Hackers Hide Malware C2 Communication By Faking News Site Traffic

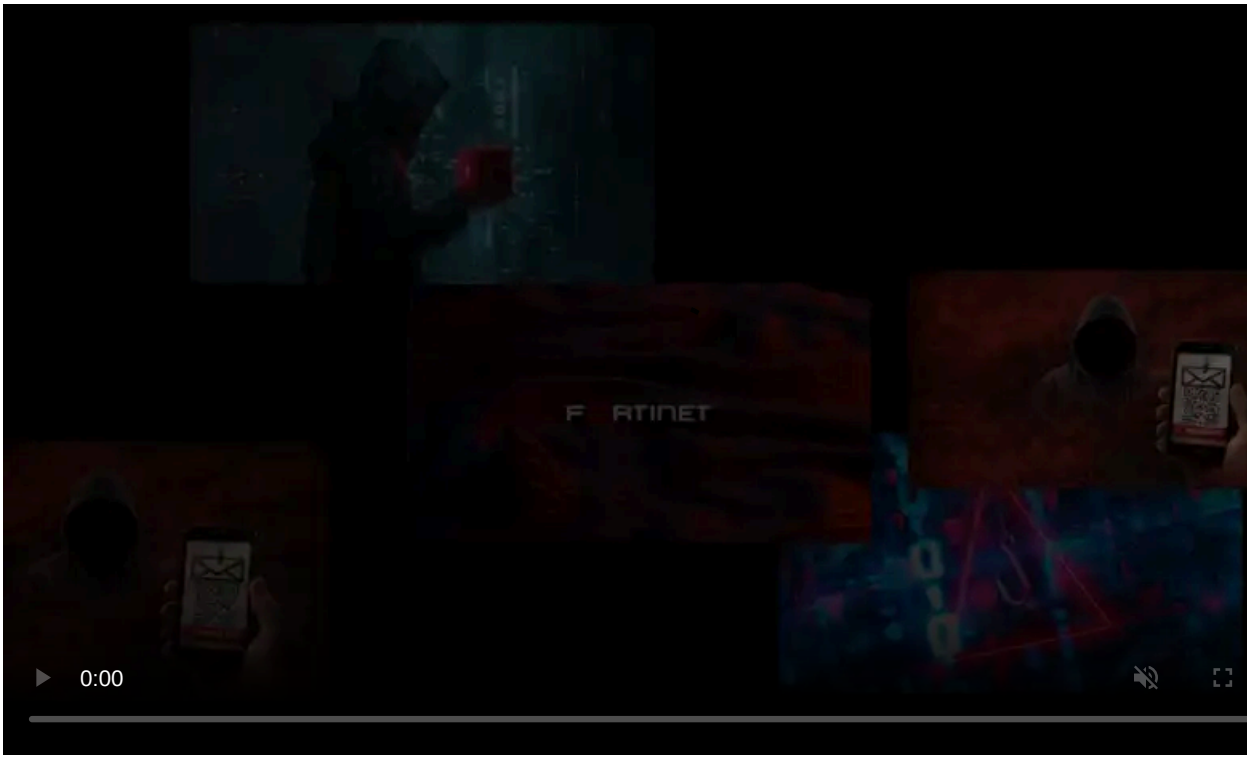
By Ionut Ilascu

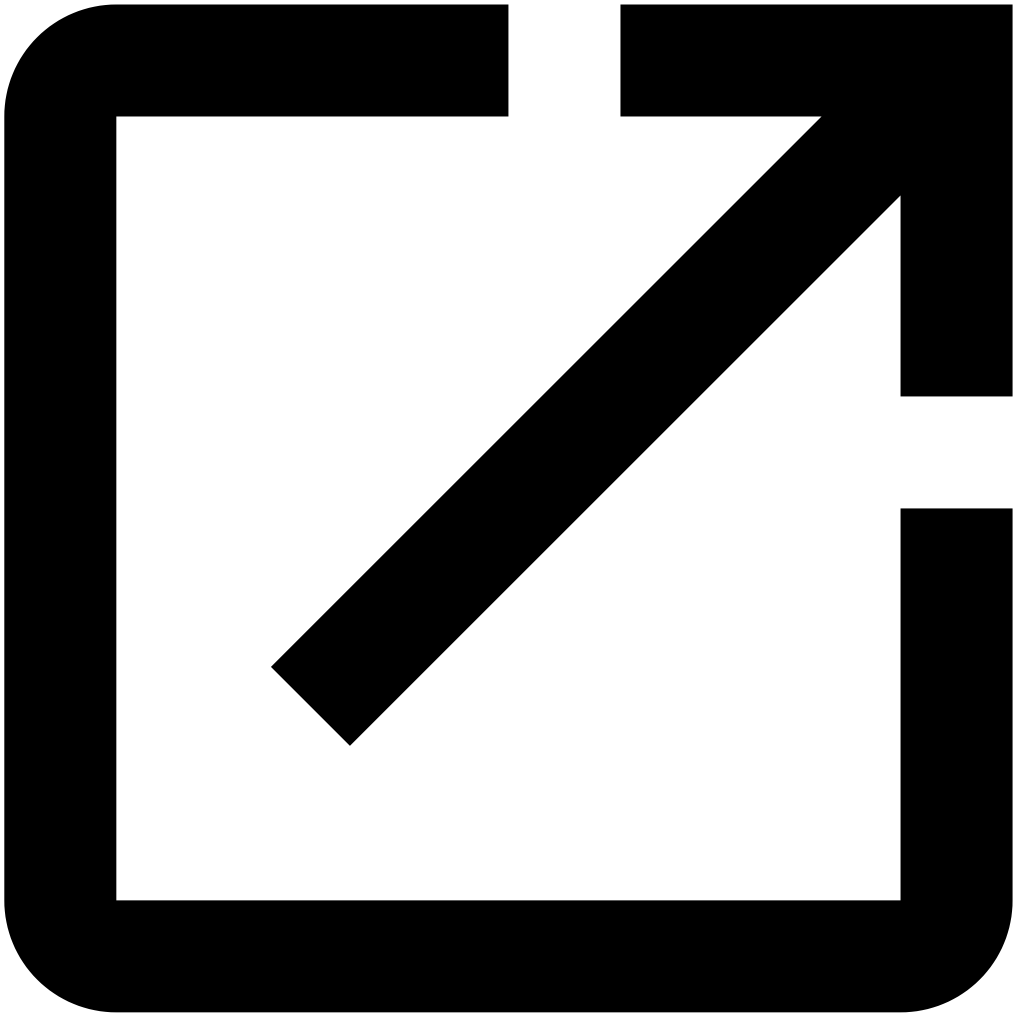
Published: 2020-03-18 · Archived: 2026-04-05 23:20:36 UTC

A cyber-espionage group active since at least 2012 used a legitimate tool to shield their backdoor from analysis attempts to avoid detection. In their effort, the hackers also used a fake host header named after a known news site.

The backdoor is referred to by the names Spark and EnigmaSpark and was deployed in a recent phishing campaign that appears to have been the work of the MoleRATs group, the low-budget division of the Gaza Cybergang. This is the actor responsible for operation SneakyPastes, detailed by Kaspersky, which relied on malware hosted on free sharing services like GitHub and Pastebin.

There are strong indications that the group used this backdoor since March 2017, deploying dozens of variants that contacted at least 15 command and control domains.


F RTINET
0:00



Researchers from multiple cyber security tracked the campaigns from this threat actor and analyzed the malware, tactics, and infrastructure used in the attacks.

Evasion tactics

The threat actor tried to hide signs of compromise using the Enigma Protector software - a legitimate tool for "protecting executable files from illegal copying, hacking, modification, and analysis."

Based on the targets observed and the theme in the documents used for lures, this looks like a politically-motivated attack aimed at Arabic speakers interested in Palestine's potential acceptance of the peace plan.

"Adversaries using EnigmaSpark likely relied on recipients' significant interest in regional events or anticipated fear prompted by the spoofed content, illustrating how adversaries may exploit ongoing geopolitical events to enable malicious cyber activity" - IBM X-Force Incident Response and Intelligence Services (IRIS)

The infection chain leading to installing the EnigmaSpark backdoor started with the delivery of a malicious Microsoft Word document. The file is written in Arabic and prompts the recipient to enable editing to view the content.

The researchers found that the document gets from a Google Drive link a malicious Word template embedded with a macro for delivering the final payload 'runawy.exe.'

To protect the operation, the hackers added some defenses such as protecting the macro with a password and applying base64 encoding scheme on the backdoor, which was also stored on Google Drive.

Additionally, the malware binary was packed with Enigma Protector that adds some resistance to hacking and cracking attempts.

Another precaution from the hackers is the use of a fake host header in the HTTP POST request that delivers victim system info to the command and control (C2) server, which was 'nysura].[com.' However, the header shows 'cnet].[com' as the destination.

Common denominator

An X-Force (IRIS) investigation revealed that the attacker used this technique with other binaries. After unpacking 'runawy.exe,' they noticed that the resulting file was the same as 'blaster.exe,' a binary delivered by an executable packed by Themida, another legitimate tool that adds protection against inspecting or modifying a compiled application.

Multiple files were discovered because they had in common the unique string "S4.4P" and the cryptographic certificate signer "tg1678A4": Wordeditor.exe, Blaster.exe (the unpacked version of runawy.exe and soundcloud.exe), HelpPane.exe, and taskmanager.exe.

In the case of Blaster, the same trick with the fake host header was used as in the case of 'runawy,' but the real destination server was different ('webtutorialz[.]com').

Previous research

The 'runawy.exe' binary file, its C2 server, and the unique string have been previously documented by researchers at other cyber security companies.

Cybereason's Nocturnus team on February 12 published a technical analysis of the Spark backdoor, detailing the capabilities of the malware:

- Collect information about the victim host
- Encrypt collected data and sending it to the attackers over the HTTP protocol
- Download other payloads
- Log keystrokes Record audio using the system's built-in microphone

- Execute commands on the infected machine

At the beginning of the month, Palo Alto Networks detailed the same Enigma-packed runaway payload that was delivered with the help of a Word document on October 31 and November 2, 2019.

The Spark backdoor was initially documented by researchers at Beijing-based Qi An Xin cyber security company, with an English version of the research published on February 14, 2019.

Researchers from all these companies attribute the Spark backdoor to the MoleRATs group, known for using malware available on hacker forums. However, they also develop custom tools, such as Spark.

Source: https://www.bleepingcomputer.com/news/security/hackers-hide-malware-c2-communication-by-faking-news-site-traffic/