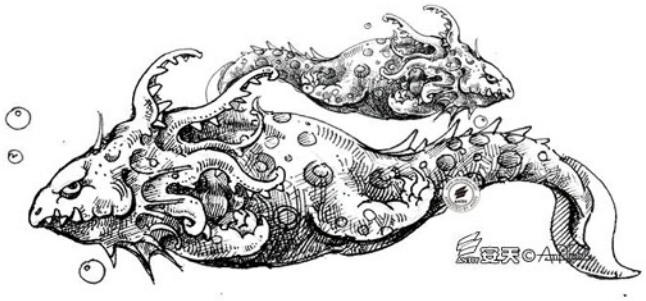
安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 09 月 17 日 (总第 152 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布针对工控恶意代码 TRISIS 的技术分析



2017 年 8 月，安天安全研究与应急处理中心（安天 CERT）基于综合情报研判，将针对工业控制系统的恶意代码 TRISIS（又名 TRITON、HATMAN）列为需要重点分析关注的威胁，并将其命名为“海渊”。该恶意代码在中东某石油天然气厂的工业控制系统中被国外安全研究人员发现，根据各方信息判断，由于攻击者准备不充分，尚未对人员及财产造成重大损失。

“海渊”（TRISIS）所攻击的目标是工业控制系统（ICS）中的安全仪表系统（SIS）控制器，其主要瞄准施耐德电气的 Tricon 安全仪表系统，通过植入固件更改最终控制元件的逻辑以达到攻击目的。其通过 Tricon 安全仪表系统所使用的 TriStation 通信协议进行攻击，因此运行此协议的所有安全控制器都可能受到影响。

安天 CERT 针对该恶意代码的攻击原理及样本展开了技术分析。发现该恶意代码的攻击流程为利用社工技巧伪装成安全仪表系统的日志软件进入目标网络，之后通过特殊 ping 包发现安全仪表系统，在确定安全仪表系统可被入侵后，会上传组合后的二进制代码，以改变安全仪表系统的梯形图（即安全仪表系统逻辑），一旦攻击成功，将有可能对工业生产设备、工厂人身安全造成巨大危害，对关键信息基础设施安全、社会安全造成巨大影响。

“海渊”（TRISIS）恶意代码呈现出了一些值得关注的特点，其开发者深入了解相关工控产品的控制协议，除了上载到 PLC 中的二进制模块外，其他框架和功能代码全部采用脚本编写，非常容易被改造和加工。而其打击点则在作为工业控制系统的生产安全监测单元的 SIS 上。

从防御工作来看，由于“海渊”（TRISIS）以通过伪装为 SIS 的日志软件获得被执行的机会，因此重要的防御点即在对软件供应链的管控上。应在采购阶段，严格落实供应链的安全管控，从源头遏制危害。在工业系统的运维中，针对工控系统环境的新设备安装上线、软件的发布升级、运维手段的接入等，都应进行全面的前置检查和移动介质接入管控。对于工业基础设施来说，生产网络和办公网络中的 PC 端点防御是一个必须做好的基础性工作，对于重要 PC 节点必须形成严格的依托白名单的主动防御机制。

从现状来看，大部分工业控制系统对效率性能的考虑远多于安全考虑，而安全考量中，更多依然是以传统的应对事故视角，而非应对攻击视角。做好工业系统的安全防御工作，必须按照三同步的原则进行，在系统规划、建设、运维的全周期考虑网络安全问题。这是一个复杂和系统的工作，在可管理网络的基础上，建设可防御的网络，推动从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的整体叠加演进。这个过程需要大量基础扎实的工作和预算投入。对已有系统的安全改造，因为涉及到生产业务的连续性、稳定性，可能牵扯到更多的问题。

完整版报告请扫描二维码进行阅读

一周简讯

- 1、安全厂商发现 IOT 僵尸网络 Mirai 和 Gafgyt 新变种
- 2、零日漏洞经纪人披露 Tor 浏览器中 NoScript 漏洞
- 3、研究人员发现 Mongo Lock 勒索软件分发活动
- 4、研究人员在微软门户网站上发现 3,090 个欺诈页面
- 5、Keybase 的浏览器扩展程序将信息暴露给第三方
- 6、研究人员通过破解 RSA 密钥发现 Chainshot 恶意软件
- 7、安全厂商披露银行木马 Kronos 变体 Osiris 攻击细节

每周安全事件

类 型	内 容
中文标题	越来越多的 iOS 程序收集用户信息出售
英文标题	A growing number of iOS apps collect and sell location data
作者及单位	Pierluigi Paganini
内容概述	研究人员表示越来越多的 iOS 应用程序收集 iPhone 用户的位置数据、WiFi 网络 ID 和其他数据，并将其出售给广告公司。调查发现这些应用程序都嵌入了由广告和营销公司提供的跟踪代码。许多情况下，隐藏的跟踪代码可以在任何时候运行，不断发送用户的 GPS 坐标等信息。 某些应用还会收集其他类型的设备信息，包括加速计信息（X 轴，Y 轴，Z 轴）、广告标识符（IDFA）、电池电量百分比和状态（电池或 USB 充电器）、蜂窝网络 MCC/MNC 、蜂窝网络名称、GPS 海拔高度和 / 或速度、出发 / 到达某个位置的时间戳等。研究团队发布的报告列出了 12 个获得数据的公司，包含跟踪代码的 24 个应用程序以及包含窃取资金代码的 100 个新闻应用程序。
链接地址	https://securityaffairs.co/wordpress/76056/breaking-news/ios-apps-collect-data.html

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	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.Asacub.d[prv,exp,rmt,spy] 2018-09-10	该应用程序伪装正常应用，运行后加载恶意子包。子包会接收远程指令控制，隐藏图标，发送短信，下载文件，拦截删除短信，上传用户短信、通讯录、通话记录、程序安装列表等隐私信息，还会诱导用户输入银行账户相关信息并上传，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.Triada.au[exp,sys] 2018-09-11	该应用程序伪装正常应用，私自提权，下载安装指定应用并启动，造成用户流量消耗，给用户手机带来安全隐患，建议卸载。（威胁等级高）
		Trojan/Android.RcsDataSysSpy.a[prv,rmt,spy] 2018-09-12	该应用程序是间谍件，运行隐藏图标，后台接收远程指令，上传用户联系人、通话记录、通话录音、短信箱、地理位置、日历等隐私信息，造成用户隐私泄露，建议立即卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.ToriesBig.a[fra,spr,rog]	该应用程序伪装 QQ 盗号工具，通过虚假盗号界面，诱导用户将该程序和虚假盗号视频分享给多个好友，而后诱导用户下载会私自发送扣费短信的流氓应用。恶意传播该类虚假程序，可能造成用户资费损失，建议立即卸载。（威胁等级高）
		G-Ware/Android.FakeAlipay.c[exp]	该应用程序伪装支付宝官方版，运行访问支付宝网站，本身无实际功能，包含风险广告插件，获取用户位置信息、造成用户资费消耗，建议不要使用。（威胁等级中）
		Trojan/Android.InfoStealer.aq[prv]	该应用程序安装无图标，会窃取用户的短信、照片等隐私信息并上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级低）
		Trojan/Android.Locker.av[rog,lck]	该应用程序是勒索程序，运行置顶勒索界面，禁用系统 USB 连接，会影响用户手机的正常使用且难以卸载，建议不要使用。（威胁等级中）
		G-Ware/Android.StealMoneyGame.bu[pay,rog]	该应用程序付费信息不明显，以领取道具的名义频繁加载弹窗，诱导用户点击付费，造成用户资费损失，建议卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 缓冲区溢出漏洞（CVE-2018-5002）	Adobe Flash Player 的 29.0.0.171 版本及更早版本具有缓冲区溢出漏洞，成功利用可实现任意代码执行。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.AGeneric	此威胁是一种可以下载并安装推广应用的灰色软件程序。该家族样本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。该家族没有统一的行为与功能，是以启发式检出的恶意代码。（威胁等级低）
		Trojan[Downloader]/JS.Agent	此威胁是一种使用 JS 脚本编写的木马家族。该家族并没有统一的行为、统一的功能，而是像一个木马集合一样，将大量基因片段定性的恶意代码归类。一般该家族样本通过网页挂马，当用户访问网页时，恶意 JS 脚本即会触发，可能会下载恶意代码并运行，窃取用户信息并回传。（威胁等级中）
		Trojan[Dropper]/VBS.Agent	此威胁是一种具有捆绑行为的木马类程序。该家族是以基因片段定性的恶意代码分类，该家族并没有统一的行为与的功能，而是像一个木马集合一样，将大量基因片段定性的恶意代码归类。（威胁等级低）
		RiskWare[Downloader]/Win32.DriverUpd	此威胁是一种可以下载安装推广应用的风险软件类程序。该家族样本运行后连接网络下载推广应用并安装，可能弹出广告，占用系统资源，影响用户使用。（威胁等级低）
		RiskWare[RiskTool]/Android.SMSreg	此威胁是一种可以下载安装推广应用的风险软件类程序。该家族样本作为“电池提高”应用程序，声称帮助最大限度提高设备的电池使用，实际在未经用户同意或不知情的前提下收集设备数据信息。（威胁等级低）

理解和解决信息共享的挑战

Jonathan Couch / 文　安天技术公益翻译组 / 译

来自情报共享组织的网络安全威胁信息价值不断下降，逐渐沦为另一个噪声源。本文将介绍出现这一问题的原因，并提出相应的解决方案。

“网络安全信息共享”这一话题并不新鲜。事实上，多年来我们一直在谈论它。我们知道自己应该共享信息，同时也希望其他人共享信息。我们甚至看到了一些信息共享的成功案例，共享者通常是同一行业中的同行，并且具有个人或长期业务关系。他们建立了一定程度的信任，使他们能够放心地交换真正有用的信息。

但是，当我们试图通过政府和行业组织来扩展这种信息交换时，情况就不那么乐观了。在公司层面，由于实际或潜在的法律责任，公司通常不像个人那样愿意共享信息。因此，更广泛的、真正有益于防御社区的信息共享尚未实现。积极参与者的数量和共享信息的质量，说明信息交换并不像预期的那样有效。

质量 vs 数量：价值递减的怪圈

许多组织希望信息共享能够“两全其美”。一方面，他们希望成为行业信息共享和分析中心（ISAC）或政府共享组织的一部分，例如美国国土安全部的自动信标共享计划（AIS）或英国网络安全信息共享合作伙伴计划（CSISP）。但另一方面，他们并未建立内部计划来确定可以共享的信息类型以及如何共享。与此相反，他们只是接收其他组织共享的信息。最终，为了应对共享组织的信息交换要求，他们不得不开始共享。但这引发了信息质量问题。

随着共享组织成员的增加，成员彼此间的信任也在减弱。许多组织不太愿意共享他们认为有价值的信息——例如，他们遭遇的攻击。相反，他们倾向于共享诸如 IP 地址和域名之类的攻击信标。信息共享逐渐变得自动化，包含很少的（或没有）情境信息，有时甚至是将从其他组织接收到的信息做二次共享。在没有情境信息的情况下，其他参与者就无从得知这些信息是否与他们相关，以及是否应该优先考虑。由于一些成员只关注信息的数量，而不关注信息的质量，导致共享组织对信息共享的兴趣下降。该共享组织提供的威胁信息的价值逐渐下降，沦为另一个噪声源。

能够在社区内共享丰富的、高质量的情境信息的团队，通常依靠与大量成员之间的“信息交换”。希望随着时间的推移，小公司也将开始共享信息。但是现在，共享信息的小公司还比较少。在小公司中，只有那些更先进的、拥有更多威胁运营计划的公司才会共享高价值的信息。除此之外，其他小公司主要是信息的使用者。随着这种“不平等感”的蔓延，整个共享结构将会崩溃。

打破这一怪圈：三步走

但是，情况也并非那么让人绝望。事实上，我们可以通过三种方法加强信息共享，使其能够按照预期提供价值。

第一步：建立信息共享和使用计划

组织需要从法律和合规的角度了解他们可以共享的内容。这将使他们能够在“共享”和“合规”之间取得平衡——不至于反应过度并关闭信息共享，也不会在无意中共享受隐私法保护的专有信息。通过明确的指南，安全团队可以提供包含情境的高质量信息。他们还需要了解他们将要使用哪些信息，以及如何使用。这将确保他们从接收的情报中获取最大的价值，既不会被大量的共享信息淹没，同时又不会错过其中可能蕴含的高价值信息。

第二步：监控信息质量

随着信息共享组织的壮大，战术信息的自动共享出现激增，这导致了信息质量的下降。共享组织必须监控信息的质量，确保传递给其他成员的信息是有价值的，无论是“已知信标”还是包含情境的信息，以便接收者可以确定该威胁与其自身环境的相关性。

第三步：设计所有人参与的方式

需要注意的问题是：以共享信息的数量衡量共享是否成功，并非一种有效的方法。为了保持质量和数量的平衡，我们需要考虑形成具有信任关系的子群（subgroup）。同时，较小的组织也应获取高价值的威胁信息。我们必须接受这样一个观念：在最初阶段，小公司可能无法提供太多信息，主要作为信息的接收者。

双管齐下的方法可以帮助满足他们的需求。首先，较小的组织应该加入或创建自己的行业共享社区，然后积极共享在其网络中发现的情境信息等情报。反过来，这将有助于更大的行业共享组织更好地保护整个行业——包括该行业中的小公司。其次，与托管安全服务提供商（MSSP）签订合同的小型组织，应该从提供商处获取此类情报。这种社区防御模式通常是 MSSP 对客户承诺的一部分，因此小公司应确保其供应商能够提供此类情报。

通过解决数量 / 质量挑战来打破信息价值递减的怪圈，信息交换将会蓬勃发展。最终，我们将能少些纸上谈兵，多些信息共享。

原文名称	Understanding & Solving the Information-Sharing Challenge
作者简介	Jonathan Couch。Jonathan Couch 是 ThreatQuotient 公司高级战略副总裁。
原文信息	2018 年 9 月 6 日发布于 Dark Reading 原文地址 https://www.darkreading.com/risk/understanding-and-solving-the-information-sharing-challenge-/a/d-id/1332717

安天发布《oledbg32.dll 窃密木马分析报告》

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发现一种窃密木马，原始文件名为 oledbg32.dll。该木马自 2015 年开始出现，最初并未受到关注。但在 2017 年 3 月的某次 WannaCry 攻击中，攻击者使用了 oledbg32.dll 收集受害者信息，最终植入 WannaCry。

该样本为 DLL 格式，有五个导出函数。System32iRun 修改注册表使 System32Run 开机自启动后调用 System32Run，而 System32Run 运行后并没有发现网络行为。SysWOW64Run、SysWOW64iRun 是 System32Run、System32iRun 的 64 位版本。对 DllEntryPoint 进行分析发现：其首先调用 InternetOpen 进行初始化，然后扩充字串 "%TEMP%\\ib.exe" 及 "%TEMP%\\ib.tmp"，创建两个线程，分别调用 1000E0F0 及 10010C20 处的函数，10010C20 处的函数为分配内存，1000E0F0 处的函数删除 %TEMP% 下的 oledbg.log 并在 %TEMP% 下创建文件 ib.exe，然后连接网络，提交 GET 请求 "http://akamai.co.nf/index.php?action=GComGicwMTg%3d&t=fH9lbGBlY3x8eXlpfm9mYXR8YA%3d%3d&m=&p=&f="，连接失败后调用 sleep 等待 6 小时后重新进行连接，成功后连接网络下载 http://akamai.co.nf/ib.tmp 并保存在 %TEMP% 下。接下来复制 ib.tmp 并重命名为 ib.exe，成功后删除 ib.tmp，ib.exe 运行后生成 ntap.dll 及 ntap.exe，ntap.dll 只有一个导出函数，运行后创建文件 c:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\thum.db，内容为加密的字符串 1422281865,attached。ntap.exe 运行后生成 c:\Documents and Settings\Administrator\Application Data\Adobe\Update\NotifyUpdates.dll 并创建任务计划，在登录时运行该 DLL 文件。

NotifyUpdates.dll 为主要载荷，可以获取 MAC 地址、操作系统版本、系统当前时间，运行后创建批处理脚本，该批处理脚本可以将系统信息（系统时间、已经安装的补丁）、当前进程、c:\Program Files 及 C:\Documents and Settings\Administrator\Recent 中的内容、当前网络连接、ARP 地址表写入创建的 .tmp 文件中，最后通过 POST 请求将存有系统信息的 .tmp 文件上传至 C&C 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。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

目前，安天追影产品已经实现了对该类恶意代码的检出。

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、文件来源信息分析鉴定器、数字证书鉴定器、文件元数据分析鉴定器、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。

概要信息

文件名	oledbg.dll
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	216 KB
MD5	86759CE27D0FE0B203AAA19D4390A416
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.BTSGeneric
判定依据	静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=86759CE27D0FE0B203AAA19D4390A416

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	附加信息	
延时	★★★	Sleeptime	0x0000EA60
		Sleeptime	0x000493E0
		Sleeptime	0x01499700

常见行为

获取主机用户名称	★
查找浏览器进程	★★
获取驱动器类型	★
查找指定内核模块	★
获取计算机名称	★
获取系统版本	★★
结束进程	★★
获取 socket 本地名称	★
连接网络	★
独占打开文件	★
获取系统内存	★★
创建特定窗体	★
增加 run 自启动项	★
感染文件	★★
自启动	★

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.dll	86759ce27d0fe0b203aaa19d4390a416	N/A	N/A
target.dll.dmp	ba4dfc2462e8d1e846d220bdb65bc411	N/A	N/A
.....	.....	.....	.....