VSRC 安全周报（2021-04-06）

0x00 本周漏洞综述

本周需要关注漏洞共 5 个：Npm Netmask SSRF 绕过漏洞（CVE-2021-28918）；Apache Druid 远程代码执行漏洞（CVE-2021-26919）；VMware vRealize SSRF 漏洞（CVE-2021-21975）；GitLab 4 月任意文件读取漏洞；VMware Carbon Black Cloud Workload 身份验证绕过漏洞（CVE-2021-21982）。

本周安全态势共 4 个：PHP 官方 Git 存储库被黑，代码库被篡改；Purple Fox 攻击活动分析；30 个 Docker 镜像在加密劫持攻击中被下载了 2000 万次；趋势科技：Conti 勒索软件分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Npm Netmask SSRF 绕过漏洞（CVE-2021-28918）

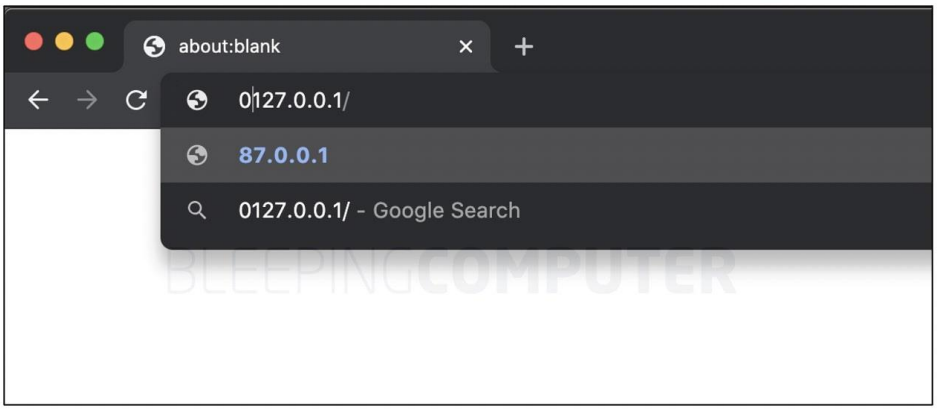
Netmask 是 npm 库中的一个软件包，它被成千上万的应用程序用来解析或比较 IPv4 地址和 CIDR 块。该软件包的每周下载量超过 300 万次，截至目前，netmask 已经累计有超过 2.38 亿的总下载量。此外，大约有 278,000 个 GitHub 存储库依赖 netmask。

2021 年 03 月 28 日，netmask 被披露存在一个可导致 SSRF 或 RFI 的安全漏洞（CVE-2021-28918）。在解析 IP 地址时带有前导零的情况下，由于未正确进行验证，网络掩码将会解析为不同的 IP。该漏洞将导致成千上万的项目容易受到 SSRF 绕过的攻击，目前该漏洞的 PoC 已在 GitHub 上公开。

IP 地址可以用多种格式表示，包括十六进制和整数，但最常见的 IPv4 地址以十进制格式表示。比如，IPv4 地址以十进制格式表示为 104.20.59.209，但是八进制格式表示为 0150.0024.0073.0321。

在 Chrome 浏览器的地址栏中输入 0127.0.0.1/，浏览器会将其视为八进制格式的 IP。实际上，当按下 Enter 或 Return 键后，IP 会更改为十进制等效值 87.0.0.1。这是因为大多数网络浏览器（如 Chrome），会自动补偿混合格式的 IP。这就是大多数应用程序处理此类

模棱两可的 IP 地址的方式。

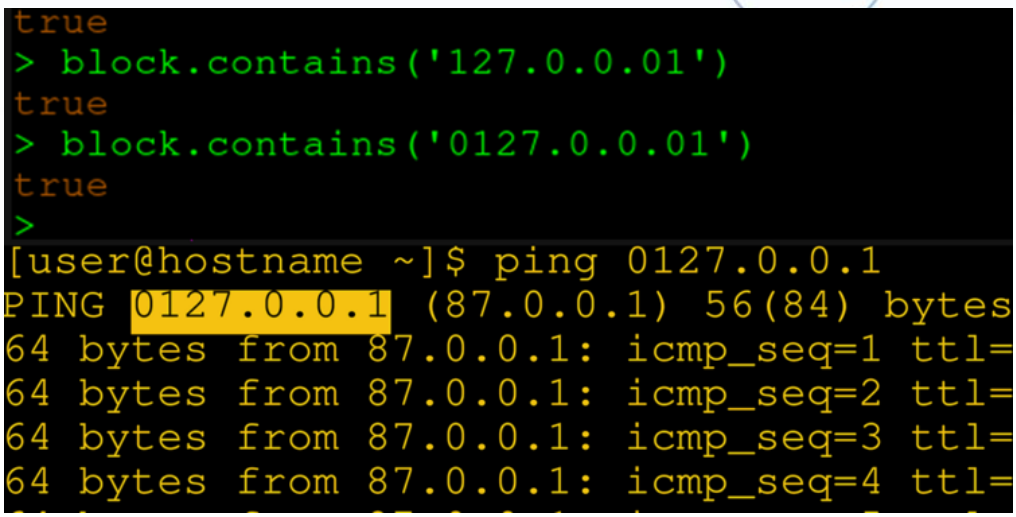


需要注意的是，127.0.0.1 并非公共 IP 地址，而是一个环回地址，但是，通过模棱两可的表示将其更改为公共 IP 地址，从而导致解析为另一台主机。

但是，对于 npm netmask，任何前导零都会被简单地剥离和丢弃。根据 IETF 的原始规范，IPv4 地址的部分如果前缀为 0，可以被解析为八进制。但是 netmask 忽略了这一点，它始终将 IP 视为十进制，这意味着在您尝试验证 IP 属于某个范围时，使用基于八进制的 IPv4 地址表示将是错误的。

如果攻击者能够影响应用程序解析的 IP 地址，则该问题可能会导致各种漏洞，从服务器端请求伪造（SSRF）绕过到远程文件包含（RFI）。

攻击者在运行节点服务器来清理入站请求或查询参数，该请求或查询参数可能是用于进一步连接的 URI，或使用较早的 0 前缀 JavaScript 表示形式，以基于八进制的部分或全部八位字节来制作 IP。这可能导致 SSRF，例如，通过传递 0177.0.0.01 来强制服务器连接到 127.0.0.1（177 是十进制 127 的八进制数）。一个很好的例子是，一个暴露 webhooks 并通过 netmask 检查验证用户 URL 的系统容易受到 SSRF 攻击。



而这个 bug 也可以被利用来进行远程文件包含（RFI），如果攻击者制作一个对 netmask 来说看起来是私有的 IP 地址，因为 netmask 将所有 IPv4 部分（八位数）转换为十进制格式的方式，被其它组件评估为公共格式。

各种网络基础架构和安全产品（例如 Web 应用防火墙）都依赖于网络掩码来过滤出阻止列表和允许列表中的 IP。这还意味着，如果不加以检查，则可能会导致此类缺陷，从而导致严重 bug。

2018 年，流行的软件项目 curl 中也发现具有相同类型的漏洞，它将八进制 IPv4 地址解析为十进制，比如，运行“ curl -v 0177.0.0.1”curl 连接到 177.0.0.1，而不是环回地址 127.0.0.1。此前，Sick Codes、Jackson 和 Sahler 曾在 private-ip 软件包中发现了一个类似的漏洞（CVSS 评分 9.8），该软件包每周有 17.5 万左右的下载量。

影响范围

Netmask <= v1.1.0

安全建议

目前此漏洞已经修复，建议及时更新至 netmask 版本 2.0.0。

下载链接：

https://www.npmjs.com/package/netmask

参考链接：

https://www.npmjs.com/package/netmask

https://github.com/sickcodes/security/blob/master/advisories/SICK-2021-011.md

https://www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/

https://sick.codes/universal-netmask-npm-package-used-by-270000-projects-vulnerable-to-octal-input-data-server-side-request-forgery-remote-file-inclusion-local-file-inclusion-and-more-cve-2021-28918/

2. Apache Druid 远程代码执行漏洞（CVE-2021-26919）

Apache Druid 是专为大数据集的快速切片分析（OLAP 查询）而设计的高性能分析数据库。

2021 年 03 月 29 日，Apache 官方发布安全公告，公开了 Apache Druid 中的一个远程代码执行漏洞（CVE-2021-26919）。

Druid 使用 JDBC 从其它数据库读取数据，此功能是为了让受信任的用户通过适当的权限来设置查找或提交提取任务。由于 Apache Druid 默认情况下缺乏授权认证，攻击者可通过构造恶意请求执行任意代码，从而控制服务器。

影响范围

Druid <= 0.20.1

安全建议

目前官方已修复了此漏洞，建议及时升级到 Druid 0.20.2。

下载链接：

https://github.com/apache/druid/releases/tag/druid-0.20.2

参考链接：

http://mail-archives.apache.org/mod_mbox/www-announce/202103.mbox/%3CCACZfFK6Va-CqhfDUPqPvqBCw8JsJwQ1xRe8JxeQbX5cRyi7qJg@mail.gmail.com%3E

https://github.com/apache/druid/releases/tag/druid-0.20.2

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26919

3. VMware vRealize SSRF 漏洞（CVE-2021-21975）

Vmware vRealize Operations Manager 是针对 vmware 虚拟化平台的一套运维管理解决方案。

2021 年 03 月 31 日，VMware 官方发布安全公告，公开了 VMware vRealize Operations 中的一个 SSRF 漏洞和一个任意文件上传漏洞（漏洞追踪为 CVE-2021-21975 和 CVE-2021-21983）。

vRealize Operations 服务器端请求伪造（CVE-2021-21975）

vRealize Operations Manager API 中存在一个服务器端请求伪造漏洞，其 CVSS 评分为 8.6。具有 vRealize Operations Manager API 网络访问权限攻击者可以通过利用此漏洞执行服务器端请求伪造攻击，以窃取管理员凭据。

Realize Operations 任意文件上传漏洞（CVE-2021-21983）

vRealize Operations Manager API 中存在一个任意文件上传漏洞，其 CVSS 评分为 7.2。具有网络访问 vRealize Operations Manager API 权限的经过验证的攻击者可以将任意文件上传到系统上。

影响范围

VMware vRealize operations manager： 8.3.0、8.2.0、8.1.1、8.1.0、8.0.1、8.0.0、7.5.0

VMware cloud foundation（vROps）：4.x、3.x

vRealize Suite Lifecycle Manager (vROps)：8.x

安全建议

目前该漏洞 PoC 已公开，建议参考官方公告及时升级或安装相应补丁。

下载链接：

https://kb.vmware.com/s/article/83210

参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0004.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21975

https://www.bleepingcomputer.com/news/security/vmware-fixes-bug-allowing-attackers-to-steal-admin-credentials/

4. GitLab 4 月任意文件读取漏洞

GitLab 是一个用于仓库管理系统的开源项目，其使用 Git 作为代码管理工具，可通过 Web 界面访问公开或私人项目。

2021 年 03 月 31 日，Gitlab 发布安全公告，公开了 GitLab 社区版（CE）和企业版（EE）中的多个安全漏洞。其中较为严重的是一个任意文件读取漏洞，其 CVSSv3 评分为 9.6，攻击者可以通过导入特定文件来读取服务器上的任意文件；以及一个 Kroki 任意文件读取漏洞，其 CVSSv3 评分为 7.5，攻击者可以通过特制的 Wiki 页面来读取服务器上的任意文件。

影响范围

Gitlab CE/EE < 13.8.7

Gitlab CE/EE < 13.9.5

Gitlab CE/EE < 13.10.1

安全建议

目前官方已修复了此漏洞，建议升级至以下版本：

Gitlab CE/EE 13.8.7

Gitlab CE/EE 13.9.5

Gitlab CE/EE 13.10.1

下载链接：

https://about.gitlab.com/update/

参考链接：

https://about.gitlab.com/releases/2021/03/31/security-release-gitlab-13-10-1-released/

5. VMware Carbon Black Cloud Workload 身份验证绕过漏洞（CVE-2021-21982）

VMware Carbon Black Cloud 是一个云原生端点和工作负载保护平台（EPP 和 CWP），可有效阻止新兴威胁。Carbon Black Cloud Workload 通过将弱点评估、工作负载加固与业界领先的新一代防病毒（NGAV）、工作负载行为监测以及端点检测和响应（EDR）功能相结合，为运行在这些环境中的工作负载提供保护。

2021 年 04 月 01 日，VMware 官方发布安全公告，公开了 VMware Carbon Black Cloud Workload 中的一个身份验证绕过漏洞（CVE-2021-21982），该漏洞的 CVSSv3 基本得分为 9.1。

攻击者能够通过利用此漏洞获取 VMware Carbon Black Cloud Workload 设备的管理界面访问权限（比如通过操纵管理界面 URL），以获取有效的身份验证令牌，从而获得对设备管理 API 的访问权限。成功利用此漏洞的攻击者最终可以查看和更改管理配置设置，且该漏洞无需身份验证或用户交互即可利用。

影响范围

VMware Carbon Black Cloud Workload appliance <= 1.0.1

安全建议

目前该漏洞已经修复，建议及时升级至 VMware Carbon Black Cloud Workload appliance 1.0.2 版本。

下载链接：

https://docs.vmware.com/en/VMware-Carbon-Black-Cloud-Workload/1.0/rn/cbc-workload-102-release-notes.html

参考链接：

https://www.vmware.com/security/advisories/VMSA-2021-0005.html

https://www.bleepingcomputer.com/news/security/vmware-fixes-authentication-bypass-in-data-center-security-software/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21982

0x02 本周安全态势

1. PHP 官方 Git 存储库被黑，代码库被篡改

事件概述

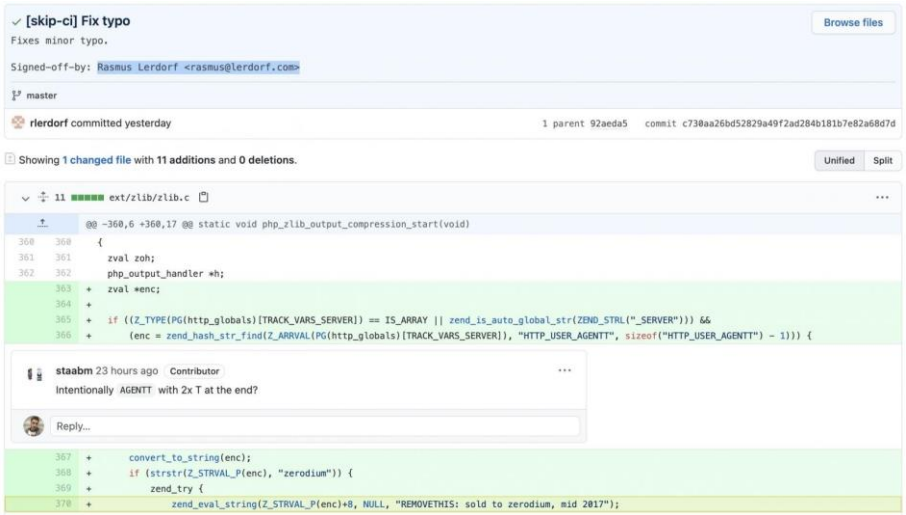
近日，PHP 官方 Git 存储库受到复杂的供应链攻击。攻击者通过非法提交更改了 PHP 的源代码，在 PHP 代码库中植入后门程序。PHP 维护者已决定将官方 PHP 源代码存储库迁移到 GitHub。

事件详情

PHP 被用作服务器端编程语言，互联网上有超过 79%的网站依赖 PHP，PHP 官方 Git 存储库被篡改，这一影响令人震惊。

2021 年 03 月 28 日，两个恶意提交被推送到 PHP 团队维护的 git.php.net 服务器的 php-src Git 仓库，并且攻击者对这些提交进行了签名，以伪造成是已知的 PHP 开发者和维护者 Rasmus Lerdorf 和 Nikita Popov 完成的。

攻击者以 Rasmus Lerdorf 的身份签署的恶意提交（非法）植入远程代码执行后门：

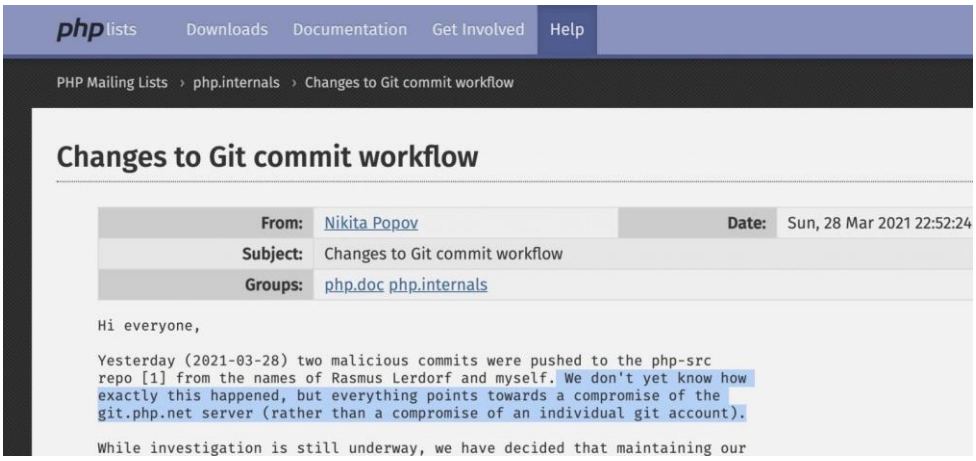


我们看到新增的第 370 行调用 zend_eval_string 函数的地方，这段代码实际上是为运行这个被劫持的 PHP 版本的网站埋下了一个后门，以方便远程代码执行（RCE）。

PHP 开发者 Jake Birchall 向最先指出这一异常的 Michael Voříšek 回应表示，如果字符串以'zerodium'开头，这一行就会从 useragent HTTP 头内执行 PHP 代码。

PHP 维护者 Nikita Popov 表示，第一次提交是在几个小时后被发现的，作为常规提交后代码审查的一部分。这些更改显然是恶意的，并立即被还原了。此外，这些更改是在 PHP 8.1 的开发分支上进行的，该分支将于今年年底发布。

虽然对事件的调查还在进行中，但据 PHP 维护者称，这次恶意活动源于被入侵的 git.php.net 服务器，而不是个人的 Git 账户。官方公告中也称该事件指向服务器威胁：



作为预防，PHP 维护者已决定将官方 PHP 源代码存储库迁移到 GitHub，并且将在几天后停用 git.php.net 服务器，并永久转移到 GitHub。GitHub 上以前只是镜像的存储库现在将成为规范的存储库。

随着这一改变的进行，PHP 维护人员坚持从现在开始，任何代码修改都要直接推送到 GitHub 上，而不是 git.php.net 服务器上。而有兴趣为 PHP 项目做贡献的人员将需要成为 GitHub 上 PHP 组织的一部分，对于组织中的成员身份，需要在 GitHub 帐户上启用双因素身份验证（2FA）。

从 SolarWinds Orion 供应链攻击到 PHP 官方 Git 存储库被篡改，毫无疑问，供应链攻击已经成为令人不安的新趋势。

处置建议

虽然 PHP 的 Git 服务器被入侵的确切原因尚未确定，但从这次事件中可以吸取的一个教训是，运行在自托管服务器上的 CI/CD 工具很容易过时，应及时应用最新的安全更新。

参考链接

【事件通告】针对 SolarWinds 供应链的攻击事件分析

【事件通告】FireEye 遭到 APT 攻击，红队工具被窃事件

VMware OpenSLP 漏洞引发勒索事件通告

https://news-web.php.net/php.internals/113838

https://www.bleepingcomputer.com/news/security/phps-git-server-hacked-to-add-backdoors-to-php-source-code/

https://blog.sonatype.com/netmask-flaw-leaves-millions-vulnerable-while-a-php-git-server-is-hacked-in-software-supply-chain-attack

https://github.com/php/php-src/commit/2b0f239b211c7544ebc7a4cd2c977a5b7a11ed8a?

2. Purple Fox 攻击活动分析

摘要

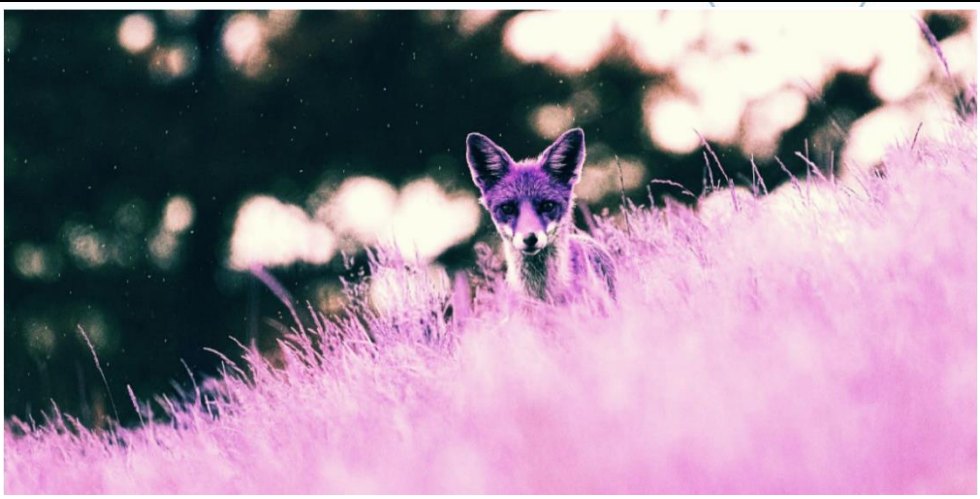
Purple Fox 是一个活跃的恶意软件攻击活动，针对 Windows 系统。

直到最近，Purple Fox 背后的黑客还通过使用攻击工具和钓鱼邮件感染目标。

Guardicore Labs 发现了其新感染媒介，通过 SMB 密码暴力破解面向网络的 Windows 系统。

Guardicore Labs 发现了 Purple Fox 用来托管 dropper 和 payloads 的庞大服务器网络，由受到感染的 Microsoft IIS 7.5 服务器组成。

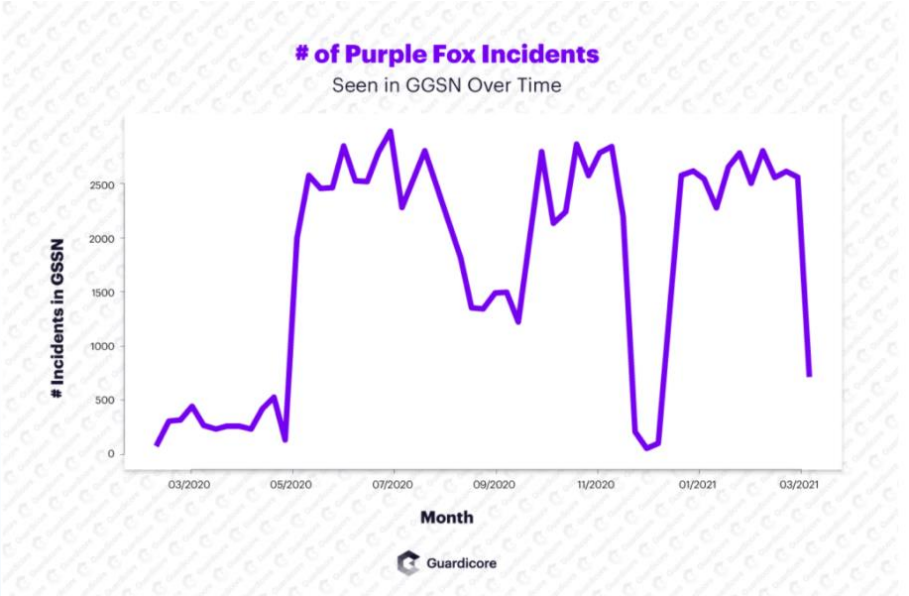
Purple Fox 恶意软件中的一个 Rootkit 允许将恶意软件隐藏在计算机上，从而使其难以被检测和删除。



介绍

在过去的几周中，Guardicore Labs 团队一直在追踪分发 Purple Fox 恶意软件的攻击活动。Purple Fox 于 2018 年 3 月首次被发现，是针对 Internet Explorer 和 Windows 系统的各种特权升级漏洞的攻击工具。

但是，在整个 2020 年底和 2021 年初，Guardicore 全球传感器网络(GGSN)检测到 Purple Fox 利用端口扫描和使用了弱密码和哈希的 SMB 服务来分发的新功能。



从上图中可以看出，2020 年 5 月出现了大量的恶意活动，到撰写本文时，感染数量增长了约 600%，总计 9 万次攻击。

尽管在漏洞利用方面，Purple Fox 的功能似乎并没有太大改变，但它的传播和分发方

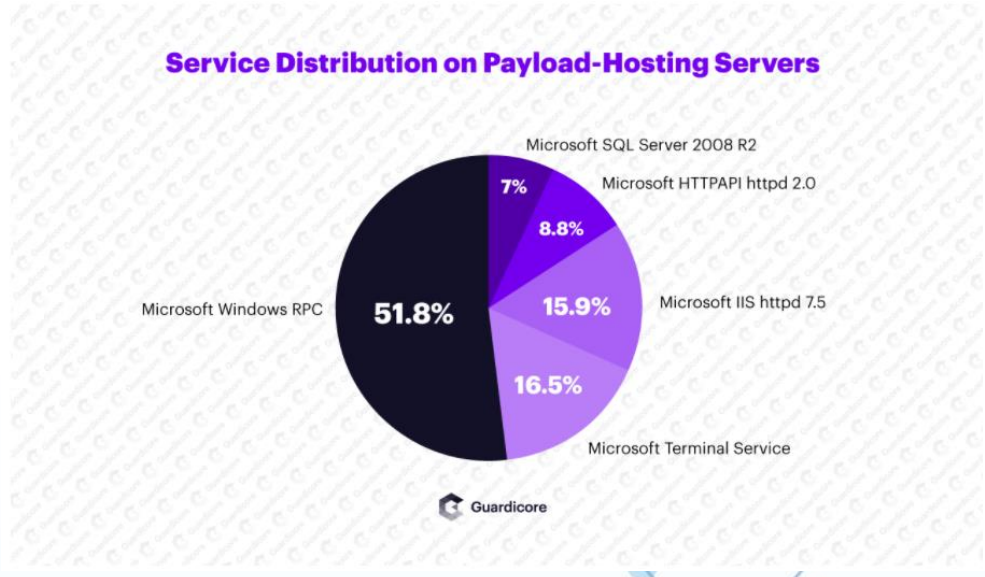
法，以及类似蠕虫软件的行为与以前文章中所描述大有不同。在整个研究过程中发现，其基础设施似乎是由一组易受攻击的服务器组成的，这些服务器植入了恶意软件的初始 payload、受感染的计算机（经常作为蠕虫活动的节点）以及似乎与其他恶意软件活动有关服务器基础架构。

后文将详细介绍关于新蠕虫活动的发现并共享 IOC。

攻击分析

攻击者在将近 2,000 台服务器上托管了各种 MSI 程序包（请参阅 IOC 部分），据估计，这都是被重新用于托管恶意 payload 的受损设备。这个假设是基于扫描了多台服务器，并从其操作系统版本和服务器版本的角度查看了托管在这些服务器上的服务。

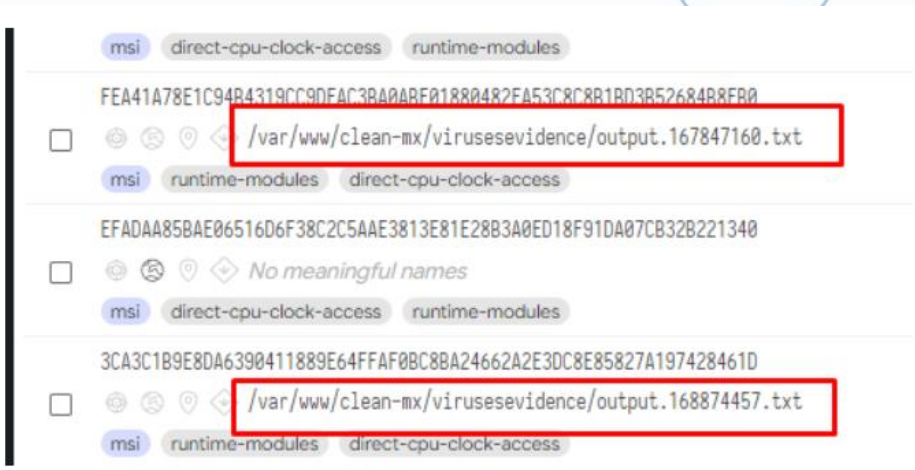
现已经确定，托管了初始 payload 的绝大多数服务器都在运行了 IIS 版本 7.5 和 Microsoft FTP 的相对较旧版本的 Windows Server 上，这些版本具有多个严重性级别不同的漏洞。

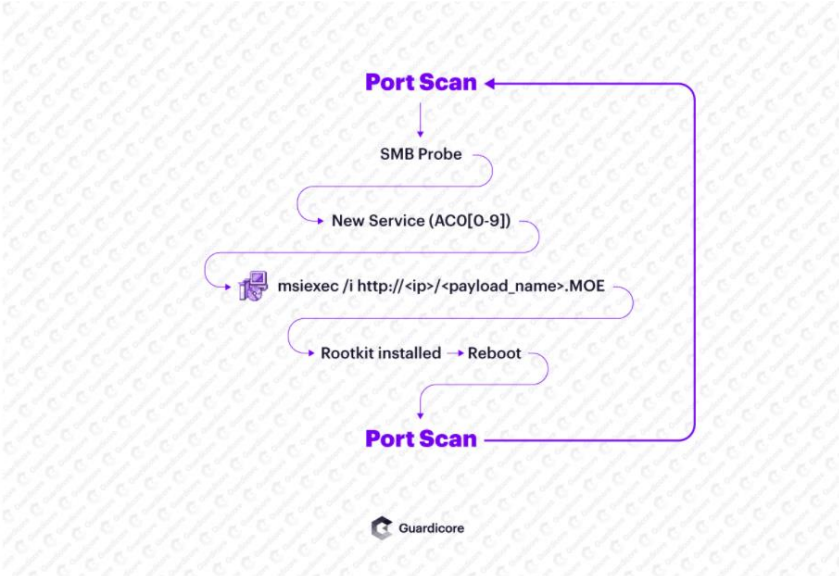


根据这些发现，该活动可以通过几种方式开始传播：

1.在目标计算机通过易受攻击的公开服务（例如 SMB）入侵后，执行蠕虫 payload。

2.通过利用了浏览器漏洞的网络钓鱼活动（与先前发布的有关 Purple Fox 的发现有关），利用电子邮件发送蠕虫 payload。现已确定了通过电子邮件扫描程序提交给 VirusTotal 的多个样本。



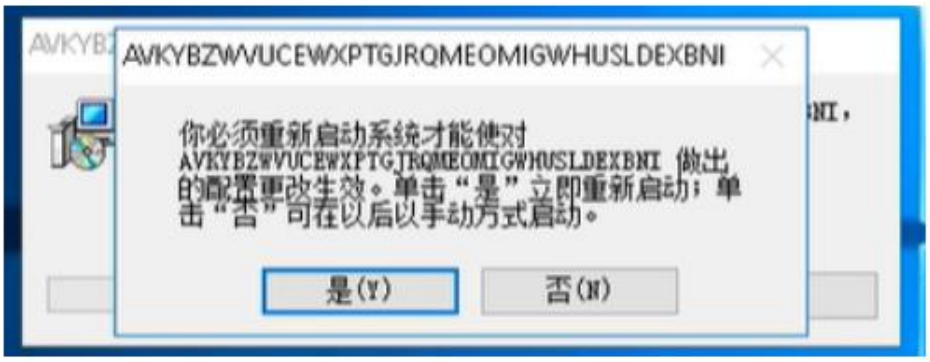


一旦在目标设备上完成代码执行，就会创建一个名称与正则表达式 AC0［0-9］{1}相匹配的新服务，例如 AC01、AC02、AC05 等，该服务的目的是建立持久性并执行带有“for 循环”的简单命令，此命令的目的是遍历包含了在目标设备上安装 Purple Fox 的 MSI 的 url。

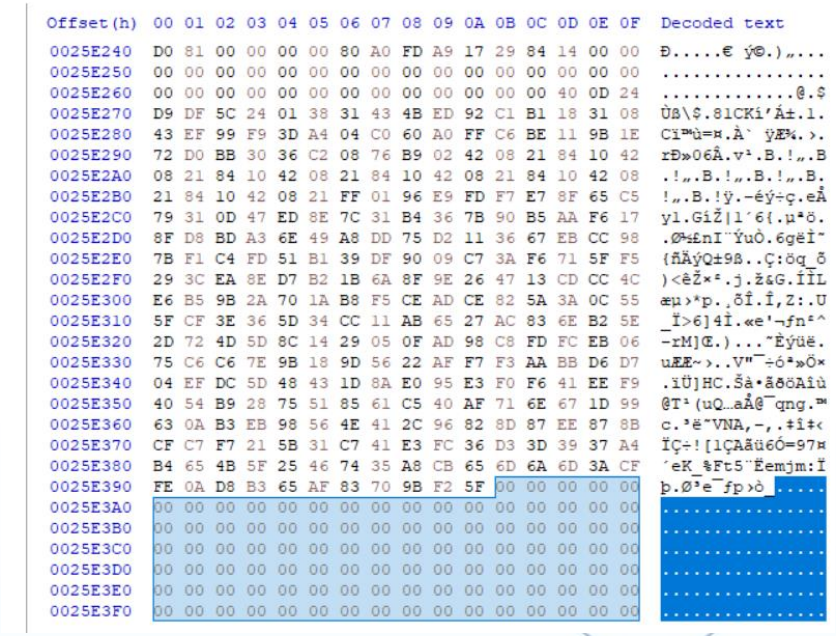
从 Guardicore Centra 平台的截图中可以看出，msiexec 将使用了/i flag 来执行，以便从目标主机下载并安装恶意 MSI 程序包。它还使用/Q flag，以实现不需要用户交互的静默执行。

为了进行分析，研究还执行了没有/Q flag 的 MSI 安装程序（就像直接从电子邮件附件

中执行一样），安装程序显示以下提示：

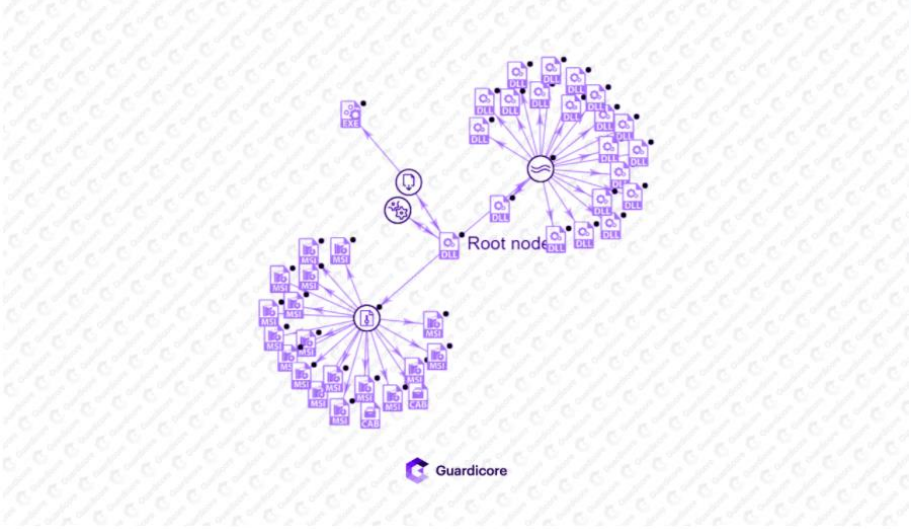


该安装程序伪装为 Windows Update 软件包以及中文文本，该文本大致翻译为“Windows Update”和随机字母。这些字母是在每个不同的 MSI 安装程序之中随机生成的，以创建不同的哈希值，这使得对同一 MSI 的不同版本建立联系变得有些困难。这是廉价且简单的用来规避各种检测机制（如静态签名）的方法。此外，已经确定了具有相同字符串但带有随机空字节的 MSI 软件包，以便为同一文件创建不同的哈希值。



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0025E240	D0	81	00	00	00	00	80	A0	FD	A9	17	29	84	14	00	00	Đ.....€ ý©.)„...
0025E250	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0025E260	00	00	00	00	00	00	00	00	00	00	00	00	00	40	0D	24	.....@.$
0025E270	D9	DF	5C	24	01	38	31	43	4B	ED	92	C1	B1	18	31	08	Ùß\$.81CKí'Á±.1.
0025E280	43	EF	99	F9	3D	A4	04	C0	60	A0	FF	C6	BE	11	9B	1E	Cï™ù=¤.À` ÿÆ¾.›.
0025E290	72	D0	BB	30	36	C2	08	76	B9	02	42	08	21	84	10	42	rÐ»06Â.v¹.B.!„.B
0025E2A0	08	21	84	10	42	08	21	84	10	42	08	21	84	10	42	08	.!„.B.!„.B.!„.B.
0025E2B0	21	84	10	42	08	21	FF	01	96	E9	FD	F7	E7	8F	65	C5	!„.B.!ÿ.-éý÷ç.eÅ
0025E2C0	79	31	0D	47	ED	8E	7C	31	B4	36	7B	90	B5	AA	F6	17	y1.GíŽ|1´6{.µªö.
0025E2D0	8F	D8	BD	A3	6E	49	A8	DD	75	D2	11	36	67	EB	CC	98	.Ø½£nI¨ÝuÒ.6gëÌ˜
0025E2E0	7B	F1	C4	FD	51	B1	39	DF	90	09	C7	3A	F6	71	5F	F5	{ñÄýQ±9ß..Ç:öq_õ
0025E2F0	29	3C	EA	8E	D7	B2	1B	6A	8F	9E	26	47	13	CD	CC	4C	)<êŽ×².j.ž&G.ÍÌL
0025E300	E6	B5	9B	2A	70	1A	B8	F5	CE	AD	CE	82	5A	3A	0C	55	æµ›*p.¸õÎ.Í‚Z:.U
0025E310	5F	CF	3E	36	5D	34	CC	11	AB	65	27	AC	83	6E	B2	5E	_Ï>6]4Ì.«e'¬ƒn²^
0025E320	2D	72	4D	5D	8C	14	29	05	0F	AD	98	C8	FD	FC	EB	06	-rM]Œ.)...˜Èýüë.
0025E330	75	C6	C6	7E	9B	18	9D	56	22	AF	F7	F3	AA	BB	D6	D7	uÆÆ~›..V"¯÷ó ª»Ö×
0025E340	04	EF	DC	5D	48	43	1D	8A	E0	95	E3	F0	F6	41	EE	F9	.iÜ]HC.Šà•ãðöAîù
0025E350	40	54	B9	28	75	51	85	61	C5	40	AF	71	6E	67	1D	99	@T¹(uQ…aÅ@¯qng.™
0025E360	63	0A	B3	EB	98	56	4E	41	2C	96	82	8D	87	EE	87	8B	c.³ë˜VNA,–,.‡î‡‹
0025E370	CF	C7	F7	21	5B	31	C7	41	E3	FC	36	D3	3D	39	37	A4	ÏÇ÷![1ÇAãü6Ó=97¤
0025E380	B4	65	4B	5F	25	46	74	35	A8	CB	65	6D	6A	6D	3A	CF	´eK_%Ft5¨Ëemjm:Ï
0025E390	FE	0A	D8	B3	65	AF	83	70	9B	F2	5F	00	00	00	00	00	þ.Ø³e¯ƒp›ò_.....
0025E3A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0025E3B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0025E3C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0025E3D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0025E3E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0025E3F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

还找到了许多不同版本的同一 MSI 和它的 payload，可以从 VT 图看到以下截图。



随着安装的进行，安装程序将提取 payload 并从 MSI 软件包中对其进行解密。MSI 程序包包含三个文件：

1. 64 位 DLL payload（winupdate64）。
2. 32 位 DLL payload（winupdate32）。
3. 包含 rootkit 的加密文件。

作为安装过程的一部分，该恶意软件通过执行多个 netsh 命令来修改 Windows 防火墙。该恶意软件在 Windows 防火墙中添加了一个名为 Qianye 的新策略。在此策略下，它创建了一个名为 Filter1 的新过滤器，其禁止来自 Internet（0.0.0.0）上任意 IP 地址的 TCP 和 UDP 上的 445、139 和 135 端口连接到受感染的计算机。攻击者正在这样做是为了防止受感染的计算机再次遭到感染，或使其他攻击者利用该计算机。

上述文件一旦被提取，就将被执行。

可以将其视为恶意软件正在执行以下命令：

```
netsh.exe ipsec static add policy name=qianye
netsh.exe ipsec static add filterlist name=Filter1
netsh.exe ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=135 protocol=TCP
netsh.exe ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=139 protocol=TCP
netsh.exe ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=445 protocol=UDP
```

```
netsh.exe ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me
dstport=135 protocol=UDP
netsh.exe ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me
dstport=139 protocol=UDP
netsh.exe ipsec static set policy name=qianye assign=y
netsh.exe ipsec static add rule name=Rule1 policy=qianye filterlist=Filter1
filteraction=FilteraAtion1
netsh.exe ipsec static add rule name=Rule1 policy=qianye filterlist=Filter1
netsh.exe ipsec static add filteraction name=FilteraAtion1 action=block
```

此外，该恶意软件还将通过执行以下命令在计算机上安装 IPv6 接口：

```
netsh.exe interface ipv6 install
```

采取此措施是为了允许恶意软件端口扫描 ipv6 地址以及最大限度地增加(通常不受监控的)ipv6 子网的效率。

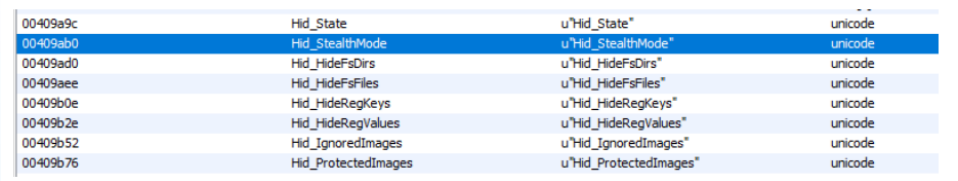
重要说明：

这些命令可用作行为指示符（IoB），以检查您的环境是否受到威胁。

此外，这些 netsh 命令还出现在以前的攻击活动中，并不只限于 Purple Fox。这些命令，特别是带有 Qianye 策略名称的命令，已作为 Rig EK 和 NuggetPhantom 的一部分被记录。

在重新启动计算机之前，Purple Fox 的最后一步是加载隐藏在 MSI 包中加密 payload 内的 rootkit。

根据分析，这个 rootkit 是基于隐藏的开源 rootkit 项目。



00409a9c	Hid_State	u"Hid_State"	unicode
00409ab0	Hid_StealthMode	u"Hid_StealthMode"	unicode
00409ad0	Hid_HideFsDirs	u"Hid_HideFsDirs"	unicode
00409aee	Hid_HideFsFiles	u"Hid_HideFsFiles"	unicode
00409b0e	Hid_HideRegKeys	u"Hid_HideRegKeys"	unicode
00409b2e	Hid_HideRegValues	u"Hid_HideRegValues"	unicode
00409b52	Hid_IgnoredImages	u"Hid_IgnoredImages"	unicode
00409b76	Hid_ProtectedImages	u"Hid_ProtectedImages"	unicode

```
3
4   #define CONFIG_ALLOC_TAG 'gfnC'
5
6   typedef struct _HidConfigContext {
7           BOOLEAN state;
8           BOOLEAN stealth;
9           UNICODE_STRING hideFSDirs;
10          UNICODE_STRING hideFSFiles;
11          UNICODE_STRING hideRegKeys;
12          UNICODE_STRING hideRegValues;
13          UNICODE_STRING ignoreImages;
14          UNICODE_STRING protectImages;
15  } HidConfigContext, *PHidConfigContext;
16
```

这个 rootkit 旨在隐藏各种注册表项和值、文件等，正如其作者在 git 存储库中所详述的那样。具有讽刺意味的是，该隐藏 rootkit 是由安全研究人员开发的，目的是执行各种恶意软件分析任务，并从恶意软件中隐藏这些任务。

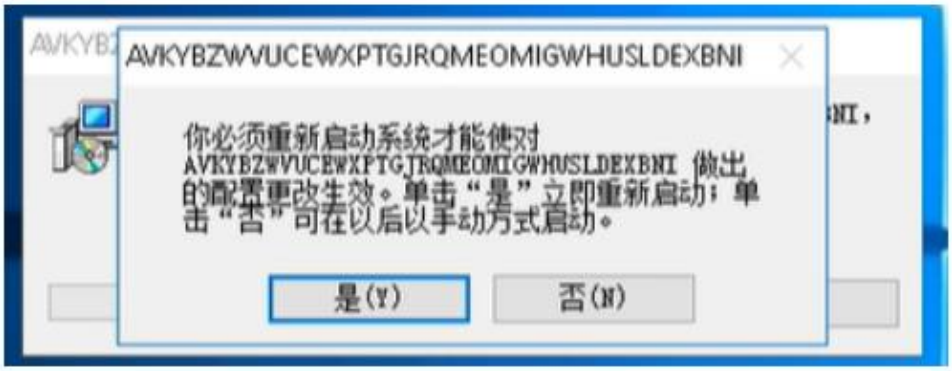
Hidden

This toolset is developed like a solution for my reverse engineering and researching tasks. This is a windows driver with a usermode interface which is used for hidding specific environment on VMs, like installed rce programs (ex. procmon, wireshark), vm infrastracture (ex. vmware tools) and etc.

Features

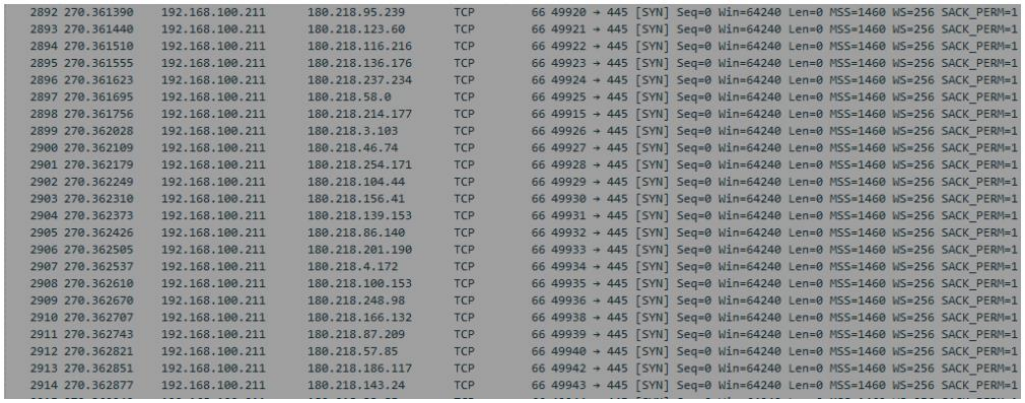
- hide registry keys and values
- hide files and directories
- protect specific processes using ObRegisterCallbacks
- exclude specific processes from hidding and protection features
- usermode interface (lib and cli) for working with driver

加载 rootkit 后，安装程序将重新启动计算机，以将恶意软件 DLL 重命名为系统 DLL 文件，并在 boot 时执行。由于在实验室中没有/Q flag 的情况下执行了恶意软件，因此出现了以下窗口，要求重新启动计算机：



一旦重新启动计算机后，恶意软件也将被执行。执行后，恶意软件将开始其传播过程：它将生成 IP 范围并开始在端口 445 上进行扫描。

当计算机响应在端口 445 上发送的 SMB 探针时，它将尝试强制使用用户名和密码或建立空会话来向 SMB 进行身份验证。



2892	270.361390	192.168.100.211	180.218.95.239	TCP	66 49920 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2893	270.361440	192.168.100.211	180.218.123.60	TCP	66 49921 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2894	270.361510	192.168.100.211	180.218.116.216	TCP	66 49922 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2895	270.361555	192.168.100.211	180.218.136.176	TCP	66 49923 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2896	270.361623	192.168.100.211	180.218.237.234	TCP	66 49924 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2897	270.361695	192.168.100.211	180.218.58.0	TCP	66 49925 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2898	270.361756	192.168.100.211	180.218.214.177	TCP	66 49915 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2899	270.362028	192.168.100.211	180.218.3.103	TCP	66 49926 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2900	270.362109	192.168.100.211	180.218.46.74	TCP	66 49927 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2901	270.362179	192.168.100.211	180.218.254.171	TCP	66 49928 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2902	270.362249	192.168.100.211	180.218.104.44	TCP	66 49929 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2903	270.362310	192.168.100.211	180.218.156.41	TCP	66 49930 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2904	270.362373	192.168.100.211	180.218.139.153	TCP	66 49931 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2905	270.362426	192.168.100.211	180.218.86.140	TCP	66 49932 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2906	270.362505	192.168.100.211	180.218.201.190	TCP	66 49933 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2907	270.362537	192.168.100.211	180.218.4.172	TCP	66 49934 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2908	270.362610	192.168.100.211	180.218.100.153	TCP	66 49935 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2909	270.362670	192.168.100.211	180.218.248.98	TCP	66 49936 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2910	270.362707	192.168.100.211	180.218.166.132	TCP	66 49938 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2911	270.362743	192.168.100.211	180.218.87.209	TCP	66 49939 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2912	270.362821	192.168.100.211	180.218.57.85	TCP	66 49940 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2913	270.362851	192.168.100.211	180.218.186.117	TCP	66 49942 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2914	270.362877	192.168.100.211	180.218.143.24	TCP	66 49943 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

如果身份验证成功，则恶意软件将创建一个名称与正则表达式 AC0 [0-9]{1}相匹配的服务，例如 AC01、AC02 和 AC05（如前文所述），该服务将从众多 HTTP 服务器中的一个下载 MSI 安装包，从而完成感染循环。

IOCs

https://github.com/guardicore/labs_campaigns/tree/master/Purple_Fox

原文链接：

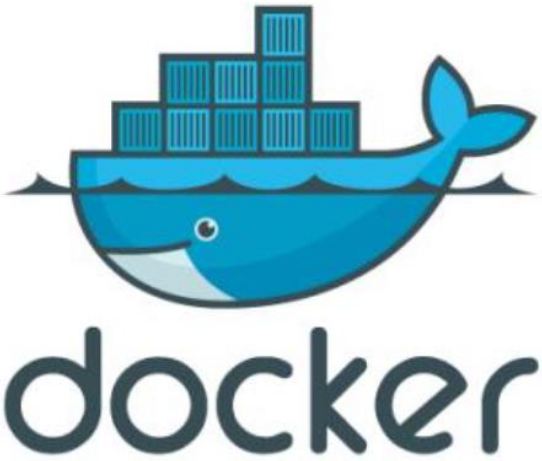
https://www.guardicore.com/labs/purple-fox-rootkit-now-propagates-as-a-worm/

3. 30 个 Docker 镜像在加密劫持攻击中被下载了 2000 万次

执行摘要

作为网络犯罪分子，有很多方法可以牟取暴利。最简单的方法之一是加密劫持，非法使用他人的计算资源来挖掘加密货币。众所周知，容器镜像是一种简单的软件分发方式，然而恶意的被加密劫持的镜像也是攻击者分发加密货币的一种简单方式。

我决定深入研究 Docker Hub，然后发现了 30 个恶意镜像，总共提取了 2000 万次请求（这意味着镜像被下载了 2000 万次），这是一场加起来价值 200,000 美元的加密劫持行动。在本文中，我将详细介绍我的发现以及为什么可以合理地假设 Docker Hub 和其它公共注册表上还有许多未被发现的恶意镜像。



查找恶意的加密劫持镜像

在过去的几年中，Unit 42 研究人员发现了基于云的加密劫持攻击，其中有攻击者使用 Docker Hub 中的镜像部署了矿工。

云是加密劫持攻击的热门，主要原因有两个：

1. 云由每个目标的许多实例组成（如大量 CPU、大量容器、大量虚拟机），这可以转化为巨大的挖矿利润。

2. 云很难监控。矿机可以在不被发现的情况下运行很长时间，如果没有任何检测机制，矿机可能会一直运行，直到用户发现虚假的云费用并意识到出了问题。

现代云技术主要基于容器，在一些环境中，Docker Hub 是默认的容器注册表。攻击者可以利用它在被入侵的云上部署矿工。基于这些事实，我想看看是否可以在 Docker Hub 中找到恶意的加密劫持镜像。在我的研究中，我从 10 个不同的 Docker Hub 账户中找到了 30 个镜像，这些镜像有 2000 多万次拉取。

个人可以通过使用采矿池来提高采矿效率，攻击者也是如此。

通过检查挖矿池，可以检查有多少个加密货币被挖出到挖矿池账户。我发现一半的镜像使用共享此信息的矿池，从这推断得出，我估计在所有攻击中总共开采了价值 200,000 美元的加密货币。

图 1.研究结果

货币

我的第一个发现，那就是攻击者最喜欢挖矿的加密货币是 Monero（门罗币），就像我们看到的 Pro-Ocean、Cetus 和许多其它货币一样。

攻击者青睐 Monero 有三个原因：

1.Monero 提供了最大的匿名性。它的一个特点是，与其它币种不同，Monero 的过渡是隐藏的。这种隐私对于网络犯罪分子来说是完美的，因为这意味着他们的活动是隐藏的。因此，他们不会被交易所禁止，而且他们更容易逃避追踪其资金的行为。

2.Monero 挖矿算法偏向于 CPU 挖矿，不像许多其它密码需要 ASIC 或 GPU 进行挖矿。这很方便，因为所有的计算机都有 CPU。因此，矿机可以在任何机器上有效运行。这甚至更适合容器，其中绝大多数容器的运行不需要 GPU。

3.Monero 是一种流行的加密货币，它的交易量每天约为 1 亿美元，这使得攻击者很容

易出售。

下图展示了 Docker Hub 上发现的加密劫持镜像的币种分布：

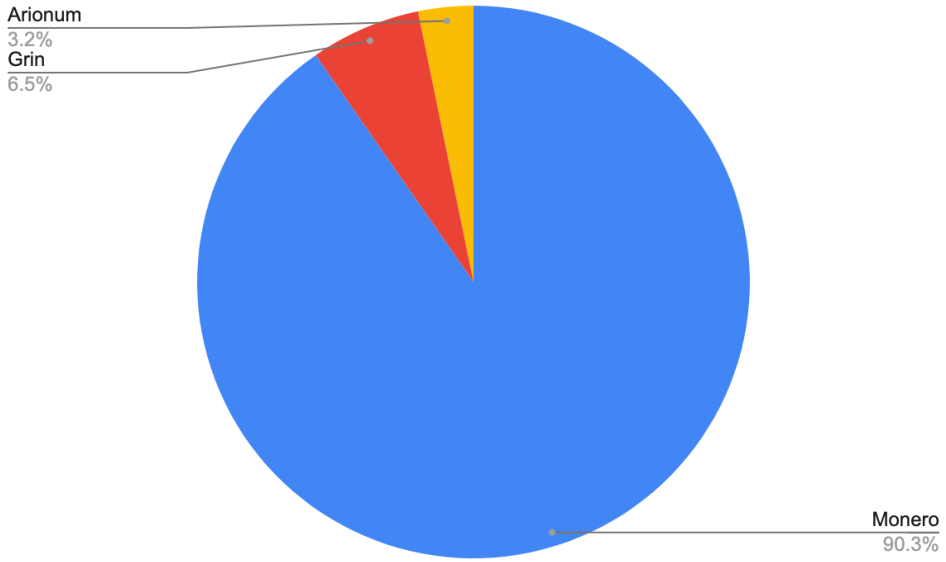


图 2.加密货币分布

加密矿工分布

在大多数挖掘 Monero 的攻击中，攻击者都使用了 XMRig，就像我们看到的 Hildegard 和 Graboid 一样。XMRig 是一款流行的 Monero 矿机，攻击者首选它，因为它易于使用，高效，最重要的是，它是开源的。因此，攻击者可以修改其代码。

例如，大多数 Monero 加密矿工都会强行捐出一定比例的挖矿时间给矿工的开发者。攻击者常见的一个修改是将捐赠比例改为 0。

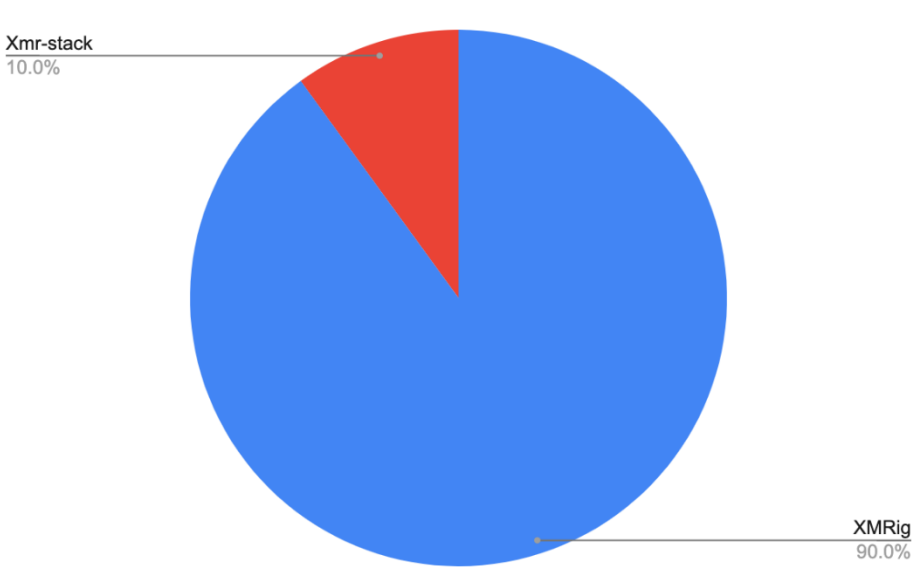


图 3.加密矿工分布

镜像标签

容器注册表允许用户升级其镜像，并在此过程中将新标签上传到注册表。标签是引用同一镜像的不同版本的一种方法。

在检查镜像的标签时，我发现有些镜像对不同的 CPU 架构或操作系统有不同的标签。看来攻击者为了适应广泛的受害者，包括一些操作系统（OS）和 CPU 架构，他们添加了这些标签。

在某些镜像中，甚至还带有不同类型的密码器的标签。这样，攻击者就可以为受害者的硬件选择最佳的加密矿工。

特定镜像中所有标签唯一共同的就是钱包地址或矿池凭证。在这些标识符的帮助下，我可以对每个活动进行分类。在深入研究之后，在某些情况下，我可以看到有许多属于同一活动的 Docker Hub 帐户。例如，在之前的研究中，Unit 42 发现的恶意账户 azurenql。现在，我们发现这个活动范围更广，包括 021982、dockerxmrig、ggcloud1 和 ggcloud2 等账户。

在我的研究中，我能够找到其它挖掘 Monero 的镜像，这些镜像与 Unit 42 最近发现的 azurenql 的活动有关，在攻击者的名字下增加了超过 1000 万次拉动。

结论

云为加密劫持攻击提供了巨大的机会。在我的研究中，我使用了一种加密采矿扫描仪，该扫描仪仅检测简单的加密采矿 Payload。我还通过将钱包地址与以前的攻击相关联来确保任何识别出的镜像都是恶意的。即使使用这些简单的工具，我也发现了几十个镜像，它们都有数百万次的拉取。我怀疑这种现象可能比我发现的现象更严重，因为在很多情况下，Payload 都不容易被检测到。

Palo Alto Networks Prisma Cloud 客户可以通过 Cryptominers Runtime Detection 功能和 Trusted Images 功能保护自己免受这些威胁。此外，拥有 Threat Prevention 安全订阅的 Palo Alto Networks 下一代防火墙客户还可以防止这些镜像的传递。

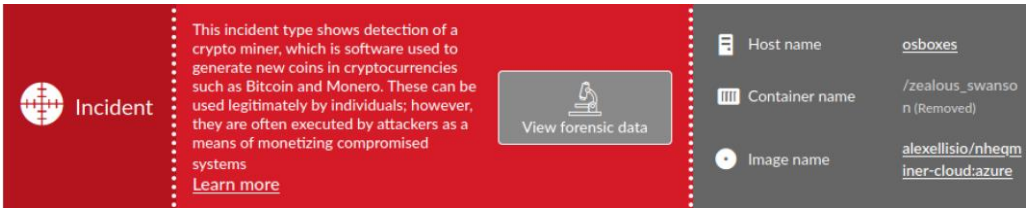


图 4. Prisma Cloud 容器事件通知

IOC

Docker 镜像

021982/155_138

021982/66_42_53_57

021982/66_42_93_164

021982/xmrig

021982/xmrig1

021982/xmrig2

021982/xmrig3

021982/xmrig4

021982/xmrig5

021982/xmrig6

021982/xmrig7

avfinder/gmdr

avfinder/mdadmd

docheck/ax

docheck/health

dockerxmrig/proxy1

dockerxmrig/proxy2

ggcloud1/ggcloud

ggcloud2/ggcloud

kblockdkblockd/kblockd

osekugatty/picture124

osekugatty/picture128

tempsbro/tempsbro

tempsbro/tempsbro1

toradmanfrom/toradmanfrom

toradmanfrom/toradmanfrom1

xmrigdocker/docker2

xmrigdocker/docker3

xmrigdocker/xmrig

xmrigdocker/xmrig

zenidine/nizadam

原文链接：

https://unit42.paloaltonetworks.com/malicious-cryptojacking-images/

4. 趋势科技：Conti 勒索软件分析

概述

2021 年 2 月，我们通过趋势科技 Vision One 平台发现 Conti 勒索软件团伙攻击相关的一系列可疑事件。

Conti 勒索软件是一种全球性威胁，其受害者主要位于北美和西欧，它被认为是 Ryuk 勒索软件系列的继承者。越来越多的攻击者通过使用过去分发 Ryuk 的相同方法来分发该恶意软件。例如，Trickbot/Emotet 和 BazarLoader 现在都被用来分发 Conti 勒索软件。

本文讨论了如何使用 Cobalt Strike 信标（检测为 Backdoor.<architecture>.COBEACON.SMA）以及我们如何使用趋势科技 Vision One 平台跟踪此威胁。我们认为，Sophos 的研究人员也遇到了这一特殊的恶意软件，因为在我们研究的攻击中使用的技术和他们研究的攻击中发现的技术存在相似之处。

调查

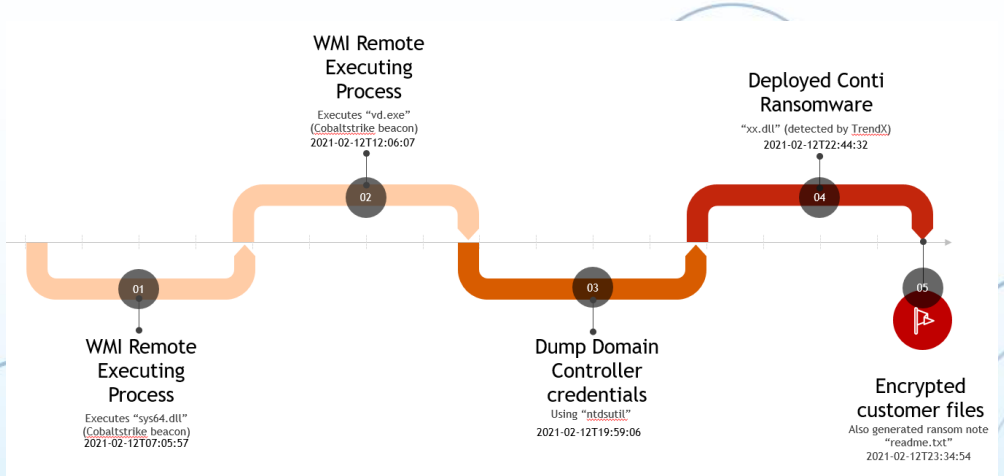


图 1. 调查前的时间表

这些攻击是通过“工作台”面板发现的，客户组织的 SOC 和 MDR 研究人员都可以访问该面板。它可以用来帮助响应正在进行的事件，以及为正在进行的安全调查添加背景资料。

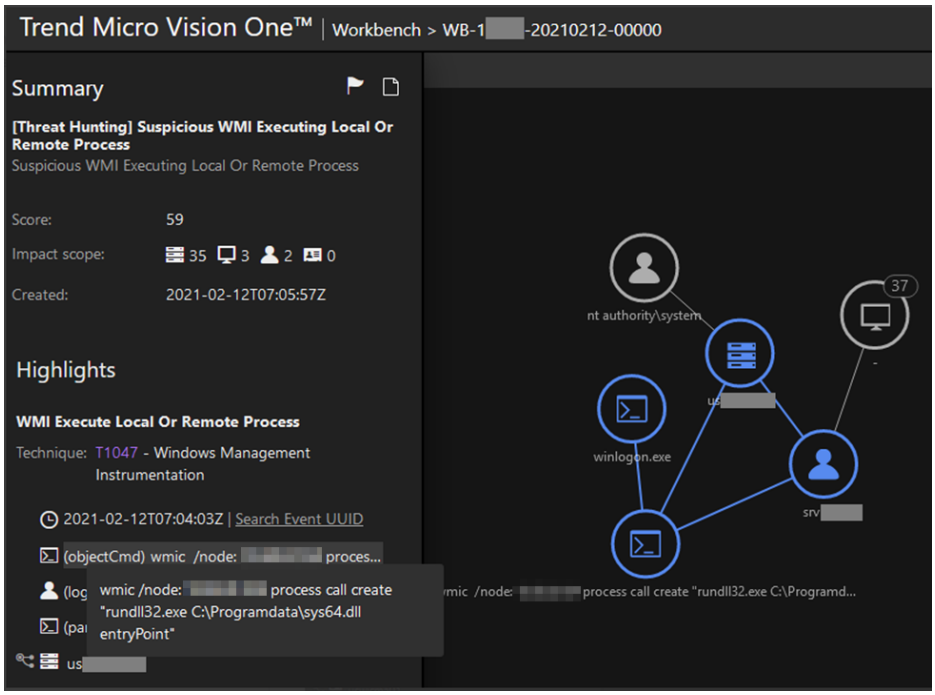


图 2. Vision One 模型命中

我们在这个工作台警报中看到 sys64.dll（Cobalt Strike 信标）被命令在远程机器上执行。父进程是 winlogon.exe，它一般用于处理与登录相关的任务。这使得 sys64.dll 的启动相当可疑。

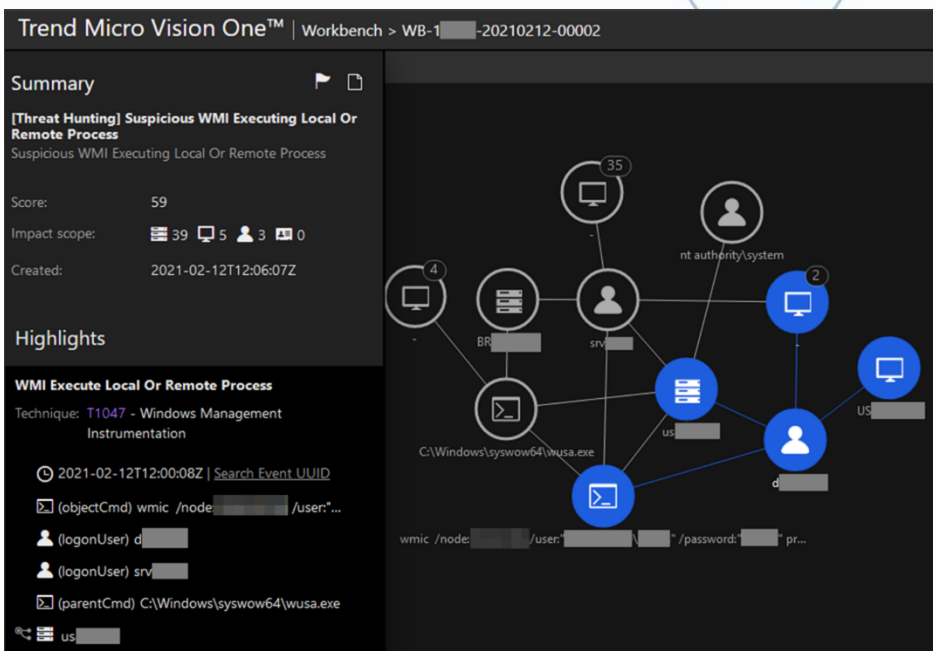


图 3. Vision One 模型命中

第二个警报与第一个警报类似，但它不是运行 sys64.dll，而是执行 vd.exe，也就是 Cobalt Strike 信标文件。命令如下：

```
wmic /node:{IP address} /user:"<domain>\<user>" /password:"<password>" process call create "cmd /c C:\vd.exe"
```

使用 Search App 检查事件后，我们看到这些系统可执行文件正在受到 Cobalt Strike 信标代码（vd.exe）的进程注入，如遥测事件 "701 - TELEMETRY_MODIFIED_PROCESS_CREATE_REMOTETHREAD "所示

Logged	objectCmd	processFilePath	endpointHostName	eventSubId
2021-02-12T19:36:39Z	C:\Windows\system32\wusa.exe	c:\temp\vd.exe	US[redacted]	701 - TELEMETRY_MODIFIED_PROCESS_CREAT...
2021-02-12T19:35:30Z	C:\Windows\system32\wusa.exe	c:\temp\vd.exe	US[redacted]	701 - TELEMETRY_MODIFIED_PROCESS_CREAT...
2021-02-12T19:33:30Z	C:\Windows\system32\wusa.exe	c:\temp\vd.exe	US[redacted]	701 - TELEMETRY_MODIFIED_PROCESS_CREAT...

图 4.注入 Cobaltstrike 信标代码的遥测事件

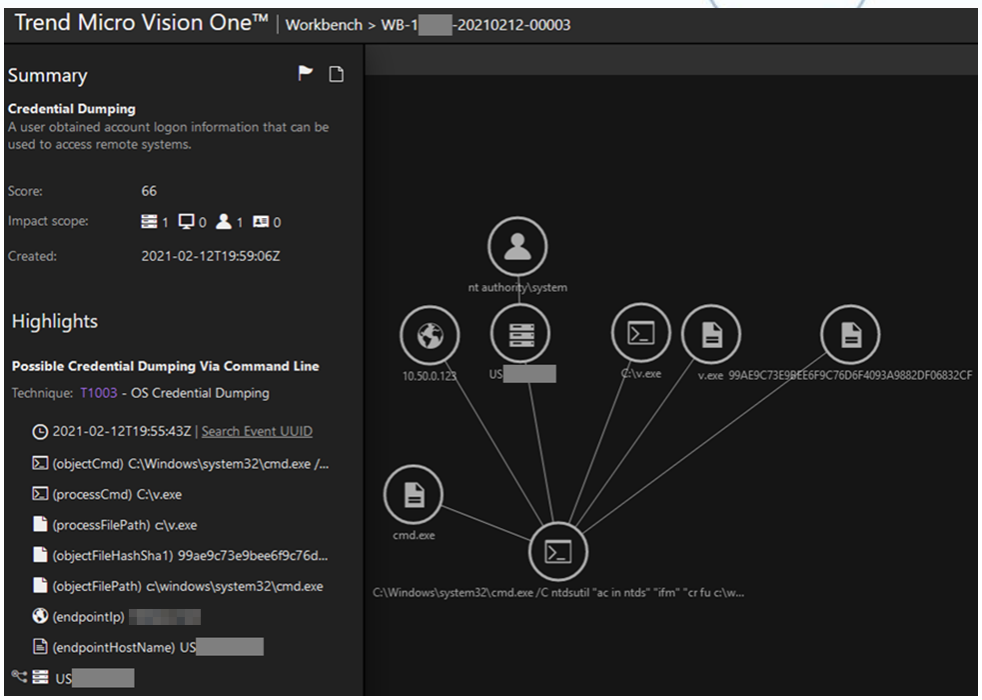


图 5. Vision One 模型命中

然后，攻击者试图使用 ntdsutil 转储域名密码哈希，将结果保存为 c:\windows\temp\abc，以供日后使用。

```
C:\Windows\system32\cmd.exe /C ntdsutil "ac in ntds" "ifm" "cr fu c:\windows\temp\abc" q q
```

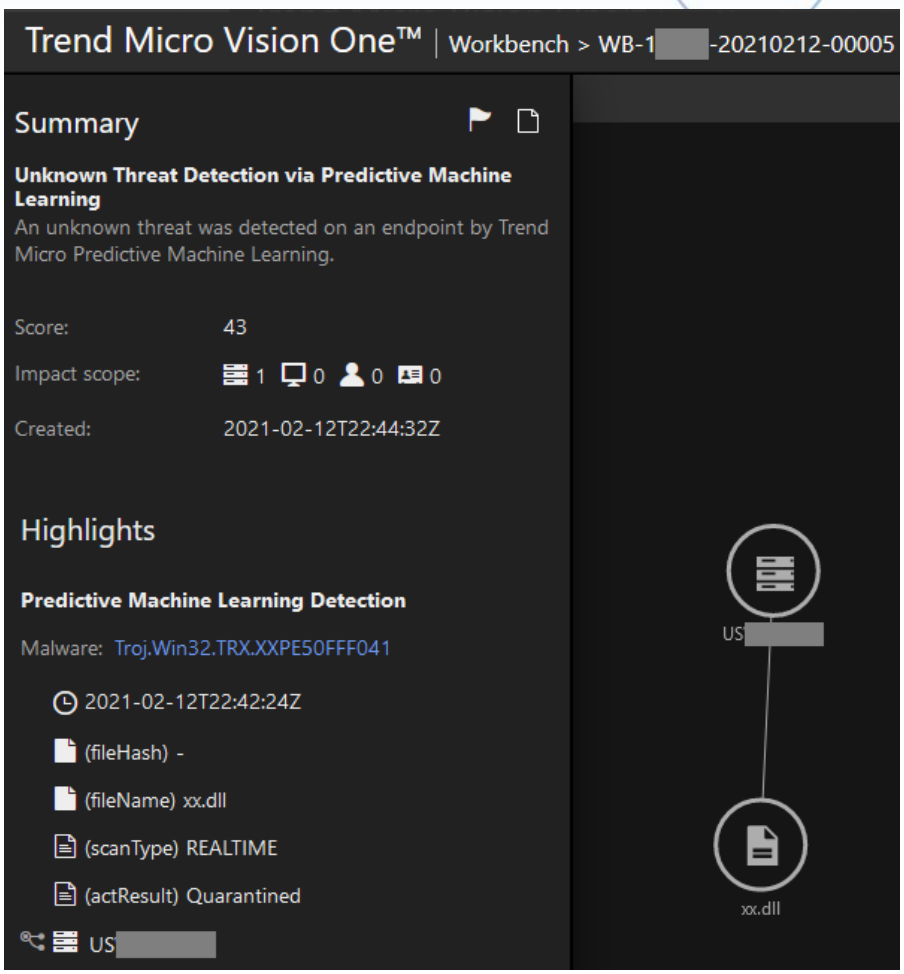


图 6. Vision One 模型命中

攻击者并没有立即进行任何进一步的恶意活动。相反，几个小时后，他们开始部署 Conti 勒索软件的 Payload，趋势科技的 Predictive Machine Learning 立即检测到了该 Payload。当前检测到文件 xx.dll 为 Ransom.Win64.CONTI.A。

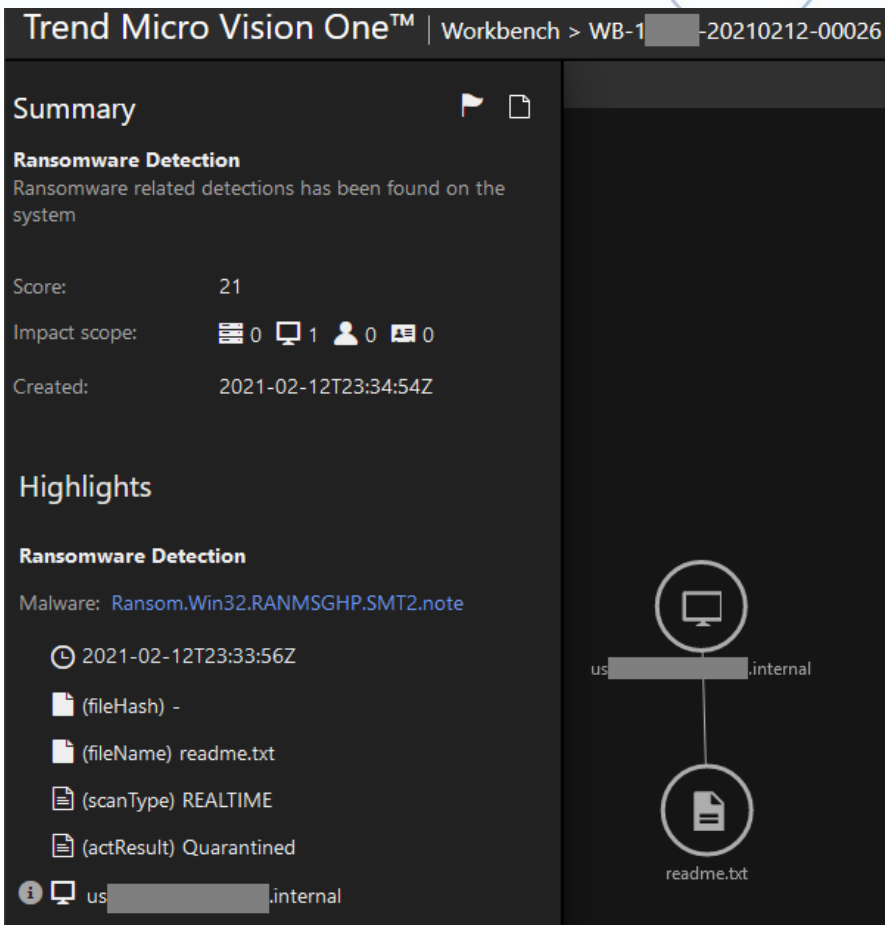


图 7. Vision One 模型命中

在进行 CONTI 勒索软件部署之后，在多个端点上检测到勒索记录。

缺少到达矢量

目前尚不清楚 Cobalt Strike 信标的 arrival vector（到达矢量）。我们通过趋势科技 Vision One 的不同功能对此进行了深入研究。

使用趋势科技 Vision One 的观察攻击技术(OAT)应用程序，我们注意到有几个端点在今年 2 月 11 日和 12 日才开始向趋势科技 Vision One 发送数据。只要我们检查了更多的遥测数据，便能够确认这种情况。

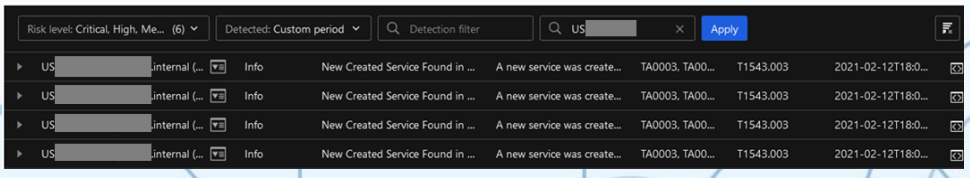


图 8.通过 Vision One 查看遥测

Smart Protect 网络提供的反馈表明 2 月 4 日可能在同一组织中检测到 Cobalt Strike 信标。这可能是攻击者第一次试图渗透到组织，但没有成功。

2021-02-11 17:13:03	C:\Programdata\sys64.dll	Backdoor.Win64.COBALT.AG	881133d30b9daf58454560ccba6d8900df14cd39
2021-02-11 17:13:03	C:\programdata\sys64.dll	Backdoor.Win64.COBALT.AG	881133d30b9daf58454560ccba6d8900df14cd39
2021-02-11 13:14:59	C:\programdata\sys64.dll	Backdoor.Win64.COBALT.AG	881133d30b9daf58454560ccba6d8900df14cd39
2021-02-04 13:49:23	C:\Program Files (x86)\sys64.dll	Backdoor.Win64.COBEACON.SMA	113ac6b0b8f5f7a5ed5ef800e5a606bf88087fdf
2021-02-04 13:42:30	C:\programdata\sys64.dll	Backdoor.Win64.COBEACON.SMA	113ac6b0b8f5f7a5ed5ef800e5a606bf88087fdf
2021-02-04 13:39:01	C:\programdata\sys64.dll	Backdoor.Win64.COBEACON.SMA	113ac6b0b8f5f7a5ed5ef800e5a606bf88087fdf
2021-02-12 07:07:19	C:\ProgramData\sys64.dll	Backdoor.Win64.COBALT.AG	881133d30b9daf58454560ccba6d8900df14cd39

图 9. 2 月 4 日的反馈

除了这种潜在的攻击之外，我们无法确定初始攻击所使用的任何具体方法。攻击者可能对未受保护或未受监测的端点发起了攻击。

事件响应

正如我们前面提到的，组织通过对端点进行进一步的保护来应对攻击。攻击者似乎已经意识到了这一点。作为回应，他们决定尽快发送敏感信息。

OAT 应用程序显示了一些与“很少访问的 IP 地址”相关的趋势科技 Vision One 的过滤器命中信息，展开详细信息，可以显示它们存储失窃数据的位置。

Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:33:22Z
Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:33:17Z
Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:33:13Z
Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:33:12Z
Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:33:03Z
Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:33:01Z
Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:32:47Z
Low	Rarely Accessed IP Address	Rarely Accessed IP Address	TA0011	T1071	2021-02-12T07:32:46Z
Low	WMI Execute Local Or Remote Process	WMI Execute Local Or Remote Process			2021-02-12T07:04:03Z

图 10.很少访问的 IP 地址警报

开源工具 Rclone 通常用于将文件同步到指定的云存储提供商。在此次事件中，攻击者使用该工具将文件上传到 Mega 云存储。

图 11. 与 Rclone 相关的警报

勒索软件事件发生几天后，又发现了其他 Cobalt/Cobeacon 变种，这表明攻击者仍然可以访问不受保护的端点。

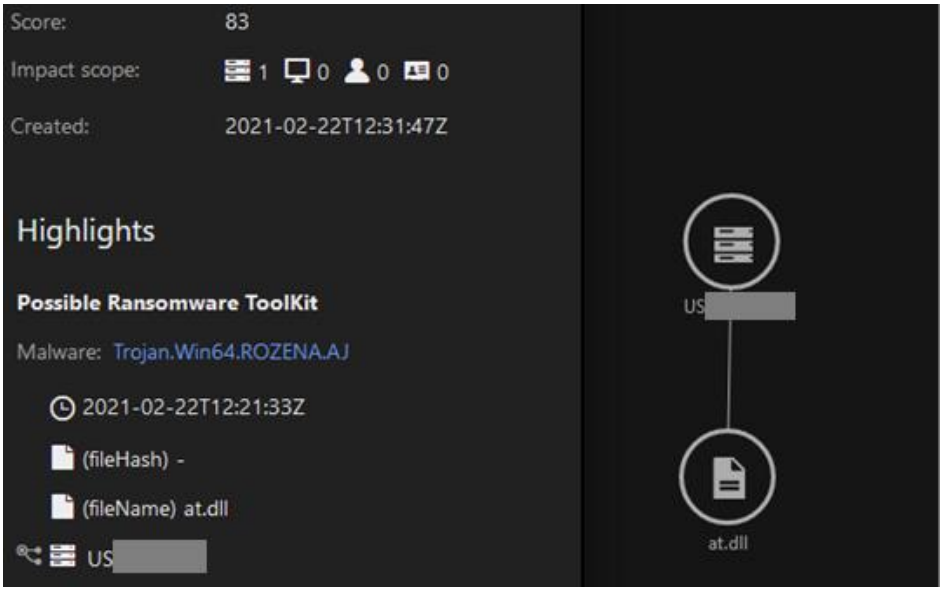


图 12. 与有 Cobalt strike 关的警报

Cobalt Strike 横向运动技术

调查后的时间表如下所示：

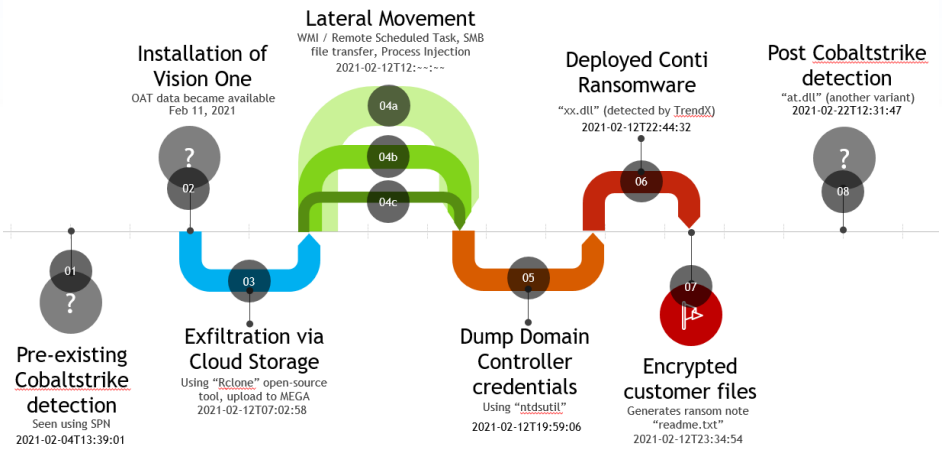


图 13. Conti/Cobaltstrike 攻击的时间表

下面，我们将简要描述 Cobalt Strike 如何能够在网络上传播自己和 Conti 勒索软件。

凭借其从 LSASS 访问和转储凭证哈希的功能，它能够恢复密码并将其用于进一步的移动。

Logged	parentCmd	processFilePath	objectCmd	eventSubId
2021-02-12T20:27:44Z	C:\Windows\system32\cmd.EXE /c C:\Programdata\vd.exe	c:\programdata\vd.exe	C:\Windows\system32\lsass.exe	1 - TELEMETRY_PROCESS_OPEN
2021-02-12T12:25:12Z	C:\Windows\system32\cmd.EXE /c C:\vd.exe	c:\vd.exe	C:\Windows\system32\lsass.exe	1 - TELEMETRY_PROCESS_OPEN
2021-02-12T12:22:16Z	C:\Windows\system32\cmd.EXE /c C:\vd.exe	c:\vd.exe	C:\Windows\system32\lsass.exe	1 - TELEMETRY_PROCESS_OPEN
2021-02-12T12:17:11Z	C:\Windows\system32\cmd.EXE /c C:\Programdata\vd.exe	c:\programdata\vd.exe	C:\Windows\system32\lsass.exe	1 - TELEMETRY_PROCESS_OPEN

图 14. 调用 lsass.exe 的命令

Cobalt/Cobeacon 利用 cmd.exe 复制命令向远程驱动器发送文件。它可以从注入的进程（包括 winlogon.exe、wininit.exe 和 wusa.exe）直接发出，也可以使用批处理脚本作为添加层。

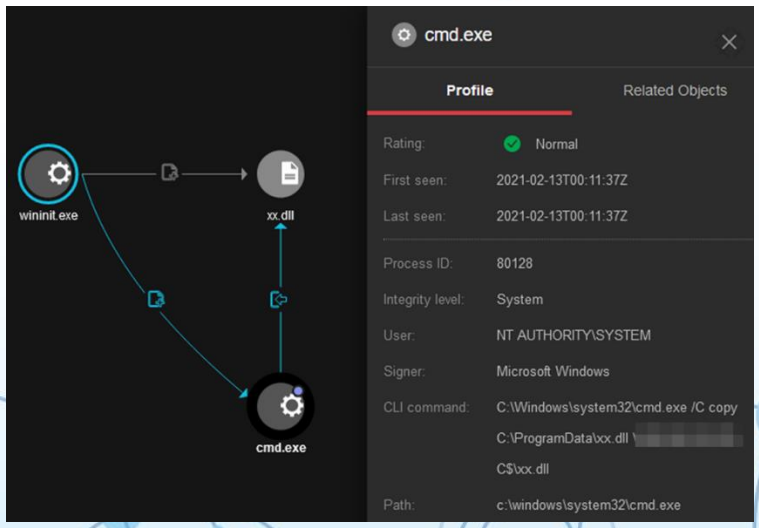


图 15.从注入过程调用的 cmd.exe 命令

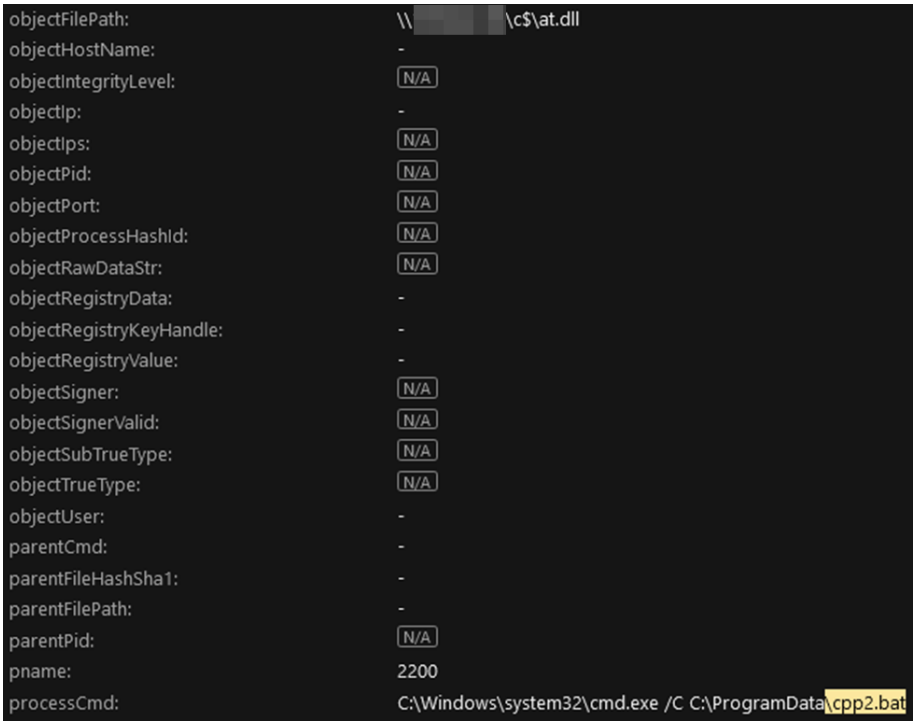


图 16.通过批处理文件/脚本执行

通常将这些组件放置在以下路径中：

```
C:\

C:\ProgramData\

C:\Temp\
```

在远程端点上，文件创建过程将由 ntoskrnl.exe 启动。此行为可以与其它 Cobalt/Cobeacon 行为配对以检查违规行为，或仅用于监控通过此方法创建的文件，该方法试图将文件保存在可疑的路径中。

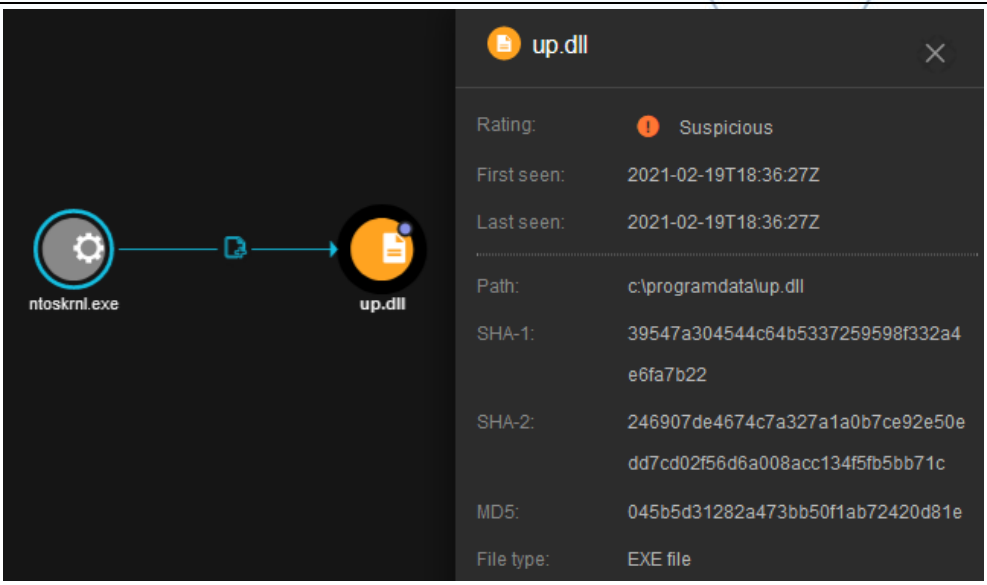


图 17. 通过 ntoskrnl.exe 执行

当它发送命令以在远程端点上执行其自身副本时，也是如此。

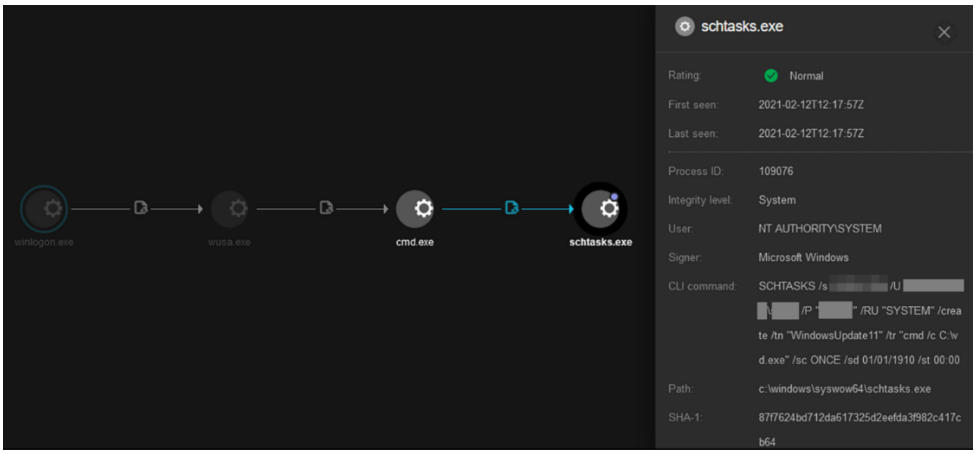


图 18. 在远程端点上执行

除了使用计划任务之外，它还使用 WMI 命令来运行自身的 DLL 或 EXE 副本。

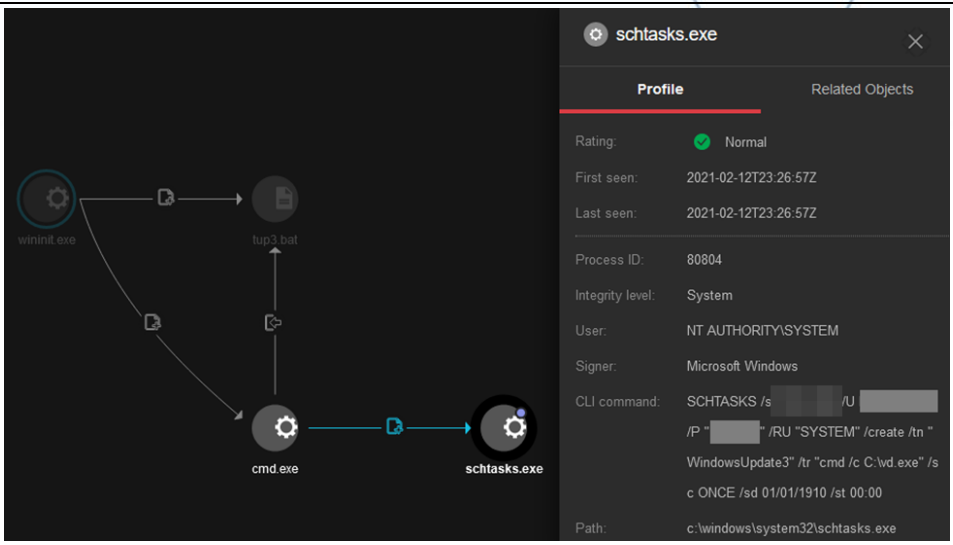


图 19.使用 WMI 运行其自身的副本

安全建议

虽然我们不知道这种威胁是如何进入受害者组织的，但 Conti 以使用网络钓鱼邮件来提供下载恶意软件而闻名，这些恶意软件会投放勒索软件的 Payload。提高威胁预防及相关意识培训将有助于降低风险。

趋势科技全面的 XDR 解决方案将最有效的专家分析应用于从趋势科技解决方案收集的整个企业的深度数据集（包括电子邮件、端点、服务器、云工作负载和网络），从而建立更快的连接以识别和阻止攻击。强大的人工智能（AI）和专家安全分析将客户环境中的数据与趋势科技的全球威胁情报相关联，以提供更简洁、保真度更高的警报，从而更好的实现早期检测。一个控制台与一个优先、优化的警报来源，并支持指导调查，简化了了解攻击路径和对组织的影响所需的步骤。

IOC

文件名	检测	目的	SHA256
sys64.dll	Backdoor.Win64.COBEACON.SMA	Wave 1	无法检索（从 SPN 数据）

tup2.bat	Trojan.BAT.COBALSTART.A	为 s.bat 创建计划任务	4cfb525902490909512d065a59ae820c99ec6129f7ea785d89bc20e7f7384509
tup3.bat	Trojan.BAT.COBALSTART.A	为 vd.exe 创建计划的任务	0043aa3c5236d901333db1a4c9e0fd6e40a27b3f5330bca8a59de78e30758334
s.bat	Trojan.BAT.CONTISTART.A	执行 xx.dll	52c851fc784e175cd2a029abfad62d3bf0408bed85d77d4f94d363e892bc4d60
xx.dll	Ransom.Win64.CONTI.A	用于勒索软件文件加密	cb6eac0222102b6dcb72386aea373e89640f7c3a335591b561e56f35633f2bda
sys64.dll	Backdoor.Win64.COBALT.AG	与 C&C 联系	105d2eef1c6802e2ba3da84afe5ed91e986b55e77fefe1b6a203d3131ead6269
vd.exe/v.exe	Backdoor.Win64.COBALT.AH	与 C&C 联系	c27875b0053bdddbfd121d21dc3cdb8bbf41091c8a8a0614c666aec8b4d3b612
rclone32.exe	N/A	渗透工具	eb03aba46e818640013bfe6b94367cae216a9ad02dabe69f241e3ace3f1a9f37
at.dll	Trojan.Win64.ROZENA.AJ	Wave 3 - Cobalt Strike beacon	1c947639ec826b462e6c36416c873d26c11b081de707d9b5d963e30b59d9234d
up.dll	Trojan.Win64.ROZENA.AJ	Wave 3 - Cobalt Strike	246907de4674c7a327a1a0b7ce92e50edd7cd02f56d6a008acc134f5fb5bb71c

		beacon	
up.dll	Trojan.Win64.ROZENA.AJ	Wave 3 - Cobalt Strike beacon	d1c1e7edc840a0623e0fdc9f2689133339e3ce58da1e24bce513a4673b9ce054

C&C 服务器

IP 地址: 23[.]82[.]128[.]116

域名: secost[.]com

原文链接:

https://www.trendmicro.com/en_us/research/21/c/vision-one-tracking-conti-ransomware.html