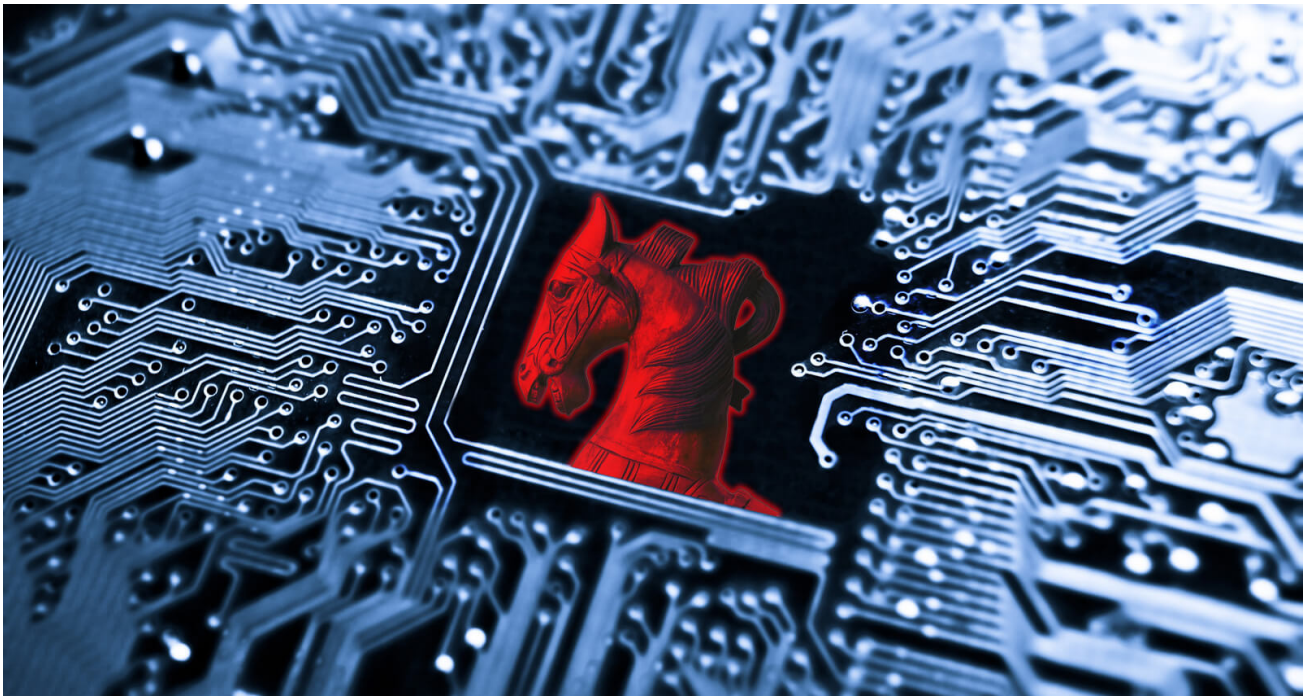
BazarBackdoor sneaks in through nested RAR and ZIP archives

bleepingcomputer.com/news/security/bazarbackdoor-sneaks-in-through-nested-rar-and-zip-archives/

Ionut Ilascu

By
Ionut Ilascu

- July 14, 2021
- 03:29 PM
- 2

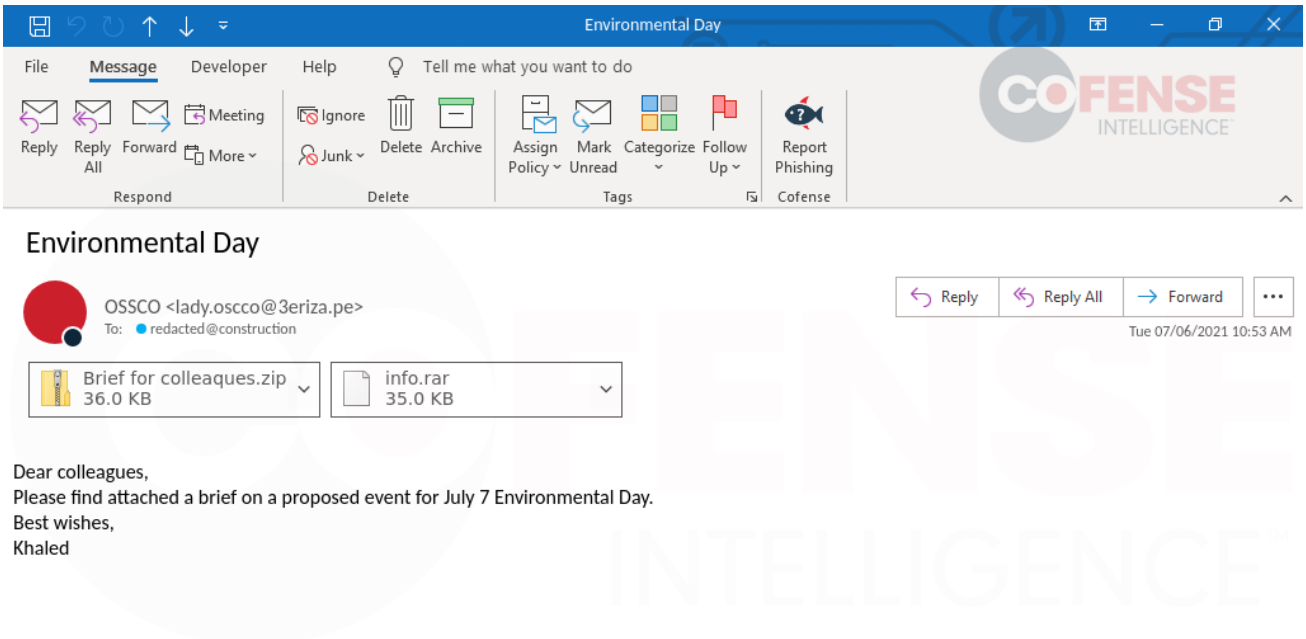


Security researchers caught a new phishing campaign that tried to deliver the BazarBackdoor malware by using the multi-compression technique and masking it as an image file.

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.

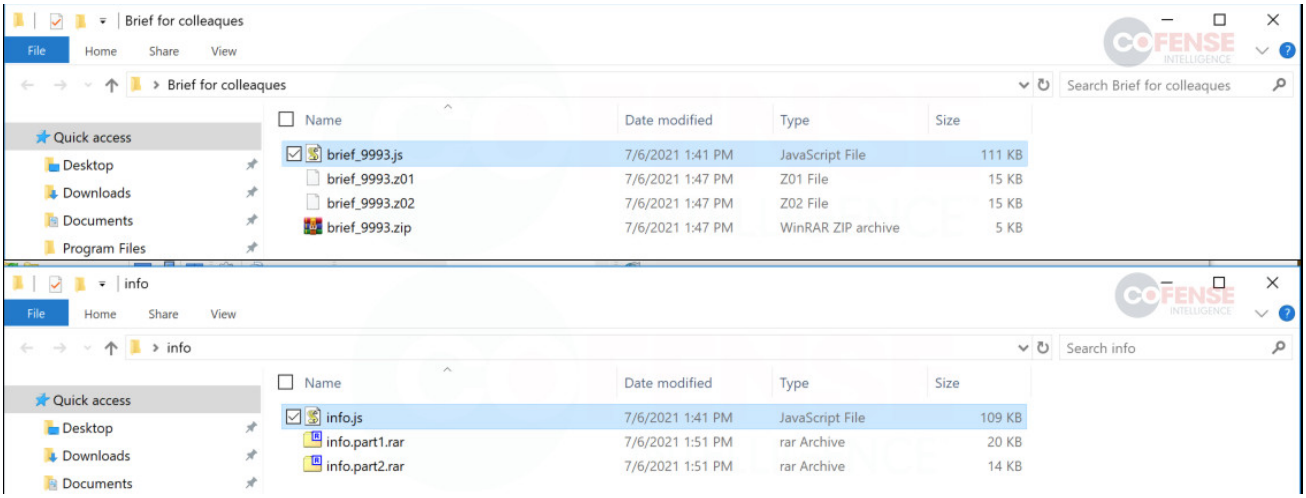
The new BazarBackdoor campaign deployed earlier this month and lured enterprise recipients with an “Environmental Day” theme, officially celebrated on June 5.



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.

Related Articles:

Google exposes tactics of a Conti ransomware access broker

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

Intuit warns of QuickBooks phishing threatening to suspend accounts

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Phishing websites now use chatbots to steal your credentials

- BazarBackdoor
- MalSpam
- Phishing
- RAR
- TrickBot
- Zip

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

- 

  IvoryHoward - 6 months ago

  -
  -

  Interesting!

- 

  IvoryHoward - 6 months ago

  -
  -

  Thanks!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: