Privacy Tools (Not) for You

By Silent Push Threat Team

Published: 2021-12-03 · Archived: 2026-04-05 19:17:44 UTC

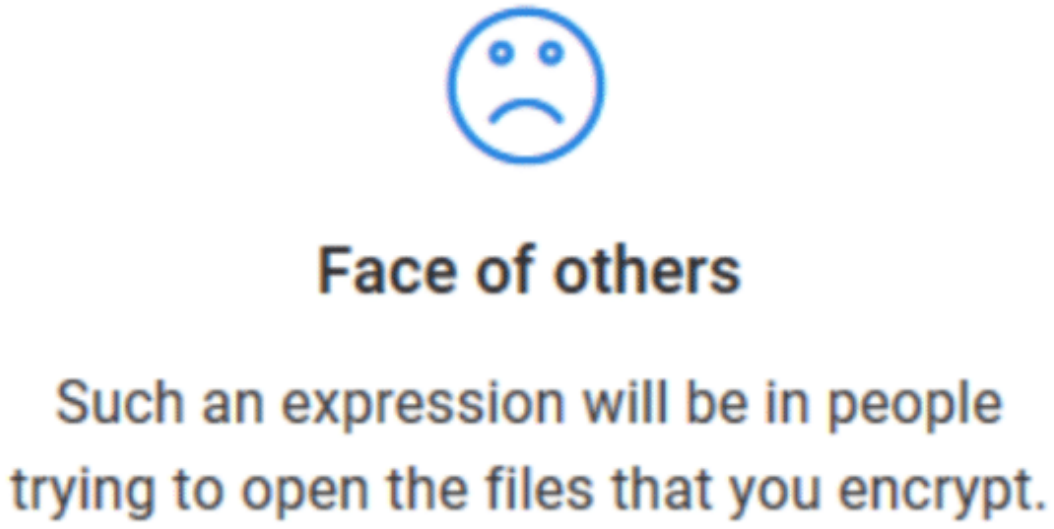
While looking through one of the malicious domain feeds managed for Silent Push customers, three interesting domains were noticed:

privacytoolzforyou-7000[.]com
privacytoolzfor-you7000[.]com
privacy-tools-for-you-777[.]com

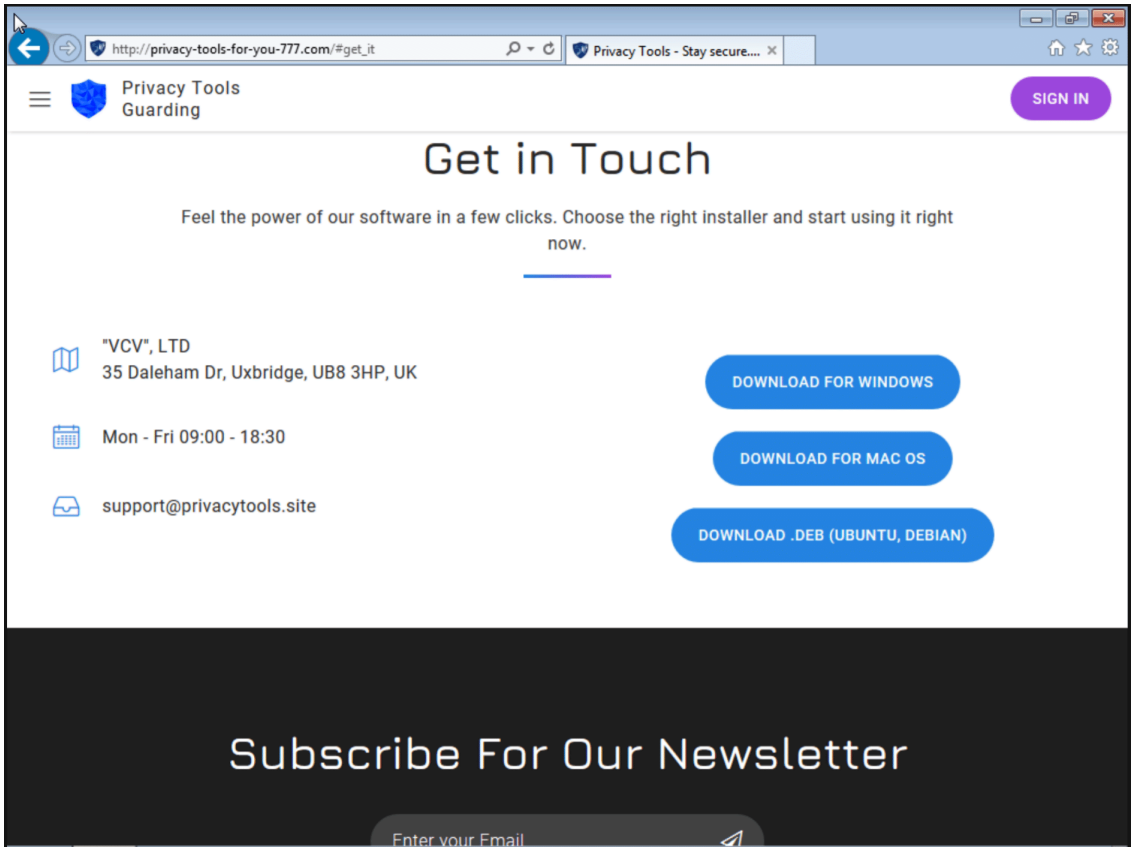
Curious to learn what was on these domains, the last one was opened in a safe environment. It was registered only yesterday (the other two domains were registered on 19 November), is currently live and was not detected by Safe Browsing, to which it has since been reported.

The site suggests it offers privacy tools as a “secure & easy way to file protect”:

The design of the website looks pretty slick and while clearly not written by a native speaker of English, it includes cute bits such as:



The options to sign in to the website or to purchase the full version of the product don’t appear to work (nor should one expect them to: the site is served over unencrypted HTTP), but thankfully there is a trial version that can be used.



The links to macOS and Linux versions of the product don't work, but the download for Windows works. It serves a Windows executable from:

http://privacy-tools-for-you-777[.]com/downloads/installer.exe

Unsurprisingly, the downloaded file received isn't a privacy tool at all, but a piece of malware. It has SHA256 hash 47906fc0ac7d3be54c62933e5f66a285cd34f161ce1d8a1bbdf80dc2e1df1441, though URlhaus reports that many others files have been served from the same URL.

All of these files have been detected as SmokeLoader, an old but still active malware downloader that has been used to serve other kinds of malware, such as the RedLine and Raccoon infostealers.

A search for similar domains in Silent Push's database gave 26 domains in total, such as privacy-toolz-for-you-3000[.]top and privacytoolsforyoufree[.]xyz, some going back as early as June of this year (see the full list at the bottom of this post).

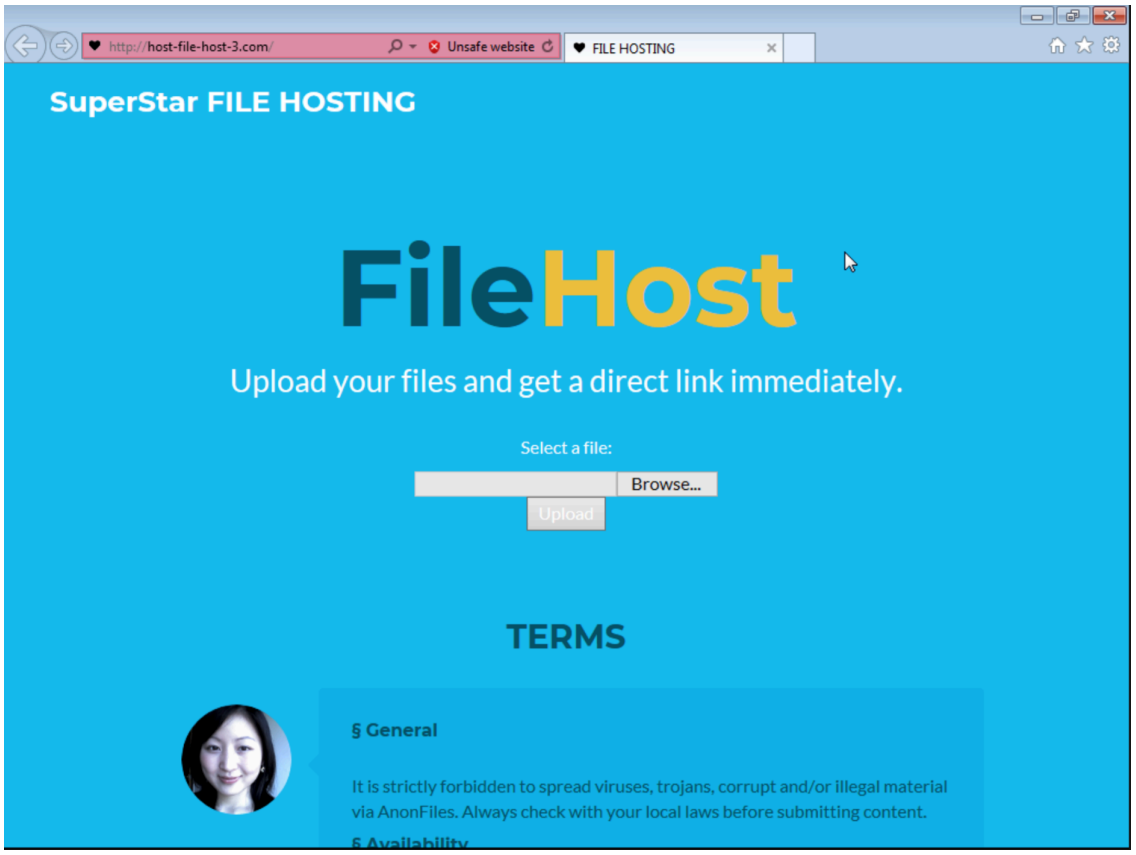
Most of these were active for a few weeks or even less. There is strong evidence to suggest they were run by the same actor and also served SmokeLoader; see for example this entry in URLhaus. This Proofpoint blog post, which shows the same Privacy Tools website, suggests the campaign may go back even further.

The campaign switched to its current bulletproof hosting provider, which is currently being tracked, some time in September.

Rogue file hosters

Interestingly, the malicious file downloaded has also been served from host-data-coin-11[.]com. This is likely more than a coincidence: the file is on the same Silent Push feed and uses the same bulletproof infrastructure. A search for domains with a similar pattern returned eighteen more domains, all of which use the same infrastructure.

At least one of these domains is still active and after clicking through the Safe Browsing warning, ended up on a 'Superstar file hosting' website.



A file was able to be selected from a computer — only .exe files appear to be allowed — and uploaded, after which a URL was provided that did indeed serve the very same file that had uploaded. The same URL pattern has been seen in malware served from those domains and seems likely that this front-end has also been used by the actors themselves.

Interestingly, some of these domains also appear to have been served as C2 domains for SmokeLoader, as can be seen in this sandbox report.

Conclusion

It is unclear what the exact link is between the two kinds of domains, but it is very likely they are operated by the same actor.

It is also unclear in what context the URLs were served, but it's possible that they have been distributed in specific places, such as forums for cryptocurrency enthusiasts, which are a popular target for infostealers.

Silent Push maintains many feeds for its customers, that often include domains like the ones mentioned in the blog post, even before they become active. The Silent Push API, which supports regular expressions, allowed me to search for similar domains.

Indicators of compromise

Fake privacy tools:

privacy-tools-for-you-777[.]com
privacy-toolz-for-you-3000[.]top
privacy-toolz-for-you-403[.]top
privacy-toolz-for-you-404[.]top
privacy-toolz-for-you-5000[.]top
privacy-toolz-for-you-502[.]top
privacy-toolz-for-you-503[.]top
privacytools-for-you3000[.]xyz
privacytools1234foryou[.]xyz
privacytoolsforyou[.]xyz
privacytoolsforyoufree[.]xyz
privacytoolz123foryou[.]club
privacytoolz123foryou[.]top
privacytoolz123foryou[.]xyz
privacytoolzfor-you5000[.]top
privacytoolzfor-you6000[.]top
privacytoolzfor-you7000[.]com
privacytoolzfor-you7000[.]top
privacytoolzforyou-5000[.]top
privacytoolzforyou-6000[.]top
privacytoolzforyou-7000[.]com
privacytoolzforyou-7000[.]top
privacytoolzforyou[.]xyz
privacytoolzforyou5000[.]top
privacytoolzforyou6000[.]top
privacytoolzforyou7000[.]top

File hosters and/or SmokeLoader C2:

coin-coin-coin-2[.]com
file-file-file1[.]com
file-file-file2[.]com
file-file-host4[.]com
file-file-host6[.]com
file-file-host8[.]com
file-host-host0[.]com

file-host-host6[.]com
host-coin-data-1[.]com
host-data-coin-11[.]com
host-file-file0[.]com
host-file-file4[.]com
host-file-host-3[.]com
host-file-host0[.]com
host-file-host6[.]com
host-file-host9[.]com
host-host-file6[.]com
host-host-file8[.]com
host-host-host5[.]com

Would you like to use our feeds or platform to protect your organization? Please contact Silent Push so we can help you.
