安天发布《Taurus 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 Taurus 的窃密木马。Taurus 是 2019 年公开售卖的窃密木马，该木马主要通过垃圾邮件传播，目的是窃取用户敏感信息。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。

Taurus 是一款具有反调试、反虚拟机和反沙箱检测的窃密木马。该窃密木马通过垃圾邮件传播，一旦用户打开附件中的 Word 文档并启用宏便会运行恶意宏执行 PowerShell 连接远程服务器下载并执行 Taurus 窃密木马。该木马执行后将自身注入到 dllhost.exe（用于管理 DLL）进程中。Taurus 运行后会窃取各种凭证包括 FTP 凭证、电子邮件凭证、用户浏览器中存储的凭证、Cookie、浏览器历史记录和信用卡信息等。除此之外，该木马还包括窃取加密货币钱包、窃取 Skype 历史、从应用程序中窃取会话文件、收集系统信息，例如系统配置和已安装软件列表等。Taurus 窃密木马将窃密的数据进行压缩并上传至远程服务器。

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。

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、关联分析鉴定器、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 BD 静态分析鉴定器、YARA 自定义鉴定器、动态行为鉴定器、关联分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	4da
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	876 KB
MD5	07DB6CFE1A8EB12035663D1F6FA11518
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Script.AGeneric
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

◆危险行为

行为描述	危险等级
加载内核文件	★★★

◆常见行为

行为描述	危险等级
获取系统版本	★
获取系统信息（处理器版本、处理器类型等）	★
加载运行时 DLL	★
打开自身进程文件	★
检测自身是否被调试	★★
创建窗口	★
查找窗口	★
连接网络	★
下载 PE	★★
获取驱动器类型	★
访问文件尾部	★
获取键盘状态	★
疑似桌面控制	★

◆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 2020 年 7 月 13 日 (总第 238 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天智甲率先完成 麒麟软件操作系统全平台兼容适配

近日，安天旗下的智甲终端防御系统（信创版）（以下简称：安天智甲）与麒麟软件有限公司旗下的所有操作系统，率先完成了兼容性互认证测试。本次兼容认证测试涵盖了兼容性测试、稳定性测试、性能测试和安全可靠性测试等。测试结果表明，安天智甲产品在麒麟软件操作系统上完全兼容，可为操作系统提供威胁检测处置与终端防御管理能力，完全满足用户需求。目前，安天智甲已完成与所有主流厂商国产操作系统发行版的全平台适配。

▲智甲与银河麒麟桌面操作系统兼容性认证

▲智甲与银河麒麟
高级服务器系统兼容性认证

安天智甲起步早、运行稳、适配全，集病毒查杀、实时防护、勒索病毒 / 挖矿病毒防护、漏洞检测与修复、终端管理、主机防火墙、外设管控、EDR、资产管理、主机加固、文件分析、威胁处置等多种功能于一体，为国产操作系统提供全面的安全防护能力。其内置国际领先的下一代检测引擎 AVL-SDK，可精准检测包括感染式病毒、蠕虫、木马、黑客工具、风险软件、流氓软件等八大类别，近四万个家族，超过 1200 万的病毒变种（覆盖百亿级样本 HASH），还可给出包括病毒类型、活跃平台、家族名、变种号、典型行为等精准信息。

安天是较早为国产化操作系统提供安全防护产品的厂商，同时也为多款国产操作系统提供了早期的安全规划建议。早在 2015 年，在国家相关部门的统一规划下，安天就与中标麒麟、中科方德、银河麒麟等国产操作系统厂商进行了深入的代码级合作，实现了预装试点。2016 年，成为唯一一家成功支撑“万台规模应用示范 SMZY 计算机采购项目”的厂商，获得了主管部门的高度认可。此次适配的麒麟软件有限公司，旗下拥有“中标麒麟”“银河麒麟”两大产品品牌，目前已形成服务器操作系统、桌面操作系统、嵌入式操作系统和麒麟云等产品，旗下操作系统，已连续 8 年位列中国 Linux 市场占有率第一名。按照“国产硬件 + 国产化操作系统”的双国产组合计算，安天智甲已实现对近百种国产版本的兼容适配，有效保障了国产信创环境的安全可靠。

安天未来将继续发挥技术优势，聚焦信创行业发展，积极投入国产化安全领域，并联合更多合作伙伴，共同推动国家安全自主创新建设。

微信扫描二维码关注公众号查看原文

Lazarus 针对美国和欧洲进行 Magecart 攻击

Sansec 研究表明，朝鲜 Lazarus（HIDDEN COBRA）组织针对美国和欧洲在线购物者进行支付卡窃取攻击（Magecart 攻击）。Lazarus 设法获得大型零售商在线商店代码，例如国际时尚连锁店 Claire's 7。Lazarus 如何获得访问权限尚不清楚，但是攻击者经常使用鱼叉式攻击（诱骗邮件）来获取零售人员的密码。通过未经授权的访问，Lazarus 将其恶意脚本注入到商店结帐页面。一旦客户完成交易，支付卡窃取器将截获的数据（如信用卡号码）发送到 Lazarus 控制的收集服务器。

（原文链接：https://sansec.io/research/north-korea-magecart）

Purple Fox 漏洞利用工具包新增两个漏洞

Proofpoint研究人员发现Purple Fox漏洞利用工具包新增加了两个漏洞，现在可针对CVE-2020-0674和CVE-2019-1458进行漏洞利用。CVE-2020-0674是一个Internet Explorer中脚本引擎内存损坏漏洞，微软在2020年2月周二的安全更新中发布该漏洞补丁。CVE-2019-1458是一个本地特权提升(LPE)漏洞，曾在Operation WizardOpium中被利用，由微软在2019年12月周二的安全更新中发布该漏洞补丁。

（原文链接：https://www.proofpoint.com/us/blog/threat-insight/purple-fox-ek-adds-exploits-cve-2020-0674-and-cve-2019-1458-its-arsenal）

每周安全事件

类 型	内 容
中文标题	Honey Trap 行动：APT36 攻击印度国防组织
英文标题	Operation ‘Honey Trap’: APT36 Targets Defense Organizations in India
作者及单位	Kalpesh Mantri
内容概述	Seqrite 研究人员发现与巴基斯坦有联系的威胁组织 APT36 的活动有所增加，此次所观察到名为“Honey Trap”的行动针对印度国防组织和其他政府组织的人员。APT36 使用美女虚假资料来引诱目标打开其电子邮件或在信息平台上聊天。当目标打开包含的附件时，将释放基于 MSIL 的 Crimson RAT，该 RAT 用于数据窃取活动并将其发送到 CnC 服务器。
链接地址	https://www.seqrite.com/blog/operation-honey-trap-apt36-targets-defense-organizations-in-india/

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 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
活跃漏洞	Microsoft ChakraCore 和 Edge 安全漏洞（CVE-2020-1073）	高	ChakraCore 脚本引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。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。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。
	Microsoft Excel 安全漏洞（CVE-2020-1226）	高	当 Microsoft Excel 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。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。
	Microsoft Windows 和 Windows Server 安全漏洞（CVE-2020-1300）	高	当 Microsoft Windows 无法正确处理 cabinet 文件时，会触发远程代码执行漏洞。若要利用此漏洞，攻击者需要诱使用户打开经特殊设计的 cabinet 文件或欺骗网络打印机并诱骗用户安装伪装成打印机驱动程序的恶意 cabinet 文件。
较为活跃样本家族	Trojan[Ransom]/Win32.Blocker	中	此威胁是一种赎金类木马家族。该家族木马运行后会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。
	Virus/Win32.PolyRansom	中	此威胁是一种感染类病毒家族。该家族病毒运行一定的时间后，会阻止访问操作系统。当重新进入操作系统时，会要求用户支付比特币或一定数额的金钱。
	Trojan[Backdoor]/Win32.Salgorea	中	此威胁是一种可以下载恶意代码的木马类家族。该家族样本运行后连接网络下载恶意代码并执行。
	Trojan[Banker]/Win32.Shifu	中	此威胁是一种以窃取网络银行敏感信息 (如银行账号、密码、信用卡信息等）为目的的木马类家族。该家族木马通过修改注册表实现开机启动，收集记录用户网银信息，并将所有收集的信息发送给黑客。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族木马主要是利用漏洞传播并组建僵尸网络。
	Trojan[Dropper]/Android.Shedun	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马运行后，通过欺骗用户授权安装，其可获得专为视觉障碍用户设计的 Android Accessibility Service 的控制权限。
	Trojan[Spy]/Android.SmForw	中	此威胁是安卓平台上一种间谍类木马家族。该家族木马运行后，长久驻留系统，持续监控用户，收集用户系统信息，造成用户隐私泄露。

无接触支付的安全风险

苏·波伦巴 / 文 安天技术公益翻译组 / 译

无接触支付最早于上世纪 90 年代出现，现在风头正盛。公司和消费者试图在面对面交易中以尽可能减少物理交互的方式完成业务。

回想一下，我们其实一直在推动无接触支付的发展。企业对数字方法的依赖不断增长，并针对各种交互实施新的规程。例如，“安检”时，要求顾客不携带行李或钱包，并掏出口袋里的所有物品，以通过金属探测器，从而简化闸口和售票亭的安全检测。

消费者将携带的物品减到最少，这意味着手头的现金也会减少。他们通过手机开展业务的次数越多，就会越便捷，效率也就越高。但是，在这种情况下，企业能否确保手机的安全呢?

无接触支付的兴起

苏米特 · 阿加瓦尔（Sumit Agarwal）因创造了消费者正在推动无接触支付的发展——信用卡公司透露，2020 年第一季度信用卡的使用量呈两位数增长。Mastercard 首席执行官阿杰 · 邦加（Ajay Banga）在接受《福布斯》采访时表示，消费者“正在寻找一种快速在商店购物的方式。通过这种方式，他们无需兑换现金、接触终端或其他任何东西。”

无接触支付方法通常由公司使用。中小型企业（SMB）向数字支付转移的速度较慢，在数字化转型和网络安全增强方面通常落后于大型企业。随着越来越多的客户认为使用手机进行无接触支付是最安全的交易方式，这种落后情况有望改变。

此外，信用卡公司并非无接触交易的唯一参与者。诸如 Venmo、Zelle 和 PayPal 之类的应用以及公司自有的支付方式更受消费者青睐。甚至美国政府也将新冠疫情的补贴通过某应用发放给其公民。

便捷带来风险

无接触支付很方便；但是像其他技术一样，它会带来移动安全和数据隐私风险。鉴于无接触支付不需要 PIN 码，一旦用户的信用卡或设备失窃，其账户可能会被犯罪分子轻松访问。如果手机没有适当的安全保护措施，则任何人都可以轻松进行手机支付。此外，许多此类交易都不开收据，因此手机的所有者很难证明这些交易是诈骗。

无接触信用卡使用射频识别（RFID）技术传输数据，而黑客已经成功伪造了扫描仪或刷卡机，旨在窃取通过 RFID 传输的数据。如果黑客窃取了银行卡或钱包的信息，就可以创建克隆卡。另一方面，手机钱包依靠“近场通信”（NFC）近距离传输数据，仍然是进行金融交易最安全的方法之一。

无接触支付可以通过更安全的传输方法和手机锁定来减少诈骗。相比而言，更大的威胁是数据隐私泄露。无接触系统从用户那里收集大量数据，并使用这些信息来跟踪用户。当然，每当用户将应用下载到智能手机上时，都会存在恶意软件或中间人（MitM）攻击风险，攻击者可以访问设备上存储的信息——如银行账户、个人信息或机密工作文件等。此外，还有可能出现旨在窃取敏感数据的社会工程和网络钓鱼诈骗。

增强手机安全以降低风险

消费者需要关注与无接触手机支付相关的风险，企业也需要减轻潜在风险。特别是，如果公司内部的移动设备既用户个人也用于企业用途时，尤其要注意此类风险。虽说 NFC 技术的安全性可以媲美在受信环境中使用信用卡，但是我们还可以采取下述方法增强客户交易的安全性。

●交易时采用多因子身份鉴别（MFA）。手机支付对每个人来说都是快速和简便的，但是要想确保安全，需要花几秒钟输入口令、数字签名或某种形式的物理 / 生物特征识别信息。

●确保所有交易均已加密。

●使用以设备为中心的加密技术，以验证信息是否来自某台设备（这些信息不与其他设备共享）。这样，黑客就无法窃取信息并利用这些信息进行手机支付了，这能够减少诈骗的发生。

●确保公司根据“支付卡行业（PCI）安全标准委员会”指南进行信用卡交易，根据数据隐私法规使用和存储收集到的信息。

无接触支付是最安全的金融交易方式之一。随着更多的企业开始使用该技术，更多的消费者希望尽可能减少物理接触，未来几个月内手机钱包的使用将会能加。现在，企业应着手解决手机支付的安全问题，这样能够免于在未来遭受网络安全事件。

原文名称	The Security Risks of Contactless Payment
作者简介	苏 · 波伦巴（Sue Poremba）。苏 · 波伦巴是一位自由作家。
原文信息	2020 年 6 月 26 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/articles/the-security-risks-of-contactless-payment/
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。