安天发布《Phobos 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现 Phobos 勒索软件家族新变种，该勒索软件家族于 2019 年初被发现，一直在不断更新。本次事件中的变种最早于 2019 年 9 月末被发现，其传播方式主要为 RDP 暴力破解和钓鱼邮件。Phobos 勒索软件家族在全球多个行业扩散，感染面积大，变种更新频繁。

Phobos 运行后，不仅会加密文档文件还会加密可执行文件，加密后创建两种类型的勒索信，一种为 txt 格式，另一种为 hta 格式。Phobos 勒索软件变种使用“RSA+AES”算法加密文件，暂时没有解密工具。安天 CERT 分析发现，Phobos 勒索软件家族与 2016 年出现的 CrySIS/Dharma 勒索软件家族所使用的加密方式、部分代码段、勒索信外观与内容，以及用于加密文件的命名方式都较为相似，不排除为同一作者或 Phobos 勒索软件攻击者购买、利用 CrySIS/Dharma 勒索软件相关代码的可能性。

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。

最终依据反病毒引擎鉴定器、BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	782d18.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	51 KB
MD5	4CBCF650C75C6CD0CC16ED24C3B24DE6
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Wacatac
判定依据	反病毒引擎

◆ 操作系统

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
文件篡改	★★★★★
扫描 445 端口尝试访问系统共享文件夹	★★★
检测虚拟机	★★★★★
疑似查找游戏进程	★★★★

◆常见行为

行为描述	危险等级
打开自身进程文件	★
加载运行时 DLL	★
检测虚拟机获取计算机名	★
检索系统内存信息	★
创建挂起进程	★★
.....	.....

◆完整报告地址

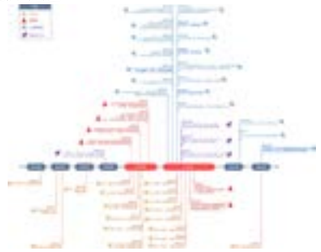
安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 10 月 28 日 (总第 205 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

震网事件的九年再复盘与思考

震网事件已过去多年，但却从未离开我们的视线。今天看来，在前期分析震网系列事件的过程中，我们缺少一种真正意义上的框架化方法。依然更多的是从自身习惯的反恶意代码视角来看待整个攻击过程。尽管我们给震网这样的复杂攻击提出了一个 A²PT（即高级的高级可持续性威胁）的命名，但分析中始终缺乏作业到作战视角的思考。在相关专家的指导下，我们对网空博弈、敌情想定有了新的体悟，逐渐从威胁框架视角进行方法论切换，实现自我能力完善。也希望通过威胁框架这一视角来解读“震网”这场看起来依然高度复杂的“昨天的战争”。本文也详细解读了一个值得思考的问题，震网作为一种没有感染属性的蠕虫，为何会有大量的样本存在。

在信息技术发展历史上，出现过大量典型的安全事件，但为什么“震网”被视为具有威胁里程碑意义？震网被认为是第一个以现实世界中的关键工业基础设施为目标的恶意代码，并达到了预设的攻击目标，或者说，这是第一个“网络空间”意义上的重大攻击事件，而非传统的网络攻击事件。尽管此前也存在着一些通过信息攻击手段影响工业设施的传闻，但基本都缺乏技术层面的实证支撑。

从安天此前提出的观点来看，震网的里程碑意义并不是在于其相对其他简单的网络攻击的复杂性和高级性，而在于其证实了通过网络空间手段进行攻击，可以达成与传统物理空间攻击（甚至是火力打击）的等效性。在 2016 年的报告中，安天研究人员将上世纪 70、80 年代的“凋谢利刃与巴比伦行动”（在 1977 年 ~1981 年间发生的以、美联合，在两伊战争期间针对伊拉克核反应堆进行军事打击的事件）与震网事件进行对比分析看出，通过大量复杂的军事情报和成本投入才能达成的物理攻击效果仅通过网络空间作业就可以达成，而且成本也大大降低。正如美国陆军参谋长前高级顾问 Maren Leed 所讲的——网络武器可以有许多适应环境的属性，从生命周期的成本角度看，它们比其他的武器系统更为优越。



▲震网事件时间轴

震网整体结构和运行逻辑

震网的结构非常复杂。其中又经历了从 0.5 到 1.x 的版本更迭，其破坏机理从以干扰离心机阀门、造成超压导致离心机批量损坏调整为修改离心机转数。同时其开发框架也发生了变化。我们以流行更为广泛的 1.x 版本为对象，进行整体结构和运行逻辑梳理。震网的核心是仅在内存中解密存在的 DLL 文件（以下简称主 DLL 文件）。DLL 文件包含 32 种不同的导出函数以及 15 种不同的资源，每一个导出函数都有不同的控制功能，其中主要涉及导出函数 15（初始入口点）、导出函数 16（安装）、导出函数 32（感染连接的移动设备，启动 RPC 服务）、导出函数 2（钩挂 API 以感染 Step7 工程文件）等；每个资源也分别执行不同的功能，主要涉及资源 250、资源 201、资源 242 等；导出函数正是利用这些不同功能的资源来控制震网执行不同的分支操作。

震网的传播主要包括两种方式，一种是移动设备感染，利用 LNK 漏洞或者通过 autorun.inf 文件进行传播；另一种是网络传播，涉及 WinCC 数据库感染、网络共享传播、打印机后台处理程序漏洞传播、Windows 服务器漏洞传播等多种方式。这两种传播方式虽然不同，但最终都会释放主 DLL 文件，进行后续的安装和执行操作。震网感染目标系统后，会启动 RPC 服务器监听网络，将网络上其他感染计算机都连接到 RPC 服务器，并查询远程计算机安装的震网版本，以执行对等通信和更新，如果远程计算机上的震网版本较新，则本地计算机就会请求新版本并自我更新，如果远程机器上的震网版本较旧，则本地计算机上的震网就将自身副本发送给远程机器。这样，震网可以在任何感染机器上更新并最终传播到所有机器。

直面检测引擎与威胁情报面临的挑战

安天基于传统检测引擎在威胁对抗中，是攻击方重点绕过环节的特点，自 2016 年起开始研发下一代威胁检测引擎。安天下一代引擎延续并深化了安天传统引擎格式识别、深度解析等特点，继承对海量恶意代码精准的分类到变种的识别能力。同时，以没有可信的格式和对象为前提，形成对检测对象全格式识别，对更多重点格式形成深度解析能力。不止为调用环节输出判定结果，同时也可以将检测对象的向量拆解结果结构化输出，形成支撑产品场景和态势感知场景研判分析、关联与追溯的数据资源。

探索检测引擎与威胁情报更好的结合，建立起更可靠的基础标识能力与响应机制，更有效的支撑 TTP，乃至人员组织相关的情报，建立起更完善的知识工程运营体系，这对我们来说，将是一个需要长期努力的方向。

微信扫描二维码阅读完整报告

每周安全事件

类 型	内 容
中文标题	Autoclerk 数据库泄露影响超过 179GB 的敏感数据
英文标题	Open database leaked 179GB in customer, US government, and military records
作者及单位	Charlie Osborne for Zero Day
内容概述	研究人员披露了一个开放的数据库，该数据库公开了包含酒店顾客以及美国军事人员和官员的敏感数据的记录。周一，由 Noam Rotem 和 Ran Locar 领导的 vpnMentor 的网络安全团队表示，该数据库属于 Autoclerk，成千上万的预订信息被公开，包括全名、出生日期、家庭住址、电话号码、日期和旅行费用、一些登记时间和房间号码，以及“部分遮挡”的信用卡详细信息。
链接地址	https://www.zdnet.com/article/autoclerk-database-leaked-customer-government-and-military-personal-records/

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.Slocker.i[rog,lck] 2019-10-20	高	该应用程序为勒索软件，运行后请求用户激活设备管理器，置顶界面勒索用户付费解锁，造成用户手机无法正常使用，建议卸载。
		Trojan/Android.FakeSmsProvider.a[pay,exp,fra] 2019-10-21	中	该应用程序包含恶意代码，运行后私自发送短信，从服务器获取数据，私自插入营销短信到短信数据库，造成用户资费损耗，建议卸载。
		Trojan/Android.fakewechat.w[prv,fra] 2019-10-22	中	该应用程序伪装成微信相关应用，运行后请求激活设备管理器，诱导用户输入微信账号密码并上传，造成用户隐私泄露，建议卸载。
	较为活跃样本	G-Ware/Android.HiddenApp.cp[exp,rog]	中	该应用程序伪装正常应用，运行隐藏图标，联网获取配置信息，访问推广链接，弹出广告界面，还会下载未知应用，造成用户流量资费损耗，建议卸载。
		Trojan/Android.LockScreen.cr[rog,lck]	中	该应用程序包含恶意代码，运行后锁定用户界面，影响手机正常使用，建议卸载。
		Trojan/Android.IyaPS.a[prv,exp]	中	该应用程序安装无图标，运行解析用户短信，根据短信指令，发送位置、系统信息至指定号码，造成用户的隐私泄露和资费消耗，建议卸载。
		RiskWare/Android.Clicker.ah[exp]	低	该应用程序无实际功能，运行加载调查问卷页面，可能造成用户的资费消耗，建议卸载。
		Trojan/Android.phonespy.e[prv,spy]	低	该应用程序是一款间谍软件，运行后监听用户短信、窃取用户短信并上传至服务器。造成用户隐私泄露，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft XML 远程代码执行漏洞（CVE-2019-1060）	高	当 Microsoft XML Core Services MSXML 分析器处理用户输入时，存在远程代码执行漏洞。攻击者需要诱使用户单击电子邮件或即时消息中的链接以使用户链接到恶意网站，成功利用此漏洞的攻击者可以远程运行恶意代码控制用户的系统。
	较为活跃样本	Trojan[Backdoor]/Win32.Haxdoor	中	此威胁是一种具有后门行为的 rootkit 木马家族。该家族样本运行后会隐藏自身进程；在后台窃取用户击键信息、屏幕截图、运行的进程的信息，并将这些信息发送给攻击者。
		Trojan[Exploit]/JS.ADODB	中	此威胁是一种可以利用漏洞的木马家族。该家族样本一般是 JS 脚本，运行后可以下载恶意代码，利用 adobe 相关漏洞执行远程恶意代码。
		Trojan/PHP.Agent	中	此威胁是一种以 PHP 页面为载体的木马类程序。该家族样本运行后一般会连接远程服务器下载恶意代码，打开后门收集用户信息。
		GrayWare[AdWare]/Win64.AGeneric	低	此威胁是一种可以弹出广告的灰色软件家族。该家族样本基于 64 位系统，运行后连接远程服务器下载推广应用并安装，占用系统资源，影响用户使用。
		GrayWare[AdWare]/NSIS.Baserch	低	此威胁是一种可以安装浏览器工具栏的灰色软件家族。该家族样本运行后安装浏览器搜索工具栏，在用户浏览网页时弹出广告，影响用户使用。

网络安全如何促进企业发展

Peter Bello / 文 安天技术公益翻译组 / 译

由于高级网络犯罪活动的泛滥，网络安全行业在过去十多年里呈指数级发展，这已经不是什么秘密了。将网络安全视为减轻网络风险的必要措施，能够给企业提供更多的机会。企业领导人需要将网络安全视为能够加速企业发展的推动力。

目光短浅的公司将网络安全视为保护数据所需的间接成本。这些公司正在丧失创新和发展的机会。在这个数字化技术日益颠覆的时代，那些部署网络安全措施来保护关键资产、为移动员工赋能、实现 IT 基础设施现代化，并精简合规性的公司，将超越那些仅将网络安全视为一种数据保护手段的竞争对手。

保护关键资产

在数字化中心的世界里，保护关键资产比以往任何时候都更加重要。这通常是公司和政府机构向网络安全投资的原因。网络安全涉及从用户和设备证书、移动设备管理、多因子身份鉴别（MFA）、基于角色的访问控制、特权帐户管理、单点登录（SSO）、企业和云身份管理等所有内容。

向用户和非个人实体签发强大的身份，同时保护静止和传输中的数据，对于保持强大的网络安全态势至关重要。通过良好的策略和实践采用公钥基础设施（PKI）将有助于实现这一目标——无论 PKI 是本地的还是基于云的。这是网络安全的关键因素之一，但并非唯一的因素。

为移动员工赋能

在移动性日益增强的世界里，仅仅关注 PC 的安全性已经不够了。移动员工是一种新的规范，企业在提高生产力的同时，还能从地理上扩展员工队伍——这对企业创新和发展至关重要。

为了向移动员工赋能，企业面临着新的挑战，如正确审查移动用户、向这些用户部署数字证书，以及实施正确的移动安全技术、工具和策略。

创新需要灵活性，而灵活性需要移动性。在移动基础设施中保持强大的网络安全态势，是警告风险、实现和加速发展的关键。

实现 IT 基础设施的现代化

越来越多的公司正在“迁移到云”，以支持企业和移动员工，并实现更强大和无缝的协作。与本地部署的解决方案相比，托管云环境为员工协作和从任何位置访问数据提供了显著的优势，这反过来又有助于企业创新和发展。

迁移到云还可以极大地节省成本，这是因为企业不必维护和不断更新本地环境所需的 IT 基础设施。

然而，云迁移也面临着网络安全挑战，如数据泄露、拒绝服务、不安全的外部应用程序、远程身份管理等，这些都可能阻碍云的采用和部署。为了利用云进行创新和发展，企业需要内部或外部专家资源来正确规划、设计、构建和实施强大的云计算环境和支持策略。

精简合规性

遵守政府和数据隐私条例是很棘手的，其结果通常是为了避免风险而抑制企业发展和扩张。尤其是，如果企业没有内部网络安全专家来降低这种风险，为企业发展和扩张铺平道路。

企业可以在保持强有力的安全态势的同时实现合规性。但是，企业很难跟上不断变化的威胁和保护标准，以及了解这些标准的含义。目前，经美国国家标准与技术研究所（NIST）批准的用于资源保护的加密技术 FIPS 140-3 正在进行更改。接下来，物联网（IoT）的普及以及正确识别“物”的有效性或潜在威胁，将引起高度关注。

在这个不断变化的环境中，灵活调整和优化合规性环境比以往任何时候都更加重要，以便公司能够通过创新产品和扩大业务范围不断发展。然而，开发有效的计划和部署正确的安全技术增加了复杂性。成功的企业需要进行风险分析，制定策略和规程，选择正确的安全技术，部署云、本地、虚拟设备或混合解决方案，测试解决方案，以确保合规性。

采用新视角看待网络安全

网络安全和创新是密不可分的，但很多企业并没有把两者联系起来。为编制其《2019 年网络战略路线图报告》，Gartner 要求 IT 基础设施和运营（I&O）领导人说明其企业最重要的目标。调查显示，创新并不是企业的首要任务，只有 19% 的受访者将创新排在第二或第三位。毫不奇怪，提高网络质量和降低成本是最重要的两大目标。

这与思科最近的一项调查《网络安全推动发展：关键发现》的结论一致。在这项调查中，71% 的公司高管认为，网络安全风险阻碍了公司的创新。同样，39% 的高管表示，出于对网络安全的担忧，他们搁置了关键任务计划。

目前，与网络安全相关的负面因素通常是企业的关注点，即保护数据的关键需求和所需的间接成本。但网络安全也有其优势，即能够为企业赋能，使企业在激烈的竞争和数字化进程中加速发展。

原文名称	How cybersecurity accelerates business growth
作者简介	Peter Bello。Peter Bello 是 Cygnacom Solutions 公司总裁。
原文信息	2019 年 10 月 21 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2019/10/21/cybersecurity-accelerates-business-growth/
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。