

APT-C-26 (Lazarus) 组织利用WinRAR漏洞部署Blank Grabber木马的技术分析

 ctfiot.com/286651.html

```
@Errors.Catch
def StealWallets(self) -> None:
```

APT-C-26

Lazarus

APT-C-26 (Lazarus) 是近年来最为活跃、最具破坏性的国家级 APT 组织之一，其攻击活动跨越金融、制造、航空航天、政府机构及加密货币等多个高价值行业。该组织不仅具备复杂的跨平台攻击能力，还持续投入资源开发专用的漏洞利用链、持久化工具和多阶段载荷框架，以最大化攻击成功率和隐蔽性。

一、概述

近期360高级威胁研究院捕获Lazarus组织利用WinRAR漏洞CVE-2025-8088进行投毒攻击的新型样本，攻击者将含有恶意脚本的RAR文件伪装为正常工具包诱导用户下载，受害者一旦解压文件便会触发恶意脚本释放，随后该脚本下载Blank Grabber信息窃取木马。该木马主要针对Chromium系浏览器的密码、Cookies、自动填充数据，窃取Discord与Telegram完整会话，并针对MetaMask、Exodus、Electrum等20余种主流加密钱包的种子私钥进行窃取。通过此次详细分析及曝光披露，希望相关企业和个人能够提高安全防范意识，采取有效措施保护企业资产和用户财产免受损失。

二、攻击活动分析

1. 载荷投递分析

Lazarus组织通过投递名为“Pharos.rar”的压缩包文件针对受害者展开攻击，基本信息如下：

MD5 faa9dec02bad43b1af68a4194dea8762

文件名称 Pharos.rar

文件大小 115 KB (118,528 字节)

“Pharos.rar”是一个携带“CVE-2025-8088”漏洞，伪装成“Pharos-Automation-Bot”项目的压缩包文件。“CVE-2025-8088”是WinRAR程序存在的路径穿越漏洞，其漏洞成因在于WinRAR工具在处理ADS数据流时对于ADS流的路径没有进行充分校验导致攻击者可以构造恶意的ADS流路径(ADS通过路径中的“：”符号区分本体数据和流数据)，从而将指定文件写入攻击者指定的目录下从而实现任意代码执行。

如下是分别使用360压缩程序和WinRAR打开“Pharos.rar”文件展示图，360压缩将其显示为一个文件目录，而WinRAR程序并没有显示，这样就迷惑了受害者，以至受害者认为没有其他文件。

如图可见，“Pharos.rar”压缩包有多个RarBlock区块，其中0号区块是主区块，1到22号区块以File区块和NTFS区块两两交替分布，表示每个文件实体后紧跟一个NTFS Alternate Data Stream (ADS) 数据。

每个NTFS区块中，有多个属性结构体，其中Name为“STM”，标识该数据流属性，以及DataArea字段存储ADS文件的实际路径。

通过分析，WinRAR会逐个解析RarBlock结构体，当解析到携带ADS流的RarBlock结构体时，会判断Name字段是否是“STM”，如果是执行“cve_2025_8088_start”，并将RAR文件中的压缩文件本体路径传入。

cve_2025_8088_start函数逻辑是这样的，首先解析RarBlock结构体中的RecordData数据（这部分数据在RAR文件中表示的是ADS路径）。然后判断ADS路径是否以“：”开头，

然后将传入的文件本体路径和获取到的ADS路径进行拼接。

最后，根据拼接好的路径传入指定函数中，继而通过CreateFileW函数创建携带ADS流的文件。

但是，WinRAR7.12并没有对待创建的文件路径进行校验，导致异常的文件路径“[dir]Pharoscontract_adress_1.txt:..AppDataRoamingMicrosoftWindowsStart MenuProgramsStartup1.bat”传入CreateFileW中，而合法的文件路径为“[dir]Pharos\contract_adress_1.txt:1.bat”，即ADS名称部分（冒号后）不能包含路径分隔符“\”。这点在WinRAR 7.13的补丁中已被修复，通过强制校验ADS路径格式，确保其符合规范，从而阻断利用异常路径实现任意文件写入的攻击手法。

一旦用户解压上述攻击者投递的恶意文档，就会触发目录穿越漏洞，将名为“1.bat”的恶意载荷释放到“C:\Users\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup”目录，以展开后续攻击。

释放到自启动目录下的1.bat脚本是一个伪装成“Windows Defender 更新提示”并下载、执行恶意载荷（stub.pyw）的恶意脚本，内容如下所示。

其执行时首先调用powershell弹出Windows Defender 更新警告框，诱导用户关闭杀软。接着从Dropbox下载一个Python脚本（stub.pyw）到%USERPROFILE%\Downloads目录并执行。1.bat执行警告框如下图所示：

2. 攻击组件分析

下载的stub.pyw是一个用多层嵌套字符串反序+base64解码+zlib解压缩的动态执行器（loader）。它从混淆的字节串中还原出压缩的Python代码，然后使用exec()执行。

经过63轮反序+base64解码+zlib解压缩后可得到第一次明文。如下图所示：

但是得到的明文又分两部分，第一部分继续是使用相同方式混淆的代码，第二部分明文是基于的Python木马。

针对第一部分混淆的代码继续经过63轮解压缩得到明文，其主要功能是判断当前机器是否有Python环境，没有则安装以便后续代码执行，然后在启动目录下写入Tsunami Injector脚本。

具体做法是从Python官网下载Python 3.11安装包，Startup目录下写入Windows Update Script.pyw形成持久化。

Windows Update Script.pyw会继续创建计划任务，并解密url列表从Pastebin下载Tsunami-Installer。解密方式采用hex+xor+base64解码+反序的方式，如下图所示：

Tsunami-Installer后续会下发多个加密货币挖矿程序和凭证窃取程序。

第二部分的Python代码是一个开源的信息窃取木马（Stealer），项目名称为“Blank Grabber”，项目地址为<https://github.com/Blank-c/Blank-Grabber>。Blank Grabber的通信模式支持Discord和Telegram两种方式，在配置Setting里进行定义，同时配置里面还定义了哪些功能的开启，如下图所示。

根据配置可知本次使用Telegram进行通信，其Bot Token和ChatID为：7400917372:AAHuzyKxmWHc4L7jUOENK0BGNB0k1pI65IE\$783432595。其执行时隐藏窗口，接着创建互斥体“il9MGMxYXWAExxAm”，然后开启窃密行动。

首先窃取浏览器密码+Cookies+自动填充+历史记录数据，主要包括基于Chromium内核的浏览器如：Chrome、Brave、Opera、Microsoft Edge、Yandex Browser等。

窃取Telegram会话数据。

窃取DiscordToken数据，支持所有 Chromium 浏览器，还特别增加了Firefox浏览器的适配，获取数据包括完整Token、邮箱、手机号、付款方式、Nitro状态等。

接着窃取钱包，涵盖Zcash、Armory、Bytecoin、Jaxx、Exodus、Ethereum、Electrum、Atomic Wallet、Guarda、Coinomi、MetaMask、Phantom、TronLink、Binance Wallet等20多种主流钱包。

Blank Grabber木马的功能较齐全，不再一一叙述，其完整功能及本次木马开启的功能如下表所示：

功能	功能描述	是否开启
PingMe	发送消息时@everyone提醒攻击者	
Vmprotect	反虚拟机/反沙箱	
Startup	开机自启动（复制到StartUp文件夹）	
Melt	运行完毕后自删除	
UacBypass	UAC提权绕过	
ArchivePassword	设置ZIP/RAR 压缩包密码（当前为 1）	是
HideConsole	隐藏黑色控制台窗口	是
Debug	输出调试日志	
RunBoundOnStartup	释放并运行资源中绑定的额外文件	
CaptureWebcam	摄像头捕获	
CapturePasswords	窃取浏览器保存的账号密码	是
CaptureCookies	窃取浏览器的Cookies（含登录态）	是
CaptureAutofills	窃取浏览器自动填充（姓名、电话、地址、身份证等）	是

CaptureHistory	窃取浏览器历史记录	是
CaptureDiscordTokens	窃取所有Discord Token（含邮箱、付款方式、Nitro）	是
CaptureGames	窃取Minecraft、Steam、Epic、Growtopia等游戏会话	
CaptureWifiPasswords	窃取已连接过的所有WiFi密码	
CaptureSystemInfo	窃取系统信息、硬件信息、IP归属等	
CaptureScreenshot	多显示器全屏截图	
CaptureTelegram	窃取Telegram会话数据	是
CaptureCommonFiles	窃取文件	
CaptureWallets	窃取 MetaMask、Exodus、Electrum等20+加密钱包种子/私钥	是
FakeError	运行时弹出假错误弹窗迷惑用户	
BlockAvSites	修改hosts屏蔽杀毒软件官网	
DiscordInjection	向Discord客户端注入JS后门	

从上分析可知，Lazarus组织利用Blank Grabber木马精准开启了“浏览器全家桶 + Telegram + Discord + 加密钱包”四大最值钱功能，目的很纯粹，旨在系统性收集受害者的凭证与资产信息，为后续账户接管、资金转移和供应链渗透创造条件。

三、归属研判

通过对本次攻击活动的深入分析，发现攻击方式与Lazarus组织技术特征较为符合，具体总结如下：

1. 本次样本使用的解混淆方式：多轮反序+base64解码+zlib解压缩和Lazarus组织之前攻击方式相同。

2. 本次样本释放的Tsunami Injector和安全研究机构 HiSolutions对Lazarus Tsunami框架的详细分析报告[1]基本一致，具体到文件名，函数名及解压密码“!!!HappyPenguin1950!!!”等都与报告相同。

3. 本次攻击也是针对加密货币领域，诱饵名“Pharos.rar”伪装成“Pharos-Automation-Bot”（一个在加密货币量化交易圈广为人知的自动化交易机器人项目），精准迎合了目标人群（加密货币玩家、量化开发者与DeFi从业者），符合Lazarus组织持续针对加密货币领域特点。

综上，将本次攻击活动归属到APT-C-26（Lazarus）组织。

总结

APT-C-26（Lazarus）组织利用PyPI供应链投毒攻击已造成多起金额高达数百万美元的加密货币盗窃事件。该组织通过不断迭代跨平台投毒技术和结合最新漏洞实现快速武器化，显示出其对加密货币领域的高度关注和持续投入。建议所有使用Python开发环境以及处理外部RAR文件的用户及企业立即升级WinRAR至最新版本、严格审查PyPI软件包来源可靠性，并部署针对性检测规则，以有效防范该组织的供应链攻击和后续加密资产窃取行为。

附录 IOC

MD5

faa9dec02bad43b1af68a4194dea8762

273af5e2e0130baee7d3b55081be5ad5

41df3b66ebcfb6e4d4d581d678299041

参考

[1]<https://research.hisolutions.com/2025/04/rolling-in-the-deepweb-lazarus-tsunami/>

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

360高级威胁研究院是360数字安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外广泛认可，为360保障国家网络安全提供有力支撑。

| 本篇文章来源于微信公众号: 360威胁情报中心