安天发布《WebCobra 挖矿木马样本分析报告》

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 WebCobra 的挖矿木马。该木马来自俄罗斯，它可以自动探测系统架构，来选择释放和安装不同的挖矿软件。

WebCobra 通过流氓 PUP 安装程序进行传播，其主要的植入程序是一个 Microsoft 安装器，用于检查运行环境。在 x86 系统上，它会将 Cryptonight 挖矿软件的代码注入到一个正在运行的进程中，并且启动进程监视器；在 x64 系统上，它会检查 GPU 配置，并从远程服务器下载和启动 Claymore’s Zcash 挖矿软件。木马程序启动后，还会采用一些反调试、反模拟和反沙箱技术，以及检测系统上正在运行的其他安全软件。WebCobra 通过将 ntdll.dll 和 user32.dll 文件载入内存中，修改里面 API 函数的前 8 个字节，来逃避安全软件的检测，并且使用一个死循环，不断检查所有已打开窗口的标题栏文本，来确定自己是否运行在一个专为恶意软件设计的隔离环境中。以上这些步骤可以使该恶意软件在系统中隐匿相当长的一段时间。

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 BD 静态分析鉴定器、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	f31285ae705ff60007bf48aefbc7ac75a3ea507c2e76b01ba5f478076fa5d1b3
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	70 KB
MD5	7F3FD916EC1155253B5C8BD54B3C9459
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.AGeneric
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=7F3FD916EC1155253B5C8BD54B3C9459

◆ 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	★★★

◆ 常见行为

查找窗口	★
疑似桌面控制	★

◆ 进程监控

PID	创建	命令行
472	target.exe	"c:\496d283af9a449fda55912732efb7023\share\target.exe"

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
472-1.dmp	8f2d2263d233ed5f5adc59b10369efd0	N/A	N/A

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 02 月 18 日 (总第 171 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

原创春联贺岁 再踏新征程

用原创对联的方式迎接新春佳节，是安天人自创业以来一直坚持的传统。趁新春喜气还未消散，小编在此奉上安天 2019 己亥猪年的贺岁春联！

上联：协同联动 猎杀威胁 一颗恒心打造实战态感

下联：能力导向 治理先行 百战铁流重越漫道雄关

横批：再上征程

同时，安天向使用安天产品与服务的客户、向长期支持我们的专家领导、向共同与威胁战斗的业内同仁以及一直以来关注安天的朋友们送上最诚挚的祝福！

祝大家在新的一年中时时顺心、事事如意，愿我们为之奋斗的网络安全事业再攀高峰！

新年新起点，新春新气象。安天将继续勇往直前，朝着春联中所期望的目标不断前行，打造面向实战化运行的战术型态势感知，筑牢网络安全防线，守卫网络空间安全的星辰与大海！

更多历年安天原创春联请扫描二维码：

Microsoft 建议用户停止使用传统 IE 浏览器

微软网络安全专家建议用户停止使用传统的 IE 浏览器，希望 IE 用户转向使用现代的 Edge 浏览器。微软在 2015 年停止了对 IE 浏览器的支持。研究人员表示 IE 是兼容性解决方案，不支持新的网络标准，虽然许多网站都能正常运行，但大多数开发者都没有针对 IE 测试网站。而使用现代的 Edge 浏览器，用户会得到更好的安全保护。

（来源：http://www.ehackingnews.com/2019/02/microsoft-advises-its-users-to-stop.html）

谷歌商店中出现首个 Clipper 恶意软件

研究人员于 2019 年 2 月在 Android 应用商店 Google Play 上发现了恶意剪辑器 Clipper，其冒充名为 MetaMask 的合法服务，主要目的为窃取受害者的凭据和私钥，以控制受害者的以太坊资金。在线加密货币钱包的地址由长字符串组成，用户倾向于使用剪贴板复制和粘贴地址，而不是打字。该 Clipper 的恶意软件正利用了这一点。通过拦截剪贴板的内容，替换为想要破坏的内容。在加密货币交易的情况下，受影响的用户最终可能将复制的钱包地址静默切换到攻击者的地址。目前谷歌安全团队已从商店中删除了该应用。

（来源：https://www.welivesecurity.com/2019/02/08/first-clipper-malware-google-play/）

研究人员发现利用 EXE 文件攻击 Mac 新方式

研究人员发现 Windows 平台上运行的 EXE 文件在 Mac 平台上运行的样本。EXE 文件投送的恶意载荷覆盖了 Mac 的内置保护机制，如 Gatekeeper，因该例程只检查 Mac 文件，所以绕过了代码签名检查和验证。该样本是 Mac 和 Windows 的流行防火墙应用程序的安装程序 Little Snitch，其捆绑了 .EXE 文件，执行后窃取系统和应用程序信息，并下载一个针对 Mac 的广告程序。目前没有看到特定的攻击模式，但英国、澳大利亚、亚美尼亚、卢森堡、南非和美国的感染率较高。研究人员表示在其它平台上运行恶意 EXE 文件可能会对非 Windows 系统产生更大的影响。

（来源：https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac-downloads-info-stealer-and-adware/）

每周安全事件

类 型	内 容
中文标题	16 家网站近 6.2 亿用户信息被挂暗网出售
英文标题	620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts
作者及单位	Chris Williams
内容概述	近日，一个名为 Dream Market 的暗网市场上挂出了 6.2 亿用户信息，交易通过比特币转账进行，打包售价不高于 2 万美元，卖家宣称这些数据来自 16 个被攻击的网站，包括 Dubsmash、MyFitnessPal、MyHeritage 等，数据包括账户持有人姓名、电子邮件地址和密码，密码经过哈希处理或单向加密，因此必须先破解才能使用。根据来源网站的不同，某些数据还包含位置、个人详细信息和社交媒体身份验证信息等内容。
链接地址	https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

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

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.Fbsba.a[exp] 2019-02-10	该应用程序伪装系统应用，安装无图标，运行后会诱导用户激活设备管理器，私自下载并动态加载未知文件，造成用户流量资费损耗，可能会私自提权、窃取用户隐私，请卸载。（威胁等级高）
		Trojan/Android.phoneMonitor.b[prv,rmt,spy] 2019-02-11	该应用程序包含风险代码，运行后窃取用户短信、联系人、通话记录、通话录音等信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Downloader.fb[rog,exp] 2019-02-12	该应用程序运行后会配置代理连接，私自联网下载指定文件，用于加载未知子包。造成用户资费损耗，建议卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.fakewechat.n[rog]	该应用程序伪装微信，包含风险代码，运行后隐藏图标，后台加载未知应用，模拟点击自动安装，并私自启动。存在较大的安全隐患，建议立即卸载。（威胁等级中）
		Trojan/Android.BankerSpy.m[prv,rmt]	该应用程序包含恶意代码，运行后窃取用户短信、联系人、银行凭证信息，监听通话，造成用户隐私泄露以及财产损失，建议卸载。（威胁等级中）
		Trojan/Android.SmsSend.pn[exp,rog]	该应用程序伪装成 QQ 相关工具，运行后会诱导用户输入 QQ 号码，并通过短信转发，造成用户的隐私泄露，同时发送多条特定短信至指定号码，还会造成用户的资费消耗，建议卸载。（威胁等级高）
		RiskWare/Android.QQspy.ee[prv,exp]	该应用程序为下载安卓源码的应用，运行后会让用户注册账号登陆，注册时让用户填写 QQ 账号，上传到云端服务器，诱导用户加群。存在一定风险，建议卸载。（威胁等级中）
		Trojan/Android.cloudsms.a[prv,rmt,exp]	该应用程序包含恶意代码，运行后后台可监听用户短信，接收短信远程控制指令，窃取用户短信、联系人、通话记录、手机文件、手机 SIM 和固件信息，锁定用户手机，启动其他应用，并将用户信息通过短信上传。造成用户隐私泄露，影响用户手机正常使用，建议卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office 安全功能绕过漏洞（CVE-2019-0540）	当 Microsoft Office 不验证 URL 时，会存在安全功能绕过漏洞。攻击者通过设计一个特殊构造的文件并诱使用户将其打开，进而获取用户计算机中存储的数据。（威胁等级高）
	较为活跃样本	Trojan/Win32.Hijacker	此威胁是一种木马类程序。该家族样本运行后安装浏览器扩展，可以改变用户浏览器设置并推送广告，有一定威胁。（威胁等级低）
		RiskWare[WebToolbar]/Win32.MutiBar	此威胁是一种可以安装浏览器扩展的风险软件家族。该家族使用特殊的安装程序，采用各种方法来获取权限，从而安装其它软件组件。（威胁等级低）
		Trojan[Clicker]/HTML.Agent	此威胁是一种由 HTML 语言编写的可以实施自动点击功能的木马家族。该家族并没有统一的行为与功能，而是像一个木马类程序集合一样，将大量以基因片段定性的恶意代码归类。（威胁等级中）
		GrayWare[AdWare]/Win64.MultiPlug	此威胁是一种具有广告件行为的灰色软件家族。该家族的样本在运行后会在浏览器、桌面弹窗或通知中心显示无法关闭的广告。（威胁等级低）
		Trojan[Backdoor]/Linux.Gafgyt	此威胁是一种 Linux 平台上的具有窃密行为的后门家族。该样本运行后会在 Linux 上开启一个后门并允许远程控制端在计算机上执行任意操作，并且会收集机器上的信息上传给远程控制端。（威胁等级中）

三项基本安全实践保护 DNS 免受攻击

Kris Beevers / 文 安天技术公益翻译组 / 译

基本的、分层的 DNS 安全方法可以大大降低 DNS 和 BGP 相关攻击的可能性。以下是各机构应实施的三项基本预防措施。

上周，火眼公司发布了一份研究报告，分析了一项全球性的域名系统（DNS）劫持攻击，该攻击被认为是两年前开始的大规模间谍活动的一部分。该报告称，黑客通过其恶意服务器重定向公司的网络流量，记录公司凭证以供未来攻击之用。考虑到目标机构（主要是电信、互联网基础设施、政府和商业实体，大部分是国家攻击者感兴趣的目标）的性质，这一点尤为严重。

尽管该攻击活动的范围很广泛，但是其使用的方法并不独特或复杂。与网络犯罪分子青睐的其他策略一样，这些攻击是低成本且易于执行的，以未采取基本安全措施的机构为目标。

在 DNS 劫持攻击中，攻击者接管属于 DNS 提供商和注册商的帐户，操纵受害者的 DNS 记录，重定向传入的流量。这导致的结果是，进行 DNS 查询（尝试访问网站或应用程序）的最终用户设备获得虚假信息，使用户访问伪装成合法网站的虚假网站。

DNS 劫持和其他中间人攻击（如 DNS 缓存投毒和边界网关协议 [BGP] 劫持）并不总是明显的。它们可能在很长的时间内都未被发现，导致公司的数据被盗和直接经济损失。在 2018 年末，当局关闭了一项持续多年的广告诈骗项目，该项目通过 BGP 劫持攻击了超过一百万个 IP 地址；此外，该项目还采用了其他策略，获取了近 3000 万美元的收益。不过，该项目非常复杂和不寻常。在大多数情况下，此类攻击难以大规模执行，因此往往是针对性的。通常，某些网站是为特定目的（例如经济收益）而注册的。去年，加密货币的投资者发现了下述严酷的现实：攻击者在 BGP 劫持活动中标记了几个网站，利用这些网站窃取凭证；然后，他们利用这些凭证登录用户帐户，进行挖矿。

幸运的是，基本的、分层的 DNS 安全方法可以大大降低 DNS 和 BGP 相关攻击的可能性。以下是各机构应实施的三项基本预防措施。

对 DNS 提供商和注册商帐户应用多因子身份验证

各机构应实施严格的访问控制，以限制负责修改 DNS 设置的合法用户的访问权限。如果公司有多个 DNS 管理员，则可以根据其角色为其分配不同的职能，只允许他们访问完成工作所需的区域和记录。实施多因子身份验证和单点登录来加强访问控制非常重要。如果公司使用脚本或 API 来更新 DNS，则应使用强身份验证密钥，并将密钥使用设置为“仅允许有效源使用”（即 IP 白名单）。

最后，各机构与其域名注册商交互时应采用基本的安全实践，并及时更新授权联系人列表。这样一来，公司就能保持对其域名的控制，避免错过来自注册商的到期通知。

监控 DNS 活动日志以快速发现问题

对公司来说，跟踪每个 DNS 响应可能有些困难。不过，通过监控 DNS 活动和 IDS 日志，公司可以更轻松地观察 DNS 配置变化和流量模式变化，而这些变化可以揭示关键攻击信标。例如，DNS 记录配置的意外和计划外更改，或流量的突然变化，表示可能出现了恶意 DNS 活动。

启用 DNSSEC 和区域签名

在用户的一系列查询中，DNS 服务器会进行回复；而域名系统安全扩展（DNSSEC）提供递归 DNS 解析器，以检查授权 DNS 服务器回复的信息的真实性。许多企业处理财务、医疗或个人数据，因此他们有责任保护客户免受这种形式的攻击。DNSSEC 通过对 DNS 的每个区域进行数字签名和验证，来保护 DNS 信息的完整性。

DNS 是一项重要的技术，它将 IT 基础设施、应用程序和在线服务等（从服务器到用户的所有内容）连接起来，这使其成为网络犯罪分子青睐的目标。随着全球企业更积极地转向互联的数字化活动，这种攻击向量将会越来越重要。公司应快速采取行动，实施和维护上述基本的预防措施，这对于防止攻击以及保护公司和客户数据至关重要。

原文名称	3 Basic Security Practices Will Protect Your DNS From Compromise
作者简介	Kris Beevers。Kris Beevers 是 NS1 公司的首席执行官。
原文信息	2019 年 1 月 23 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/network-security/3-basic-security-practices-will-protect-your-dns-compromise/1239498345
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。