安天发布《Magecart 第五小组开始使用 KPOT 开展窃密活动》报告

2019 年 8 月，安天 CERT 监测到了多起利用 KPOT 木马进行窃密的事件。分析人员通过对其 C2 以及脚本进行关联，判定这些窃密事件是由 Magecart 第五小组发起的。Magecart 是一个获取经济利益为主要目的的窃取支付信息的组织集合。Magecart 第五小组最早出现于 2016 年，利用 KPOT 窃取用户加密货币钱包信息、应用账户信息以及浏览器 cookies 等多种信息。攻击者主要利用了垃圾邮件以及 RIG 和 Fallout 漏洞利用工具包来传播木马。

KPOT 运行后会从 C2 服务器获取控制指令，根据控制指令窃取指定信息，并将信息加密后回传到 C2 服务器。KPOT 会获取系统语言版本判断当前语言所对应的国家，避开以下国家进行窃密：俄罗斯、亚美尼亚、阿塞拜疆、白俄罗斯、格鲁吉亚、哈萨克斯坦、塔吉克、土库曼和乌兹别克。该木马主要功能包括：窃取 Chrome、Firefox、Internet Explorer 浏览器的 cookies 和口令；窃取 shype、telegram、discord、battle.net、Steam 账户信息；窃取多种 FTP 和 Jabber 客户端账号信息；窃取多种 windows 凭证信息；窃取多种加密货币文件；获取屏幕截图。

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类窃密木马的鉴定；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、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据反病毒引擎鉴定器、BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	9f5e85a120c4c5d393d5a4f5196ab48771c347e870236bf760968c8233976333.exe
文件类型	BinExecute/Microsoft.PE[:X86]
大小	441 KB
MD5	E55ADC77DA695DF375AB985469B5E5E4
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Chapak
判定依据	反病毒引擎

◆ 操作系统

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
疑似桌面控制	★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1034	192.168.122.1	53
192.168.122.111	1033	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1034
192.168.122.1	53	192.168.122.111	1033
192.168.122.111	137	192.168.122.255	137
192.168.122.111	138	192.168.122.255	138
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.111	68
192.168.122.61	138	192.168.122.111	138
192.168.122.111	137	192.168.122.61	137

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 10 月 21 日 (总第 204 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天产品巡礼（系列二）——探海威胁检测系统

探海威胁检测系统是安天自主研发的网络威胁监测设备，以网络流量为检测分析对象，实现对网络扫描探测、远程漏洞利用、攻击载荷投放、僵尸网络活动、病毒扩散传播、木马远程控制等网络行为的检测和告警，能精准检测出已知海量恶意代码和网络攻击活动，有效发现网络可疑行为、资产和各类未知威胁。探海可与安天威胁情报服务结合，对多个 APT 攻击组织的载荷工具和 C2 基础设施实现带有精确组织指向的报告告警。

设备支持基于细粒度协议解析和还原留存的全要素采集能力，在实际工作场景中可以按照客户预设策略进行按需采集。设备的高速检测模式、全要素采集 + 检测模式、按需采集 + 检测模式和流量缓存等工作模式可以根据客户配置快速切换。针对还原文件，在安天 AVL SDK 下一代威胁检测引擎的支持下，进行海量恶意代码检测，并对所有还原对象进行格式识别和向量拆解，亦可投放到安天追影威胁分析系统进行联动分析。弥补了传统边界设备和入侵检测设备的检测深度不足，可以全面改善提升用户网络威胁发现，特别是海量已知威胁的精准判断和未知威胁发现能力。所有流量采集数据、文件拆解数据、分析数据均可通过标准接口提供给态势感知平台进行深度分析，为后续威胁分析、取证、溯源、猎杀等工作提供了必要的基础。

探海威胁检测系统可以为政府、军队、能源、金融、交通等行业客户持续提供监测能力，支撑客户的重大活动安全保障、高级威胁监测和安全事件响应。

功能简介

探海基于高速并行协议栈进行网络数据处理，基于综合网络行为检测引擎、AVL SDK 下一代威胁检测引擎、TrustStream 引擎、IoC 威胁情报检测等组合机制，通过多维度检测手段，实现威胁的发现、威胁源头定位，并对扫描、攻击、传输、投放、控制、心跳、升级、窃密回传等各种攻击行为进行检测。同时，通过对网络元数据、网络传输数据、载荷行为数据等信息的全要素、细粒度记录，对潜在威胁、未知威胁实现提早发现，提升用户对定向攻击等高级威胁的发现和溯源能力，协助用户持续观测资产安全遭遇的威胁状况、预警网络安全事件，有力支撑用户网络安全应急响应工作。

探海经过安天十余年的自主研发积累，形成了在协议解析及文件还原、网络入侵检测、恶意代码检测、特别是高级威胁监测等方面的领先优势。安天长期研发自主先进的威胁检测引擎，并从 2002 年开始支撑国家相关部门进行大规模恶意代码疫情的监测处置，并从 2010 年将技术能力和分析应急的重心逐步转入到应对高级网空威胁行为体所发动的 APT（高级持续性威胁）中，在高级威胁发现、分析、溯源方面取得了一系列进展；在威胁情报方面，安天基于大规模主动捕获感知环节的部署、海量样本与事件自动化分析体系和样本与威胁情报交换体系，形成了对多源异构样本和数据源的采集、分析、处理能力，形成了从信标规则到 TTP 情报的生产体系。这些均为探海的产品能力提供了有效支撑。

微信扫描二维码阅读原文

北佛罗里达州妇产科数据泄露影响约 52 万患者信息

北佛罗里达州妇产科（OB-GYN）于 2019 年 5 月 6 日加入了佛罗里达州妇女保健中心，并于今年 7 月 27 日意识到其网络遭到了网络攻击。该漏洞被认为发生在 2019 年 4 月 29 日或之前。受事件影响的医疗或个人信息可能包括姓名、人口统计信息、出生日期、社会保险号码、驾照或身份证号码、就业信息、医疗保险信息和健康信息，如治疗、诊断以及相关信息和医疗图像。已通过信函联系了北佛罗里达州妇产科（OB-GYN）的所有 528,188 名患者，并警告他们的个人数据可能已经泄露。

（原文链接：https://www.infosecurity-magazine.com/news/florida-womens-clinic-data-breach/）

全球性科技公司 Pitney Bowes 遭到恶意软件的攻击

Pitney Bowes 公司称：财富 500 强公司中 90% 是其客户，为这些大公司提供快递等服务，同时也为超过 100 万家其他公司提供配送服务。Pitney Bowes 公司证实，该公司已成为恶意软件攻击的受害者。恶意软件攻击对其部分系统的信息进行了加密，并干扰了客户对其服务的访问。该公司的邮件系统产品和在线会计报告都受到了此次事件的影响。具体来说，客户不能在他们的邮件机上重新填写邮资或上传交易记录，也不能检索会计报告。Pitney Bowes 公司表示，没有证据表明客户账户或数据受到了影响，也不认为存在其他客户风险。

（原文链接：https://www.zdnet.com/article/pitney-bowes-claims-customer-data-safe-following-malware-attack/）

每周安全事件

类 型	内 容
中文标题	Windows 10 安全更新导致开始菜单出现问题
英文标题	Windows 10 Start menu problems: We'll fix them in late October, says Microsoft
作者及单位	Liam Tung
内容概述	上周早些时候，一些用户开始报告说，KB4524147 的安全更新导致了打印机问题，而另一些用户则说，他们看到了一条“严重错误”消息，说明开始菜单无法工作。一些用户通过卸载更新解决了开始菜单的问题。微软表示，将修复过去几周以来一直影响 Windows 10 用户的启动菜单问题。微软员工在周六的帖子中说：“我们已经意识到了这个问题，并估计将于 10 月下旬发布解决方案。”
链接地址	https://www.zdnet.com/article/windows-10-start-menu-problems-well-fix-them-in-late-october-says-microsoft/

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	RiskWare/Android.FakeShenszstudent.a[sys] 2019-10-13	高	该应用程序为非官方应用，包含风险代码，运行有锁屏、激活设备管理器、恢复出厂设置、清除流量数据、重启等敏感行为，可能会删除系统文件，造成未知风险，请谨慎使用。
		Trojan/Android.Nileeye.a[prv] 2019-10-14	中	该应用程序包含风险代码，运行收集用户隐私信息上传到远程服务器，该程序可能配合其他程序实施网络钓鱼行为，存在隐私泄露风险，请卸载。
		Trojan/Android.HiddenAds.jc[exp,rog] 2019-10-15	低	该应用程序伪装为其他应用，运行隐藏图标，后台联网获取广告信息，会造成用户的资费消耗，建议卸载。
	较为活跃样本	RiskWare/Android.QQshare.p[exp]	中	该应用程序运行诱导加入指定 qq 群，进行分享推广引流，以及付费使用部分功能。可能造成用户资费消耗，存在一定的风险，为避免造成财产损失，建议谨慎使用。
		RiskWare/Android.Daikuan.p[rog	中	该应用程序行访问第三方网贷网站，可能没有财产权益保障，会造成用户财产损失，请谨慎使用。
		Trojan/Android.InfoStealer.bh[prv]	中	该应用程序包含恶意代码，运行后会获取用户通讯录并上传至服务器，造成用户隐私泄露，建议卸载。
		Trojan/Android.Evile8game.a[exp,rog]	低	该应用程序包含恶意代码，运行后联网加载恶意子包，上传用户手机基本信息，推送流氓广告，模拟用户点击进行刷量操作。造成用户流量消耗，建议卸载。
		Trojan/Android.Dropper.dp[exp,rog]	低	该应用程序内嵌恶意代码，动态释放恶意子包，反射调用，私自下载未知文件，会造成用户流量资费损耗，请卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	VBScript 远程代码执行漏洞（CVE-2019-1238）	高	VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理员用户权限登录，那么攻击者就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[Downloader]/JS.Small	中	此威胁是一种具有下载行为的木马类程序。该家族通过安装免费在线程序或第三方软件入侵用户电脑。该家族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。该家族会为黑客打开后门，允许黑客窃取用户的信息。
		Trojan[Exploit]/VBS.CVE-2014-6332	中	此威胁是一种可以利用漏洞下载恶意代码的木马家族。该家族以 VBS 脚本编写，攻击者可以下载恶意代码到感染者计算机中，窃取计算机信息。
		Trojan[Backdoor]/ASP.Ace	中	此威胁是一种带有后门的木马类程序。该家族进入用户电脑后会为黑客打开后门，进行远程控制系统。
		GrayWare[AdWare]/Win32.ELEX	低	此威胁是一种可以下载推广应用的灰色软件程序。该家族样本运行后会添加开机自启并注入到系统进程中。该家族样本可以连接网络下载并安装推广应用，在用户浏览网页时会弹出广告，占用系统资源，影响用户使用。
		RiskWare[RiskTool]/Win32.ChromePatcher	低	此威胁是一种风险软件类程序。该家族样本运行后会在感染者计算机中生成文件，自动在网络发布指定信息。

通过身份识别和鉴别构建数字信任

Valerie Bradford / 文 安天技术公益翻译组 / 译

根据梅里亚姆·韦伯斯特（Merriam-Webster）的说法，信任的字典定义是“某人或某物真实性的可靠保证”。在当今的数字世界中，信任是一个棘手的概念。无论是银行、零售商、保险公司、航空公司还是其他任何机构，要想在线开展业务，都必须对用户有一定程度的信任——相信他们是其所声称的本人，而不是企图窃取资金或数据的骗子或恶意机器人。但是，要构建对在线或移动用户的信任可能比看起来更加困难，需要对用户进行身份识别（identification）和鉴别（authentication）。

身份是什么

我们可以将“某人的真实性”视为其身份。了解数字用户身份的第一步被称为识别——这是用户声称自己是谁，以及识别用户身份的过程。用户可以使用其全名、账户，或者简单地使用用户名来标识自己的身份。在许多情况下，例如在开设新账户时，用户必须首先提供或证明其身份。

身份鉴别不同于识别

但是，仅凭身份识别还不足以在任何给定的数字交互中构建信任。你告诉我你的名字叫山姆（Sam），并不意味着我应该相信你。当然，我不会让你仅凭这种交互就取走山姆的毕生积蓄。信任是对所声称身份的可靠保证，这种保证以身份鉴别的形式进行。身份鉴别通常被定义为：证明用户确实是他们所声称身份的能力。

目前有多种鉴别用户身份的方式。最常用的方式可能是口令。我们通常将口令视为“用户所知道的内容”；也就是说，只有身份的真正所有者才能知道的信息。不幸的是，在当今世界，情况并非如此。

当用户开通一个新的在线账户时，他们可能会重用已有的口令。为什么用户会这样做呢——鉴于用户有大量的账户，他们需要记忆这些账户（如 90 个账户）的口令；而通过重用口令，他们就不用记忆众多的口令了，实现“一令行天下”。虽然这样看起来倒是方便了用户，但是安全性却降低了。

当今的身份鉴别策略

鉴于此，其他类型的身份鉴别开始出现。多因子身份鉴别（MFA）、无口令身份鉴别和自适应身份鉴别等策略在身份鉴别过程中增加了分析层次，使规避变得更加困难。多因子身份鉴别需要支持用户身份声明的其他因子。除了用户知道的内容（例如口令）之外，用户还需要证明自己拥有的东西（例如设备）和他们本身的信息（例如生物特征）。

另一方面，无口令身份鉴别完全省去了“用户知道的内容”。相反，它使用针对数字信任框架的情境数据来帮助企业决定信任用户的程度。这些情境数据可以是有关用户、设备、用户的活动、行为和网络环境的信息。添加到此分析中的信息层越多，越有助于构建数字信任，而不会因基于口令的身份鉴别遭受挫败。

诈骗检测：身份鉴别的另一个作用

无口令身份鉴别发挥了身份鉴别的另一个作用：诈骗检测。除了评估身份，证明用户是他们所声称的本人之外，企业还应考虑用户不是其所声称的本人的可能性。诈骗检测（例如身份鉴别）应该是多层的。用户或设备的情境分析应包括查找否定标识符——无论用户是人还是机器人，设备是 root 还是越狱设备，用户是否安装了恶意软件等。了解与数字用户或交互有关的风险，会影响对该身份的信任程度。

身份、鉴别和数字信任

最后，现代企业需要一种包含身份识别和身份鉴别的策略，以便为构建数字信任奠定基础。通过更好地了解用户（包括其行为和交互背后的完整情境），企业可以在不牺牲安全性的情况下实现更好的客户体验。

原文名称	How Authentication and Identification Work Together to Build Digital Trust
作者简介	Valerie Bradford。Valerie Bradford 是 IBM Security 的产品营销专家。
原文信息	2019 年 10 月 15 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/posts/how-authentication-and-identification-work-together-to-build-digital-trust/
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。