安天发布《Phobos 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Phobos 的勒索软件，Phobos 勒索软件最早在 2019 年初被发现，其传播方式主要为 RDP 暴力破解和钓鱼邮件。安天 CERT 分析人员通过关联分析发现 Phobos 勒索软件与 Dharma 勒索软件有许多相似之处，故怀疑这两款勒索软件的作者可能是同一个人。

勒索软件 Phobos 执行后，会弹出 UAC（用户账户控制）会话框，受害者一旦点击“是”按钮，Phobos 便会调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录和禁用防火墙。并追加后缀名“.acute”。Phobos 会将自身复制到 %AppData% 和 Startup 文件夹中，修改注册表项以达到开机自启动的目的。Phobos 还会创建 2 种不同类型的勒索信，一种格式为 .txt，另一种格式为 .hta。两种勒索信的命名均为 info，两种勒索信中包含联系邮箱地址、USER_ID、购买比特币支付赎金说明等。目前被加密的文件在得到密钥前暂时无法解密。

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，避免一切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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、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（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、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 BD 静态分析鉴定器、反病毒引擎鉴定器、动态行为鉴定器将文件判定为木马程序。

◆概要信息

文件名	a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	71 KB
MD5	E59FFEAF7ACB0C326E452FA30BB71A36
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Blocker
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=E59FFEAF7ACB0C326E452FA30BB71A36

◆运行环境

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
删除全盘所有卷影副本	★★★★
执行解释型脚本	★★★
在启动时禁用 Windows 错误恢复	★★★★
文件篡改	★★★★★
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
打开自身进程文件	★
获取计算机名	★
自我复制	★★
Run 自启动	★
创建挂起进程	★★
获取驱动器类型	★
获得计算机用户名	★
创建窗口	★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 08 月 05 日 (总第 194 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

中央网信办网络安全协调局副局长胡啸一行莅临安天参观调研

近日，中央网信办网络安全协调局副局长胡啸在黑龙江省委网信办副主任王希忠、国家互联网应急中心黑龙江分中心主任张光耀的陪同下莅临安天总部参观调研。

安天相关负责人介绍了安天的发展现状、核心技术布局以及基于叠加演进模型的能力导向建设模式指引规划设计，构建动态综合网络防御体系以应对高级网空威胁行为体体系化攻击的思路，展示了作为积极防御指控中枢的战术型态势感知平台的研发进展，交流了安天产品和解决方案在重要信息系统和关键信息基础设施的部署情况和效果。

胡啸副局长指出，网络安全企业的发展壮大，既是企业家的目标，也是国家网络安全工作的需要。网络安全企业要在维护国家网络安全中发挥重要作用。

微信扫描二维码阅读全文

纽约通过 SHIELD 改进法案以加强数据保护

纽约州长 Andrew M. Cuomo 签署了 SHIELD（Stop Hacks and Improve Electronic Data）改进法案，旨在保护纽约人的私人数据。该法案在美国各州和联邦机构就 2017 年数据泄露事件进行调查后宣布达成 6.5 亿美元和解协议之后签署，扩大了当前数据泄露通知法的信息范围，增加了民事处罚并扩大了数据泄露的定义。纽约州长还签署了 S3582 参议院法案，该法案将在信用报告机构（CRA）处理涉及社会安全号码的数据泄露事件后提供合理的消费者保护。

（原文链接：https://www.bleepingcomputer.com/news/security/new-york-passes-law-to-update-data-breach-notification-requirements/）

Office 365 Webmail 在邮件中显示用户 IP 地址

通过 Office 365 发送电子邮件时，用户本地 IP 地址将作为额外的邮件头注入到邮件中。研究人员测试了 Gmail、Yahoo、AOL、Outlook.com 和 Office 365 的 Webmail 界面，只有 Office 365 的 Webmail 接口会注入用户的本地 IP 地址。不希望继续使用此标头的 Office 365 管理员可以在 Exchange 管理中心中创建一个删除标头的新规则。

（原文链接：https://www.bleepingcomputer.com/news/microsoft/microsoft-office-365-webmail-exposes-users-ip-address-in-emails/）

新 Android 勒索软件家族通过在线论坛传播

ESET 研究人员发现了一个新的 Android 勒索软件家族，检测为 Android / Filecoder.C。该勒索软件家族至少自 2019 年 7 月 12 开始活跃，通过各种在线论坛传播，并且通过带有恶意链接的 SMS 消息进一步传播给所有联系人。勒索软件具有 42 种语言版本，在发送消息之前选择与受害者设备的语言设置的相同语言版本。勒索软件使用非对称和对称加密，私钥使用 RSA 算法加密，其中硬编码的公钥存储在代码中并发送给 C2。攻击者可以解密该私钥，并在受害者支付赎金后，将该私钥发送给受害者以解密他们的文件。

（原文链接：https://www.welivesecurity.com/2019/07/29/android-ransomware-back/）

SanDisk SSD 仪表板中的漏洞可导致数据丢失

Trustwave 研究人员在 SanDisk SSD 仪表板中发现两个安全漏洞，可导致数据丢失和感染恶意软件。其中一个漏洞为 CVE-2019-13466，由该应用程序使用硬编码密码来保护客户报告数据导致，可导致在将其发送到 SanDisk 进行检查的过程中丢失数据。另一个漏洞为 CVE-2019-13467，由该应用程序使用 HTTP 而不是 HTTPS 与 SanDisk 站点进行通信而导致，攻击者可利用该漏洞进行中间人攻击，提供恶意软件。目前以上漏洞已被修复，用户需尽快升级至 2.5.1.0 版来修复以上漏洞。

（原文链接：https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/sandisk-ssd-dashboard-vulnerabilities-cve-2019-13466-cve-2019-13467/）

每周安全事件

类 型	内 容
中文标题	研究人员在暗网发现超过 2300 万张被盗支付卡
英文标题	23 MILLION STOLEN CREDIT CARDS FOR SALE ON THE DARK WEB IN THE FIRST HALF OF 2019
作者及单位	Benjamin Preminger
内容概述	研究人员在暗网发现 2019 年上半年出售的超过 2300 万张被盗信用卡和借记卡号码，其中大多数属于美国消费者，在美国用户中，平均每三张信用卡中就有近两张被盗。其次受影响较多的是英国，占比超过 7%。来自俄罗斯的被盗卡的数量最少，在 2300 万张被盗卡中只有 316 张卡属于俄罗斯用户。信用卡信息售价仅为 5 美元，主要有两种类型：一种包括支付卡的所有详细信息以及 CVV，另一种包含磁条数据。
链接地址	https://www.cybersixgill.com/stolen_credit_cards/

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

恶意代码类别	名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.Monokle.a[prv,rmt,spy] 2019-07-28	高	该应用程序是一款间谍软件，安装无图标，后台接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置、浏览器记录、用户账号、社交软件信息，私自拍照、录音、录像、截屏、监听并拦截短信、发送短信、拨打电话、键盘记录、下载恶意文件等。并将用户隐私上传至服务器。造成用户隐私泄露，建议立即卸载。
		RiskWare/Android.KouKouCha.a[exp] 2019-07-29	中	该应用程序聚合了多个风险网站，包含短信轰炸、刷赞、薅羊毛、免费视频 vip、博彩网站等，诱导用户加群，具有一定的风险，请谨慎使用。
		Trojan/Android.ScamApp.a[exp,fra] 2019-07-30	低	该应用程序伪装为换脸应用，无实际功能，运行跳转指定网页，诱导用户填写多个调查问卷，警惕网页频繁弹出广告造成用户的资费消耗，建议用户卸载该程序。
	较为活跃样本	Trojan/Android.nbank.j[prv]	中	该应用程序运行后隐藏图标，窃取用户短信、联系人、sim 卡账号并上传。造成用户隐私泄露，建议立即卸载。
		Trojan/Android.mntSpy.a[prv]	中	该应用程序伪装 google 服务，运行隐藏图标，获取用户 /mnt 文件夹下文件并上传至 ftp 服务器，造成用户隐私泄露，请立即卸载。
		RiskWare/Android.ltbocai.a[rog]	中	该应用程序为博彩类应用，会给您带来财产损失。此类程序一般以欺骗形式引诱推荐安装，是一种典型的网络赌博诈骗手段，请立即卸载。
		Trojan/Android.msaPoison.a[prv]	中	该应用程序运行隐藏图标，窃取用户短信，手机号码和通讯录并上传，造成用户隐私泄露，请卸载。
		G-Ware/Android.FakeSexApp.m[pay,fra]	中	该应用程序伪装色情应用，诱导用户点击诱惑性图片，后台私发订阅短信，会造成用户资费损耗，请卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Excel 远程代码执行漏洞（CVE-2019-1110）	高	当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件中存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理员权限登录，那么攻击者就可以控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	较为活跃样本	Trojan[Downloader]/JS.IstBar	中	此威胁是一种带有下载功能的木马类程序。该家族使用 JS 脚本语言编写。该家族运行后，会在计算机中下载并运行其它恶意程序、广告插件等，同时修改注册表文件，在启动项中添加文件。该家族还会尝试连接网络，在本地的文件夹中下载家族相关文件并运行。
		Trojan/Win32.Ahea	中	此威胁是一种木马程序。该病毒家族会试图获取管理员权限，添加开机启动，尝试在后台下载并安装其他恶意程序。
		Trojan[Rootkit]/Win64.Perion	中	此威胁是一种具有隐蔽自身行为的木马家族。该家族的样本在执行后会在用户的设备里安装一个后门，使得远程控制者对此设备有完全的访问权限，并获取该设备上的数据。
		Trojan/BAT.DelFiles	低	此威胁是一种基于 Windows 批处理文件的木马家族。该家族的样本在执行后会删除用户计算机上的文件，使系统无法运行。
		GrayWare/Win32.MegaSearch	低	此威胁是一种可以推送广告的灰色软件家族。该家族样本运行后下载并安装推广应用，在用户浏览网页时可以弹出广告、占用系统资源、影响用户使用。

“威胁猎杀”的七个实用方法

Bricata/ 文 安天技术公益翻译组 / 译

攻击者为了达到其攻击目的，必需设法规避既有规则的检测。根据不同的研究结果显示，一般来说，企业的安全团队通常需要数周甚至六个月以上的时间，才能检测到企业网络中的威胁。

即便拿这里检测威胁所需的最短时间——数周，对于企业的安全而言，也太长了。这在很大程度上催生了“威胁猎杀”（threat hunting）的概念，这是指即使没发生网络告警，也会主动寻找恶意活动的方法。

在过去的几年中，我们发现几个垂直市场（金融服务、医疗、法律和政府）对这一概念有很大的兴趣——攻击者对这些行业的最敏感的数据资产进行攻击。事实上，Gartner 在“2019 年七大安全和风险管理趋势”中就提到了威胁猎杀：

“随着安全告警复杂性和频率的增加，威胁防御开始向威胁检测转变，这要求企业对安全运营中心（SOC）进行投资。据 Gartner 称，到 2022 年，50%的 SOC 将转变为集成事件响应、威胁情报和威胁猎杀功能的现代 SOC，而在 2015 年这一比例还不到 10%。”

为帮助安全领导者创建威胁猎杀团队、计划和中心，我们对最近围绕威胁猎杀的一些最有用的方法进行了汇总。

企业是否需要威胁猎杀计划

“在威胁猎杀中，企业采用以分析师为中心的方法，来识别自动化、防御性和检测性方案所遗漏的隐蔽高级威胁。”Gartner 公司的一篇博客指出（本文参考了 Gartner 前分析师安东 · 楚瓦金 [Anton Chuvakin] 博士的研究，安东 · 楚瓦金博士最近加入了谷歌母公司 Alphabet 旗下的一家公司）。“这种方法与严重依赖于规则和算法的威胁检测截然不同。”

上述定义有助于企业回答这一问题，因为实施威胁猎杀的企业“通常已最大程度地实现了告警分类、检测内容开发流程，以及事件响应功能。”这篇文章建议企业从诸如“企业是否是隐蔽高级威胁的目标”这样的简单问题开始。

威胁猎杀需要转变思维方式

威胁猎杀旨在“识别未触发告警的威胁”，Elastic 公司的凯文 · 基尼 （Kevin Keeney）在发布于 GCN 网站的一篇文章中写道。从本质上看，威胁猎杀是主动的，而不是被动地对告警做出反应。

威胁猎杀需要转变思维方式。它假设企业环境中存在威胁，认为可以通过积极猎杀的方式来识别它们。

为威胁猎杀确定目标

有两种方法可以为威胁猎杀确定目标，这可能需要安全团队与高管进行对话，保罗 · 鲁本斯（Paul Rubens）在 eSecurity Planet 的一篇报道中指出。一种方法是从企业内部着眼，“考虑公司关键数字资产（研究数据、客户名单或生产信息等）面临的威胁；然后考虑这些信息会被如何窃取。”他写道。另一种方法是从企业外部着眼，“根据威胁情报源，了解攻击者对其他企业的攻击活动，然后考虑这些攻击活动是否会影响到本企业。”

用于威胁猎杀的数据源

网络数据是“必不可少的数据源，可用于查找企业环境中攻击活动的迹象”，IT 安全经理和 SANS 认证讲师戴维 · 马什本（David Mashburn）在发布于 Dark Reading 的一篇文章中指出。“诸如网络数据流日志、防火墙日志、代理日志、DNS 日志和 DHCP 日志等数据都可以在威胁猎杀中发挥作用。”他指出，访问和收集其中一些数据源时，可能会遇到组织障碍——这就是我们为何提倡高保真元数据和数据包捕获（PCAP）能力。

专注于猎杀特定属性

实施威胁猎杀的一种方法是：识别一项威胁，然后定义攻击者在该攻击中使用的特定属性，如协议、漏洞或 URL 等。对属性的分析越具体，在对数据集进行分类和过滤时这些属性的作用就会越凸显。如果企业设立了红队，可以请他们提供取证元素，以帮助开发这些特定属性。

利用数学和概率学识别网络异常

猎杀特定属性的另一种方法是：过滤掉日常事务，识别异常活动。这是沃尔玛威胁猎杀团队负责人弗农 · 哈伯泽策尔（Vernon Habersetzer）喜欢的一种方法。在 RSA 大会的演讲中，他指出企业网络中的日常事务是“正常活动”，因此可以过滤掉这些活动，专注于异常活动。这种思想是对数学和概率学的应用，用以过滤掉大型网络上的正常活动，只关注那些不太对劲、值得进一步研究的活动。

威胁猎杀作为专业开发计划

威胁猎杀的重点是识别未知威胁。然而，威胁猎杀的过程也能够提供很多学习机会。其中一种方法是将三级分析师与一级分析师配对（译者注：SOC 四级人才梯队中的两个角色：三级分析师和一级分析师。一级为基础安全分析师；三级为威胁猎杀分析师），让他们合作进行威胁猎杀。在这个过程中，威胁猎杀可以产生积极的双倍效应：威胁猎杀分析师对初级分析师的指导和培训。这种培训是提高人才留用率的好办法，这样，企业就能利用现有资源解决网络安全方面的技能差距和人才短缺问题了。

原文名称	A Shift in Mindset: 7 Practical Ideas Every CISO Should Know About Threat Hunting
作者简介	Bricata
原文信息	2019 年 7 月 23 日发布于 Security Boulevard。 原文地址 https://securityboulevard.com/2019/07/a-shift-in-mindset-7-practical-ideas-every-ciso-should-know-about-threat-hunting/
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。