Unknown Title

警惕！APT-C-08（蔓灵花）组织首次借WinRAR漏洞CVE-2025-6218实施网络攻击

APT1天前发布 admin 60 0 0

APT-C-08

蔓灵花

APT-C-08（蔓灵花），又称BITTER。是一个拥有南亚地区政府背景的APT组织，近几年来持续发起针对南亚及周边国家的APT攻击，主要攻击政府、驻外机构、高校和军工行业等相关单位，以窃取敏感信息为主，具有强烈的政治背景。

该组织攻击载体变化多样，善于使用各类恶意文档作为攻击入口，引诱用户打开从而下载恶意载荷让其中招，以此来窃取敏感信息。

一、概述

近期，我们捕获到蔓灵花组织利用CVE-2025-6218（WinRAR目录穿越漏洞）实施攻击的样本，鉴于该漏洞利用难度低、危害性高且系该组织首次使用，加之WinRAR压缩程序一般不主动升级的特性，我们决定披露这批样本，以便用户及时发现并规避风险。

二、攻击活动分析

1. 载荷投递分析

MD5　　f6f2fdc38cd61d8d9e8cd35244585967

文件名称 Provision of Information for Sectoral for AJK.rar

文件大小 51.4 KB (52,674 字节)

利用漏洞 CVE-2025-6218

攻击者投递的载荷是一个名为“Provision of Information for Sectoral for AJK.rar”的压缩包文件，该压缩包文件利用WinRAR的目录穿越漏洞，使攻击者突破预期的文件系统边界，将恶意文件释放至未经授权的目录位置，当相关进程访问或加载该目录下的文件时，从而达到执行恶意代码的目的。

攻击者为了提高漏洞利用的成功率，构造了两个特殊的文件路径，分别为“ /.. /.. /AppData/Roaming/Microsoft/Templates/Normal.dotm”和“ /.. /.. /..

/AppData/Roaming/Microsoft/Templates/Normal.dotm”，值得注意的是攻击者构造的特殊路径中，在“..”符号后存在一个空格，这是漏洞能够触发的原因所在。

CVE-2025-6218漏洞成因在于WinRAR7.11及以前版本在提取文件进行路径规范化的过程中，程序会校验路径中的分隔符“\”的前一个字符，会判断当前字符串是否为“ ”(空格)和“.”（点号），如果不为这两个字符，就不会进行任何处理。

同时路径中又不能以“ ”（空格）开头，如果是以空格开头就需要转化为字符“_”。但是，开发者在后续对路径的处理中，又忽略了路径中间存在“ ”（空格）的情况。

所以，我们只需要构造“\.. \” 这样的路径，就会执行异常路径处理过程，将不符合规定的字符移出。

显然，在执行完异常字符处理流程之后，路径中带有的异常字符“ ”（空格）已经被移除。

当受害者利用WinRAR解压带有漏洞利用的压缩包文件之后，恶意的Normal.dotm会释放到C:Users[username]AppDataRoamingMicrosoftTemplates目录下，该目录是系统中 Microsoft Word 模板文件的默认存放路径，当受害者打开“Document.docx”文件或者电脑中的其他word文档时，便会加载通过漏洞释放的“Normal.dotm”文件，从而实现恶意代码执行。

2. 恶意载荷分析

MD5 4bedd8e2b66cc7d64b293493ef5b8942
文件名称 Normal.dotm
文件大小 19.9 KB (20,403 字节)

加载的Normal.dotm是一个宏文件，其目的是使用“net use”将远程目录映射到本地，然后执行远程目录下的“winnsc.exe”文件。

winnsc.exe是一个Downloader,执行时获取主机名、用户名及系统版本等信息采用post的方式发送到服务器https[:]//teamlogin.esanojinjasvc[.]com/teamesano/drivers/teamzid.php，根据服务器响应下载后续载荷并执行。

后续下载的多个载荷为蔓灵花组织常用木马组件，其中一个为C#木马，这里不再展开详细叙说，具体如下：

三、关联分析

MD5 84128d40db28e8ee16215877d4c4b64a
文件名称 Weekly AI Article.rar
文件大小 596 KB (610,436 字节)

CVE编号 CVE-2025-6218

同时，我们还捕获到了蔓灵花组织测试的另外一个利用CVE-2025-6218漏洞的投递载荷。攻击者还是将恶意载荷释放到C:Users[username]AppDataRoamingMicrosoftTemplates下，一旦受害者打开其他docx文件，就会加载该恶意载荷。

MD5 f8b237ca925daa3db8699faa05007f12
文件名称 Normal.dotm
文件大小 20.0 KB (20,480 字节)

加载的Normal.dotm是一个宏文件，其目的是使用cmd执行从远端
https[:]//www.tapeqcqoptions[.]com/d6Z2.php?rz=%computername%下载回来的cmd命令。

总结

APT-C-08（蔓灵花）组织近年来依旧保持活跃态势，持续利用各类已知漏洞与新型载荷开展攻击行动，展现出高度的组织化和专业化特征。近期监测到该组织在攻击活动中结合使用WinRAR目录穿越漏洞，将恶意文件释放到系统关键目录，从而实现隐蔽持久化与后续控制。
本文针对其使用的漏洞样本进行了深入分析，希望帮助用户了解此类攻击链条及防范手段。同时也提醒用户提高安全意识，在日常工作中谨慎处理未知压缩包、邮件附件和超链接，避免因轻信而在毫无防护的情况下遭受入侵，造成敏感信息和重要数据的泄露。

附录 IOC

MD5

4bedd8e2b66cc7d64b293493ef5b8942

f6f2fdc38cd61d8d9e8cd35244585967

f16f2e4317c37085cad630d41001f7c3

84128d40db28e8ee16215877d4c4b64a

f8b237ca925daa3db8699faa05007f12

418d73efd622ebec29759c081768db16

5d677781d6c7d4ddee967c1cc7e869ce

C&C

koliwooclients[.]com

teamlogin.esanojinjasvc[.]com

tapeqcqoptions[.]com

johnfashionaccess[.]com

wmiapcservice[.]com

团队介绍
TEAM INTRODUCTION
360高级威胁研究院
360高级威胁研究院是360政企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，赢得业内外的广泛认可，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

上一篇

APT-C-60（伪猎者）的近期活动分析与技术演进

下一篇

没有更多了...

相关文章