安天智甲有效阻断 DaVinci 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 DaVinci 的勒索软件，该勒索软件发现于 2020 年 8 月中旬，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序，该勒索软件程序执行后不会对文件进行加密，而是调用 CMD 命令行程序直接删除文件，创建屏幕锁程序作为勒索信。经验证，安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻断 DaVinci 勒索软件的行为。

DaVinci 勒索软件运行后，生成屏幕锁程序覆盖用户桌面，快速将屏幕锁程序结束后未发现对文件进行加密和添加后缀名的行为，而是通过调用 CMD 命令行程序删除文件，在 CMD 命令行界面中可以观察到遍历文件的行为，以及有访问文件路径成功和访问文件路径失败的记录，执行命令将可访问路径下的文件进行删除，通过屏幕锁程序掩盖其行为。屏幕锁程序界面为勒索软件说明，包含订阅 YouTube 账号、关注 Instagram 账号、发送价值 300 美元的比特币到指定钱包地址和通过邮箱与攻击者进行联系。

▲DaVinci 勒索信

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、元数据信息鉴定器、数字证书鉴定器、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、文件相似分析鉴定器、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将文件判定为木马程序。

◆ 概要信息

文件名	E3AD4136679055F898D6F8DCFEEE0782
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	98 KB
MD5	E3AD4136679055F898D6F8DCFEEE0782
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/MSIL.Encoder
判定依据	反病毒引擎

◆ 操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
搜索文件	★★★★
查询软件限制策略	★★★
通过 CMD 隐藏删除自身	★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
将程序错误返回给调用者	★★
获取系统版本	★
镜像劫持	★★
检测自身是否被调试	★★
使用 windows COM 库 API	★★
.....	.....

◆扫描二维码查看完整报告

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 8 月 31 日 (总第 245 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天发布 2020 版 Smokeloader 僵尸网络变种分析报告

概述

近期，安天 CERT 通过网络监测发现了一起僵尸网络事件，经分析人员判定，该僵尸网络名为 Smokeloader，它从 2011 年开始在黑客论坛出售，一直处于更新状态。安天 CERT 分析人员发现本次活跃的 Smokeloader 样本是 2020 年最新的版本。Smokeloader 主要通过垃圾邮件携带恶意宏代码的 Office 文档进行传播，该样本具备远程下载其它组件、窃取用户敏感信息和发起 DDoS 攻击等功能。该僵尸网络曾被发现用来传播 GandCrab 勒索软件 [1]、Kronos 银行木马 [2] 等多款臭名昭著的恶意软件。

2020 版本的 Smokeloader 使用多种规避检测和对抗分析的技术，如运行环境的检测、花指令、代码自解密、反虚拟机等。运行成功后将自身添加为计划任务，保证自身的持久化。Smokeloader 在获取系统基本信息后，将其加密发送到攻击者服务器，接收返回信息，下载插件并注入内存中运行，插件功能主要包括窃取网站信息、收集邮件信息、窃取虚拟货币信息、监控浏览器、键盘记录、下载 Team Viewer 等三种远程控制软件进行隐蔽控制等。此外 Smokeloader 还会下载远程控制程序、挖矿木马和勒索软件。

Smokeloader 为了达成目的做了充分的“多手准备”：为了实现远程控制功能，下载了三种远程控制程序来提升远控的成功机率；为了实现窃取浏览器凭证等信息，使用了多套技术装备提升窃取浏览器信息的成功机率；使用了多种反调试、反虚拟机和反查杀等技术对抗安全人员的分析、自动化分析环境的检测和安全软件的查杀。攻击者使用了 Anyplace Control、AnyDesk 和 Team Viewer 三种远程控制软件，它们的特点是网络流量均由各自的服务器进行通信，即攻击者与受害者不直接通信，而是通过上述三款远程控制软件的服务器进行中转，导致追踪攻击者的难度增大。

事件对应的 ATT&CK 映射图谱

该起事件针对目标系统投放 Smokeloader 僵尸网络，通过对该事件进行 ATT&CK 映射，展示攻击者在该事件中使用的技术特点。

▲事件对应的 ATT&CK 映射图谱

样本概览

● 样本标签

病毒名称	Trojan/Win32.Wacatac
原始文件名	atx777.exe
MD5	E116B79051AFDA3B8B39EA718EACF2D2
文件格式	BinExecute/Microsoft.EXE[:X86]
文件大小	206 KB(210,944 字节)
时间戳	2019-08-30 14:17:38
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C/C++
VT 首次上传时间	2020-06-25 09:00:31
VT 检测结果	56/72

▲Smokeloader 样本标签

● 样本功能流程概览

Smokeloader 僵尸网络通常使用垃圾邮件传播，邮件附件携带恶意宏文档，文档启用宏后下载 Smokeloader 僵尸网络，该僵尸网络运行后首先通过 shellcode 技术与自身程序创建系统 ntdll.dll 方式来规避检测，然后通过检测系统注册表中是否存在特定的关键词方式判断是否在虚拟机中运行。样本首先判断自身是否在 Windows7 以上系统环境中运行，否则退出进程。样本成功执行后将恶意代码注入到系统 Explorer 进程中，将自身添加为计划任务，间隔 10 分钟运行一次，保证自身的持久化。样本在获取系统基本信息后，将其加密发送到攻击者服务器，并下载落地多个实体文件，包括 Avaddon 勒索软件、CoinMiner 挖矿木马、远程控制软件（Team Viewer、AnyDesk、Anyplace Control）等，此外该僵尸网络还在内存中下载了多个插件。

通过安天威胁情报综合分析平台关联 Smokeloader 样本，发现了大量与该僵尸网络相关联的域名、IP、样本等信息。（详见安天微信公众号原文内容）

防护建议

安天提醒广大用户，提高网络安全意识，及时进行系统更新和漏洞修复，避免下载非正版的应用软件、非官方游戏及注册机等；安装具有主动防御能力的终端防护软件（如安天智甲）以对勒索软件提供有效防护；及时备份重要文件，文件备份应与主机隔离；尽量避免打开社交媒体分享的不明来源链接，将信任网站添加书签并通过书签访问；避免使用弱口令或统一的口令；接收邮件时要确认发送来源是否可靠，避免打开可疑邮件中的网址和附件，避免轻易下载来源不明的附件。

目前，安天智甲终端防御系统（V5.0.5.08181344）可实现对以上恶意软件的查杀与有效防护。

扫码了解详细样本分析等更多内容

每周安全事件

类 型	内 容
中文标题	费城运输局业务因恶意软件攻击而中断
英文标题	Malware Attack Stifles Philadelphia Area Transit Agency
作者及单位	PATRICIA MADEJ
内容概述	两周前的一次恶意软件攻击继续扼杀宾夕法尼亚州东南部费城运输管理局（SEPTA）。由于 SEPTA 恶意软件攻击的严重性“非常高”，因为它是造成如此多破坏的原因。这次袭击导致 SEPTA 关闭了工资单和远程计时功能，位于 12th 和 Market Street 的 SEPTA 总部没有互联网。SEPTA 已经为大多数员工找到了一种通过基于云的系统重新获得电子邮件访问权限的方法。
链接地址	https://www.govtech.com/public-safety/Malware-Attack-Stifles-Philadelphia-Area-Transit-Agency.html

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	威胁等级	简要描述
活跃漏洞	Microsoft Windows Jet Database Engine 安全漏洞（CVE-2020-1473	高	当 Windows Jet 数据库引擎不正确地处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。攻击者可以通过诱使受害者打开经特殊设计的文件来利用此漏洞。
	Microsoft Windows Codecs Library 安全漏洞（CVE-2020-1560）	高	当 Microsoft Windows Codecs 库处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以获取信息，从而进一步入侵用户系统。若要利用此漏洞，需要攻击者发送经特殊设计的文件到目标程序。
	Microsoft Windows Graphics Components 安全漏洞（CVE-2020-1561）	高	Microsoft 图形组件在内存处理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对目标系统执行任意代码。若要利用该漏洞，攻击者需要诱使用户打开一个经过特殊设计的文件。
较为活跃样本家族	Trojan[Proxy]/Win32.Qukart	中	此威胁是一类可以窃取用户信息的木马家族。该家族木马运行后连接远程服务器接受攻击者恶意操作，收集系统信息并回传。
	Trojan[Banker]/Win32.Banbra	中	此威胁是一种以窃取网络银行敏感信息为目的木马家族。该家族木马伪装成正常数据，以获取认证。该病毒木马利用各种途径，使黑客获得数字证书来伪造文件。该家族木马还会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据发送给远程黑客。
	Trojan/Win32.Blamon	中	此威胁是一种可以窃取密码信息的木马家族。该家族样本运行后会窃取用户账户信息，记录键盘击键等。
	Trojan[Backdoor]/Linux.Gafgyt	中	此威胁是一种 Linux 平台上的具有窃密行为的后门家族。该家族木马运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操 作，并且会收集机器上的信息上传给远程控制端。
	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/Android.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。
	Trojan/Android.Hqwar	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，伪装成系统应用，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗。

了解移动安全威胁

姆祖基·鲁西 / 文 安天技术公益翻译组 / 译

只要有利可图，攻击者就有可能利用安全漏洞和薄弱的入口点来访问敏感的消费者个人信息。

这导致相当一部分消费者不再使用移动银行服务。金融机构颇为头疼，他们必须弄清楚如何通过移动渠道，以安全可靠的方式提供全面的金融服务。然而，在“移动设备优先”体验的需求下，推出移动银行服务的压力与日俱增。

要想为消费者提供无缝、全渠道的服务，金融机构必须了解他们所面对的攻击者及其诈骗策略。下面，我们将详细分析目前的移动银行安全威胁。

移动设备使用率上升导致移动恶意软件激增

银行恶意软件已经成为一种非常普遍的移动威胁。在全球新冠疫情下，诈骗者利用了人们的恐惧和不确定性心理，导致此类威胁更加严重。Malwarebytes 的最新报告指出，近几个月来，移动银行恶意软件激增，其目的在于窃取个人信息，利用在家办公的环境中安全措施较弱的远程连接和移动设备来访问更有价值的公司网络。

移动恶意软件引发的数据泄露事件，会给企业带来数百万美元的经济损失，并严重损害其客户信任度和忠诚度。

过早推出产品导致软件质量和安全性不足

保护移动设备是一项艰巨的任务。移动应用开发人员需要考虑多个实体，包括设备制造商、移动操作系统开发人员、应用开发人员、移动运营商和服务提供商等。我们无法以同样的方法保护所有平台或设备。这意味着，开发人员必须不断克服各种独特挑战，才能降低诈骗风险。

现实情况是，在如此复杂的生态系统中，移动应用开发人员并非总能了解所有风险，这会导致不安全的移动数据、连接和交易。此外，新兴技术和创新不断出现，市场飞速发展，给开发人员带来了更大的压力。开发人员缺乏相关资源和时间，无法妥善地保护消费者，这会导致消费者遭受攻击和敏感数据泄露。

数字安全协议中的漏洞

在任何给定时间，上述生态系统中的每个实体都必须确认交易另一端实体的合法性。移动银行应用中缺少诸如安全套接字层(SSL)和传输层安全性（TLS）之类的数字安全协议，因此很难在每个实体之间建立加密链接，无法阻止网络钓鱼和中间人攻击。

如果移动生态系统继续以目前的速度发展，就会越来越复杂，而且会连接越来越多的第三方服务和网络。鉴于此，我们必须要修复已损坏的 SSL 证书验证系统。

不可靠的移动设备识别

另一个问题是设备识别。在移动生态系统中，各实体识别设备的唯一方法是设备指纹。在此过程中，设备的某些特定属性（操作系统、Web 浏览器的类型和版本、设备的 IP 地址等）被组合在一起进行识别。然后，相关实体从数据库中提取这些信息，用于防止诈骗等目的。

数据隐私问题和设备上有限的数据共享，削弱了身份验证的过程和可靠性。如果我们没有足够的离散数据点来建立可靠的数字指纹，则整个系统都将失效。

身份鉴别技术亟待更新

诈骗者总是在寻找拦截机密登录信息的方法。利用这些信息，他们就能访问受保护的账户。双因子身份鉴别（2FA）已成为银行首选的安全方法，该方法能够可靠地鉴别试图访问移动渠道的用户并防御网络犯罪分子。

通常，2FA 依赖于用户在尝试登录时通过短信发送至其手机的一次性密码（OTP）。不幸的是，随着网络钓鱼技术（尤其是通过短信的网络钓鱼）的发展，黑客得以访问移动设备和通过短信发送的 OTP，还可以访问用户账户并确认诈骗交易。

此外，攻击者还可以使用其他策略（例如 SIM 卡劫持）来访问敏感信息和账户。

缺乏行业法规和标准

如果不建立严格的在线银行安全标准和指南来保护最终用户，那么消费者对银行的信任度就会降低，这会阻碍用户对移动银行市场的接受。美国联邦金融机构检验委员会（FFIEC）尚未就移动设备的身份验证和识别问题发布足够的指导。监管机构必须将出台移动安全标准作为头等大事，尤其是在新技术和移动恶意软件持续扰乱市场的情况下。

银行要牢记的基本问题是：在竞争激烈的金融服务市场中，客户信任是最重要的货币。在提供无缝、全渠道的客户体验的竞赛中，银行应实现这样一种平衡：集成更好的安全协议同时又不损害可用性。要想在动态的安全环境中独树一帜，银行需研究最新的工具和技术，并与第三方服务提供商建立可信赖的合作伙伴关系。

原文名称	Know the threats to mobile security
作者简介	姆祖基 · 鲁西 (Mzukisi Rusi) 。姆祖基 · 鲁西是 Entersekt 北美分部的技术交付主管。
原文信息	2020 年 8 月 21 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/08/21/know-the-threats-to-mobile-security/
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。