安天周观察

主办：安天　2017 年 6 月 19 日（总第 91 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天参加中俄总理定期会晤委员会通信与信息技术分委会第十六次会议

6 月 4 日至 8 日，中俄总理定期会晤委员会通信与信息技术分委会第十六次会议在俄罗斯首都莫斯科召开，安天随中国代表团出席了信息技术与网络安全工作组会议。这是继 2015 年后，安天第二次参加该会议。

在会议举行期间，来自中俄两国的网络与信息安全企业就各自关心的问题交换了意见，并就上报分委会的会议纪要达成共识。卡巴斯基 (Kaspersky) 负责重要基础设施安全方面的主管与安天的代表就威胁情报交换等问题进行了深入交流与讨论。

会议期间，安天还拜访了俄罗斯另外一家网络安全企业大蜘蛛 (Dr.Web)，并与其 CEO、海外合作负责人就在中国进行恶意代码研究等议题进行了深入交流。这是两年后，安天再次访问大蜘蛛公司。

安天荣获“一带一路”国际高峰合作论坛“安保贡献突出集体”荣誉

5 月 14 至 15 日，“一带一路”国际合作高峰论坛（以下简称“高峰论坛”）在北京召开。安天作为网络安保提供商荣获了由“高峰论坛”筹委会安全保卫组颁发的“安保贡献突出集体”荣誉。

“高峰论坛”是国际社会各方共享互利合作成果的盛会，也是加强国际合作，对接彼此发展战略的重要合作平台，因此，做好网络安全保障工作至关重要。

安天在本次“高峰论坛”网络安全保卫工作中，按照安保工作的统一部署，高质高效的完成了技术检测、24 小时实时监测、应急处置、驻站值守等支持工作，出色完成了各项安保任务，有效保障了“高峰论坛”期间的网络安全。

安天作为连续十年，五次蝉联“国家级”网络安全应急服务支撑单位的厂商，多次在重大网络事故和网络安全事件的响应中发挥关键作用，曾参加过十七大、十八大、2010 年起的历届两会、北京奥运会、上海世博会、广州亚运会、2014 年 APEC 会议、抗战胜利 70 周年阅兵、G20 峰会等重大活动的安保工作，并荣获重大活动信息安全保卫工作突出贡献奖。

安天会一如既往，在维护国家网络安全工作中贡献自己的一份力量。

安天发布《针对『暗云Ⅲ』的样本分析及解决方案》

5 月 26 日 19 时，我国发生了一次大规模的 DDoS 攻击事件。参与攻击的源地址覆盖广泛，几乎在全国所有省市运营商的骨干网络上均有明显活动。研究人员将此次攻击命名为：RainbowDay，暗云Ⅲ。

6 月 12 日，CNCERT 综合安天等厂商对已获知的样本情况和分析结果，发布《关于“暗云Ⅲ”木马程序有关情况通报》。

6 月 14 日，安天发布《安天针对“暗云Ⅲ”的样本分析及解决方案》，报告对“暗云Ⅲ”进行全面样本分析并给出解决方案和工具。“暗云Ⅲ”木马通过游戏微端、外挂、私服登录器等方式进行传播，并利用多种技术手段增强其隐蔽性。经过多次取证分析发现，“暗云Ⅲ”恶意代码的感染量较大，并且其恶意代码的功能非常复杂，可利用带有正常数字签名的文件进行传播，同时具有下载文件执行、刷流量、DDoS 攻击等行为。

根据“暗云Ⅲ”木马程序的传播特性，安天建议用户近期采取积极的安全防范措施。推荐安装安天智甲终端防御系统和安天 RainbowDay（暗云Ⅲ）专杀工具。针对未感染用户，安天智甲可有效防御此类 Bootkit 恶意代码，拦截恶意代码下载的可疑文件，阻断其进行网络行为。针对已感染用户，安天专杀工具可对“暗云Ⅲ”木马进行查杀，并对系统进行修复。

报告原文　工具下载

每周安全事件

类 型	内 容
中文标题	恶意软件 Industroyer 直击电网，拉响工控基础设施威胁警报
英文标题	Experts spotted Industroyer ICS Malware and linked it to Ukraine Power Outage
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，据外媒报道，杀毒软件公司 ESET 研究人员发现一款新型恶意软件 Industroyer，旨在破坏工控系统 (ICS) 工作流程（特别是变电站 ICS)。近期，研究人员发表详细报告并推测该恶意软件与发生在 2016 年 12 月的乌克兰变电站攻击事件有关。 根据工控安全公司 Dragos 提供的理论攻击描述，黑客使用恶意软件 Industroyer 在 HMI 中将断路器开启命令设置为无限循环操作，导致目标系统变电站频繁出现断电现象。此外，目标设备操作人员无法通过操控 HMI 关闭断路器。为恢复正常通信，操作人员必须先用变电站扰乱通信后手动修复该问题。另外，黑客还可通过开启无限循环使断路器不断开关，触发保护机制、致使变电站关闭。
链接地址	http://securityaffairs.co/wordpress/59989/malware/industroyer-malware.html

每周值得关注的恶意代码信息

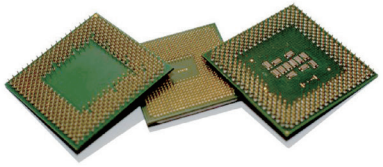
经安天检测分析，本周有 7 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.KsClean.a[exp] 2017-06-10	该应用程序运行后释放恶意子包，诱导用户安装以及激活设备管理器，后台推送广告，会造成用户流量资费损耗，建议卸载。（威胁等级高）
		RiskWare/Android.Bodog.a[exp] 2017-06-13	该应用程序是一款博彩应用，运行后会加载博彩网站，建议注意保护自身财产，使用健康绿色软件。（威胁等级低）
		Trojan/Android.Vampire.a[sys，exp，prv]2017-06-13	该应用程序运行私自提权，静默下载安装恶意应用，进行恶意吸费、隐私窃取、恶意推广等高危行为，会造成用户隐私泄露和资费损耗。（威胁等级中）
	较为活跃样本	Trojan/Android.E4AQQspy.ap[exp，prv]	该应用程序伪装成 QQ 相关程序，诱导用户填写 QQ 账号密码并且上传到指定服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.emial.fv[prv，fra，exp]	该应用程序伪装 Samsung 相关应用，监听短信、地理位置、通话、QQ 语音并通过邮件转发，将窃取的短信发送到指定号码。造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级高）
		Trojan/Android.Hqwar.e[prv，exp，rmt]	该应用程序伪装成正常应用，运行会隐藏图标，接收指令上传通讯录和短信，同时访问钓鱼界面，诱导用户输入银行账号密码，建议立即卸载，避免造成隐私泄露和资财产损失。（威胁等级高）
		PornWare/Android.sexgame.n[exp，rog]	该应用程序为色情游戏应用，诱导用户点击确认，其扣费提示不明显，用户会在无意操作中完成支付，造成用户的资费消耗，建议谨慎使用。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Apache Hadoop 远程权限提升漏洞 (CVE-2017-7669)	Apache_Hadoop2.8.0，3.0.0-alpha1，3.0.0-alpha2 版本中，LinuxContainerExecutor 没有有效验证输入，以 root 权限运行 docker 命令。启用 docker 功能后，经身份验证的用户可以 root 权限运行命令。（威胁等级高）
	较为活跃的样本	Trojan[Backdoor]/Win32.Agent	此威胁是一种木马类后门程序，是一个通过代码基因来定性的木马类程序，家族变种之间具有相同或者相似的源码和核心技术。它可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级高）
		Trojan[Downloader]/Win32.Delf	此威胁是使用 delphi 语言编写具有下载行为的木马类程序，运行后会连接网络并下载其它恶意程序执行。通过以邮件、挂马、捆绑正常软件来进行传播。（威胁等级中）
		Trojan[Dropper]/Win32.FrauDrop	此威胁是一种具有捆绑行为的木马类程序。该家族会损坏被感染电脑的注册表文件，阻止用户访问系统。该家族会随系统运行自启动，并利用连续弹窗和虚假警告消息欺骗用户，还会损坏任务管理器和系统还原功能。此外，该家族会感染操作系统，收集用户隐私信息发送给黑客。（威胁等级中）
		Trojan[Backdoor]/Linux.Mayday	此威胁是一种木马类后门程序，在 linux 平台上运行。它可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级中）

Platinum 首次利用英特尔芯片管理功能

Michael Mimoso / 文　安天公益翻译小组 / 译

近日，在东南亚运作的 Platinum APT 组织利用英特尔芯片的功能，将恶意软件和漏洞加载到受感染的机器上。



近期，微软发布了对 Platinum 组织的最新研究报告，该组织热衷于使用以前未开发的资源攻击计算机并规避检测。

在 2016 年 4 月，微软介绍了 Platinum 如何利用 Windows Server 2003(Windows 8 已经将其删除) 引入的热补丁 (hotpatching) 功能，以便在运行的进程中注入恶意代码。Platinum 的目标主要是战略性的，包括政府机构、国防承包商和情报机构，以及电信等关键行业。

微软表示，Platinum 的一个文件传输工具能够利用英特尔主动管理技术 (AMT)，特别是其串行 LAN(Serial-over-LAN，简称 SOL) 通信通道，在目标机器上运行恶意代码。微软和英特尔表示，这是 APT 组织首次以这种方式利用芯片组。

微软称：“该通道独立于操作系统，通过其上的任何通信不会被主机设备上运行的防火墙和网络监控程序发现。在该事件之前，我们没有发现任何恶意软件利用 AMT SOL 功能进行通信。”

微软将调查结果告知了英特尔。两家公司表示，这不是 AMT 的漏洞，而是属于其功能的滥用。巧合的是，他们在 5 月初披露了一个严重的 AMT 提权漏洞，该漏洞允许攻击者远程访问和完全控制受感染的机器，但它与该事件无关。

微软在报告中表示，它仅在少数机器上发现了文件传输工具。

微软表示，该攻击有先决条件：因为 AMT 是默认关闭的，因此攻击者需要获得管理员权限。

微软表示：“目前尚不清楚，Platinum 能否配置工作站来使用其功能，或者搭载以前启用的工作站管理功能。无论哪种情况，在利用功能之前，Platinum 都需要在目标系统上获得管理员权限。”

AMT 功能存在于 Intel vPro 处理器和芯片上，用于远程管理。SOL 通过 TCP 公开一个虚拟串行设备，并独立于主机服务器上运行的操作系统和网络。只要主机设备以物理方式连接到网络，AMT 和 SOL 就能够利用英特尔管理引擎的网络堆栈进行通信。因为它绕过主机服务器的网络堆栈，因此不会被主机上的防火墙阻止。主机不会发现任何恶意流量，包括服务器上运行的任何杀毒软件或入侵检测软件也很难发现。

微软表示，Platinum 自 2009 年以来一直在亚洲活跃，并非常谨慎地保密其攻击工具，包括零日漏洞。

一年多前，研究人员披露 Platinum 利用 Windows 热补丁功能。他们利用该功能，将恶意代码注入到运行的进程中，而无需重启受感染的服务器。像 SOL 一样，热补丁功能需要管理员权限，这意味着攻击者必须首先进行感染机器。

与许多其他 APT 组织一样，该组织利用网络钓鱼活动在网络上创建据点。Platinum 使用受感染的 Office 文档，利用未修复和已知的漏洞将后门程序和其他代码安装到受感染的机器上。

原文名称	Platinum APT First to Abuse Intel Chip Management Feature
作者简介	Michael Mimoso，Threatpost 编辑。
原文信息	2017 年 6 月 9 日发布于 Threatpost， 原文地址 https://threatpost.com/platinum-apt-first-to-abuse-intel-chip-management-feature/126166/
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。

安天发布《Fireball 家族样本分析报告》

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，名为 Fireball 的恶意代码家族正在世界范围内活跃。经分析，该家族具有控制感染机器的浏览器，监控流量、窃取数据，利用应用 Deal Wifi 和 Mustang 浏览器捆绑传播等恶意行为。此外，Fireball 样本属于广告件，被感染的机器会成为僵尸网络的一部分。

Fireball 使用捆绑的方式进行传播，用户免费下载软件后，该恶意软件会自动安装恶意浏览器插件，控制受害者的浏览器配置，替换默认主页和搜索引擎。该虚假搜索引擎为：trotux.com，并将用户的搜索请求重定向到雅虎，但植入了追踪的像素，用来收集受害者信息的捆绑软件中有一些是其他应用，比如 Deal Wifi 和 Mustang 浏览器或者“Soso Desktop”、“FVP 图片查看器”。

Fireball 家族样本具有一定复杂性，使用了反安全软件的技术，以及多层架构和 C&C 服务器，能够监控受害者的网络流量，会在目标系统中执行恶意代码、安装插件，甚至直接安装恶意软件，以此在受害者系统和网络中留下后门。

研究人员称，全球范围内约有 2.5 亿台计算机受影响，其中 20% 处在企业网络中。受感染的机器遍布各个国家，包括印度、巴西、墨西哥、印尼、美国等。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，不要通过非官方网站下载软件程序，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此类样本的检出。

木马程序

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

文件被内部组件发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、数字证书鉴定器、可交换信息 (EXIF) 鉴定器、动态行为 (Windows7) 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 BD 静态分析鉴定器、静态分析鉴定器将文件判定为木马程序。

文件名	e3f69a1fb6fcaf9fd93386b6ba1d86731cd9e5648f7cff5242763188129cd158
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	98 KB
MD5	69FFDF99149D19BE7DC1C52F33AAA651
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.TGeneric
判定依据	静态分析

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office2007、flash、wps、FoxitReader、AdobeReader

其他行为

行为描述	危险等级	行为描述	危险等级
获取系统内存	★★	获取 socket 本地名称	★
连接网络	★	映像挂钩	★★
自启动	★		

根据动态行为 (Windows7) 得出该文件具有以下行为：获取系统内存、获取 socket 本地名称、连接网络、映像挂钩、自启动。

根据动态行为 (默认环境) 得出该文件具有以下行为：延时、独占打开文件、获取系统内存、获取主机用户名称、查找浏览器进程、查找指定内核模块、获取计算机名称、获取系统版本、获取 socket 本地名称、连接网络、映像挂钩、获取驱动器类型、创建特定窗体、自启动。

运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认、ie6、office2003、flash、wps、FoxitReader、AdobeReader

危险行为

行为描述	危险等级
延时	★★★

其他行为

行为描述	危险等级	行为描述	危险等级
独占打开文件	★	获取系统内存	★★
获取主机用户名称	★	查找浏览器进程	★★
查找指定内核模块	★	获取计算机名称	★
获取系统版本	★★	获取 socket 本地名称	★
连接网络	★	映像挂钩	★★
获取驱动器类型	★	创建特定窗体	★
自启动	★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=69FFDF99149D19BE7DC1C52F33AAA651