APT

o检测的Melofee 木马新变种曝光，专攻RHEL 7.9系统

Alex.Turing
2024年11月12日 • 8 min read

简介

2024年7月27日，XLab的大网威胁感知系统检测到 IP 地址 `45.92.156.166` 正在传播一个名为pskt的ELF 文件，它在 VirusTotal 上尚无检测。该样本触发了两条告警：文件存在 Overlay 区段，且通信域名疑似模仿微软。经过分析，我们确认这是一个专门针对 Red Hat Enterprise Linux (RHEL) 7.9 的 Melofee 后门木马变种。

Melofee 是一个用 C++ 编写的后门木马，支持信息收集、进程管理、文件操作和 SHELL 等功能，最早于 2023 年 3 月被 ExaTrack 披露，据信隶属于 **APT 组织 Winnti**。此次捕获的样本相比旧版本在文件结构和功能层面均有显著升级。文件结构方面，新变种内嵌了一个 RC4 加密的内核级驱动模块，专门用于隐藏活动痕

迹，包括样本文件、进程和网络通信。在功能上，新样本在持久化、单一实例机制以及功能号设计方面也有所变化。

通过比较样本中的 RTTI（运行时类型信息），甚至可以看到源码层面的改动。例如，先前样本中的网络连接类名为 `TLSSocket`，而本次样本的类名已更改为 `TlsConn`，这暗示 Melofee 可能在安全社区的监测之外被持续重构和使用。

值得注意的是，我们在溯源过程中还发现了一个有趣的**误关联**。新变种使用的 C2 地址为 `filemanage.micrsofts-file.com`。根据 PDNS 系统记录，该 C2 的二级域名 `micrsofts-file.com` 及其关联域名 `www.micrsofts-file.com` 在 2023 年 11 月至 2024 年 6 月期间解析至 IP 地址 `91.195.240.123`。该IP也出现在 2024 年 7 月 BlackBerry 发布的 APT 组织 SideWinder 分析报告中，且在 VirusTotal 上，它已被多家安全厂商标记为恶意。这是否意味着 Melofee 已在多个组织间流通，成为跨组织使用的工具，而非某个特定组织的专属？

我们认为答案是否定的。`91.195.240.123` 实际上是域名注册商 NameSilo 提供的 Parking IP，**我们认为将其标记为恶意属于误报**。NameSilo 会自动将新注册的二级域名及 `www` 三级域名解析至该 IP，因此，正常域名、不相关的恶意域名及 APT 活动可能共享此 IP，导致误导性的关联。

由于视野有限，我们尚不清楚攻击者的具体入侵手段及其后续目的，欢迎知情者提供更多线索，以帮助完善技战术矩阵。鉴于样本及域名的低检测率，以及Melofee家族的高隐匿性我们决定撰写本文，与社区分享我们的发现，共同维护网络安全。

本文将深入分析以下要点：

- Overlay 结构及其解密方法
- 驱动模块功能
- Melofee功能

技术细节

目前我们只捕获了一个样本，它的基本信息如下所示：

```
MD5: 603e38a59efcf6790f2b4593edb9faf5
Magic: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, Buil
```

此变种的的功能相对直观，可根据运行方式是否带有参数，划分为 **感染模式** 和 **管理模式** 两种：

- **感染模式**（无参数启动）：当 Melofee无参数启动时，进入感染模式。在此模式下：
  - 通过 `/tmp/lock_tmp1` 文件确保仅有一个实例运行。
  - 借助 `crontab` 实现持久化，并将进程名称伪装为 `[md]`或 `wwwwww`。
  - 解密并安装驱动模块，在驱动支持下，实现目录，文件、进程，网络连接，特定内容等多维度的隐匿。
  - 解密并连接至 C2 服务器，建立通信，等待接收和执行服务器下发的指令。
- **管理模式**（带参数启动）：当 Melofee 带有参数启动时，进入管理模式，接受一个参数控制驱动的隐藏状态。可用参数为：
  - **hide**：启用驱动的隐藏功能。
  - **show**：关闭驱动的隐藏功能。
  - **kill**：停止进程。

这种设计使得Melofee可以在感染和管理两种模式下灵活运作，满足不同场景下的隐蔽性和控制需求。下文将详细分析 Melofee 的技术细节，重点包括解密过程、驱动模块以及后门功能等方面。

Part1: 解密

Melofee 将 RC4 加密的驱动模块以 `drv_overlay` 结构体的格式附加在文件尾部，作为 Overlay 部分存储。

```
struct drv_overlay
{
    int encrypted_payload[payload_size];
    int payload_size;
    char flag[12];
}
```

在这个样本中flag的值为`EV#?YLFAkoip`，payload_size为0x6a08，从playload_szie往前的0x6a08字节为encrypted_payload。

使用秘钥**87JoENDi**对encrypt_payload进行解密，就得到了驱动模块kworkerx，可以看出它针对的操作系统为RHEL 7.9，内核版本为3.10.0。

C2配置同样使用RC4加密，秘钥为`87JoENDi`。

```
------------------------------------------------------------------------
C2 CipherText
00000000  a2 a4 96 0e 27 ee 40 54 a5 3a 52 8e 65 cf b1 e1  |¢¤..'î@T¥:R.eÏ±á|
00000010  29 69 32 86 ae 56 4d 28 a2 b8 da 6e e1 05 5d 65  |)i2.®VM(¢¸Úná.]e|
00000020  fc 86 88 50 43 17                                 |ü..PC.|
------------------------------------------------------------------------
```

解密后的C2配置为`0:filemanage.micrsofts-file.com:443:60`，它包含以下4部分：

- 连接的类型
- C2 Domain
- C2 Port
- Interval

Part2: 驱动模块分析

解密得到的驱动模块kworkerx的基本信息如下所示，经过分析我们确定，它实际上是由开源项目Reptile修改而来。

```
MD5: 839f60efee25f07df7b23ba9d6bef892
Magic: ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), BuildID[sha1]=c4400284
```

原生的Reptile支持以下通过12种功能，可以分成隐藏，后门2大类；kworkerx主要使用其中的隐藏功能。

`kworkerx` 通过在初始化函数中挂钩 `tcp4_seq_show` 来隐藏网络通信记录，所有 443 端口的通信都不显示。对于进程、文件和目录的隐藏，kworkerx则通过挂钩 fillonedir、filldir、filldir64 以及 vfs_read 等函数来实现。

此外，kworkerx 还挂钩了 `inet_ioctl` 函数，以便与用户空间通信，接收控制命令。

当用户空间调用ioctl函数时，若传入的第二个参数为 **0xE0E0E0E**，则会进入kworkerx的处理函数 `khook_inet_ioctl`。在该函数中，根据第三个参数的值来开启或关闭 kworkerx 提供的各种隐藏功能。

ARG.CMD	CAPABILITY
0	show all
1	hide all
2	hide proc
3	show proc
5	file tampering
7	hide file,dir
8	unhide_chdir
9	hide_chdir

Part3: 功能分析

Melofee通过init_module函数安装kworkerx内核驱动模块后，默认就开启了TCP连接的隐藏，再通过IOCTL发送相应的控制指令，开启进程，目录，持久化的隐藏。

我们在虚拟机中首次以无参数形式执行该样本，结果显示其成功隐藏了进程、样本文件、持久化脚本及网络连接。随后，使用 show 参数再次运行样本，进程、样本文件和持久化脚本重新显现，但网络连接依然保持隐藏状态。最终，通过 rmmod 命令卸载 kworkerx 模块后，隐藏的网络连接才得以恢复显示。

Melofee 在安装驱动模块后，会解密 C2 配置并建立通信，等待接收指令并执行。本次捕获的样本支持的功能与 ExaTrack 分析报告中的描述基本一致，但在功能号上存在差异。

CMD ID	CAPABILITY
0x11	uninstall
0x22	collect device info
0x33	launch new command thread
0x34	write file
0x35	read file
0x36	create new tcp connection
0x37	list directory
0x38	create directory
0x3a	delete directory
0x3b	create process to exec cmd
0x3c	exec command with output (including set new c2 ip)
0x3d	collect process info
0x3e	kill process
0x3f	launch shell
0x7b	ping back

总结

Melofee 提供的功能较为简洁，但具备极强的隐匿性。该家族的样本并不常见，攻击者可能将其使用范围限定在高价值目标上。网络管理员可以通过 `/tmp/lock_tmp1` 文件以及 `kworkerx` 等实体判断系统是否受到感染。如发现感染迹象，可按照前文描述删除相关驱动、进程、文件和持久化内容。

我们欢迎读者提供新的见解和情报。如您对我们的研究感兴趣，可通过X平台与我们联系。

IOC

MD5

```
603e38a59efcf6790f2b4593edb9faf5 *pskt
839f60efee25f07df7b23ba9d6bef892 *kworkerx
```

C2

```
filemanage.micrsofts-file[.]com:443
```

Downloader

```
http://45.92.156[.]166/klove/pskt
```

What do you think?

0 Responses

 Upvote

 Funny

 Love

 Surprised

 Angry

 Sad

0 Comments Login ▾

G Start the discussion...

LOG IN WITH OR SIGN UP WITH DISQUS

Name

♡ Share Best Newest Oldest