Microsoft Detects New TA505 Malware Attacks After Short Break

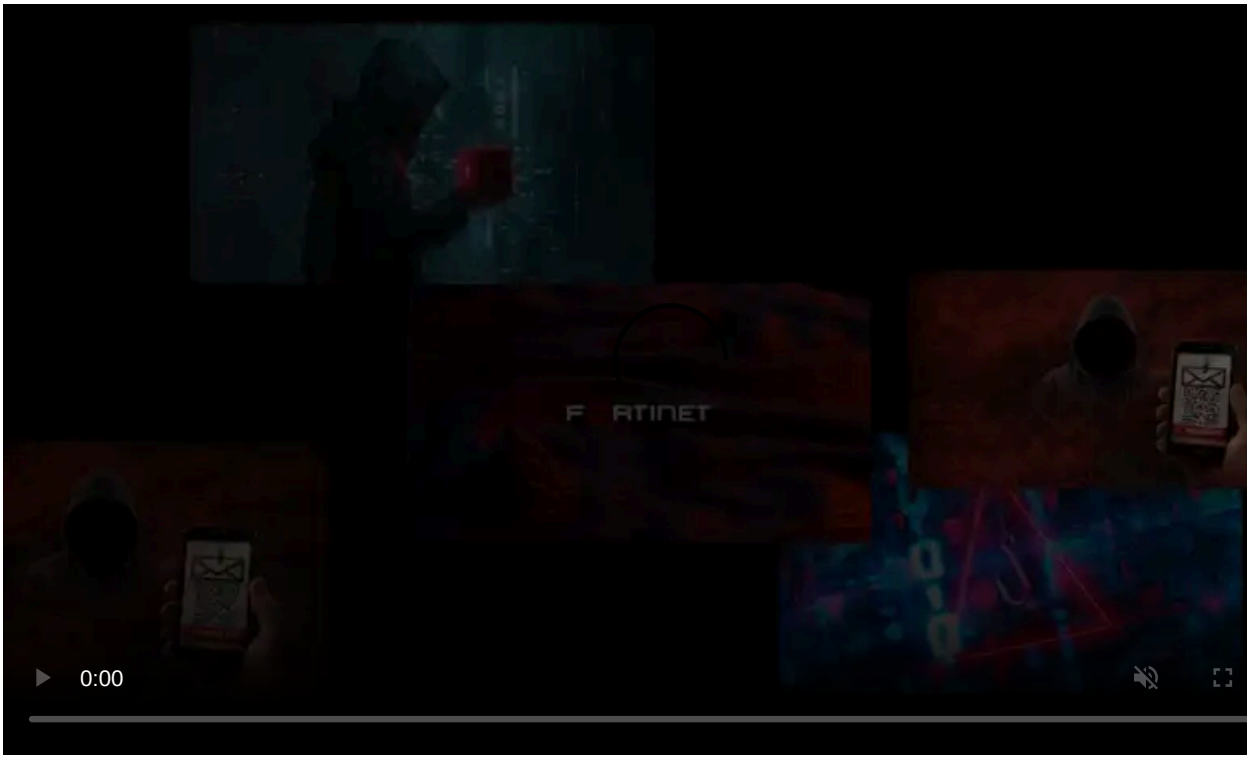
By Sergiu Gatlan

Published: 2020-01-31 · Archived: 2026-04-06 03:11:10 UTC

Microsoft says that an ongoing TA505 phishing campaign is using attachments featuring HTML redirectors for delivering malicious Excel documents, this being the first time the threat actors have been seen adopting this technique.

The new campaign is detailed in a series of tweets from the Microsoft Security Intelligence account, with the researchers saying that the final payload is being dropped using an Excel document that bundles a malicious macro.

TA505 (also tracked SectorJ04) is a financially motivated cybercrime group active since at least Q3 2014 [1, 2] known for focusing on attacks against retail companies and financial institutions via large-sized malicious spam campaigns driven by the Necurs botnet.


F RTINET
0:00

This threat actor distributed remote access Trojans (RATs) and malware downloaders that delivered the Dridex and Trick banking Trojans as secondary payloads, as well as Locky, BitPaymer, Philadelphia, GlobeImposter, Jaff ransomware strains on their targets' computers. [1, 2]

Kafeine from ProofPoint told BleepingComputer that the switch to HTML attachments occurred in the middle of January 2020.

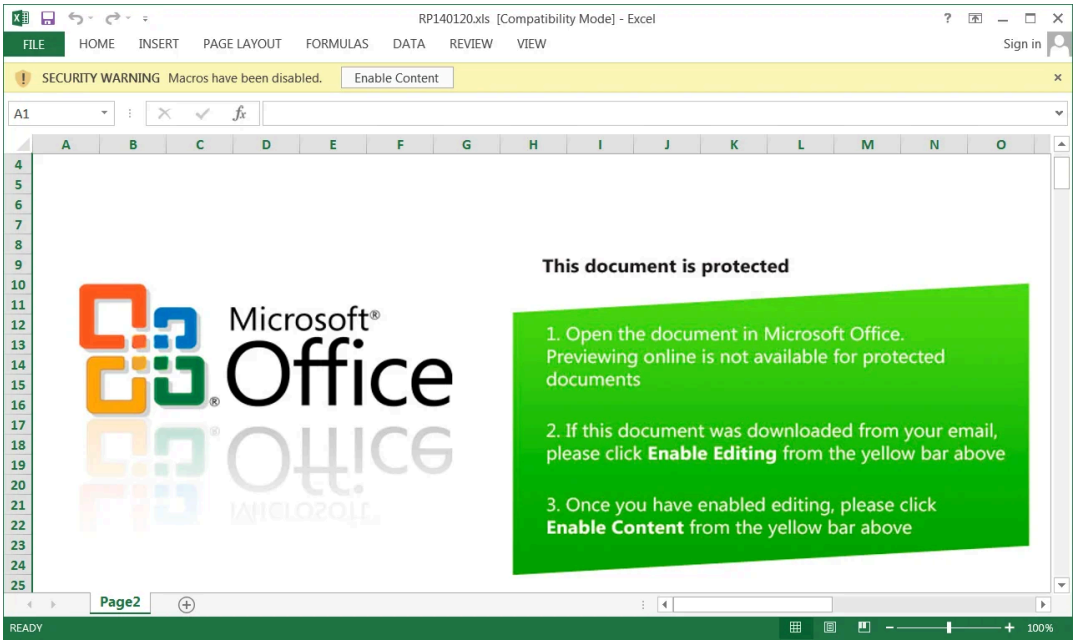
TA505 back from vacation

"The new campaign uses HTML redirectors attached to emails. When opened, the HTML leads to the download a malicious macro-laden Excel file that drops the payload," Microsoft Security Intelligence's researchers explain. "In contrast, past Dudear email campaigns carried the malware as an attachment or used malicious URLs."

As mentioned in the beginning, this campaign also marks the adoption of HTML redirectors as this is the first time Microsoft observed this technique being used by TA505 as part of their attacks.

Past email campaigns distributing the malware would deliver the payload onto the victim's computer within the attachment or via malicious download URLs.

The phishing messages come with HTML attachments which will automatically start downloading the Excel file used to drop the payload.

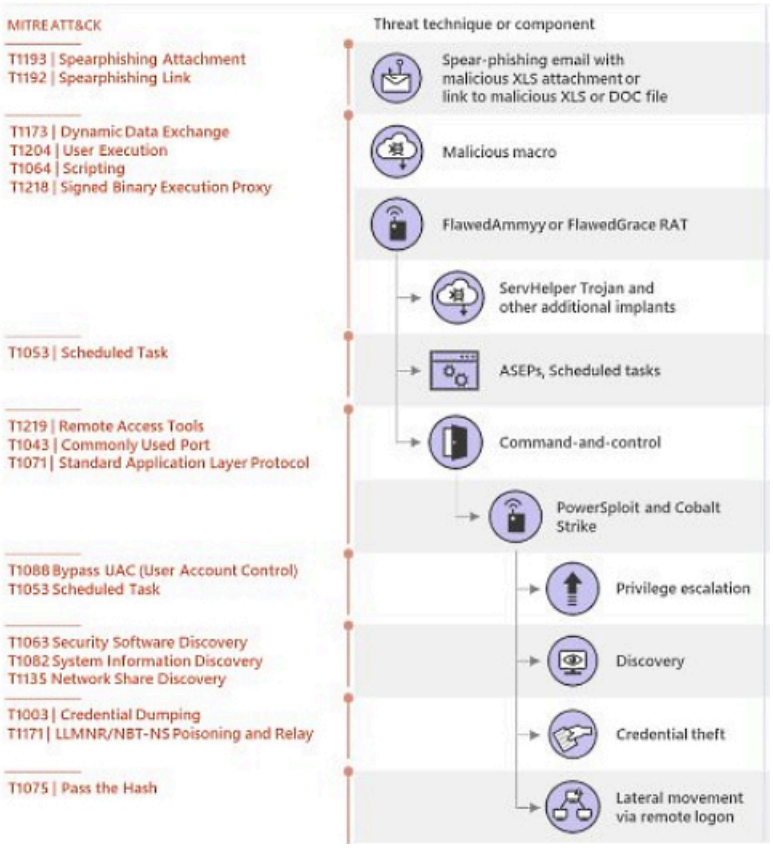


The victims are instructed to open the Excel document on their computer as online previewing is not available and to enable editing to get access to its contents.

"Once you have enabled editing, please click Enable Content from the yellow bar above," the bait Microsoft Office doc adds.

The operators behind this phishing campaign also use localized HTML files in different languages for victims from all around the world.

Also, the attackers make use of an IP traceback service that enables them to "track the IP addresses of machines that download the malicious Excel file."

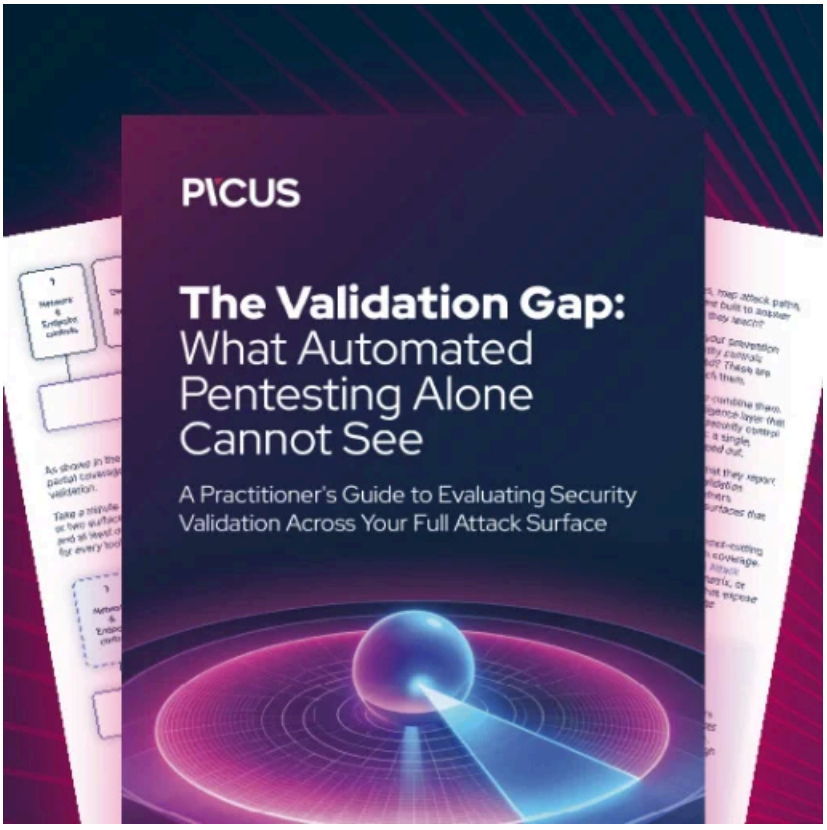


Threat Analytics report (*Microsoft*)

Once executed on the victim's computer, the malware will also attempt to drop a remote access trojan (RAT) tracked by Microsoft as GraceWire and as FlawedGrace by Proofpoint.

Microsoft Security Intelligence provides a full list of indicators of compromise (IOCs) including SHA-256 hashes of the malware samples used in the campaign here and here.

Update: Cleared up TA505 / Evil Corp confusion.



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/microsoft-detects-new-ta505-malware-attacks-after-short-break/