AZORult Campaign Adopts Novel Triple-Encryption Technique

By Tom Spring

Published: 2020-02-03 · Archived: 2026-04-05 18:44:07 UTC

Popular trojan is sneaking its way onto PCs via malspam campaign that uses three levels of encryption to sneak past cyber defenses.

A recent wave of AZORult-laced spam caught the attention of researchers who warn that malicious attachments associated with the campaign are using a novel obfuscation technique, in an attempt to slip past spam gateways and avoid client-side antivirus detection.

What makes this campaign unique is the use by threat actors of a triple-encrypted AZORult downloader being pushed by the otherwise non-descript malspam assault. AZORult is remote access trojan popular on Russian forums and most recently spotted last month in a spam campaign perpetrated by a hacker with an affinity toward singer-songwriter Drake.

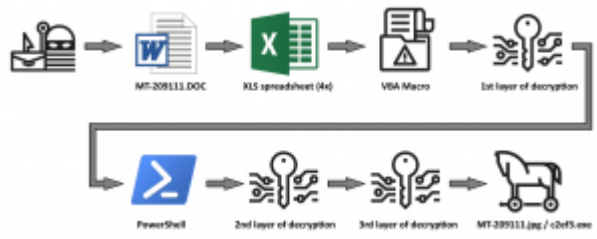
The malware-laced messages are “fairly uninteresting” and consist of a standard phishing hook, according to researcher Jan Kopriva, contributing to the Internet Storm Center blog. However, he added, the attacker’s use of three layers of encryption could present a challenge for signature and heuristics-based detection tools.

“Distributed as an attachment of a run-of-the-mill malspam message, the file with a DOC extension didn’t look like anything special at first glance. However, although it does use macros as one might expect, in the end, it turned out not to be the usual simple maldoc,” Kopriva wrote.

The infection chain starts with a typical phishing email asking for a “product list for January purchase,” for example. Attached to the email is what appears to be a Microsoft Office Word document (DOC), however the file type is actually a Rich Text File (RTF).

If someone is gullible enough to click on the file labeled “DOC” in the spam message, the RTF file opens. Immediately after opening, four identical Excel spreadsheets – embedded as OLE objects in the RTF body – spawn. As each Excel document launches, the end user is bombarded with requests to enable macros for each specific Excel document.

“The displaying of seemingly unending pop-ups would probably be one of the more effective ways to get users to allow macros to run, since they might feel that it would be the only way to stop additional prompts from displaying,” Kopriva wrote.



Click to Zoom

In this instance, attackers are spawning the Excel instances by abusing the "\objupdate" mechanism inherent in RTF files that allow "objects" to update before displaying themselves.

Should macros be enabled in any of the Excel documents, a payload is decrypted, decoded and executed using a Visual Basic for Applications "shell" command. "One small point of interest was that the payload, which it was supposed to decrypt, was not contained in the macro itself but rather in one of the cells (136, 8) of the spreadsheet," Kopriva said.

The next stage of the decryption happens as the first payload is executed and converts into a second decryption envelope, this time a PowerShell. The researcher notes that the second level encryption, like the first, was not complex and mainly served as a an obfuscation mechanism rather than anything else.

The payload this time is considerably obfuscated C# code, designed, said the researcher, to "download a file from a remote server [and] save it as c2ef3.exe in the AppData folder and execute it."

The third level of encryption manifests itself in the link used by the dropper to download the final AZORult infostealer malware. "The link to the remote file was protected with a third layer of encryption using the same algorithm we have seen in the PowerShell envelope," he wrote.

Kopriva also notes that the C# code tries to bypass the Microsoft Anti-Malware Scanning Interface using a memory patching technique first identified by CyberArk researchers in 2018 and used frequently including last week in a similar attack.

"With the use of Word, Excel, PowerShell and three layers of home-grown encryption, this downloader really turned out to be much more interesting than a usual malspam attachment," the researcher wrote.

While this malspam campaign is unique, it is unclear how effective the payload has been when it comes to going undetected.

"My guess is that triple encryption might be a little bit more effective than most of the usual obfuscation techniques, since it is applied multiple times on multiple layers (i.e. the first instance of the decryption algorithm was in a VBA macro and the second and third in PowerShell/C#). Any sandboxing would defeat it as easily as most other obfuscation mechanisms, however it isn't a bad way to defeat signature and heuristics-based detection tools," Kopriva told Threatpost.
