安天发布《基于驱动的 MITM 恶意软件分析报告》

近期，安天捕风团队捕获到了一个名为“itranslator_02.exe”的恶意样本，该恶意样本文件带有一个无效的证书签名。一旦受害者打开 exe 文件，恶意软件就会安装两个驱动，控制受害者的 Windows 系统，同时监控受害者使用浏览器的互联网活动轨迹，窃取用户账户密码信息。

当 itranslator_02.exe 运行时，会在 program-data 目录中新建目录并释放名为 wintrans.exe 的新文件，并使用参数 P002 启动 wintrans.exe。此处恶意样本将 P002 作为受害者计算机的 GUID 来使用，并在恶意攻击活动中利用该值与 C&C 服务器通信。

Wintrans.exe 启动成功后，会尝试下载一个 DLL 模块（iTranslator.dll），并将其保存到同目录下；然后在受害者系统上创建一个线程，用以创建名为 iTranslatorSvc 的驱动服务，该驱动启动类型被修改为 SYSTEM_START，这样每当系统启动时都会启用该驱动。接下来，wintrans.exe 会将名为 iTranslator（Windows 驱动文件）的一个文件释放到 Windows 目录中，最后 wintrans.exe 会将受害者的系统等信息发送到攻击者的服务器。

下载的 iTranslator.dll 可以在首次安装时由 wintrans.exe 加载运行，也可以在 Windows 系统启动时由 winlogon.exe 负责加载及运行，而后者由 iTranslatorSvc 驱动负责加载。经过分析发现，iTranslator.dll 并不仅仅是一个 DLL 文件，而是一个文件容器，其资源区中包含许多其他文件，这些文件随后会释放到受害者的本地目录中。

经进一步分析，安天捕风团队发现 iTranslator.dll 释放出来的 13 个文件都用于在受害者系统上执行 MITM 攻击（中间人攻击），其中 12 个用于控制 Firefox 浏览器，其中 1 个是 iNetfilterSvc 模块，这是一个驱动程序（NetfilterSvc），用来透明过滤 Windows 系统中通过网络传输的数据包，以及安装 Sample CA 2.cer，然后 iTranslator.dll 会与 iTranslatorSvc 及 NetfilterSvc 驱动进行通信，交换数据。Sample CA 2.cer 是一个根证书，会以可信根证书颁发机构形式安装到 Firefox 以及 Windows 系统中（针对 IE 和 Chrome）。通过这种方法，使浏览器不会向用户发出任何的不安全警告，而恶意软件可以监控受害者在所有主流浏览器上的活动。

如果想删除该恶意软件，可以重启主机并进入安全模式，然后执行如下操作：

1、删除 %WINDIR%\iTranslator 和 %WINDIR%\system32\iTranslator.dll 文件；

2、删除 %WINDIR%\nss 和 %WINDIR%\SSL 以及 %ProgramData%\itranslator 目录；

3、删除 HKLM\SYSTEM\CurrentControlSet\services\iTranslatorSvc 注册表键值；

4、删除 HKLM\SYSTEM\CurrentControlSet\services\NetfilterSvc 注册表键值；

5、删除所有浏览器中的 Sample CA 2 证书。

安天建议广大用户及时更新设备系统，修补相关漏洞，修改设备登陆的默认密码，避免弱口令的使用，并安装杀毒、防毒软件。

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：

文件被页面手工提交发现，经由文件来源信息鉴定器、YARA 自定义鉴定器、文件元数据鉴定器、BD 静态分析鉴定器、数字证书鉴定器、动态 (WinXP) 鉴定器、动态 (Win7 x86) 鉴定器、反病毒引擎鉴定器、聚类分析鉴定器、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、反病毒引擎鉴定器将文件判定为木马程序。

文件名	B73D436D7741F50D29764367CBECC4EE67412230FF0D66B7D1D0E4D26983824D
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.89 MB
MD5	E7A621363966950DED0489F6C613FE45
病毒类型	木马程序
威胁名称	Trojan/Win32.AGeneric
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=E7A621363966950DED0489F6C613FE45

行为描述	危险等级	行为描述	危险等级
访问下载站点	★★★	检测虚拟机	★★★★★

◆ 常见行为

行为描述	危险等级
壳行为填充导入表	★★
释放 PE 文件	★
获取驱动器类型	★
创建服务	★
启动指定服务	★
获取系统信息（处理器版本、处理器类型等）	★
疑似桌面控制	★

◆ 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

◆ 进程监控

PID	创建	命令行
1792	target.exe	"C:\8aba84e9da3d4f9db8fd14ff19bf266e\share\target.exe"
1908	wintrans.exe	"C:\ProgramData\itranslator\wintrans.exe" P002

◆ 危险行为

安天周观察
安天官方微博 安天官方微信
主办：安天 2018 年 11 月 12 日 (总第 159 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天负责人参加黑龙江省民营企业家座谈会并发言

为深入贯彻落实习近平总书记在全国民营企业家座谈会上的重要讲话精神，激发民营企业创新创业热情，广泛听取民营企业家促进民营经济振兴发展的意见建议，黑龙江省委在近日组织并召开了全省民营企业家座谈会，省委书记张庆伟同志主持会议并发表讲话，省委省政府主要领导同志出席会议。

安天负责人肖新光第二个发言，就如何落实好习近平总书记重要讲话精神，推动民营企业更好的发展提出了建议：根据高科技民营企业的领域特点，协助企业对接国家战略资源，创造出新的市场机遇；以协助高科技民营企业留用当地高校优秀毕业生作为人才战略的政策发力点；对高科技民营企业员工持股激励给予相应的财税支持。

肖新光表示，通过认真学习领会总书记的重要讲话，更加坚定了企业发展的信心和恒心，增强了企业的紧迫感和责任感。安天将进一步践行网络安全国家队的责任和使命，发扬民营企业的创新与活力，把握产业发展机遇，尽快成长为保障网络强国的产业支点。

Evernote 修补了其应用程序的存储 XSS 漏洞

Evernote 修补了应用程序中的漏洞 CVE-2018-18524，该漏洞影响了 Windows 6.14 的 Evernote。当重命名和打开图像文件时，Evernote 允许使用诸如“onclick =” alert(1) “之类的字符和短语，由于缺少验证，攻击者可以创建存储的 XSS（跨站点脚本）。XSS 攻击可能导致帐户泄露、浏览器劫持以及通过漏洞利用工具包执行恶意软件负载。Evernote 在应用程序的最新更新 Evernote For Windows 6.16.1 测试版中修复了这个漏洞。

（原文链接：https://www.zdnet.com/article/evernote-for-windows-patch-resolves-stored-xss-vulnerability/）

2018 保密技术大会 安天分享保密场景下的态势感知体系

近日，以“坚持创新驱动，携手打造保密产业良好生态”为主题的 2018 年保密技术交流大会暨产品博览会在青岛举行，本届大会共吸引了 600 余家单位参展。作为信息安全领域的重要企业之一，安天亦参与其中，同时，安天研发副总裁王小丰也在专题论坛上带来了题为《保密场景下的态势感知体系》的分享。

本届大会由中国保密协会主办，旨在推动企业与用户、企业与企业、国内与国际进行保密技术交流合作，增强机关、单位干部职工保密意识，普及公众信息安全保密防范常识。安天展台展出了安天智甲终端防御系统及网络安全态势感知与应急处置平台的省级应用案例，吸引了众多参观者驻足浏览。

在 10 月 31 日下午的“科技驱动保密产业发展”专题论坛上，安天研发副总裁王小丰分享了《保密场景下的态势感知体系》。他指出，态势感知能力的规划和建设，需要以“全面支撑动态综合的网络安全积极防御体系”为目标，建设“感知威胁”、“理解分析威胁”、“预测下一步攻击”、“联动响应处置”、“协同情报、累积知识”五类关键能力。

同时，他介绍了安天在态势感知上的主要研发方向，包括“全面监测和按需采集结合，达成全要素的数据采集和威胁感知能力”，“基于知识和深度分析，达成有效的威胁理解能力”，“通过漏洞、攻击者等多线索分析，达成合理的攻击预测能力”，“联动设备、工具、人员及环境，达成快速的响应联动能力”，“利用情报和生产情报结合，达成情报协同能力”等方面的解决方案和实际应用效果。

近年来，安天为多个国家和地方主管部门、行管部门研发实施了监测型态势感知解决方案，效果获得了用户好评。这些工作也同时推动了安天对“高信息价值、高防护等级、高威胁对抗”场景下的网络安全建设规律和解决方案的思考，重新认识了重要信息系统和关键信息基础设施对态势感知和积极防御的安全需求。在监测型态势感知的经验积累下，安天持续加强对实战型态势感知的研发投入，努力与关键基础设施管理者、行业客户携手共建实战化的态势感知体系，依托全面持续监测能力，逐渐形成分析预测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，推动客户整体安全能力建设的叠加演进。

每周安全事件

类 型	内 容
中文标题	SPI 恶意软件针对 macOS 用户进行中间人攻击
英文标题	Inside Searchpageinstaller | Macos Malware Deploys A Mitm Attack
作者及单位	Philip Stokes
内容概述	SearchPageInstaller（SPI）是自 2017 年以来一直存在的广告软件，研究人员最近发现该恶意软件针对 macOS 用户。SPI 不是简单地将浏览器重定向到非目标页面，而是将广告注入到用户搜索返回的 html 文档的顶部。因此，攻击者需要在受感染的计算机上启用 HTTP 和 HTTPS 代理，在脚本中添加要实现的内容，并替代搜索页面结果顶部的广告。 SPI 使用 mitmproxy(一种开源 HTTPS 代理)将脚本注入到网页主体中，mitmproxy 本质上充当服务器和客户端之间的“中间人”，“动态”创建虚拟证书让服务器认为它是客户端，客户端认为它是服务器。借助 SPI 二进制文件，用户提交密码后，就会手动安装 mitmproxy CA 证书。尽管 SPI 是一个风险相对较低的广告软件活动，但它能够操纵普通的 http 和加密的流量，值得注意。
链接地址	https://www.sentinelone.com/blog/inside-searchpageinstaller-macos-malware-deploys-mitm-attack/

每周值得关注的恶意代码信息

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.SmsPayment.n[exp,pay] 2018-11-05	该应用程序包含恶意代码，运行后会拦截用户短信，私自发送付费短信，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.AppSpy.a[prv,spy] 2018-11-06	该应用程序为手机监控软件，运行可以选择激活设备管理器，隐藏图标，伪装为系统应用，后台窃取用户位置、短信内容、通话记录并上传到服务器，造成用户隐私泄露。若非自主安装，建议卸载。（威胁等级中）
		Trojan/Android.Fakegoogleplay.g[exp] 2018-11-07	该应用程序伪装 Google Play 更新应用，无实际功能，运行隐藏图标，后台推送广告，造成用户流量资费损耗，请卸载。（威胁等级低）
	较为活跃样本	G-Ware/Android.FakeCJFZ.a[fra,pay]	该应用程序伪装吃鸡外挂，本身无实际功能，诱导用户扫码转账，可能造成用户资费损失，建议不要使用。（威胁等级低）
		G-Ware/Android.AIDEshare.a[spr,fra]	该应用程序伪装 QQ 相关工具，运行诱导用户加 QQ 群，分享传播盗号、骗钱类恶意应用。同时存在泄露个人账号信息的风险，建议不要使用。（威胁等级中）
		G-Ware/Android.SexPay.d[exp,rog]	该应用程序包含色情内容，推送诱惑性内容诱导用户充值付费，后台私自发送订阅短信，为避免用户财产损失，请使用健康绿色软件。（威胁等级中）
		Tool/Android.vnc.a[prv,rmt]	该应用程序包含 VNC 远控工具，运行可操作手机执行相应命令，请谨慎使用，若非自主安装，建议卸载。（威胁等级中）
		RiskWare/Android.DZbocai.a[rog]	该应用程序为博彩应用，可能给用户的财产带来较大风险，且难以保障财产权益，请谨慎使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Word 任意代码执行漏洞（CVE-2018-8504）	Microsoft Word 中存在远程代码执行漏洞，该漏洞源于软件未能妥当地处理 ProtectedView 中的对象。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.SwiftBrowse	此威胁是一种有广告行为的灰色软件类程序。该家族与 Swift Browser 浏览器扩展有关，它通常与正常软件捆绑到一起进行传播，它会在电脑上收集用户信息，并根据这些信息获取用户习惯并推送广告。（威胁等级低）
		Trojan[Rootkit]/Boot.Cidox	此威胁是一种可以修改 MBR 并在系统内核之前加载的木马家族。该家族通常以正常的应用程序伪装，会监控网络流量和击键组合，在电脑中留下隐蔽的后门，并试图攻击局域网内的其他机器。（威胁等级中）
		Trojan[Backdoor]/PHP.C99Shell	此威胁是一种使用 PHP 语言编写的带有后门的木马类程序。该家族样本一般使用 PHP 语言编写，通常利用 webshell 从而达到控制网站服务器的目的。（威胁等级中）
		GrayWare[AdWare]/OSX.Vsrch	此威胁是一种具有窃取用户信息并回传行为的灰色软件类程序。该家族的样本仅在 OSX 平台上运行。该家族的样本会在后台收集敏感信息并上传，并且会占用大量系统资源。(威胁等级中)
		GrayWare[AdWare]/NSIS.OutBrowse	此威胁是一种使用 Nullsoft 安装程序打包器的具有广告行为的灰色软件类程序。该家族的样本在安装时不提供拒绝或退出的选项，在强制安装软件后还会额外弹出广告信息。(威胁等级低)

ICS 设备易受“边信道”攻击

Eduard Kovacs/ 文 安天技术公益翻译组 / 译

上个月，《安全周刊》（SecurityWeek）在佐治亚州亚特兰大市举行了工业控制系统（ICS）网络安全会议，与会研究人员警告称，“边信道”攻击可能会对 ICS 构成严重威胁。

动力管理公司伊顿（Eaton）首席工程师迪莫斯·安德烈乌（Demos Andreou）对能源领域（特别是配电站）常用的保护设备进行了分析。

通过观察 ICS 的物理实现并获取相关信息，攻击者可以执行“边信道”攻击，从系统中提取数据。目前有好几种边信道攻击方法，但安德烈乌的研究着眼于“时耗分析”和“功耗分析”攻击。“时耗分析”是指分析执行各种计算所花费的时间，“功耗分析”是指分析执行加密操作时功耗的变化。

安德烈乌表示，攻击者可以针对 ICS 设备发起时耗和功耗分析攻击。不过，前者更容易检测和阻止，因此他将研究重点放在后者上。

虽然边信道攻击已经出现了很长时间，但很少有研究论文描述它们对工业系统的影响。值得注意的是，臭名昭著的“熔毁”（Meltdown）和“幽灵”（Spectre）边信道攻击也影响到了 ICS，但它们只涉及软件，依赖于“推测执行”（speculative execution）。（译者注：推测执行是当今主流处理器 [包括 AMD、ARM 和 Intel] 中广泛采用的一项优化技术。其基本思路是利用处理器的空闲时间提前执行一些将来“可能用得上，但也可能被放弃”的计算 [包括分支预测、预读内存和文件数据]，从而极大提升系统的整体运行速度。）

安德烈乌在接受《安全周刊》采访时表示，他希望提高大家对边信道攻击风险的认识，让他们知道这种攻击不仅在理论上可行，而且已被攻击者付诸实践——即使利用有限的资源也可以执行。

在伊顿公司，安德烈乌和同事对工业控制系统及网络开展了合规性和道德渗透测试研究。他们旨在确保公司产品的安全性，保护客户网络不受网络威胁。

功耗分析攻击依赖于时钟周期（即示波器显示的两个脉冲之间的时间量）内半导体的功耗变化。示波器的信号形成功率配置文件，能够提供有关数据处理方式的信息。通过观察和测量在输入正确和错误口令字符时的功耗，并比较它们之间的差别，研究人员就可以获取口令的一个字符。同理，也可以获取整个加密密钥。

安德烈乌表示，他对三家主要供应商的保护设备进行了成功的实验。但他认为，如果其他公司使用的微处理器也容易受到此类攻击，那么他们的产品也会受到影响。虽然被测试的设备已有 5 到 10 年的历史，但他表示，更新的产品可能也有相同的漏洞，这是因为这类攻击直到最近才被付诸实践，供应商不太可能来得及采取措施来降低风险。开源软件和廉价硬件的可用性使得边信道攻击更容易执行。

安德烈乌指出，能够对保护设备进行物理访问的攻击者，可以使用示波器和运行开源软件的专用硬件设备来获取加密密钥。他表示，此类攻击所需的硬件成本约为 300 美元。

对于他分析的保护设备，攻击者可以提取加密密钥并使用密钥来执行配置更改。安德烈乌说，这些设备用于保护电网，更改其配置会造成严重的后果。恶意行为者更改设备的配置后，设备可能会出现故障或者向操作员返回错误数据。这些设备是分布式的，由主系统控制，来自一个设备的错误读数可能会对网络中的其他设备产生影响。此外，安德烈乌解释说，攻击者可以进行当下并不明显的配置更改。例如，一些保护设备在不同的季节具有不同的设置，黑客可以确保他们所做的更改只在换季时生效，这样就能够掩盖攻击了。

安德烈乌指出，功耗分析攻击可能会造成严重的威胁，因为它们几乎无法检测到——即使受到攻击，设备看上去也像是在执行正常操作。在现实场景中执行此类攻击并非易事，但并非不可能。安德烈乌指出，这些设备通常是无人监管的，因此对它们进行物理访问并不困难。恶意内部人员、顾问和维修人员都有很多机会发动攻击。另一方面，只有在设备执行涉及加密密钥的操作时，攻击者才能够执行攻击——即，必须在测量到功耗变化时执行攻击。这需要对设备进行逆向工程，并提前了解目标产品的类型。

执行攻击可能需要花费数小时，其中大部分时间涉及物理准备（例如，打开目标设备、连接传感器）。软件部分的准备要快得多，可以在几分钟内获得密钥。例如，如果使用高级加密标准（AES），攻击者可以一次提取密钥的一个字节。如果使用 AES-128，他们则需要对加密密钥 16 个字符中的每个字符进行 00 到 255 的组合，并监控每个组合的功率配置文件。

安德烈乌在演讲中介绍了此类攻击的其他技术细节。

原文名称	ICS Devices Vulnerable to Side-Channel Attacks: Researcher
作者简介	Eduard Kovacs。Eduard Kovacs 是 SecurityWeek 的特约编辑。
原文信息	2018 年 11 月 05 日发布于 SecurityWeek 原文地址 https://www.securityweek.com/ics-devices-vulnerable-side-channel-attacks-researcher
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。