VSRC 安全周报（2021-05-25）

0x00 本周漏洞综述

本周需要关注漏洞共 2 个：AMD SEV 安全绕过漏洞（CVE-2021-26311）；Pega Infinity 身份验证绕过漏洞（CVE-2021-27651）。

本周安全态势共 1 个：FireEye：DARKSIDE 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. AMD SEV 安全绕过漏洞（CVE-2021-26311）

SEV（Secure Encrypted Virtualization）是 AMD 提出的安全加密虚拟化技术，它使主内存控制器具备加密功能以对虚拟机内存数据进行保护。

近日，芯片制造商 AMD 针对 SEV 安全绕过漏洞（追踪为 CVE-2020-12967 和 CVE-2021-26311）发布了相关攻击指南。针对这两个漏洞的攻击和相关细节将由相关研究小组在今年的第 15 届 IEEE 进攻技术研讨会（WOOT'21，2021 年 5 月 27 日）上发表。

AMD SEV 可以隔离虚拟机和虚拟机管理程序，但即使使用了适当的保护机制，攻击者也可以利用这两个漏洞者将任意代码注入到虚拟机。

AMD SEV/SEV-ES 任意代码执行漏洞（CVE-2020-12967）

该漏洞是 AMD SEV/SEV-ES 功能中缺乏嵌套页表保护造成的，如果攻击者拥有破坏服务器管理程序的权限，则可能导致 Guest VM 中的任意代码执行。

AMD SEV/SEV-ES 任意代码执行漏洞（CVE-2021-26311）

该漏洞存在于 AMD SEV/SEV-ES 功能中。根据该安全公告，可以在证明机制未检测到的 Guest 地址空间中重新排列内存，如果攻击者拥有破坏服务器管理程序的权限，则可以利用此漏洞制实现 Guest VM 中的任意代码执行。

影响范围

该漏洞影响所有 AMD EPYC 处理器（第一/第二/第三代 AMD EPYC™处理器和 AMD EPYC™嵌入式处理器）

安全建议

目前 AMD 已通过 SEV-SNP 功能修复了此漏洞，但该功能仅在第三代 AMD EPYC™中支持，建议第三代 AMD EPYC™用户尽快应用 SEV-SNP 功能。

相关链接：

https://developer.amd.com/sev/

参考链接：

https://developer.amd.com/sev/

https://uzl-its.github.io/undeserved-trust/

https://securityaffairs.co/wordpress/117981/security/amd-sev-attacks.html?

https://www.ieee-security.org/TC/SP2021/SPW2021/WOOT21/

2. Pega Infinity 身份验证绕过漏洞（CVE-2021-27651）

PEGA（Pega systems）公司是规则驱动流程自动化市场的领导者，业务遍布全球，并专注于大型企业客户，其客户领域涉及医疗保健公司、保险公司、银行、通信服务提供商等。

Pega infinity 是 PEGA 公司的一套企业软件套件，结合了客户参与和数字流程自动化功能，从而降低了复杂性，并可以实现随着数字化转型而发展的可扩展无代码应用程序。

近日，Pega 修复了 Pega infinity 中的一个身份验证绕过漏洞（CVE-2021-27651），该漏洞的 CVSSv3 评分为 9.8。由于重置密码的脆弱验证机制，攻击者可以通过利用本地账户的密码重置功能来绕过本地身份验证检查，最终实现未授权访问或命令执行。

影响范围

Pega Infinity 8.2.1 - 8.5.2

安全建议

目前 Pega 已经修复了此漏洞，建议尽快应用安全更新。

下载链接：

https://collaborate.pega.com/discussion/pega-security-advisory-a21-hotfix-matrix

参考链接：

https://collaborate.pega.com/discussion/pega-security-advisory-a21-hotfix-matrix

https://www.pega.com/infinity

https://nvd.nist.gov/vuln/detail/CVE-2021-27651

0x02 本周安全态势

1. FireEye：DARKSIDE 勒索软件分析

DARKSIDE 勒索软件

DARKSIDE 勒索软件于 2020 年 8 月被首次发现，其背后的运营者及其附属机构曾发起过全球性的犯罪狂潮，并影响了超过 15 个国家的多个行业和组织。与其它勒索软件一样，这些犯罪分子会进行多方面的勒索，如数据窃取、本地加密，以威胁受害者支付解密赎金。

DARKSIDE 勒索软件以勒索软件即服务（RaaS）的形式运作，其利润在其运营者、合作伙伴或附属机构之间分享，后者会向运营组织提供访问权并部署勒索软件。Mandiant（FireEye 的威胁情报平台）目前跟踪了多个部署了该勒索软件的威胁活动集群，这与 DARKSIDE 的关联附属机构一致。这些集群在整个入侵过程中展现出了不同程度的技术复杂性。虽然攻击者通常是利用合法工具进行各个阶段的操作，但至少发现了一个威胁集群还利用了已修复的 0 day 漏洞。

指定目标

通过我们的事件响应以及 DARKSIDE 报告，Mandiant 已经识别出了多个 DARKSIDE 受害者。大多数受害组织都位于美国，并且涉及多个行业，包括金融服务、法律、制造、专业服务、零售和技术。自 2020 年 8 月之后，DARKSIDE 的博客上公开指定的受害人数总体上有所增加，但在 2021 年 1 月期间指定的受害人数明显下降（图 1），这可能是攻击者在假期中休息了。受害人数的整体增长表明，多个附属机构对 DARKSIDE 勒索软件的使用有所增加。

图 1：已知的 DARKSIDE 受害者（2020 年 8 月至 2021 年 4 月）

DARKSIDE 勒索软件服务

从 2020 年 11 月开始，使用俄语的犯罪分子 darksupp 在俄语论坛 exploit.in 和 xss.is 上宣传 DARKSIDE RaaS。2021 年 4 月，darksupp 发布了 Darkside 2.0 RaaS 的更新，其中包括几个新功能和他们目前正在寻找的合作伙伴和服务类型的描述（表 1）。附属机构从每个受害者那里保留一定比例的赎金费用。根据论坛上的描述，RaaS 运营商对低于 50 万美元的赎金收取 25%，但对高于 500 万美元的赎金，这一比例下降到 10%。

除了提供 DARKSIDE 勒索软件的构建，该服务的运营商还维护一个可通过 TOR 访问的博客。犯罪分子利用这个网站来宣传受害者，试图向这些组织施压，以迫使其支付赎金。他们在暗网上最近一次更新的宣传广告也表明，这些犯罪分子可能对受害组织进行 DDoS 攻击。犯罪分子 darksupp 表示，禁止附属机构针对医院、学校、大学、非营利组织和公共部门实体，也禁止以独立国家联合体（CIS）国家的组织作为目标。犯罪分子采取这种措施来避免执法行动，因为针对这些部门的攻击可能会引起更多审查。

宣传广告日期/版本	功能/更新	相关报告
2020 年 11 月 10 日（V1）	能够从管理面板中为 Windows 和 Linux 环境生成构建。	20-00023273 链接： https://advantage.mandiant.com/reports/20-00023273
	使用 Salsa20 加密和 RSA-1024 公钥加密文件。	
	通过 TOR 访问管理面板，客户可以使用 TOR 管理面板来管理 Darkside 版本、付款、博客文章以及与受害者交流。	
	管理面板包括“博客”部分，该部分允许客户将受害者信息和公告发布到 Darkside 网站，以威胁受害者并强迫他们支付赎金要求。	
2021 年 4 月 14 日（V2.0）	自动测试解密。从加密到取款的过程是自动化的，不再依赖于支持。	21-00008435 链接： https://advantage.mandiant.com/reports/21-00008435
	目标可用 DDoS（第 3 层，第 7 层）	
	寻求合作伙伴为他们以及具有渗透测试技能的个人或团队提供网络访问权限。	

表 1：DARKSIDE 广告线（exploit.in）上列出的需要注意的功能和更新。

DARKSIDE 附属机构

DARKSIDE RaaS 附属机构需要通过一个面试，然后才能获得管理面板的访问权（图 2）。在这个面板中，附属机构成员可以执行各种操作，例如创建勒索软件版本、为 DARKSIDE 博客指定内容、管理受害者以及联系支持。Mandiant 上至少确定了五名使用俄语的犯罪分子，这些犯罪分子目前或以前是 DARKSIDE 的子公司。与这些犯罪分子相关的部分广告旨在寻找初始访问供应商或能够在已获得的访问中部署勒索软件的攻击者。据称，一些声称使用 DARKSIDE 的犯罪分子还与其它 RaaS 附属计划合作，包括 BABUK 和 SODINOKIBI（又名 REvil）。

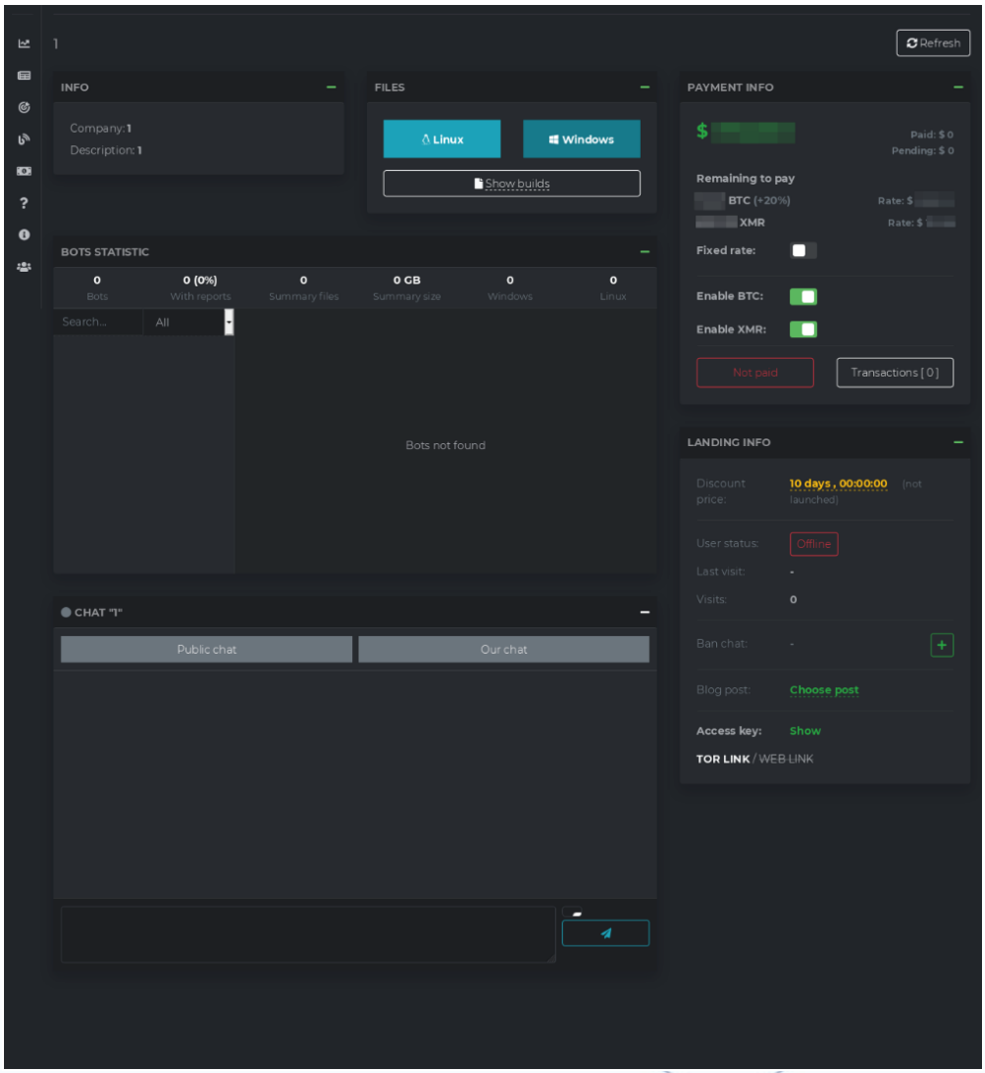


图 2：DARKSIDE 联盟面板

攻击生命周期

当前 Mandiant 上跟踪了五个涉及部署 DARKSIDE 的威胁活动集群，这些集群可能代表 DARKSIDE RaaS 平台的不同分支机构。在观察到的整个事件中，这些犯罪分子通常依赖于各种可公开获得的合法工具，而这些工具通常用于后勒索软件攻击的攻击生命周期中的各个阶段（图 3）。这些 UNC 组（网络入侵活动集群）的其中三个的详细信息如下所示。

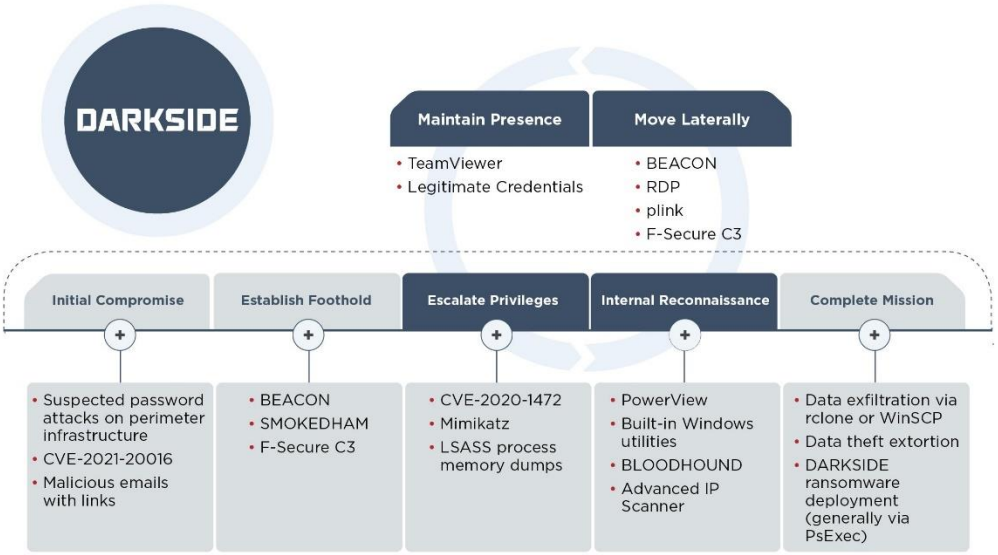


图 3：在 DARKSIDE 勒索软件攻击中发现的 TTP

UNC2628

- UNC2628 自 2021 年 2 月之后一直处于活动状态，其入侵过程相对较快，攻击者通常在两到三天内部署勒索软件。我们有一些证据表明 UNC2628 已经与其它 RaaS 进行了合作，包括 SODINOKIBI（REvil）和 NETWALKER。
- 在多个案例中，我们观察到在交互式入侵行动开始之前，针对企业 VPN 基础设施的可疑认证尝试。这些认证模式与密码喷射攻击相一致，尽管现有的证据不足以将这种前兆活动明确的归于 UNC2628。
- 在有凭证的情况下，攻击者似乎可以使用合法凭据通过公司 VPN 基础结构获得初始访问权限。
- UNC2628 已使用各种合法帐户与受害人环境进行了交互，但在许多情况下，UNC2628 还创建并使用了用户名为'spservice'的域帐户。在所有已知的入侵中，UNC2628 使用了大量 Cobalt Strike 框架和 BEACON Payload。归属于此攻击者的 BEACON 命令和控制（C2）基础结构包括以下内容：

- hxxps://104.193.252[.]197:443/
- hxxps://162.244.81[.]253:443/
- hxxps://185.180.197[.]86:443/
- hxxps://athaliaoriginals[.]com/
- hxxps://lagrom[.]com:443/font.html
- hxxps://lagrom[.]com:443/night.html
- hxxps://lagrom[.]com:443/online.html
- hxxps://lagrom[.]com:443/send.html
- hxxps://lagrom[.]com/find.html?key=id#-

- 在某些情况下，有证据表明犯罪分子使用 Mimikatz 进行凭据盗窃和特权提升。
- 攻击者似乎已经使用诸如“ net”和“ ping”之类的内置命令来执行内部网络的基本侦察，尽管有可能通过 BEACON 进行了额外侦察，但在现有的日志来源中没有体现。
- UNC2628 几乎完全通过 RDP 在环境中使用合法凭据和 Cobalt Strike BEACON Payload 进行了横向移动。这个威胁集群同时使用 HTTPS BEACON Payload 和 SMB BEACON，后者几乎完全使用以“\.\pipe\UIA_PIPE “开头的命名管道。
- 归因于此威胁集群的入侵已经从入侵迅速发展到数据盗窃和勒索软件的部署，因此并不十分注重在受影响的环境中维持一个持久的立足点。 尽管如此，UNC2628 还是通过收集合法凭证、创建攻击者控制的域账户（spservice）以及创建旨在启动 BEACON 的 Windows 服务来保持访问。值得注意的是，UNC2628 多次用名为“CitrixInit“的服务加载 BEACON。
- UNC2628 还采用了 F-Secure 实验室的自定义命令和控制（C3）框架，部署了配置为通过 Slack API 代理 C2 通信的中继。根据犯罪分子的其它 TTP，他们可能使用 C3 来混淆 Cobalt Strike BEACON 流量。
- 该攻击者通过 SFTP 使用 Rclone 将数据泄露到云托管环境中的系统。Rclone 是一个命令行实用程序，用于管理云存储应用程序的文件。值得注意的是，用于数据渗出的基础设施在多次入侵中都被重复使用。在一个案例中，数据泄露发生在入侵开始的同一天。

- UNC2628 使用 PsExec 将 DARKSIDE 勒索软件加密器部署到多个文本文件中包含的主机列表中。
- 攻击者使用了以下目录，在其中放置了后门副本、勒索软件二进制文件、PsExec 副本以及受害者主机列表：
  - C:\run\
  - C:\home\
  - C:\tara\
  - C:\Users\[username]\Music\
  - C:\Users\Public

UNC2659

UNC2659 至少从 2021 年 1 月就开始处于活动状态。我们观察到该攻击者在 10 天内完成了整个攻击周期。UNC2659 值得注意的是，他们使用了 SonicWall SMA100 SSL VPN 产品中的一个漏洞，该漏洞后来被 SonicWall 修复。攻击者似乎是直接从合法的公共网站上下载了攻击生命周期中各个阶段使用的若干工具。

- 攻击者通过利用 CVE-2021-20016，即 SonicWall SMA100 SSL VPN 产品中的一个漏洞获得了初始访问权，目前该漏洞已经修复。有证据表明，攻击者可能利用该漏洞禁用了 SonicWall VPN 的多因素身份认证选项，虽然这一点尚未得到证实。
- 攻击者利用 TeamViewer（TeamViewer_Setup.exe）在受害者环境中建立持久性。现有证据表明，攻击者直接从以下网址下载 TeamViewer，并浏览了可以从中下载 AnyDesk 实用工具的位置：hxxps://dl.teamviewer[.]com/download/version_15x/TeamViewer_Setup.exe。
- 攻击者似乎直接从 rclone[.]org - hxxps://downloads.rclone[.]org/v1.54.0/rclone-v1.54.0-windows-amd64.zip 下载文件 rclone.exe。攻击者被发现使用 rclone 通过 SMB 协议向 pCloud 云端托管和存储服务渗出了数百 GB 的数据。
- 攻击者在受害者环境中部署了 power_encryptor.exe 文件，通过 SMB 协议对文件进行加密并创建赎金票据。

- Mandiant 观察到攻击者在部署勒索软件加密器之前，浏览了 ESXi 管理界面并禁用了快照功能，从而影响了多个 VM 映像。

UNC2465

UNC2465 的活动至少可以追溯到 2019 年 4 月，其特点是他们使用类似的 TTPs 在受害者环境中分发基于 PowerShell 的.NET 后门 SMOKEDHAM。在部署 DARKSIDE 的情况下，存在数月之久的间隔，从初始访问到勒索软件的部署，只有断断续续的活动。在某些情况下，这表明最初的访问可能是由一个单独的攻击者提供的。

- UNC2465 利用钓鱼邮件和合法服务来交付 SMOKEDHAM 后门。SMOKEDHAM 是一个.NET 后门，支持键盘记录、屏幕截图和执行任意.NET 命令。在一次事件中，攻击者似乎与受害者建立了联系，然后发送了恶意的 Google Drive 链接，该链接提供了包含 LNK 下载程序的存档。较新的 UNC2465 电子邮件使用了 Dropbox 链接，其中包含恶意的 LNK 文件的 ZIP 归档，当执行时，该归档文件最终会导致 SMOKEDHAM 被下载到系统中。
- UNC2465 已使用 Advanced IP Scanner、BLOODHOUND 和 RDP 在受害环境中进行内部侦察和横向移动活动。
- 攻击者使用 Mimikatz 进行凭证采集，以提升在受害者网络中的权限。
- UNC2465 还使用公开的 NGROK 工具绕过防火墙，将 RDP 和 WinRM 等远程桌面服务端口暴露在开放的互联网上。
- Mandiant 已经观察到威胁者使用 PsExec 和 cron 任务来部署 DARKSIDE 勒索软件。
- UNC2465 致电受害者的客户支持热线，告诉他们数据被盗，并指示他们遵循赎金记录中的链接。

总结

我们认为，攻击者已经更加熟练地进行了多方面的勒索行动，这直接导致了过去几年中影响严重的勒索软件事件数量的迅速增加。勒索软件运营商已经采用了其它勒索策略，旨在增加受害者默认支付赎金价格的可能性。例如，在 2021 年 4 月底，DARKSIDE 运营商发布了

一份通知，称他们的目标是在纳斯达克和其它股票市场上市的组织，他们表示愿意向股票交易商提供有关即将发生的泄密事件的信息，以便让他们在宣布泄密事件后因股票价格下跌而获得潜在的利润。在另一个值得注意的例子中，一个攻击者能够获得受害者的网络保险单，并在赎金谈判过程中利用这一信息，鉴于他们对保单限额的了解，因此拒绝降低赎金数额。这进一步证明，在勒索软件事件的后开发阶段，攻击者可以进行内部侦察并获取数据以增强其谈判能力。我们预计，攻击者用来向受害者施加压力的勒索策略将在整个 2021 年继续发展。基于 DARKSIDE 勒索软件是由多个附属机构分发的，我们预计与该勒索软件相关的整个事件中所使用的 TTP 将存在一定的差异。

附录 A：DARKSIDE 勒索软件分析

DARKSIDE 是一种用 C 语言编写的勒索软件，可以将其配置为对固定磁盘、可移动磁盘以及网络共享上的文件进行加密。DARKSIDE RaaS 附属机构可以访问管理面板，他们在该面板上为特定的受害者创建构建程序。该面板允许对每个勒索软件构建进行某种程度的自定义，如选择加密模式以及是否应该加密本地磁盘和网络共享（图 4）。以下恶意软件分析基于文件 MD5：1a700f845849e573ab3148daef1a3b0b。最新分析的 DARKSIDE 样本具有以下显著差异：

- 禁用了向 C2 服务器发送 beaconing 的选项，删除了包含 C2 服务器的配置项。
- 包括一种持久性机制。在这种机制中，恶意软件创建并启动自己作为一个服务。
- 包含一组硬编码的受害者凭证，用于尝试作为本地用户登录。如果根据被盗凭证检索到的用户令牌是一个管理令牌，并且是域管理员组的一部分，它将被用于网络枚举和文件权限访问。

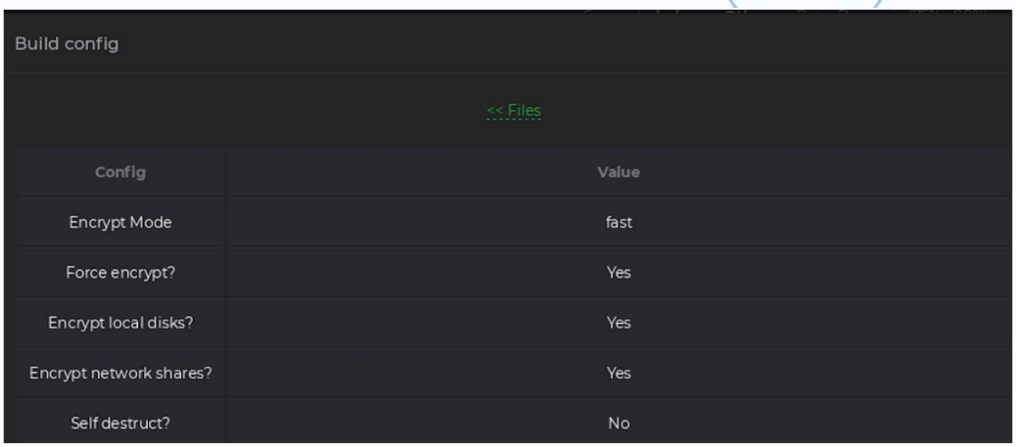


图 4：管理面板中出现的 DARKSIDE 构建配置选项

基于主机的指标

持续机制：

该恶意软件的早期版本不包含持久性机制。如果攻击者需要持久性，则需要外部工具或安装程序。在 2021 年 5 月观察到的 DARKSIDE 版本实现了一个持久性机制，通过该机制，恶意软件创建并启动自己的服务，其服务名称和描述使用八个伪随机定义的小写十六进制字符（例如”.e98fc8f7”）命名，这些字符也被恶意软件附加到它创建的各种其它工件上。 这串字符被称为<ransom_ext>：

Service Name: <ransom_ext>

Description: <ransom_ext>

文件系统工件

创建的文件：

%CD%\LOG<ransom_ext>.TXT

README<ransom_ext>.TXT

<original_filename_plus_ext><ransom_ext>

May version: %PROGRAMDATA%\<ransom_ext>.ico

注册表伪像：

5 月观察到的 DARKSIDE 版本设置了以下注册表项：

HKCR\<ransom_ext>\DefaultIcon\<ransom_ext>\DefaultIcon=%PROGRAMDATA%\<ransom_ext>.ico

细节

配置

该恶意软件会初始化一个 0x100 字节的密钥流，用于解密字符串和配置数据。字符串将根据需要进行解密，并在使用后用 NULL 字节覆盖。该恶意软件的配置大小为 0xBE9 字节，解密后的部分配置的如图 5 所示。

```
00000000  01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.................
00000080  95 AA A8 7C 2B 6A D5 12 0E 73 B3 7D BD 16 25 62  •ª¨|+jÕ..s³}
½.%b
00000090  A4 A8 BF 19 73 F7 E0 BC DF 02 A8 94 32 CF 0C C0
¤¨¿.s÷à¼ß.¨"2Ï.À
000000A0  C5 83 0F 14 66 02 87 EE FD 29 96 DF 02 05 C1 12  Åƒ..f.‡îý)–
ß..Á.
000000B0  3E 43 A7 59 E1 F0 C4 5D AE E1 20 2E 77 D9 CA 3C  >C§YáðÄ]®á
.wÙÊ<
000000C0  AD C6 BC 84 75 1C E7 0B F0 30 2A 51 13 7A B2 66
.Æ¼„u.ç.ð0*Q.z²f
000000D0  44 73 79 E1 E4 69 C3 CA 1B C1 76 63 65 95 EA CA
DsyáäiÃÊ.Ávce•êÊ
000000E0  F6 10 68 0D CE 36 61 F9 57 B9 19 50 31 D4 E1 70
ö.h.Î6aùW¹.P1Ôáp
000000F0  EC 7B 33 1E 4F 17 E1 80 1D BC CF 8C D8 C5 66 41
ì{3.O.á€.¼ÏŒØÅfA
00000100  E5 0A 00 00 02 6E 01 02 15 03 43 01 8E 24 0E 72
å....n....C.Ž$.r
<cut>
```

图 5：部分解密的配置

样本的 0x80 字节的 RSA 公钥 blob 从偏移量 0x80 开始。位于偏移量 0x100 的 DWORD 值被乘以 64，并分配了与结果相等的内存量。从偏移量 0x104 开始的其余字节将被 aPLib 解

压缩到分配的缓冲区中。解压缩的字节包括赎金记录和恶意软件的其它配置元素，如下所述（如终止过程、要忽略的文件）。解压后的前 0x60 字节的配置如图 6 所示。

```
00000000  02 01 01 01 00 01 01 00 01 01 01 01 01 01 01 01
................
00000010  01 01 01 01 01 01 24 00 72 00 65 00 63 00 79 00
......$.r.e.c.y.
00000020  63 00 6C 00 65 00 2E 00 62 00 69 00 6E 00 00 00
c.l.e...b.i.n...
00000030  63 00 6F 00 6E 00 66 00 69 00 67 00 2E 00 6D 00
c.o.n.f.i.g...m.
00000040  73 00 69 00 00 00 24 00 77 00 69 00 6E 00 64 00
s.i...$.w.i.n.d.
00000050  6F 00 77 00 73 00 2E 00 7E 00 62 00 74 00 00 00
o.w.s...~.b.t...
<cut>
```

图 6：部分解压缩的配置

图 6 的第一个字节表示加密模式。这个样本被配置为使用 FAST 模式进行加密。支持的值如下。

- 1：FULL
- 2：FAST
- 其它值：AUTO

图 6 中从偏移量 0x02 到偏移量 0x15 的各个字节是布尔值，决定了恶意软件的行为。恶意软件根据这些值执行表 2 中列出的操作。表 2 还确定了当前样本中启用或禁用的功能。

偏移量	已启用	描述
0x01	Yes	未知
0x02	Yes	加密本地磁盘
0x03	Yes	加密网络共享
0x04	No	执行语言检查
0x05	Yes	删除卷影副本

0x06	Yes	清空回收站
0x07	No	自删除
0x08	Yes	必要时执行 UAC 绕过
0x09	Yes	调整令牌特权
0x0A	Yes	记录中
0x0B	Yes	功能未使用，但导致以下字符串被解密： https://google.com/api/version https://yahoo.com/v2/api
0x0C	Yes	忽略特定的文件夹
0x0D	Yes	忽略特定文件
0x0E	Yes	忽略特定的文件扩展名
0x0F	Yes	功能未使用；与以下字符串有关：“ backup”和“ here_backups”
0x10	Yes	未使用功能：与以下字符串相关：“ sql”和“ sqlite”
0x11	Yes	终止流程
0x12	Yes	停止服务
0x13	Yes	功能未使用；与包含重复字符串“ blah”的缓冲区有关
0x14	Yes	投下赎金票据
0x15	Yes	创建一个 mutex

表 2：配置位

UAC 绕过

如果恶意软件没有提升权限，它就会试图根据操作系统（OS）版本执行两种用户账户控制（UAC）绕过方法中的一种。如果操作系统早于 Windows 10，恶意软件会使用已记录的 slui.exe 文件处理程序劫持技术。这包括将注册表 HKCU\Software\Classes\exefile\shell\opencommand\Default 设置为恶意软件路径，并使用“runas”执行 slui.exe。

如果操作系统版本是 Windows 10 或更新版本，恶意软件会尝试使用 CMSTPLUA COM 接口进行 UAC 绕过。图 7 中列出的解密字符串被用来执行此技术。

```
Elevation:Administrator!new:
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
```

图 7：解密的 UAC bypass 字符串

加密设置

该恶意软件根据系统的 MAC 地址生成一个伪随机文件扩展名。在 2021 年 5 月观察到的 DARKSIDE 版本中，文件扩展名是使用 MachineGuid 注册表值作为种子而不是 MAC 地址生成的。文件扩展名由八个小写的十六进制字符组成（如“.e98fc8f7”），被称为<ransom_ext>。文件扩展名的生成算法已在 Python 中重新创建。如果启用了日志记录，恶意软件会在其当前目录下创建日志文件 LOG<ransom_ext>.TXT。

该恶意软件支持命令行参数“-path”，攻击者可以利用此参数指定要加密的目录。

我们分析的样本没有被配置为执行系统语言检查。如果该功能被启用且检查成功，字符串“This is a Russian-Speaking System，Exit“将被写入日志文件，恶意软件将退出。

防恢复技术

该恶意软件在系统上定位并清空回收站。如果该进程在 WOW64 下运行，它将使用

CreateProcess 执行图 8 中的 PowerShell 命令以删除卷影副本。

```
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]
('0x'+'4765742D576D694F626A6563742057696E33325F536861646F7763
6F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex
$s"
```

图 8：编码的 PowerShell 命令

图 8 中的解码命令为 “Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}”。 如果恶意软件不是在 WOW64 下运行，它就会使用 COM 对象和 WMI 命令来删除卷影副本。图 9 中的解密字符串用于简化这一过程。

```
root/cimv2
SELECT * FROM Win32_ShadowCopy
Win32_ShadowCopy.ID='%s'
```

图 9：与删除卷影副本相关的的解密字符串

系统操纵

任何名称包含图 10 中所列字符串之一的服务都会被停止并删除。

```
vss
sql
svc$
memtas
mepocs
sophos
veeam
backup
```

图 10：与服务相关的字符串

在 2021 年 5 月观察到的版本还被配置为停止和删除包含图 11 中列出的字符串的服务。

```
GxVss
GxBlr
GxFWD
GxCVD
GxCIMgr
```

图 11：5 月版本中与服务相关的其它字符串

任何包含图 12 中所列字符串之一的进程名称都被终止。

```
sql
oracle
ocssd
dbsnmp
synctime
agntsvc
isqlplussvc
xfssvccon
mydesktopservice
ocautoupds
encsvc
firefox
tbirdconfig
mydesktopqos
ocomm
dbeng50
sqbcoreservice
excel
infopath
msaccess
mspub
onenote
outlook
powerpnt
steam
thebat
thunderbird
visio
winword
wordpad
notepad
```

图 12：与流程相关的字符串

文件加密

根据其配置，该恶意软件以固定磁盘、可移动磁盘以及网络共享为目标。一些进程可能被终止，因此相关文件可以被成功加密。但是，该恶意软件并没有终止图 13 中列出的进程。

```
vmcompute.exe
vmms.exe
vmwp.exe
svchost.exe
TeamViewer.exe
explorer.exe
```

图 13：不被终止的进程

该恶意软件使用图 14 中列出的字符串，在加密过程中忽略某些目录。

```
windows
appdata
application data
boot
google
mozilla
program files
program files (x86)
programdata
system volume information
tor browser
windows.old
intel
msocache
perflogs
x64dbg
public
all users
default
```

图 14：用于忽略目录的字符串

图 15 中列出的文件将被忽略。

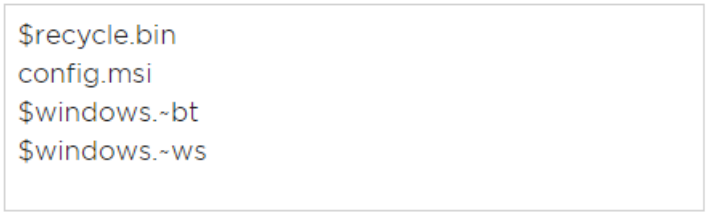


图 15：被忽略的文件

在 2021 年 5 月观察到的版本被额外配置为忽略图 16 中列出的文件。

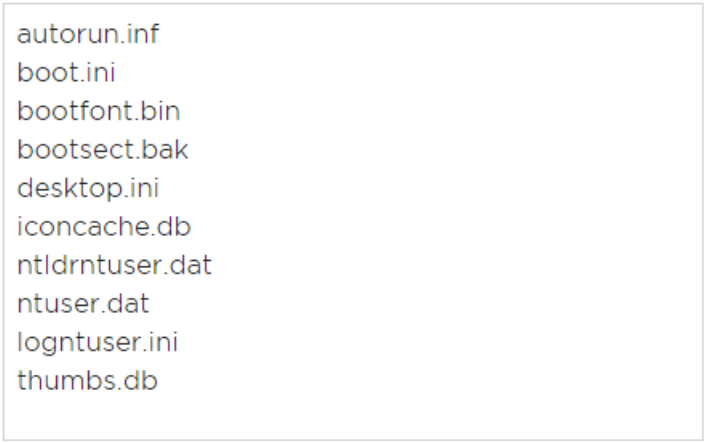


图 16：5 月版本中其它被忽略的文件

根据图 17 中列出的扩展名，其它文件将被忽略。

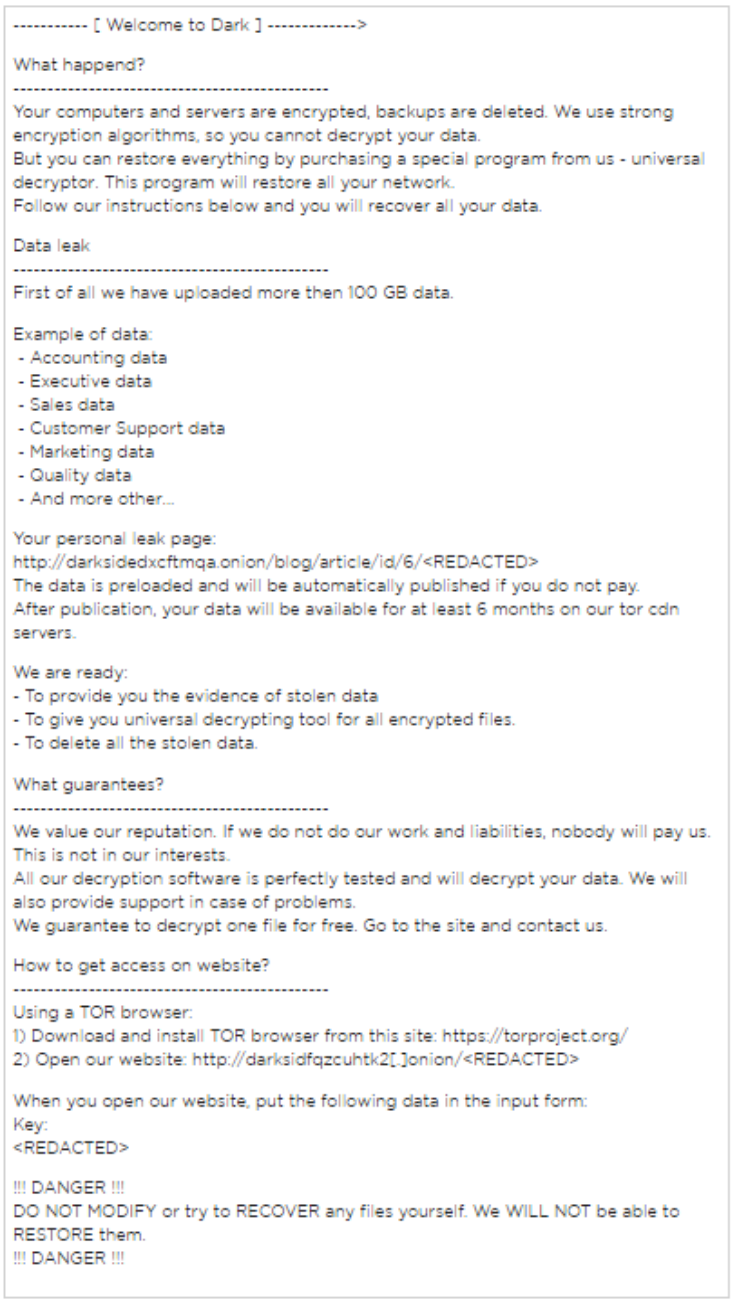
图 17：文件扩展名

文件使用 Salsa20 进行加密，并使用 RtlRandomEx 随机生成一个密钥。每个密钥都使用嵌入式 RSA-1024 公钥进行加密。

赎金票据

该恶意软件将图 18 中所示的赎金记录写入 README 〈ransom_ext〉 .TXT 文件，该文件

将写入其遍历的目录中。



---------- [Welcome to Dark] ---------->

What happend?

Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak

First of all we have uploaded more then 100 GB data.

Example of data:
- Accounting data
- Executive data
- Sales data
- Customer Support data
- Marketing data
- Quality data
- And more other...

Your personal leak page:
http://darksidedxcftmqa.onion/blog/article/id/6/<REDACTED>
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.

What guarantees?

We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?

Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2[.]onion/<REDACTED>

When you open our website, put the following data in the input form:
Key:
<REDACTED>

!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!

图 18：赎金票据

解密的字符串

```
Global\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
https://google.com/api/version
https://yahoo.com/v2/api
sql
sqlite
$recycle.bin
config.msi
$windows.~bt
$windows.~ws
windows
appdata
application data
boot
google
mozilla
program files
program files (x86)
programdata
system volume information
tor browser
windows.old
intel
msocache
perflogs
x64dbg
public
all users
default
386
adv
ani
bat
bin
cab
cmd
com
cpl
cur
deskthemepack
diagcab
diagcfg
diagpkg
dll
drv
exe
hlp
icl
icns
```

图 19：解密的字符串（1）

```
ico
ics
idx
ldf
lnk
mod
mpa
msc
msp
msstyles
msu
nls
nomedia
ocx
prf
psl
rom
rtp
scr
shs
spl
sys
theme
themepack
wpx
lock
key
hta
msi
pdb
vmcompute.exe
vmms.exe
vmwp.exe
svchost.exe
TeamViewer.exe
explorer.exe
oracle
ocssd
dbsnmp
synctime
agntsvc
isqlplussvc
xfssvccon
mydesktopservice
ocautoupds
encsvc
firefox
tbirdconfig
mydesktopqos
ocomm
```

图 19：解密的字符串（2）

dbeng50
sqbcoreservice
excel
infopath
msaccess
mspub
onenote
outlook
powerpnt
steam
thebat
thunderbird
visio
winword
wordpad
notepad
vss
sql
svc$
memtas
mepocs
sophos
veeam
backup
\r\nblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblah\r\nblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblah\r\nblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblah\r\nblahblahblah\r\n
\r\n---------- [Welcome to Dark] ---------->\r\n\r\nWhat happend?\r\n----------\r\nYour computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.\r\nBut you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.\r\nFollow our instructions below and you will recover all your data.\r\n\r\nData leak\r\n----------\r\nFirst of all we have uploaded more then 100 GB data.\r\n\r\nExample of data:\r\n - Accounting data\r\n - Executive data\r\n - Sales data\r\n - Customer Support data\r\n - Marketing data\r\n - Quality data\r\n - And more other...\r\n\r\nYour personal leak page: http://darksidedxcftmqa[.]onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wkw2inG8O72jWaOcKbrxMWbPfKrUbHC\r\nThe data is preloaded and will be automatically published if you do not pay.\r\nAfter publication, your data will be available for at least 6 months on our tor cdn servers.\r\n\r\nWe are ready:\r\n- To provide you the evidence of stolen data\r\n- To give you universal decrypting tool for all encrypted files.\r\n- To delete all the stolen data.\r\n\r\nWhat guarantees?\r\n----------\r\nWe value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.\r\nAll our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.\r\nWe guarantee to decrypt one file for free. Go to the site and contact us.\r\n\r\nHow to get access on website? \r\n----------\r\nUsing a TOR browser:\r\n1) Download and install TOR browser from this site: https://torproject.org/\r\n2) Open our website: http://darksidfqzcuhtk2[.]onion/<REDACTED>\r\n\r\nWhen you open our website, put the following data in the input form:\r\nKey:\r\<REDACTED>\r\n\r\n!!! DANGER !!!\r\nDO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them. \r\n!!! DANGER !!!\r\n
-path

图 19：解密的字符串（3）

```
INF
DBG
/C DEL /F /Q
 >> NUL
ComSpec
README
.TXT
Start Encrypting Target Folder
Encrypt Mode - AUTO
Started %u I/O Workers
Encrypted %u file(s)
Start Encrypt
[Handle %u]
File Encrypted Successful
Encrypt Mode - FAST
Encrypt Mode - FULL
This is a Russian-Speaking System, Exit
System Language Check
Encrypting Network Shares
Encrypting Local Disks
README
.TXT
Encrypt Mode - AUTO
Started %u I/O Workers
Encrypted %u file(s)
Start Encrypt
[Handle %u]
File Encrypted Successful
Encrypt Mode - FAST
Encrypt Mode - FULL
Terminating Processes
Deleting Shadow Copies
Uninstalling Services
Emptying Recycle Bin
This is a Russian-Speaking System, Exit
System Language Check
Start Encrypting All Files
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]
('0x'+'4765742D576D694F626A6563742057696E33325F53686I646F7763
6F7079207C20466F72456I63682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2
"$_,2))};iex $s"
root/cimv2
WQL
SELECT * FROM Win32_ShadowCopy
ID
Win32_ShadowCopy.ID='%s'
.exe
LOG%s.TXT
README%s.TXT
Software\Classes\exefile\shell\open\command
\slui.exe
runas
Elevation:Administrator!new:
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
explorer.exe
```

图 19：解密的字符串（4）

附录 B：检测和搜寻指标

Yara 检测

以下 YARA 规则不建议在生产系统上使用，除非组织先通过内部的测试流程进行验证，以确保适当的性能并限制误报的风险。这些规则旨在识别相关活动，但如果恶意软件家族发生变化，它们需要进行相应的调整。

```
rule Ransomware_Win_DARKSIDE_v1__1
{
    meta:
        author = "FireEye"
        date_created = "2021-03-22"
        description = "Detection for early versions of DARKSIDE ransomware
samples based on the encryption mode configuration values."
        md5 = "1a700f845849e573ab3148daef1a3b0b"
    strings:
        $consts = { 80 3D [4] 01 [1-10] 03 00 00 00 [1-10] 03 00 00 00 [1-
10] 00 00 04 00 [1-10] 00 00 00 00 [1-30] 80 3D [4] 02 [1-10] 03 00 00 00
[1-10] 03 00 00 00 [1-10] FF FF FF FF [1-10] FF FF FF FF [1-30] 03 00 00
00 [1-10] 03 00 00 00 }
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and
$consts
}
```

图 20：DARKSIDE YARA 规则

```
rule Dropper_Win_Darkside_1
{
    meta:
        author = "FireEye"
        date_created = "2021-05-11"
        description = "Detection for on the binary that was used as the dropper leading to
DARKSIDE."
    strings:
        $CommonDLLs1 = "KERNEL32.dll" fullword
        $CommonDLLs2 = "USER32.dll" fullword
        $CommonDLLs3 = "ADVAPI32.dll" fullword
        $CommonDLLs4 = "ole32.dll" fullword
        $KeyString1 = { 74 79 70 65 3D 22 77 69 6E 33 32 22 20 6E 61 6D 65 3D 22 4D 69 63 72 6F
73 6F 66 74 2E 57 69 6E 64 6F 77 73 2E 43 6F 6D 6D 6F 6E 2D 43 6F 6E 74 72 6F 6C 73 22 20 76 65
72 73 69 6F 6E 3D 22 36 2E 30 2E 30 2E 30 22 20 70 72 6F 63 65 73 73 6F 72 41 72 63 68 69 74 65
63 74 75 72 65 3D 22 78 38 36 22 20 70 75 62 6C 69 63 4B 65 79 54 6F 6B 65 6E 3D 22 36 35 39 35
62 36 34 31 34 34 63 63 66 31 64 66 22 }
        $KeyString2 = { 74 79 70 65 3D 22 77 69 6E 33 32 22 20 6E 61 6D 65 3D 22 4D 69 63 72 6F
73 6F 66 74 2E 56 43 39 30 2E 4D 46 43 22 20 76 65 72 73 69 6F 6E 3D 22 39 2E 30 2E 32 31 30 32
32 2E 38 22 20 70 72 6F 63 65 73 73 6F 72 41 72 63 68 69 74 65 63 74 75 72 65 3D 22 78 38 36 22
20 70 75 62 6C 69 63 4B 65 79 54 6F 6B 65 6E 3D 22 31 66 63 38 62 33 62 39 61 31 65 31 38 65 33
62 22 }
        $Slashes = { 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C }
    condition:
        filesize < 2MB and filesize > 500KB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) ==
0x00004550 and (all of ($CommonDLLs*)) and (all of ($KeyString*)) and $Slashes
}
```

图 21：DARKSIDE Dropper YARA 规则

```
rule Backdoor_Win_C3_1
{
    meta:
        author = "FireEye"
        date_created = "2021-05-11"
        description = "Detection to identify the Custom Command and
Control (C3) binaries."
        md5 = "7cdac4b82a7573ae825e5edb48f80be5"
    strings:
        $dropboxAPI = "Dropbox-API-Arg"
        $knownDLLs1 = "WINHTTP.dll" fullword
        $knownDLLs2 = "SHLWAPI.dll" fullword
        $knownDLLs3 = "NETAPI32.dll" fullword
        $knownDLLs4 = "ODBC32.dll" fullword
        $tokenString1 = { 5B 78 5D 20 65 72 72 6F 72 20 73 65 74 74 69 6E
67 20 74 6F 6B 65 6E }
        $tokenString2 = { 5B 78 5D 20 65 72 72 6F 72 20 63 72 65 61 74 69
6E 67 20 54 6F 6B 65 6E }
        $tokenString3 = { 5B 78 5D 20 65 72 72 6F 72 20 64 75 70 6C 69 63
61 74 69 6E 67 20 74 6F 6B 65 6E }
    condition:
        filesize < 5MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) ==
0x00004550 and (((all of ($knownDLLs*)) and ($dropboxAPI or (1 of
($tokenString*)))) or (all of ($tokenString*)))
```

图 22：自定义命令和控制（C3）YARA 规则

检测 DARKSIDE

FireEye 产品在攻击生命周期的多个阶段检测到这种活动。下表包含旨在识别和防止恶意软件的特定检测以及在这些入侵中发现的方法。为了简洁，此列表不包括 FireEye 对 BEACON、BloodHound/SharpHound 以及在此活动和广泛的入侵操作中发现的其它常见工具和恶意软件的现有检测。

平台	检测名称
网络安全 电子邮件安全 按需检测 恶意软件分析 文件保护	● Ransomware.SSL.DarkSide ● Trojan.Generic ● Ransomware.Linux.DARKSIDE ● Ransomware.Win.Generic.MVX

	● Ransomware.Win.DARKSIDE.MVX ● Ransomware.Linux.DARKSIDE.MVX ● Ransomware.Win32.DarkSide.FEC3 ● FE_Ransomware_Win_DARKSIDE_1 ● FE_Ransomware_Win32_DARKSIDE_1 ● FE_Ransomware_Linux64_DARKSIDE_1 ● FE_Ransomware_Linux_DARKSIDE_1 ● FEC_Trojan_Win32_Generic_62 ● FE_Loader_Win32_Generic_177 ● FE_Loader_Win32_Generic_197 ● FE_Backdoor_Win_C3_1 ● FE_Backdoor_Win32_C3_1 ● FE_Backdoor_Win32_C3_2 ● FE_Backdoor_Win_C3_2 ● Backdoor.Win.C3 ● FE_Dropper_Win_Darkside_1
端点安全	Real-Time（IOC） ● BABYMETAL（后门） ● DARKSIDE RANSOMWARE（家族） ● 可疑的 PowerShell 用法（方法） ● 可疑的 Powershell 用法 B（方法） 恶意软件防护（AV/MG） ● Generic.mg.* ● Gen:Heur.FKP.17 ● Gen:Heur.Ransom.RTH.1 ● Gen:Trojan.Heur.PT.omZ@bSEA3vk

	● Gen:Variant.Razy.* ● Trojan.CobaltStrike.CB ● Trojan.GenericKD.* ● Trojan.Linux.Ransom.H UAC 保护 ● 检测到恶意 UAC 绕过程序
Helix	● VPN 分析[异常登录] ● WINDOWS 分析[异常 RDP 登录] ● TEAMVIEWER CLIENT [用户代理] ● WINDOWS 方法论[Plink 反向隧道] ● WINDOWS 方法论-服务[PsExec]

相关指标

UNC2628

指标	描述
104.193.252[.]197:443	BEACON C2
162.244.81[.]253:443	BEACON C2
185.180.197[.]86:443	BEACON C2
athaliaoriginals[.]com	BEACON C2
lagrom[.]com	BEACON C2
ctxinit.azureedge[.]net	BEACON C2

45.77.64[.]111	登录源
181ab725468cc1a8f28883a95034e17d	BEACON 样本

UNC2659

指标	描述
173.234.155 [.] 208	登录源

UNC2465

指标	描述
81.91.177 [.] 54：7234	远程访问
koliz [.] xyz	文件托管
los-web [.] xyz	EMPIRE C2
sol-doc [.] xyz	恶意基础架构
hxxp：// sol-doc [.] xyz / sol / ID-482875588	下载网址
6c9cda97d945ffb1b63fd6aabcb6e1a8	下载器 LNK
7c8553c74c135d6e91736291c8558ea8	VBS 启动器
27dc9d3bcffc80ff8f1776f39db5f0a4	Ngrok 实用程序

DARKSIDE 勒索软件加密器

DARKSIDE MD5 样本

04fde4340cc79cd9e61340d4c1e8ddfb

0e178c4808213ce50c2540468ce409d3

0ed51a595631e9b4d60896ab5573332f

130220f4457b9795094a21482d5f104b

1a700f845849e573ab3148daef1a3b0b

1c33dc87c6fdb80725d732a5323341f9

222792d2e75782516d653d5cccfcf33b

29bcd459f5ddeeefad26fc098304e786

3fd9b0117a0e79191859630148dcdc6d

47a4420ad26f60bb6bba5645326fa963

4d419dc50e3e4824c096f298e0fa885a

5ff75d33080bb97a8e6b54875c221777

66ddb290df3d510a6001365c3a694de2

68ada5f6aa8e3c3969061e905ceb204c

69ec3d1368adbe75f3766fc88bc64afc

6a7fdab1c7f6c5a5482749be5c4bf1a4

84c1567969b86089cc33dccf41562bcd

885fc8fb590b899c1db7b42fe83dddc3

91e2807955c5004f13006ff795cb803c

9d418ecc0f3bf45029263b0944236884

9e779da82d86bcd4cc43ab29f929f73f

a3d964aaf642d626474f02ba3ae4f49b

b0fd45162c2219e14bdccab76f33946e

b278d7ec3681df16a541cf9e34d3b70a

b9d04060842f71d1a8f3444316dc1843

c2764be55336f83a59aa0f63a0b36732

c4f1a1b73e4af0fbb63af8ee89a5a7fe

c81dae5c67fb72a2c2f24b178aea50b7

c830512579b0e08f40bc1791fc10c582

cfcfb68901ffe513e9f0d76b17d02f96

d6634959e4f9b42dfc02b270324fa6d9

e44450150e8683a0addd5c686cd4d202

f75ba194742c978239da2892061ba1b4

f87a2e1c3d148a67eaeb696b1ab69133

f913d43ba0a9f921b1376b26cd30fa34

f9fc1a1a95d5723c140c2a8effc93722

原文链接：

https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html