Mokes and Buerak distributed under the guise of security certificates

By AMR

Published: 2020-03-05 · Archived: 2026-04-05 22:22:38 UTC

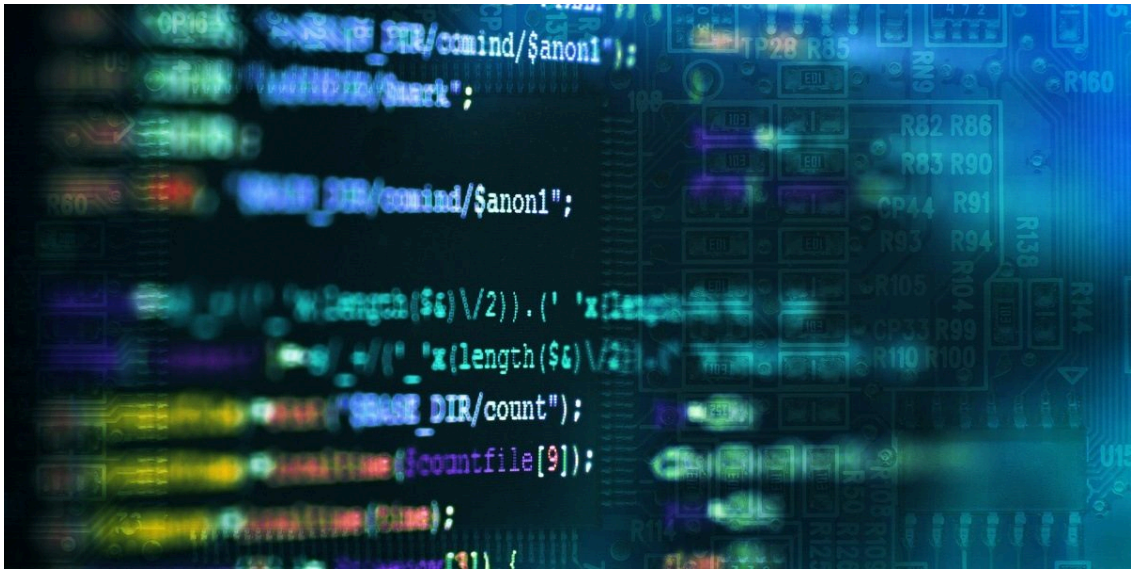
Incidents

Incidents

05 Mar 2020

1 minute read

- Expert AMR

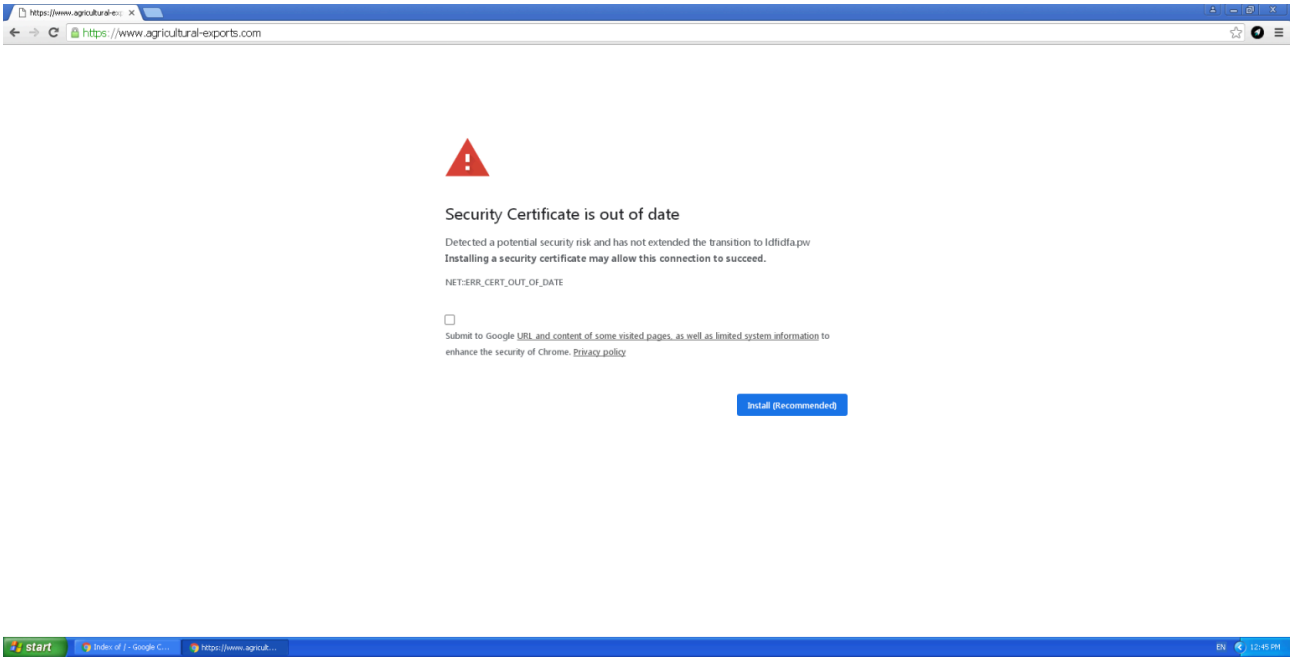


The technique of distributing malware under the guise of legitimate software updates is not new. As a rule, cybercriminals invite potential victims to install a new version of a browser or Adobe Flash Player. However, we recently discovered a new approach to this well-known method: visitors to infected sites were informed that some kind of security certificate had expired. Unsurprisingly, the update on offer was malicious.

We detected the infection on variously themed websites — from a zoo to a store selling auto parts. The earliest infections found date back to January 16, 2020.

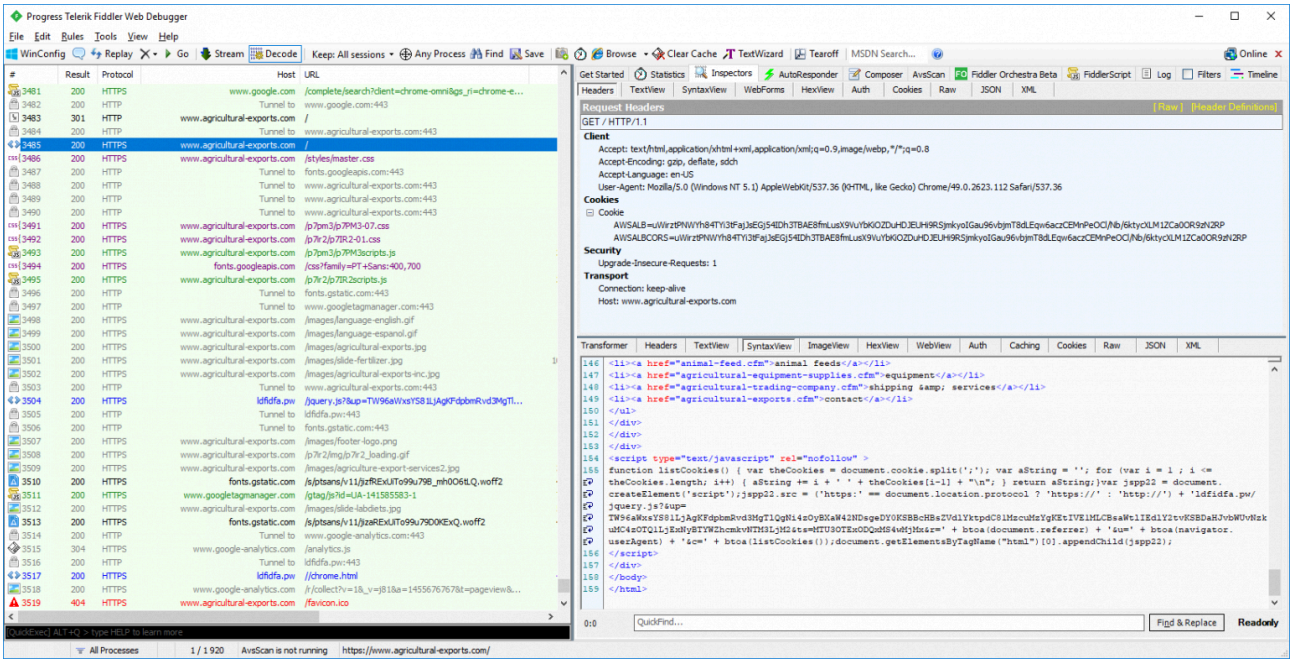
Attack pattern

This is what visitors of any of the hacked websites saw:



The alarming notification consists of an iframe — with contents loaded from the third-party resource ldfidfa[.]pw — overlaid on top of the original page. The URL bar still displays the legitimate address. This is what the

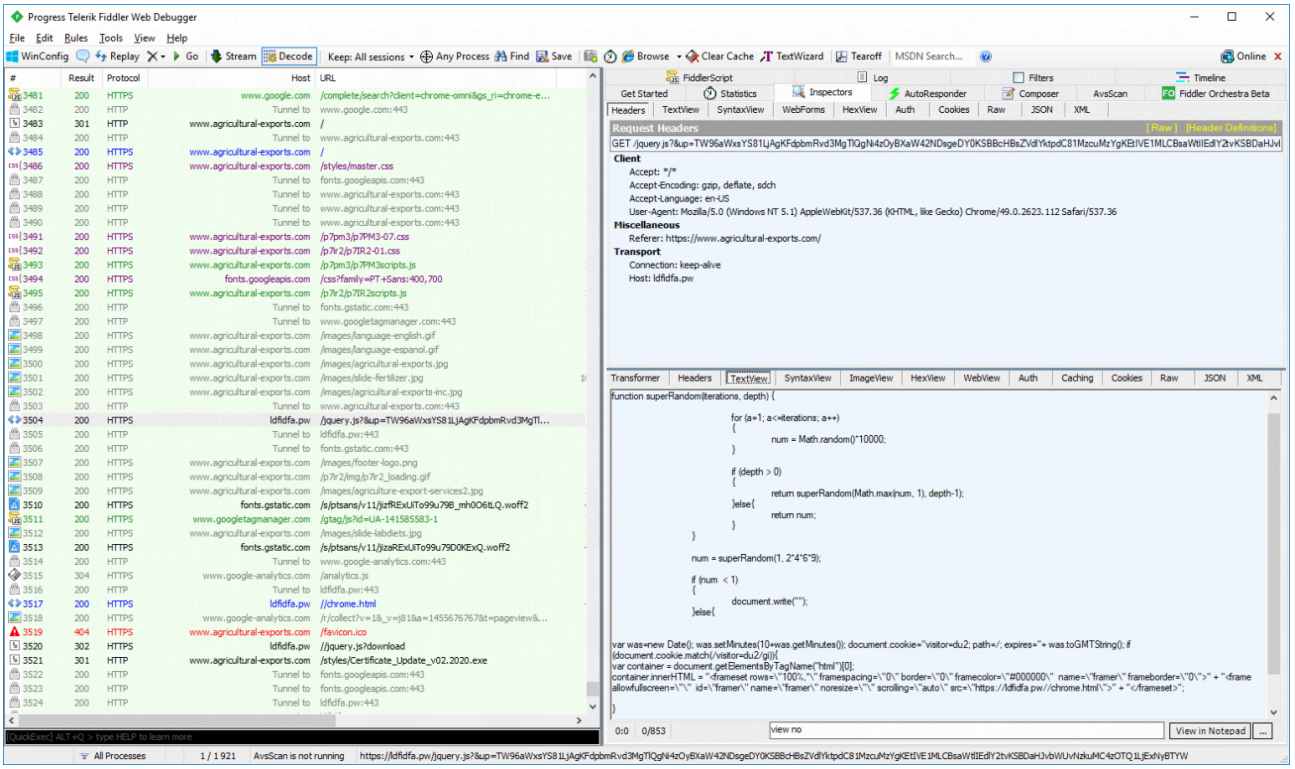
malicious piece of code inserted into the original HTML page looks like:



From the screenshot it can be seen that the script parameters depend on the referrer, user_agent, and cookie values of the user. While the following fixed values are used as the user_agent_X and timestamp_X strings:

- user_agent_X = Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/537.36
- timestamp_X = 1579118411.0231 (01/15/2020 @ 8:00pm (UTC))

The code inserted by the cybercriminal loads the external malicious script ldfidfa[.]pw/jquery.js?&up= &ts= &r= &u= &c=



Malicious jquery.js script

The jquery.js script overlays an iframe that is exactly the same size as the page. The iframe content is loaded from the address https[:]//ldfidfa[.]pw//chrome.html. As a result, instead of the original page, the user sees a seemingly genuine banner urgently prompting to install a certificate update.

Clicking the Install (Recommended) button on the banner initiates the download of the file Certificate_Update_v02.2020.exe, which we detect as Exploit.Win32.ShellCode.gen. Analysis of the file showed it to be Trojan-Downloader.Win32.Buerak, packed using Nullsoft Scriptable Install System. It is not the only malware distributed by the attackers. For example, Backdoor.Win32.Mokes was spread via the same campaign earlier in January.

IoC

Exploit.Win32.ShellCode.gen
B3290148681F8218ECB80CA430F9FDBA (Certificate_Update_v02.2020.exe)

Trojan-Downloader.Win32.Buerak
CE1931C2EB82B91ADB5A9B9B1064B09F

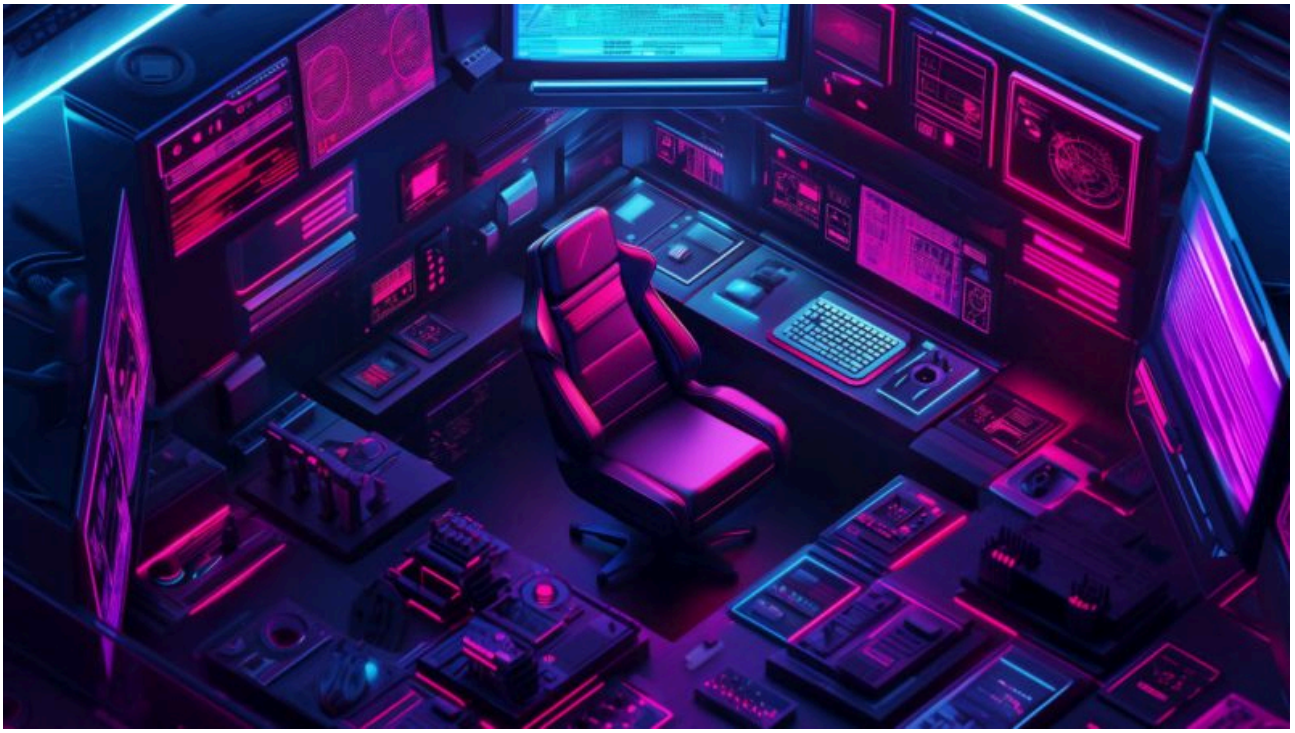
Backdoor.Win32.Mokes
094ADE4F1BC82D09AD4E1C05513F686D
F869430B3658A2A112FC85A1246F3F9D
5FB9CB00F19EAFBF578AF693767A8754
47C5782560D2FE3B80E0596F3FBA84D3

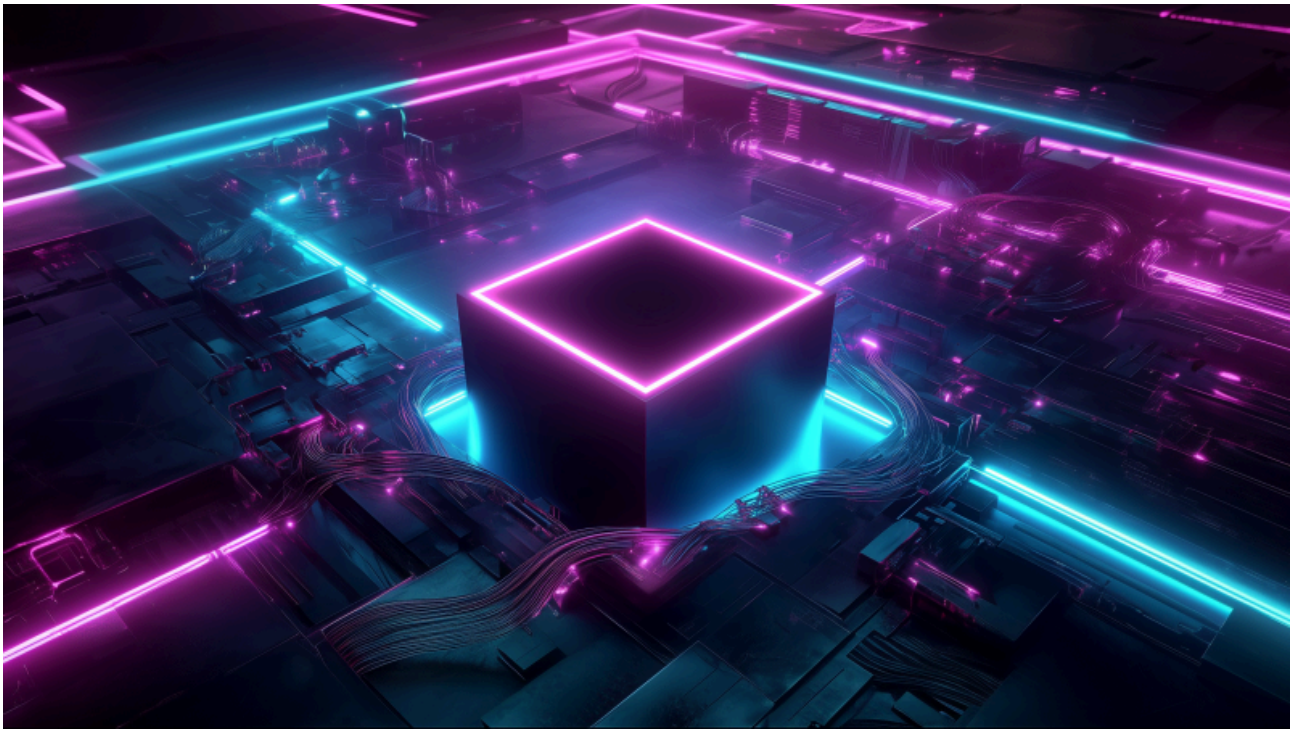
C&C

kkjjhhdff[.]site (47.245.30[.]255)

oderstrg[.]site

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
