安天发布《ERIS 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 ERIS 的勒索软件，ERIS 最初是由国外安全研究员 Michael Gillespie 在 2019 年 5 月发现。该勒索软件最初主要通过垃圾邮件进行传播。据国外漏洞利用工具包研究员 nao_sec 所说，在近期的样本中发现该勒索软件使用 RIG 漏洞利用工具包通过广告联盟进行分发。根据 nao_sec 的说法，用户访问 popcash 广告联盟时，会被重定向到 RIG 漏洞利用工具包，该工具包将尝试利用浏览器中的 Shockwave（SWF）漏洞进行植入。一旦成功，它将自动下载并安装 ERIS 勒索软件到计算机上。

勒索软件 ERIS 执行后，会加密计算机上的文件，创建文件的加密副本，删除卷影副本并追加后缀名“.eris”。该勒索软件使用“RSA+Salsa20”算法加密文件，通过二进制查看被加密的文件发现文件末尾都带有“_FLAG_ENCRYPTED”标记，表明文件已被该勒索软件加密。加密结束后，ERIS 会创建一个名为“@ READ ME TO RECOVER FILES @.txt”的勒索信，勒索信中包含比特币地址、USER_ID、解密说明。目前被加密的文件在未得到密钥时暂无法解密。

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、字符串分析鉴定器、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、静态特征检测鉴定器、安全云鉴定器、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	574b7439b7469ed10331f4f383da0631a78c71b388eab0db1399d8606108b0ea
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	805 KB
MD5	7FD8FC98D8028AFB6426244E61524B69
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Nebuler
判定依据	BD 静态分析

完整报告地址：https://1.119.163.6/vue/details?hash=7FD8FC98D8028AFB6426244E61524B69

◆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
壳行为填充导入表	★★
获取系统信息（处理器版本、处理器类型等）	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
获取驱动器类型	★

◆衍生物分析

文件名	文件 MD5	家族相似性	yara 扫描
93732c85adee3d61_00000000.eky	f1c58075333d17a8262dcc07221984ec	N/A	N/A
c35ac80342bc7ac0_00000000.pky	7888aed7faa2a134f09cbb53a175a220	N/A	N/A

◆UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	137	192.168.122.255	137
0.0.0.0	68	255.255.255.255	67
192.168.122.111	138	192.168.122.255	138
192.168.122.1	67	192.168.122.111	68

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 07 月 29 日 (总第 193 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天连续六届蝉联“国家级”应急服务支撑单位

7 月 17 日下午，在广州举办的“2019 第十六届中国网络安全年会”上举行了“第八届网络安全应急服务支撑单位授牌仪式”。本次支撑单位遴选工作自 2019 年 4 月起启动，共选出 103 个支撑单位，其中国家级 11 个、省级 69 个、反网络诈骗领域 5 个、工业控制领域 18 个。安天凭借自身在网络安全领域的核心技术实力和专业的安全服务能力，已连续 12 年、6 届入选 CNCERT 网络安全应急服务支撑单位（国家级），并成为首批入选 CNCERT 网络安全应急服务支撑单位（工业控制领域）的企业之一。

“CNCERT/CC 网络安全应急服务支撑单位”评选工作于 2004 年启动，旨在评选出长期从事网络安全领域工作，拥有国内领先的高水平技术、人员和资源积累，具有领先技术优势、综合实力强、机构分布广、社会认可度高的企事业单位。在担任国家级网络安全应急服务支撑单位的 12 年中，安天在 CNCERT 的统一指导和协调下，配合各分中心承担了高级持续性威胁（APT）深度分析工作、恶意代码监测信息共享与分析工作、安全漏洞信息报送与处置工作、网络安全信息报送工作、网络安全应急处置支撑工作以及网络安全专项工作等。

安天十几年来能坚持履行作为国家级应急服务支撑单位的职责，离不开自身对公共安全支撑能力的长期建设。2007 年，安天将病毒分析组改制为安天安全研究与应急处理中心，即安天 CERT。安天 CERT 基于多年的恶意代码检测、APT 攻击对抗与深度分析等技术积累，依托产品体系、支撑体系和威胁情报赋能，为客户提供监测分析、安全保障和应急处置等特色化安全服务。在逆向分析方面，具备依托安天大规模自动化分析处理体系的逆向分析、关联分析、同源分析平台的人机协同能力，及对“白象”等网空威胁行为体追踪溯源到自然人的成功案例。在威胁情报方面，具备对多源异构威胁情报数据的采集、分析、处理能力。这些均为有效开展威胁猎杀提供了基础支撑能力。由安天 CERT 的威胁猎杀分析师、取证工程师、逆向分析工程师、情报工程师所组建的专业威胁猎杀团队，正在积极开展威胁猎杀实践。

微信扫描二维码阅读全文

深圳市政协主席戴北方一行莅临安天总部参观指导

7 月 22 日，深圳市政协主席戴北方、副主席张晓莉等一行在哈尔滨市政协主席姜国文的陪同下莅临安天总部参观指导。

在展厅内，安天相关负责人向来宾汇报了安天的发展历程及现况、研发能力、核心技术以及在技术创新与知识产权等方面取得的成果，同时汇报了安天承担的应急响应工作情况与战术型态势感知平台研发情况。

在讲解中，相关负责人介绍了安天在全国的网络安全布局。早在 2010 年，安天就在深圳成立了研发中心，其产品和服务主要面向于网络犯罪追踪、高级威胁发现需求的企业、机构用户等。深圳研发中心是国家互联网应急响应中心广东分中心优秀通报单位，也是广东网警开展打击网络犯罪工作的支持单位。在粤港合作的大背景下，安天与广州大学成立了网络空间高级威胁对抗联合实验室，积极投入深圳鹏城实验室网络靶场等项目建设。

在参观过程中，来宾对安天作为网络安全国家队作出的突出贡献表示了肯定， 并对本地政企机构与安天展开更多的合作表示期待与支持。

研究人员发现 Comodo 反病毒产品中五个漏洞

研究人员在 Comodo Antivirus 和 Comodo Antivirus Advanced 中发现了五个漏洞，其中四个漏洞在 12.0.0.6810 版本中检测到，另外一个在 11.0.0.6582 版本中检测到。CVE-2019-3969 漏洞允许可以访问目标系统的攻击者逃避 Comodo Antivirus 沙箱并将权限升级到 SYSTEM。CVE-2019-3970 是一个任意文件写入漏洞，允许攻击者修改病毒定义，导致误报或使恶意软件绕过基于签名的检测。CVE-2019-3971 是拒绝服务漏洞，由于用于 memcpy 源地址的硬编码 NULL 而导致访问冲突，从而导致应用程序终止。CVE-2019-3972 是越界读取漏洞，可以通过修改结构数据导致超出范围读取进而导致 CmdAgent.exe 崩溃。CVE-2019-3973 是越界写漏洞，可能导致内核崩溃。

（原文链接：https://www.tenable.com/security/research/tra-2019-34）

每周安全事件

类 型	内 容
中文标题	安全厂商披露针对亚洲公司的 DLTMiner 攻击活动
英文标题	CB TAU Technical Analysis: DLTMiner Campaign Targeting Corporations in Asia
作者及单位	JARED MYERS
内容概述	Carbon Black 发现与 DLTMiner 活动有关的新攻击。DLTMiner 活动于 2019 年 1 月报道，活动利用了永恒之蓝漏洞以及 RDP 暴力破解，用于进行加密货币挖矿。新攻击活动目标为亚洲的组织，研究人员确定了两名受害者，分别位于越南和美国医院。
链接地址	https://www.carbonblack.com/2019/07/23/cb-tau-technical-analysis-dltminer-campaign-targeting-corporations-in-asia/

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.SmsSpy.by[prv,exp] 2019-07-21	高	该应用程序该应用运行后隐藏图标，包含恶意代码，后台监听用户短信并上传，诱导用户点击按键，私自发送短信至指定号码。造成用户隐私泄漏和资费消耗，建议立即卸载。
		Trojan/Android.Locker.bt[rog,lck] 2019-07-22	中	该应用程序伪装游戏外挂，运行请求 root 权限，而后安装勒索子包并重启，勒索子包会置顶界面，影响用户手机的正常使用，建议立即卸载。
		Trojan/Android.Fakeyouwon.a[exp,rog] 2019-07-23	中	该应用程序非官方应用，包含恶意代码，运行后加载恶意网页脚本，频繁推送流氓广告，加载风险网页。造成用户流量消耗，严重影响用户手机体验，建议不要使用。
	较为活跃样本	Trojan/Android.wm01.b[prv,rmt,spy]	中	该应用程序运行隐藏图标，检测设备是否 root、是否为模拟器，私自窃取通知栏信息、通话记录、相册、联系人、短信、wifi 网络参数、设备信息、装机应用列表等隐私信息，联网获取远程指令，执行发送短信、录音、定位跟踪、拍照等风险操作，造成用户隐私严重泄露，建议立即卸载。
		Trojan/Android.Androrat.k[prv,rmt,spy]	中	该应用程序运行隐藏图标，激活设备管理器，联网获取远程指令，窃取用户短信，通讯录，通话记录，浏览器记录，定位，照片和视频等隐私信息，造成用户隐私泄露，请立即卸载。
		Tool/Android.FahrezoneBypass.a[rog]	中	该应用程序是一款游戏过安全检测工具，使用 va exposed 技术，可能用于游戏作弊，请用户谨慎使用。
		Tool/Android.DiDiPluging.a[rog]	低	该应用程序为一款滴滴打车的司机抢单工具，运行会请求监控用户窗口进行模拟点击抢单，请谨慎使用。
		G-Ware/Android.FakeApp.gp[fra,exp]	低	该应用程序是虚假应用，无实际功能并且会加载广告，会造成用户流量资费损耗，请卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 远程桌面服务远程代码执行漏洞 CVE-2019-0887	高	当经过身份验证的攻击者滥用剪贴板重定向时，远程桌面服务中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在用户的系统上执行任意代码。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[Backdoor]/Win32.Sixer	中	此威胁是一种具有后门行为的木马家族。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[PSW]/Win32.Makuha	中	此威胁是一种具有窃取密码行为的木马家族。该家族的样本在执行后会监视用户的键盘输入，并将用户输入的密码发送给远程的控制端。
		Trojan[GameThief]/Win32.MFirst	中	此威胁是一种具有偷取用户游戏账号信息的木马家族。该家族的样本在执行后会在用户启动游戏时监视用户的键盘输入并获取用户的账号用户名和密码。
		GrayWare[AdWare]/Win32.Topa	低	此威胁是一种具有广告件行为的灰色软件家族。该家族的样本在执行后会在通知区域和页面上弹出广告，影响用户的使用体验。
		GrayWare[AdWare]/Win32.AddLyrics	低	此威胁是一种具有广告件行为的灰色软件家族。该家族的样本在执行后会安装一个浏览器插件，为用户提供歌词，同时在界面上弹出广告。

为何说事件响应必须采用“杀伤链”视角

Stan Engelbrecht/ 文 安天技术公益翻译组 / 译

虽然事件响应（IR）在不断发展，但它仍然面临“跳出单个事件，从更完整的视角进行响应”的挑战。目前，IR 工具仍然非常有效，特别是随着编排和自动化技术的发展，许多 IR 工具已经转变为“安全编排、自动化及响应”（SOAR）工具，但它们仍然受到这种狭隘视角的限制。

IR 发展的下一步，是采用基于“杀伤链”（kill chain）的视角。这是因为，严重的网络攻击很少是单一事件；它们更有可能是一系列事件的组合，而这些事件的关联并不总是那么明显。

在前一篇专栏文章中，我分析了网络杀伤链是什么、MITRE 公司如何在这个概念的基础上创建了 ATT&CK 矩阵，以及为何说网络杀伤链对安全运营团队是有价值的等问题。在本文中，我将专门探讨 IR，并分析为何说从杀伤链层面了解网络攻击是检测和阻断严重攻击的最佳方法。

Carbanak 银行劫案

严重的网络攻击通常不是单一的事件，而是攻击者为实现攻击目标所执行的一系列活动。最近几年发生的重大银行劫案就是很好的例子：FIN7 网络犯罪组织利用 Carbanak 后门，窃取了涉事银行大笔资金。

这一系列利润丰厚的盗窃案，不仅仅是攻破涉事银行网络和从 ATM 机提取现金的问题。它们是一系列耗时冗长的攻击活动，有的甚至持续了数月。举例来说，2018 年针对一家欧洲银行的攻击涉及鱼叉式网络钓鱼、漏洞扫描、

域控制器感染、Cobalt Strike 监听、主机感染、远程访问、对命令服务器的渗透等攻击活动。

在这些攻击活动中，攻击者技术娴熟，动作低调，使得研究人员难以检测到攻击迹象。他们通常在工作时间执行攻击，以便将攻击活动与正常活动相混淆。但是某些攻击活动，如数据渗漏，则是在晚上和周末执行的，而且仅限于短会话，旨在避免银行员工发现异常的流量高峰。

打破攻击链

鉴于上述原因，采用基于事件的视角进行攻击检测和响应，已经不再是防御诸如 Carbanak 等高级持续性威胁的理想方法了。攻击者手段高明，他们的许多活动，单独看起来都是合法的。只有在鱼叉式网络钓鱼攻击的完整杀伤链视角下，才能发现其恶意意图。

从传统的 IR 视角来看，我们的目标是阻止单一攻击活动。在这种情况下，如果一个鱼叉式网络钓鱼邮件被标记了，则该邮件的发件人就会被阻断。但是，这并没有解决掉正在进行的攻击的其他威胁因素——可能还有十几封钓鱼邮件设法规避了检测，但我们却没有采取任何措施来识别它们。采用杀伤链视角，我们可以识别出正在发生的鱼叉式网络钓鱼攻击，并着手查找杀伤链中的其他链条。例如，检测到一封恶意电子邮件后，我们可以对其进行分析拆解，并根据相关信息搜索其他可能的鱼叉式网络钓鱼邮件。如果检测到了其他的钓鱼邮件，我们就可以根据攻击者下一步的目标（钓鱼邮件的收件人）来查找其他攻击迹象了。通过这种框架，我们可以构建一个相互关联的，包含多起事件、攻击信标、端点和外部各方的网络。随着杀伤链被逐步揭开，我们可以在攻击者达到最终目标之前尽可能地破坏链条——无论最终目标是谁。

前进一步

随着 IR 技术的发展，IR 已不再是纯粹的响应过程，因此“事件响应”一词已经不再恰当了。以前，IR 的目标是将攻击影响控制在最低限度、了解发生的攻击事件，以及修复被利用的漏洞。而现在，从杀伤链的视角来看，我们所响应的“事件”可能只是攻击的一小部分，因此我们还有机会在任何损害发生之前进行主动干预。

攻击者似乎总是能领先一步。而基于事件的响应、基于特征的检测和其他传统安全方法，无论执行过程有多完善，也无法完全消除这种差距。安全团队需要将基于对攻击者意图的响应、基于行为的检测和杀伤链视角结合起来，以便领先于攻击者。支持这种转变的技术已经开始出现，这让我对 IR 的未来非常乐观。

原文名称	Why Incident Response Must Adopt a Kill Chain Perspective
作者简介	Stan Engelbrecht。Stan Engelbrecht 是 D3 Security 公司的网络安全实践主管。
原文信息	2019 年 7 月 19 日发布于 Security Week。 原文地址 https://www.securityweek.com/why-incident-response-must-adopt-kill-chain-perspective
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。