总体威胁态势

在此处下载完整的英文报告

Talos 在 2022 年整体威胁格局中观察到的几个主要趋势。根据 Cisco Talos Incident Response 检测中的遥测和案例研究，我们观察到威胁发起者活动存在以下趋势：采用流行红队工具的破解版/泄露版；使用离地攻击二进制文件 (LoLBins)，例如 PowerShell 和 Microsoft PS Exec；以及 USB 攻击有所增加。

两用工具

开发恶意工具会占用大量资源，并且可能会导致威胁发起者暴露行踪。为了避免这些高昂成本并额外增加一层匿名性，许多攻击者转用攻击性框架和红队框架，以支持整个攻击生命周期间的一系列操作。

Cobalt Strike 仍然是网络威胁发起者的常用选项（图 **1**）。这种合法的网络防御工具和威胁仿真软件功能齐全，包括侦察、漏洞利用活动和各种攻击模拟，因此对于攻击者而言是一款极具功能实用性的工具。

多年来，Talos 和安全社区一直在使用 Cobalt Strike，不断开发更有效、更可靠的检测方法。在这一年里，我们还看到威胁发起者通过改用其他攻击性框架（例如 Sliver 和 Brute Ratel）来适应这些形势变化（图 **2**）。

此外，Talos 还发现了威胁发起者为自身目的而开发的两个独立式攻击性框架，分别称为“Manjusaka”和“Alchimist”。Alchimist 已在广泛使用，虽然在撰写本文时我们尚未观察到 Manjusaka 被广泛使用，但全球威胁发起者很有可能会使用它。

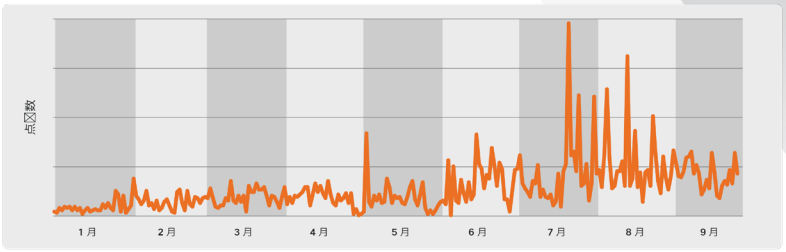

图 ***1.*** *Cisco Secure Endpoint* 针对 *Cobalt Strike* 命名的管道使用情况的检测。

Cobalt Strike

- 这是一种合法的网络防御工具和威胁仿真软件，功能齐全，包括侦察、后渗透活动和各种攻击包，因此对于攻击者而言是一款极具功能实用性的一款工具。
- 信标作为 Cobalt Strike 的负载，用于通过 HTTP、HTTPS 或 DNS 生成攻击和创建出站流量。可以将 Cobalt Strike 信标与作为 Metasploit 框架一部分的 Meterpreter 进行比较，渗透测试人员和攻击性安全研究人员在提供服务时使用这些信标

Brute Ratel

- 2020 年发布的一款成熟的合法红队工具，用作攻击仿真工具。此后，威胁发起者一直利用它来为攻击生命周期的各个阶段提供支持。
- Brute Ratel 是专门为躲避终端检测和响应 (EDR) 以及防病毒 (AV) 解决方案的检测而设计的

Sliver

- 一种可用于执行安全测试的开源红队框架和攻击仿真工具。Sliver 的植入程序使用每个二进制文件的非对称加密密钥进行动态编译，并通过多种协议（mTLS、HTTP、DNS）支持 C2。
- MacOS、Windows 和 Linux 支持 Sliver 植入程序。Sliver 有多种功能，包括分阶段和无阶段负载、动态代码生成、命名管道数据透视、内存中 .NET 程序集执行等。

图 ***2.*** 常见两用工具的比较。

总体威胁态势

离地攻击二进制文件

离地攻击二进制文件 (LoLBins) 是预装在操作系统上的合法实用程序和工具，经常遭到攻击者滥用。由于这些工具本质上属于可信工具，主要用于常规活动，因此网络防御者在监控恶意行为时可能会忽视利用 LoLBins 发起的攻击。我们不断看到攻击者在各个攻击阶段利用合法工具和实用程序来支持其行动。

根据我们的遥测数据，25 个最常用的 Cisco Secure Endpoint Behavioral Protection 签名中有 4 个与 PowerShell 相关，突出表明威胁发起者始终依赖此原生 Windows 实用程序进行恶意攻击 (**图 3**)。攻击者通常使用 PowerShell 来支持一系列活动，包括安装 ChromeLoader 等广告软件、下载加密货币挖掘程序或利用 Elasticsearch 等软件中的漏洞发起攻击。

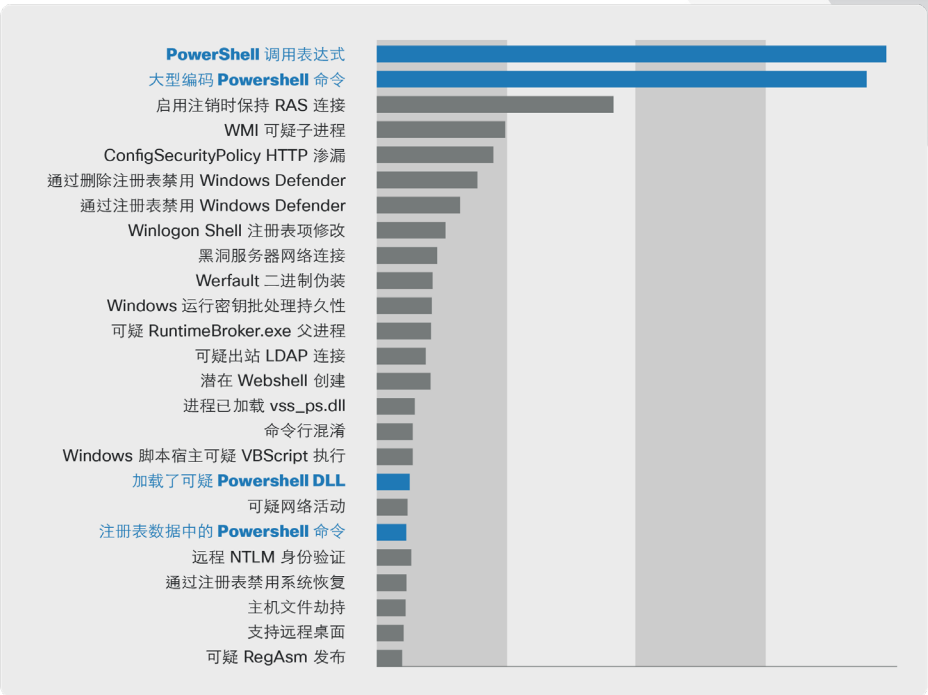

图 ***3.*** 排名前 *25* 的最活跃 *Cisco Secure Endpoint Behavioral Protection* 签名。

USB 威胁

通过可移动存储设备传播恶意软件的攻击方式可以追溯到软盘驱动器时期。在整个 2022 年，Talos 观察到 Cisco Secure Malware Analytics 中针对各种 USB 和外部驱动器相关行为的检测均有所增长，突出表明攻击者对这种过时但有效的策略屡试不爽。这些行为包括将可执行文件写入 USB 驱动器或对 USB 驱动器上的文件设置隐藏属性，使其一直不被检测到 (**图 4 和图 5**)。

这种增长一定程度上是由于 Raspberry Robin 恶意软件所致，其可在使用共享 USB 驱动器的设备之间进行传播。但是，我们也观察到 APT 组织使用 USB 驱动器访问作为其攻击途径。

通过观察 2022 年的形势，我们发现，USB 攻击已卷土重来，攻击者将调整其策略，以在企业将注意力从旧攻击途径上转移开时乘虚而入。

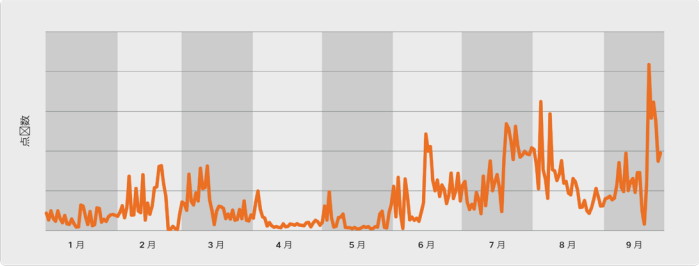

图 ***4.*** 针对用于写入 *USB* 的可执行文件的 *Cisco Secure Malware Analytics* 检测。

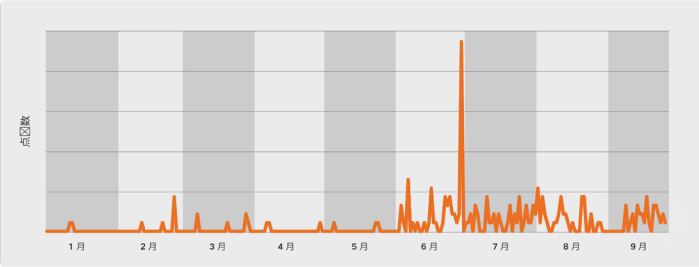

图 ***5.*** 针对为 *USB* 设备上文件设置隐藏属性的 *Cisco Secure Malware Analytics* 检测。