Malicious Microsoft Excel add-ins used to deliver RAT malware

bleepingcomputer.com/news/security/malicious-microsoft-excel-add-ins-used-to-deliver-rat-malware/

Bill Toulas

By
Bill Toulas

- March 24, 2022
- 03:56 PM
- 0

Researchers report a new version of the JSSLoader remote access trojan being distributed via malicious Microsoft Excel addins.

The particular RAT (remote access trojan) has been circulated in the wild since December 2020, linked to the financially-motivated Russian hacking group FIN7, also known as "Carbanak."

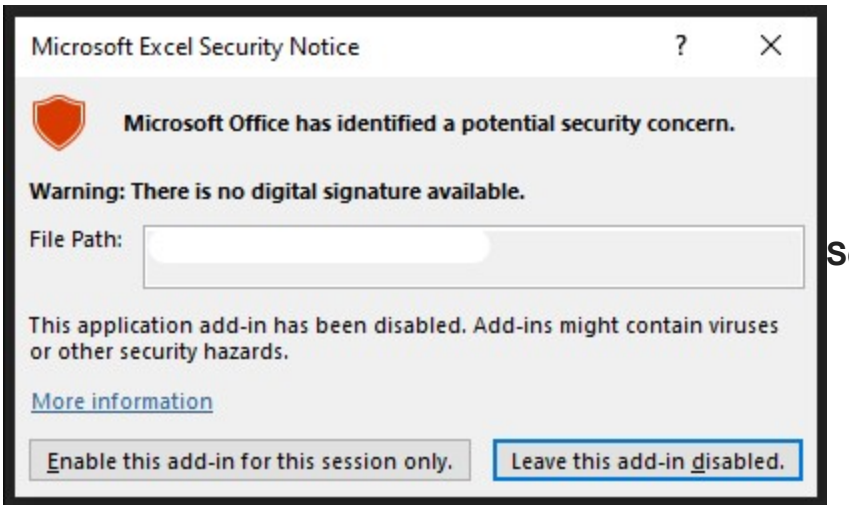
JSSLoader is a small, lightweight RAT that can perform data exfiltration, establish persistence, fetch and load additional payloads, auto-update itself, and more.

Excel add-ins

The latest campaign involving a stealthier new version of JSSLoader was observed by threat analysts at Morphisec Labs, who say the delivery mechanism is currently phishing emails with XLL or XLM attachments.

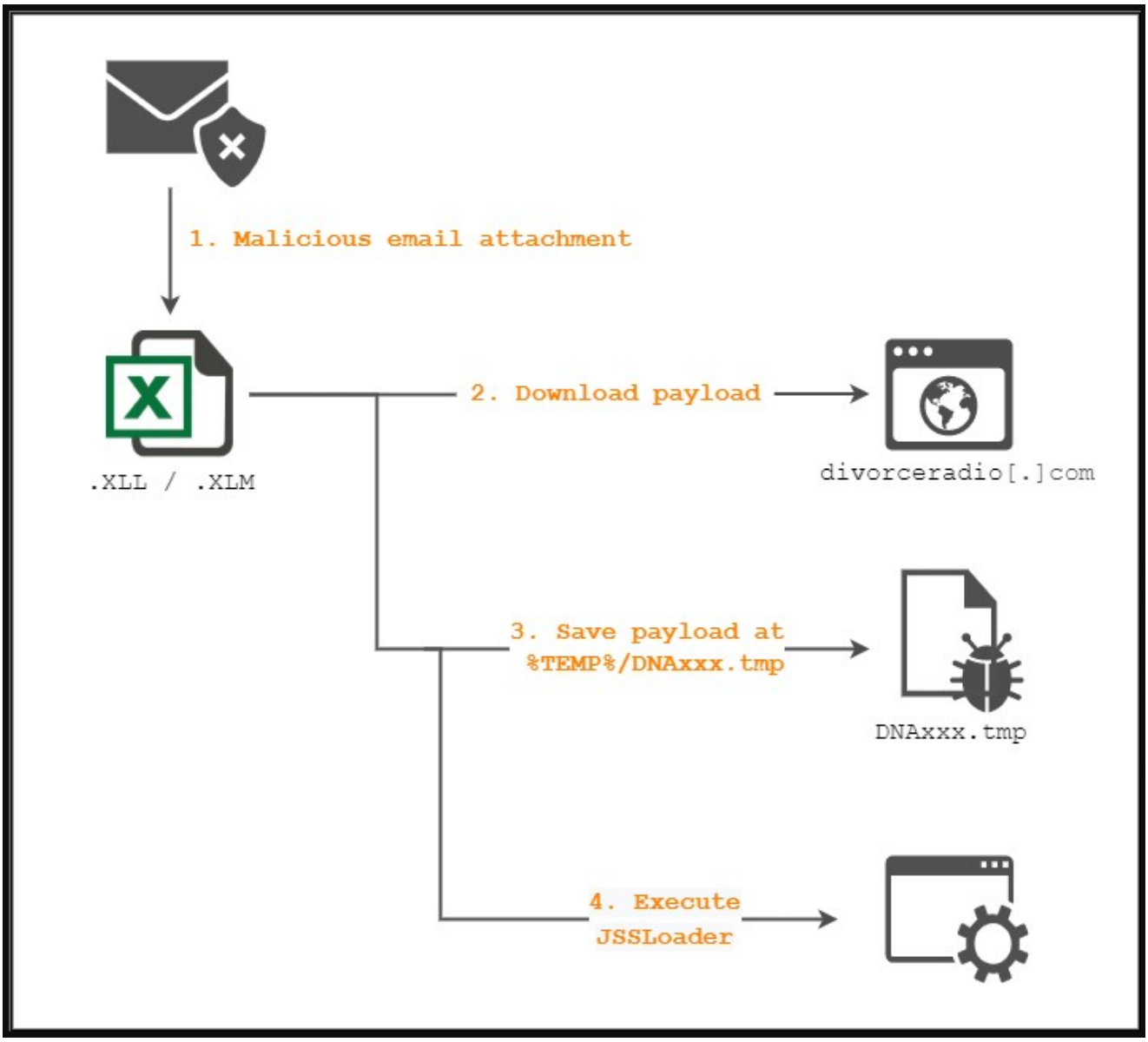
Abuse of Excel XLL add-ins isn't new, as they are commonly used for legitimate purposes, such as importing data into a worksheet or extending the functionality of Excel.

In the ongoing campaign, however, the threat actors use an unsigned file, so Excel will show the victim a clear warning about the risks of executing it.



Security warning about unsigned XLL file
(Morphisec)

When enabled, the XLL files use malicious code inside an xlAutoOpen function to load itself into memory and then download the payload from a remote server and execute it as a new process via an API call.



Malware loading and execution flow *(Morphisec)*

More sophisticated obfuscation

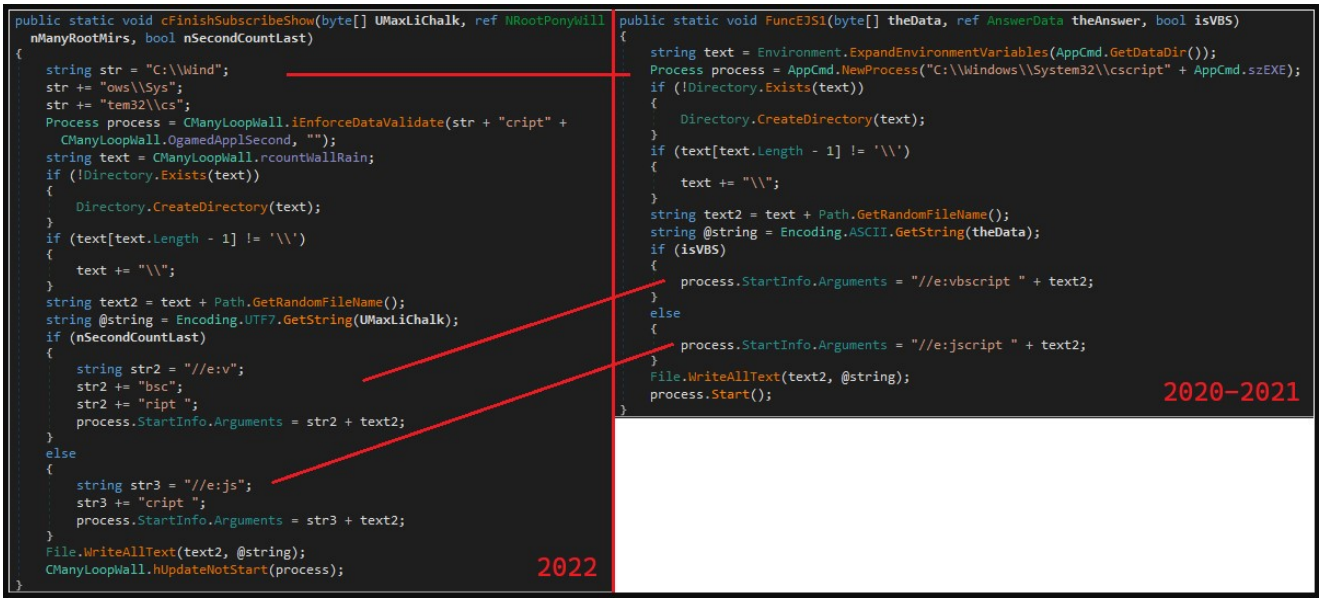
The threat actor regularly refreshes the User-Agent on the XLL files to evade EDRs that consolidate detection information from the entire network.

```
retries_countdown = 10;
v22 = 0;
while ( 1 )
{
  hSession = WinHttpOpen(L"Paris", 1u, 0, 0, 0);
  if ( hSession )
    break;
  Sleep(0x3E8u);
  if ( --retries_countdown <= 0 )
    return;
}
```

```
retries_countdown = 10;
v22 = 0;
while ( 1 )
{
  hSession = WinHttpOpen(L"curl/7.78.0", 1u, 0, 0, 0);
  if ( hSession )
    break;
  Sleep(0x3E8u);
  if ( --retries_countdown <= 0 )
    return;
}
```

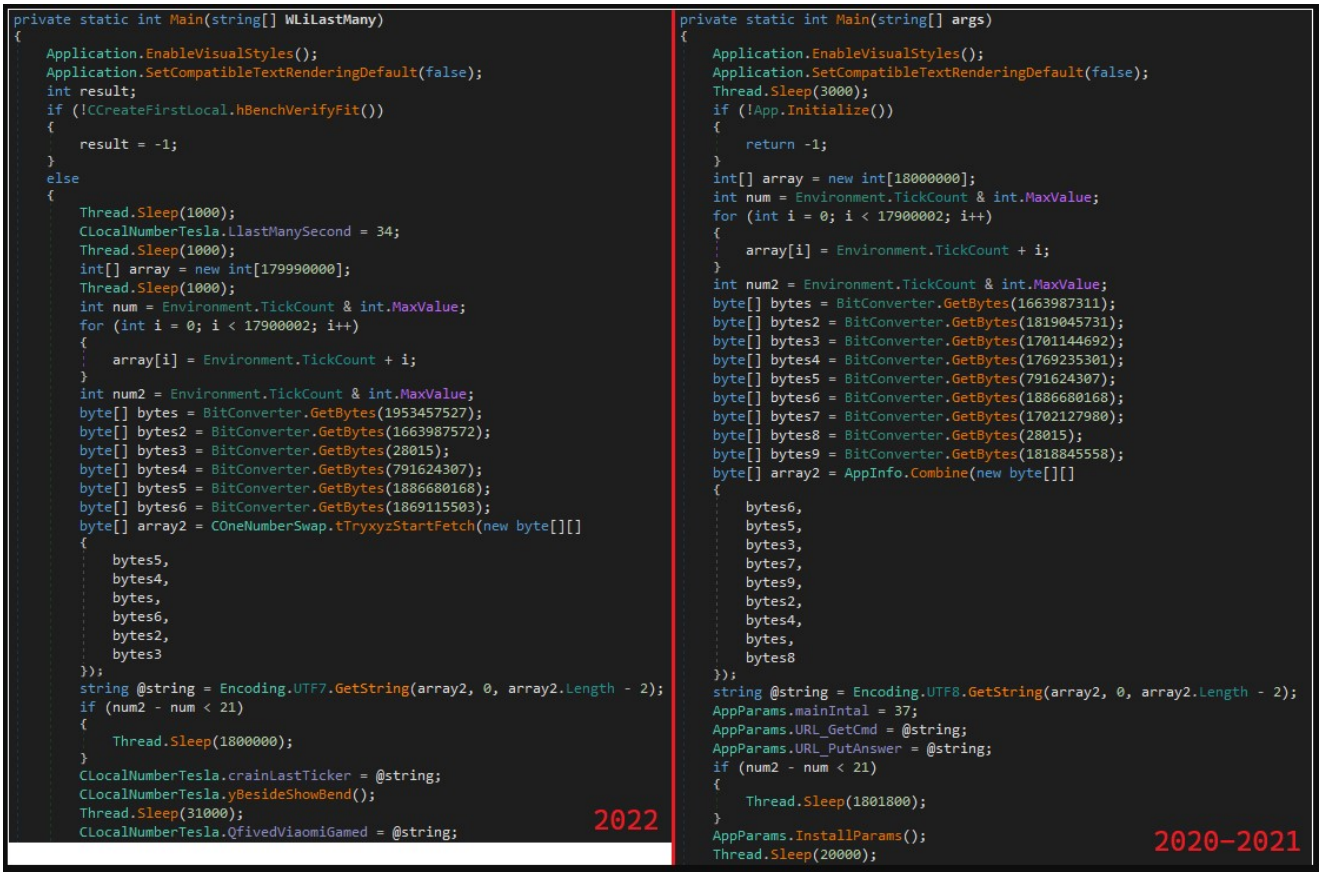
Changing the User-Agent on each XLL sample *(Morphisec)*

Compared to older versions, the new JSSLoader has the same execution flow, but it now comes with a new layer of string obfuscation that includes renaming all functions and variables.



String obfuscation added on the new JSSLoader *(Morphisec)*

To evade detection from string-based YARA rules used by defenders, the new RAT has split the strings into sub-strings and concatenates them at runtime.



Strings comparison between new and old versions *(Morphisec)*

Finally, the string decoding mechanism is simple so as to leave a minimal footprint and reduce the chances of being detected by static threat scanners.

Morphisec reports that these new additions combined with the XLL file delivery are enough to prevent detection from next-generation antivirus (NGAV) and endpoint detection and response (EDR) solutions challenging or even implausible.

This enables FIN7 to move in the compromised network undeterred for several days or weeks before the defenders load matching signatures on tools that complement AI-based detection solutions.

FIN7 is a resourceful threat group that has previously delivered malware-laced USBs alongside teddy bear gifts, attempted to hire network penetration experts by posing as a legitimate security firm, and sent ransomware-carrying USBs via post mail.

The new and stealthier version of JSSLoader is only one part of their arsenal, helping them hide in networks for longer without being detected and stopped.

Related Articles:

New stealthy Nerbian RAT malware spotted in ongoing attacks

New NetDooka malware spreads via poisoned search results

Hackers target Russian govt with fake Windows updates pushing RATs

Ukraine supporters in Germany targeted with PowerShell RAT malware

FIN7 hackers evolve toolset, work with multiple ransomware gangs

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.