安天发布《Astaroth 窃密木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Astaroth 的窃密木马。该窃密木马最早在 2017 年底被发现，主要通过钓鱼邮件进行传播，目标是窃取欧洲和巴西用户的个人信息和其主机的系统信息。

当用户点击邮件附件中 .lnk 快捷方式文件时，该恶意代码将运行 WMIC(Windows 管理命令行工具) 程序下载一个包含混淆 JavaScript 脚本的 XSL 文件。该 JavaScript 脚本通过执行 Bitsadmin(命令行工具) 程序下载四个 Base64 编码的 DLL 文件，使用 Certutil 工具 (证书服务安装命令程序) 对这些文件进行解码操作，使用 Regsvr32 加载前三个 DLL 文件，并将第四个 DLL 文件 (Astaroth 窃密木马主程序) 注入到 Userinit 进程中。

Astaroth 窃密木马主要功能包括键盘记录、剪贴板记录、监控密钥状态、监控 IE 浏览器以及窃取计算机的初始信息（包括相关网络、区域设置和键盘语言以及感染机器的位置）。Astaroth 窃密木马专门针对 IE 浏览器。当用户使用 IE 浏览器访问银行或企业网站时，开启键盘记录功能，窃取用户登录凭证、账号密码等信息。

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该窃密木马的鉴定；安天智甲已经实现了对该窃密木马的查杀。

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、字符串分析鉴定器、反病毒引擎鉴定器、动态 (WinXP) 鉴定器、聚类分析鉴定器、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	e44548f0c7d26a6d11f3ab29753e36f525559dc2e443bff96346f1be17cd644a
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	1.43 MB
MD5	A882D96751F0D49B04751BE7EE319B5D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Occamy
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=A882D96751F0D49B04751BE7EE319B5D

◆ 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

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
壳行为填充导入表	★★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
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
192.168.122.1	67	192.168.122.111	68

◆进程监控

PID	创建	命令行
1376	rundll32.exe	"C:\WINDOWS\system32\rundll32.exe" c:\5d0bfbc7b85646e4a1cad1aa7a13acec\share\target.dll,TMethodImplementationIntercept
1880	rundll32.exe	"C:\WINDOWS\system32\rundll32.exe" c:\5d0bfbc7b85646e4a1cad1aa7a13acec\share\target.dll,DllMain

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 09 月 16 日 (总第 200 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天将亮相 2019 年国家网络安全宣传周 解读实战化威胁猎杀

2019 年国家网络安全宣传周于 9 月 16 日至 22 日在全国范围内统一开展，主题是“网络安全为人民，网络安全靠人民”，由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、国家广播电视总局、全国总工会、共青团中央、全国妇联等部门联合举办。据悉，今年网安周将深入贯彻落实习近平总书记关于网络强国的重要思想，围绕中华人民共和国成立 70 周年特别是党的十八大以来网络安全领域取得的重大成就，贯彻落实《网络安全法》以及数据安全管理、个人信息保护等方面的法律、法规、标准，通过多种形式，多个传播渠道，发动企业、媒体、社会组织、群众广泛参与，深入开展宣传教育活动。

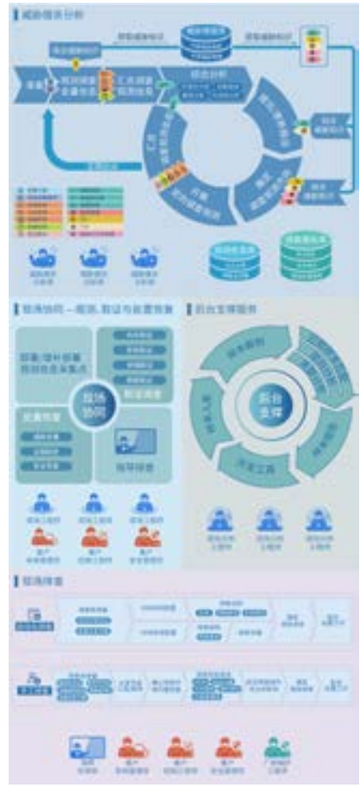
今年网络安全宣传周的开幕式、网络安全博览会、网络安全技术高峰论坛等重要活动将在天津市举行，邀请了来自政府、科研机构、高校、社会组织、企业、媒体的近千位嘉宾出席。

安天作为网络安全国家队，积极参与了各地网安周相关活动，将同时在天津、黑龙江、辽宁、河北、内蒙古、 广东 、山东等多地亮相，带来安天战术型态势感知平台以及安天实战化威胁猎杀服务的详细介绍，届时，欢迎各位莅临安天展位参观交流。

实战化威胁猎杀，让威胁无处遁形

近年来，关键信息基础设施频繁出现重大安全事件，这些浮出水面的事件说明全球大量关键信息基础设施已被高级网空威胁行为体长期潜伏。面对严峻的大国博弈和复杂的地缘安全形势，我国信息基础设施需以“敌已在内”作为整个防御工作的基本敌情设定，亟待全面建设动态综合防御体系，并展开“威胁猎杀”行动，从而做到将潜伏威胁“找出来”和“赶出去”。

威胁猎杀是深入的、以“人”为主导的调查过程，是积极防御层面一种主动和迭代的威胁检测方法，旨在发现关键信息资产中潜伏的威胁。威胁猎杀团队、威胁猎杀工具、数据与知识是支撑威胁猎杀的关键要素，三个要素之间相互协同配合。其中，高水平的威胁猎杀团队是威胁猎杀工作的灵魂。威胁猎杀团队需要自动化威胁猎杀工具的支撑，而猎杀工具的有效性取决于猎杀团队的水平；威胁猎杀工具以数据为采集和处理对象，实现知识与情报驱动的自动化关联分析；猎杀团队分析数据产生知识，数据与知识又能够为猎杀团队提供威胁线索。



威胁猎杀是一种协同配合的工作方法，基于工作性质、工作重点部位与参与人员组织，安天将威胁猎杀划分为威胁猎杀分析、现场协同与后台支撑服务、现场排查三个层面。这三个层面相应人员在负责各自工作的同时，也会根据其他层次的输入信息进行工作，并生成相应的输出信息给予不同的层面，实现三个层次相互之间的协同联动进而展开威胁猎杀工作。

威胁猎杀是针对重要信息资产场景的一种高投入服务。做好基础结构安全和纵深防御层面的工作，全面增强网络的可管理性，并进一步改善可防御性将为威胁猎杀工作形成良好的基础支撑条件，全面降低威胁猎杀的成本。通过战术型态势感知平台指挥控制威胁猎杀的积极防御层面的安全工作，可以进一步形成一个高效的围绕网空防御人员的闭环体系。依托态势感知与积极防御体系支撑威胁猎杀工作，并通过常态化威胁猎杀驱动网空安全防御体系持续完善和优化。

每周安全事件

类 型	内 容
中文标题	研究人员发现 Red Lion 人机界面编程软件存在漏洞
英文标题	Several Vulnerabilities Found in Red Lion HMI Software
作者及单位	Eduard Kovacs
内容概述	趋势科技研究人员在美国 Red Lion 公司制造的人机界面 (HMI) 编程软件中发现了一些漏洞，包括已被列为高危的漏洞。Red Lion 的 Crimson 编程软件，特别是版本 3.0 及之前版本和 3112.00 版本之前的 3.1 版本，受到四个漏洞的影响，漏洞编号为 CVE-2019-10996，CVE-2019-10978，CVE-2019-10984 和 CVE-2019-10990。其中最严重的一个漏洞允许攻击者通过说服目标用户打开特制的 CD3 文件，在当前进程的上下文中远程执行任意代码。
链接地址	https://www.securityweek.com/several-vulnerabilities-found-red-lion-hmi-software

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.SpyMavrodi.b[prv,sys,spy] 2019-09-08	高	该应用程序伪装为其他应用，后台获取短信、联系人、键盘记录、用户位置、用户手机固件信息等上传，造成用户隐私泄露；利用脏牛漏洞（CVE-2016-5195）本地提权，获取对系统目录的操作权限，给用户手机带来安全隐患，建议卸载。
		Trojan/Android.Joker2.a[prv,pay,exp] 2019-09-09	中	该应用程序包含恶意代码，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息。造成用户隐私泄露和经济损失，建议卸载。
		G-Ware/Android.CanvasAd.a[exp,rog] 2019-09-10	中	该应用程序包含恶意代码，隐藏广告视图，并通过模拟点击恶意刷量，造成用户资费损耗，建议卸载。
	较为活跃样本	Trojan/Android.snamappspy.a[prv]	中	该应用程序运行激活设备管理器，窃取用户短信，通讯录，通话记录，照片，视频等隐私信息并通过邮箱上传，造成用户隐私泄露，建议卸载。
		Trojan/Android.MWSpy.a[prv,spy]	中	该应用程序伪装为 word，实际为间谍件，运行隐藏图标，后台上传用户联系人、短信、通话记录、程序安装列表、邮箱账户、社交聊天信息等隐私，还会监听电话，执行通话录音，上传录音文件，会造成用户隐私泄露，请卸载。
		Trojan/Android.kendalspy.a[prv,spy]	中	该应用程序伪装系统应用，运行隐藏图标，后台获取用户短信，通讯录，通话记录，照片，定位等隐私信息到远程服务器，造成用户隐私泄露，请立即卸载。
		Trojan/Android.7techspy.a[prv,spy]	中	该应用程序为间谍工具，伪装为正常应用，可以通过设置隐藏图标，后台收集用户短信、定位、照片、通话记录等隐私信息到远程服务器，造成用户隐私泄露，建议卸载。
		RiskWare/Android.wodemoTool.a[exp,rog]	低	该应用程序一般为灰色工具类应用，运行后加载指定网址，可能存在一定风险，请用户谨慎使用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft 图形组件远程代码执行漏洞（CVE-2019-1144）	高	当 Windows 字体库不正确地处理经特殊设计的嵌入字体时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。攻击者可随后安装程序、查看、更改或删除数据，或者创建拥有完全用户权限的新帐户。
	较为活跃样本	Trojan/MSIL.Fakromup	中	此威胁是一个使用 C# 写成的木马类家族。该家族的样本在执行后，攻击者即获得该设备上的信息并有能力进行进一步的控制。
		Trojan[Exploit]/SWF.Downloader	中	此威胁是一种以 SWF 为载体的木马家族。该家族的样本利用了 SWF 的漏洞，在播放 SWF 文件的时候产生溢出并下载恶意软件从而使执行者的机器完全处于对方控制之下。
		RiskWare[RiskTool]/Win32.PsKill	低	此威胁是一个风险软件家族。该家族的样本执行后，可以终结用户指定的进程，对系统的稳定性造成潜在影响。
		RiskWare[WebToolbar]/Win32.MusIn	低	此威胁是一种可以安装浏览器扩展的风险软件家族。该家族的样本在执行后会在浏览器中添加工具栏，并在特定的页面推送广告。
		RiskWare[RiskTool]/Win32.SystemTweaker	低	此威胁是一个可以修改系统设置的风险软件家族。该家族的样本在执行后可以由用户定义设置，对系统的稳定性造成影响。

供应链安全：选择供应商的五种 IT 策略

Randy Barr/ 文 安天技术公益翻译组 / 译

随着 SaaS 解决方案、API 集成和云计算的激增，现代企业中的几乎所有内容都与大量外部实体互联。事实上，虽然这种互联会扩大企业的威胁范围，使企业面临更大的风险，但是许多业务流程都依赖于这种互联。

这种互联性意味着，供应商的漏洞也会成为企业的漏洞。2017 年夏季的大规模 NotPetya 攻击就是一个很好的例子，该攻击造成数百家公司的网络瘫痪。从针对乌克兰的准网络战攻击开始，几乎全球所有公司和机构（从丹麦航运巨头马士基 [Maersk] 到宾夕法尼亚州的一家医院）的网络都遭遇了攻击，造成了 100 亿美元的损失——而这些基本上都是附带损害。勒索软件像野火一样蔓延，甚至那些与原始目标完全无关的企业也会遭到攻击，这让企业意识到了供应商安全问题。

但是，从那时起，在实施更好的供应链网络安全风险管理方面，似乎没有出现什么变化。Gartner 最近的一项研究发现，83％的企业在进行尽职调查后发现了第三方风险；而超过 70％的企业和 IT 高管承认，他们不了解第三方合作伙伴在安全方面的尽职程度。令人不安的是，超过一半的企业表示，他们与合作伙伴的关系基于相互信任。

在这种风险下，仍有大量的企业未能将供应链安全放在首位，这令人非常不安。大多数情况下，企业的问题在于：企业完成供应商的选择后，才会让 IT 团队启动供应商评估流程。业务部门有权进行初步评估和尽职调查，并且只有在合同已准备好并等待签署的情况下，才会让 IT / 安全团队进行供应商审查。这意味着，如果 IT 团队叫停交易，他们就变成了“坏人”。

为了解决这个问题，IT 团队必须采取更具战略性的方法来确保供应链安全，即让业务部门尽早评估供应商的安全性。企业可以采取以下五种策略，以便业务部门在尽职调查期间更彻底地审查供应商，使 IT 团队不必在实现交易的最后一刻才介入审查。

培训企业员工，使其了解网络安全风险。

IT 部门的员工时刻关注网络安全问题。但是，其他部门的员工可不会这样。这些员工对网络安全风险的意识不高——如果知道企业所面临的威胁形势有多严峻，他们会很惊讶。因此，对员工开展网络安全培训至关重要。企业应将网络安全培训作为常规要求，以便那些做出供应商决策的人员（甚至只是日常用户）了解哪些方面存在风险以及如何减轻风险。通过提高员工的风险意识，企业可以建立一个更加警惕的防御前线。

制定供应商基准安全策略。

企业应创建一组供应商必须满足的特定指南、策略和控制要求，只有满足这些要求的供应商才能通过审核。这应该包括供应商内部员工的安全培训、双因子身份验证、安全开发策略、生命周期管理、渗透测试、资产管理、移动设备安全、变更和访问控制，甚至物理 / 环境要求等。企业以书面形式向供应商提出要求，并将其作为不可协商的条件，以便业务部门进行更彻底的供应商尽职调查，有助于 IT 团队随后的安全审查。

要求合规性验证。

企业应确保，业务部门了解遵守企业或行业规定的重要性。在如今的环境中，企业不仅要对自己的合规性负责，还要对供应商的合规性负责。这意味着，如果发生供应商泄漏事件，企业在某些情况下需承担同等责任。企业应遵守 GDPR、PCI、HIPAA 等法规。此外，企业应注意，不同的市场有不同的要求。因此，企业的业务部门应要求供应商出示证明，以便验证其符合业务所在地区或国家的法规。

要求查看供应商的数据流。

基本上，大多数公司都依靠云资源进行存储或计算——几乎没有企业运行自己的内部数据中心。这意味着，企业的数据可能会暴露给许多供应商、承包商以及与他们开展业务的其他第三方，如通过 API 连接到供应商的系统，或在供应商的网络外部传输。企业有权利和责任了解供应商的数据流，以及可能访问企业数据的人员。业务部门应要求查看供应商的数据流图，如果供应商声称这是其“专有的”，那么企业就要警惕了。

采用连续、迭代的方法来确保供应商安全。

很多企业依赖于即时验证，如验证协议或进行认证。但是，如今的业务环境和威胁情境变化太快，年度审计已经无法满足要求。Gartner 提出了一种迭代方法，在第三方风险产生影响之前予以识别和修复，以快速降低风险。企业应将供应商合规性审查作为一个迭代过程，以增强其降低风险的能力，从而节省大量的时间、资金和精力。

在合同谈判之前或在合同谈判期间，企业应为业务部门提供供应商安全检查手册，使业务部门具备进行更彻底的尽职调查的知识和能力。此外，企业还应在 IT 审查之前尽可能全面地进行供应商的安全和合规性检查。这样，IT 部门就不必在最后一刻叫停交易了。这样不仅可以保护企业，还可以消除 IT 与其他业务部门之间的对抗关系，使其增强协作。

原文名称	Supply chain security: Five IT strategies for choosing vendors wisely
作者简介	Randy Barr。Randy Barr 是 Topia 公司的首席信息安全官。
原文信息	2019 年 9 月 5 日发布于 Help Net Security。 原文地址 https://www.helpnetsecurity.com/2019/09/05/supply-chain-security-strategies/
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。