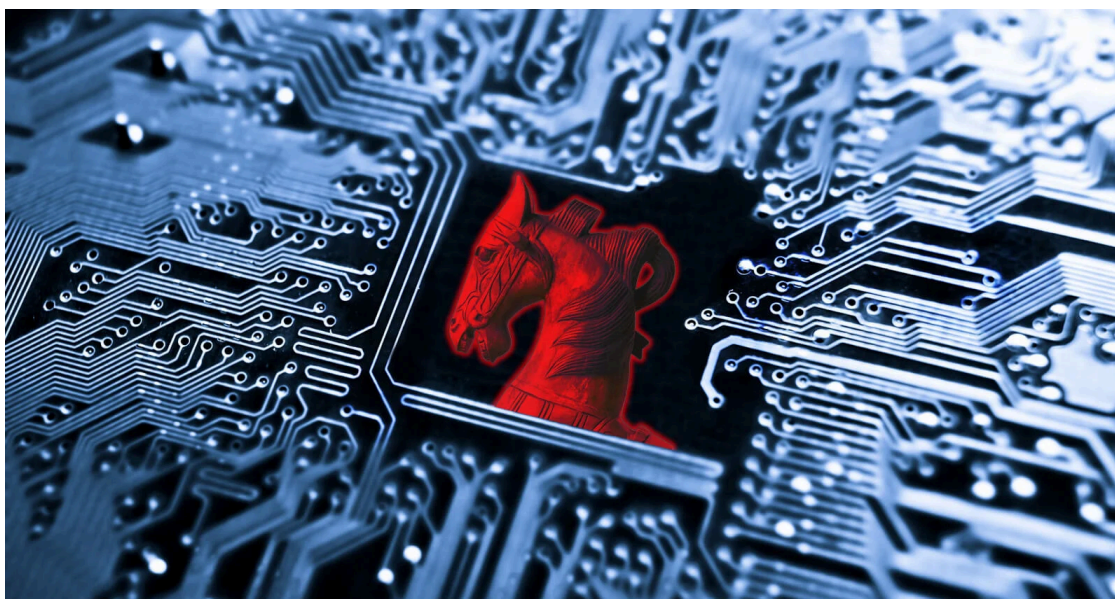


BazarBackdoor sneaks in through nested RAR and ZIP archives

By Ionut Ilascu

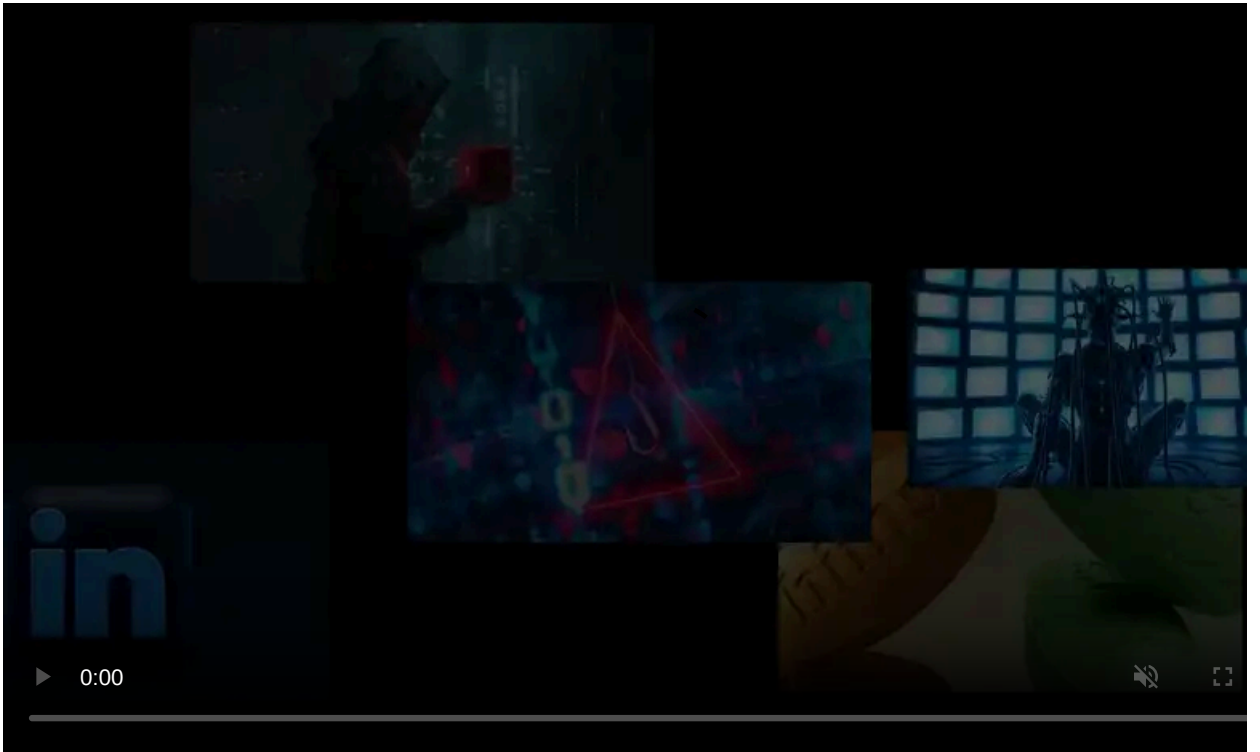
Published: 2021-07-14 · Archived: 2026-04-05 17:30:44 UTC



Security researchers caught a new phishing campaign that tried to deliver the BazarBackdoor malware by using the multi-compression technique and masking it as an image file.

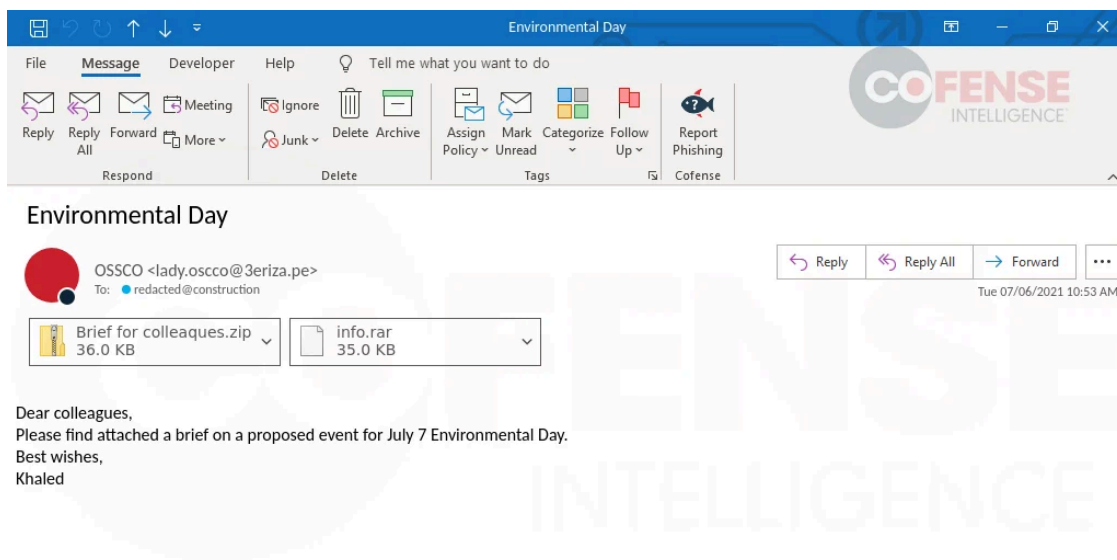
The multi-compression or nested archive method is not new but gained in popularity recently as it can trick email security gateways into mislabeling malicious attachments as clean.

It consists of placing an archive within another. Researchers at Cofense say that this method can bypass some secure email gateways (SEGs), which can have a limit to how deep they check a compressed file.



Visit Advertiser website [GO TO PAGE](#)

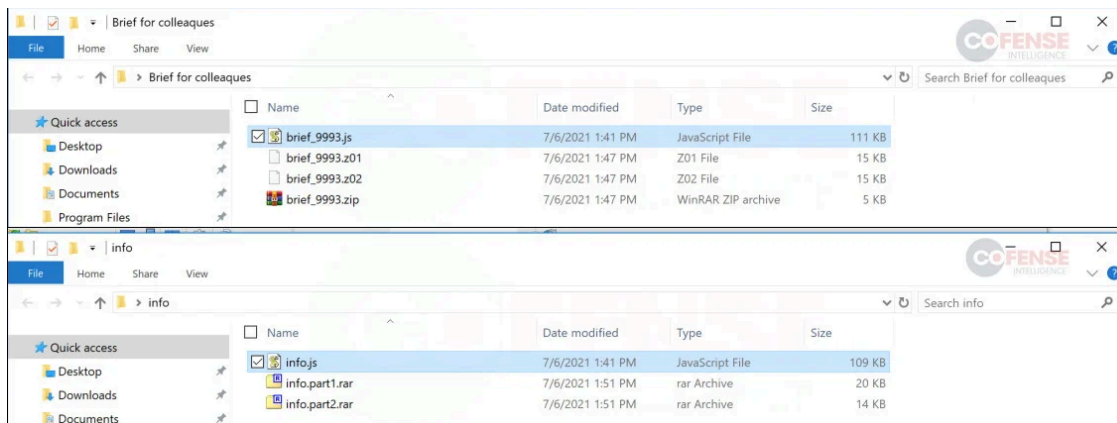
The new BazarBackdoor campaign deployed earlier this month and lured enterprise recipients with an “Environmental Day” theme, officially celebrated on June 5.



Tactic: Attached JavaScript | Threat: BazarBackdoor | SEG: Microsoft ATP

Both attached nested ZIP and RAR archives in the attachment contained a JavaScript file that ultimately delivered Trickbot’s BazarBackdoor malware, a stealthy backdoor typically used on corporate targets to provide remote access to the threat actor.

Cofense analyzed the recent malspam campaign and found that the role of the highly obfuscated JavaScript file was to download a payload with an image extension.



Cofense [explains](#) that “nesting of various archive types is purposeful by the threat actor as it has the chance of hitting the SEG’s decompression limit or fails because of an unknown archive type.”

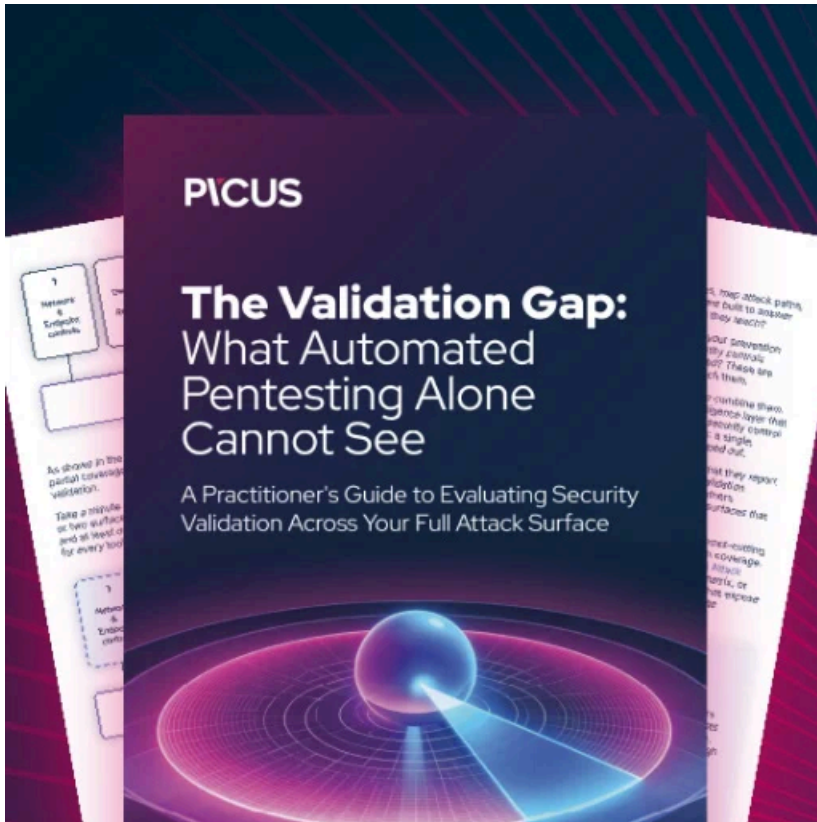
Obfuscated files can also pose problems to an SEG if there are several layers of encryption for the payload, increasing the chances of the malicious file passing undetected.

“Once executed, the obfuscated JavaScript would download a [BazarBackdoor] payload with a .png extension via an HTTP GET connection,” Cofense says, adding that the payload is an executable with the wrong extension.

Once deployed on a victim computer, BazarBackdoor may download and execute the Cobalt Strike, a legitimate toolkit designed for post-exploitation exercises, to spread laterally in the environment.

After gaining access to high-value systems on the network, threat actors can launch ransomware attacks, steal sensitive information, or sell the access to other cybercriminals.

Earlier this year, security researchers discovered a [BazarBackdoor variant written in the Nim](#) programming language, showing the effort Trickbot developer goes to keep the malware undetected and relevant to cybercriminal activities.



[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/bazarbackdoor-sneaks-in-through-nested-rar-and-zip-archives/>