VSRC 安全周报（2021-08-24）

0x00 本周漏洞综述

本周需要关注漏洞共 4 个： Realtek SDK 8 月多个安全漏洞；SonicWall Analytics 远程代码执行漏洞（CVE-2021-20032）；ThroughTek Kalay P2P SDK 远程代码执行漏洞(CVE-2021-28372)；Cisco Small Business 路由器远程代码执行漏洞（CVE-2021-34730)。

本周安全态势共 1 个：Trend Micro：PrintNightmare 攻击检测与分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Realtek SDK 8 月多个安全漏洞

漏洞概述

2021 年 8 月 16 日，研究人员公开披露了台湾芯片设计商 Realtek 公司的 SDK 中的 4 个安全漏洞，未经身份验证的远程攻击者能够利用这些漏洞使设备崩溃（拒绝服务）、注入任意命令并以最高权限执行任意代码。这些漏洞至少影响了 65 个不同供应商生产的近 200 种产品，并且作为供应链漏洞，它们影响了供应链下游的数十万台设备。

漏洞详情

在物联网领域的许多嵌入式设备中都可以找到 Realtek 芯片组。研究人员表示，超过 65 家硬件制造商的产品采用了 Realtek RTL819xD 模块，该模块实现了无线接入点功能并包含其中一个易受攻击的 SDK。并且受影响的设备使用广泛，从住宅网关、旅行路由器、

Wi-Fi 中继器、IP 摄像机到智能闪电网关，甚至是联网玩具。

研究人员披露的 4 个漏洞如下，其中前 2 个漏洞的 CVSS 评分为 8.1（高危），后 2 个漏洞的 CVSS 评分为 9.8（严重）。但要利用这些漏洞，攻击者需与设备在同一网络，或者能够通过互联网访问设备。

- CVE-2021-35392：通过 UPnP 的 Wi-Fi 简单配置堆栈缓冲区溢出
- CVE-2021-35393：通过 SSDP 的 Wi-Fi 简单配置堆缓冲区溢出
- CVE-2021-35394：MP Daemon 诊断工具命令注入
- CVE-2021-35395：管理 Web 界面多个漏洞

影响范围

Realtek SDK v2.x

Realtek “Jungle” SDK v3.0/v3.1/v3.2/v3.4.x/v3.4T/v3.4T-CT

Realtek “Luna” SDK 最高版本 1.3.2

安全建议

目前这些漏洞已经在部分版本中修复。建议参考以下版本及时升级更新:

Realtek SDK branch 2.x：Realtek 不再支持。

Realtek "Jungle" SDK：Realtek 正在开发补丁，需向后移植

Realtek "Luna" SDK：升级到 1.3.2a

下载链接：

https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en

已知的受影响制造商及产品链接如下：（涉及 D-Link、华为、联通、合勤等）

https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/

参考链接：

https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/

https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf

https://www.theregister.com/2021/08/16/realtek_wifi_sdk_vulnerabilities/

2. SonicWall Analytics 远程代码执行漏洞（CVE-2021-20032）

漏洞概况

CVE ID	CVE-2021-20032	时 间	2021-08-10
类 型	RCE	等 级	严重
远程利用	是	影响范围	
攻击复杂度		可用性	
用户交互		所需权限	

PoC/EXP	未公开	在野利用	否

漏洞详情

SonicWALL Analyzer 是 SonicWALL 推出的应用流量分析解决方案之一，支持 SonicWALL 防火墙等产品。Analyzer 主要为 IT 管理人员提供实时和历史应用流量分析与安全事件报告，从而使其具备深入分析网络性能与安全的能力。

2021 年 8 月 17 日，SonicWALL 发布安全公告，修复了 SonicWall Analytics 中的一个远程代码执行漏洞（CVE-2021-20032），其 CVSSv3 评分为 9.8。

由于 SonicWall Analytics On-Prem (本地) 的某些版本中 Java Debug Wire Protocol（JWDP）接口安全配置错误，未经身份验证的远程攻击者可以利用此漏洞在系统上执行任意代码。

影响范围

Analytics On-Prem <= 2.5.2518

安全建议

目前此漏洞已经修复。建议受影响用户及时升级更新到 Analytics On-Prem 2.5.2519 或更高版本。

临时缓解措施

阻止对受影响版本上的 9000/TCP 端口的访问。

注：SonicWall Analytics 2.5 及更早版本的部署是本地部署，应位于内部安全网络分段中。

下载链接：

https://mysonicwall.com/

参考链接：

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0018

https://www.sonicwall.com/support/product-notification/?sol_id=210809113238240

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20032

3. ThroughTek Kalay P2P SDK 远程代码执行漏洞（CVE-2021-28372）

漏洞概况

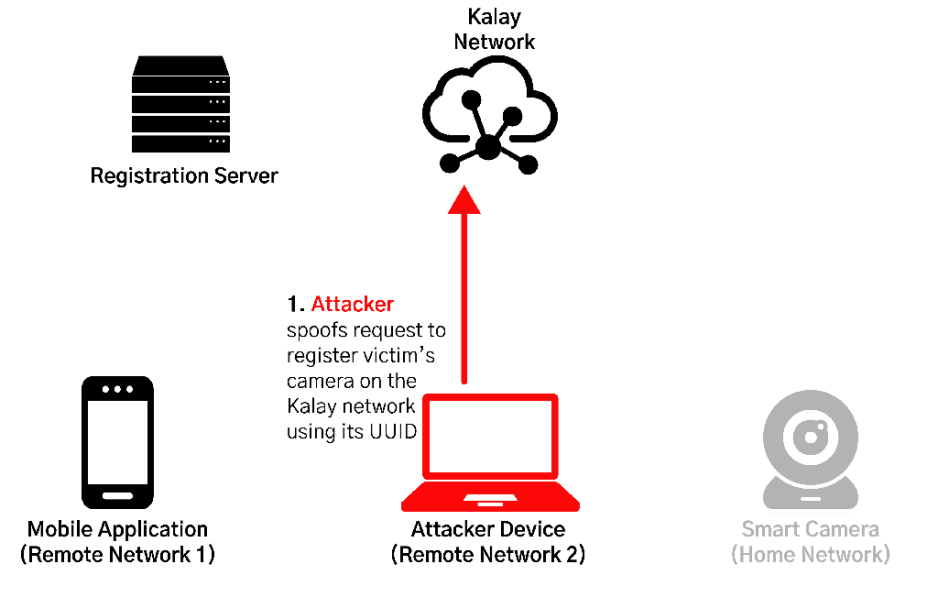
CVE ID	CVE-2021-28372	时 间	2021-08-18
类 型	RCE	等 级	严重
远程利用	是	影响范围	
攻击复杂度	低	可用性	高
用户交互	是	所需权限	无
PoC/EXP	已公开	在野利用	

漏洞详情

2021 年 8 月 17 日，Mandiant(FireEye)与美国网络安全和基础设施安全局(CISA) 合作披露了一个严重的物联网安全漏洞(CVE-2021-28372, CVSSv3 评分为 9.6) 。该漏洞为 ThroughTek Kalay P2P SDK 中的远程代码执行漏洞,影响了数百万使用 ThroughTek Kalay IoT 云平台连接的物联网设备。

该漏洞由 Mandiant 红队的研究人员于 2020 年末发现，远程攻击者可以利用此漏洞入侵物联网设备。ThroughTek 表示,其平台上有超过 8300 万个活跃设备和超过 11 亿的月连接,其客户包括物联网摄像头制造商、智能婴儿监视器和数字视频录像机（DVR）产品。

成功利用此漏洞的远程攻击者能够收听实时音频、观看实时视频数据、破坏设备凭据、远程控制受影响设备并执行其它操作。攻击所需的唯一信息是目标用户的 Kalay 唯一标识符 (UID) ,该标识符可以通过社会工程获得。此外,攻击者还可以使用 RPC (远程过程调用) 功能来完全接管设备。



Kalay 协议是以软件开发工具包（SDK）的形式实现的，它被内置于客户端软件（如移动或桌面应用程序）和联网的物联网设备，如智能相机中。由于 Kalay 协议是由原始设备制

造商（OEM）和经销商在设备到达消费者之前集成的，因此暂时无法确定受此漏洞影响的产品和公司的完整名单。

影响范围

以下版本的 Kalay P2P SDK 受此漏洞影响：

- 3.1.5 及更早版本
- 带有 nossl 标签的 SDK 版本
- 不使用 AuthKey 进行 IOTC 连接的设备固件
- 使用 AVAPI 模块而不启用 DTLS 机制的设备固件
- 使用 P2PTunnel 或 RDT 模块的设备固件

安全建议

目前 ThroughTek 已发布了 SDK 更新,建议参考以下方式及时修复或升级:

- 如果使用 ThroughTek SDK v3.1.10 及以上版本，请开启 AuthKey 和 DTLS；
- 如果使用 v3.1.10 之前的旧版本 ThroughTek SDK，请将库升级到 v3.3.1.0 或 v3.4.2.0，并启用 AuthKey 和 DTLS。

通用安全建议

- 尽量减少所有控制系统设备或系统的网络暴露情况，并确保它们不能从互联网访问。
- 将控制系统网络和远程设备置于防火墙之后，并将其与商业网络隔离。
- 当需要远程访问时使用安全的方法，如虚拟专用网络（VPN），并确保 VPN 是最新版本。

下载链接：

https://www.throughtek.com/please-update-the-sdk-version-to-minimize-the-risk-of-sensitive-information-being-accessed-by-unauthorized-third-party/

参考链接：

https://www.fireeye.com/blog/threat-research/2021/08/mandiant-discloses-critical-vulnerability-affecting-iot-devices.html

https://us-cert.cisa.gov/ics/advisories/icsa-21-229-01

https://securityaffairs.co/wordpress/121226/hacking/kalay-cloud-platform-critical-flaw.html?

4. Cisco Small Business 路由器远程代码执行漏洞（CVE-2021-34730）

漏洞概况

CVE ID	CVE-2021-34730	时 间	2021-08-18
类 型	RCE	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

2021 年 8 月 18 日，Cisoc 发布安全公告，修复了 Cisco Small Business RV 系列路由中的远程代码执行漏洞（CVE-2021-34730），其 CVSSv3 评分为 9.8（严重）。

由于对传入的 UPnP (通用即插即用) 流量验证不当，Cisco Small Business RV110W、RV130、RV130W 及 RV215W 路由器的 UPnP 服务存在安全漏洞，攻击者可以通过向受影响的设备发送恶意的 UPnP 请求来利用此漏洞。成功利用此漏洞的攻击者能够以 root 用户身份在系统上执行任意代码或导致设备重新加载，从而造成拒绝服务。

影响范围

如果配置了 UPnP，此漏洞会影响以下 Cisco Small Business RV 系列路由器：

- RV110W Wireless-N VPN Firewalls
- RV130 VPN Routers
- RV130W Wireless-N Multifunction VPN Routers
- RV215W Wireless-N VPN Routers

注：UPnP 服务在 LAN 接口上默认启用，在 WAN 接口上默认禁用。如果在 LAN 和 WAN 接口上都禁用了 UPnP，则该设备不易受到攻击。

安全建议

由于 Cisco Small Business RV110W、RV130、RV130W 和 RV215W 已经不再提供技术支持，Cisco 尚未发布软件更新来修复此漏洞。

缓解措施

可以通过禁用受影响的功能缓解此漏洞。要在设备的 LAN 接口上禁用 UPnP 或查看 UPnP 是否启用，请执行以下操作：

1.打开 web 管理界面，选择"基本设置 > UPnP"。

2.选中禁用复选框（如果未选中禁用复选框，则设备上已经启用了 UPnP）。

下载链接：

https://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/eos-eol-notice-c51-742771.pdf

参考链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5?

https://software.cisco.com/download/home

https://nvd.nist.gov/vuln/detail/CVE-2021-34730

0x02 本周安全态势

1. Trend Micro：PrintNightmare 攻击检测与分析

概述

PrintNightmare 漏洞是最新的 Windows 打印后台处理程序漏洞集，包括 CVE-2021-1675、CVE-2021-34527、CVE-2021-34481 和 CVE-2021-36958。该漏洞是 Print Spooler 服务中的代码执行漏洞（远程和本地），会影响运行该服务的所有 Windows 版本。

许多研究人员已经提出了基于不同的实现方式（通过 TCP 和服务器信息块或 SMB）的多种漏洞利用变体。通过使用不同的函数调用打印系统异步远程协议（MS-PAR），滥用 RpcAsyncAddPrinterDriver，可以在服务器和工作站上利用 PrintNightmare，而滥用打印系统远程协议（MS-RPRN）则可以滥用 RpcAddPrinterDriverEx 实现 impacket。

在本文中，我们分享了 PrintNightmare 的实现以及如何使用趋势科技 Vision One™和 Cloud One™等产品检测该漏洞，以减轻在系统（例如打印后台处理程序服务）中发现的关键漏洞带来的安全风险。通过网络和端点记录的漏洞利用尝试的指标和属性，能够使安全团队和分析人员能够更广泛地了解攻击企图，以便立即做出响应。

时间线

PrintNightmare 的时间线如下：

- 6 月 8 日：作为 6 月安全更新的一部分，修复了打印后台处理程序服务中的权限提升（EOP）漏洞，该漏洞被标记为 CVE-2021-1675。
- 6 月 21 日：同一错误后来被归类为远程代码执行（RCE）和 EOP 漏洞。
- 6 月 29 日：具有不同 RCE 和 EOP 概念验证的研究人员意外地公开了 PoC，因为他们误以为其发现的漏洞与 6 月安全更新中修复的漏洞相同。之后，研究人员删除了 PoC，但它们已经被复制并最终被搜索引擎缓存。
- 7 月 1 日：一个新的 0 day 漏洞公开披露，微软将其标记为 CVE-2021-34527。
- 7 月 6 日:微软发布了 CVE-2021-34527 的带外补丁,但它只阻止了一部分 RCE，具体来说，该补丁只阻止了 DLL 的路径实现，如"\\server\share\"。
- 7 月 7 日：研究人员报告了这一漏洞，同时报告了通用命名规则（UNC）表示路径的形式"\??\UNC\"，而不是使用"\\"，可以绕过该补丁。
- 7 月 15 日：微软披露，在 Print Spooler 服务中发现了一个新的 EOP 漏洞，并将其标记为 CVE-2021-34481。
- 8 月 10 日： Microsoft 更新了 CVE-2021-34481 并发布了补丁以防止漏洞利用。

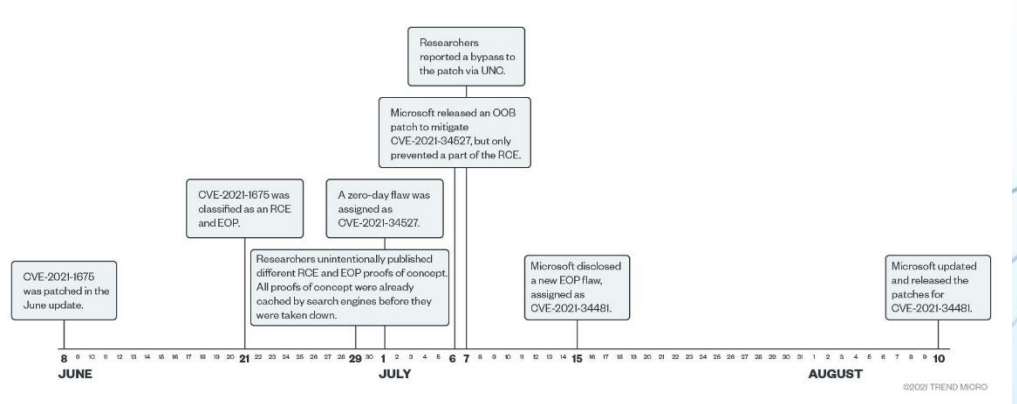


图 1. PrintNightmare 漏洞利用和补丁开发时间表

注：8 月，微软还披露了一系列 Windows 打印后台处理程序服务漏洞，如 CVE-2021-36936、CVE-2021-36947、CVE-2021-34483 和 CVE-2021-36958，其中 CVE-2021-34483 为权限提升漏洞，其它均为远程代码执行漏洞。

遵循已经公开的不同 PoC/EXP，我们在此详细介绍了我们对 PrintNightmare 的观察。在下文中，我们确定了用户环境中潜在危害的指标（IOC），以及通过趋势科技 Vision One 和 Cloud One 平台检测和保护针对此漏洞的攻击。

Print Spooler Service

Print Spooler 服务使客户和服务器能够执行与打印有关的任务。在打印服务器上，Spooler 共享向打印客户端公开的打印队列。在打印客户端上，Spooler 服务向应用程序公开打印 API，接收应用程序的打印输出，并将其发送到共享打印队列或打印服务器。

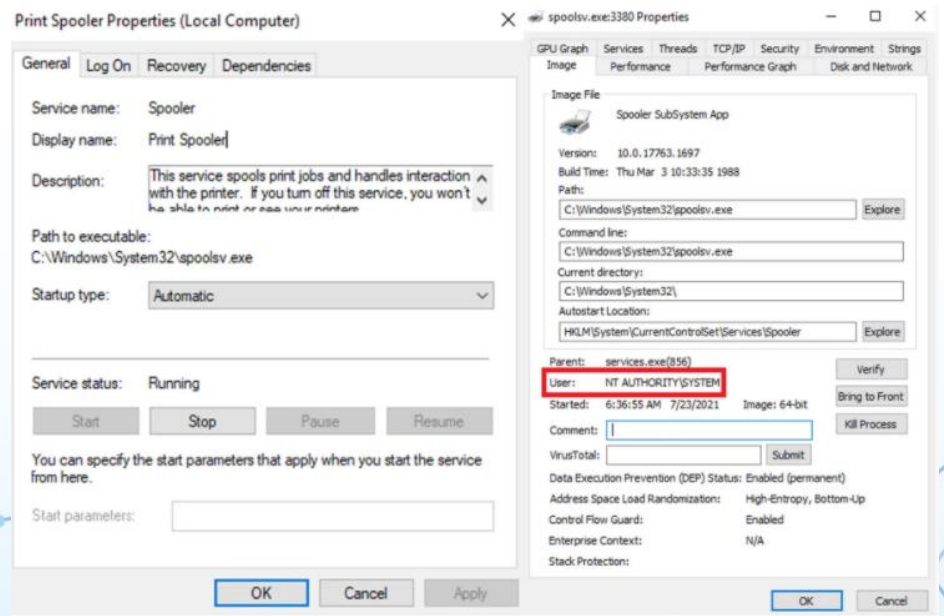


图 2. Print Spooler 服务

为了查看 Spooler 服务的细节，我们使用 Sysinternals 的 Process Explorer，其中的二进制文件（"spoolsv.exe"）以最高权限（即 SYSTEM 用户的权限）运行。该服务在过去曾出现过多个安全漏洞，它们与 Print Spooler 如何加载打印机驱动程序有关。成功利用这些漏洞将能够在系统上执行代码，由于该服务本身以最高权限运行，因此执行代码也使用最高权限。

目前，已经检测到威胁者积极利用这个漏洞的迹象。由于该攻击是基于网络的，它甚至可以被其他具有较低系统权限的用户执行，因为大多数机器（如域控制器和打印服务器）上默认情况下没有禁用 spooler 服务。利用此漏洞，攻击者可以在系统上执行代码，因此该漏洞将成为提升权限的首选技术。

例程

我们观察到的一些迹象表明存在潜在的漏洞利用。我们在本节中详细介绍了它们，以供今后的防御参考。

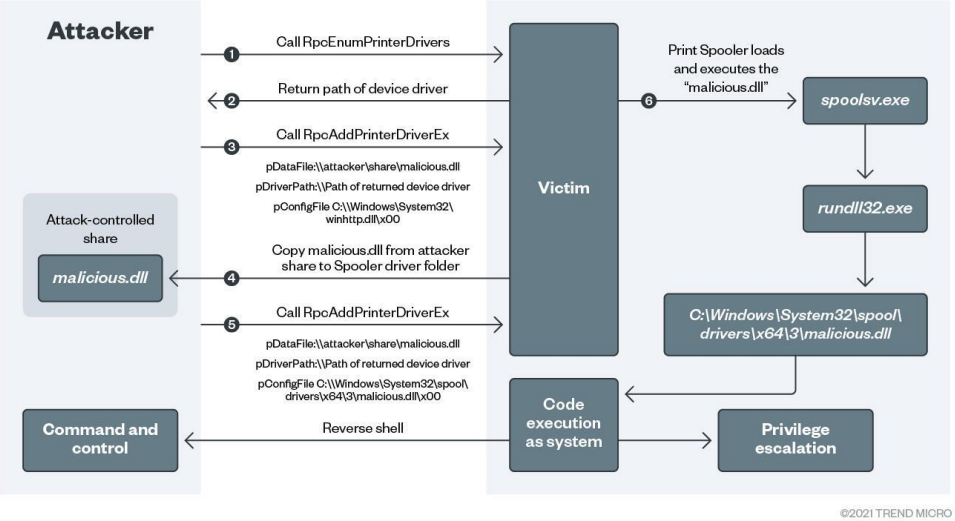


图 3. PrintNightmare 漏洞利用

对 Spooler 服务的利用可以细分为以下几点：

1. Print Spooler 服务中的漏洞被攻击者利用。

2.受害机器访问攻击者控制的 SMB 共享上的恶意 DLL 文件。

3.DLL 文件被写到磁盘上。

4. DLL 文件由 Print Spooler 服务加载和执行。

5.如果 DLL 文件格式错误，Print Spooler 服务将崩溃。

6.基于 DLL 代码，观察到命令和控制（C&C）或权限升级。

如果默认情况下未启用 Print Spooler 服务的事件日志记录，我们建议管理员或用户使用以下 PowerShell 命令启用它：

```
$logs = Get-LogProperties 'Microsoft-Windows-PrintService/Operational'
$logs.Enabled = $true
Set-LogProperties -LogDetails $logs
```

管理员还可以导航到“应用程序和服务”日志并启用管理和操作事件，以检测滥用的企图。

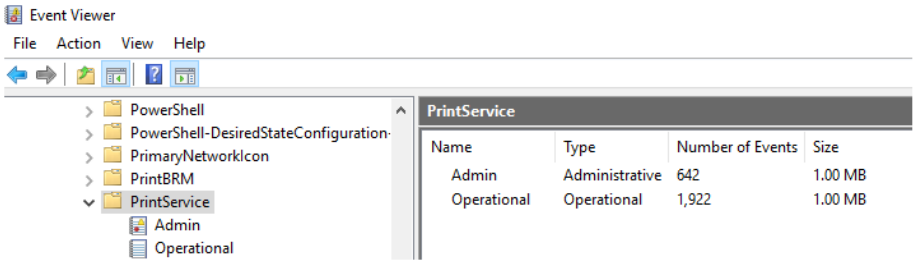


图 4. 浏览“应用程序和服务”日志

在利用 PrintNightmare 时，我们观察到易受攻击的系统上记录了以下活动。从攻击者控制的 SMB 共享中获取恶意 DLL 文件并写入目标系统的磁盘，当 DLL 文件被注入到一个进程的内存中（本例为 "spoolsv.exe"），然后在进程监视器上观察到 "Load Image"操作。一旦 DLL 文件被加载到进程中，恶意代码就会被执行。

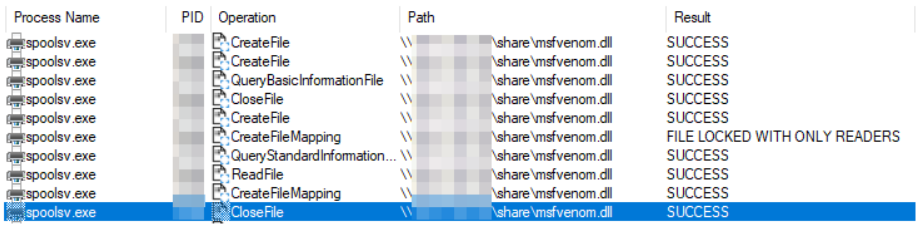


图 5. 从攻击者控制的 SMB 中获取恶意 DLL 文件

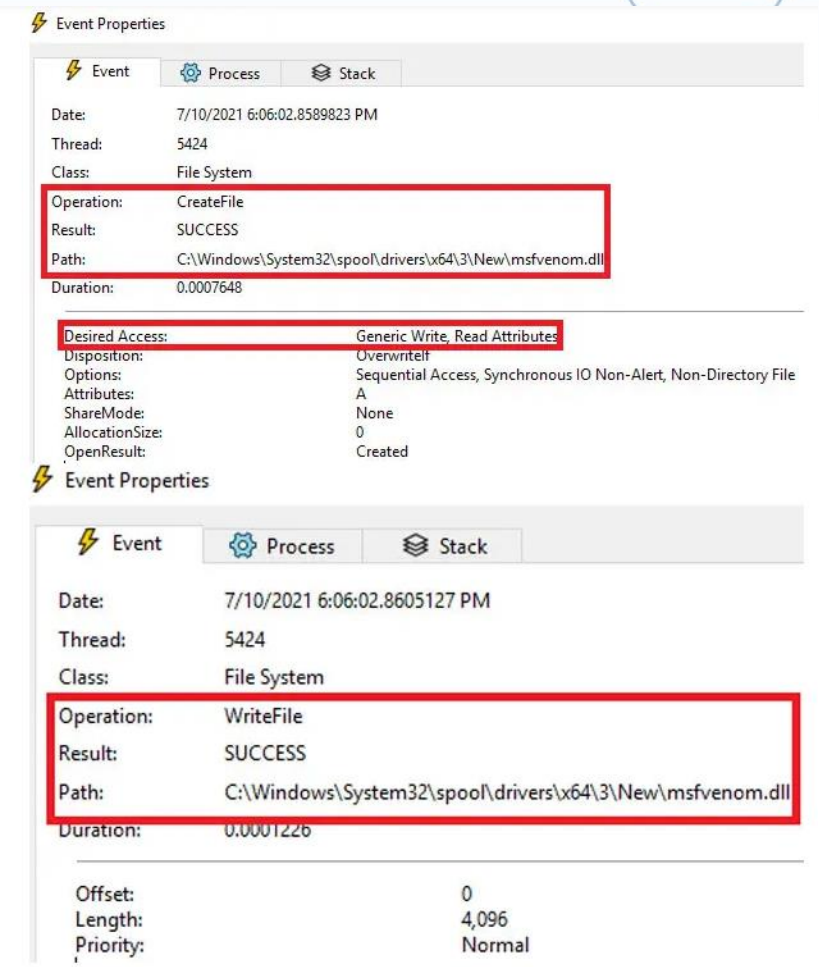


图 6. 在受害者主机上创建攻击者的 DLL

该攻击由两个阶段组成：

阶段 0

1.SMB 共享中的 DLL 路径对 "RpcAddPrinterDriver "进行了一次调用，数值为"pDataFile"。

2.在路径"%windir%\System32\spool\drivers\x64\3\"中寻找 DLL。

3.在"%windir%\System32\spool\drivers\x64\3\New\name_of_dll>.dll "处打开一个新的文件句柄。

4. 一旦 "WriteFile " 操作完成，路径被重命名为

"%windir%System32\spool\drivers/x64\3<name_of_dll>.dll"。

5.DLL 最终驻留在上述重命名的路径中。

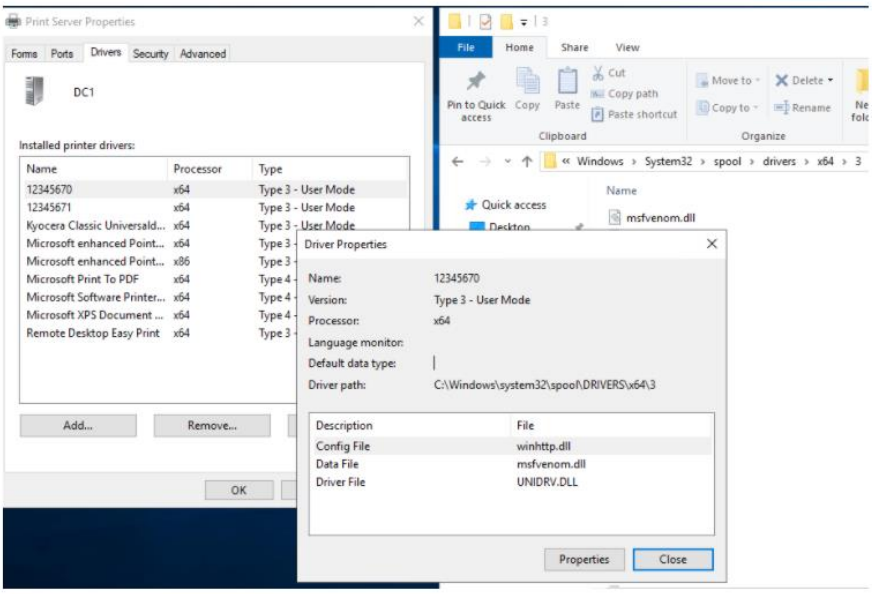


图 7. 在阶段 0 中，一旦"WriteFile"操作完成，DLL 就驻留在重命名的路径中

阶段 1

1.完成阶段 0 后，DLL 已经驻留在"%windir%\System32\spool\drivers\x64\3"路径中。

2.为了在 Print Spooler 服务中加载 DLL，要进行 "RpcAddPrinterDriver "调用，指定 "pConfigFile "为上传的 DLL 的本地路径。

3.当 DLL 在进程"spoolsv.exe "中被加载时，观察到 "Load Image "操作。

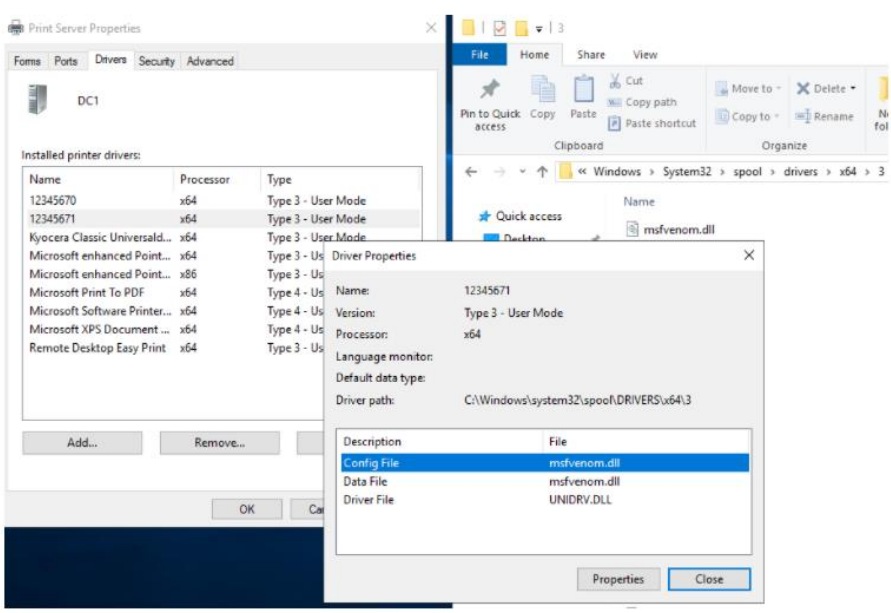
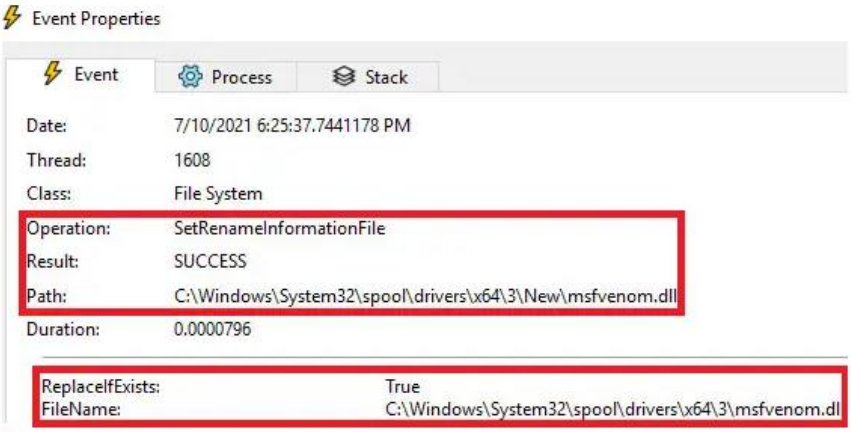


图 8. 在 Print Spooler 服务中加载 DLL



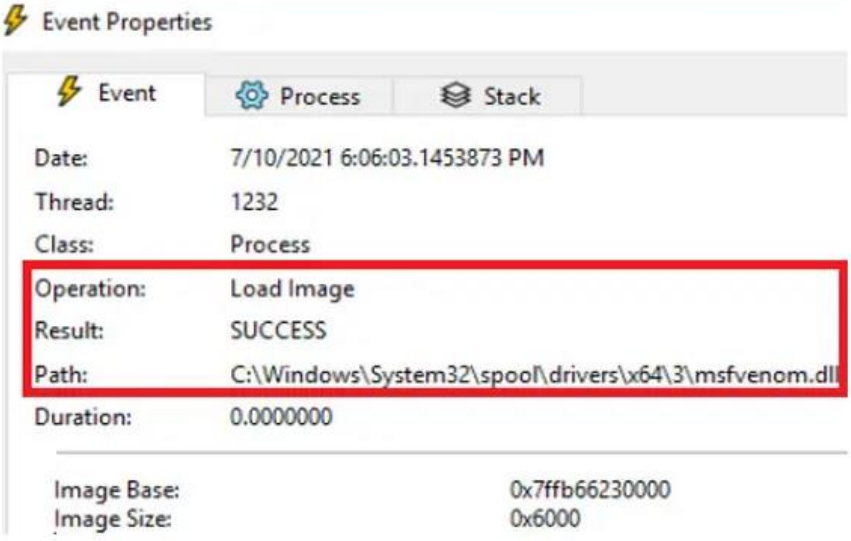


图 9. 在阶段 1，观察到的 DLL 被加载到进程“spoolsv.exe”中。

使用 Process Explorer,我们可以看到进程的脉络，识别进程生成的顺序。当 "spoolsv.exe "加载恶意的 DLL 时，rundll32 会执行该 DLL。根据 DLL 的代码（在这种情况下，它将给攻击者提供一个反向 shell），“cmd.exe”是从“rundll32.exe”派生出来的，而“rundll32.exe”又是从“spoolsv.exe”派生出来的。根据进程脉络，分析师和 IT 团队可以了解特定活动的来源。这也有助于缩小威胁搜寻的范围。

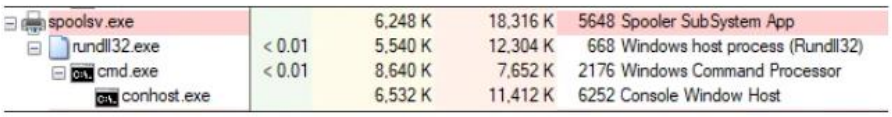


图 10. 可视化 "spoolsv.exe "的层次结构

当试图在 Print Spooler 服务中加载 DLL 时，在打印机服务的事件日志中观察到以下事件 ID。

1.当 DLL 格式错误时，从事件源 "Microsoft-Windows-PrintService/Operational " 观察到事件 ID 808。这里我们看到详细信息中的 DLL 的路径，说明 Print Spooler 加载恶意 DLL 失败。这个事件 ID 是一个高可信度的指标，表明可能存在 PrintNightmare 漏洞的利用（阶段 1）。

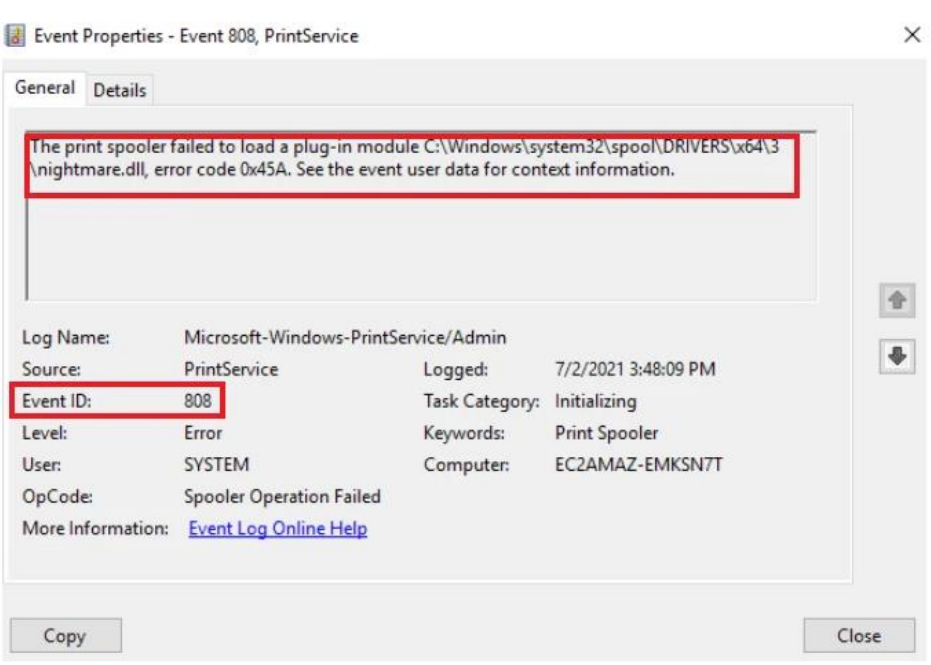


图 11. 事件 ID 808

2.当在 Print Spooler 中添加或更新一个新的打印机驱动程序时，会观察到事件 ID 316。我们可以在细节中看到 DLL 文件的名称，并且会记录成功和不成功的利用尝试（阶段 0）的事件。

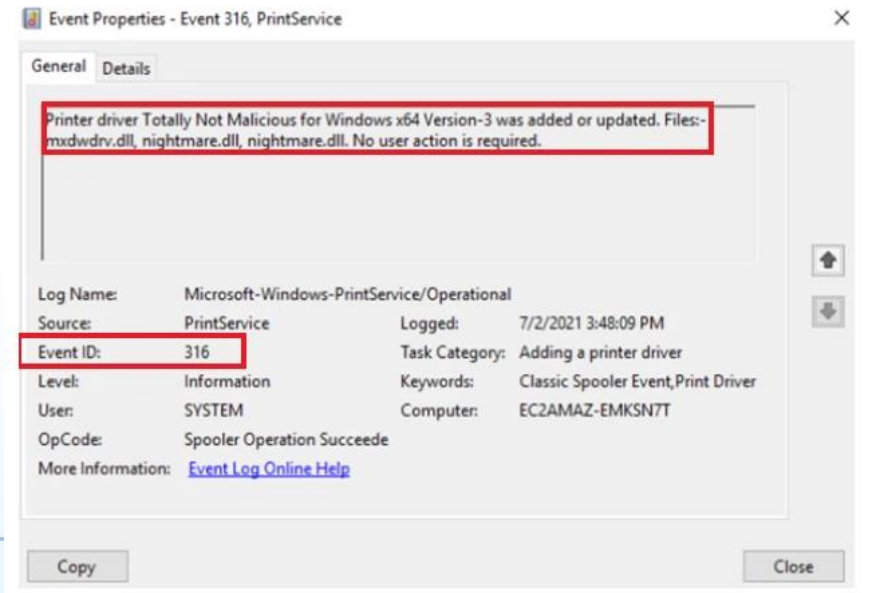


图 12. 事件 ID 316

Trend Micro 产品检测

Trend Micro Cloud One-Workload Security

进入趋势科技 Cloud One 控制台，启用以下模块：

1.打开实时扫描的反恶意软件模块

2.日志检查模块。规则 1011017 -- Microsoft Windows - Print Spooler Failed Loading Plugin Module (PrintNightmare)

3.处于 "预防模式 "的入侵预防系统（IPS）模块

a.规则 1011016 -- 通过 TCP 协议识别的 DCERPC AddPrinterDriverEx 调用

b.规则 1011018 –通过 SMB 协议识别的 DCERPC AddPrinterDriverEx 调用

4.活动监测

这些模块能够深入了解工作负载，并检测我们在上文观察到的事件。我们在 Vision One 中全面利用这些检测结果。

Cloud One-检测

当 Print Spooler 服务加载格式错误的 DLL 时，会触发日志审查规则“1011017 - Microsoft Windows - Print Spooler Failed Loading Plugin Module (PrintNightmare)”。事件源被视为“Microsoft-Windows-PrintService/Admin”，事件 ID 为 808。

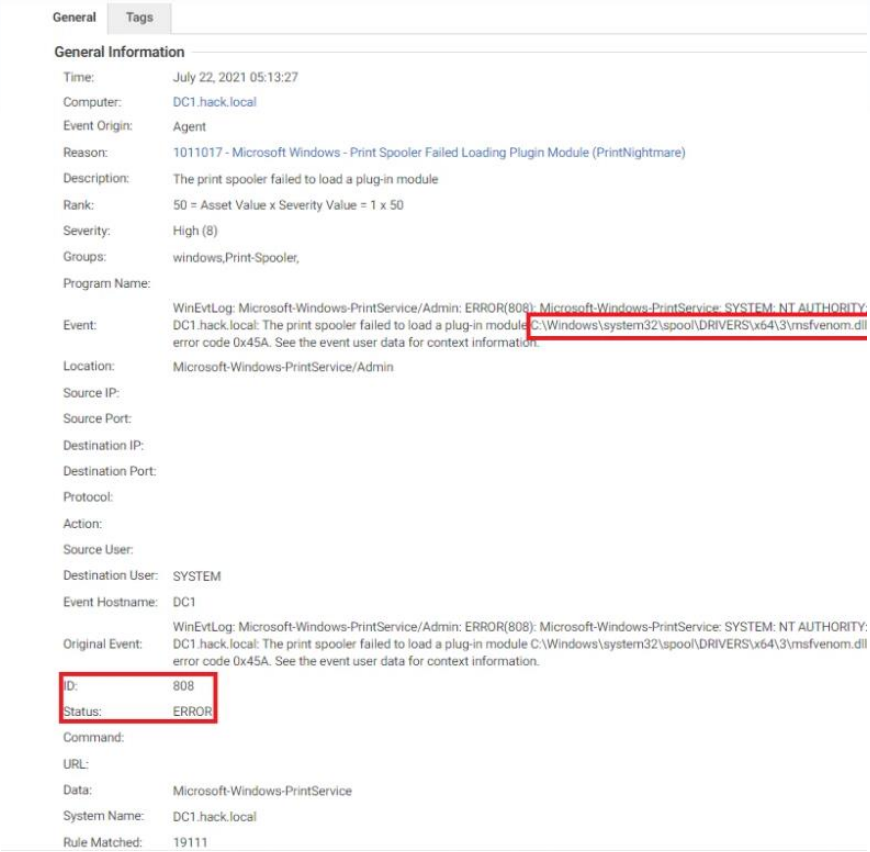


图 13. 格式错误的 DLL 触发日志审查规则。

当攻击者和受害者之间约定的通信协议是 SMBv1 或 SMBv2 而没有加密时，PrintNightmare 的 MS-RPRN 和 MS-PAR 实现会触发 IPS 事件日志。

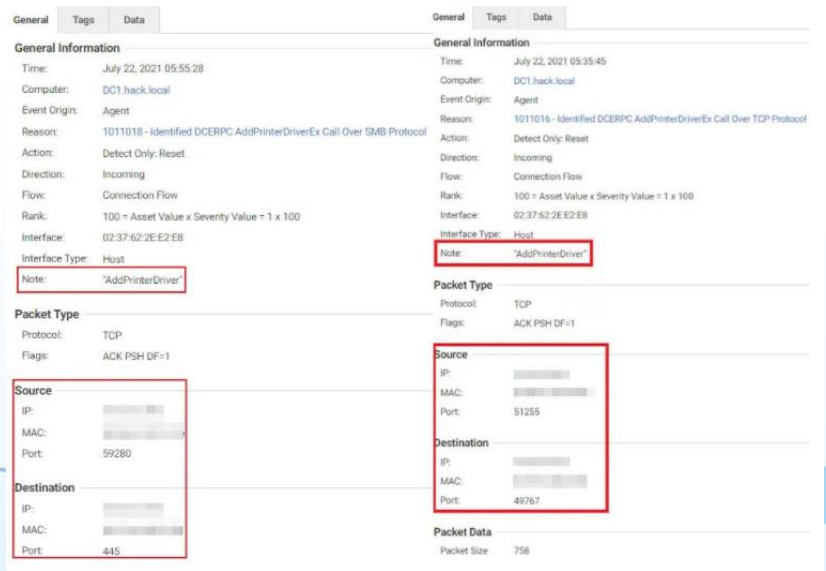


图 14. PrintNightmare 实现触发 Cloud One IPS 事件。

此外，当在磁盘上创建的 DLL 中观察到有已知的恶意签名时，反恶意软件模块会被触发。先进的文件信誉服务与趋势科技™智能保护网络™（SPN）一起，能够实时监测机器上创建的新文件，并根据 SPN 维护的模式标记出恶意文件。

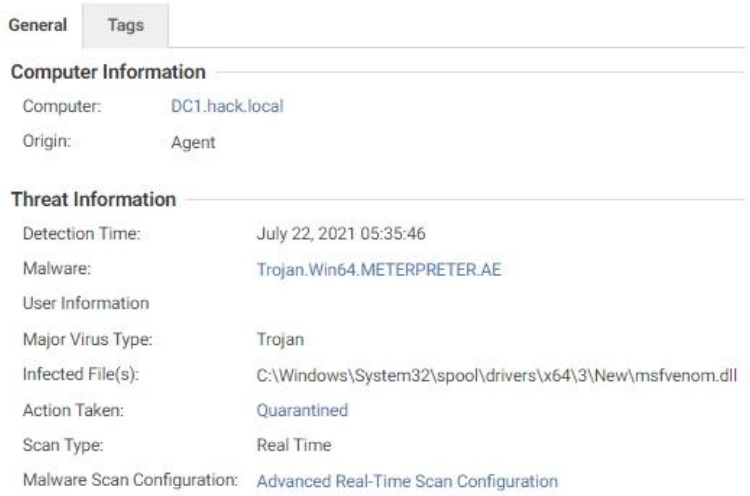


图 15. 恶意签名触发反恶意软件模块以阻止它们。

Trend Micro Vision One™ Workbench App

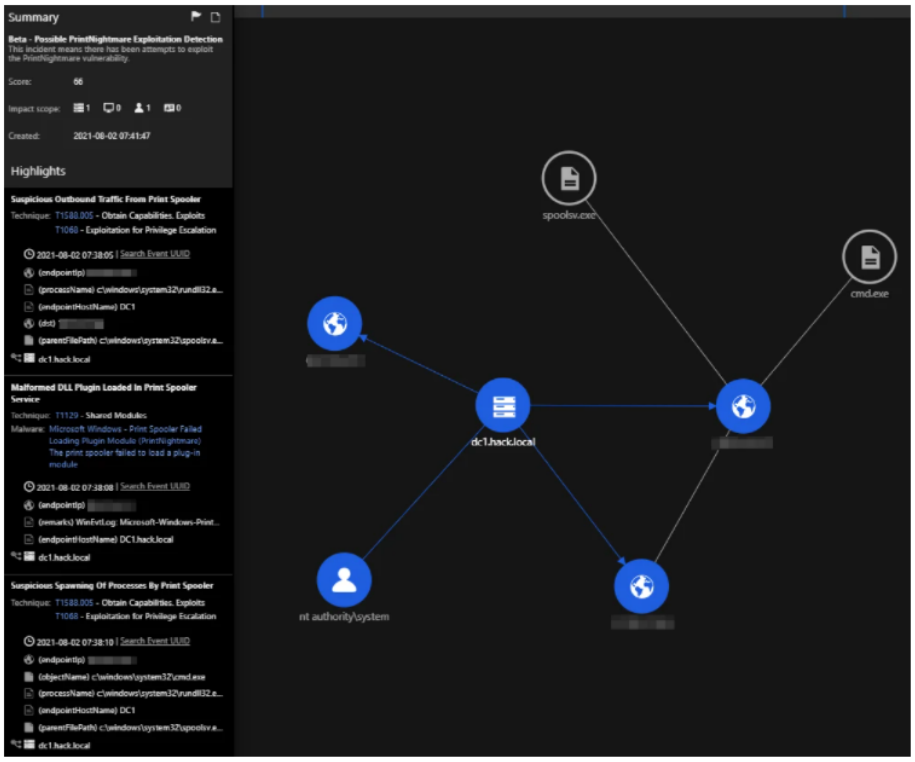


图 16. 检测和跟踪在 Trend Micro Vision One Workbench 上发现的可疑出站流量

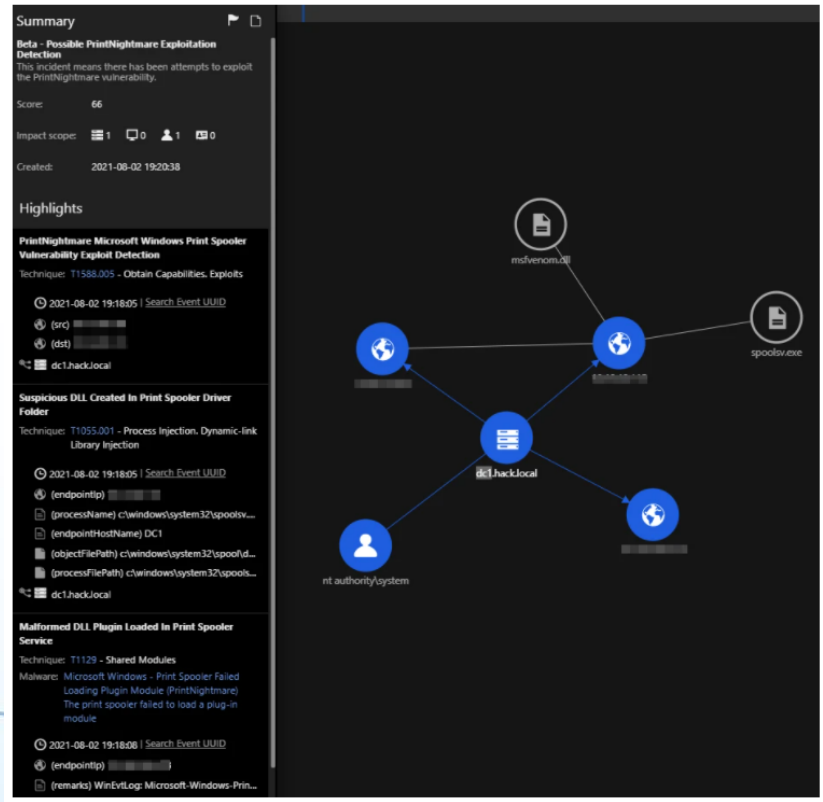


图 17. 使用 Trend Micro Vision One Workbench 映射系统中的 PrintNightmare 漏洞

查看 Vision One Workbench 的根源分析（RCA），我们看到进程的脉络，其中"msfvenom.dll "是由 Print Spooler 服务("spoolsv.exe")创建，随后生成了 "rundll32.exe"，它执行了恶意的 DLL。

执行后，有一个从 Print Spooler 服务的子进程到攻击者机器的回调，该机器有一个在端口 4444 上侦听的 meterpreter 处理程序。在获得 meterpreter 回调后，我们投放一个命令提示符（"cmd.exe"）shell 并运行"whoami"。

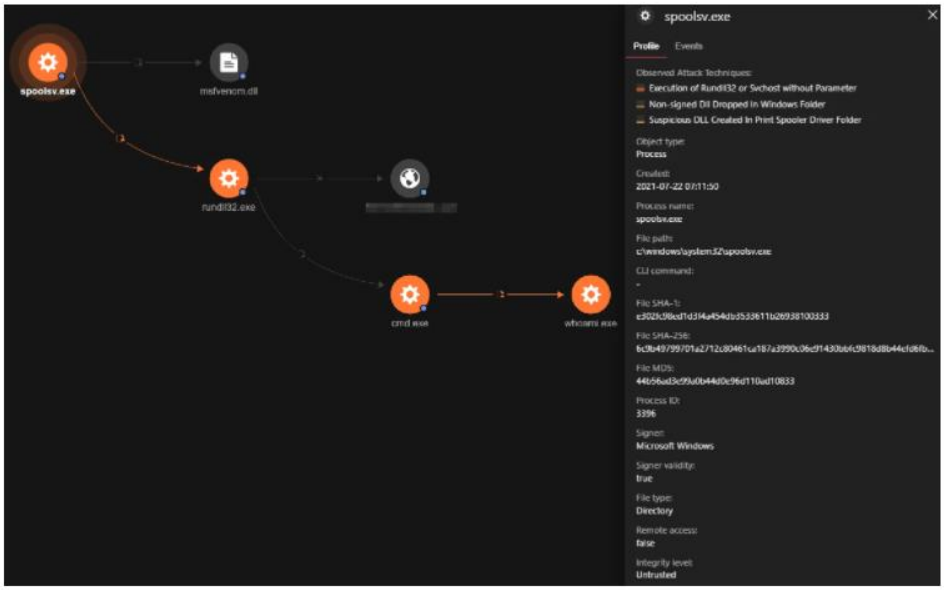


图 18. 趋势科技 Vision One 工作台的进程脉络

RCA 中显示的每个对象都有与之关联的特定属性。例如，对象 "msfvenom.dll "与下列观察到的攻击技术（OAT）相关联。如图 18 的右上角所示，"在打印后台处理程序驱动程序文件夹中创建的可疑 DLL "和 "在 Windows 文件夹中丢弃的未签名 DLL"，如上图所示。

我们还突出显示了 DLL 的哈希值，之后可用于查找组织内可能出现的事件。其它字段，如“First Seen”、“Last Seen”和空的“Signer”字段，可以更深入地了解 DLL 的元数据。

图 19. 在 Workbench 上看到的哈希和字段信息可用于检查公司内其它系统中的类似事件。

RCA 显示了从 Print Spooler 服务中的可执行程序 "rundll32.exe "观察到的活动。从日志中，我们可以了解到以下内容：

1.可执行程序 "rundll32.exe "来自 "spoolsv.exe"。

2.此事件之后是一个源自 "rundll32.exe "的出站连接。

3.在观察到出站活动的 4 秒钟后，“rundll32.exe”派生出了“cmd.exe”。

4.在观察到 "cmd.exe "两秒后，攻击者运行了 "whoami"。

图 20. 从可执行文件“rundll32.exe”跟踪记录的活动

Trend Micro Vision One™-Hunting Queries

为了从 PrintNightmare 环境中寻找潜在的 IOC，以下趋势科技 Vision One 的搜索查询很有用：

1.在"%windir%\System32\spool\drivers\x64\3\New "下面的文件夹中创建 DLL 文件

```
eventSubId:101 AND (objectFilePath:\\windows\system32\spool\drivers\x64\3\New AND objectFilePath:*.dll) AND NOT (objectFilePath:winhttp.dll OR objectFilePath:unidrv.dll)
```

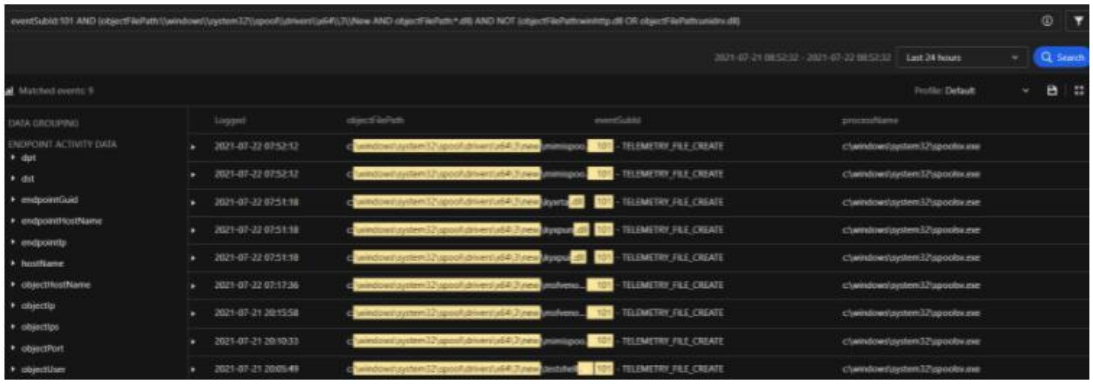


图 21. 使用 Trend Micro Vision One 搜索查询创建的 DLL 文件

2.从 Print Spooler 服务中产生的可疑进程

```
eventSubId:2 AND (parentFilePath:spoolsv.exe AND processFilePath:rundll32.exe)
```

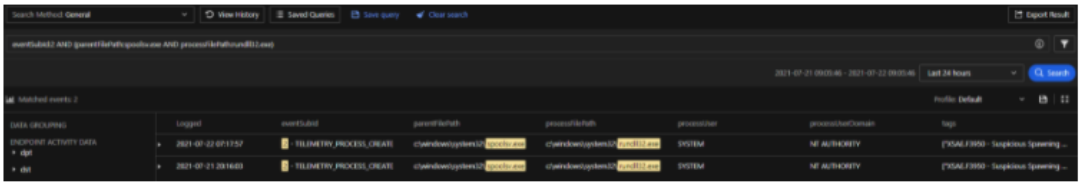


图 22. 寻找来自 spooler 服务的可疑进程

3.源自 Print Spooler service 的子进程的出站连接

```
eventSubId:204 AND parentFilePath:spoolsv.exe AND (processFilePath:(*cmd.exe* OR *powershell.exe* OR *rundll32.exe*))
```

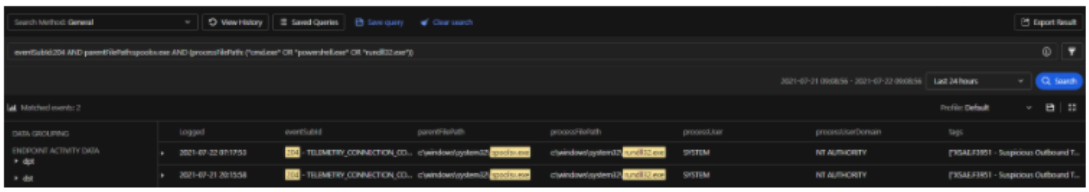


图 23. 寻找来自外部和未知系统的连接

4.从文件路径'\\Windows\\System32\\spool\\drivers\\x64\\3\\'检测恶意软件

事件名称：“MALWARE_DETECTION”

文件路径：\\Windows\\System32\\spool\\drivers\\x64\\3

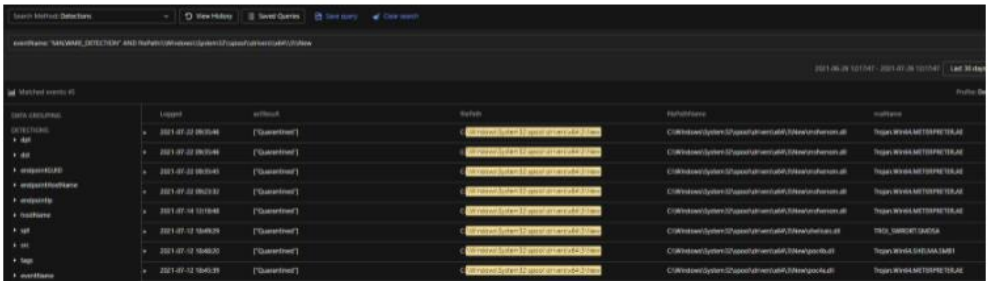


图 24. 从 Print Spooler 服务驱动程序中查找恶意软件

5.查找 Print Spooler 服务中加载的格式错误的 DLL

事件名称: "LOG_INSPECTION_EVENT"

规则名称:*PrintNightmare*.

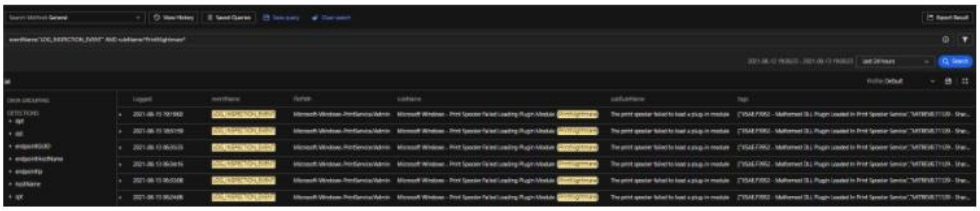


图 25. 在 Print Spooler 服务中查找格式错误的 DLL

结论

PrintNightmare 漏洞最初公开披露的原因是安全研究人员与研究之间的混乱，从不连贯的披露到绕过官方补丁，其 PoC 已被纳入各种框架中，如 Metasploit 框架（MSF）和 Mimikatz 等工具。此外，利用 PrintNightmare 漏洞很快会成为攻击者进行权限升级和横向移动的首选方法，因为该攻击可以实现 RCE 和本地权限提升，所需权限低，且不需要用户互动。目前，PrintNightmare 已被多个威胁者积极利用，如勒索软件 Vice Society、Conti（疑似）和 Magniber。

由于 Print Spooler 服务在大多数 Windows 版本上默认启用，并且在大多数企业环境中保持开放状态，因此更容易被恶意行为者利用。如果 Active Directory (AD) 环境中存在易受攻击的端点，则攻击者可以在运行 Print Spooler 服务的任何系统（包括域控制器和打印服务器）上获得最高权限。

通过对此类攻击的分析，以及如 Trend Micro Vision One 和 Cloud One 之类的安全产品，安全人员能够及时检测并阻止这种威胁，以最大程度保护用户的资产。

通用安全建议

- 及时应用补丁，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。
- 加强系统和网络的访问控制，修改防火墙策略，关闭非必要的应用端口或服务，减少将危险服务（如 SSH、RDP 等）暴露到公网，以减少攻击面。
- 预防 0day 漏洞和恶意软件，安全产品实时更新最新规则或相关防护指标。
- 加强系统用户和权限管理，启用多因素认证机制和最小权限原则，用户和软件权限应保持在最低限度。

- 启用强密码策略并设置为定期修改。
- 定期备份数据，确保在需要时可以在紧急情况下快速访问它。
- 使用最新、全面的威胁情报信息，监控网络和安全事件，以快速响应攻击。
- 将防御策略集中在检测横向移动和数据渗出到互联网上，要特别注意传出的流量，以检测网络犯罪的连接。
- 对员工进行安全培训。

原文链接：

https://www.trendmicro.com/en_us/research/21/h/detecting-printnightmare-exploit-attempts-with-trend-micro-vision-one-and-cloud-one.html