安天发布《勒索软件 Sodinokibi 运营组织的关联分析》报告

2019 年 5 月，安天 CERT 监测到了多起利用钓鱼邮件传播 Sodinokibi 勒索软件的事件。Sodinokibi 从 2019 年 4 月 26 日开始出现，其传播方式主要为钓鱼邮件、RDP 暴力破解和漏洞利用。该勒索软件运行后，尝试加密磁盘中的文件（不加密罗马尼亚语、俄罗斯语、乌克兰语、白俄罗斯语、爱沙尼亚语等语言的操作系统）；修改桌面背景并创建一封勒索信，勒索信中提供了付款和解密网站，该网站需要提交勒索信中的 Key 和加密后缀才可以访问。提交后进入到解密界面，勒索者向受害者勒索价值 1300 美元的比特币，若受害者不在 7 天内支付则赎金价格翻倍。

安天 CERT 分析人员通过代码、C2、邮件、漏洞利用等关联分析认为该勒索软件团伙是一个不断套用、利用其他现有恶意工具作为攻击载体，传播勒索软件、挖矿木马、窃密程序，并在全球范围内实施普遍性、非针对性勒索、挖矿、窃密行为的具有一定规模的黑产组织。该组织和 GandCrab 组织有着千丝万缕的关系，分析人员猜测 Sodinokibi 和 GandCrab 运营成员有重合部分，在 GandCrab 组织宣布停止运营之后，部分 GandCrab 成员不愿收手，继续运营新修改的勒索软件 Sodinokibi。

勒索病毒给企业和个人的数据安全带来了严重的威胁，一旦主机被入侵，主机中的文件都有可能被加密，而且被加密文件将难以恢复，因此防护显得极为重要。安天建议广大用户，不要将数据安全立足于加密后的数据恢复，应该安装杀毒、防毒软件（参考安天智甲工具）并及时升级系统和修补设备漏洞；对重要的数据文件进行备份，避免弱口令的使用，避免使用统一的密码。确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭。

目前，安天追影产品在本次分析的基础上已经实现了对该类勒索病毒的鉴定；安天智甲在本次分析的基础上已经实现了对该勒索病毒的查杀。

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、来源信息鉴定器、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、动态（Win7 x86）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	290 KB
MD5	FB68A02333431394A9A0CDBFF3717B24
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.DelShad
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/_lk/details.html?hash=FB68A02333431394A9A0CDBFF3717B24

◆ 运行环境

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
192.168.122.111	137	192.168.122.255	137
0.0.0.0	68	255.255.255.255	67
192.168.122.111	138	192.168.122.255	138
192.168.122.111	123	13.70.22.122	123
192.168.122.1	67	192.168.122.111	68

◆ TCP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.165	49158	23.4.240.82	80
192.168.122.165	49159	192.168.122.155	139

◆进程监控

PID	创建	命令行
2192	target.exe	"c:\a559e68818054feaaf0d733d32019773\share\target.exe"

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 07 月 01 日 (总第 189 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天蜜网捕获“利用 ElasticSearch Groovy 漏洞进行门罗币 (Dog) 挖矿”事件分析

概述

2019 年 6 月 13 日，安天蜜网捕获到利用 CVE-2015-1427(ElasticSearch Groovy) 远程命令执行漏洞的攻击行为。该漏洞原理是 Elaticsearch 将 groovy 作为脚本语言，并使用基于黑白名单的沙盒机制限制危险代码执行，但该机制不够严格，可以被绕过，从而导致出现远程代码执行的情况。安天对此次事件进行了详细的样本分析，并给出预防及修复建议。

样本分析

♦关键攻击载荷

从攻击载荷来看，攻击者通过 groovy 作为脚本语言，向 _search?pretty 页面发送一段带有恶意链接为 http://185.181.10.234/E5DB0E07C3D7BE80V520/init.sh 的 json 脚本，进行恶意 shell 脚本下载，从而实现远程代码攻击，并进行挖矿行为。

• 入侵脚本分析：init.sh

攻击者通过 http://185.181.10.234/E5DB0E07C3D7BE80V520/init.sh 下载并执行恶意脚本 init.sh 来植入 Dog 挖矿程序，同时对主机进行扫描等一系列操作。

之后执行关闭防火墙、关闭 selinux 并释放占用的资源、杀掉其他与挖矿相关的进程、设置定时任务（每 30 分钟下载一次可执行文件 update.sh），获取 ssh 权限，进行 iptables 规则转发修改，同时清理相关操作历史、日志等操作。

在此过程中，脚本会检查 sysupdate、networkservice 和 sysguard 这 3 个进程是否启动，如果没有则进行启动。

• 样本分析：sysguard、networkservice、sysupdate

三个样本为 go 语言编写并使用 UPX 加壳，安天将对应的 main_main 函数结构进行了图示。

通过与之前捕获的 systemctl 样本对比发现，此次攻击分成挖矿、扫描、函数调用三个进程进行调度。并且在 networkservice 样本中发现了相关漏洞利用函数和扫描函数。

通过对比之前捕获的样本发现两次攻击手法类似，不同的是此次攻击是通过 sysguard、networkservice（扫描）和 sysupdate 三个进程共同进行的。这也意味着，发现服务器被感染后要将这三个进程同时 kill 掉。

• 配置文件：config.json

在下载的配置文件中，安天发现了多个矿池地址，并将相关结果进行了图示。

♦受影响的服务及漏洞

报告中，安天详细罗列了受影响的服务及漏洞情况。

预防与修复建议

♦预防建议

1) 确保系统与应用程序及时下载更新为官方提供的最新补丁。

2) 禁止使用弱口令密码。

3) 定期检查服务器异常，如 CPU 持续占用高、磁盘异常情况。

4) 安装终端威胁安全防护产品 -- 安天智甲终端防御系统。安天智甲终端防御系统可以为您量身定制专属安全基线，为您打造安全的内网环境；同时，文档安全保护功能、全网病毒定点清除功能、以及国产操作系统的安全防护功能更好的解决您遇到的安全问题，保护您的服务器。

♦修复建议

1) 断网、备份重要的 crontab，关闭或删除定时任务：systemctl stop crontab 或 rm -rf /etc/cron.d/*。

2) 锁定 crontab 中的恶意文件。

3) 查看并杀掉病毒进程：同时杀掉 sysguard、networkservice、sysupdate 三个进程。

4) 删除病毒相关文件。

5) 确认无误后，重启服务器，安装漏洞补丁，并采用安天智甲终端防御系统进行预防和保护服务器的安全

微信扫描二维码查看分析详情

Excel Power Query 功能可被利用分发恶意软件

Mimecast 研究人员发现 Microsoft Excel Power Query 功能可被利用分发恶意软件。Power Query 是一个功能强大且可扩展的商业智能（BI）工具，允许用户将其电子表格与其它数据源集成在一起。研究人员表示攻击者可利用该功能，将远程动态数据交换 (DDE) 攻击动态地启动到 Excel 电子表格中，并主动控制有效载荷 Power Query。研究人员发现 Power Query 还可以用于发起复杂的、难以检测的攻击，这些攻击结合了多个攻击表面。攻击者可以将恶意内容嵌入到单独的数据源中，然后在打开电子表格时将内容加载到电子表格中，恶意代码可以被用来释放和执行恶意软件。目前 Microsoft 提供了一个解决方案来缓解此问题。

每周安全事件

类 型	内 容
中文标题	Gift Cardsharks：以商业工具为目标的大规模运动
英文标题	Meet the ‘Gift Cardsharks’ Behind the Massive Campaign Targeting Victims with Commercially Available Tools
作者及单位	Team RiskIQ
内容概述	RiskIQ 研究人员发现了一项以商业工具为目标，针对数百个组织的大规模运动“Gift Cardsharks”，其中许多组织经营礼品卡业务。研究人员在调查 IT 供应商 Wipro 被入侵时，该攻击组织首次被发现，该攻击活动可追溯至 2016 年。研究人员通过分析发现该组织利用广泛使用的电子邮件营销和分析工具来创建有效的电子邮件网络钓鱼活动，这对目标的网络安全而言似乎是合法的。该组织主要针对礼品卡零售商、分销商和卡处理商。 通过访问此礼品卡基础设施，攻击者可以使用汇款服务、票据交换所和其它支付处理机构来获利。 该组织使用的 PowerShell 脚本之一 BabySharkPro 通常与朝鲜威胁组织活动相关联，但这可能是一种混淆视听的行为。
链接地址	https://www.riskiq.com/blog/external-threat-management/giftcard-sharks/

每周值得关注的恶意代码信息

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	Trojan/Android.UpdateSpy.b[prv,rmt,exp,spy] 2019-06-23	高	该应用程序是间谍软件，运行诱导激活设备管理器，隐藏图标，接收远程指令进行录音、发送短信、拨打电话，上传用户联系人、通话录音、通话记录、短信、sd 卡中的指定格式文件（pdf、doc、xls）等隐私，造成用户隐私泄露，请卸载。
		Trojan/Android.FinansMobil.a[prv] 2019-06-24	中	该应用程序运行隐藏图标，加载银行钓鱼界面诱骗用户填写并上传，监听和上传用户短信，造成用户隐私泄露，建议卸载。
		Trojan/Android.FakeBTCTurk.a[prv] 2019-06-24	中	该应用程序伪装比特币交易应用，诱导用户授权后，后台窃取包含指定内容的通知信息，还会窃取用户的登录凭据，造成用户隐私泄露，请卸载。
	较为活跃样本	G-Ware/Android.PJbocai.l[fra,exp]	中	该应用程序伪装正常应用，运行私自下载博彩应用，而后请求 root 权限，其后安装博彩应用并卸载自身，博彩应用可能会给用户财产带来风险，建议不要使用。
		Tool/Android.mycellspy.a[prv,spy]	中	该应用程序为监控工具，可以监控手机短信，通话记录和音频，相机，照片，视频，GPS 位置，联系人，浏览器记录等，建议谨慎使用，避免造成隐私泄露。
		RiskWare/Android.repackvqs.a[rog]	低	该应用程序是非官方应用，经过重打包处理，可能被恶意篡改植入广告等，存在一定的使用风险，建议卸载该应用，下载安装官方正版应用。
		G-Ware/Android.fakeTelegram.b[exp,rog]	低	该应用程序伪装 Telegram 服务，运行隐藏图标，访问推广页面，会造成用户流量资费损耗，请卸载。
		Trojan/Android.WalHd.b[pay]	低	该应用程序为壁纸应用，运行用户点击下载壁纸时有提示发送扣费短信，请谨慎使用，注意提示信息。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows Hyper-V 远程代码执行漏洞（CVE-2019-0620）	高	当主机服务器上的 Windows Hyper-V 无法正确验证来宾系统上经身份验证的用户输入时，存在远程代码执行漏洞。攻击者可以在来宾操作系统上运行经特殊设计的恶意程序，最终在主机服务器系统上执行任意代码。
	较为活跃样本	GrayWare[AdWare]/Win32.BetterInternet	低	此威胁是一种广告类的灰色软件程序。该家族样本是一个浏览器辅助工具，可以显示广告、下载和安装文件。样本运行后会显示广告；根据用户访问的网站显示相关网站的链接和广告；存储用户曾访问过的网站；将某些 URL（包括 Web 浏览器的默认 404 错误页重定向到 Adware.Binet 指定网页）；自动更新广告软件并安装新增的特性或功能。
		Trojan[Packed]/Win32.Tpyn	中	此威胁是一种加壳类木马程序。该家族通常会压缩间谍软件文件，避免被反病毒软件检测。
		Trojan[Exploit]/Java.AGeneric	中	此威胁是一种可以利用某些漏洞的木马程序。该家族样本使用 Java 编写，没有统工的行为与功能，是以启发式检出的恶意代码。
		Trojan[Packed]/Multi.SuspiciousPacker	低	此威胁是一种压缩恶意代码的木马程序。该家族样本一般为压缩包，运行后会解压运行恶意代码，有一定威胁。
		GrayWare[AdWare]/Win32.MaxDriver	低	此威胁是一种可以下载推广应用的灰色软件程序。该家族样本运行后可以连接网络下载并安装推广应用，在用户浏览网页时会弹出广告，占用系统资源，影响用户使用。

漏洞“猎杀”

Jim Souders/ 文 安天技术公益翻译组 / 译

在 2018 年，共有 16515 个新的 CVE 漏洞被公布。截至 2018 年 11 月，每周都有超过 300 个漏洞被上报，到了 2019 年这个数字就更大了。这意味着，企业必须将系统更新和打补丁作为当务之急。

但是，及时为每台机器和设备更新操作系统、应用和浏览器的版本，是一项庞大的、看似不可能完成的任务。为了接近这一目标，企业需要采取一些策略，以便更轻松地查找漏洞、确定漏洞优先级，修复和上报漏洞，从而保护企业及其现有资源。

我们提出了以下措施，以帮助企业改进更新流程，降低漏洞带来的安全风险。

改变企业文化

企业不应将系统更新和打补丁视为一项应该做但并不紧迫的繁琐工作。相反，企业应让员工了解漏洞在企业安全中扮演的角色，让他们知道漏洞管理是更大安全策略的一部分。这种思维模式不能只局限于 IT 部门，而应扩展到每位员工。

互联网安全中心（CIS）建议企业开展基于差距或基于风险的培训。在这些培训中，IT 人员确定存在安全问题的领域——如是否与他人共享口令、是否及时更新计算机系统补丁，是否将敏感数据存储在易丢失的、非受控的 U 盘中——并针对最严峻的挑战进行培训。这有助于员工了解重要安全实践以及为何要实施这些实践，并为他们提供相关的、现实的态势指导。这些培训本质上是合作关系，旨在为所有员工提供支持，帮助他们在必要时开展合作——即使这意味着在项目运行期间重启员工机器以修复严重漏洞。

在安全意识方面，企业不能仅在员工入职时开展一次培训。在工作过程中，员工会接收到大量与其工作职能相关的新信息，可能会导致他们认为安全并非头等大事。为了改变这种文化，企业需要持续对员工进行培训。这些培训不必是劳师动众的，可以采取简单的形式，如花几分钟宣讲、每季度发送最佳实践邮件，或一年举行两次研讨会等等。

利用相关标准

除了让员工参与基本实践之外，安全团队还必须能够发现现有漏洞。目前，有许多开放标准可以帮助安全团队识别不断增长的漏洞，并提供防范漏洞的建议。安全内容自动化协议（SCAP）是最常见的协议之一，它提供了一个规范框架，支持自动配置、漏洞和补丁检查、合规检查和度量。在定义常见漏洞和确定适合企业环境的条件方面，该协议非常有用。此外，还有许多其他标准也可以帮助企业创建配置基准，如 CIS 指南、美国国防信息系统局发布的技术信息指南等。

创建基准后，企业可以参考 CVE 数据库和美国国家漏洞数据库（从各种来源获取消息）来识别漏洞。此外，企业也可以参考微软发布的安全更新。但是，这些数据库中包含大量的复杂漏洞，会让漏洞管理人员触目惊心。

寻求自动化的解决方案

自动化的漏洞管理解决方案已经出现了，能够为漏洞猎杀提供帮助。这些解决方案脱胎于上述各种数据库，旨在识别和分析影响企业端点的漏洞。市面上的自动化产品检测速度较慢，而且会干扰网络性能，这导致它们不怎么受欢迎。但是，随着技术的进步，新一代漏洞管理解决方案有望加快检测速度，增加可以搜索的漏洞数量，而且不会对网络性能产生负面影响。因此，安全团队不必再苦苦等待，他们可以迅速完成扫描，并大大缩短修复所需的时间——远少于行业平均水平 38 天。

如果企业想要部署自动化漏洞管理解决方案，请务必开展调研以找到符合需求的产品。没有任何自动化解决方案可以实现 100％的检测率，但是在短时间内达到 80％到 90％的检测率也是很不错的。

路漫漫其修远兮 .....

发现漏洞后，安全团队还有很多工作要做。他们需要评估漏洞、确定漏洞的优先级，修复和上报漏洞。如上文所述，如今的漏洞管理并不简单；但是安全团队可以防微杜渐，持续关注和解决小麻烦，防止它们演变为大麻烦，从而扭转局势，确保企业的安全。

原文名称	The Hunt for Vulnerabilities
作者简介	Jim Souders。Jim Souders 是 Adaptiva 公司首席执行官。
原文信息	2019 年 6 月 20 日发布于 Dark Reading 原文地址 https://www.darkreading.com/vulnerabilities---threats/the-hunt-for-vulnerabilities-/a/d-id/1334976
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。