Mokes and Buerak distributed under the guise of security certificates

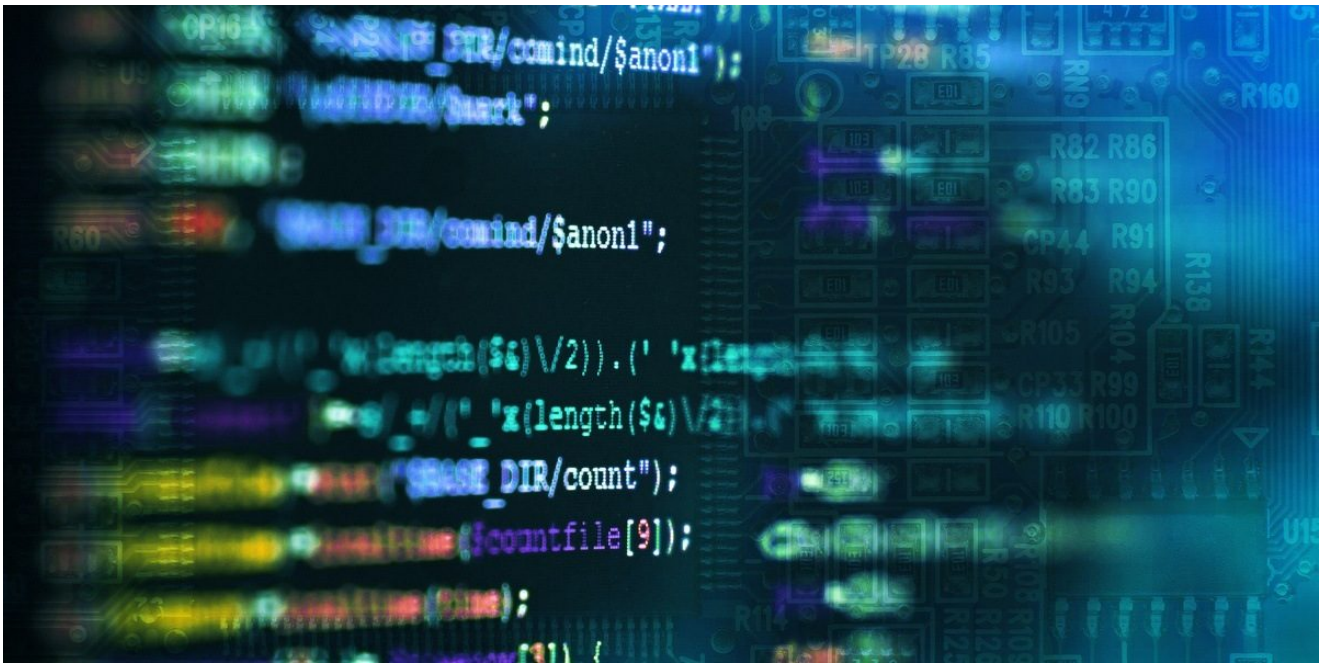
securelist.com/mokes-and-buerak-distributed-under-the-guise-of-security-certificates/96324/

Incidents

Incidents

05 Mar 2020

minute read



Authors

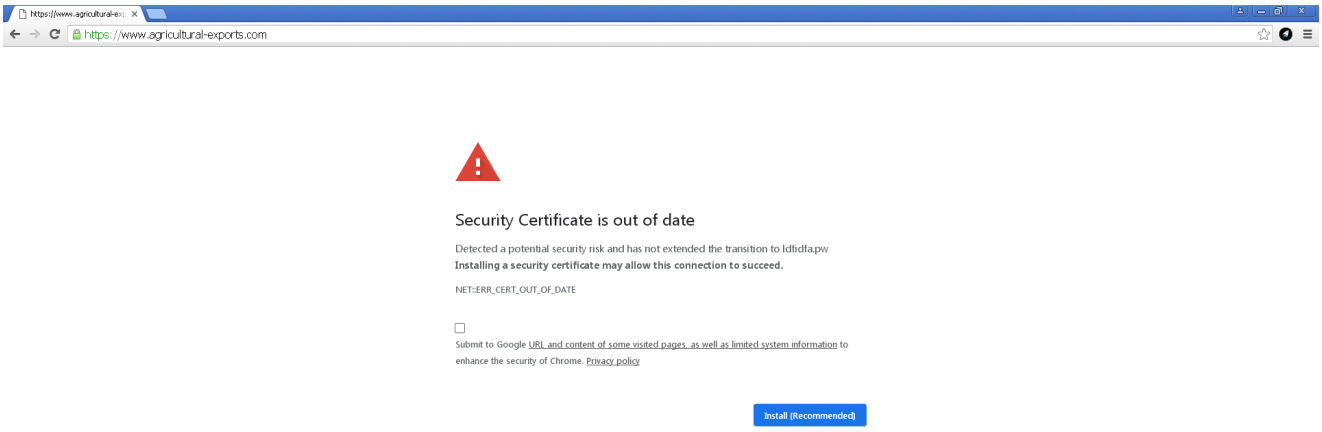
Expert AMR

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.

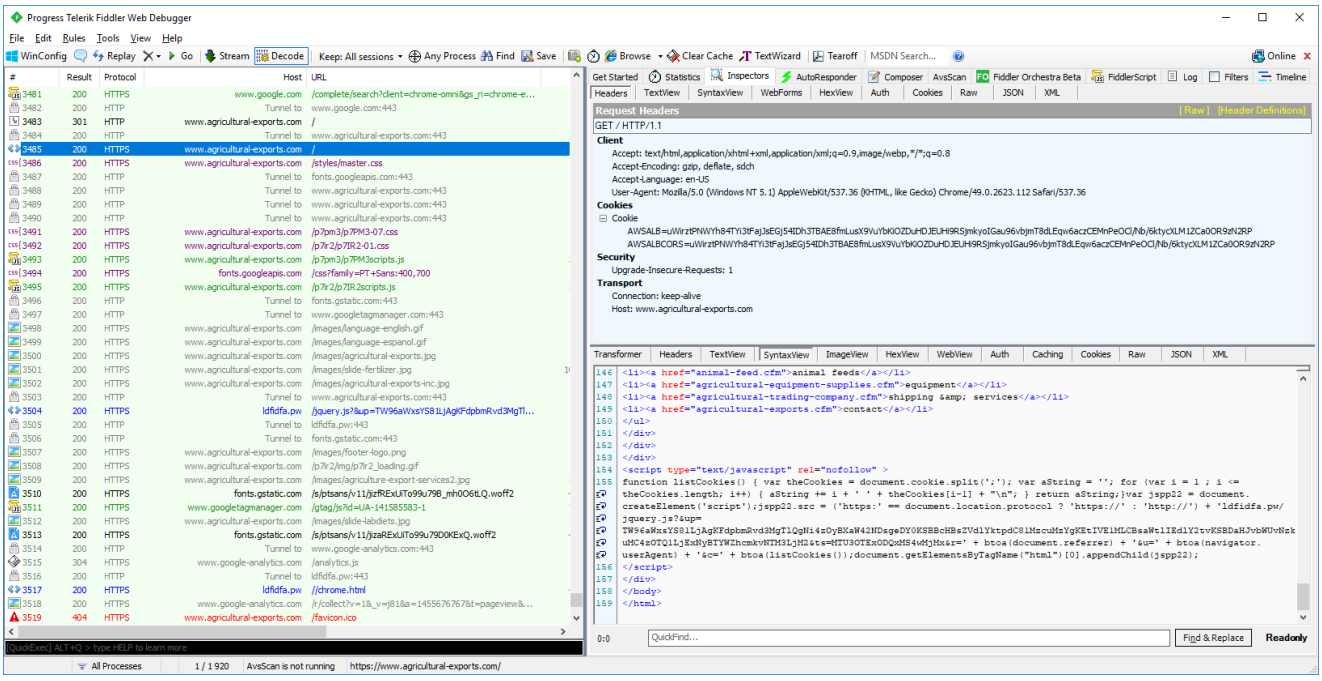
We detected the infection on variously themed websites — from a zoo to a store selling auto parts. The earliest infections found date back to January 16, 2020.

Attack pattern

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



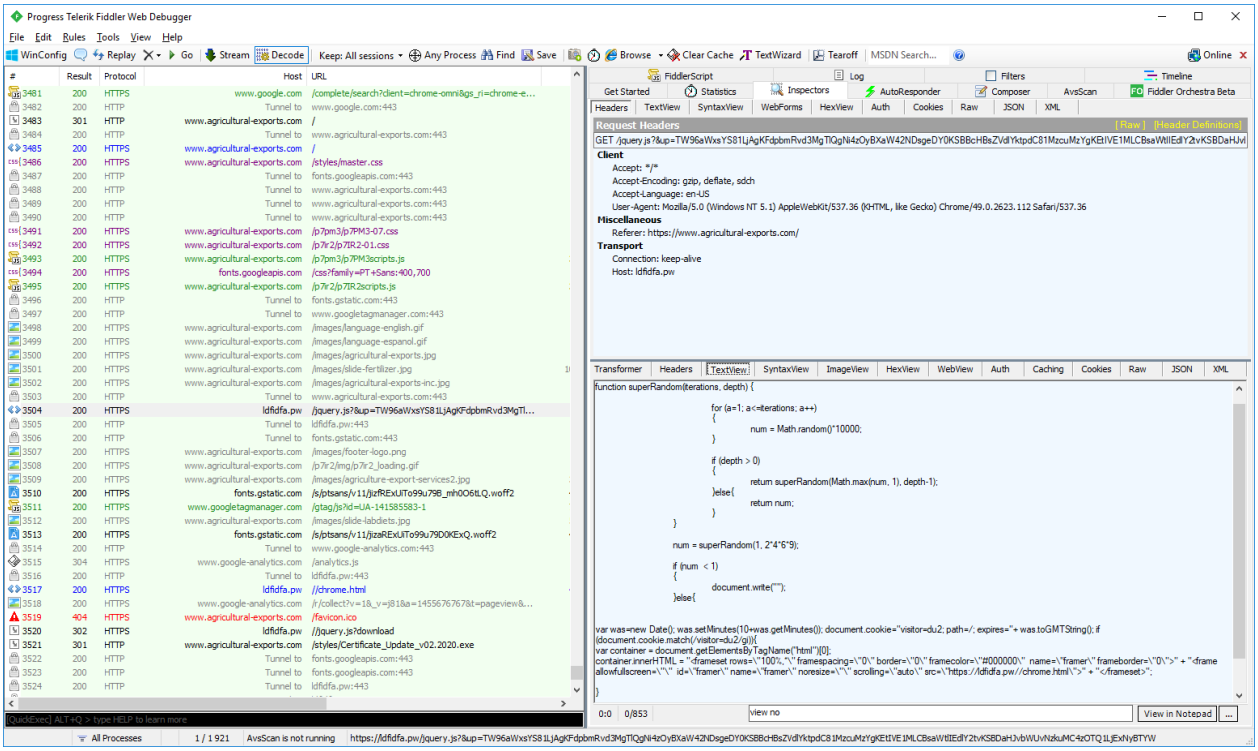
The alarming notification consists of an iframe — with contents loaded from the third-party resource ldfidfa[.]pw — overlaid on top of the original page. The URL bar still displays the legitimate address. This is what the malicious piece of code inserted into the original HTML page looks like:



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

- Backdoor
- Digital Certificates
- Trojan
- Vulnerabilities and exploits
- Website Hacks

Authors

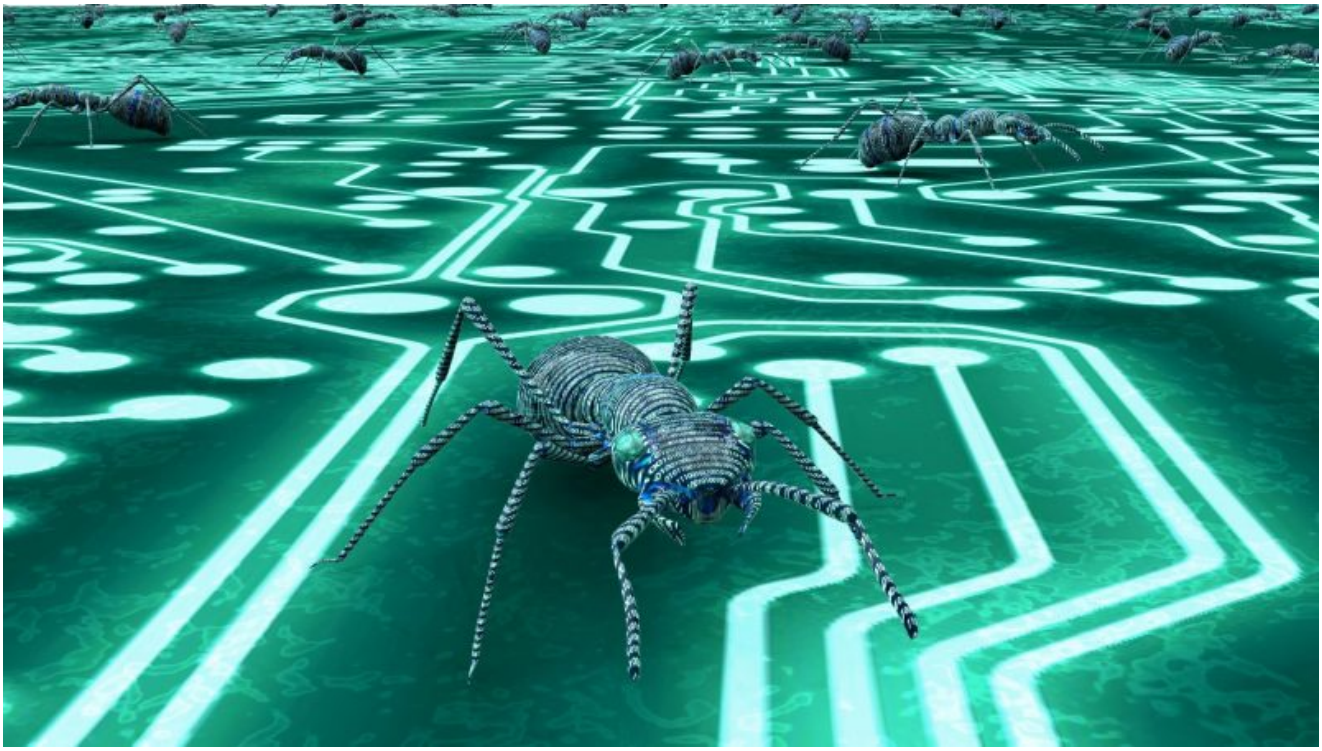
Expert AMR

Mokes and Buerak distributed under the guise of security certificates

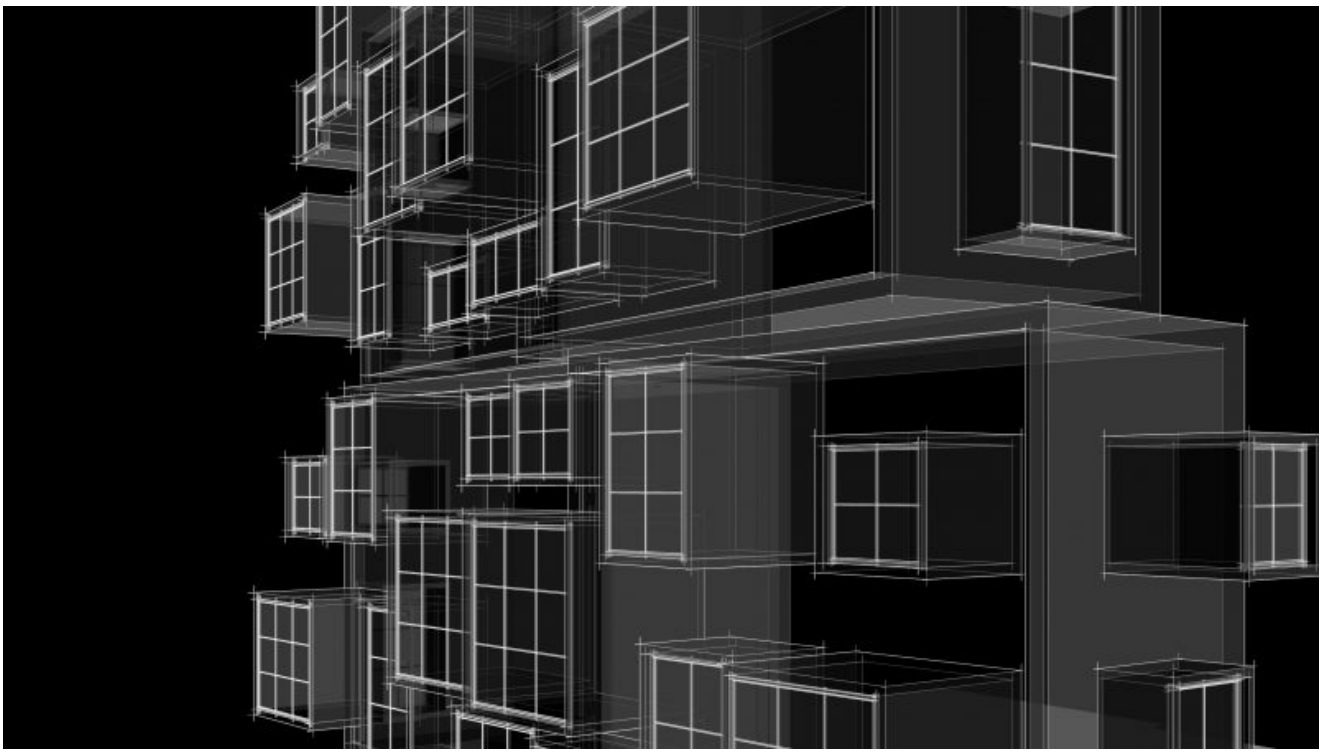
---

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors



IT threat evolution in Q1 2022. Non-mobile statistics



Emotet modules and recent attacks

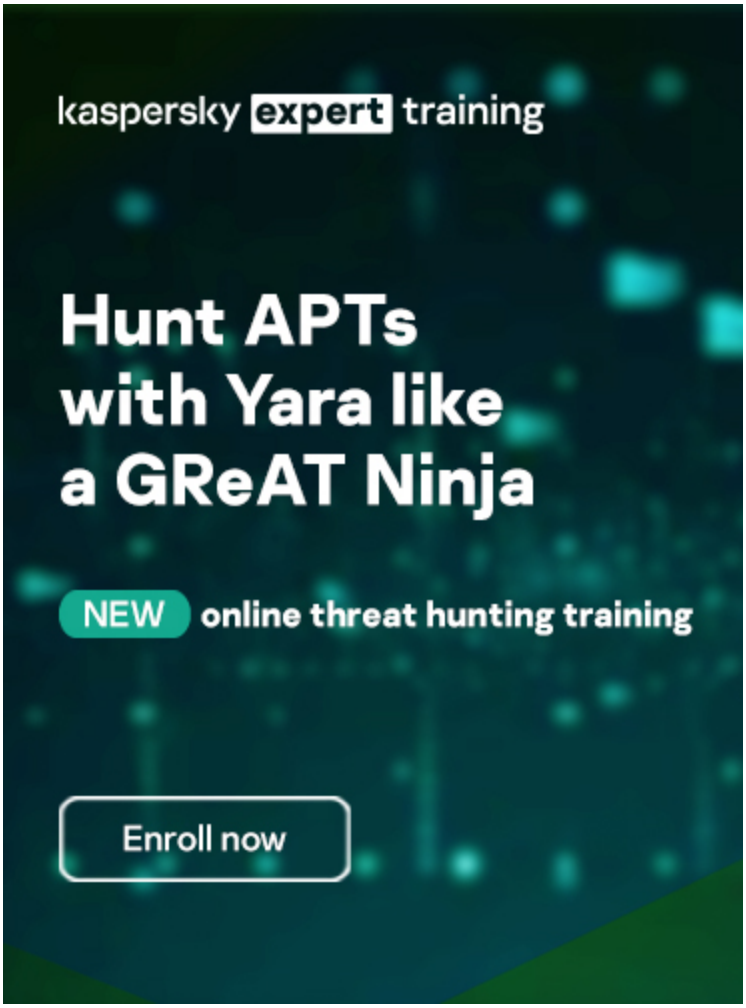
Spring4Shell (CVE-2022-22965): details and mitigations

CVE-2022-0847 aka Dirty Pipe vulnerability in Linux kernel

Kaspersky Security Bulletin 2021. Statistics

Subscribe to our weekly e-mails

The hottest research right in your inbox



Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

-
-
-