryption and decryption services but leads to the installation of multiple malware families.
- Smoke Loader is downloaded first as the malicious executable which drops follow-on malware including Racoon Stealer and RedLine malware.

Overview

Proofpoint researchers found a new threat enticing users to download malware by masquerading as a “Privacy Tools” service offering a tool that “encrypts” user data using a zip-like utility. The fake website is professional-looking and contains detailed descriptions of the alleged service including step-by-step instructions on how to download the privacy tools – which turn out to be malware.

Proofpoint researchers identified the initial payload as Smoke Loader, a popular downloader available on easily accessible forums for buying and selling malware and used by multiple threat actors. The malware subsequently installs follow-on data-stealing malware including Raccoon Stealer and RedLine. While investigating the observed campaign, Proofpoint identified additional related samples publicly shared by other researchers since March 2021.

The privacy theme is ironic considering the ultimate payload is designed to exfiltrate information from an infected host. However, it may appeal to users who are concerned about data sharing and privacy – a number that is likely increasing due to the recent mainstream marketing of user-focused privacy controls from major companies like Apple.

Campaign Details

The threat actors created a website offering privacy tools for business and personal use.

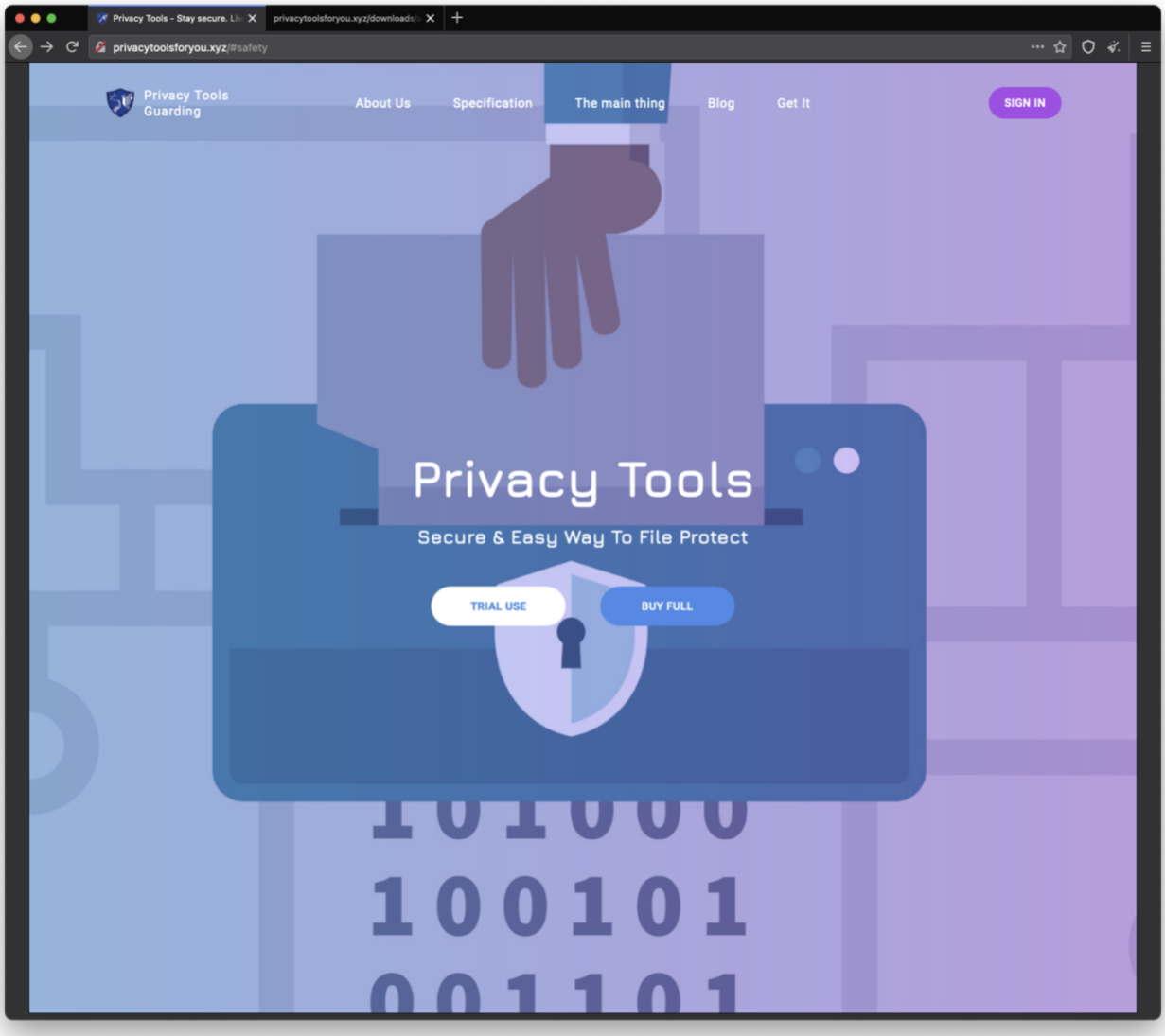

Figure 1: Screenshot of "Privacy Tools" website.

Visitors are instructed to download and install Privacy Tools software via a specific section of the website.

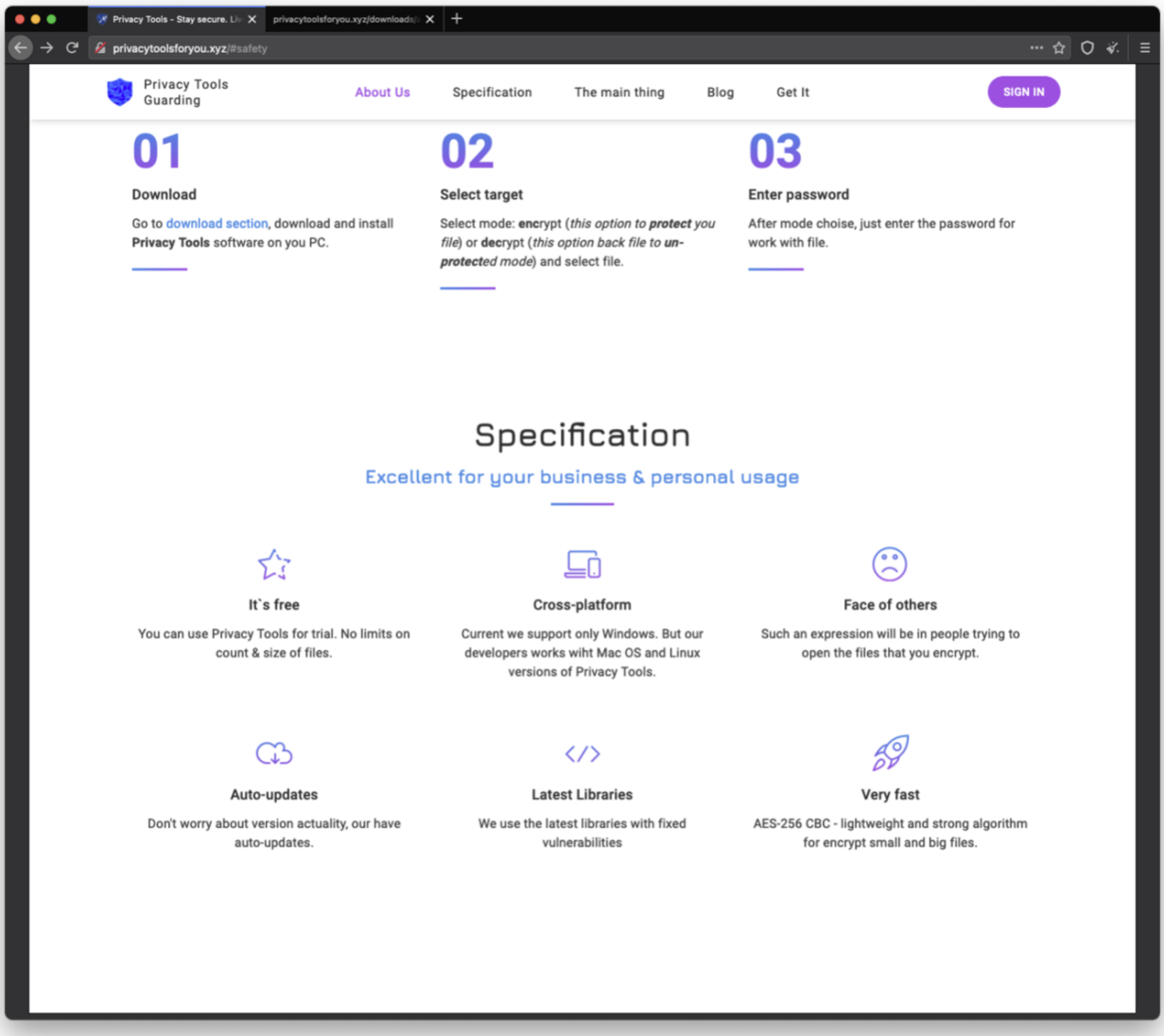

Figure 2: Screenshot of the Privacy Tools download instructions.

The compressed executables available for download purport to be file protection resources. The website actually downloads Smoke Loader, a modular downloader with multiple capabilities. Smoke Loader first appeared in 2011 and is available for purchase on criminal forums. It is commonly used by threat actors that target both individual and corporate users.

Proofpoint researchers observed that the Smoke Loader infection subsequently downloads follow-on malware to conduct information-gathering activities. Identified second-stage payloads include RedLine and Raccoon Stealer malware. Additional security researchers noticed this activity in 2021 along with Proofpoint observations.

Raccoon Stealer is an increasingly popular malware that first appeared in 2019. It was advertised as a “malware as a service” on cybercriminal forums. It can steal credentials such as passwords, website cookies, credit card data, system information, and bitcoin wallet contents. RedLine Stealer is a malware that aims to steal information from browsers such as

login, autocomplete, passwords, and credit cards. It also collects information about the user and their system, such as the username, location, hardware configuration, and installed security software. An update to RedLine Stealer in early 2021 also added the ability to steal cryptocurrency cold wallets.

Proofpoint does not attribute the activity to a specific group. One IP address identified in this campaign is associated with OpenNIC, a public service used for resolving certain types of domains that provides alternatives to domains not administered by ICANN. The privacy-themed websites delivering Smoke Loader in this campaign were registered by ssserviceshop1@yandex[.]ru via Registrar of Domain Names REG[.]ru, LLC. Multiple other privacy-themed domains and C2 IPs were also registered with the same email address and registrar.

Analyst Note:*Previous research published in May 2020 attributed a Smoke Loader-related domain registered with the same email and URL naming conventions as observed in this campaign to TA505. Proofpoint cannot confirm the veracity of that reporting. There is no available evidence to attribute the observed activity in the privacy-themed campaigns to TA505.*

Conclusion

The use of a privacy-themed lure to download information-stealing malware is an ironic yet predatory mechanism for enticing users to download malware. The lure is likely effective as the threat actors behind the campaign appear to have taken considerable time and effort to design a legitimate-looking privacy tool.

Based on additional indicators uncovered, it is likely this threat actor is conducting – and has previously conducted – similar campaigns using privacy themes and convincing lures to distribute Smoke Loader and follow-on malware. Proofpoint anticipates this type of theme and activity to continue, especially for consumers who do not have corporate privacy and security services already installed on their hosts.

Indicators of Compromise (IOCs)

Observed in Identified Smoke Loader Campaign

IOC	IOC Type	Description
privacytools[.]xyz	Domain	Website hosting fake privacy tool download
privacytoolsforyou[.]site	Domain	Website hosting fake privacy tool download

privacmytools[.]site	Domain	Website hosting fake privacy tool download
http://999080321newfolder1002002131-service1002[.]space/	URL	C2
http://999080321newfolder1002002231-service1002[.]space/	URL	C2
http://999080321newfolder3100231-service1002[.]space/	URL	C2
http://999080321newfolder1002002431-service1002[.]space/	URL	C2
http://999080321newfolder1002002531-service1002[.]space/	URL	C2
http://999080321newfolder33417-012425999080321[.]space/	URL	C2
http://999080321test125831-service10020125999080321[.]space/	URL	C2
http://999080321test136831-service10020125999080321[.]space/	URL	C2
http://999080321test147831-service10020125999080321[.]space/	URL	C2
http://999080321test146831-service10020125999080321[.]space/	URL	C2
http://999080321test134831-service10020125999080321[.]space/	URL	C2
http://999080321est213531-service1002012425999080321[.]ru/	URL	C2

http://999080321yes1t3481-service100201259990803 21[.]ru/	URL	C2
http://999080321test13561-service100201259990803 21[.]su/	URL	C2
http://999080321test14781-service100201259990803 21[.]info/	URL	C2
http://999080321test13461-service100201259990803 21[.]net/	URL	C2
http://999080321test15671-service100201259990803 21[.]tech/	URL	C2
http://999080321test12671-service100201259990803 21[.]online/	URL	C2
http://999080321utest1341-service100201259990803 21[.]ru/	URL	C2
http://999080321uest71-service100201dom25999080321[.]ru/	URL	C2
http://999080321test61-service100201259990803 21[.]website/	URL	C2
http://999080321test51-service100201259990803 21[.]xyz/	URL	C2
http://999080321test41-service100201pro25999080321[.]ru/	URL	C2
http://999080321yest31-service100201rus25999080321[.]ru/	URL	C2
http://999080321rest21-service100201259990803 21[.]eu/	URL	C2

http://999080321test11-service10020125999080321[.]press/	URL	C2
http://999080321newfolder4561-service10020125999080321[.]ru/	URL	C2
http://999080321rustest213-service10020125999080321[.]ru/	URL	C2
http://999080321test281-service10020125999080321[.]ru/	URL	C2
http://999080321test261-service10020125999080321[.]space/	URL	C2
http://999080321yomtest251-service10020125999080321[.]ru/	URL	C2
http://999080321yirtest231-service10020125999080321[.]ru/	URL	C2
http://999080321test391-service10020125999080321[.]ru/	URL	C2
http://999080321test481-service10020125999080321[.]ru/	URL	C2
http://999080321test571-service10020125999080321[.]pro/	URL	C2
http://999080321test461-service10020125999080321[.]host/	URL	C2
http://999080321test231-service10020125999080321[.]fun/	URL	C2
http://999080321tostest371-service10020125999080321[.]ru/	URL	C2

http://999080321oopoest361-service10020125999080321[.]ru/	URL	C2
http://999080321newfolder481-service10020125999080321[.]ru/	URL	C2
http://999080321newfolder471-service10020125999080321[.]ru/	URL	C2
http://999080321newfolder351-service10020125999080321[.]ru/	URL	C2
http://999080321newfolder241-service10020125999080321[.]ru/	URL	C2
http://999080321newfolder1002-service100201shop25999080321[.]ru/	URL	C2
http://999080321newfolder1002-service100201life25999080321[.]ru/	URL	C2
http://999080321newfolder1002-service100201blog25999080321[.]ru/	URL	C2
http://999080321megatest251-service10020125999080321[.]ru/	URL	C2
http://999080321infotest341-service10020125999080321[.]ru/	URL	C2
http://999080321besttest971-service10020125999080321[.]ru/	URL	C2
http://999080321shoptest871-service10020125999080321[.]ru/	URL	C2
http://999080321kupitest451-service10020125999080321[.]ru/	URL	C2

http://999080321proftest981-service10020125999080321[.]ru/	URL	C2
http://999080321clubtest561-service10020125999080321[.]ru/	URL	C2
http://999080321mytest151-service10020124259990803 21[.]ru/	URL	C2
http://999080321newfoldert161-service10020124259990803 21[.]ru/	URL	C2
http://999080321newfolder100251-service25999080321[.]ru/	URL	C2
http://999080321newfolder100241-service10020999080321[.]ru/	URL	C2
http://999080321newfolder100231-service1022020[.]ru/	URL	C2
http://999080321newfolder100221-service1022020[.]ru/	URL	C2
http://999080321newfolder1002-012525999080321[.]ml/	URL	C2
http://999080321newfolder1002-012625999080321[.]ga/	URL	C2
http://999080321newfolder1002-012725999080321[.]cf/	URL	C2
http://999080321newfolder1002-012825999080321[.]gq/	URL	C2
http://999080321newfolder1002-012925999080321[.]com/	URL	C2

http://999080321newfolder1002-01302599908032135[.]site/	URL	C2
http://999080321newfolder1002-01312599908032135[.]site/	URL	C2
http://999080321newfolder1002-01322599908032135[.]site/	URL	C2
http://999080321newfolder1002-01332599908032135[.]site/	URL	C2
http://999080321newfolder1002-01342599908032135[.]site/	URL	C2
http://999080321newfolder1002-01352599908032135[.]site/	URL	C2
http://999080321newfolder1002-01362599908032135[.]site/	URL	C2
http://999080321newfolder1002-01372599908032135[.]site/	URL	C2
http://999080321newfolder1002-01382599908032135[.]site/	URL	C2
http://999080321newfolder1002-01392599908032135[.]site/	URL	C2
http://999080321newfolder1002-01402599908032135[.]site/	URL	C2
http://999080321newfolder1002-01412599908032135[.]site/	URL	C2
http://999080321newfolder1002-01422599908032135[.]site/	URL	C2

http://999080321newfolder1002-01432599908032135[.]site/	URL	C2
http://999080321newfolder1002-01442599908032135[.]site/	URL	C2
http://999080321newfolder1002-01452599908032135[.]site/	URL	C2
http://999080321newfolder1002-01462599908032135[.]site/	URL	C2
http://999080321newfolder1002-01472599908032135[.]site/	URL	C2
http://999080321newfolder1002-01482599908032135[.]site/	URL	C2
http://999080321newfolder1002-01492599908032135[.]site/	URL	C2
http://999080321newfolder1002-01502599908032135[.]site/	URL	C2
http://999080321newfolder1002-01512599908032135[.]site/	URL	C2
http://999080321newfolder1002-01522599908032135[.]site/	URL	C2
http://999080321newfolder1002-01532599908032135[.]site/	URL	C2
http://999080321newfolder1002-01542599908032135[.]site/	URL	C2
http://999080321newfolder1002-01552599908032135[.]site/	URL	C2

192[.]71[.]245[.]208	IP	DNS
91[.]217[.]137[.]37	IP	DNS
172[.]104[.]136[.]243	IP	DNS
176[.]126[.]70[.]119	IP	DNS
94[.]103[.]153[.]176	IP	DNS
161[.]97[.]219[.]84	IP	DNS
207[.]192[.]71[.]13	IP	DNS
188[.]226[.]146[.]136	IP	DNS
178[.]63[.]116[.]152	IP	DNS
13[.]239[.]157[.]177	IP	DNS
0xa8e21be	SendRC4Key	RSA Encryption Key
0x8fc93161	RecvRC4Key	RSA Encryption Key