安天发布《GroksterMiner 挖矿木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 GroksterMiner 挖矿木马程序。GroksterMiner 将自身命名为“Lucio Dalla Discografia Completa”，目的是伪装成一个著名的意大利歌手唱片集合，诱惑歌迷运行，释放门罗币挖矿程序，并通过 P2P 网络传播，威胁极大。

样本母体程序是一个 SFX 格式（自解压）的文件，用 7-Zip 或者 WinRAR 打开后可以看见这个母体程序包含 13 个 .tmp 文件、1 个 .vbs 脚本、1 个 .bat 批处理脚本和 1 个 setup 文件。当该母体程序被双击运行时会执行 run.vbs 脚本，并且该程序在释放文件时会覆盖当前目录下的任何同名文件且无需用户确认。run.vbs 脚本退出后，继而以后台启动的方式运行 installer.bat 批处理脚本。installer.bat 脚本的最终目的是将当前文件夹下的 001.tmp 复制到自启动文件夹，并重命名为“svchost.exe”。svchost.exe 的目的是释放挖矿程序进行挖矿。该挖矿木马为了降低被检出率，使用了以下技术：使用自解压程序隐藏恶意 PE 文件内容、使用文件加壳加文件拆分技术，将恶意文件加壳后拆分为多个部分，使用时再将其组合起来。在进行 P2P 传播时，将恶意文件 DOS 头中“program”替换为随机的 7 位字符，使文件在每次运行时出现不同的 HASH 值。

安天 CERT 提醒广大政企客户，应提高网络安全意识，在日常工作中及时进行系统更新和漏洞修复，不随意下载非正版的应用软件、注册机等。收发邮件时应确认收发来源是否可靠，不随意点击或者复制邮件中的网址，不轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的良好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱密码，如果业务上无需使用远程桌面服务，建议将其关闭。

目前，安天追影产品已经实现了对该类挖矿木马的鉴定；安天智甲已经实现了对该挖矿木马的查杀。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、关联分析鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、来源信息鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、关联分析鉴定器、反病毒引擎鉴定器、信标检测鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	f9b2e61200addf760d7bd157c73201e97257b12d5177837a1bffb98f4064e76a
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	6.25 MB
MD5	D6D388E0883F8CFEA196BA1C8FB32043
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/BAT.BitMin
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=D6D388E0883F8CFEA196BA1C8FB32043

◆ 运行环境

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆常见行为

行为描述	危险等级
获取系统信息（处理器版本、处理器类型等）	★
加载运行时 DLL	★
打开自身进程文件	★
读取自身	★★
获取当前激活的窗口	★★
创建窗口	★
.....	.....

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.200	50619	224.0.0.252	5355
192.168.122.200	61940	224.0.0.252	5355
192.168.122.1	67	192.168.122.200	68
169.254.110.208	49967	224.0.0.252	5355
192.168.122.200	53748	224.0.0.252	5355
192.168.122.165	5355	192.168.122.200	55485
.....	.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 08 月 26 日 (总第 197 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

Mykings 僵尸网络近期活动分析报告

概述

2019 年 4 月，安天 CERT 在客户侧威胁检测系统（安天探海）捕获的异常网络流量中发现了 Mykings 僵尸网络的挖矿行为。Mykings 是卡巴斯基在 2017 年 2 月 21 日披露的大型僵尸网络，基于僵尸网络的主控域名“mykings.pw”，之后 360 将其命名为 Mykings。Mykings 僵尸网络通过扫描互联网上开放的 1433 及其他多个端口渗透进入受害主机，传播包括 DDoS 木马、RAT（远控木马）和 Miner（挖矿木马）等多种不同用途的恶意代码进行黑产活动。

事件发现

2019 年 4 月，安天探海威胁检测系统（Persistent Threat Detection System，简称 PTD）在某高校网络侧发出了异常网络流量告警通知，内网多个主机通过 FTP 协议将特殊命名的 TXT 文本上传至境外服务器。

受害主机信息

通过对样本分析和 C2 关联后发现 Mykings 僵尸网络是一个规模巨大的僵尸网络，于是安天对其进行了持续的监控。基于监控调查结果，受害主机操作系统主要涉及 Windows 7、Windows Server 2012 和 Windows Server 2008。其中，Windows 7 操作系统的受害主机占比最高，约为 53%，其次是 Windows Server 2012 和 Windows Server 2008。

分析人员从网络空间探测网站 shodan

的数据库中提取了 8624 份受害主机信息，并对其开放的端口情况进行了统计。从受害主机开放端口的统计情况能够看出，受害主机开放了 80、8080 等多种 web 服务器端口，其次是 3389、22 等远程访问端口，可见拥有公网 IP 的受害主机大多为 WEB 服务器。

Mykings 僵尸网络规模变化

分析人员在持续监控下发现 Mykings 僵尸网络感染量不断增长，其规模正在不断扩大。在 2019 年 4 月至 8 月期间最大感染量为 346525 台受害主机，受害机构涉及企业、高校、政府等。被监控的僵尸网络每月新增受害主机数量约十几万台（其中 7 月数据因其服务器无法连续访问导致数据量下降）。

总结

从对 Mykings 僵尸网络的综合分析来看，攻击者采用批量扫描、爆破和漏洞攻击的无差别网络攻击手段对受害主机进行自动化渗透，渗透成功后向受害主机植入 RAT（远控木马）、Miner（挖矿木马）等木马获利，同时通过信息收集脚本获取受害主机的其它信息；从对 Mykings 僵尸网络的持续监控来看，规模达几十万，可见其整体规模相当庞大；从对 Mykings 僵尸网络受害主机的统计分析来看，受害地区主要位于联网设备基数大、网络安全防护欠发达的国家和地区；从对 Mykings 僵尸网络内网中被攻击的操作系统多是 Windows 7 操作系统来看，推测永恒之蓝系列漏洞对内网仍然是巨大威胁。

防护建议

安天为您提供的安全防护建议如下：

1. 定期修改服务器口令，禁止使用弱口令；2. 确保系统与应用程序及时下载更新官方提供的最新补丁；3. 定期使用反病毒软件进行系统扫描，如反病毒软件具有启发式扫描功能，可使用该功能扫描计算机；4. 在终端安装可靠的安全防护产品，如安天智甲进行有效防护。

安天智甲终端防御系统通过诱饵文件、行为分析、文件变化审计、进程身份识别等多种能力的结合，可实现对主流僵尸网络的有效防护。经验证，安天智甲可实现对 Mykings 僵尸网络有效防护。

微信扫描二维码阅读全文

Gamaredon 组织新活动攻击乌克兰政府机构

FortiGuard 实验室最近发现 Gamaredon 组织针对乌克兰执法部门和政府机构的新攻击活动。攻击初始通过鱼叉式网络钓鱼投放的主题关于乌克兰军事冲突的诱饵存档文件，其中包括 word 文档、jpg 图片和 txt 文本文件。文档名称为乌克兰语，而内容为俄语。

用户打开文件后触发 WinRAR unacev2 模块漏洞，释放三个文件，一个为模仿谷歌浏览器的 lnk 快捷方式，另一个为相同的快捷方式通过自启动实现持久性，最后一个文件为受密码保护的自解压 RAR 存档，其使用合法 Microsoft 工具的假数字签名，通过其嵌入式的 SFX 脚本启动 C2 上托管的主要载荷，窃取信息。研究人员还发现其使用新的 Linux 恶意软件 Evil Gnome。

（原文链接：https://www.fortinet.com/blog/threat-research/gamaredon-group-ttp-profile-analysis.html）

每周安全事件

类 型	内 容
中文标题	研究人员发现新蠕虫挖矿恶意软件 Beapy
英文标题	Worm-Cryptominer Combo Lets You Game While Using NSA Exploits to Move Laterally
作者及单位	Liviu ARSENE &Eduard BUDACA
内容概述	Bitdefender 研究人员发现一种新蠕虫挖矿恶意软件 Beapy/PCASTLE。Beapy 由 Python 和 Powershell 组件组成，具有先进的挖矿能力，并利用蠕虫功能横向移动。Beapy 通过 PUA 应用程序的供应链攻击投放，利用高级工具和未修补漏洞包括 EternalBlue 漏洞等横向移动。如果受害者的机器运行流行的游戏时，将暂停资源密集型的挖矿操作。同时具有 CPU 和 GPU 挖矿组件，使用专用 RSA 密钥对 C&C 通信进行签名。
链接地址	https://labs.bitdefender.com/2019/08/worm-cryptominer-combo-lets-you-game-while-using-nsa-exploits-to-move-laterally/

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	G-Ware/Android.Locker.bv[rog,lck] 2019-08-18	高	该应用程序伪装色情应用，运行加载勒索界面，持续振动手机，要求用户付费解锁，建议卸载。
		Trojan/Android.pcTattletale.a[prv,exp,spy] 2019-08-19	中	该应用程序运行激活设备管理器，隐藏图标，监控用户手机位置、使用情况等，通过截屏、录制视频等方式记录并联网上传，造成用户的隐私泄露和资费消耗，请谨慎使用，非自主安装建议卸载。
		RiskWare/Android.FakeQQ.an[fra] 2019-08-20	低	该应用程序伪装 qq，无实际功能，运行诱导用户下载正版 qq，造成用户不必要的资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.TrackerSpy.c[prv,spy]	中	该应用程序伪装系统更新，实际是间谍件，会上传用户联系人、通话记录、短信、照片、通话录音等隐私信息，造成用户隐私泄露，请卸载。
		Trojan/Android.Randoms.a[prv,spy]	中	该应用程序运行获取用户的短信信息、通话记录、通讯录、浏览历史、位置信息等，并上传至服务器，用户可以通过注册的账号查看这些信息，请谨慎使用，非自主安装建议卸载。
		Trojan/Android.NCSpy.a[prv,rmt,spy]	中	该应用程序是间谍件，运行隐藏图标，接收指令，开启录音、上传本地文件、录音文件，还会上传联系人、通话记录、短信、位置等隐私信息，造成用户隐私泄露，请卸载。
		Trojan/Android.FakeWallet.d[fra]	中	该应用程序运行隐藏图标，窃取用户通讯录、短信 、位置信息、用户手机固件信息 、用户相机及拍照图片、用户 wifi SSID 信息等， 并通过邮件将用户信息上传，造成用户的隐私泄露，建议卸载。
		RiskWare/Android.K3bocai.a[rog]	低	该应用程序为博彩类应用，会给您带来财产损失。此类程序一般以欺骗形式引诱推荐安装，是一种典型的网络赌博诈骗手段，请立即卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows DHCP 客户端远程代码执行漏洞（CVE-2019-0736）	高	当攻击者向客户端发送经特殊设计的 DHCP 响应时，Windows DHCP 客户端会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在 Windows DHCP 客户端计算机上运行任意代码。
	较为活跃样本	Trojan/Win32.Blueh	中	此威胁是一种具有多种恶意行为的木马家族。该家族会禁用感染者计算机中的一些重要程序，将恶意代码和冗余文件添加到计算机中，导致系统速度变慢甚至崩溃。该家族也会捆绑其他恶意软件并安装。
		Trojan/WinLNK.Agent	中	此威胁是一种具有不固定行为的病毒家族。该病毒家族以快捷方式作为载体，通过修改快捷方式指向的内容，来实现下载或执行其他应用程序。该家族并没有统一的行为与功能，而是像一个灰色软件类程序集合一样，将大量以基因片段定性的恶意代码归类。
		Trojan/Win32.Ogimant	中	此威胁是一种有多种恶意行为的木马家族。该家族具有在感染者计算机桌面创建快捷方式，更改浏览器主页，下载恶意软件等行为。
		Trojan/Win32.BHOLamp	中	此威胁是一种可以收集用户信息的木马家族。该家族样本运行后注册 COM 接口，收集个人用户信息发送给第三方。
		GrayWare[AdWare]/Win32.Lola	低	此威胁是一种可以弹出广告的灰色软件家族。该家族样本运行后安装广告件，在用户浏览网页时弹出广告，占用系统资源，影响用户使用。

视频成为恶意软件攻击的传播载体

Mike Elgan/ 文 安天技术公益翻译组 / 译

大多数员工都对恶意软件攻击有所了解。例如，很多员工知道他们不能打开陌生人发来的可执行文件，或者安装在停车场捡到的 U 盘。但是，视频或视频链接也可以像可执行文件或 U 盘一样传播恶意软件。员工是否知道这一点呢？即使他们知道，他们是否会被诱骗打开恶意视频呢？

这就是企业开始关注视频恶意软件的原因。

视频是社会工程手段的完美诱饵

在恶意软件攻击中，视频可能是社会工程手段的完美诱饵。人与人之间通信和社交媒体的最新趋势，使公众每天都不可避免地打开许多视频。Facebook 和 Instagram 已经增加了非常受欢迎的、令人上瘾的视频功能，以赶上 Snapchat 和 TikTok 等新兴企业的步伐。YouTube 一直强调用有趣的视频吸引用户，而越来越多的消息传递应用也开始传播视频。

换句话说，在人们逃避现实、无聊和传递信息时，视频已成为首选的数字“解药”。用户可能认为视频文件是无害的，这意味着即使是对安全敏感的、不会点击可疑链接的用户，也很有可能会打开并播放视频。对于网络犯罪分子来说，这是很好的机会。

我们文化中的视频习惯（或上瘾），为视频恶意软件（恶意代码嵌入到视频文件中）的传播提供了条件。在更有效、更隐蔽地传播恶意软件的趋势中，视频恶意软件是很重要的一部分。它也是恶意隐写术（将秘密内容嵌入到其他媒体中）的最新，也许是最有趣的例子。当媒体是可执行文件时，它被称为“隐写软件”（stegware）。

多年来，恶意软件已经嵌入到静态图像文件格式中，例如 JPG、PNG 和 BMP 格式。而现在，视频恶意软件正受欢迎。

最新的视频恶意软件消息

由于视频具有无法抗拒的吸引力，多年来攻击者一直在利用视频。诱骗用户点击恶意链接的一种常见方法是：询问用户“这个视频里是否有你”。一想到自己出现在敏感的、公开传播的视频中，大多数用户（除非是受过安全教育的、有理性的用户）都会打开视频或点击链接进行确认。在主要的消息传递平台上，这种策略很常见，攻击者可以使视频或链接看起来像是朋友或同事发送的。

这种技术有更复杂的版本。例如，据《今日美国》报道，在 2014 年，一款名为 Trojan.FakeFlash.A 的恶意软件，将一位 Facebook“朋友”的照片放在受害者的消息中，并暗示受害者，只要点击该照片，就能看到该“朋友”的私密视频。该恶意软件感染了全球约 200 万个系统。

上述恶意软件攻击不涉及实际视频——只是以视频为诱饵，诱骗用户点击链接或打开文件。而最近的漏洞和攻击则涉及实际视频，将视频作为恶意软件传播途径。

趋势科技最近发现，攻击者在 Word 文档中嵌入了包含恶意软件的视频。这是一种相对简单的恶意软件嵌入方法——可以简单地将恶意软件添加到 Word 文件夹中的 XML 文件中。然后，攻击者可以修改文档，以便在受害者打开并点击视频时执行恶意代码。今年 7 月，赛门铁克发现了一个名为“媒体文件劫持”（media file jacking）的攻击向量，它使攻击者能够篡改 WhatsApp 和 Telegram 上的视频和图片——幸运的是，这种攻击不是以启用代码执行的方式进行的。

Android 系统中发现的另一个漏洞，为视频恶意软件的传播提供了可能性。利用 Android 版本 7-9（Nougat、Oreo 和 Pie）中的这一漏洞，网络犯罪分子可以通过视频嵌入恶意软件远程执行代码。鉴于 YouTube 等视频服务会对上传的视频进行重新编码，从而修改恶意代码并阻止其运行，因此视频必须直接发送（例如，作为电子邮件附件发送）。

此后，谷歌发布了修复此漏洞的安全更新，因此打了补丁的设备是安全的。然而，那些没有打补丁的设备（理论上超过 10 亿台）仍处于危险之中——特别是，补丁的发布使更多的攻击者了解了此漏洞。虽然此后还没有出现此漏洞被利用的报告，但这说明了视频恶意软件出人意料的可能性。

随着用户对视频的上瘾、隐蔽技术的日益高明，以及移动设备不断增加，攻击者开始积极探索通过视频传播恶意软件的可能性。现在是时候采取“反隐写”策略了。

如何应对视频恶意软件威胁

最可怕的威胁是：没人听说过或预料到的威胁。但最近的事件表明，视频恶意软件是恶意软件社会工程（以及软件工程）的一个重要领域。企业可以采取以下步骤来应对视频恶意软件。

- 建立统一的防御态势——即打破网络安全“孤岛”。
- 将高级统一端点管理（UEM）解决方案作为防御核心。
- 通过威胁情报来掌握最新的隐写攻击和漏洞。
- 阻止包含嵌入视频的 Word 文档进入公司网络。
- 随时关注所有系统和设备（尤其是移动设备）的补丁和更新。

用户喜欢视频。鉴于视频的吸引力和传播性，用户终将会打开它们。攻击者知道这一点，他们一直在研究在视频中隐藏恶意代码的新方法。企业的安全团队是否做好了反击准备呢？

原文名称	How Video Became a Dangerous Delivery Vehicle for Malware Attacks
作者简介	Mike Elgan。Mike Elgan 是一位专栏作家，为各种网站撰写文章。
原文信息	2019 年 8 月 19 日发布于 Security Intelligence。 原文地址 https://securityintelligence.com/articles/how-video-became-a-dangerous-delivery-vehicle-for-malware-attacks/
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。