安天发布《六小时处置挖矿蠕虫的内网大规模感染事件》报告

2019 年 5 月，安天接到某重要单位的求助，其内网中执行任务的上百台主机频繁出现死机、重启、蓝屏等现象。安天应急服务小组迅速抵达用户现场进行快速处置。经前后台协同联动判定，这是一起 WannaMine 挖矿蠕虫通过 EternalBlue（“永恒之蓝”）漏洞在内网中进行横向移动并反复传播感染内网主机的事件。永恒之蓝漏洞对应补丁为 MS17-010，如果主机没有安装相应补丁或关闭相关端口，则无法阻挡该病毒在内网中的渗透传播。WannaMine 最早出现于 2017 年底，它会最大限度的利用 CPU 来挖掘门罗币。

安天 CERT 提示，通过安天智甲终端防御系统可以实现内网端点系统统一补丁升级、安全加固策略配置和病毒统一查杀。在没有安天智甲部署的情况下，遇到蠕虫反复感染对应问题的用户建议采取以下缓解措施：对局域网内的所有主机采取断网操作；根据病毒所使用的漏洞和受感染终端的操作系统版本信息，安装对应的安全补丁；在不影响用户业务的前提下关闭 445 端口，通过杀毒工具进行查杀；逐步恢复网络并通过抓包工具确认网内是否存在恶意流量，并对全网终端安全状态进行确认。

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口令，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 Wannamine 挖矿蠕虫的鉴定；安天智甲已经实现了对 Wannamine 挖矿蠕虫的查杀。

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、字符串分析鉴定器、关联分析鉴定器、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、反病毒引擎鉴定器、动态行为鉴定器、关联分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	ec61768c0a7da9650f8662ae0918fc48dc2bed6b4a97f277ceb5fdd4b1ef65f4.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	6.38 MB
MD5	80402E15A81E4F513980857455EB5A9C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Miner
判定依据	反病毒引擎

◆ 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

◆危险行为

行为描述	危险等级
服务加载 DLL	★★★
通过 CMD 隐藏删除自身	★★★★
删除自身	★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
释放 PE 文件	★
修改文件创建时间	★★
创建服务	★
修改服务	★★
启动指定服务	★
.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 10 月 14 日 (总第 203 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

六小时处置挖矿蠕虫的内网大规模感染事件

应急服务背景

2019 年 5 月，安天接到某重要单位的求助，其内网中执行任务的上百台主机频繁出现死机、重启、蓝屏等现象，用户部署使用的某款杀毒软件能查出病毒告警，但显示成功清除后，病毒很快会重新出现。用户尝试采用其他工具进行处理，未能解决问题，遂向安天寻求帮助。在电话远程协助用户处置的同时，安天派出由安全服务工程师、智甲终端防御系统产品支持工程师组成的应急服务小组，携智甲终端防御系统安装盘、便携式探海威胁检测系统、拓痕应急处置工具箱，及最新病毒库、补丁包等配套资源，于接到求助当日傍晚飞抵用户现场进行处置，快速解决了问题。

现场信息采集观测和研判

安天工程师到达现场后，快速与用户进行了交流研判，共同确定了基于部署探海进行流量侧的监测分析、通过拓痕进行端点的信息采集和证据固化，制定合理安全配置加固策略，全面安装智甲终端防御系统，实现所有终端安全策略加固、统一补丁安装和全网查杀的处置流程。

安天应急服务小组在协助用户配置交换机镜像设置后，通过探海发现了大量内网扫描和基于永恒之蓝漏洞的攻击流量，以及匹配到威胁情报规则标记为矿池的域名连接请求，又通过拓痕应急处置工具对感染主机进行了扫描、对可疑文件与关联信息进行提取，结合用户已采集安全日志和其他工具，协助用户完成了证据固化。安天工程师初步判定出，这是一起 WannaMine 挖矿蠕虫，通过永恒之蓝漏洞，反复传播感染事件。安天应急服务小组根据预案，在严格执行用户“样本文件不离场”的要求下，前后台快速协同联动，在征得用户同意后，仅将扫描发现的病毒名称、样本 HASH 等信息通报给安天应急响应中心（以下简称安天 CERT），进行分析支持和研判验证。安天 CERT 从支撑平台提取相同 HASH 的样本，结合已有分析验证，在事件机理成因方面，与进场服务小组作出完全一致的判断：由于用户侧部署的原有杀毒软件无法有效支持补丁升级、且没有主机策略配置加固，导致病毒被清除后，会继续通过漏洞重新打入，致使感染源始终存在，其中部分用户终端在被永恒之蓝漏洞攻击中会蓝屏。对此，应急服务小组基于全网终端安装智甲和统一扫描，并部署智甲软件管理中心，全面提取了相关信息，分析确认了病毒最早的出现日期，为用户定位该批设备的最初感染源提供了信息支撑。

制定加固策略、分发安全补丁、查杀终端威胁

该蠕虫的传播机理为：迅速利用 EternalBlue（“永恒之蓝”）漏洞在局域网内传播自身，形成更加庞大的挖矿网络。该漏洞使用 445 端口传播，对应补丁为 MS17-010。如果主机没有安装相应补丁或关闭相关端口，则无法阻挡该病毒在内网中的渗透传播。根据智甲检测日志，出现病毒感染、蓝屏等故障的主机均未安装 MS17-010 补丁。

安天应急服务小组调研了用户现有业务系统所采用的通讯端口、协议等情况，对用户将端点做了初步分组，对默认安全策略模板（参考 STIG 标准）进行了部分定制调整。之后借助管理中心启动了补丁统一分发、策略调整和统一查杀。经安天工程师连夜不间断奋战，在到场六小时后将一百多台染毒主机、全部完成了对应补丁升级、安全策略加固和病毒查杀工作。

深度分析支持和支持归零复盘

后端分析团队基于样本 HASH 进行了深度分析并于第一时间为用户提供了 WannaMine 挖矿病毒样本的详细分析报告。

在现场病毒情况得到控制的同时，该单位相关负责人希望安天能够在其实验环境中复现该病毒的攻击过程。安天工程师根据事发现场的情况搭建了模拟环境，根据处置前固化的感染系统端点镜像，模拟现场情况并恢复了相关环境，提供了探海检测系统生成监测日志、并进行录包，指导用户通过 Wireshark 对数据包进行解析观察，在实验环境中复现了整体攻击过程和具体故障表现，为用户后续对事件进行归零复盘提供了依据。

安天应急服务小组协助用户完成最终判定，这是一起由第三方设备带毒入网导致的安全事件，昭示出供应链安全侧的安全风险。

用户评价

本次应急事件处理完成后，安天受邀参加了该单位针对此事件的归零报告评审会议，用户对本次安全事件十分重视，单位领导对安天的应急响应处置能力、技术支持水平及智甲等产品的查杀和防御能力给予了高度评价，同时提出了和安天建立长期的安全服务关系，并采购了探海和智甲产品。

应急处置方案及后续安全建议

• 应急处置方案

安天安全服务中心提示，通过安天智甲终端防御系统可以实现内网端点系统统一补丁升级、安全加固策略配置和病毒统一查杀。

在没有安天智甲部署的情况下，遇

（下转第三版）

每周安全事件

类 型	内 容
中文标题	研究人员发现 Drupalgeddon2 漏洞的新活动
英文标题	New Campaign Targets Drupalgeddon2 Flaw to Install Malware
作者及单位	Ionut Arghire
内容概述	Akamai 的安全研究人员发现，黑客继续针对名为 Drupalgeddon2 的 Drupal 漏洞将恶意软件安装到未修补的系统上。被追踪为 CVE-2018-7600，该安全漏洞影响 Drupal 版本 6、7 和 8，该漏洞已于 2018 年 3 月得到解决。现在，Akamai 安全研究员 Larry W. Cashdollar 透露，该漏洞仍然是最近观察到的恶意活动的目标，攻击者试图运行嵌入在 .gif 文件中的代码。尽管没有广泛推广，但该运动似乎针对的是各种高知名度的网站，而没有关注特定的行业。
链接地址	https://www.securityweek.com/new-campaign-targets-drupalgeddon2-flaw-install-malware

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	Trojan/Android.FakeParibu.a[prv,exp] 2019-10-06	高	该应用程序伪装成货币交易应用，运行后加载未知网页，警惕其打开虚假交易网页，还会监听并上传用户短信，私自发送短信，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.alidevs.a[exp,rog] 2019-10-07	中	该应用程序伪装汇率信息，包含敏感权限，运行后释放风险子包，联网私自下载并安装未知应用，造成用户流量消耗，存在很大安全隐患，建议不要使用。
		RiskWare/Android.Fakejiaoyou.i[fra,exp] 2019-10-08	中	该应用程序伪装交友软件，通过发送虚假诱惑性消息，以及特权服务，诱导用户付费，造成用户资费损失，建议卸载。
	较为活跃样本	Trojan/Android.spynote.d[prv,exp,rmt,spy]	中	该应用程序是间谍件，运行隐藏图标，诱导激活设备管理器，接收远程指令，上传联系人、通话记录、安装列表、位置、录音文件等隐私信息，还会接收指令拨打电话，下载未知文件，会造成用户隐私泄露和资费损耗，请卸载。
		Trojan/Android.travelntime.a[prv,rmt,exp,spy]	中	该应用程序运行隐藏图标，联网获取远程指令，后台上传用户短信、通讯录、定位、照片等大量隐私信息并私发短信，造成用户隐私泄露与资费消耗，建议卸载。
		Trojan/Android.moonshine.a[prv,rmt,spy]	中	该应用程序是一款间谍软件，运行后隐藏图标，释放恶意文件，窃取用户短信、联系人、通话记录、地理位置、手机存储文件，并上传至服务器。造成用户隐私泄露，建议立即卸载。
		Trojan/Android.FakeCointool.a[prv]	中	该应用程序伪装比特币交易相关应用，无实际功能，诱导用户开启通知读取权限，窃取通知栏信息，还会诱导用户输入比特币交易平台账户密码信息后台上传，会造成用户隐私泄露和财产损失，请卸载。
		RiskWare/Android.Luashare.a[exp]	低	该应用程序运行后诱导加入指定 qq 群，进行分享推广引流。可能造成用户资费消耗，存在一定的风险，建议谨慎使用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft SharePoint 远程代码执行漏洞（CVE-2019-1257）	高	当 Microsoft SharePoint 软件无法检查应用程序包的源标记时，会触发远程代码执行漏洞。经过身份验证的攻击者可能通过向受影响的 SharePoint 服务器发送经特殊设计的请求来利用此漏洞。
	较为活跃样本	Trojan/Win32.Nvert	中	此威胁是一种窃取用户信息的木马类程序。该家族会在删除计算机中的文件，向其他人发送垃圾邮件，占用系统内存等。
		Trojan[Ransom]/Win32.Zerber	中	此威胁是一种勒索软件家族。该家族的样本在运行后，会加密系统上多种文件格式的文件，并将文件的扩展名更改为 .zerber，在加密后，该样本会在全部的文件夹下各放置一封 HTML 格式的勒索信说明情况。
		Trojan/Win32.Rofin	中	此威胁是一种木马程序。该病毒家族会注入到系统进程中，下载并运行其他文件，接受来自黑客的命令并执行。
		GrayWare[AdWare]/Win32.OneStep	低	此威胁是一种可以弹出广告的灰色软件程序。该家族样本运行后会添加开机自启并注入到系统进程中。该家族样本收集用户信息，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。
		GrayWare/Win32.iBryte	低	此威胁是一种广告类程序。该家族可以在电脑上打开后门，并注入其他恶意程序。该家族还可以连接远程服务器，让黑客可以访问电脑并窃取用户的个人资料。

（上接第一版）

到蠕虫反复感染对应问题的用户建议采取以下缓解措施：

1) 对局域网内的所有主机采取断网操作。

2) 根据受感染终端的操作系统版本和相关病毒所使用功能的漏洞信息，安装对应的安全补丁。

3) 在不影响用户业务的前提下封堵 445 常见等传播端口，通过杀毒工具进行查杀。

4) 逐步恢复网络并通过抓包工具确认网内是否存在恶意流量，并对全网终端安全状态进行确认。

• 后续安全建议

本次事件主要是由于第三方厂家提供的设备带毒入网后引起的病毒内网传播感染事故，是一起典型的由供应链引起的病毒感染传播事件，我们对用户提出了后续安全建议：

1. 技术方面

1) 所有第三方提供的设备在入网前需进行严格的上线检测，至少应采取安全配置检查、恶意代码检测排查、漏洞修复以及配置加固等手段，对入网设备的安全合规性进行严格审查。

2) 设备上承载的操作系统、数据库、中间件及应用等应通过官方渠道或经认证的安全下载渠道获取，避免通过非官方渠道获取引入潜在的安全风险。

3) 针对已上线设备的应用软件、数据及系统的安装与更新，应建立内部统一部署平台，统一补丁源，实现验证留存，应通过带有恶意代码检测和安全验证机制的辅助检测系统的摆渡中间机进行数据交换。

4) 设备最终交付上线前，应使用病毒防护软件对其进行全面病毒检查，必要时需要安全专家协助，确保当前设备的安全状态后方可上线。

5) 因设备上线后的运转状态相对稳定，很少进行更新和修改，应配置白名单防御策略，为系统建立参考 STIG 标准的配置策略，保证系统上线后的运行安全。

6) 建议依托专业的安全服务团队提升安全事件的应急响应能力。一旦出现安全问题，能够在第一时间采取正确措施，为专业团队现场处置提供初步的威胁排查方法及处置建议。

2. 管理方面

1) 开展内部与外部供应链审查工作，政企机构不仅需审查自身内部的基础架构，还应对供应商及合作伙伴进行审查。虽然内部系统可能具有一系列安全措施用以阻止各种网络攻击，但第三方合作伙伴可能在此阶段缺少有效的防御手段。因此，需要对软硬件供应商开展彻底审查工作，只有通过审查后才能将其提供的软硬件、系统等集成至内部基础架构中。

2) 在条件允许的情况下，用户应要求供应商遵循最小暴露面的原则，制定相关流程、标准和法务协议，对用户作出入网设备的明确的安全规格需求。协议应要求供应商及时通告任何内部安全事件以及定期进行安全报告，以确保其安全状态，并培养供应商开发人员安全意识，同时通过可信的正规渠道发布软件产品，通过数字签名认证机制使软件遭到外部篡改、病毒感染等攻击等情况易于被发现。

3) 定期对用户内部员工及第三方供应商开展安全培训工作，分享供应链安全最佳实践。

3. 安全产品和工具使用方面

1）安天资产安全运维平台与智甲终端防御系统组合部署使用，可以实现统一内网端点资产管理、统一内网补丁分发升级、支持安全等级分组的模板化安全策略加固。

2）安天智甲通过安天下一代威胁检测引擎可以精准检测海量病毒，对 Rootkit、感染式病毒、扫描蠕虫、宏病毒等困扰内网用户的事件有良好的处理效果。同时借助主防机制和分布式主机防火墙，能有效拦截针对端点的各种攻击。

3）基于安天探海威胁检测系统部署，可以通过安天下一代威胁检测引擎精准检测恶意代码传播，可以及时发现内网扫描、横向移动等攻击动作。

4）安天追影安全分析系统可以增加安全分析的深度，发现漏洞利用，呈现威胁行为，并生产可利用威胁情报。

5）安天拓痕处置工具可以针对主机系统进行定期安全检查、应急检查、证据固化和风险文件提取，进行主机侧的深度分析处置。

对规模化的高价值信息资产防护，仅仅依靠产品组合使用无法保证安全，应以叠加演进模型，进行能力导向的安全规划建设，依次做好基础结构安全、纵深防御、态势感知与积极防御、威胁情报等安全工作，建设动态综合安全防御体系。

微信扫描二维码阅读原文

SAP 通过 2019 年 10 月安全更新修补 2 个超危漏洞

作为本周的 2019 年 10 月安全补丁日的一部分，SAP 本周发布了七个新的安全说明，其中两个说明被评为热门新闻（严重）。这些说明中最重要的是解决了 SAP NetWeaver Process Integration 的 B2B 附件的 AS2 适配器中缺少身份验证检查的问题。漏洞跟踪为 CVE-2019-0379，CVSS 评分为 9.3。成功利用此漏洞可能导致敏感数据被盗或操纵数据，也可能使攻击者可以访问管理功能和其他特权功能。第二个热门新闻说明修补了 SAP Landscape Management 企业版 3.0 版中的一个信息泄露漏洞。该安全漏洞的跟踪记录为 CVE-2019-0380，CVSS 评分为 9.1。

（原文链接：https://www.securityweek.com/sap-patches-critical-vulnerabilities-october-2019-security-updates）

BitPaymer 勒索软件团伙利用了 iTunes 中的零日漏洞

网络安全公司 Morphisec 在 8 月份遭受 BitPaymer 勒索软件攻击的汽车行业企业网络中发现了这种攻击和零日漏洞。苹果本周在 Windows 版 iTunes 和 Windows 版 iCloud[1，2] 中修补了零日漏洞。 实际的问题存在于两个产品附带的 bonjour updater 组件中。零日漏洞不允许 BitPaymer 勒索软件获得管理员权限，但它确实欺骗了本地安装的防病毒软件。在发现零日漏洞的证据后，Morphisec 向苹果报告了该问题，操作系统制造商于本月对其进行了修补。

（原文链接：https://www.zdnet.com/article/ransomware-gang-uses-itunes-zero-day/）