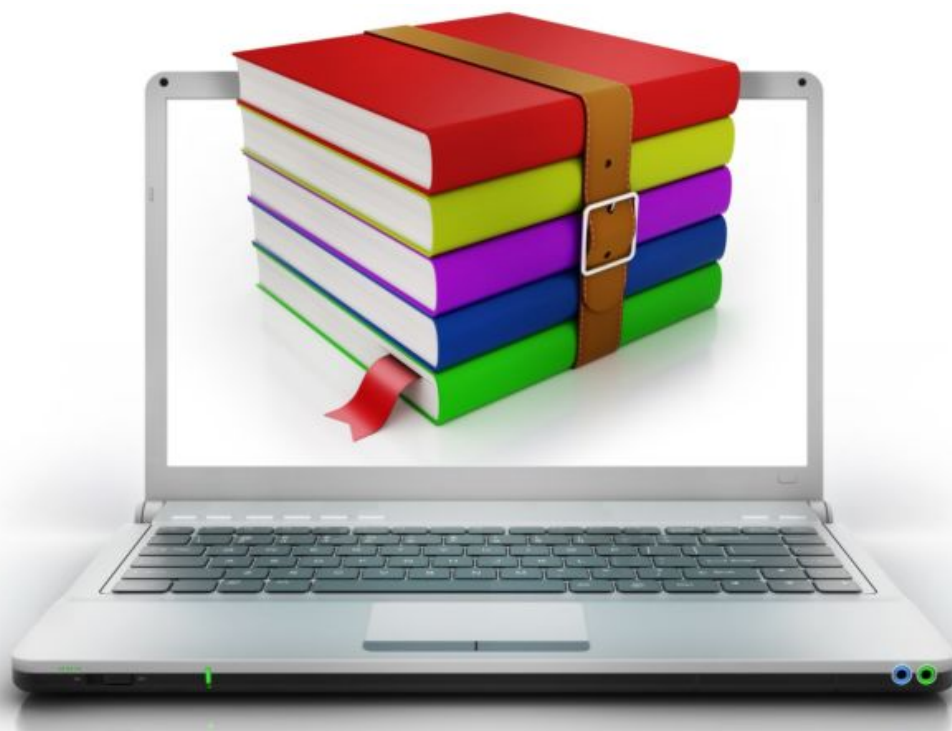


A rogue's gallery of bad actors is exploiting that critical WinRAR flaw



reader comments

54 with 45 posters participating

Share this story

A critical vulnerability in the WinRAR file-compression utility is under active attack by a wide range of bad actors who are exploiting the code-execution flaw to install password stealers and other types of malicious software.

In one campaign, according to a report published by researchers from security firm FireEye, attackers are spreading files that purport to contain stolen data. One file, titled leaks copy.rar, contains email addresses and passwords that were supposedly compromised in a breach. Attackers claim another file, cc.rar, contains stolen credit card data. Other

files have names including zabugor.rar, ZabugorV.rar, Combolist.rar, Nulled2019.rar, and IT.rar.

Hidden inside the files are payloads from a variety of different malware families. They include a keylogger known as QuasarRat and malware containing Chinese language text known as Buzy.

The FireEye report identified three other campaigns, including:

- One that impersonates an educational accreditation body that seems to use a PDF letter copied from the website of the Council on Social Work Education as a decoy. When extracted, the RAR file plants a Visual Basic script in the computer's startup folder. The script causes the computer to install a remote-access trojan called Netwire.
- An attack targeting the Israeli military industry that uses decoy files related to SysAid, a helpdesk service based in Israel. A malicious payload, dubbed SappyCache, will decrypt a file stored in a temporary folder to obtain the address of a command and control channel. SappyCache will then attempt to download and install a second-stage malware file from the server. The server never responded during the FireEye analysis.
- An attack potentially targeting a single person in Ukraine that uses a purported PDF message from the country's former President Viktor Yanukovich. The exploit drops a batch file into the startup folder that, when executed, installed a payload dubbed Empire.

FireEye isn't the only firm that's seeing such exploits. A separate report from security firm Symantec said that an espionage hacking outfit known both as Elfin and APT33 has been spotted exploiting the WinRAR vulnerability against a target in the chemical industry of Saudi Arabia.

Attackers sent a spear-phishing email to at least two employees in the targeted company. The email included a file dubbed JobDetails.rar. If extracted on a computer using a vulnerable version of WinRAR, the attack could install any file of the attackers' choice. Prior to the attack, Symantec updated its software to block exploits. The protection prevented the attack from working against the targeted company.

Adam Meyers, vice president of intelligence at security firm CrowdStrike, told Ars:

CrowdStrike tracks Elfin/APT-33 activity with a suspected nexus to the Islamic Republic of Iran under the name REFINED KITTEN. This actor has been involved in espionage operations primarily via spear phishing efforts since at least 2013. We can confirm that recently we have observed them deploying a malware we call PoshC2 targeting the Kingdom of Saudi Arabia using an employment themed lure and the recently disclosed CVE-2018-20250 vulnerability.

Interestingly, the Symantec report said that an Elfin attack on a US-based organization last February downloaded WinRAR on a compromised machine. Elfin downloaded and utilized WinRAR during their post-compromise attempts to exfiltrate data, Symantec Threat Analyst Sylvester Segura said in an email.

As Ars previously reported, the code-execution vulnerability in WinRAR went unreported for more than 19 years. It's the result of an absolute path traversal flaw that makes it possible for archive files to extract to the Windows startup folder (or any other folder of the archive creator's choosing) without generating a warning. From there, malicious payloads are automatically run the next time the computer reboots. The flaw was fixed in version 5.70. The vulnerability is especially serious, because WinRAR has an installed base of about 500 million, and the software has no means for

automatically updating itself.

Two weeks ago, a report emerged that attackers were exploiting the vulnerability to install hard-to-detect malware on vulnerable computers. The new reports indicate that the WinRAR attacks aren't likely to subside any time soon.

"We have seen how various threat actors are abusing the recently disclosed WinRAR vulnerability using customized decoys and payloads, and by using different propagation techniques such as email and URL," FireEye researcher Dileep Kumar Jallepalli wrote. "Because of the huge WinRAR customer-base, lack of auto-update feature, and the ease of exploitation of this vulnerability, we believe this will be used by more threat actors in the upcoming days."

<https://arstechnica.com/?p=1482285>