安天发布《EVILNUM 木马家族样本分析报告》

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个名为 EVILNUM 的木马家族。这类木马通过诱惑用户点击 lnk 文件来触发恶意程序的执行。目前，该家族木马主要用来攻击金融技术类行业的公司。

EVILNUM 家族的恶意软件目前存在两个版本，一种使用 JavaScript 编写，一种使用 .Net 编写。尽管编程语言不同，但是它们的核心功能非常相似，.Net 版本更像是对 JS 版本的重写。该家族木马获取 C2 服务器的方式十分特别，它首先会访问指定的网站页面（如公共论坛、GitHub 等），再解析网页内容，提取指定位置的数字，将数字除以 666，最后将结果转化成十六进制，就得到了 C2 服务器的 IP 地址。EVILNUM 的每个版本在功能上都有所差异，包括但不限于以下功能：设置自身持久化、CMD 任意命令执行、下载其他文件等。.Net 相比于 JS 版本，增加了窃取本地 Cookie 信息和屏幕截图的功能。EVILNUM 只是在攻击的第一阶段使用的木马，它负责将被感染主机的信息发送给攻击者，由攻击者决定是否在该机器上继续安装其他的恶意程序，进行下一步攻击。

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、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、动态（Win7 x86）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	bee6c5a506d6fb2cc129443c74b7676fbb9a79b53b92b2cac4c7fb8209592714
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	21 KB
MD5	8147EAD27C482AC705318B275A9B6830
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Occamy
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=8147EAD27C482AC705318B275A9B6830

◆ 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

◆ 常见行为

行为描述	危险等级
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）	★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.165	54483	192.168.122.1	53
192.168.122.165	60609	192.168.122.1	53
192.168.122.165	54738	192.168.122.1	53
192.168.122.1	53	192.168.122.165	54483
192.168.122.1	53	192.168.122.165	60609
192.168.122.1	53	192.168.122.165	54738
192.168.122.165	63213	224.0.0.252	5355
192.168.122.165	57643	224.0.0.252	5355
192.168.122.165	62288	224.0.0.252	5355
192.168.122.165	64527	224.0.0.252	5355
192.168.122.165	138	192.168.122.255	138
.....	.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 04 月 22 日 (总第 180 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天获中国互联网网络安全威胁治理联盟 2018 年度特别贡献奖

近日，安天荣获中国互联网网络安全威胁治理联盟（CCTGA）颁发的 2018 年度特别贡献奖，表彰了安天在网络安全威胁处置工作中做出的贡献。

中国互联网网络安全威胁治理联盟（以下简称“联盟”）由国家互联网应急中心（CNCERT）联合中国互联网协会网络与信息安全工作委员会共同发起成立，为行业提供了公共沟通交流的平台，加强了互联网网络安全威胁信息共享、相互协作，建立了互联网网络安全威胁治理的长效机制，有效净化了网络安全环境。安天是联盟的首批成员单位之一，并多次荣获表彰。

安天长期在威胁检测领域深耕细作，是网络安全威胁应急响应体系中的重要企业节点，在“方程式”、“白象”、“海莲花”、“魔窟”、“绿斑”等重大网络安全威胁事件中提供了先发预警、深度解析或具体的解决方案，多次在重大安全事件中发挥关键作用，技术实力得到了行业管理机构、客户和伙伴的认可。

作为引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，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。

安全研究人员发现针对越南政府的 APT 攻击

ElevenPaths 研究人员检测到恶意软件发送到属于越南政府域名的电子邮件账户。攻击初始的电子邮件日期为 2019 年 3 月 13 日，附件 ZIP 文件包含模拟 word 文档图标的 .lnk 链接文件，指向的目标包含使用 MS-DOS 混淆代码，实际为一个 base64 编码的 PowerShell，运行后将创建并运行另一个 PowerShell 文件，该文件将仅驻留在内存中，并且再次运行 WScript Shell。该脚本将再次创建三个文件：显示给用户的诱饵 doc 文档；安装 .NET 汇编文件的合法工具，用于绕过 SmartSCreen 和 AppLocker 保护；在 .NET 中创建 DLL 文件，其包含实际恶意载荷。目前研究人员还未确定该活动归因。

（原文链接：https://blog.en.elevenpaths.com/2019/04/new-research-docless-vietnam-apt.html）

跨平台 rootkit Scranos 间谍软件正积极传播

基于签名 rootkit 的恶意软件 Scranos 于 2018 年年底首次被发现，近日 Bitdefender 研究人员发现 Scranos 的幕后开发者正在不断对旧组件进行改进，并在全球范围内积极传播。Scranos 通过伪装成破解软件或合法应用程序传播，释放器也充当信息窃取器，使用恶意 dll，从常见的浏览器和 Facebook、Amazon 等窃取 cookie、登录凭证和支付信息，发送回 C&C。然后释放器安装 rootkit，通过注册一个关机回调来实现持久性。rootkit 在 svchost.exe 中注入一个下载器，下载器向 C&C 发送关于系统的信息，并接收其它下载链接。目前多数感染发生在印度、罗马尼亚、巴西、法国、意大利和印度尼西亚。

（原文链接：https://labs.bitdefender.com/2019/04/inside-scranos-a-cross-platform-rootkit-enabled-spyware-operation/）

广告活动使用 Chrome 漏洞劫持 iOS 用户会话

Confiant 发现一项大规模的恶意广告活动正在利用 iOS 版本 Chrome 浏览器中的漏洞，针对来自美国和多个欧盟国家的 iPhone 和 iPad 用户，将其重定向到广告软件、诈骗或其它恶意网站。研究人员将该活动归咎名为 eGobbler 的攻击者。该漏洞允许隐藏在在线广告中的恶意代码打破沙箱化 iframe 并将用户重定向到另一个网站，或在合法网站上显示入侵的弹出窗口。该漏洞仅影响 iOS 版本的 Chrome，Confiant 已向谷歌报告该漏洞。

（原文链接：https://blog.confiant.com/massive-egobbler-malvertising-campaign-leverages-chrome-vulnerability-to-target-ios-users-a534b95a037f）

每周安全事件

类 型	内 容
中文标题	研究人员披露利用新 0day 漏洞攻击细节
英文标题	New zero-day vulnerability CVE-2019-0859 in win32k.sys
作者及单位	Vasily Berdnikov, Boris Larin, Anton Ivanov
内容概述	研究人员在 2019 年 3 月发现尝试利用 win32k.sys 中 0day 漏洞的攻击。该漏洞被分配为 CVE-2019-0859，是 CreateWindowEx 函数中提供的 Use-After-Free 漏洞。 研究人员发现的攻击是针对 64 位版本的 Windows，使用 HMValidateHandle 技术利用该漏洞绕过 ASLR。然后使用 Base64 编码命令执行 PowerShell，该命令的主要目的是从远程下载第二阶段 PowerShell 脚本，接着执行第三阶段 PowerShell 脚本。第三个脚本依次执行解包 shellcode、分配可执行内存、将 shellcode 复制到已分配的内存、调用 CreateThread 来执行 shellcode。shellcode 的主要目的是制作一个简单的 HTTP 反向 shell，有助于攻击者完全控制受害者的系统。 目前该漏洞已在 3 月份的补丁更新中得到修复。
链接地址	https://securelist.com/new-win32k-zero-day-cve-2019-0859/90435/

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.Exodus.a[prv,spy] 2019-04-13	该应用程序是间谍软件，运行激活设备管理器，监听用户短信，窃取用户短信、联系人、通话记录、地理位置、手机文件，私自下载恶意文件，录音，拍照，并将用户隐私上传至服务器。会造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.Exodus.b[prv,rmt,spy] 2019-04-14	该应用程序是间谍软件，运行会联网上传固件信息，下载文件，监听短信、上传短信，连接到远程服务器获取指令并上传短信、通讯录、通讯记录、照片、录像、GPS 位置信息、app 列表信息、WhatsApp 和 Facebook 信息等一系列隐私信息。会造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.FakeBank.w[prv] 2019-04-15	该应用程序伪装为银行应用，针对土耳其语用户，通过虚假页面窃取用户银行信息，通过更新下载未知应用，部分样本存在窃取用户短信的行为，造成用户隐私泄露和财产损失，建议卸载。（威胁等级中）
	较为活跃的样本	RiskWare/Android.jvptvr.a[exp,rog]	该应用程序是一个广告刷量工具，运行后通过设置百度广告关键词进行刷量操作，存在一定风险，请用户不要使用。（威胁等级中）
		G-Ware/Android.StealMoneyGame.dy[pay,rog]	该应用程序是游戏应用，付费信息不明显，以领取道具名义加载弹窗，诱导用户点击付费，容易造成用户资费损失，建议卸载。（威胁等级低）
		RiskWare/Android.PJbocai.j[rog]	该应用是一款线上赌博游戏，可以通过微信等方式进行充值，可能给用户的财产带来较大风险，且难以保障财产权益，建议谨慎使用。（威胁等级低）
		RiskWare/Android.liuhebocai.a[rog]	该应用程序为博彩应用，点击广告会访问博彩网站，其内容可能给用户的财产带来较大风险，且难以保障财产权益，请谨慎使用。（威胁等级低）
		Trojan/Android.Telugu.a[prv]	该应用程序内嵌恶意代码，后台私自录音，上传通话录音文件，还会上传邮件账户信息，隐藏图标，会造成用户隐私泄露，请卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Jet 数据库引擎远程代码执行漏洞（CVE-2019-0846）	当 Windows Jet 数据库引擎不正确地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受害者系统上执行任意代码。（威胁等级高）
	较为活跃样本	Trojan/Win32.VBKryjetor	此威胁是一种有下载行为的木马家族。该家族的样本通过捆绑在其他免费软件上的方式感染用户的计算机。该家族的样本在执行后会试图连接特定的 URL 以下载其他恶意软件。（威胁等级中）
		Trojan[Ransom]/Win32.Crypmodadv	此威胁是一种勒索软件家族。该家族的样本在运行后，会加密系统上多种文件格式的文件，并将文件的扩展名更改为 .remind。在加密后，该样本会在全部的文件夹下各放置一封 HTML 格式的勒索信说明情况。（威胁等级高）
		Trojan[Downloader]/Win32.RtkDL	此威胁是一种具有下载行为的木马家族。该家族的样本在执行后会伪造成杀毒软件，提示“系统具有高风险”，建议安装一些由此样本指定的收费软件。无论是否购买，系统都会无法连接到网络，持续弹出窗口，运行缓慢并偶尔蓝屏。（威胁等级中）
		Trojan/Win32.GoogUpdate	此威胁是一种具有窃密行为的木马家族。该家族的样本在运行后会试图更新自身并将与机器相关的信息发送到特定的 URL。该样本还会记录屏幕截图、击键组合、进程列表等。（威胁等级高）
		GrayWare[AdWare]/OSX.Xamloader	此威胁是一种具有广告行为的灰色软件家族。该家族只能运行于 Mac OS X 平台上。在运行后会在后台下载广告内容并弹出消息框展示广告。（威胁等级低）

应对 AI 恶意软件的来临

Gunter Ollmann/ 文 安天技术公益翻译组 / 译

作为“首席信息安全官”（CISO），病毒和恶意软件一直盘踞在让我辗转难眠的 Top 10 威胁中，但是其威胁已持续下降了十年。不幸的是，“魔窟”（WannaCry）、NotPetya 等自传播勒索软件再一次推动了恶意软件的发展，凸显了互联系统以及联网设备的爆炸性增长所带来的风险。

这些自主（尚未由 AI 驱动）威胁造成了严重的破坏，促使 CISO 采取防御措施来对抗它们。

目前来说，诸如 HAL-9000 的智能恶意软件仍然是科幻电影中的桥段（译者注：HAL-9000 智能电脑出自科幻电影《2001：星际漫游》），“超级精英黑客组织将各类恶意软件封装到电子邮件大小的 AI 包中”同样也仅存在于科幻作品中。然而，在接下来的两到三年中，攻击者将会在六种经济可行的 AI 技术中注入恶意软件，以便提高其收集高价值数据的效率、攻击特定用户并绕过检测技术。接下来，我们将介绍这六种 AI 技术。

消除对 C & C 通信的过度依赖

通过智能自动化和基本逻辑处理技术，攻击者可以在受感染的网络中寻找目标，非重复、选择性地攻击预定目标，并在识别和收集数据时执行数据推送——一次性地推送到其控制的远程服务器，从而避免了对 C&C 的过度依赖。这种基于 AI 的技术不仅会规避黑名单技术，还会逃逸沙箱和行为分析检测。

使用数据标记 / 分类功能动态识别和捕获最有价值的数据

企业使用数据分类器和机器学习（ML）技术来标记和保护有价值的数据资产。但是，

攻击者也可以利用相同的技术来查找用户和系统接触的高价值业务数据，并减小数据文件以便进行隐蔽渗漏。这样一来，攻击者就能规避流量异常检测技术，以及常见的欺骗和蜜罐解决方案了。

使用认知和会话 AI 监控本地主机电子邮件和聊天流量，并动态模拟用户。

恶意软件的 AI 组件可以将新的会话内容插入电子邮件线程和聊天内容中，以便对员工执行社会工程攻击，诱使其泄露机密或访问恶意内容。大多数电子邮件和聊天安全解决方案都专注于入站和出站内容，很少检查内部通信。此外，会话 AI 正在迅速发展，足以对 IT 服务和技术支持人员执行社会工程攻击，使其泄露机密或进行配置临时更改。

使用语音 - 文本转换 AI 来捕获环境中的机密

通过麦克风，AI 组件可以将受感染设备附近的所有语音转换为文本。此外，在某些环境中，AI 组件可以成功捕获附近系统的击键并推断出具体的按键。通过这种方法，攻击者可以选择想要捕获的机密，将收集的数据量控制在最小程度，降低触发基于网络的检测技术的几率。

使用嵌入式认知 AI 选择性地触发恶意载荷

认知 AI 系统不仅可以识别特定的人脸或声音，还可以确定用户的种族、性别和年龄，因此恶意软件作者可以选择非常具体的目标。例如，此类恶意软件可能仅针对公司的“首席财务官”（CFO），或者仅针对 9-13 岁的女童。由于触发机制嵌入在复杂的 AI 组件中，因此自动或手动调查几乎无法确定触发恶意行为的标准。

捕获用户的行为特征

AI 学习系统可以观察用户打字、移动鼠标、使用词汇、出现拼写错误等的独特节奏和特征，并创建用户的“行为特征库”。然后，攻击者可以利用该“行为特征库”来绕过部署的高级行为监控系统。

目前，这些 AI 功能已经在售。每一项 AI 功能（共同或单独地）都可以作为代码嵌入恶意载荷中。

由于深层神经网络、认知 AI 和训练有素的机器语言分类器的解密非常复杂，恶意行为的触发机制可能会被深度隐藏，无法通过逆向工程来解密。

防御这些攻击的基本措施在于，确保企业的所有部分都是可见的并持续进行监控。此外，CISO 需要投资于具备 AI 检测和响应功能，能够快速、自动发现威胁的工具。

随着恶意软件作者利用 AI 进行网络犯罪，安全行业必须推出新一代的检测和防御技术，以应对即将到来的威胁。可以实施防御性 AI 的领域包括威胁情报挖掘、自主响应等，我们将在后面的文章中详细介绍。

原文名称	Get Ready for the First Wave of AI Malware
作者简介	Gunter Ollmann。Gunter Ollmann 是微软云和人工智能安全部门的首席安全官。
原文信息	2019 年 4 月 9 日发布于 Security Week 原文地址 https://www.securityweek.com/get-ready-first-wave-ai-malware
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。