防御当今的关键威胁

威胁报告（发布时间：2019 年 2 月）

CISCO

目录

回顾过去，展望未来

面对当今威胁形势，务必要像开车一样经常看一下后视镜。

这样不仅可以清楚了解后面的路况，还能经常快速发现后车是否要超车。

本威胁报告的作用就在于此。我们选出了过去一年左右发生的五个重要案例，不仅因为它们是重大事件，还因为我们认为这些威胁或类似威胁很可能在不久后再次出现。

以模块化的威胁为例，比如 Emotet 木马和 VPNFilter。这些威胁可以按需发起攻击和威胁，具体取决于受感染的设备或攻击者的预期目标。我们在最近的记录中发现了大量这类模块化的威胁，如果将来出现更多这样的威胁，也丝毫不足为奇。

邮件仍然是备受攻击者青睐的传播媒介，无论是对于加密货币挖矿还是对于使用邮件进行传播的 Emotet 等威胁，皆是如此。其他威胁（例如未经授权的 MDM 配置文件）也很可能使用邮件进行传播。这也强调了密切关注通过邮箱传入的内容的重要性。

作案手法

牟利仍然是攻击者的主要动机：恶意软件专为牟利而生。例如，加密货币挖矿威胁的唯一目标就是牟利。与此同时，Emotet 已经转向威胁分销网络，利用各种方式来牟利。

数据泄露也成为人们关注的焦点。这是最近许多威胁的主要动机，例如 VPNFilter，它似乎是为了窃取信息而存在的。Emotet 木马除了通过窃取网络凭证来进行自我传播外，我们还发现它传播另一种常见的信息窃取银行木马 Trickbot。

我们挑选出了五个重要的案例，因为我们认为这些威胁或其他类似的威胁可能会再次出现。

最后，有些威胁只是想在全球制造恐慌，奥运会毁灭者 (Olympic Destroyer) 恶意程序就是一个典型的例子。在过去的一年中，我们看到了许多类似的威胁，但没有一个像奥运会毁灭者一样抢占头条新闻，其唯一的目的似乎就是破坏冬季奥运会。

因此，当我们回顾 2018 年的一些影响巨大的威胁时，务必要注意使这些威胁破坏力如此惊人的原因。其中许多威胁现在可能已经进入您的视线，但是您是否将它们甩开了，还是它们的演变速度太快，让您和您的安全策略防不胜防？

面对当今威胁形势，务必要像开车一样经常看一下后视镜。这样不仅可以清楚了解后面的路况，还能经常快速发现后车是否要超车。

攻击类型和保护

我们始终建议采用分层的安全方法。我们在每个案例的结尾都添加了一些图标，用于指示各个案例中攻击者使用（或可能使用）的关键威胁媒介以及有助于防御这些威胁的工具。下面我们来介绍一下这些图标，并探讨在集成式安全架构中部署各种保护措施的好处。

高级恶意软件检测和保护技术（例如思科高级恶意软件防护 [AMP]）可以跟踪未知的文件，阻止已知的恶意文件，并防止在终端和网络设备上执行恶意软件。

思科下一代防火墙 (NGFW) 和思科下一代入侵防御系统 (NGIPS) 等**网络安全解决方案**可以检测试图通过互联网进入网络或在网络中移动的恶意文件。网络可视性和安全分析平台（例如思科 Stealthwatch）可以检测出可能表示恶意软件正在激活其负载的内部网络异常情况。最后，网络分段可以防止威胁在网络中横向移动，并遏制攻击的传播。

在安全 Web 网关 (SWG) 或**安全互联网网关 (SIG)**（例如思科 Umbrella）上**进行 Web 扫描**，可阻止用户连接恶意域、IP 和 URL（无论用户是否位于公司网络上）。这可以防止用户无意中允许恶意软件访问网络，并且可以阻止侥幸进入了网络的恶意软件返回连接命令和控制 (C2) 服务器。

邮件安全技术（例如思科邮件安全）无论部署在企业内部还是云环境中，皆可阻止威胁发起者通过发送恶意邮件来发起攻击活动。这样可以减少垃圾邮件的总量，删除恶意垃圾邮件，并扫描邮件的所有部分（如发件人、主题、附件和嵌入的 URL），以找出包含威胁的邮件。这些功能至关重要，因为邮件仍然是威胁发起者发起攻击的头号媒介。

高级恶意软件检测和防护技术（例如面向终端的思科 AMP）可以防止在终端上执行恶意软件。它还可以帮助隔离、调查和修复受感染的终端，处理绕过最强防御措施的 1% 的攻击。

Emotet 的演变：从银行木马到网络威胁分销商

Emotet 木马已经悄然活动了多年。这种策略非常有效。

说起威胁形势，最博人眼球的总是那些新的威胁，例如：研究人员发现了某种影响大量设备的漏洞，或者某个大型组织遭到了某种针对性攻击。

但是，一些最常见的威胁反而不那么引人注意。它们可能会依赖经过测试和验证的方法，而不是最新的、最强大的技术。这会无意中助长攻击者的实力。大家熟视无睹的威胁有可能会增长，而更受关注的威胁反而可能不会增长。

Emotet 就是一个典型例子。在媒体对 WannaCry 和 NotPetya 这类威胁的讨论此起彼伏时，Emotet 却悄然活动了多年。这种策略非常有效，因为 Emotet 已经发展成为当今影响力最大的威胁系列之一。

Emotet 的成功在于它的演进方式。它开始时只是“微不足道”的银行木马，后来威胁发起者迅速转向使这种威胁成为能够执行各种不同攻击的模块化平台。如今，曾经将其视为竞争对手的其他威胁系列纷纷用它来传播自己的恶意软件。随着威胁形势再次发生变化，Emotet 似乎正在成为众人瞩目的焦点。

从岌岌无名演变为模块化平台

Emotet 首次登场时，只是若干银行木马中的一种。此威胁通过垃圾邮件活动进行传播，通常使用的是发票或付款主题的垃圾邮件。它通常作为启用了宏的 Office 文档、JavaScript 文件或恶意链接附加在邮件内。尽管许多攻击活动都以特定地区 - 特别是欧洲的德语国家/地区和美国的银行为目标，但传播技术却各不相同。

起初，这种威胁主要窃取银行信息：用户名、密码、邮箱地址和其他财务详情。随着时间的推移，Emotet 开始向更广泛的受众传播。新的威胁版本为我们今天看到的模块化配置奠定了

邮件：最常见的威胁媒介

说起如今的主要威胁，大多数都绕不过邮件这一媒介。它仍然是威胁发起者传播其病毒是最常用的感染媒介，并且近期仍然会保持这种势头。

以 Emotet 木马为例。一周接一周，该威胁背后的攻击者不断发起新的网络钓鱼活动。

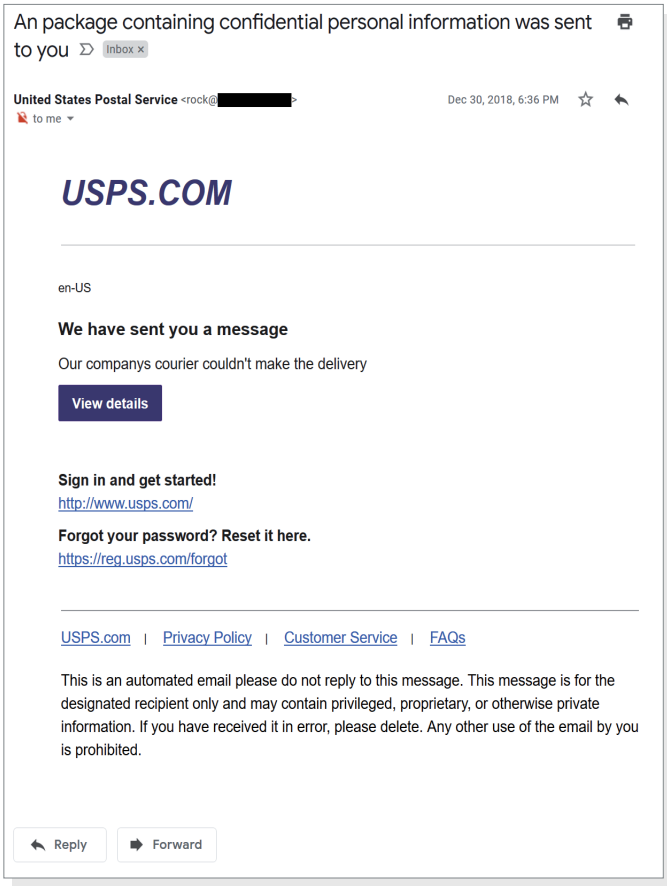
恶意加密货币挖矿威胁也是如此，频繁通过垃圾邮件活动诱使用户将挖矿软件下载到他们的计算机上。

而移动设备管理 (MDM) 威胁，似乎有可能通过社交工程邮件开始发起攻击。

（续）

基础，其中包含不同的工具，用于处理不同的功能。某些模块会窃取邮件凭证，而其他模块则重点窃取存储在浏览器中的用户名和密码。某些模块会提供分布式拒绝服务 (DDoS) 功能，而其他模块会分发勒索软件。

图 1　Emotet 的垃圾邮件样本



而这一点也丝毫不足为奇，因为很多网络钓鱼邮件在设计上具有欺骗性，尤其是在手机上查看时更是如此。对于忙碌的用户来说，邮件传达的风险和紧迫性可能会导致收件人立即采取行动，而忽视了正在伺机发起攻击的异常威胁迹象。

毫无疑问，攻击者会继续使用邮件来帮助他们传播恶意软件。

逐利而生

Emotet 的主要目的是想方设法通过受感染的计算机获利，方法就是利用模块。看起来，似乎在特定设备上安装何种模块取决于模块最大限度利用受感染设备获利的方式。请考虑以下情形:

- 计算机浏览器历史记录是否显示经常访问银行网站？如果是，那就部署银行模块，以窃取凭证和转账。
- 受感染设备是否是高端笔记本电脑，这很可能表明目标受害者收入很高？如果是，那就部署恶意软件分发模块并安装勒索软件或加密货币挖矿软件。
- 设备是否是高带宽网络上的服务器？如果是，那就安装邮件和网络分发模块，并进一步传播 Emotet。

盗亦有道

Emotet 之所以能够在如今多如牛毛的威胁格局中占有一席之地，不仅是因为它影响范围广并且具有模块化特性，还因为该威胁背后的攻击者似乎在向其他攻击者团伙推广这种分销渠道。

例如，我们观察到 Emotet 感染计算机后，它向系统植入的负载却是 Trickbot。这看似有点矛盾，因为 Emotet 自身就是众所周知的银行木马，但它却在植入其他银行木马，而不是利用自己的信息窃取模块。更有趣的是，Trickbot 被 Emotet 植入后，有时会植入 Ryuk 勒索软件。

尽管看起来很奇怪，但不同团伙之间似乎在进行合作，原因可以简单地归结为这样一个事实：联手可以获得最大的利润。如果 Emotet 无法利用某部设备进行进一步传播，Trickbot 可以从设备中盗取银行记录。如果没有找到银行记录，Ryuk 可以对设备进行加密，要求受害者支付赎金。当然，这种狼狈为奸的联盟能够持续多久，仍是未知数。

未来的发展势头

当然，威胁的发展演进很少能够不被外界察觉。在 2018 年的最后几个月内，安全行业研究人员突然开始注意到 Emotet 的规模。它之所以引起了注意，是因为垃圾邮件分发者似乎纷纷从传播加密货币挖矿恶意软件转向分发 Emotet 和远程访问木马 (RAT)。至此，它的影响已不容小觑。事实上，根据美国计算机应急响应小组 (US-CERT) 的信息，一些 Emotet 感染需要高达 100 万美元的费用才能清理掉。

Emotet 背后的攻击者似乎在向其他攻击者团伙推广这种分销渠道。

在可预见的未来，Emotet 不太可能会消失，并可能会称霸威胁榜单。鉴往知来，Emotet 终将退出舞台，逐渐被威胁格局中的其他主导者所取代。

如需深入了解此话题，请访问以下链接：

https://blog.talosintelligence.com/2019/01/return-of-emotet.html

https://www.us-cert.gov/ncas/alerts/TA18-201A

https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html

物联网攻击动机浅析：VPNFilter

Talos 提供的图片

VPNFilter 是未来几乎不可避免的恶意软件。

过去十年中，出现了许多与物联网 (IoT) 相关的威胁。Mirai 僵尸网络就是其中之一，该威胁会感染 IP 摄像头和路由器，从而发起 DDoS 攻击。谁能忘记入侵婴儿监视器的黑客，父母走进幼儿园后，却听到入侵设备的黑客与孩子交谈？

无论大家喜欢与否，从智能助手到连接互联网的医院设备，物联网早已渗透到我们的家庭和企业中。遗憾的是，在许多情况下，在此过程中，大家都忽略了适当的安全措施。因此，我们看到恶意攻击者针对此类设备发起攻击。

但是，没有哪种威胁的破坏力能超过 VPNFilter。这种威胁以多家制造商提供的大量路由器为目标，可能利用未打补丁的漏洞来侵入这些路由器。其目的之一似乎是从被它感染病毒的网络中泄漏敏感数据，但它还包含一个模块化系统，能够发起更多攻击，这就特别令人担忧。

总而言之，分布在 54 个国家/地区的至少 50 万台设备感染了这种威胁。幸运的是，思科 Talos 团队的研究人员很早就发现了该威胁。当感染加剧时，他们已准备好遏制该威胁。如今，得益于公私部门威胁情报合作伙伴和执法部门的共同努力，VPNFilte 带来的威胁已基本消除。尽管如此，在近期 VPNFilter 仍然是几乎不可避免的恶意软件。

VPNFilter 的攻击过程

第一阶段 - VPNFilter 威胁分为三大部分，或“阶段”。第一阶段的主要目标是在设备中建立持久控制。在 VPNFilter 出现前，通常只需重新启动物联网设备即可清除针对这些设备的恶意软件。在 VPNFilter 的第一阶段中，恶意软件成功实现了此目标。第一阶段还包括多个连接命令和控制 (C2) 服务器的选项，该服务器负责向恶意软件发布命令。

第二阶段 - 第二阶段是实现 VPNFilter 恶意目标的核心部分，具有收集文件、执行命令、泄漏数据和管理设备等功能。某些版本的第二阶段甚至包括一个 “终止开关”，如果激活它，可能会使受感染的设备永远无法使用。

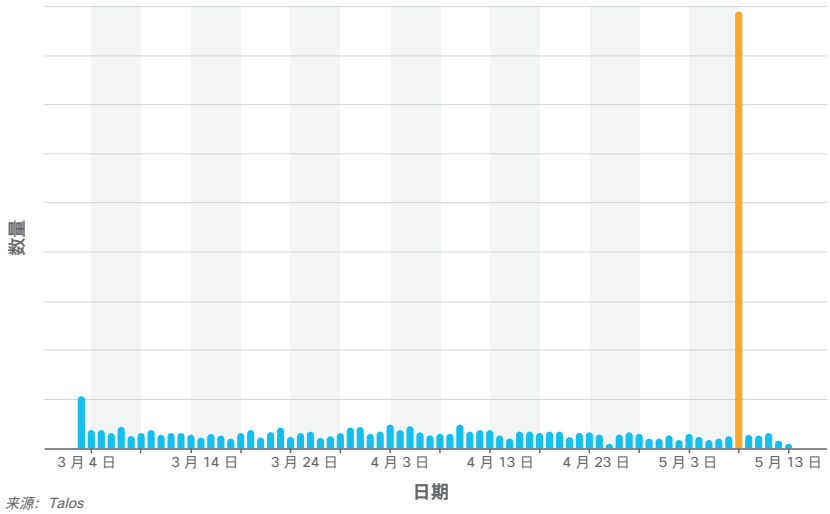
第三阶段 - 第三阶段扩展了第二阶段的功能，提供插件以辅助执行进一步的恶意操作。一些值得注意的插件具备以下功能:

- 监控网络流量
- 窃取各种凭证
- 监控特定工业物联网设备的流量
- 加密与 C2 服务器的通信
- 映射网络
- 利用终端系统的漏洞发起攻击
- 扩散到其他网络
- 发起 DDoS 攻击
- 构建可用于隐藏未来攻击源的代理网络

VPNFilter（基本）清除

Talos 团队几个月来一直在研究 VPNFilter，它的感染率相当稳定。该团队一直在监控和扫描受感染的设备，以便更好地了该解恶意软件中包含的威胁和功能。

图 2 新型 VNPFilter 感染随时间推移的发展状况



来源：Talos

直到 2018 年 5 月 8 日，感染活动出现了剧增。不仅如此，该团队还发现大多数感染活动都发生在乌克兰。紧接着，5 月 17 日，乌克兰爆发了第二波大规模 VPNFilter 感染，此时接近 NotPetya 出现一周年。由于乌克兰遭受过破坏性攻击，因此尽管研究仍在进行中，Talos 团队认为最好尽快解决这一基础设施攻击。

Talos 团队继续研究和发布有关该僵尸网络的信息，直到 2018 年 9 月，团队终于能够公布该威胁已被遏制。

不可忘却的威胁

遗憾的是，虽然 VPNFilter 可能已被消除，但在物联网设备中仍然会发现其他漏洞。迟早总会出现另一种针对物联网的威胁，这几乎是不可避免的。

抵御这类威胁绝非易事。诸如路由器之类的物联网设备通常直接连接到互联网。再加上许多用户要么不具备修复漏洞的专业技术知识，要么不认为它们是威胁，这种情况非常危险。

最后，作为网络一部分的物联网设备数量只会继续增长。VPNFilter 向我们表明，如果我们不采取适当措施保护这些设备，未来可能会发生什么情况。

如需深入了解此话题，请访问以下链接：

https://blog.talosintelligence.com/2018/05/VPNFilter.html

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html

遗憾的是，虽然 VPNFilter 可能已被消除，但在物联网设备中仍然会发现其他漏洞。迟早总会出现另一种针对物联网的威胁，这几乎是不可避免的。

移动设备管理：福祸相依

Talos 团队发现恶意攻击者已经知道了如何将 MDM 用于恶意目的。

移动设备管理 (MDM) 功能对企业来说是一个福音。利用它，组织可以更充分地控制其网络中的设备。然而，正如我们在 2018 年发现的那样，它也为资金充足的恶意攻击者打开了大门。

谈到移动恶意软件，移动操作系统可能是一个难以破解的难题。围绕移动操作系统创建的“围墙”在很大程度上能够保护它免受恶意应用的侵害。

这并不是说，恶意攻击者尚未试图攻击手机。官方应用商店中已经发现了恶意应用，但在大多数情况下，攻击者活动仅限于感染已解锁或“越狱”的设备，或者允许第三方应用的设备。

因此，虽然围墙可以确保安全，但同时也可能成为一座监狱。此种局限及其提供的安全性的缺点是，您只能从官方应用商店安装应用，或者在可以的情况下将设备保持对所有第三方应用开放。如果企业想要构建只允许自身员工访问的专有应用，但同时也希望确保其设备的安全，这就会给他们带来难题。

MDM 的推出

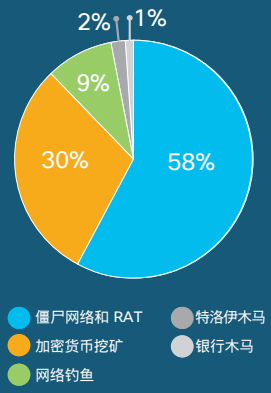
为了解决这一需求，MDM 系统应运而生。利用这种系统，企业能够使用公司移动电话，安装注册到其公司的配置文件，并最终安装他们选择的应用。MDM 通常还提供其他企业友好功能，例如控制设备设置，防止访问不需要的网站或查找丢失的设备等功能。

安全事件概览

组织面临的最常见安全事件是什么？思科认知情报小组的同事为我们提供了数据。以下列出了从 2018 年 7 月收集的五种主要安全事件的概况。

总体来说，僵尸网络和 RAT 是最主要的安全事件。此类别的威胁包括 Andromeda 和 Xtrat 等。

第二大威胁类别是加密货币挖矿软件，其中包含未公布且未经授权的 Monero 和 Coinhive 挖矿软件以及其他恶意软件。



在此概况中，最引人注意的是银行特洛伊木马所占的比例较小。随着 Emotet 活动的加剧，这无疑会发生变化。

我们将在未来的报告中重新分析此指标，以了解其变化情况。

Talos 提供的图片

毫无疑问，MDM 是一种强大的工具。强大到足以让攻击者都想要利用它，思科 Talos 团队发现恶意攻击者已经知道了如何将其用于恶意目的。

始于印度

我们的 Talos 研究人员在印度发现了通过开源 MDM 系统感染的设备。攻击者设法将恶意配置文件放到设备上并推送各种应用，目的是拦截数据，窃取短信，下载照片和联系人，以及跟踪设备的位置等。

这些应用包括 WhatsApp 和 Telegram 等流行应用的修改版本，其中添加或者“搭载”了额外的功能，让攻击者可以监控每台受感染设备上的对话。

这些设备如何陷入这种攻击仍然是一个迷。攻击者可能对这些设备进行了物理访问，趁机安装了一个赋予他们控制权限的配置文件。但是，攻击者也可能使用社交工程手段诱骗用户安装这种配置文件。

他们可能通过邮件或短信向用户发送恶意警报，试图欺骗用户，让他们以为自己需要安装这种恶意配置文件。即便如此，用户仍需要遵循一系列说明，点击一些提示，才会导致设备完全被攻破。

防御系统趋势预测

毫无疑问，这是一种强有力的攻击方法。幸运的是，它也很少见。Talos 发现的这种攻击活动是唯一公开已知的此类攻击活动。这种攻击活动执

考虑到此类攻击可能给攻击者带来的回报，我们预计未来会看到更多由资金充足的威胁攻击者发起的此类攻击。

行起来也很困难，因为它需要让用户执行很多步骤，从而为恶意活动配置设备。但考虑到潜在的回报，资金充足的威胁发起者还是会发起更多的移动设备攻击，而且 Talos 团队已经发现了这种情况。

讽刺的是，防止恶意 MDM 的最佳保护措施竟然也是利用 MDM。

组织应确保公司设备安装业界推出的相关配置文件，这些配置文件可以监控和防止安装来自第三方应用商店的恶意配置文件或应用。

此外，务必也要让用户了解 MDM 安装过程和这类攻击，以避免他们安装恶意 MDM。

如需深入了解此话题，请访问以下链接：

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM-Part2.html

勒索软件风云突变

早在 2017 年，看起来似乎勒索软件将在很长一段时间内主宰威胁格局。SamSam 和 Bad Rabbit 这类威胁占据了媒体头条，要求受害者支付加密货币，否则受害者会丢失所有数据。

而一年多之后，形势确实发生了变化。

勒索软件已被其他威胁 - 主要是恶意的加密货币挖矿超越。

为什么形势会突变？利用勒索软件，攻击者只能获得一小部分受害者支付赎金。即使他们支付了赎金，也只是一次性付款，而不会成为经常性收入来源。

与此同时，世界各地的执法机构开始打击勒索软件攻击者，这增加了他们面临的风险。随着与勒索软件有关的逮捕行动的增加，攻击者逐渐改为发起风险较小的其他类型攻击。

这并不是说勒索软件已经消失；2018 年，我们仍然看到了一些此类攻击。GandCrab 继续兴风作浪，Ryuk 通过 Emotet 和 Trickbot 感染进行传播。因此，勒索软件虽不再是影响力最大的恶意软件，但它仍然存在，需要保持警惕以避免此威胁再度爆发。

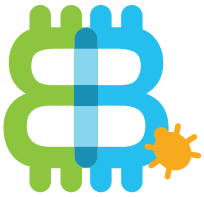
加密货币挖矿：披着羊皮的狼仍然是一匹狼

到目前为止，2018 年最突出的以牟利为目的的威胁形式是恶意加密货币挖矿。在过去一段时间里，思科 Talos 威胁情报团队就这一主题开展了大量研究。对于攻击者而言，这几乎是完美的犯罪：挖矿软件经常在用户不知情的情况下在后台工作，窃取他们的计算能力，为攻击者创造收入。

随着企业能够更好地处理勒索软件，并且全世界的执法机构开始打击勒索软件攻击者，越来越多的攻击者逐渐转为兜售风险较低的恶意加密货币挖矿软件。

当羊遇到狼

通常，用户自行安装的加密货币挖矿软件与恶意攻击者安装的加密货币挖矿软件之间并无太大差异。细微差别在于，恶意加密货币挖矿软件是在所有者不知情的情况下进行挖矿活动的。这便是攻击者十分看重的一个优势，他们可以在受害者不知情的情况下窃取利益。



用户自行安装的加密货币挖矿软件与恶意攻击者安装的加密货币挖矿软件之间并无太大差异。

在顶风冒险追本逐利的各种活动中，加密货币挖矿引起执法部门的注意的可能性更小。相反，任何在设备所有者不知情的情况下运行的软件都会让人感到不安。

加密货币挖矿，不论是否恶意，都可以带来丰厚的收益。在过去几年和 2018 年上半年，加密货币的价值不断攀升。正如其他任何与软件相关的有价事物一样，加密货币也引起了恶意攻击者的关注。另一方面，勒索软件的效益却大不如从前，这进一步促使攻击者转向加密货币。加密货币挖矿会产生经常性收入，而勒索软件通常只能获得受害支付一次性赎金。

恶意加密货币挖矿活动的危险

从防御者的角度来看，我们有充分的理由认为恶意加密货币挖矿值得高度关注。与计算机上的任何软件一样，恶意加密货币将对整体系统性能产生负面影响，并且需要额外的功率。就单个系统而言，电力成本的增加可能并不明显。但如果将其乘以组织中终端的数量，电力成本将会显著增加。

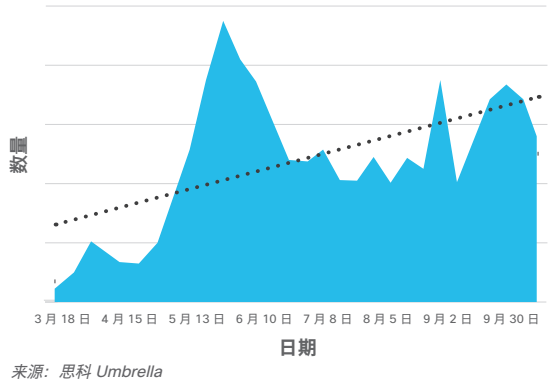
此外，加密货币矿工利用公司网络赚取收益也会造成合规性问题。对金融业的组织而言则更是如此，因为无论相关负责人是否知晓此类活动，使用公司资源创造收益的行为都受到严格的限制。

不过，也许最令人担忧的问题是，用户并不知道系统被恶意加密货币挖矿软件感染，他们在不知情的情况下运行网络时，这些恶意软件可能会导致网络配置或整体安全策略出现安全漏洞。而此类漏洞很容易被攻击者利用，谋取其他利益。那么，如果发现网络被加密货币挖矿软件感染，可以采取哪些基本措施来阻止其他恶意威胁利用相同的漏洞来进一步实施恶意活动呢？

现在发生了什么变化？

虽然存在走势陡峭的波峰和波谷，但从思科在 DNS 层上观察到的与加密货币挖矿管理相关的流量总量看来，随着时间的推移，加密货币挖矿活动呈上升趋势。

图 3 企业 DNS 加密货币挖矿流量



来源：思科 Umbrella

值得注意的是，在同一时期，许多常见加密货币的价值都出现下滑。其中一个例子是 Monero，这是恶意加密货币挖矿活动中常用的一种虚拟货币。

图 4 Monero 成交价

来源：coinmarketcap.com

由于该虚拟货币易于部署且发现之后造成的风险较低，恶意攻击者仍在继续推动恶意加密挖矿活动。事实上，加密货币挖矿软件安装在设备上后，只要它存在，就可以不断为恶意攻击者牟利。

恶意加密货币挖矿软件是如何感染系统的呢？

恶意加密货币挖矿软件可以通过各种方式进入您的环境，例如：

- 利用漏洞
- 发送包含恶意附件的邮件
- 使用僵尸网络
- 通过 Web 浏览器进行加密货币挖矿活动
- 利用恶意广告软件安装浏览器插件
- 内部恶意攻击者

遗憾的是，在近期内，恶意加密货币挖矿威胁会一直存在。垃圾邮件分发者可能会继续传播加密货币挖矿威胁。

加密货币挖矿软件可能会在网络管理员不知情的情况下，指向网络中的其他安全漏洞。

从过去到未来，牟利一直是恶意攻击者的主要动机。在许多方面，攻击者都可以将恶意加密货币挖矿活动视为一种以较少的开销快速牟利的途径。这非常正确，因为与其他威胁相比，目标受害者对恶意加密货币挖矿威胁的影响的关注更少。对于狼来说，披着羊皮看着利润滚滚而来，再完美不过了。

如需深入了解此话题，请访问以下链接：

https://blogs.cisco.com/security/cryptomining-a-sheep-or-a-wolf

https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html

https://blog.talosintelligence.com/2018/12/cryptomining-campaigns-2018.html

万众瞩目

在本报告中，我们研究了各种各样的威胁。虽然报告并未包含所有类型的威胁，但我们计划在未来几个月通过我们的每月威胁博客系列探讨以下主题。以下是即将发布的主题概览：

数字化勒索。最近一次更为阴险的网络钓鱼活动通过利用收件人的恐惧来勒索比特币。一些攻击者给收件人发邮件，声称他们通过摄像头捕获了其观看色情网站的证据。其他的包括虚假炸弹威胁。最终，这些威胁完全都是捏造的，全都是为了欺骗大量收件人向攻击者支付更多比特币。

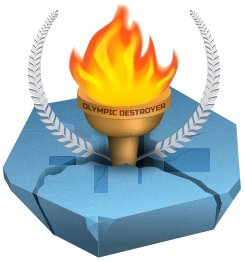
Office 365 网络钓鱼。另一种重要的网络钓鱼活动是围绕窃取 Microsoft Office 365 账户的凭证展开的。攻击者使用了许多方法来实现这一目标。我们即将发布的博客文章中将概述不同的攻击活动以及如何识别这些活动。

要及时了解我们的月度威胁博客系列，请务必订阅我们的邮件列表并访问 “每月威胁” 页面。

订阅：http://cs.co/9002ERAWM

每月威胁：
http://cisco.com/go/threatofthemonth

冬天来了：奥运会毁灭者



Talos 提供的图片

虽然这种奥运会攻击可能是一次性的，但其背后的团队并不会就此罢手。

去年一开年就不太平。原本网络安全专家对 WannaCry 和 NotPetya 两波冲击带来的影响仍心有余悸，希望新年伊始可以度过一段相对平静的日子。但是，很快这种希望就破灭了，因为 Talos 团队发现 2018 年韩国平昌冬季奥运会开幕式的网络中断是恶意软件引起的。

这种恶意软件具有高度破坏性，可以根据所入侵的环境进行定制。虽然奥运会毁灭者这个名称可能是针对那届奥运会活动而取的，但它所造成的威胁依然存在。

在那届冬季奥运会开幕式期间，体育场和媒体区域的 Wi-Fi 突然中断，并且官方网站也受到了网络中断的影响。这样大规模的网络中断会带来无数挑战，包括数据隐私风险、品牌声誉受损以及客户满意度下降。

最终，可以明显判断出这次网络中断是一次网络攻击事件，长期调查表明该恶意软件有两个特征：1) 它是一种擦除器恶意软件，目的是破坏资产（而不是作为勒索软件执行攻击），2) 更有趣的是，它经过精心设计以隐藏其来源并欺骗研究人员。这波高级攻击结合了复杂的恶意软件技术与狡猾的策略。

奥运会毁灭者究竟是如何实施破坏的？

奥运会毁灭者的传播方式还有待推测。目前比较明确的是，一旦进入目标网络，它就会在该网络中传播，并且速度很快。

根据平昌袭击事件的后果，我们分析认为最可能的情况是，这种威胁像蠕虫一样传播：快速且具有高度破坏性。该威胁文件会窃取密码，清除备份数据，并以存储在服务器上的数据为目标，在非常短的时间内造成巨大的破坏。

奥运会毁灭者极具破坏性，并且专门用于摧毁信息。

攻击者使用合法工具执行横向移动，此次事件中所用的工具是 PsExec（一种允许您在远程计算机上运行程序的 Windows 协议）。由于此次攻击爆发的时间恰逢奥运会开幕式，因此它是远程触发的。

奥运会毁灭者可能希望通过使用与其他威胁发起者相关的旧代码片段来掩盖其编写者的身份。有些安全研究人员也受到了这种误导，其中有些人甚至由此断定此次攻击就是那些旧代码编写者所为。

还会有更多威胁发生...

虽然奥运会毁灭者恶意软件实际动机尚不明确，但是思科 Talos 团队发现此次事件是老练的高级攻击者所为。这就说明，尽管奥运会毁灭者是一种定制的攻击，其幕后团队并不会就此罢手。他们可能会再次使用这种高效的方法来制造进一步的混乱，或进行盗窃或做其他坏事。因此，在防御这种性质的恶意软件时，我们需要保持警惕。

2018 年就是这样开始的。我们衷心希望 2019 年举办任何其他重大盛会时都不会出现任何恶意和复杂的攻击。

如需深入了解此话题，请访问以下链接：

https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html

思科网络安全报告系列简介

过去十年中，思科发布了大量权威的安全和威胁情报信息，专门面向关注全球网络安全状态的安全专业人员。这些全面的报告详细介绍了威胁形势及其对组织的影响，以及防范数据泄露不利影响的最佳实践。

为了采用新方法提高思想领导力，思科安全公司以思科网络安全报告系列为主题发布了一系列基于研究的数据驱动出版物。我们进一步拓展了主题数量，为兴趣不同的安全专业人士提供不同的报告。凭借安全行业威胁研究人员和创新者渊博的专业知识，2019 年度系列报告系列包括数据隐私基准研究、威胁报告和 CISO 基准研究，以及全年后续推出的其他报告。

有关详细信息，请访问 www.cisco.com/go/securityreports。

美洲总部
思科系统公司
加州圣荷西

亚太总部
Cisco Systems (USA), Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV 荷兰
阿姆斯特丹

思科在全球设有 200 多个办事处。www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。

发布于 2019 年 2 月 THRT_01_0219_r2