安天发布《Vidar 信息窃取木马分析报告》

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名为 Vidar 的新型信息窃取木马。攻击者使用 Fallout 漏洞利用工具包，通过恶意广告来传播 Vidar 病毒。Vidar 不仅能窃取用户敏感信息，而且还具有加载器功能，可以使系统继续感染其他恶意软件，受到二次攻击。

Vidar 在 2018 年 10 月首次出现，它与 Arkei 窃取木马的相似度极高，并且拥有这类木马的一些典型功能，如窃取浏览器历史记录，加密货币钱包数据、应用数据、即时消息会话、屏幕截图、系统快照等信息。值得注意的是，Vidar 正作为一款应用产品在应用商店和论坛出售，购买者可以通过配置文件设置他们感兴趣的数据，生成自定义的木马文件。当 Vidar 运行后，它将搜索配置文件中指定的数据，通过未加密的 HTTP POST 请求将这些数据上传至 C2 服务器，其中包括系统详细信息（系统概述、正在运行的进程、已安装的程序）以及受害者的个人信息（IP 地址、国家、城市、ISP）。之后，Vidar 还可以通过 C2 服务器下载其他恶意软件对系统进行二次攻击。在最近的恶意活动中，Vidar 与 GrandCrab 勒索软件结合，给用户造成双重打击。

安天 CERT 提醒广大政企客户，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。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、YARA 自定义鉴定器、文件来源信息鉴定器、数字证书鉴定器、文件元数据鉴定器、动态 (Win7 x86) 鉴定器、反病毒引擎鉴定器、动态（WinXP）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。

最终依据动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	2679fa8e9fd0c1f6f26527d53759bb596fda43a741b4dfcc99a8c0907836a835
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	556 KB
MD5	8B2403119F61C4F01F8FAF07A36CD064
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	动态行为鉴定器

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=8b2403119f61c4f01f8faf07a36cd064

◆ 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

◆ 危险行为

行为描述	危险等级
延时	★★★
检测虚拟机	★★★★★

◆ 常见行为

连接网络	★
枚举进程	★
访问文件尾部	★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★★
获取 CPU 信息	★★
疑似查找浏览器进程	★★
获取 CPU 信息	★★
疑似桌面控制	★

◆ 进程监控

PID	创建
472	lsass.exe
2152	target.exe
2116	target.exe

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 01 月 28 日 (总第 170 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天态势感知平台再度获奖——被评为中国信息安全产业年度“优秀创新型产业解决方案”

1 月 18 日上午，为及时跟踪信息安全领域产业动态，加强杂志与产业界沟通联络，最大限度发挥产业优势，携手共建我国网络强国事业，由《中国信息安全》杂志社发起的 2018 年度信息安全领域创新型产品解决方案和领军专家宣传活动（以下简称“双推活动”）在中关村军民融合产业园举行。安天态势感知平台获评年度“优秀创新型产品解决方案”，安天集团创始人、首席架构师肖新光获评 2018 年度中国信息安全产业“领军人物”。

由《中国信息安全》杂志社主办的“双推”活动开始于 2018 年 10 月，本次活动属公益性质，旨在借助各相关媒体，大力宣扬获得推荐的网络安全创新产品和领军人物事迹，弘扬为网络强国事业做出贡献的典型单位与个人。本次活动邀请了多位院士，以及业内的领导和专家组成评审团，采取函评、网评与会评相结合的方式，对推出的单位和个人事迹进行评审。

安天态势感知平台分为面向网信主管部门和职能部门的“监测型态势感知解决方案”以及正在研发的面向重要信息系统及关键信息基础设施的“战术型态势感知平台体系解决方案”。

态势感知在积极防御体系中对于提供响应决策、支持保障业务弹性和风险控制至关重要。但当前在态势感知实践中，往往更偏重于面向策略调整的宏观态势感知，难以支撑有效积极防御体系。面向实战化运行的战术型态势感知能够为威胁对抗行动提供实时监控响应能力，指挥对网络潜伏威胁进行猎杀清除，在攻防时间周期上适应高速多变的攻击行动，提升网络安全防护工作的积极性和主动性。

安天为重要信息系统和关键信息基础设施定制面向实战化运行的战术型态势感知解决方案，全面覆盖了网络和信息化基础设施各个组成实体，实现全生命周期的资产集中安全运维；通过将威胁知识与客户专有多源安全数据结合，配套高阶威胁情报与持续追溯服务，持续将威胁应对经验转换为客户的防护与响应能力。

要做好网络安全态势感知工作，需要准确把握四种变化：

- 对手的变化：从应对单点威胁到应对高级网空威胁行为体，网空防御者不能脱离具体的防御场景和其所承载的信息价值。
- 视角的变化：从自我闭环走向赋能客户，实现与攻击者的对抗闭环，客户侧安全防御人员最熟悉自身的信息系统，是网空防御工作的主角，应将客户置于闭环上。
- 思路的变化：从网络安全监测平台走向战术型态势感知平台，安天在监测型态势感知平台基本研发成熟的情况下，正在紧锣密鼓的加快研发实战化运行的战术型态势感知平台。
- 效果的变化：从单点防护能力到动态综合防御能力，坚持实战化的导向，构建动态综合网络安全防御体系。

在深刻掌握这些变化的基础上，遵循网络强国战略指导思想，以网络安全能力叠加演进为导向，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

尊敬的读者：

2019 年春节即将来临，《安天周观察》于春节期间休刊两期，恢复出版时间为 2019 年 2 月 18 日。感谢所有读者对《安天周观察》一直以来的支持与关注！

祝大家春节快乐！

2019 年 1 月 28 日

每周安全事件

类 型	内 容
中文标题	在线赌场服务器数据泄漏公开 1.08 亿条投注信息
英文标题	Online casino group leaks information on 108 million bets, including user details
作者及单位	Catalin Cimpanu
内容概述	一家在线赌场发生数据泄露，暴露超过 1.08 亿条投注信息，包含有关当前投注、获胜、存取款的信息、支付卡详细信息。泄露的用户数据包括真实姓名、家庭住址、电话号码、电子邮件地址、出生日期、网站用户名、帐户余额、IP 地址、浏览器和操作系统详细信息、上次登录信息和播放游戏列表。数据从 ElasticSearch 服务器泄露，ElasticSearch 是一种可移植的高级搜索引擎，公司可以通过安装这些搜索引擎来改进其网络应用的数据索引和搜索功能。此类服务器通常处理公司最敏感的信息，安装在内部网络上，不在线公开。研究人员还在该服务器上发现 kahunacasino.com、azur-casino.com、easybet.com 和 viproomcasino.net 等域名，分析表明这些域名来自同一家公司。
链接地址	https://www.zdnet.com/article/online-casino-group-leaks-information-on-108-million-bets-including-user-details/

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 5 个 PC 平台的恶意代码和漏洞值得关注

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.fadog.a[prv,rmt,spy] 2019-01-20	该应用程序是一款监控软件，运行后会接收远程控制指令，获取系统 root 权限，窃取用户短信、通话记录、联系人、地理位置、社交软件记录、浏览器历史记录、手机文件、SIM 卡信息等大量隐私信息，私自截屏、拍照、录音、录像，监听用户短信、通话，私自发送短信、拨打电话，并将隐私信息上传。造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.Robobt.a[prv,exp,sys,rmt,spy] 2019-01-21	该应用程序伪装正常应用，接收短信远程指令，修改设备网络状态、锁定设备或执行双清指令、开启 / 关闭录音，删除通话记录，上传用户音频文件、位置信息等，还会私自回复短信，造成用户隐私泄露和资费损耗，请立即卸载。（威胁等级高）
		Trojan/Android.newfullad.a[exp,rog,fra] 2019-01-22	该应用程序伪装正常应用，运行后频繁弹出全屏广告诱导用户下载，联网上传用户正版应用下载统计信息，私自下载非正版恶意应用，向广告商发送虚假安装信息。存在欺诈行为，造成用户流量消耗，使手机存在安全隐患，建议立即卸载。（威胁等级高）
	较为活跃的样本	Tool/Android.TheftProtector.a[prv,exp]	该应用程序是一款防盗软件，运行后会隐藏图标，监听并拦截指定号码的短信，发送短信和拨打电话至指定号码。若非用户主动安装，建议卸载。（威胁等级中）
		G-Ware/Android.dpatriot.a[rog,sys]	该应用程序运行会在手机存储路径下循环创建大量无用文件夹、文件，占用系统空间、系统资源，可能造成用户手机卡顿，影响用户的正常使用，建议不要使用。(威胁等级低）
		Tool/Android.AppleRobotSMS.a[prv]	该应用程序是一款苹果手机抢购工具的移动端，会有上传短信和自动发送短信等行为，可能会造成隐私泄露，请谨慎使用。（威胁等级低）
		RiskWare/Android.FDSync.a[prv,bkd]	该应用程序为 HTC 内置应用，留有后门，可能会上传用户短信、联系人等信息，存在一定风险，请谨慎使用。（威胁等级中）
		Trojan/Android.Fridayspy.a[prv,rmt]	该应用程序伪装系统应用，运行后会隐藏图标，接收远程指令开关 WIFI 和蓝牙，上传用户通讯录、通话记录和手机固件信息，造成用户隐私泄露，请立即卸载。(威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 内核信息泄漏漏洞（CVE-2019-0536）	当 Windows 内核不正确地处理内存中的对象时会触发该漏洞。成功利用此漏洞的攻击者可以获取内核信息，从而进一步入侵用户系统。已经过身份验证的攻击者可以通过运行经特殊设计的应用程序来利用此漏洞。（威胁等级高）
	较为活跃样本	Trojan/Win32.Badur	此威胁是一种木马类程序。该家族通过向用户系统中下载、安装大量应用程序获利，如百度卫士、YYMusic、知乎客户端等。用户系统会因安装大量应用程序而导致运行变慢，CPU、内存及网络资源等被大量占用。（威胁等级中）
		Trojan[Dropper]/Win32.Daws	此威胁是一种具有捆绑行为的木马类程序。该家族木马感染用户系统后，会自动释放出其它恶意程序并运行，释放的程序大多为盗号类木马程序。（威胁等级中）
		Trojan[PSW]/Win32.Tepfer	此威胁是一种盗号类木马程序。该家族样本运行后会盗取被感染计算机上的用户账户信息（用户名、密码等）。该家族能通过垃圾邮件、可疑链接、恶意网站等途径传播。该家族可以修改计算机的系统设置，更改或删除重要文件，捆绑间谍软件、恶意软件及广告件等，使系统性能下降。（威胁等级中）
		Trojan[Spy]/Win32.Zbot	此威胁是一种能够进行远程控制、组建僵尸网络、窃取用户信息的间谍类木马程序。该家族会窃取被感染电脑的重要信息，并生成工具包。该工具包允许黑客获得更高权限来远程控制电脑。（威胁等级高）

数据隐私：如何不辜负消费者信任

Jessica Davis / 文 安天技术公益翻译组 / 译

如果你希望消费者忠诚于你的公司或品牌，就应该保护和尊重他们的数据。

大概一两年前，沃尔玛公司名下山姆会员店（Sam's Club）为消费者提供了一款名为“扫描即得”（Scan and Go）的新应用。这些大型连锁店在店内布置了不少折叠桌椅，店铺代表坐在桌台后，向消费者介绍如何使用该应用并发放用户手册。

使用该应用的步骤是：下载应用，在手机上打开应用，使用会员 ID 登录；挑选完商品后，使用该应用扫描商品的条形码。这样一来，消费者就可以通过该应用付款了，无需排队结账。支付成功后，该应用会生成一个二维码，这个二维码相当于传统意义上的购物发票。出口处的工作人员检查客户手机上的二维码，就可以放行了。这种购物方式简单又快捷。

我近几年一直在研究大数据和分析，在该应用发布时，我并未注册。虽然我欣赏这种便利，但是我在犹豫：如果注册这款应用，我会向山姆店透露多少个人数据呢？（不过，我是山姆店的会员，经常使用会员卡购物，他们可能早已拥有了我的所有数据。）最近有一次，我比较赶时间，就下载这款应用尝试了一下。我不得不承认，它确实很方便。

“我们曾经开玩笑说，一杯免费啤酒就能赢得我们的个人数据。”Gartner 副总裁兼分析师罗伯特·赫图（Robert Hetu）说，“有时候让你提供数据真的不难。”

消费者已经习惯于提供他们的数据了。我们下载的每个应用都会请求权限，例如：访问联系人列表、访问手机和媒体、访问你的地理位置等等。各个网站和广告网络

也会跟踪我们的浏览记录。我们需要担心的不是国家安全局（NSA）的监视，而是日常光顾的公司的监视。但是现在，消费者对收集其数据的公司的态度正在发生变化。

“消费者有一种新的恐惧。”赫图说。很大一部分原因在于，Facebook 多次违背消费者信任，允许合作伙伴收集其用户的数据。此外，我们几乎每天都会看到这样的头条新闻：越来越多的公司未对消费者数据尽到保护之责，有的公司甚至在出售消费者的数据。例如，移动运营商出售用户的位置数据。

赫图表示，“信任”是公司与消费者的关系赖以存在的基础，因此违背消费者的信任不是一个好主意。如果公司想要消费者忠诚，就需要创建与客户之间的信任关系。

“所谓信任是指，消费者相信山姆会员店不会以入侵性的方式使用其数据。”赫图说，“而山姆会员店也不会试图窥探消费者在家里都使用哪些应用。”

一旦公司违背了消费者的信任，消费者就会删除公司的应用或停止光顾该公司。如果公司大规模违背客户信任，那么其声誉就会遭到严重的损害，导致其他的消费者也不信任该公司，不会向其提供自己的数据。

作为消费者，我们经常使用各种各样的设备——从电子门锁到数字助理，再到跟踪我们走了几步、所在位置和心跳频率的智能手表。这为消费者的数字安全带来了更大的风险，公司任何不负责任的举动都会让事情发展到令人毛骨悚然的程度。如果我们将数据和信任交给公司，那我们就应该得到保护。

赫图表示，Gartner 建议各公司，即使只在美国运营，也要遵守欧盟的《通用数据保护条例》（GDPR），将其作为保护消费者隐私的参考框架。他说，在美国，消费者的数据隐私不受联邦政府监管，而是由 50 个州各自监管。

当然，公司可以创建 50 个不同的隐私计划。或者，公司可以采用最严格的隐私计划，以确保以消费者希望的方式来处理其数据。如果是这样，操作起来想必会更麻烦。因此，Gartner 建议公司遵守 GDPR。

“遵守 GDPR 是创建客户信任的好办法。”赫图说。

原文名称	Data Privacy: How to be Worthy of Consumer Trust
作者简介	Jessica Davis。Jessica Davis 是 Enterprise Apps 的资深编辑。
原文信息	2019 年 1 月 11 日发布于 Information Week 原文地址 https://www.informationweek.com/big-data/data-privacy-how-to-be-worthy-of-consumer-trust/a/d-id/1333626
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。