安天发布《Mehdi 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一个名为 Mehdi（又名 Tor+）的勒索软件变种，该勒索软件隶属于 Sorus 勒索软件家族，此家族于 2019 年 11 月被发现，主要通过钓鱼邮件进行传播，邮件附件中包含一个名为 SF.exe，签名为 Tor+ 的勒索程序，邮件内容诱使用户运行该勒索程序。

Mehdi 勒索软件执行后，加密计算机上的可执行程序和文档文件，在原文件名后追加名为“.Tor+”的后缀，在含有被加密文件的位置创建名为“ReadME-Unlockme501@protonmail.ch.txt”的勒索信，在桌面弹出标题为 Tor+ 的勒索提醒对话框，勒索信内容包含勒索说明、联系邮箱和 USER_ID 等，勒索提醒比勒索信更加直观的告知受害者已被加密，还包含如何购买比特币教程。Mehdi 勒索软件使用“AES+RSA”加密算法加密文件，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等。目前被加密的文件在未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口令；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、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据关联分析鉴定器、关联分析鉴定器将文件判定为木马程序。

◆概要信息

文件名	df3c756f7fe7996693d9fb384938b65b29cadefabdb96284501e0735f1b74e8b
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	172 KB
MD5	30D47318531D58B03AF35E6BEA1505DA
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Ransom
判定依据	BD 静态分析

◆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

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
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）	★
获取系统版本	★
检测自身是否被调试	★★
镜像劫持	★★
检索系统内存信息	★
获取计算机名	★
.....	.....

◆进程监控

PID	创建	命令行
1424	target.exe	"c:\7727b2c0158240d2945c5e6dc5fe18c3\share\target.exe"
1848	cmd.exe	"cmd.exe" /c vssadmin.exe delete shadows /all /quiet
1920	vssadmin.exe	vssadmin.exe delete shadows /all /quiet

◆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 12 月 30 日 (总第 214 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

【寒夜远征】第七届安天网络安全冬训营即将启幕

网络空间威胁对抗与防御技术研讨会暨第七届网络安全冬训营——“寒夜远征”将于 2020 年 1 月 8、9 两日在黑龙江太阳岛花园酒店（全总哈尔滨劳模技能交流基地）举行。

本届冬训营基本情况介绍

2019 年，威胁框架在更多文献中已经取代了杀伤链模型，成为描述攻击活动的通用语言。一年前 Cyber Threat Framework 2.0 的发布、修订以及 ATT&CK 不断的演进完善，形成了极为理想的公共模型与知识基础。安全厂商围绕威胁框架，在威胁建模、威胁检测、安全能力评估、防御体系完善、TTP 情报共享等方面进行了多种实践。

威胁框架借鉴杀伤链模型，对攻击过程的全生命周期的建模和行为动作的原子化拆解，建立了描述网络安全威胁活动的通用原则以及对威胁动作的严谨分类方法，使之能够更全面且细粒度的，通过统一的原则描述威胁活动。通过威胁框架，不同的人员、团队可以在统一的话语体系中实现协同和分享，对推动威胁分析、研判、情报共享和防御体系的完善都有极为关键的价值。

在上一届安天网络安全冬训营上，安天已经从多个角度介绍了威胁框架的理念和价值。在今年安天发布的重点报告《安天发布“方程式组织”攻击中东 SWIFT 服务商事件复盘分析报告》《震网事件的九年再复盘与思考》中，均对相关事件从威胁框架视角做了映射和解析。自 2019 年 6 月 30 日，安天从引擎到主线的端点防护、流量监测、威胁分析产品，均支持对威胁框架（双标支持 ATT&CK 和 CTF）知识标签的输出，并在态势感知平台中完成了标签整合。但对于如何更深入的理解威胁框架，有效发挥威胁框架在威胁分析、事件研判、情报分享、防御指引中的作用，还有太多工作需要做。对威胁框架，我们也产生了更多的思考，也包括迷惑。

因此我们将本届冬训营主题定为“威胁框架：认知与实践”，希望结合工作中的探索，分享和共商对威胁框架安全价值的理解和实践思考。我们会围绕用户的关切，分析来自不同层级威胁行为体的攻击事件，介绍在检测引擎、端点防护、流量监测、深度分析、态势感知等方面威胁框架的结合进展，及在重要信息系统和关键基础设施中建立有效防御体系的探索实践。

往届冬训营回顾

自 2014 年起，在相关主管部门和职能机构指导下，安天以“直面实际威胁，形成价值落地”为导向，连续承办了六届网络安全冬训营。根据年度网络安全形势和工作主题，安天为每届冬训营设定了四字营语，分别是：“凛冬将至”、“北风乍起”、“朔雪飞扬”、“冰峰屹立”、“红旗漫卷”和“铁流鏖战”。本届冬训营，营语为“寒夜远征”。

从 2016 年开始，为了让议题内容更为聚焦，安天决定每届冬训营围绕一个核心主题进行。第三届冬训营主题为“情报的支撑，塔防的实践”，探讨了如何构建有效的纵深防御体系；第四届冬训营以“有效防护，价值输出”为主题，自我批判作为安全厂商和研究者的主观局限和技术优越感，回归安全技术为用户提供有效的防护能力和价值保障的本质；第五届冬训营主题为“敌情想定是前提，网络安全实战化”，旨在以客观充分的敌情想定为前提，以实战化作为网络空间安全防御的要求，让安全技术、产品与服务能够随时应对真实的威胁，为客户实现有效的安全价值。第六届冬训营主题为“战术型态势感知指控积极防御；协同响应猎杀威胁运行实战化”，分享战术型态势感知的探索实践，及在客户侧安全规划、能力集成、威胁应对、应急响应等方面的经验。

在过去的几届冬训营上，来自政企机构、安全研究机构、知名大学和安全厂商的演讲嘉宾与安天的工程师，共同分享研讨网络安全领域的前沿探索和工作心得。相关议题对充分认识网空敌情，深入了解高级威胁，让网络安全技术能力转化为有效客户价值，产生了积极的作用，受到相关机构和行业领域专家的好评。随着网络强国战略的不断推进实施，网络安全所面临的风险挑战也会更加严峻，对能力型网络安全企业的使命要求也在不断提高。从与恶意代码对抗的小闭环，走向全面赋能客户、助力客户建设防御体系，有效实现威胁对抗大闭环，对安天人来说是一个艰难的过程，也是必须完成的突破。这也是我们把本届冬训营营语定为“寒夜远征”的原因，“寒夜”是严峻的安全威胁挑战，“远征”是我们达成目标的信念与行动。

安天与客户携手，智者安天下，共同创造网络安全防御的未来。

报名方式

请通过冬训营官网（wtc.antiy.cn）或关注安天官方微信公众号了解报名方式及会议详情。

会务组联系人：齐磊

联系方式：0451-87805059，18646141007

微信扫描二维码阅读原文

每周安全事件

类 型	内 容
中文标题	Citrix 中的漏洞导致全球约 8 万家公司可能面临风险
英文标题	Citrix Vulnerability Puts 80000 Companies from Around the World at Risk
作者及单位	Bill Toulas
内容概述	Positive Technologies 的安全专家 Mikhail Klyuchnikov 发现了一个超危漏洞，该漏洞影响 Citrix Application Delivery Controller 和 Citrix Gateway。正如研究人员所声称的，该漏洞可以被利用，使攻击者能够通过任意代码执行远程访问本地公司网络，而无需访问帐户或了解凭据。漏洞跟踪为 CVE-2019-19781，它的危险等级为超危（在 CVSS 上为 10）。受影响的产品被 158 个国家的约 80000 家公司使用。这个特殊的漏洞可能刚刚被发现，但它已经存在了大约五年半，黑客只需要一分钟就可以利用它。Citrix 正在就此问题通知其客户，并提出了一套缓解措施，因为目前还没有补丁程序。
链接地址	https://www.technadu.com/citrix-vulnerability-80000-companies-around-the-world-at-risk/88242/

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.Triout.b[prv,spy] 2019-12-22	高	该应用程序是一款间谍软件，运行后窃取用户短信、联系人、通话记录、地理位置、浏览器历史记录、手机存储文件、社交软件记录等大量隐私信息，私自拍照、录音、录像，监听通话和短信，并将隐私信息上传至服务器。造成用户隐私泄露，建议立即卸载。
		Trojan/Android.SmsSpy.cq[prv] 2019-12-23	中	该应用程序伪装为系统应用，运行隐藏图标，获取用户短信并转发至指定邮箱，造成用户的隐私泄露，建议卸载。
		Trojan/Android.FakeJioPrime.b[exp,spr] 2019-12-24	低	该应用程序伪装正常程序，无实际功能，运行私自群发推广链接短信，访问推广网页诱导用户下载安装，会造成用户资费损耗，请卸载。
	较为活跃样本	Trojan/Android.emial.ha[prv,rmt]	中	该应用程序伪装其他应用，运行隐藏图标，后台私自发送短信到指定号码，接收远程短信指令窃取用户短信，会造成信息泄露和资费消耗，建议卸载。
		Trojan/Android.SmsSpy.cp[prv,exp]	中	该应用程序运行后监听用户短信并发送到指定号码，还会删除用户短信，造成用户隐私泄露和资费损耗，建议卸载。
		RiskWare/Android.SexApp.dm[rog,exp]	低	该应用程序包含色情内容，可能影响用户身心健康，请注意提示信息，使用健康绿色软件。
		RiskWare/Android.xiaoqibocai.a[rog]	低	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。
		G-Ware/Android.HiddenAds.jz[exp,rog]	低	该应用程序运行后隐藏图标，后台推送广告，造成用户资费损耗，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 远程桌面协议 (RDP) 拒绝服务漏洞（CVE-2019-1453）	高	Windows 远程桌面协议 (RDP) 存在一个拒绝服务漏洞，攻击者可通过 RDP 连接并发送经过特殊设计的请求来触发此漏洞。成功利用此漏洞的攻击者，可能导致目标系统 RDP 服务停止响应。
	较为活跃样本	Trojan[Spy]/Win32.Zbot	中	此威胁是一种能够进行远程控制、组建僵尸网络、窃取用户信息的间谍类木马程序。该家族会窃取被感染电脑的重要信息，并生成工具包。该工具包允许黑客获得更高权限来远程控制电脑。
		Trojan[Downloader]/Win32.Genome	中	此威胁是一种具有下载行为的木马类程序。该家族能修改被感染电脑的注册表，损坏、删除系统文件。该家族还可以设置后门，修改用户电脑的浏览器设置等。该病毒可以随电脑开机自启动。
		Trojan[PSW]/Win32.Tepfer	中	此威胁是一种盗号类木马程序。该家族样本运行后会盗取被感染计算机上的用户账户信息（用户名、密码等）。该家族能通过垃圾邮件、可疑链接、恶意网站等途径传播。该家族可以修改计算机的系统设置，更改或删除重要文件，捆绑间谍软件、恶意软件及广告件等，使系统性能下降。
		GrayWare[AdWare]/MSIL.DomaIQ	低	此威胁是一种广告类程序。DomaIQ 是一个安装管理器，它可以管理你要安装或更新的软件，其中包括工具栏、浏览器加载项、游戏应用程序等。该家族是广告插件的一种。
		Trojan/Win32.Badur	低	此威胁是一种木马类程序。该家族通过向用户系统中下载、安装大量应用程序获利，如百度卫士、YYMusic、知乎客户端等。用户系统中因安装大量应用程序而导致系统变慢，CPU、内存及网络资源等被大量占用。

2020 年十大安全措施

Joshua Goldfarb/ 文 安天技术公益翻译组 / 译

在 2020 年即将来临之际，很多人开始制定新一年的安全措施了。虽然只有一部分人能够坚持自己的措施，但是我们可以从这种实践中学到一些知识。本着这种精神，我提出了企业应该在 2020 年制定并保持的十大安全措施。

关注风险

在大学期间学习物理时，我经常会陷入困境。当我寻求帮助时，我得到的答案通常是“回到第一原则”。最终，我学会了这一点，不再需要旁人提醒。网络安全也不例外。当我们陷入困境时，我们需要回到第一原则，即关注风险。更具体地说，这涉及衡量、最小化、管理和减轻风险。关注风险可以帮助安全企业评估其安全策略，使企业了解这些策略是否有助于其规避遇到的安全风险。

具有战略性

在观看网球比赛或乒乓球比赛时，人们通常会盯紧传来传去的球。然而，安全计划是不同的。在安全领域中，不乏让人分心的事物，它们会吸引我们的注意力并使我们脱离焦点。无论是新危机、新建议、热门技术，还是我们可能遇到的其他干扰，我们都需要战略性地思考和执行。我们应该明确定义愿景和策略，并且根据每个决策对愿景和策略的支持程度对其进行评估。通过这种方法，企业可以投资于改善安全状况的活动，同时最大程度地减少对非此类活动的投资，从而增强其安全态势。

制定计划

我们都知道，如果想要出差，就要制定计划。我要去哪里？要参加什么会议？此行的目的是什么？住在哪里？是否收集了所需的所有资料？这是我们出差之前可能会考虑的部分问题。网络安全领域需要相同的方法。很多安全团队没有制定计划，不清楚其受众、目标、所需工具以及需要完成哪些工作。新年伊始，制定计划是一个好方法。

执行计划

如果不能执行计划，那么制定计划也没什么用了。计划不仅要具有战略性，而且要执行。根据分配的预算，将每个战略计划分解为能够在期望时间内实施的运营和战术部分。未能制定详细的计划，可能会导致安全企业无法实现其愿景。当然，这也不利于安全团队保护企业。执行安全计划，能够将“增强安全性”的愿景转变为现实。

度量

“度量标准”已成为不受整个安全行业待见的词汇。不应该这样的！事实上，精心设计的度量标准可以帮助安全企业评估和衡量风险、性能以及许多其他指标。度量标准具有许多优点，但其主要优点是：能够评估安全计划的进展并根据需要进行调整，以及向领导和高管展示安全计划的价值。设计更好的度量标准，有助于企业增强安全性。

减少“噪音”

不幸的是，很多安全企业总是被“噪音”困扰。如果不加以检查，误报、干扰以及其他形式的噪音会使大多数安全团队难以招架。增强聚焦，减少干扰，改善工作队列和工作环境，有助于安全团队履行防卫企业的职责。

实施最佳实践

安全行业中似乎有很多关于最佳实践的话题。“说”和“做”可不是一回事。对企业来说，知道最佳实践而不实施，是无法改善其安全状况的。如果企业认为最佳实践对其有帮助，那么请投入资源予以实施。否则，请停止谈论最佳实践，并转向你认为有助于企业安全运营的内容。实施适当的最佳实践，可以帮助企业改善其安全状况。

不要过度分析

我经常看到安全团队不堪重负，这让我很惊讶。虽然我们当然不希望做出在逻辑和理由上缺乏基础的快速决策，但我们也不想过度分析每个决策。对每个决策进行适当分析，可确保安全团队不会一时冲动，也不会因过度分析而不堪重负。

放弃陈旧知识

安全领域有很多旧知识。其中一些是真正的智慧；而其他的则是长期存在的信念，并没有什么根据。如果一条知识被证明是有效的，并且可以衡量其可行性，那么企业应该遵守它。否则，则应该放弃它。这有助于企业建立安全程序并进行改进。

要有自知之明

人贵有自知之明。大多数人和企业都无法以值得信任的局外人视角看待自己。虽然要实现这种自省并不容易，但这是非常有必要的。只有当我们退后一步，看到我们所有的优势和缺点时，我们才能开始朝着更好的安全态势迈进。如果我们无法诚实地看待自己，则可能需要寻求外部资源来做这一点。以局外人的视角看待自己，是加强信息安全防御的第一步。

原文名称	Top Ten New Year's Security Resolutions
作者简介	Joshua Goldfarb。Joshua Goldfarb 是一位经验丰富的信息安全领导者，他帮助企业完善和改进其安全计划。
原文信息	2019 年 12 月 18 日发布于 Security Week 原文地址 https://www.securityweek.com/top-ten-new-years-security-resolutions
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。