利用隐写术实施***

转载

普通网友 于 2019-04-20 23:06:42 发布 100 收藏
原文链接：http://blog.51cto.com/14046599/2382047
版权

低调但有效的隐写技术虽然是旧把戏，但将代码隐藏在看似正常的图像中，还是可能逃脱许多网络安全人员的法眼。
网络安全的一大挑战就是，过度关注某一类威胁，这意味着有可能被另一种威胁杀个措手不及，尤其是在我们的网络和***面不断扩大时，这种情况更严重。所以，除了威胁载体之外，我们还需要用整体的眼光关注威胁技术和威胁策略中的问题。总而言之，安全人员既要准备好随时迎战下一个0 day威胁，同时也不能对熟悉的常见漏洞放松警惕。
出于各种原因，尤其是为了节省成本，网络犯罪分子特别喜欢以换汤不换药的方式反复使用已有的恶意软件。把现成的***工具修修补补，要比重新创建一个省事得多，如果技术好，调整后工具完全有可能骗过安全人员。Fortinet最近的一份报告发现，最近又活跃起来的隐写术就是其中一个需要重点监控的“旧把戏”。

当心被隐写术骗了

保密技术贯穿了人类社会的通信历史。密码学是古代保密技艺中最着名的，不过隐写术也有悠久而传奇的历史。隐写术是一种加密技术，可以将某些内容——消息、代码或其它内容 – 隐藏到其它载体中，例如数字照片或视频，从而使其能够以不避讳的方式传递。十多年前，隐写术曾是向受害者传播恶意软件的常用手段，但近期的发展为这种旧式***注入了新的活力。
如今，作为夺旗（CTF）比赛的一部分，安全专业人员最常遇到隐写术。最近的一个例子来自2018年的Hacktober.org CTF活动，其中标志“TerrifyingKitty”嵌入在图像中。这种策略很聪明，部分原因是因为该技术已经非常老旧了，许多年轻的安全专业人员在寻求解决问题时甚至都不会考虑它。
然而，隐写术的应用并不仅限于娱乐和游戏。网络***者再次开始将这种技术全面融入他们的***方案和工具中。最近的例子包括Sundown Exploit Kit和新的Vawtrak和Gatak / Stegoloader恶意软件系列。
隐写术之前逐渐过气的原因之一是它通常不能用于高频威胁（虽然僵尸网络Vawtrak在2018年第四季度的活动非常频繁）。由于这些威胁仅限于特定的交付机制，因此它们通常无法实现网络犯罪分子希望达到的高***量，即使是Vawtrak的***量在一天内也从未超过十来家公司。因此，当FortiGuard实验室的研究人员观察到，使用隐写术将恶意有效负载隐藏到在社交媒体上传递的表情包中，从而导致恶意软件样本激增时，他们的好奇心被激发了，故此他们对代码进行了一些逆向工程操作，想一探究竟。
与几乎所有其它恶意软件一样，嵌入在这些表情包中的恶意软件首先尝试联系命令和控制（C2）主机，然后下载与***相关的其它代码或命令。不过，有趣的地方就在这里。
这个恶意软件不是直接接收命令，而是按照指令在相关联的Twitter馈送中寻找附加图像，下载这些图像，然后提取隐藏在那些图像内的命令以传播其恶意活动。它通过搜索包含诸如/ print（屏幕截图），/ processes（编写正在运行的进程列表）和/ docs（从不同位置写入文件列表）等修改值命令的图像标记来完成此操作。
这种方法非常巧妙，因为大多数安全流程都专注于识别和阻止受感染设备与C2服务器之间发送的通信和命令。这种独特的隐藏方法表明，我们的对手在不断尝试如何能够悄无声息地达到***目的。利用社交媒体上共享的图像，以及安全人员传统的二维安全防护方法，就是很好的例证。
因此，尽管隐写术是一种低频***媒介，但网络犯罪分子已经开始利用它结合社交媒体的普遍性和快速传播性来传递恶意有效负载。在这种情况下，一个从小规模开始的***媒介 ，即使是在公司网络之外，也可以快速扩展***范围。
这里的难点在于无法专注于整个***频谱。正如我们常说，坏人只需要做对一次，而安全人员一次都不能做错。安全专业人员当然需要通过持续的网络安全意识培训来防范此类创新性***，但他们还需要确保整个***面上的透明可见性。对于许多组织而言，这就需要重新思考和重新设计其安全基础架构。
虽然越来越多的破坏度指标（indicators of compromise）可用于检测恶意隐写代码，但大多数情况下，隐写***都是0 day威胁。因此必须能够及时获取最新的威胁情报和行为分析，并结合自动化和AI技术，进而实现快速威胁响应，多管齐下才能有效防御隐写威胁。

强化安全性的建议

回顾2018年的数据，要有效的应对当今不断变化的威胁，需要打破“烟囱式”独立防护系统，将许多传统上不同的安全工具结合在一起，建立一种协作方法，帮助安全人员全面掌握网络中状况。
随着现代网络威胁的数量、速度和种类的增加，孤立的防护设备和平台愈加显得疲于应对。组织和企业需要一种更统一的防御姿态，帮助公司在整个分布式环境中的多个层检测已知和未知威胁。如果能够再与内部网络分段策略相结合，组织不仅可以更好地检测，还可以以自动化手段遏制网络中横向扩展的威胁。

针对本文中讨论的威胁，实现强有力的反隐写杀伤链需要包括以下工具：

- 使用威胁情报，以追踪最近的隐写技术和其它威胁创新。
- 观察并测试可疑的隐写模糊恶意软件。
- 检查可能隐藏恶意内容的应用程序和其它代码。
- 阻止已知的隐写消息流量。
- 加快更新漏洞补丁、更新升级和策略控制并确定其优先级。

安全人员需要随时了解和跟踪网络中流行的和有破坏力的威胁，以保护其网络免受应用程序***、恶意软件、僵尸网络和0 day漏洞（如隐写技术）的影响。网络安全领域从未有过沉闷的时刻，IT团队必须不断了解最新的威胁，包括以新形式重新出现的旧威胁，才能保证其网络安全。

转载于:https://blog.51cto.com/14046599/2382047