安天发布《Cardinal 远控家族样本分析报告》

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种名为 Cardinal 的远控木马家族。该家族最早发现于 2017 年，通过一个叫 Carp 的下载木马传播，并在近两年间不断更新版本。在近期针对以色列金融技术行业的攻击活动中，发现该木马最新版本已更新为 Cardinal 1.7.2，该版本使用了各种混淆技术阻碍对代码的检测分析。

该样本使用 .Net 编译，并且嵌入了三个资源文件。当木马运行后，首先读取资源中的位图文件，对其像素数据进行解密处理，从而得到一个 dll 文件，该文件也使用 .Net 编译。dll 文件运行后，会从原始样本中读取并解密名为”strings”的资源文件，该资源包含了配置信息，它指示了 dll 接下来的操作模式。在安装模式下，dll 文件会将 GUID 写入 %TEMP%\[random].ini，并创建目录 %APPDATA%\Microsoft\Windows\IEConfig，然后创建一个 .lnk 文件并设为自启动项。该 .lnk 文件执行如下命令：C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden “%APPDATA%\Microsoft\Windows\IEConfig\[random]\sqlreader.exe，其中 sqlreader.exe 是原始样本的一个副本。最后，木马解密最后一个资源文件，得到一个 .Net 可执行文件，该文件会被注入到 RegSvcs.exe 或 RegAsm.exe 这两个合法的系统进程中去。若机器被该木马感染，攻击者可以对受害主机进行一系列操作，如收集用户信息、设置反向代理、执行远程命令、键盘记录、窃取浏览器 Cookie 等。

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、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	9e6671a8af28e0ab6c37c044d85a2406b665a171ae3bef46f3e90d06e33027ae
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	608 KB
MD5	F73A462D2BCB182B3BCAB63274D0E37C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.BTSGeneric
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=F73A462D2BCB182B3BCAB63274D0E37C

◆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）	★
获取计算机名	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
壳行为填充导入表	★★
创建特定窗体	★
设置调试器权限	★
疑似桌面控制	★

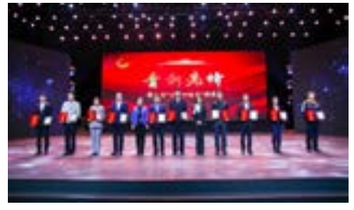
◆静态启发式检测

检测类型	检测点	详细说明
PE 结构	非微软的版本信息	非受信厂商的版本信息。具有较低的受信级别。
PE 结构	PE 有附加数据	PE 文件包含附件数据通常用来对抗云检测。云检测通常使用全文 HASH 进行检测，在 PE 尾部增加一段数据，不影响程序正常执行，但会使程序的全文 HASH 发生改变，从而逃避云检测的查杀。

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 15 日 (总第 179 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

青春心向党 建功新时代 | 安天工程师荣获“青新先锋”称号

近日，由共青团哈尔滨市委员会、哈尔滨广播电视台共同主办的“青春心向党 建功新时代”第二季“青春创想季”群英荟在哈尔滨举行。安天工程师尹尚书在众多候选人中脱颖而出，荣获“青新先锋”称号，登台接受表彰。



《青春创想季》节目由共青团哈尔滨市委员会、哈尔滨广播电视台共同打造，栏目分为“青创之星”、“青年工匠”、“青新先锋”三个类型，深入挖掘宣传哈尔滨市青年中创新、创业、创优的突出典型，本季共有 60 位优秀青年展示了自身的风采和事迹。

安天工程师尹尚书从事网络安全工作至今已十一年，他的工作职责是提供专业的安全服务，保障用户的网络安全。作为引领威胁检测与防御能力发展的网络安全国家队，安天参与并承担了 2005 年后历次国家重大政治社会活动的安保工作，并多次获得杰出贡献奖、安保先进集体等称号，尹尚书便是这些安保工作的主要参与者之一。

2016 年，举世瞩目的 G20 峰会在杭州举行，安天承担了重要的网络安保任务。在会议召开前，尹尚书带领团队对千余个网站进行安全测试，发现并协助修复了百余处安全漏洞，避免了攻击者利用漏洞对这些网站进行攻击。G20 召开期间，他带领团队进行 24 小时应急值守，在网络安全领域为 G20 的顺利召开保驾护航。由于工作突出，他获得了 G20 峰会安保贡献突出个人。

尹尚书曾说：“网络安全，是一场没有硝烟的战争。威胁无处不在，作为正义的一方，应该时刻保持警惕，不能松懈。”这既是他的工作信条，亦是安天团队的坚持。安天以保障国家网络安全为己任，始终站在威胁对抗的第一线，不断打磨自身的安全产品与服务，为捍卫国家主权、安全和发展利益，为保障客户安全价值而不断奋斗。

研究人员发现 GoBrut 僵尸网络新 ELF 变种

研究人员发现与 Magecart 组织有关的僵尸网络 GoBrut 出现了可以针对 Unix 的新 ELF 变种。GoBrut 是用 Golang 编写的恶意软件，它被用来暴力破解运行内容管理系统（CMS）和 SSH、MySQL 等技术的服务器。研究人员发现针对 Magento CMS 和 phpMyAdmin 进行暴力破解的 2 个攻击向量，并且发现一个新 C2，其专门用于针对 WordPress 进行暴力破解，目前观察到大约 1,568 个 WordPress 站点的约 11,000 个受感染服务器。

（原文链接：https://blog.alertlogic.com/gobrut-botnet-elf-variant-and-new-c2-discovered/）

研究人员发现复杂的新 APT 框架 TajMahal

研究人员在 2018 年秋季发现一个以前未知且技术复杂的 APT 框架 TajMahal。这个完整的间谍框架由两个名为“Tokyo”（东京，其用作第一阶段感染）和“Yokohama”（横滨）的包组成，其包括后门、加载器、协调器、C2 通信器、录音器、键盘记录器、屏幕和网络摄像头抓取器、文档和加密密钥窃取程序、受害者计算机的文件索引器。加密的虚拟文件系统中存储了多达 80 个恶意模块，这是已知 APT 工具集中插件数量最多的工具集之一。TajMahal 至少在过去五年中进行开发和使用，目前发现了一名来自中亚国家外交领域的受害者，样本确认日期为 2014 年 8 月，而已知样本的第一个时间戳是 2013 年 8 月，最后一个是 2018 年 4 月。

（原文链接：https://securelist.com/project-tajmahal/90240/）

海莲花组织更新其 macOS 恶意软件结构

2019 年 3 月初，来自 APT 组织海莲花（OceanLotus）的新 macOS 恶意软件样本被上传到 VirusTotal。新版本后门与之前版本具有相同功能，但其结构的更改增加了检测难度。样本使用带有“UPX”字符串和 Mach-O 签名的 UPX 进行打包，更新了其 C2 服务器和收集信息的数据，使用外部库进行网络渗透，字符串使用 AES-256-CBC 加密，使用 IDA Hex-Rays API 自动执行字符串解密。目前研究人员还未发现与该样本相关的释放器，还未确定初始攻击向量。

（原文链接：https://www.welivesecurity.com/2019/04/09/oceanlotus-macos-malware-update/）

每周安全事件

类 型	内 容
中文标题	Mirai 新变种可感染多种 IoT 处理器驱动设备
英文标题	Mirai Compiled for New Processors Surfaces in the Wild
作者及单位	Ruchna Nigam
内容概述	研究人员发现了使用新处理器编译的 Mirai 恶意软件变种。变种扩展了处理器架构，能够感染运行 Altera Nios II、OpenRISC、Tensilica Xtensa 和 Xilinx MicroBlaze 处理器的物联网设备。受感染设备的数量增加，这意味着 Mirai 攻击者可获得更多的资源用于拒绝服务攻击（DDoS）。新样本中采用 XOR 加密，包含 DDoS 攻击选项参数，在托管 Mirai 样本的 IP 中包含以前被利用的漏洞：ThinkPHP 远程执行代码、D-Link DSL2750B OS 命令注入、Netgear 远程执行代码、CVE-2014-8361、CVE-2017-17215，这些漏洞也可能继续用于新变种的攻击中。
链接地址	https://unit42.paloaltonetworks.com/mirai-compiled-for-new-processor-surfaces/

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.bhdfhh.a[prv,rmt,spy] 2019-04-08	该应用程序运行后隐藏图标，接收远程指令上传用户短信、联系人、通话记录等隐私信息，执行私自发送短信、打电话、录音、拍照等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.MeshAgent.a[prv,exp,rmt,spy] 2019-04-09	该应用程序为间谍件，安装无图标，接收远程指令，发送短信、拨打电话、连接 wifi、访问网页、删除 wifi 记录，还会上传联系人信息、应用安装列表、设备信息等隐私信息，会造成用户资费损耗和隐私泄露，请卸载。（威胁等级高）
		Trojan/Android.FakeAlipay.i[prv] 2019-04-10	该应用程序伪装支付宝订单或收款助手，后台窃取用户支付宝账号密码、账户 ID、交易记录等隐私，会造成用户隐私泄露，请卸载。（威胁等级中）
	较为活跃的样本	RiskWare/Android.Fake360root.a[rog,fra]	该应用程序伪装 360 超级 ROOT，无实际功能，被植入了其他应用，运行后释放无极 VPN 应用，存在一定风险，建议用户卸载，使用正版软件。（威胁等级中）
		RiskWare/Android.tianyubocai.a[rog]	该应用程序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，请谨慎使用。（威胁等级低）
		RiskWare/Android.kgqpbocai.a[rog]	该应用程序是一款线上赌博游戏，可以通过微信、支付宝等方式进行充值，可能给用户的财产带来较大风险，且难以保障财产权益，请谨慎使用。（威胁等级低）
		Trojan/Android.FakeAlipay.h[prv]	该应用程序伪装成支付宝相关应用，诱导用户输入支付宝账号密码，上传服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.FakeMessage.b[prv]	该应用程序伪装蓝牙应用，无实际功能，运行后隐藏图标，会联网上传用户手机基本信息，造成用户信息泄露，建议不要使用。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 特权提升漏洞（CVE-2019-0730）	当 Windows 不正确地处理对 LUAFV 驱动程序 (luafv.sys) 的调用时，会触发特权提升漏洞。成功利用此漏洞的攻击者可以在本地系统执行任意代码。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账户。（威胁等级高）
	较为活跃样本	RiskWare[Downloader]/Win32.Ocna	此威胁是一种可以下载推广应用并安装的风险软件家族。该家族样本运行后连接网络下载推广应用并安装，占用系统资源，影响用户使用。（威胁等级中）
		RiskWare[Downloader]/Win32.Montiera	此威胁是一种可以下载推广应用并安装的风险软件家族。该家族运行后会收集信息回传给攻击者，并在电脑中下载恶意程序并执行。（威胁等级中）
		Trojan[Rootkit]/Boot.Pihar	此威胁是一种可以修改 MBR 并在系统内核之前加载的木马家族。该家族会监控网络流量和击键组合，在电脑中留下隐蔽的后门，并试图攻击局域网内的其他机器。（威胁等级中）
		Trojan[Dropper]/Script.AGeneric	此威胁是一种由脚本语言编写并且具有捆绑行为的木马类程序。该家族没有统一的行为与功能，是以启发式检出的恶意代码。（威胁等级中）
		Trojan[Downloader]/Win32.Stantinko	此威胁是一种下载者木马程序，该家族样本运行后连接网络，下载其他恶意代码到用户系统中运行。（威胁等级中）

“无服务器计算”带来的安全挑战

Mirko Zorz/ 文 安天技术公益翻译组 / 译

对许多企业来说，“无服务器计算”（又称“功能即服务”[Function-as-a-Service]）是一个福音：它简化了代码开发和部署过程，同时提高了服务器资源的利用率，最大限度地降低了成本和安全开销。

“无服务器基础设施的采用速度比大多数人意识到的要快，”应用安全提供商 Data Theorem 首席运营官道格 · 杜利（Doug Dooley）说，“在过去的 4 年里，无服务器基础设施的采用率远超 Docker 等虚拟容器——前者是后者的 2 倍多。这种快速采用对企业安全带来了巨大的影响。”

无服务器计算及其安全性

无服务器技术简化了云计算，并带来了新的经济模型。通过使用公有云产品来部署无服务器应用执行模型，企业还可以将更多安全任务移交给云提供商。

这样一来，企业只需保护应用层就行了：即，管理和监控应用和数据访问、实施合法的应用行为、监控错误和安全事件等。

不过，无服务器计算是一项相对较新的技术，许多开发和安全团队还在努力理解和应对它所带来的安全风险。

“目前，许多安全工具依赖于连接到底层服务器、虚拟机、客户机操作系统、数据库、虚拟容器和虚拟网络接口。”杜利指出。

“一旦应用开发人员选择在无服务器基础设施上构建应用，那些底层组件就无法使用了。因此，许多安全团队正忙着开发新的解决方案，以期保护基于无服务器框架（如 Amazon Lambda、Azure Functions 和 Google Cloud Functions）的应用和 API。”

采用无服务器技术的安全挑战

企业需要关注其环境中的“影子 API”（Shadow API），原因如下：

• 云提供商获得投资，能够更容易、更快速、更便宜地在其平台上构建大规模应用。

• 在扩展后端应用和 API 方面，无服务器是软件工程师和 DevOps 团队的首选技术。

“冷启动”（cold-start）问题和潜在的“巨额费用攻击”（denial-of-wallet，DoW）可能会带来重大的挑战。

如果无服务器应用不常被访问，并且虚拟容器和数据库需要一段时间才能进行响应，就有可能会出现“冷启动”问题。杜利指出，企业正在开发新的解决方案来应对这些问题，确保安全工具不会误认为应用处于脱机状态。

DoW 攻击可能会导致巨大的损失。

“当大多数应用遭遇 DoS 攻击时，它们就无法响应新请求了，这是因为：资源已被 DoS 攻击者发起的大量虚假请求所占用。”他解释说。

“但是，对于无服务器应用来说，扩展足够的基础设施来处理新请求的任务，已经移交给云提供商。如果无服务器应用的扩展没有上限，则 DoS 攻击会给应用开发商带来巨大的经济负担。鉴于企业无法承受此类攻击的高昂成本，我们将此类攻击称为‘巨额费用攻击’（DoW）攻击。”

不过，到目前为止，最紧迫的挑战似乎是可见性问题。

“如果你向任何 IT 或信息安全领导者询问，他们将多少业务应用和 API 连接到了无服务器基础设施，他们很可能无法给出答案。”他说。

DevOps 团队是无服务器应用的创造者和早期采用者，他们不需要请求权限来构建无服务器应用。此外，在默认情况下，他们也是无服务器应用和 API 安全问题的第一响应者。

“对大多数企业 IT 和安全领导者来说，无服务器应用是一个盲点。但是，随着企业获得更多的经验和经济利益，IT 和安全团队将会强势介入，以期提高对新威胁和潜在风险的可见性和洞察力。”

给 CISO 的建议

尽管存在上述问题，但杜利建议首席信息安全官（CISO）不要阻止企业采用无服务器技术。

他认为，这跟阻止采用移动、云和“软件即服务”（SaaS）技术一样毫无意义，并且会使 CISO 被视为创新、成本节约和业务敏捷性的障碍。

相反，他建议 CISO 鼓励安全团队采用无服务器等新技术，同时充分考虑到安全问题和潜在风险。

“安全团队可以提供自动化分析，帮助软件工程师和 DevOps 团队快速发现和检查企业发布和使用的无服务器应用和 API。而这些新 API 是将无服务器应用与其他组件互联的基础。”他总结道。

原文名称	The security challenges that come with serverless computing
作者简介	Mirko Zorz。Mirko Zorz 是 Help Net Security 网站的主编。
原文信息	2019 年 4 月 4 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2019/04/04/enterprise-serverless-security/
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。