安天周观察

主办：安天　2017 年 11 月 06 日（总第 110 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天智甲成功入围中央国家机关政府采购名录

近日，中央国家机关政府采购中心发布了《中央国家机关 2017 年软件协议供货采购项目中标公告》，安天智甲终端防御系统（英文简称 IEP，以下简称“安天智甲”）成功入围。

中央政府采购对投标企业有极高要求，也是各地方政府采购的重要依据。采购单位覆盖中央直属近万个机关单位，是中央垂直单位对所有供应厂商的一次严格筛选，入围的厂商及产品必须通过专家的多次评审，安天智甲以在产品技术、品牌口碑、安全服务等各方面具备的突出优势，成功入围此次采购名录。

安天是专注于威胁检测防御技术的能力型安全厂商，以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命。成立十七年来，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

此次成功入围标志着安天通过了国家官方机构的考验，获得了权威部门认可。安天将不负所望，为用户提供自主可靠的杀毒软件产品及优质的安全服务，守护用户的终端网络安全。

■ Sage 勒索软件新变种：新增反分析和提权功能

飞塔公司（Fortinet）发出警告称，今年年初浮出水面的 Sage 勒索软件新增反分析功能，以达到提权和逃避分析的目的。

Fortinet 还发现，Sage 的代码显示，更多字符串经过加密处理试图隐藏恶意行为。恶意软件开发人员使用 ChaCha20 加密算法，并且每个加密的字符串均拥有自己的硬编解密密钥。

这款恶意软件还执行各种检查，以确定是否会被加载到沙盒或虚拟机环境进行分析。

Sage 会枚举设备上的所有活动进程，计算每个进程的哈希值，然后对比黑名单进程的硬编列表检查哈希值。此外，Sage 还会检查完整的执行路径，当发现诸如 sample、malw、sampel、virus、{sample’s MD5} 和 {samples’s SHA1} 之类的字符串时，便会终止运行。

Sage 新变种还会检查计算机和用户名，以此确定是否与沙盒环境中通常使用的名字一致。新变种还使用 x86 指令 CPUID 获取处理器信息，并与 CPU 黑名单 ID 列表进行对比。

更为重要的是，这款恶意软件会枚举服务控制管理器下运行的服务，检查计算机是否在运行反病毒软件。同时还会对比一组 MAC 黑名单地址进行检查。

Sage 能利用已修复的 Windows 内核漏洞（CVE-2015-0057）或滥用 eventvwr.exe 并执行注册表劫持绕过用户帐户控制（UAC），从而达到提权的目的。（来源：https://www.easyaq.com/news/1545708570.shtml）

■ iPhone 的一个 seriousprivacy 问题，应用程序开发者可以通过启用摄像头默默地查看你的照片和记录你的生活

奥地利开发商和谷歌工程师，菲利克斯·克劳斯，已经发现了一个在苹果 iPhoneshang 上的 seriousprivacy 问题。

克劳斯表示，该问题是苹果软件处理相机的方式造成的直接后果。如今几乎所有的 application，包括 WhatsApp,Facebook, 和 Snapchat, 都会请求访问你的相机允许用户应用程序内拍照。小心，它不是一个安全漏洞，相反，它由苹果的设备实现，但是可以被恶意利用静静地监视用户的活动。

一旦相机用户授予权限，开发人员可以，访问前面和后面的相机；随时记录你的应用前景；拍照和视频；立即上传图片 / 视频需要；运行实时人脸识别检测面部特征或表达式。（来源：http://securityaffairs.co/wordpress/64958/digital-id/iphone-camera-control.html）

一周简讯

- 研究者发现 Chrome 广告件伪装成扩展程序
- 安全厂商发布 QtBot 恶意传播活动的分析
- 安全厂商揭示 ONI,MBR-ONI 勒索攻击活动
- 安全厂商在移动 APP 中发现恶意挖矿软件
- Firefox 阻塞 HTML5 画布指纹来保护隐私

安天 CERT 搜集整理，详情请见：http://bbs.antiy.cn

每周安全事件

类 型	内 容
中文标题	“沉默”木马记录了银行个人电脑的伪视频，用来帮助网络抢劫
英文标题	"Silence" Trojan Records Pseudo-Videos of Bank PCs to Aid Bank Cyber-Heists
作者及单位	Catalin Cimpanu；BleepingComputer
内容概述	卡巴斯基实验室的专家们发现了一种新的木马，专家命名为“沉默”。该木马大多数袭击是针对俄罗斯的银行。 专家们分析沉默木马是如何攻击的。这一切都是从黑客进入银行职员的电子邮件帐户开始的。这可以通过恶意软件完成，或者因为员工已经从公开泄露的数据集中包含的帐户重新使用密码。 沉默小组使用银行员工的受损帐户向其他银行工作人员发送钓鱼邮件。这些电子邮件包含 CHM（编译的 HTML）文件附件。如果受害者下载并打开此文件，CHM 文件将运行下载并安装第一阶段恶意软件有效负载的 JavaScript 命令。在这种特殊情况下，它是一个 Win32 可执行文件，可以在受感染的主机上收集数据，并将信息发送给攻击者的命令和控制（C & C）服务器。
链接地址	https://www.bleepingcomputer.com/news/security/-silence-trojan-records-pseudo-videos-of-bank-pcs-to-aid-bank-cyber-heists/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 9 个移动平台恶意代码和 4 个 PC 平台的恶意代码值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.capushe.a[rmt,exp] 2017-10-31	该应用程序运行后隐藏图标，激活设备管理器，上传手机固件信息，远程控制，接收指令后私发短信或推送广告，下载未知应用，建议立刻卸载。（威胁等级中）
		Trojan/Android.reeve.a[prv,exp,rog]] 2017-11-01	该应用程序运行后会上传用户手机固件、位置、安装包等信息，加载广告子包，推送广告，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.droidjack.a[prv,rmt,spy] 2017-11-02	该应用程序是一款远控程序，运行后接受远控指令，窃取用户短信、联系人、通话记录、地理位置，浏览器历史记录等隐私信息，私自监听通话、拦截短信，并上传至服务器，造成用户隐私泄露，请立即卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.emial.gj[prv]	该应用程序为拦截马，伪装成中国移动诱骗用户，获取设备管理器权限，私发短信，后台拦截短信并上传，泄漏用户隐私，请立即卸载。（威胁等级中）
		G-Ware/Android.E4ALocker.d[rog,fra,lck]	该应用程序运行后置顶界面，模仿 WannaCry 的勒索界面诱骗勒索用户扫码付费解锁，使用户手机无法正常使用，建议立即卸载。（威胁等级低）
		G-Ware/Android.FakeWzry.b[fra,exp]	该应用程序伪装王者荣耀充值插件，运行加载欺诈性充值界面，诱导用户分享、付费使用，程序本身无实际功能，可能造成用户资费损失，建议不要使用。（威胁等级中）
		Trojan/Android.PhoneTools.b[prv,spy]	该应用程序为手机监控工具，安装无图标，运行无明显提示，警惕该程序被恶意利用，窃取用户、短信、通话记录、位置信息，造成隐私泄露。（威胁等级中）
		G-Ware/Android.StealMoneyGame.o[exp,pay,rog]	该应用程序为游戏应用，运行后联网上传固件信息获取支付信息，静默发送注册短信，有提示发送付费短信，但提示不明显，拦截并删除包含特定字符的短信，可能造成用户隐私泄露和资费消耗，请谨慎使用。（威胁等级低）
		G-Ware/Android.Downloader.do[exp,rog]	该应用程序运行解密加载子包，子包中静默下载应用，造成用户资费消耗和未知风险，请立即卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Office 远程代码执行漏洞 CVE-2017-11826	微软 Office 系列办公软件（Word、Excel、Powerpoint 等）存在远程代码执行漏洞（CVE-2017-11826）。目前该漏洞影响范围包括 Office 2007、2010、2016 三个版本。该漏洞通过特制 RTF 格式文档感染 Windows 操作系统，系统一旦被感染，可被植入木马后门，窃取用户数据。（威胁等级高）
	较为活跃样本	Trojan[Backdoor]/Win32.Thunkan	此威胁是一种可以释放恶意代码的木马程序。该家族样本运行后释放恶意代码，一般为 sys 格式，有一定威胁。（威胁等级高）
		Trojan[Banker]/Win32.Banaris	此威胁是一种可以监视用户系统的木马程序。该家族样本运行后连接远程服务器，记录用户系统信息并回传给攻击者。（威胁等级中）
		Trojan[Ransom]/Win32.Cryptor	此威胁是一个勒索软件家族。该家族的样本在执行后会加密多个类型的文件，并生成一个 KEY 文件（秘钥文件）和一个 LST 文件（加密过的加密文件列表），在加密后向用户勒索赎金。（威胁等级中）

安天智甲有效防御最新宏逃避手段

■【事件概述】

安天在近期捕获的样本中发现一例利用“自动”宏 AutoClose 来逃避沙箱检测的 Office 样本。攻击者诱使受害者点击垃圾邮件中的恶意链接，下载恶意文档。当用户打开 Office 文档文件并且启用宏时，并无异常，一旦用户关闭文档，AutoClose 会立即调用 PowerShell 程序下载其他恶意样本载荷，载荷可能是银行木马、勒索软件等。攻击者可以利用此技术逃避具有宏分析能力的沙箱。随着攻击者持续对该技术的使用和改进，加之其易于实现，这种攻击手段正在成为越来越多恶意代码的常见功能。

目前，安天智甲终端防御系统（英文简称 IEP，以下简称“安天智甲”）对此类威胁已经能够有效防御，保障用户的终端安全。

■【样本分析】

当用户关闭文档后，即会执行以下恶意宏代码。

```
Sub AutoClose()
Application.Run "jGxtAEORSi"
End Sub
Public Sub jGxtAEORSi()
Dim NwcqRUKSrRlHRZgljZYoAo
NwcqRUKSrRlHRZgljZYoAo = " love and love "
tVhzwszkcKhl = ActiveDocument.Name
lenght = Len(tVhzwszkcKhl)
If lenght > 30 Then
MsgBox NwcqRUKSrRlHRZgljZYoAo
Else
pCHPhSPPVlEQvs (NwcqRUKSrRlHRZgljZYoAo)
End If
End Sub
```

恶意宏部分代码

首先检查文件名长度是否超过 30 字符，若超过，攻击者则认为是分析人员正在分析以 md5，sha256 形式命名的文件。所以如果长度超过 30 字符，则弹出消息框：

否则解析文件中的 base64 编码。解码数据如图

base64 解码数据

利用 cmd 创建目录 dImJbtbSOG，调用 PowerShell 下载恶意样本 YYHhvsddE.exe，由于链接失效未能下载原始载荷，关联分析 YYHhvsddE.exe 文件名得到勒索软件 Locky 样本 36e3d3024719d6e96f99300cc4941730，最后创建 YYHhvsddE.exe 进程并执行攻击。

■【防御技术】

安天智甲的主动防御机制根据 Office 文档宏函数和 PowerShell 运行原理，建立了一套三重拦截手段，可提供有效防护：

第一，格式深度分析 Office 文档，抽取宏函数，针对加密宏进行解密还原，并进行代码分析、规则匹配；

第二，Office 文档运行后，监控文档是否恶意修改系统环境或运行恶意代码，并向用户告警；

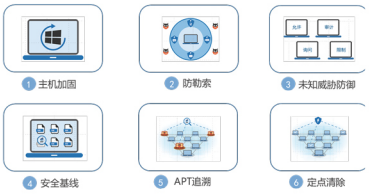
第三，在默认的防御策略中禁止了 PowerShell、WScript 脚本的调用，有效防御注入式和宏脚本类恶意代码，并向用户告警。

根据本次恶意代码运行跟踪情况，安天智甲能够有效防御此恶意代码的启动，如下图：

■【产品展示】

安天智甲是一款面向政府、军工、能源、金融、交通、运营商等各行业用户的企业级防护产品，产品集成了病毒检测查杀、系统加固、主动防御、介质管控、文档保护、行为画像等功能，并能有效与管理中心和安天态势感知产品互动，协助客户建立更全面的资产防护体系和风险认知能力，使态势感知能够有效落地。

1、安天智甲：更强大的功能——不仅仅是反病毒



2、安天智甲：更广阔的适配性——全面适配国产化系统

3、安天智甲：更精准的威胁感知——3D可视化拓扑、感知全局态势

终端威胁详情展示

网络拓扑结构展示

4、安天智甲：更全面的场景应用——多场景支持、满足差异化需求

安天发布《新型僵尸网络“Wonder Botnet”分析报告》

近日，安天CERT（安全研究与应急处理中心）在梳理网络安全事件时注意到并拦截到了一个新型的僵尸网络，名为“Wonder botnet”。该僵尸网络由国外安全研究人员发现，其标榜可以免费创建一个Netflix服务的高级账户，但下载安装之后却并非此工具，而是安装了一个BOT，并将其命名为“Wonder botnet”，它的命令与控制服务器是隐藏在一个网站的后方，是另一个网站的镜像网址。

安天CERT拦截到的恶意代码实体使用.NET框架编写。样本运行后尝试连接“pastebin.com”域名来测试用户系统是否联网，如果不能联网，则程序会出现崩溃界面。如果正常通讯，则恶意代码会连接网络下载BOT恶意代码实体。该僵尸网络恶意代码在临时目录释放恶意文件副本，创建C:\ProgramData\Microsoft\Windows\StartMenu\Programs\ Startup”注册表来添加启动项，通过查询虚拟机的相关DLL文件来反沙箱检测，创建MD5算法的ID生成感染标志。

僵尸网络的功能包括：更新升级自身、启动、停止自身、开机与重启用户机器，添加与更改文件，屏幕截图，创建压缩包文件进行收集信息并回传至远程服务器。

安天CERT提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要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好习惯。目前，安天追影产品已经实现了对该类恶意代码的检出。

病毒程序

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

文件被页面手工提交发现，经由YARA自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、数字证书鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据智能学习鉴定器将文件判定为病毒程序。

文件名	c3f5f5bfe39b55ffe0343950e0a4bf0433c35679a01daf07ce6c0ccc7d4da9b7
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	366 KB
MD5	486954967E02A2E1577BD7DD91026102
病毒类型	病毒程序
恶意判定/病毒名称	Virus[Tool]/MSIL.Injector
判定依据	智能学习

运行环境

操作系统	内置软件
Windows XP 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
延时	★★★

常见行为

行为描述	危险等级	行为描述	危险等级
获取系统内存	★★	打开自身进程文件	★
查找指定内核模块	★	创建特定窗体	★

该文件具有以下行为：延时；获取系统内存；打开自身进程文件；查找指定内核模块；创建特定窗体；获取驱动器类型；获取系统版本；获取计算机名称；获取主机用户名称；启动服务；访问dns；独占打开文件；查找浏览器进程；获取socket本地名称；查找特定窗体；读取自身文件；释放PE文件。

获取驱动器类型	★	获取系统版本	★★
获取计算机名称	★	获取主机用户名称	★
启动服务	★	访问dns	★
独占打开文件	★	查找浏览器进程	★★
获取socket本地名称	★	查找特定窗体	★
读取自身文件	★★	释放PE文件	★

进程监控

PID：232	创建：dumprep.exe
	命令行：C:\WINDOWS\system32\dumprep.exe 988 -dm 7 7 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WERae08.dir00\svchost.exe.mdmp 16325836412031840
PID：348	创建：dumprep.exe
	命令行：C:\WINDOWS\system32\dumprep.exe 988 -dm 7 7 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WERae08.dir00\svchost.exe.hdmp 16325836412031852
PID：576	创建：dwwin.exe
	命令行：C:\WINDOWS\system32\dwwin.exe -d C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WERae08.dir00\manifest.txt
PID：1296	创建：wuauclt.exe
	命令行："C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3dc]SUSDSd9a58876cda26049acd3d3258e202fe2