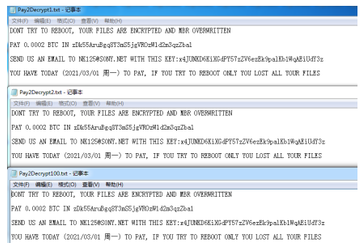
安天智甲有效防护 BleachGap 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个 BleachGap 勒索软件。最早于 2021 年 2 月被发现，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。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止 BleachGap 勒索软件的加密行为。

BleachGap 勒索软件样本运行后，终止 IE、firefox 等指定进程，停用任务管理器，复制自身到 %AppData%/ Microsoft/ Windows/Start Menu/Programs/Startup/ 目录，并创建计划任务实现自启动，删除系统卷影副本，以防止恢复加密文件。创建多个线程，在短时间内完成对计算机上相关文件的加密，在被加密文件的文件名后追加以“.lck”命名的后缀。加密完成后，在桌面创建 100 个名为“Pay2Decrypt(1-100).txt”的勒索信，勒索信具体内容包含了勒索说明、勒索金额、比特币钱包地址、KEY 以及联系邮箱。

BleachGap 勒索软件采用“AES-256”加密对称加密算法加密文件，获取密钥后可通过命令“aescrypt.exe -d -p KEY -o 原文件名 加密文件名”进行解密，aescrypt.exe 文件位置可在 %Temp% 搜索。



▲BleachGap 勒索信

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给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密码；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。目前，安天追影产品已经实现了对该类勒索软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

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，下为其自动生成的分析报告：

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 、聚类分析鉴定器、反病毒引擎鉴定器、动态（Win XP）鉴定器、动态（Win7 x86）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、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、动态行为鉴定器、关联分析鉴定器、信标检测鉴定器将文件判定为木马程序。

◆概要信息

文件名	9e4f1334d3712298cb3d18e38cd954c893c890d09ad457683c8d7956a9bdb635 (1)
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1007 KB
MD5	46A1769D81D7DCDA455F0F05B9B29648
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.BleachGap
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=46A1769D81D7DCDA455F0F05B9B29648

◆危险行为对比

行为描述	危险等级	动态 (WinXP)	动态 (Win7 x86)
检测虚拟机	★★★★★	√	√
删除全盘所有卷影副本	★★★★★	√	√
禁用任务管理器	★★★	√	√
修改文件权限	★★★	√	√

◆常见行为对比

行为描述	危险等级	动态 (WinXP)	动态 (Win7 x86)
资源释放	★★	√	√
读取自身	★★	√	√
自我复制	★★	√	√
创建挂起进程	★★	√	x
WMIC 调用执行	★★	√	√
检测自身是否被调试	★★	√	√
镜像劫持	★★	√	√
获取当前激活的窗口	★★	x	√
设置文件属性为隐藏	★★	x	√
隐藏执行 powershell	★★	x	√
疑似查找浏览器进程	★★	x	√
添加计划任务	★★	x	√
加载运行时 DLL	★	√	√
释放 PE 文件	★	√	√
获取驱动器类型	★	√	√
……	……	……	……

◆扫描二维码查看完整报告

安天周观察
安天对外开放资料平台 安天官方微信
主办：安天 2021 年 03 月 08 日 (总第 268 期) 试行 本期 4 版 扫描上方二维码查询安天所有对外开放资料

APP 广告乱象系列三——弹窗广告的关闭键岂是摆设？

安天移动安全在持续关注和披露当前移动应用中涉及的恶意广告行为的过程中发现，在商业利益的驱动下，不少正常的移动应用也存在携带和主动触发恶意广告行为的情况，且随着广告算法化和智能化的升级，使得这类行为本身更难以被检测和广谱发现。

应用通过监听系统广播的方式实现自启动，并设置定时器频繁执行后台广告弹窗，甚至延时执行后台广告弹窗等恶意广告行为问题依旧存在。在流量利益的驱使下，有些开发者试图通过各种技术手段进行对抗，玩起了猫鼠游戏，将骚扰用户的恶意广告行为掩藏在正常功能性弹窗的伪装之下，其本质仍然是恶意广告行为，严重破坏了用户的正常体验。本期分享的是：用户点击“关闭按钮”仍会二次外弹广告，严重骚扰用户的恶意广告行为。

以往，应用通过监听系统广播消息，或者拦截按键消息，在不涉及触发应用的功能性实现前提下，只触发广告弹窗行为是恶意广告应用中非常普遍的现象。近期，有些开发者企图通过技术手段“升级”这类恶意广告行为来进行对抗，主要问题如下：

·在未告知用户、未经用户同意，且无合理的使用场景的情况下，应用通过监听用户解锁动作推送正常的功能性广告，并为之后二次外弹广告埋下伏笔；

·推送正常功能性广告后，由功能性广告关闭按钮触发二次广告推送，违背用户意愿，强制推送广告，侵犯了用户的自主选择权，严重破坏了用户的正常体验；

·有些开发者恶意推送广告并强制用户观看，成为用户反映强烈的问题之一，剥夺了用户对广告说“不”的权利，也是对相关法律法规的挑战；

当前，无论是监管部门、手机厂商还是安全厂商都在持续关注移动恶意广告乱象问题。安天移动安全在检测分析中发现，弹窗广告的一大特点就是网民不能自主选择，只能被动接受，这等于强制向用户进行广告曝光，因此现在被普遍应用，甚至可以说是泛滥成灾。希望有关开发者正视问题，将选择权还给用户，不要让“关闭”键成为摆设。

作为网络健康生态助推者，安天移动安全愿和各方一道共同促进移动互联网环境持续向好，为开发者提供更加专业的产品安全辅导和配套服务，不断提升开发者安全运营水平，联合建立行业规范，助力网络安全新格局建设。

安天移动安全是安天科技集团旗下专注移动用户安全的科技公司。经过 10 年的技术积累，自主创新的安全引擎已成为国民级安全内核，为智能终端的用户生态实现全场景覆盖的移动应用安全治理，对导致用户权益受损的不良行为和黑灰产进行技术响应，并为开发者提供专业安全辅导和配套产品服务。

（原文连接：https://mp.weixin.qq.com/s/B1cFAzKYED_gHKtsLdL_oA）

扫描上方二维码阅读原文

谷歌发布更新修复了被积极利用的零日漏洞

谷歌在 2021 年 3 月 2 日发布的 Chrome 89.0.4389.72 版本中修复了一个零日漏洞，该版本针对 Windows、Mac 和 Linux 用户。谷歌将零日漏洞评为高度严重性，Microsoft 浏览器漏洞研究的 Alison Huffman 于 2021-02-11 报告了该安全漏洞。尽管 Google 表示已经知道有积极利用 CVE-2021-21166 攻击的报道，但该搜索巨头并未分享有关这些攻击背后的威胁行为者的任何信息

（原文链接：https://www.bleepingcomputer.com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-bug-this-year/）

攻击者可利用 WiFi Mouse 应用漏洞劫持台式电脑

无线鼠标实用程序缺少适当的身份验证，因此使 Windows 系统容易受到攻击。发现该漏洞的研究人员 Christopher Le Roux 表示，该移动应用程序称为 WiFi Mouse，它允许用户使用智能手机或平板电脑控制 PC 或 Mac 上的鼠标移动。该应用程序有一个未修复的漏洞，该漏洞允许共享相同 Wi-Fi 网络的使用者通过该软件开放的通信端口完全访问 Windows PC，可以使攻击者劫持台式计算机。

（原文链接：https://threatpost.com/unpatched-bug-in-wifi-mouse-opens-pcs-to-attack/164480/）

每周安全事件

类 型	内 容
中文标题	RTM 团伙攻击活动利用新的 Quoter 勒索软件
英文标题	RTM Cybergang Adds New Quoter Ransomware to Crime Spree
作者	Lindsey O'Donnell
内容概述	臭名昭著的 RTM 银行木马的幕后黑手是一个讲俄语的组织，这个组织现在正进行一个三重威胁攻击活动，除了众所周知的银行恶意软件，攻击者还利用了最近发现的一种名为 Quoter 的勒索软件家族，作为一种新的双重勒索网络攻击策略的一部分。卡巴斯基在本周发布的一份报告中称，此次三重威胁攻击从 2020 年 12 月开始进入“活跃阶段”，目前仍在进行中，已通过恶意电子邮件攻击了至少 10 家俄罗斯交通和金融部门的组织。
链接地址	https://threatpost.com/rtm-banking-trojan-quoter-ransomware/164447/

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	Apache Unomi 远程代码执行漏洞（CVE-2020-13942）	高	Apache Unomi 在 1.5.2 之前版本中存在远程代码执行漏洞，攻击者可以利用该漏洞发送符合语法的恶意表达式使 Unomi 服务器执行任意代码和系统命令。
	Siemens TIA Administrator 权限提升漏洞（CVE-2020-25238）	高	Siemens TIA Administrator 存在权限提升漏洞。攻击者可利用漏洞以系统权限执行代码。
	VMware vCenter Server 远程代码漏洞 （CVE-2021-21972）	高	VMware vCenter Server 存在远程代码漏洞，攻击者利用该漏洞可直接通过 443 端口构造恶意请求，执行任意代码，控制 vCenter。
较为活跃样本家族	Trojan/Win32.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	Trojan[Backdoor]/Win32.Tiny	中	此威胁是一种窃密类木马家族。该家族木马运行后连接远程服务器下载恶意代码并执行，可以窃取用户敏感信息。
	Trojan/Win32.Fsysna	中	此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。
	Trojan[Downloader]/Win32.Banload	中	此威胁是一种具有下载行为的木马类程序，样本运行后连接网络下载其他恶意代码并安装，有可能导致用户信息被窃取，有一定威胁。
	Trojan/Win32.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan[SMS]/Android.Opfake	中	此威胁是一种基于 Android 的恶意应用程序。该家族没有统一的行为与功能，一般会窃取用户短信、发送包含恶意 URL 的短信或进行其他与短信有关的恶意操作。

小型安全团队有效网络安全管理的十种策略

安天技术公益翻译组 / 译

Cynet 公司表示，小型安全团队面临的挑战与大型团队不同，因此其 IT 专家必须比大型企业的同行更具创造力并更加务实。

在过去的几年中，我们看到，各种规模的企业遭受的网络攻击不断增加。例如，企业电子邮件被泄露，端点受到持续威胁，勒索软件攻击不断增加等。与拥有庞大网络安全团队的大型企业不同，中小型企业（SEM）面临各种挑战，包括缺乏专用资源、设备管理不善、缺乏培训以及 IT 管理框架水平低等等。

在这种情况下，这些 SME 的首席信息安全官（CISO）努力进行调整，试图克服这些挑战。在最近的一项调查中，他们提出了十项建议，旨在帮助企业保持尽可能高的安全水平。

与高管沟通

安全团队应以每年一次的频率制定应对网络攻击的策略 / 计划，并在董事会会议上予以介绍。他们需要介绍新威胁的统计信息、趋势和概述，以及这些威胁带来的业务风险以及公司防御此类攻击的能力，而非具体的技术。此外，他们应在计划中设定预算和期望，并向董事会介绍可以做什么和不能做什么，以及相关的风险。

通过合规性来增加安全预算

与网络安全预算相比，合规预算“说什么就是什么”。合规性是指，企业的运营需要遵守相应的法规，这是一种强制性的要求。安全团队可以利用合规预算来增强安全环境，以实现合规性。他们可以通过“控制与法规矩阵”检查企业在合规性上的差距。这是一种前瞻性的方法，有助于企业轻松实现合规性，了解其在下一项法规出台时仍存在哪些差距。

考虑产品的端到端成本

从初始部署到安装后分析、告警和维护，新安全解决方案的成本涉及多个领域。在购买新的网络安全产品时，安全团队应了解除实际产品成本和安全范围、升级频率和要求、仪表板 /SIEM 监控告警、误报率等以外的相关投资。他们可以要求供应商提供试用期，以便更好地了解和评估这些参数。

整合安全平台

安全平台有很多层，每一层都会增加整体 IT 的复杂性。安全团队可以寻找整合了多种技术的产品。

最知名和 / 或最昂贵的产品不一定最好

安全团队应参考比较网站、阅读博客并与同事交谈，以借鉴他们在各种解决方案上的经验。此外，他们应了解这些解决方案在第三方评估和安全有效性方面的排名。

专注于特定告警

安全团队会根据告警进行操作。小型团队没有资源来跟踪每个告警，因此他们应设置策略来定义何时需要处理特定告警。他们应跟踪已经自动修复的告警，因为最初的威胁可能是大型攻击活动的一部分。

寻找不会阻碍运行的安全解决方案

如果安全策略阻碍了员工的运行速度，他们就会试图绕过这些策略。与其为公司的所有员工创建统一的策略，不如针对每个角色创建多种策略并确定如何克服挑战。

尽可能实现自动化

如果企业有诸多手动任务，可以通过实现这些任务的自动化来节省时间。安全团队可以采用新的自动化技术，以避免手动执行繁琐或重复性的工作。

不仅要看产品本身

安全团队应避开缺乏优质客户支持的产品或服务，以防解决方案半途而废。在了解新产品时，他们应询问供应商提供多少产品培训、是否有初始安装成本、是否有专门的客户成功经理、客户服务的质量如何、服务级协议，以及是否提供“托管检测和响应”（MDR）服务？

采用 SaaS 产品以节省成本、费用和资源

SaaS 解决方案能够减少部署和管理要求，节省维护资源和成本。许多 SaaS 产品有强大的处理能力，它们在云架构中会更加有效。安全团队应检查安全堆栈，确认哪些解决方案可以用 SaaS 解决方案替代，并在不牺牲安全的情况下受益于集中的管理、处理和运营成本。

Cynet 首席执行官艾尔·格鲁纳（Eyal Gruner）表示：“通过一些额外的研究、恰当的工具和支持服务，小型网络安全团队可以实现企业级安全，确保企业受到适当的保护。目前，技术、医疗、零售、金融服务和保险行业的 CISO 增加了安全投入，受益于此，这些小型团队的安全专家能够获得高水平的指导，以增强企业的安全态势。”

原文名称	10 strategies small security teams can use for effective cybersecurity management
原文信息	2021 年 03 月 03 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/03/03/strategies-small-security-teams/
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。