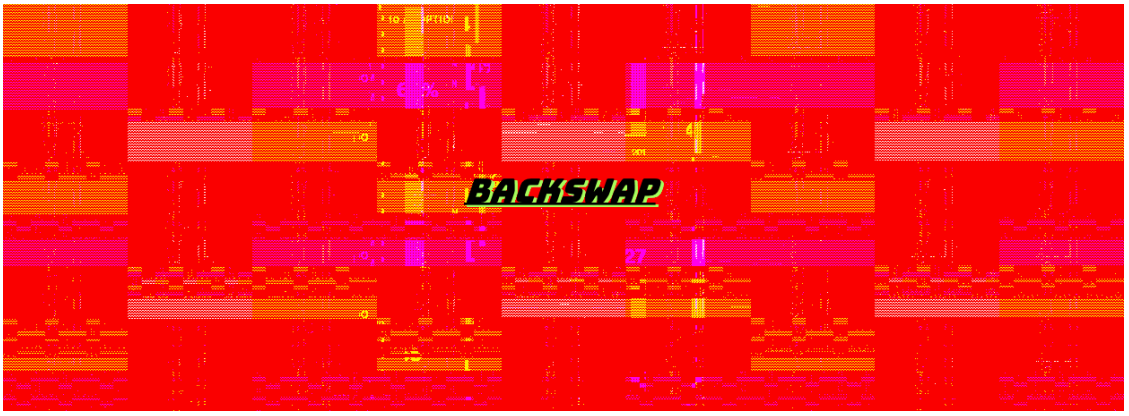
BackSwap Banking Trojan Uses Never-Before-Seen Techniques

By Catalin Cimpanu

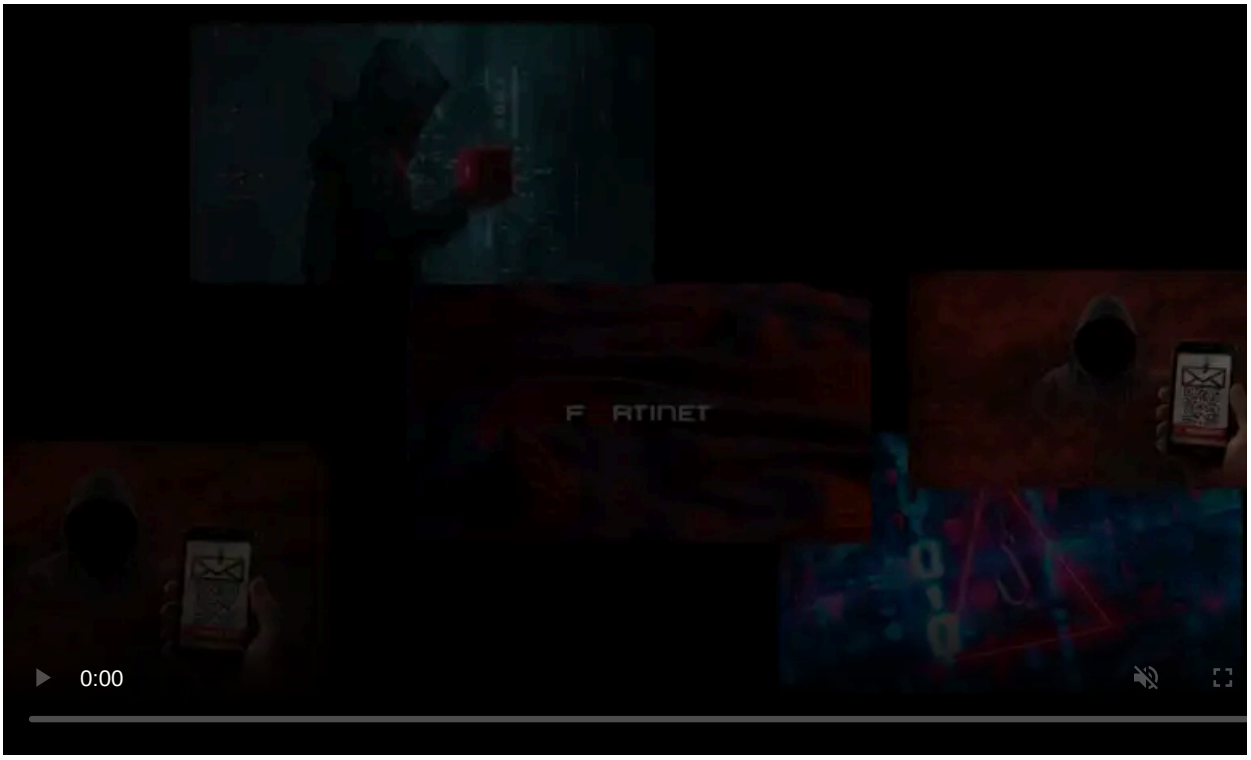
Published: 2018-05-25 · Archived: 2026-04-05 22:41:14 UTC

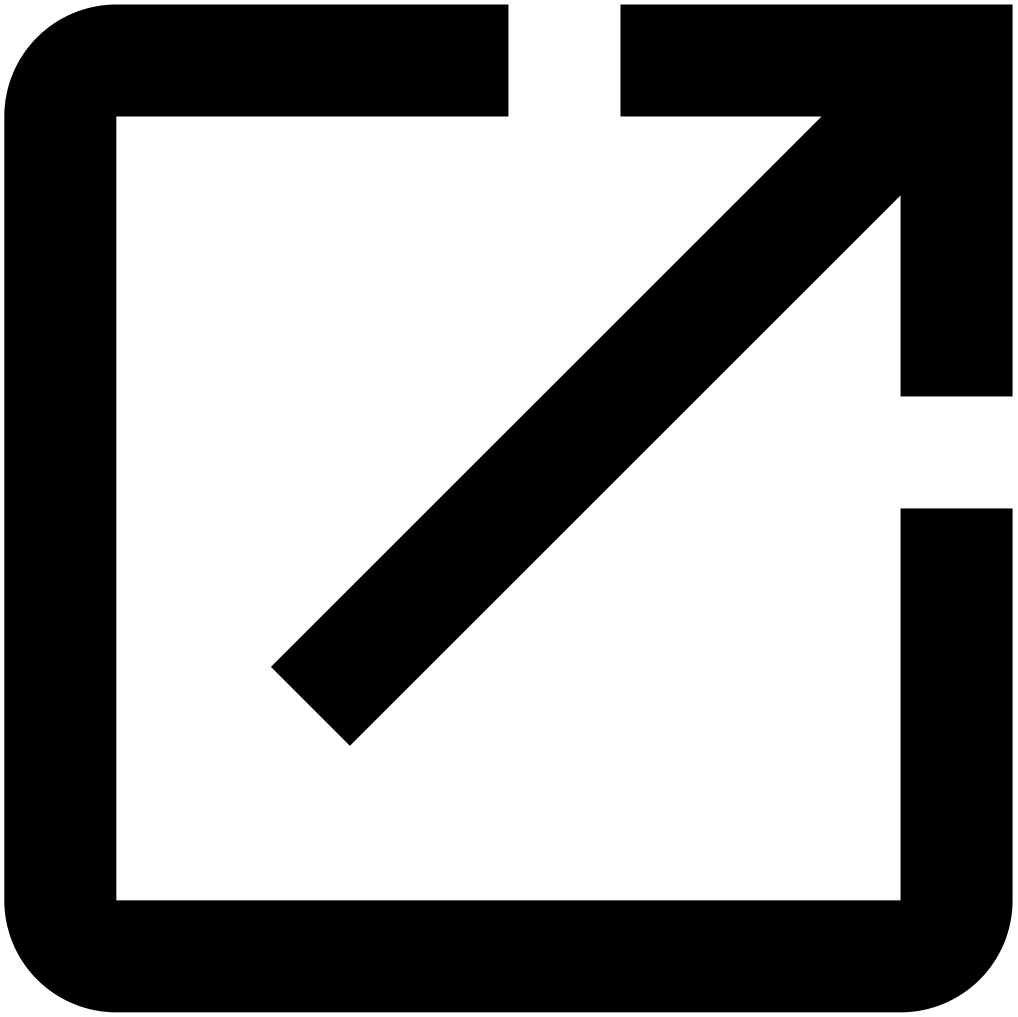


Security researchers have discovered a new banking trojan named BackSwap that uses never-before-seen techniques to facilitate the theft of online funds.

The techniques the trojan uses have not been observed with another malware family, and they can bypass antivirus software detection and security protections put in place at the browser level.

Experts believe these techniques will soon be copied by other groups and spread around to trigger a new wave of banking trojan attacks right when infections with this malware type have begun to go down.


F RTINET
0:00



Previous techniques used by banking trojans

Until now, all previous banking trojans used two main tricks to steal money from victims. The first technique, now rarely used, relied on altering local DNS and Internet settings by intercepting requests for banking-related sites and redirecting the user via a proxy to a clone website of the original banking portal, where crooks would collect login credentials and act as a middleman between the user and the bank.

The second technique, currently the go-to solution for all major banking trojans like Dridex, Ursnif, Zbot, Trickbot, Qbot, and others, relied on injecting malicious code inside the browser's process.

This technique was efficient in the beginning, but antivirus vendors have modified their apps to scan for process injection attempts, and have become quite good at detecting these events.

Browser vendors have similarly modified their software to prevent banking trojans from easily tapping into the browser's internal functions that allow trojans to meddle with a page's content.

Nowadays, the process injection technique is more of a headache for banking trojan makers, as they have to review and modify their injection code after every browser update because browser vendors always change something that breaks the attackers' previous code.

This constant hassle and improved AV protection are, maybe, one of the reasons why many cybercriminal groups have moved from distributing banking trojans to new types of malware such as in-browser miners, coinminers, ransomware, and others.

BackSwap uses Windows UI-related code to detect visited sites

But in a report published today, ESET revealed it discovered the BackSwap trojan, which came with three new techniques that are completely different from all previous trojans.

Furthermore, these techniques bypass both AV and browser-related protections because they don't tamper with the browser process at all.

The first technique BackSwap deploys is a technique used for detecting when the user is accessing a banking-related website. According to ESET, BackSwap uses a native Windows mechanism named the "message loop."

According to Wikipedia, "the message loop is an obligatory section of code in every program that uses a graphical user interface under Microsoft Windows." Browsers are GUI apps, meaning they also use message loops.

BackSwap simply taps into the Windows message loop to search for URL-like patterns, such as "https" strings and other terms related to a bank's name.

BackSwap abuses a browser's developer console

Once it detects the browser is accessing and loading a banking-related website, BackSwap uses one of two techniques to tamper with the loaded content. For both techniques, the trojan doesn't inject code inside the browser's process but merely simulates key presses.

Initial versions of the BackSwap trojan used the following method to alter what users are seeing inside web pages.

1) The malware inserts the malicious script into the clipboard.
2) Malware makes browser window invisible.
3) BackSwap simulates pressing the key combination for opening the developer’s console (CTRL+SHIFT+J in Google Chrome, CTRL+SHIFT+K in Mozilla Firefox).
4) BackSwap simulates CTRL+V to paste the content of the clipboard inside the browser's developer console.
5) Trojan simulates an ENTER key press to execute the malicious code.
6) Malicious code alters the banking portal's code to give the attacker control of what the user sees.

7) The malware sends the console key combination again to close the console.
8) BackSwap makes browser window visible again.

This entire attack takes under a second to execute, and users will have a hard time noticing that something went wrong or even distinguishing it from a regular browser freeze.

BackSwap abuses "javascript:" protocol

But despite its simplicity, the BackSwap crew seems to have abandoned this first technique, and moved to a new one, which interacts with the browser's address bar.

1) The malware simply simulates pressing CTRL+L to select the browser's address bar.
2) BackSwap simulates DELETE key to clear the URL field.
3) The malware "types" in the address bar the string "javascript:" one letter at a time. The code is typed one letter at a time to circumvent browser self-XSS protections.
4) Malware pastes its malicious JavaScript code after the "javascript:" string.
5) Browser simulates an ENTER key press to execute the code.
6) Trojan clears the address bar to remove any signs of compromise.

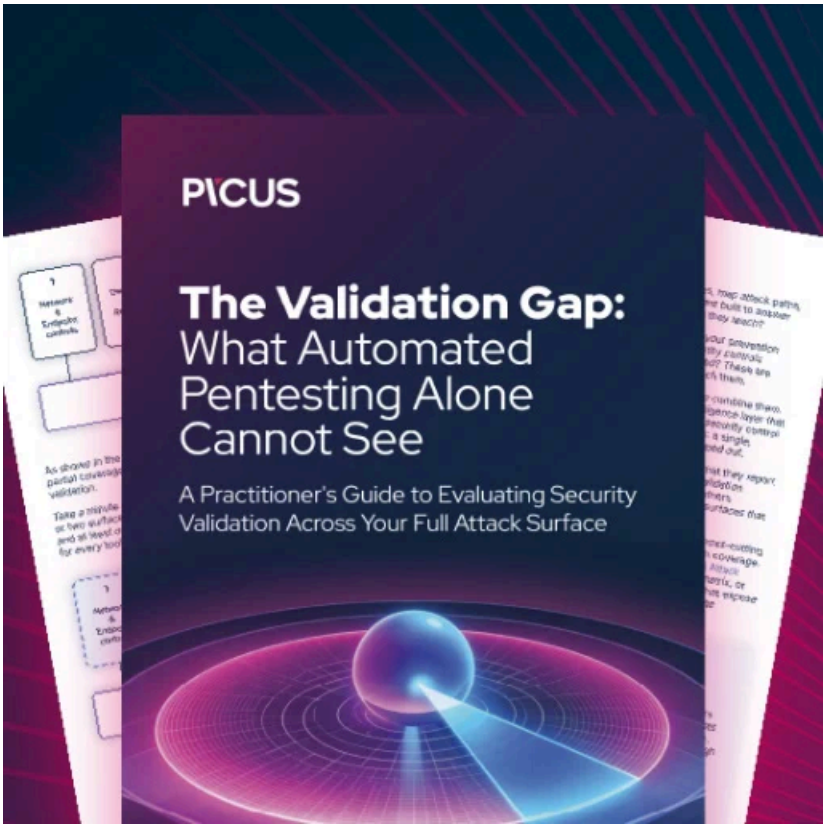
ESET says BackSwap supports attacks against Google Chrome, Mozilla Firefox and Internet Explorer, but with little tweaks, the techniques should work against all browsers, since all modern browsers today support a developer console and the "javascript:" protocol.

BackSwap currently targets Polish banks only

BackSwap's techniques are incredibly easy to execute, and don't necessarily rely on high-level knowledge of the Windows OS to implement, like previous banking trojan attacks.

While they're bound to spread to other banking trojan families in the upcoming future, at the moment, this trojan is not a global threat. Researchers say that current versions of BackSwap come with support for altering the web portals of only five Polish banks —PKO Bank Polski, Bank Zachodni WBK S.A., mBank, ING, and Pekao.

Nonetheless, ESET said it notified browser vendors about BackSwap's new techniques in the hopes they'd deploy countermeasures in upcoming browser versions, and mitigate these types of attacks before they go mainstream with other malware families.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/backswap-banking-trojan-uses-never-before-seen-techniques/