安天周观察

主办：安天　2016 年 5 月 30 日（总第 41 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

习近平总书记视察安天哈尔滨总部

5 月 25 日，习近平总书记在黑龙江调研期间，在黑龙江省委书记王宪魁、省长陆昊、哈尔滨市委书记陈海波、市长宋希斌的陪同下，视察了安天哈尔滨总部。安天创始人、首席技术架构师肖新光、安天哈尔滨总部负责人李岱为习总书记做参观引导，并进行汇报。

安天负责人向习总书记汇报了安天的核心技术——反病毒引擎的相关情况。安天人对总书记讲的“ 核心技术要取得突破，就要有决心、恒心、重心。”感同身受，创业以来，以“不怕死在反病毒引擎”上的决心，以十五年磨一剑的恒心，先后根据不同时期的威胁特点，分别以“高速网络检测引擎”、“先进移动检测引擎”和 “高级威胁辅助检测引擎”为重心，进行了艰苦的研发工作，取得了一定的成绩。

总书记网信座谈会讲话中提出了做好“全天候全方位态势感知工作”的工作要求。安天负责人通过网络安全态势感知系统，介绍了安天对病毒疫情和高级威胁的捕获能力，并通过安全事件场景可视化再现模块，详细地向习总书记介绍了安天对几起 APT 攻击事件的捕获、分析、溯源过程。总书记非常仔细地倾听，对安天负责人拿起的每一份材料都接过去翻看。

总书记非常看重关键基础设施的安全防护，强调关键信息基础设施是“网络安全的重中之重，也是可能遭到重点攻击的目标。”安天负责人汇报了和国防科大等高校进行的合作项目，联合研发团队正在研发利用超算资源，实现对关键信息基础设施的仿真模拟和防护演练工作，特别展示了去年某国国家电网遭遇网络攻击停电事件的仿真演示。习总书记非常细致地观看了演示，并认真翻看了安天对相关事件的长篇分析报告。安天负责人进一步向习总书记汇报介绍了围绕安天反病毒引擎核心技术研发的 APT 高级威胁检测、防护产品和解决方案，以及其在相关部委与关键基础设施中的使用及部署情况。

安天负责人向总书记汇报：在网络安全和信息化工作座谈会后，同志们信心与干劲更足了，思路清晰了。总书记对安天负责人说，**“你们也是国家队，虽然你们是民营企业。”**这不仅是总书记对安天人的认可，更是对于民营网络安全企业这个群体的认可，对工作在民营企业中的网络安全工作者的认可。

总书记将网络安全产业定性为“战略新兴产业”，并对安天、对网安产业人提出了要求“网络安全是国家安全的重要组成部分，维护国家网络安全需要整体设计、加强合作，在相互学习、相互切磋、联合攻关、互利共赢中走出一条好的路子来。”

安天参加万人徒步大赛

5 月 28 日，安天哈尔滨总部的小伙伴们参加了“第十五届新晚报万人徒步大赛”，这已是安天第 4 年参加该活动，徒步队伍中的一抹安天蓝再次为大赛增添了一道亮丽的风景。

安天参加 2016 年中国网络安全年会并发表演讲

5 月 24-26 日，“2016 中国网络安全年会”在成都召开，安天出席并发表了多篇演讲。

24 日，安天威胁情报首席专家潘博文，在 CNCERT 国际合作论坛，发表了题为《Mobile Threat Intelligence Cooperation between Security Vendor and CERT》的演讲，对移动威胁的演变、进化、威胁情报体系建设和应用进行了阐述。25 日，安天联合创始人、首席战略官方华发表了题为《熊猫的伤痕——中国遭遇的 APT 攻击》的演讲，介绍了 APT 的由来和趋势，选取了安天捕获、分析的几例典型攻击事件，分析了不同能力团队的技术特点。26 日，安天移动安全团队总经理潘宣辰，在移动互联网安全生态分论坛，发表了题为《移动威胁情报体系支撑生态实践分享》的演讲，介绍了基于有效检出带来的感知能力和基于工程化分析能力的支撑作用等内容。

在年会的现场展台，安天免费分发了最新的原创技术文章汇编等资料，受到了广大安全从业者及爱好者的欢迎。

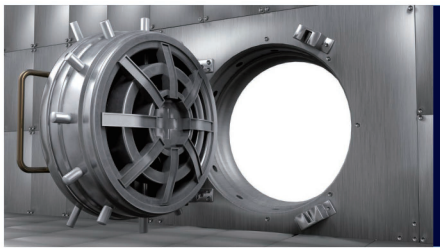
每周安全事件

类 型	内 容
中文标题	瑞士军工企业遭遇 TURLA APT 攻击
英文标题	Unraveling Turla APT Attack Against Swiss Defense Firm
作者及单位	Tom Spring；Threat post
内容概述	近日，瑞士计算机紧急预备小组发布了一份事故调查报告。在报告中披露了关于针对瑞士军工企业 RUAG 集团网络攻击的相关细节。此次攻击是一次典型的网络间谍式攻击，黑客采用了网络间谍软件 Turla，木马程序以及 Rootkit 恶意软件等相结合的一种复杂的攻击方式，是一次经过周密部署后发动的网络间谍活动。目标是攻击政府、军队、军工企业以及各国驻外大使馆的网络系统，窃取机密数据。
链接地址	https://threatpost.com/unraveling-turla-apt-attack-against-swiss-defense-firm/118254/

每周值得关注的恶意代码信息

经安天检测分析，本周 10 个移动平台和 4 个 PC 平台的恶意代码家族值得关注

平台分类	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.Appscomeon.a[exp，prv]2016-05-22	该应用程序作为一个插件运行会上传手机设备信息及位置信息，频繁联网，自我更新，另外可能会下载其他未知插件，造成一定的隐私泄露和资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.RecordCallSpy.a[prv，spy] 2016-05-23	该应用是一款间谍程序，需要设置接收邮箱地址，运行诱导激活设备管理器，隐藏桌面图标，执行开启环境录音，通话录音操作并上传录音文件，会造成用户隐私泄露，如非本人安装，建议及时卸载。（威胁等级高）
		Trojan/Android.CaesarSpy.a[rmt，prv，rog，exp] 2016-05-25	该应用伪装成 Service Google，程序运行后会请求激活设备管理器，隐藏图标，连接远程服务器互通数据，获取设备固件信息、SIM 卡相关信息、用户短信信息和通讯录信息上传到远程服务器，从服务器端获取指令执行拨打指定电话、发送指定短信，造成用户隐私泄露和资费消耗。（威胁等级高）
		Trojan/Android.WMegaApps.a[exp，rmt，sys] 2016-05-25	该程序是一款游戏应用，后台连接远程服务器获取指令数据，接收指令隐藏图标，获取网址下载更新并弹窗诱导安装，会造成一定资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.nfaSpy.a[prv] 2016-05-25	该应用伪装成 Device Policy，运行后会隐藏图标，后台联网上传用户短信和通讯录等隐私信息，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.TinySMS.a[pay，sys] 2016-05-26	该应用程序仿造游戏道具支付密钥，联网获取付费数据，执行短信付费操作，屏蔽回执短信，还会下载未知程序动态加载，存在一定安全风险，会造成用户经济损失，建议及时卸载该程序。（威胁等级高）
	较为活跃的样本	Trojan/Android.Mobilespy.u[prv，spy]	该应用程序是一款间谍软件，安装后需要设置上传邮箱地址信息，运行后会上传手机联系人信息和短信箱内容，会造成用户隐泄露和资费消耗，非本人安装请及时卸载该程序。（威胁等级高）
		G-Ware/Android.jianmo.ab[rog，exp]	该应用运行后会锁定用户界面，要求用户输入密码解锁，向指定号码发送大量短信，造成用户资费消耗。（威胁等级低）
		Trojan/Android.emial.de[prv，exp]	该应用运行后会请求激活设备管理器，隐藏图标，获取用户手机号和 IMEI 等信息发送到指定号码；获取短信信息、通讯录信息和 GPS 位置信息发送到指定邮箱；监听短信、拦截指定短信并获取短信号码和内容发送到指定邮箱，造成用户隐私泄露和资费消耗。（威胁等级高）
		Trojan/Android.tsttTrack.a[prv，rmt，spy]	该应用是一款间谍程序，需要配置邮箱信息，运行后上传用户配置信息，执行隐藏图标操作，还会通过短信远控代码，执行上传地理位信息，收件箱内容，更换远控号码等操作，会造成用户隐私泄露和资费消耗，建议及时卸载该程序。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 畸形 EPS 文件漏洞 (CVE-2015-2545)(MS15-099)	Microsoft Office 是一款微软发布的办公处理应用套件。Microsoft Office 处理 EPS 文件存在内存破坏，允许攻击者构建恶意文件，诱使应用解析，可使应用程序崩溃或执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Win32.Puflug	此威胁是一种具有下载行为的木马类程序，运行后连接网络下载其他恶意代码并安装，可能使用户信息被窃取，有一定威胁。（威胁等级中）
		Trojan[Clicker]/Win32.Wistler	此威胁是一种具有点击行为的木马类程序，运行后会修改系统设置及默认浏览器主页设置，弹出广告窗，使浏览器重定向至其他网页。同时，该家族会为黑客打开后门，允许黑客窃取用户信息。（威胁等级中）
		GrayWare[AdWare]/Win32.WebRebates	此威胁是一种可以下载并安装推广应用的灰色软件程序，运行后连接网络下载推广应用并安装，占用系统资源，影响用户使用。（威胁等级中）



SWIFT 网络安全堪忧

Michael Mimoso/ 文　安天公益翻译小组 / 译

继大规模诈骗之后，SWIFT 银行网络于近日更新了全球金融机构的安全资源，其官员还提醒各银行保护各自的基础设施。

前不久，孟加拉国、越南和厄瓜多尔银行遭到了攻击者的渗透，他们窃取 SWIFT 系统的凭证，继而窃取了数千万美元的资金。孟加拉银行 (孟加拉国央行) 遭受的攻击最严重，超过 8000 万美元被洗劫一空。据报道，该银行未启用防火墙，而是使用售价为 10 美元的交换机来管理连接到 SWIFT 网络的计算机。

SWIFT 代表环球银行金融电讯协会，是金融机构发送和接收交易的专用网络。

黑客们针对安全措施薄弱或未配备安全措施的银行，窃取 SWIFT 网络凭证，用以进行欺诈交易。继越南银行的攻击后，SWIFT 在 5 月 13 日的声明中暗示，银行内部人员可能参与了攻击活动。

SWIFT 在声明指出：“攻击者显然非常了解目标银行的运行措施，这些信息可能是由恶意内部人员提供的，可能是通过网络攻击获取的，也可能是这两者的结合。”

近日，SWIFT 再次发表声明，警告银行及其用户欺诈仍然是一个重要问题，并安抚他们，SWIFT 网络仍然是安全的。

SWIFT 的官员表示，他们将继续分享最新的攻击信息和帮助企业主动防御诈骗的最佳方法，特别是涉及凭证安全和网络访问的方法。

SWIFT 表示，他们汇集了新的和现有的信息，放置于 SWIFT 网站 (SWIFT.com) 限制性客户板块的名为 KB tip 5020928 的资源中。

SWIFT 在声明中说：“我们将持续更新该资源，包括任何新恶意软件或之前出现过的手法的其他感染信标 (IOC)。我们建议各个机构的 IT 安全团队每天查阅该资源。我们会将客户机构的所有新的、相关的网络事件信息添加到该KB资源中，让您的安全团队获得最新的信息，提高他们的反应和应对能力。”

SWIFT 在声明中多次强调，各个金融机构有责任保持各自网络的完整性。

SWIFT 指出：“各机构的作用是至关重要的。将这些措施作为你们安全协议的一部分，SWIFT 就能够更好地支持你们解决任何可能出现的问题，了解案件之间的模式，提供建议，并提醒其他用户，使其免遭类似攻击。”

孟加拉银行大劫案发生在今年 2 月，攻击者使用窃取的凭证来访问 SWIFT 网络，在银行网络中注入恶意软件，将资金转移到了菲律宾的账户中。SWIFT 指出，该恶意软件用来掩盖攻击者的踪迹。BAE Systems 公司的研究人员分析了名为 evtdiag 的组件，这是一个针对孟加拉银行的 SWIFT 联盟访问软件量身定制的恶意软件。SWIFT 称，该恶意软件只影响 SWIFT 网络的客户端，核心信息服务不受影响。

本月初，路透社报道称，孟加拉国警方指责 SWIFT 的技术人员引入了最终被利用的漏洞。

路透社援引了与孟加拉国警方刑事调查部门主管默罕默德・阿拉姆和孟加拉银行一位匿名官员的谈话。这名银行官员声称技术人员犯了错误，违反了安全协议，使得任何一个具有“简单密码”的人都能够打开 SWIFT 消息。

该银行官员对路透社记者说：“从 SWIFT 系统建立之初，SWIFT 就应负责检查漏洞。但是，他们玩忽职守。”

4 天后，SWIFT 发布了第二份警告，这次是针对越南先锋银行的攻击。SWIFT 称，攻击向量是银行用于检查对账单信息 (特别是支付确认) 的 PDF 阅读器。

攻击者使用木马化的 PDF 阅读器清除他们的踪迹。SWIFT 警告说，可能有内部人员搞鬼，因为他们了解涉事的PDF阅读器。

原文名称	SWIFT Network Doubles Down on Security
作者简介	Michael Mimoso，Threatpost 编辑。
原文信息	2016 年 5 月 23 日《Threatpost》发布，原文地址 https://threatpost.com/swift-network-doubles-down-on-security/118241/
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《勒索者与 DDOS 结合体样本分析》报告

近日，安天追影小组分析了一个勒索者与 DDOS 结合体样本，该样本与其他勒索软件相似，也是通过 word 文档中嵌入式宏执行 shell 命令，生成 vbe 脚本进而下载并运行恶意软件。该勒索者病毒不仅加密磁盘文件进行勒索，还会将受害者做为 DDOS 攻击载体来进行 DDOS 攻击，攻击目标的 IP 范围为 85.93.0.0-85.93.63.255，端口为 6892。

经过分析发现该勒索者家族为臭名昭著的“Cerber”勒索软件的变种，Cerber 出现于 2016 年 3 月，因其感染 windows 用户后将文件扩展名修改为“.cerber”而得名，其采用 AES-256 加密算法加密受害者文件。值得一提的是 Cerber 也是首款会“讲话”的勒索软件，其会通过电脑合成音制作提示消息，提示的内容为“警告！警告！警告！ 你的文档、照片、数据库以及其他重要文件已经被锁定”，由此看来恶意软件的制作者也是“煞费苦心”。

样本行为

1）样本加密行为：该病毒运行后，加密系统中的文件、图片、视频等文件并生成提示交赎金文件，页面显示有明显“CERBER”标识。

2）样本运行行为：该病毒运行后，有自删除、向其他进程写入数据、释放 PE 文件、设置自启动、修改文件创建时间等行为。

3）样本网络行为：样本运行后以毫秒级的时间间隔向 IP 范围为 85.93.0.0-85.93.63.255，端口为 6892 的目的地址发送 UDP 攻击包。

面对勒索软件呈现出的泛滥趋势，安天追影小组提醒广大用户加强个人信息安全防范意识，不随意打开陌生邮件及其附件，不随意点击陌生链接，不随意运行不明应用程序，通过官方网站下载正版软件，及时升级应用程序，重要文件要定期进行备份，以防万一。

木马程序

安天【追影高级持续威胁分析系统】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：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、YARA 自定义规则鉴定器、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 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。最终依据动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

文件名	D0F6CFB56F9B23EEDCE0F2AC30233FD1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	175 KB
MD5	D0F6CFB56F9B23EEDCE0F2AC30233FD1
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Dropper]/Win32.Zeqbeq
判定依据	智能学习

◆ 危险行为

行为描述	危险等级
删除自身	★★★★
其他进程写入可疑数据	★★★

该文件具有以下行为：删除自身、其他进程写入可疑数据、读取自身文件、获取驱动器类型、设置调试器权限、释放 PE 文件、增加 run 自启动项、获取系统版本、创建挂起的进程、设置自启动项、访问其他进程内存、获取计算机名称、篡改系统文件创建时间、复制自身文件、创建特定窗体、独占打开文件、打开自身进程文件、查找特定窗体、请求加载驱动的权限。

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
读取自身文件	★★	获取驱动器类型	★
释放 PE 文件	★	设置调试器权限	★
创建挂起的进程	★★	增加 run 自启动项	★
访问其他进程内存	★	获取系统版本	★★
篡改系统文件创建时间	★★	设置自启动项	★★
复制自身文件	★★	获取计算机名称	★
独占打开文件	★	创建特定窗体	★
查找特定窗体	★	打开自身进程文件	★
请求加载驱动的权限	★		

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=D0F6CFB56F9B23EEDCE0F2AC30233FD1