Avaddon ransomware shows that Excel 4.0 macros are still effective

By Ionut Ilascu

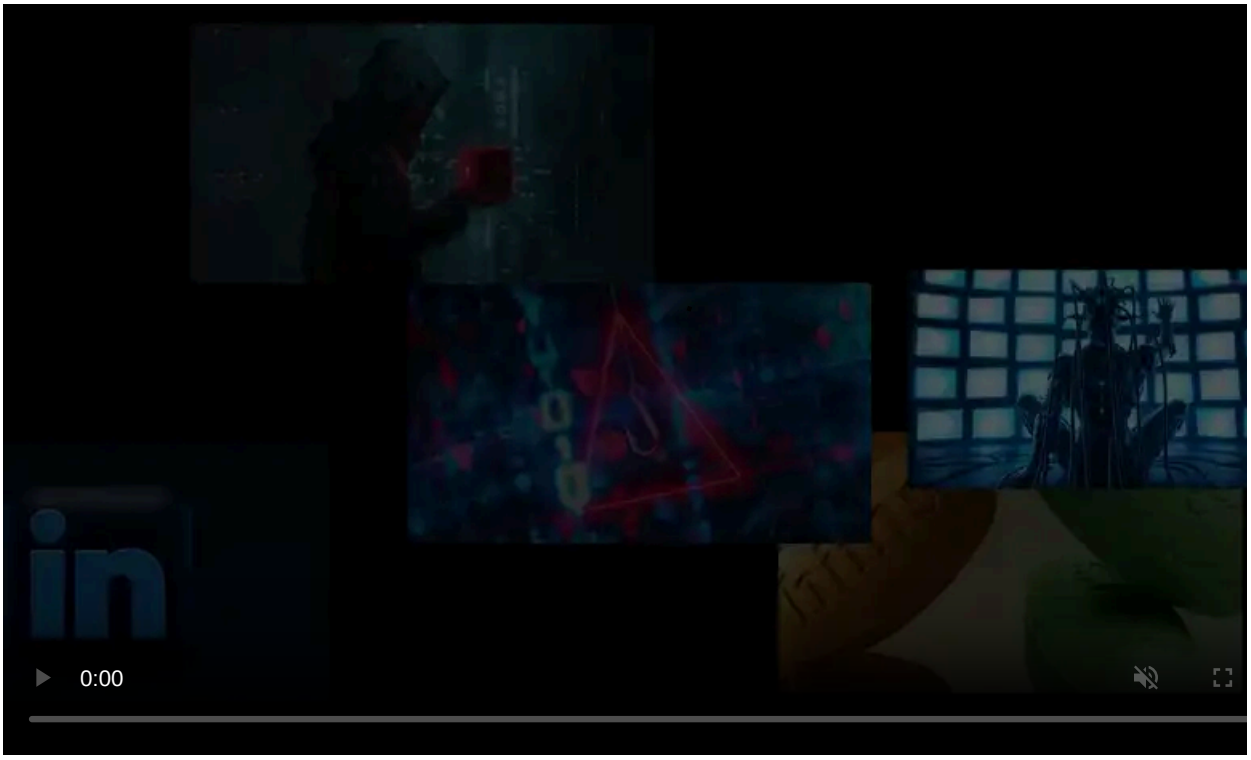
Published: 2020-07-03 · Archived: 2026-04-05 15:49:03 UTC

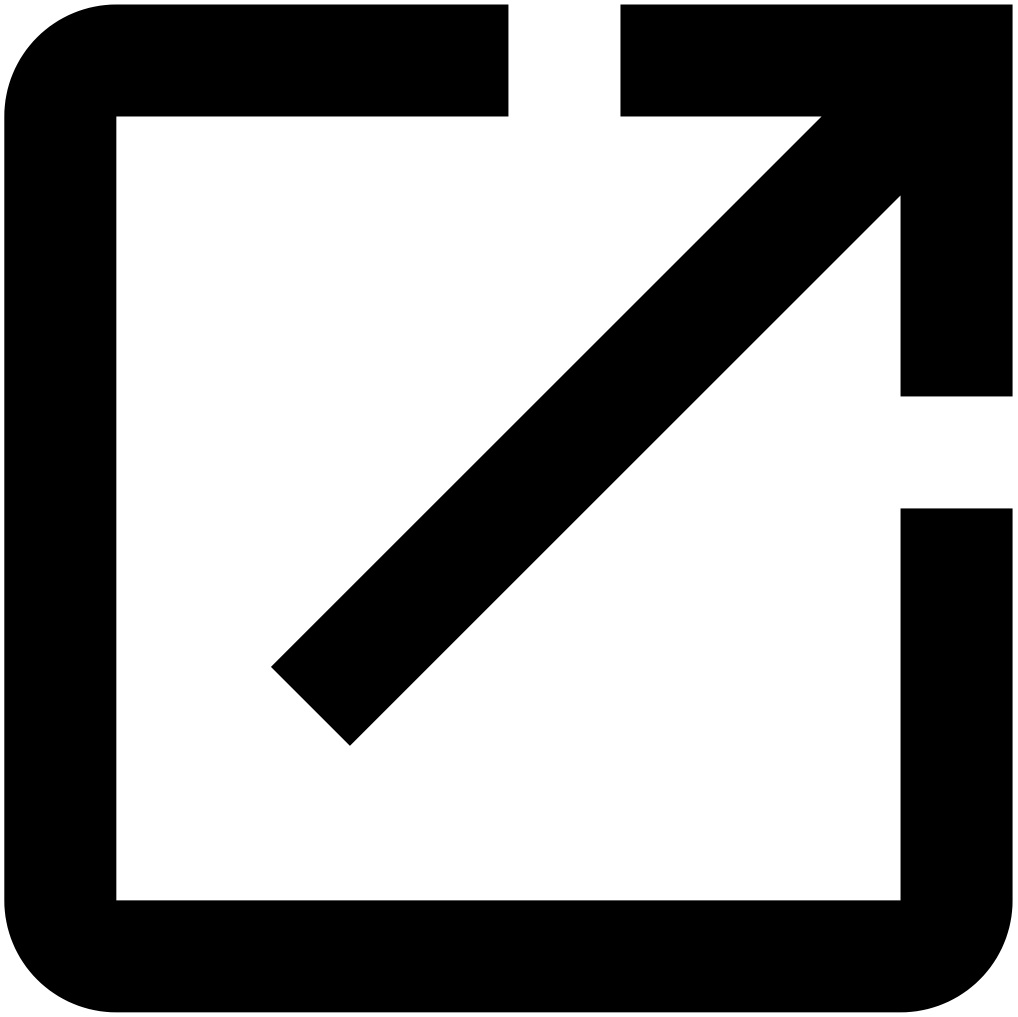
Avaddon ransomware has been spreading this week via an old technique that's making a comeback, Microsoft cautions on Thursday.

The attacks appear to be more targeted and rely on malicious Excel 4.0 macros to download the malware directly on the system.

Campaign focused on Italy

This file-encrypting malware emerged at the beginning of June, delivered "with a wink and a smile" in a massive spam campaign that did not focus on a particular type of user. Its operators are currently recruiting affiliates for spreading the ransomware payload.


0:00



The encryption routine is solid and files cannot be unlocked for free. A sample analyzed by BleepingComputer asked for a ransom of $900.

Microsoft Security Intelligence notes that the latest effort from the attacker focused on specific targets mainly in Italy, sending out emails with documents laced with malicious Excel 4.0 macros.

One such email found by malware hunter JamesWT_MHT pretends to be a notification from the Labor Inspectorate to a small business regarding work violations during "a period of crisis."

The subject of the message is alarming, informing the recipient of impending penalties and potential legal action. In the attachment, there is a ZIP archive named "Official notification."

The archived document contains an Excel 4.0 macro (XML), which is still compatible with modern software where VBA code is used instead.

When run, the macro downloads an Avaddon ransomware sample directly, without an intermediary downloader, Microsoft notes. This trend has been observed in other file-encrypting malware lately.

Using old macro bears fruit

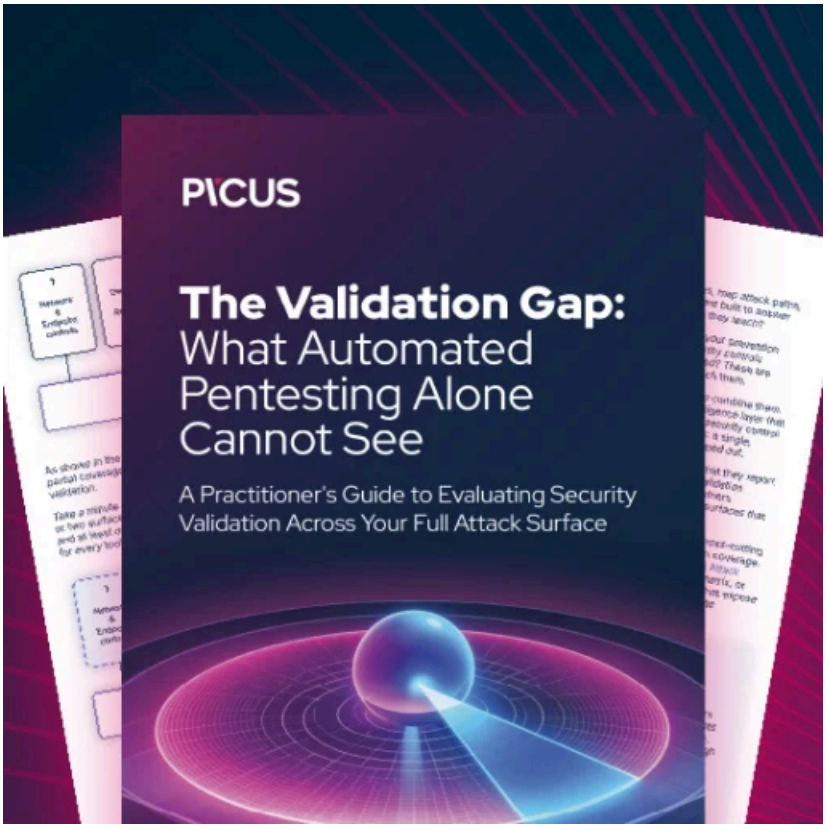
Choosing Excel 4.0 macros to spread the malware may seem peculiar, especially since it is was introduced in Microsoft Office products 28 years ago. However, Avaddon and numerous other threat actors have started using it recently.

In the case of Avaddon, this seems to yield results as the ransomware identification website ID Ransomware received a large number of submissions from victims. As seen below, the rise started on June 18 and then again on June 28 and 30, which is consistent with Micosoft's observations.

"While an old technique, malicious Excel 4.0 macros started gaining popularity in malware campaigns in recent months. The technique has been adopted by numerous campaigns, including ones that used COVID-19 themed lures" - Microsoft Security Intelligence

Launched in 1992, Excel 4.0 uses XML-based macros that store functions in BIFF (Binary Interchange File Format) records. This makes them more difficult to analyze compared to VBA macros that have dedicated streams and that are being used since Excel 5.0.

Microsoft noticed an increase in malicious email campaigns with Excel 4.0 macro over the past few months. Since April, the attackers started using the Covid-19 theme.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shows-that-excel-40-macros-are-still-effective/