

Stantinko: A massive adware campaign operating covertly since 2012

By Frédéric VachonMatthieu Faou

Archived: 2026-04-05 15:41:55 UTC

ESET Research

Since the beginning of 2017, ESET has been conducting an investigation into a complex threat mainly targeting Russia and Ukraine. Stantinko has stood out.

20 Jul 2017 • , 6 min. read

Overview

Since the beginning of 2017, ESET researchers have been conducting an investigation into a complex threat mainly targeting Russia and Ukraine. Standing out because of its prevalence and its sophistication, Stantinko turned out to be quite a puzzle to solve. Slowly putting the pieces together, the global picture began to take shape, exposing a massive adware campaign affecting approximately half a million users.

Making heavy use of code encryption and rapidly adapting so as to avoid detection by anti-malware, Stantinko's operators managed to stay under the radar for at least the last five years, attracting very little attention to their operations.

To infect a system, they trick users looking for pirated software into downloading executable files sometimes disguised as torrents. FileTour, Stantinko's initial installation vector, then loudly installs a lot of software to distract the user while it covertly installs Stantinko's first service in the background. Video 1 shows a fictive user running the malicious executable.

Video 1. Video of a user downloading and running the malicious file

Ett fel inträffade.

Det går inte att köra JavaScript.

Stantinko's operators control a huge botnet that they monetize mainly by installing malicious browser extensions that perform ad injection and click fraud. However, they don't stop there. The malicious Windows services they install enable them to execute *anything* on the infected host. We've seen them being used to send a fully featured backdoor, a bot performing massive searches on Google, and a tool performing brute-force attacks on Joomla and WordPress administrator panels in an attempt to compromise and potentially resell them.

Figure 1 shows the full Stantinko threat from the infection vector to the final persistent services and related plugins.

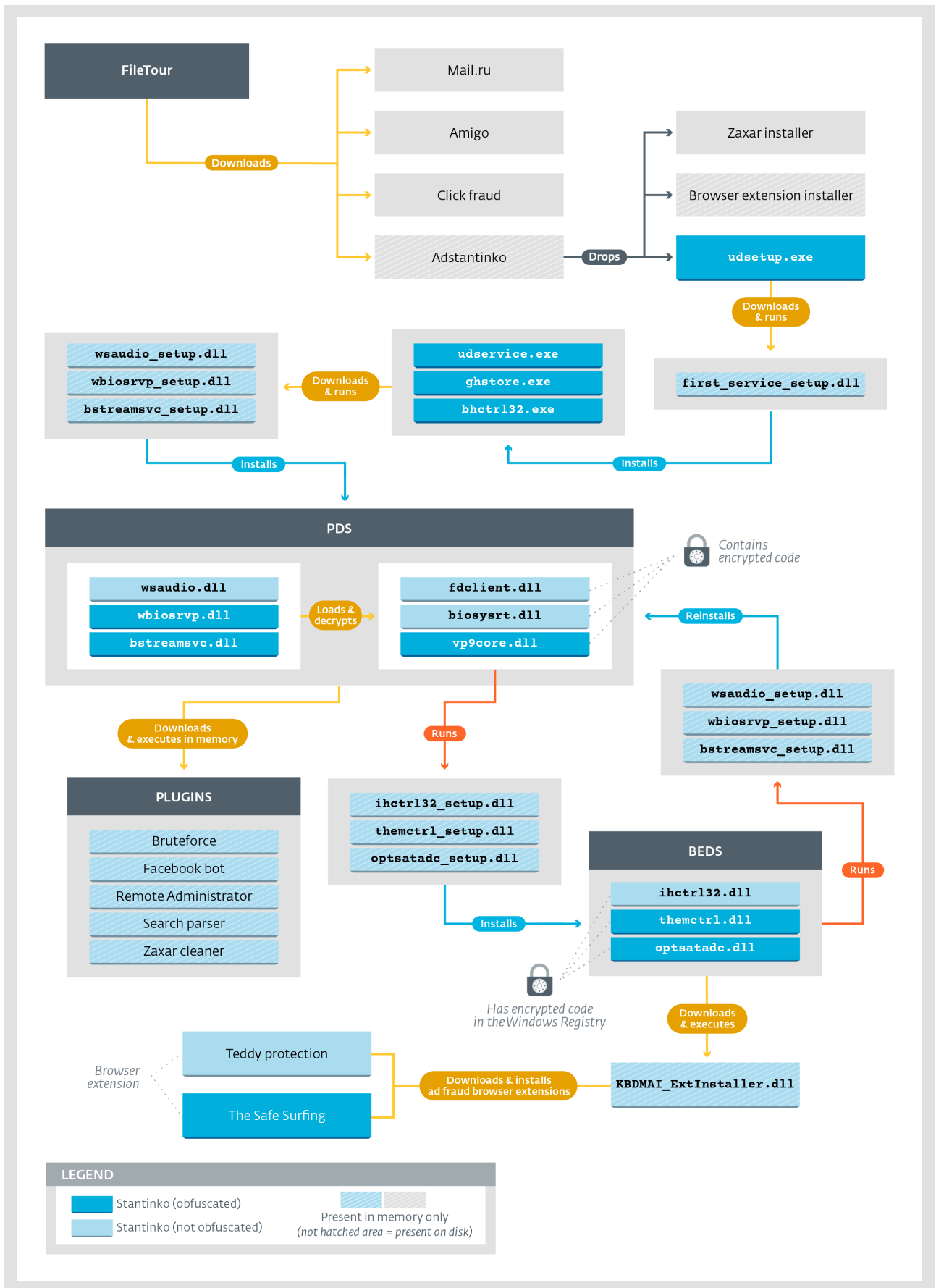


Figure 1 – Full diagram of the Stantinko threat

Key features

Stantinko stands out in the way it circumvents antivirus detection and thwarts reverse engineering efforts to determine if it exhibits malicious behavior. To do so, its authors make sure multiple parts are needed to conduct a complete analysis. There are always two components involved: a loader and an encrypted component. The malicious code is concealed in the encrypted component that resides either on the disk or in the Windows Registry. This code is loaded and decrypted by a benign-looking executable. The key to decrypt this code is generated on a per-infection basis. Some components use the bot identifier and others use the volume serial number from its victim PC's hard drive. Making reliable detections based on the non-encrypted components is a very difficult task, since artifacts residing on the disk do not expose malicious behavior until they're executed.

Moreover, Stantinko has a powerful resilience mechanism. After a successful compromise, the victim's machine has two malicious Windows services installed, which are launched at system startup. Each service has the ability to reinstall the other in case one of them is deleted from the system. Thus, to successfully uninstall this threat, both services must be deleted at the same time. Otherwise, the C&C server can send a new version of the deleted service that isn't detected yet or that contains a new configuration.

Stantinko's main functionality is to install malicious browser extensions named *The Safe Surfing* and *Teddy Protection*. Both extensions were available on the Chrome Web Store during our analysis. At first sight, they look like legitimate browser extensions that block unwanted URLs. However, when installed by Stantinko, the extensions receive a different configuration containing rules to perform click fraud and ad injection. In Video 2, the *The Safe Surfing* extension is installed. The user is redirected when clicking a link on the Rambler search engine.

Teddy Protection
offered by teddy-protection.com
★★★★★ (1671) | [Accessibility](#) | 481,817 users

AVAILABLE ON CHROME

OVERVIEW | REVIEWS | SUPPORT | RELATED

ТЕДДИ ЗАЩИТА

Безопасный интернет: surfите уже сегодня!
Вам надоели бороздки с вирусами?
Тревожит, что Ваши дети могут получить нежелательную и даже опасную информацию?
Вас беспокоит безопасность персональных данных?
Teddy Protection - новое расширение.
Наш "Безопасный" Teddy с легкостью защитит Вас и Вашего ребенка от мошеннических действий разработчиков, создающих опасные сайты.

БЕЗОПАСНЫЙ САЙТ
Вы уверены этот сайт не безопасный?
информация об этом сайте
teddy-protection.com

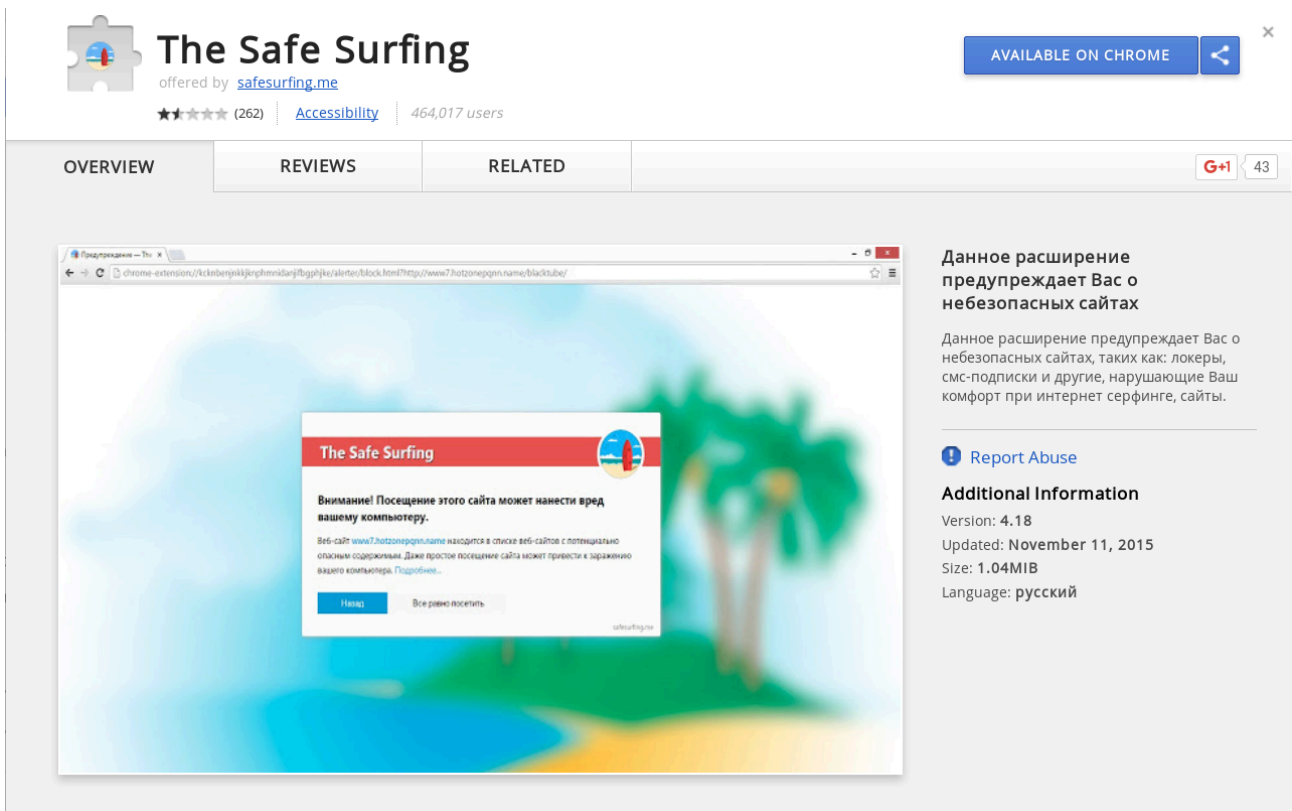
Контроль рекламы
Защитное подключение к сайту HTTPS
Отсутствие агрессивной рекламы
Отсутствие сайтов и черных списков
Ваше мнение о безопасности сайта

вирусы | ПОЧТОВЫЕ ПОДПИСКИ | БЛОКИРОВАНИЕ

Website
Report Abuse

Additional Information
Version: 2.5.1
Updated: March 6, 2017
Size: 144KiB
Languages: See all 3

Figure 2 – Teddy Protection on the Chrome Web Store



Video 2. Search traffic redirection on Rambler website



Stantinko is a modular backdoor. Its components embed a loader allowing them to execute any Windows executable sent by the C&C server directly in memory. This feature is used as a very flexible plugin system allowing the operators to execute anything on an infected system. Table 1 is a description of known Stantinko plugins.

Table 1. Known Stantinko Plugins

Module Name	Analysis
Brute-force	Distributed dictionary-based attack on Joomla and WordPress administrative panels.
Search Parser	Performs massive distributed and anonymous searches on Google to find Joomla and WordPress websites. It uses compromised Joomla websites as C&C servers.
Remote Administrator	Backdoor that implements a full-range of actions from reconnaissance to data exfiltration.
Facebook Bot	Bot performing fraud on Facebook. Its capabilities include creating accounts, liking picture or pages, and adding friends.

Monetization

Although the developers of Stantinko use methods that are most often seen in APT campaigns, their final aim is to make money. Thus, they are present in one of the most profitable cybercrime markets.

First, these days click fraud is a major source of revenues in the cybercrime ecosystem. [Research](#) conducted by the firm White Ops and the Association of National Advertisers (US) has estimated the global cost of click fraud in 2017 will be \$6.5 billion.

As explained above, Stantinko installs two browser extensions, *The Safe Surfing* and *Teddy Protection*, which inject advertisements or redirect the user. It allows the Stantinko operators to be paid for the traffic they provide to advertisers. Figure 4 is a summary of the redirection process.

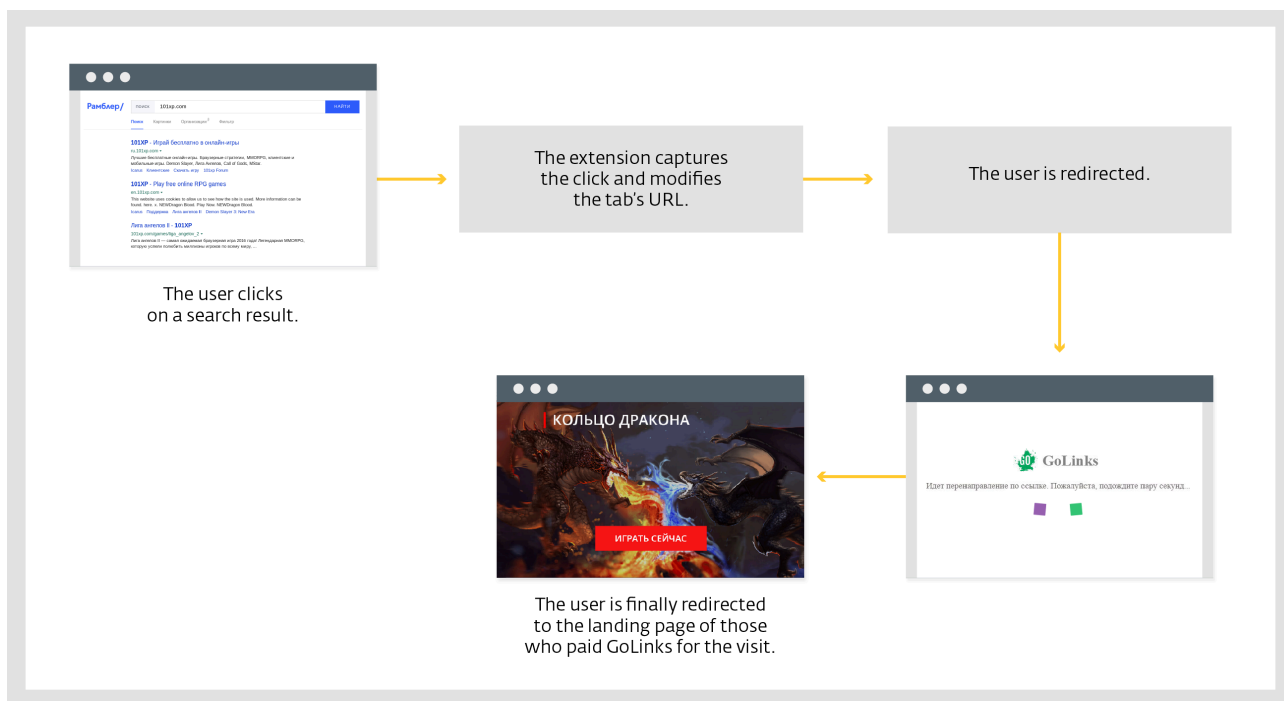


Figure 4 – Click fraud redirection process

Our study also shows that they are really close to the advertisers. In some cases, including the example in Figure 4, the user will reach the advertiser's website directly after the Stantinko-owned ad network. On the other hand, traditional click-fraud malware relies on a series of redirections between several ad networks to launder their malicious traffic. This shows that not only are the Stantinko operators able to develop highly stealthy malware, but they are also able to abuse the traditional ad-serving economy without getting caught.

Second, they are also trying to gain fraudulent access to the administrative accounts of Joomla and WordPress websites. Their attack relies on a brute-force attack using a list of credentials. The aim is to guess the password by trying tens of thousands of different credentials. Once compromised, these accounts can be resold on the underground market. Then, they could be used to redirect site visitors to exploit kits elsewhere or to host malicious content.

Third, our study also shows how Stantinko perpetrates social network fraud. This type of fraud has already been described by ESET researchers in the [Dissecting Linux/Moose](#) white paper. It is really profitable as, for instance, prices are around \$15 per 1000 Facebook likes even though they are actually generated by fake accounts controlled by a botnet.

The Stantinko operators developed a plugin that can interact with Facebook. It is able, among other things, to create accounts, 'like' a page or add a friend. To bypass Facebook's CAPTCHA, it relies on an online anti-CAPTCHA service pictured in Figure 5. The size of the Stantinko botnet is an advantage as it allows its operators to distribute the queries among all the bots. Thus, it is more difficult for Facebook to detect this type of fraud.

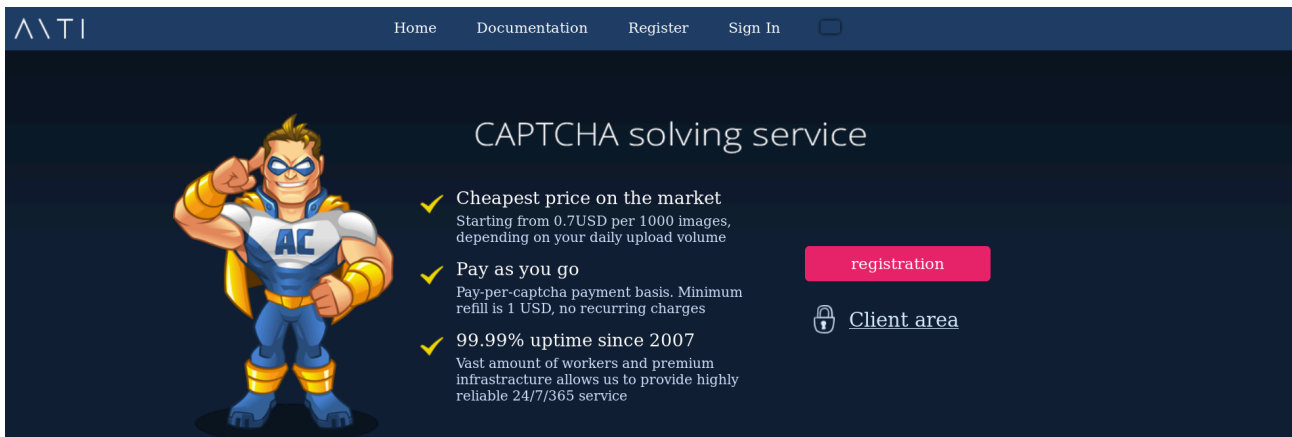


Figure 5 – Anti-CAPTCHA service used by Stantinko

Conclusion

Stantinko is a botnet mostly dedicated to ad-related fraud. Using advanced techniques such as code encryption and storing code in the Windows Registry, its operators were able to stay under the radar for the past five years. This led to a botnet of approximately 500,000 infected machines.

They were also able to publish their two ad injection browser extensions on the Chrome Web Store. One of them was first released on the Chrome Web Store in November, 2015.

Even though it isn't noticeable to the user, due to the absence of CPU intensive tasks, Stantinko is a major threat, as it provides a large source of fraudulent revenue to cybercriminals. Moreover, the presence of a fully featured backdoor allows the operators to spy on all the victimized machines.

For a comprehensive technical analysis of Stantinko, refer to our [white paper](#). The Indicators of Compromise are provided on our [GitHub account](#). For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com.

Source: <https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/>