安天发布《DeathRansom 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 DeathRansom 的勒索软件，DeathRansom 勒索软件最早于 2019 年 11 月 19 日被发现，主要通过垃圾邮件和恶意软件进行传播。该勒索软件目前发现有两代变种，第一代只修改后缀名，不对文件进行加密；第二代不修改后缀名，直接对文件和可执行程序进行加密。

第一代 DeathRansom 勒索软件运行后，在原文件名后追加名为“.wctc”的后缀，但将追加的后缀名删除后，即可恢复文件正常使用，不会造成任何影响；第二代 DeathRansom 勒索软件伪装成闹钟形式的图标，运行后不对计算机内的文件和可执行程序后缀名进行修改，直接进行加密，导致加密后的文件无法正常运行或读取，并在桌面生成名为“read_me.txt”的勒索信，勒索信内容包含勒索说明、USER_ID、比特币支付地址、购买比特币的教程和邮箱联系方式等。DeathRansom 勒索软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、关联分析鉴定器、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、来源信息鉴定器、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、关联分析鉴定器、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	13d263fb19d866bb929f45677a9dcbb683df5e1fa2e1b856fde905629366c5e1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	293 KB
MD5	8EA78E5A123C13C3BDA144D0FCF430C0
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Agent
判定依据	BD 静态分析

◆ 操作系统

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
加载运行时 DLL	★
疑似桌面控制	★

◆进程监控

PID	创建	命令行
1320	target.exe	"c:\87039776143d4fa2bcc3dcc68933ad87\share\target.exe"

◆衍生物分析

文件名	文件 MD5	家族相似性	yara 扫描
1320-1.dmp	2f16c2364eeba62d245cec5694bc3527	N/A	N/A

◆ TCP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1032	192.168.122.61	139

◆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 02 日 (总第 210 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

浅谈对《网络安全威胁信息发布管理办法（征求意见稿）》的理解

2019 年 11 月 20 日，中央网信办发布《网络安全威胁信息发布管理办法 (征求意见稿)》（以下简称《办法》）。该《办法》出台是落实《网络安全法》的重要举措。《办法》对发布涉及计算机病毒、网络攻击、网络侵入、网络安全事件等可能威胁网络正常运行活动的相关安全威胁信息，以及包括系统漏洞、网络风险等在内的可能暴露网络脆弱性的安全威胁信息，从发布内容、发布流程、发布方法等方面，对研究机构、网络安全厂商、个人研究者，以及信息发布平台运营单位做出了较为具体的规范。《办法》兼顾了既要确保信息发布有利于防范网络安全威胁和风险，推动政企机构和公众了解威胁和风险并进行处置响应，又要避免不当发布引发消极后果。

网络威胁信息发布是网络安全厂商、应急组织、研究机构和个人研究者通过分析研究深入了解威胁，并进行公开信息披露的过程。这些公开披露的信息，是公众和相关人员了解威胁机理、背景、影响面、应对方法等信息的重要来源，有助于网络安全运维人员制定应对决策、作出前置准备、应对攻击后果、展开响应处置。在面对网空威胁行为体对我国的高级攻击活动中，全面的、高质量的分析报告，亦曾起到过迫使攻击者在一段时间内收敛攻击活动的效果。因此，网络威胁信息发布是网络安全工作中一个非常重要的环节，但也存在着一些“双刃剑”的问题。

从内容上来看，部分威胁信息发布，基于攻击者的攻击视角教程化详尽展开，导致成为攻击示范。少数分析中直接包含了原始攻击载荷，可能导致二次扩散和感染的风险。还有的针对具体的信息系统和业务系统漏洞，公开了攻击入口和攻击方法，可能诱发攻击。甚至可能导致产生一些攻击方的自动化攻击手段，可以直接机读导入攻击入口，进行自动化攻击。此次公布的《办法》对类似的情况进行了约束和限制，明确列出威胁信息不得包含的细节内容，意在全面降低威胁信息发布的负面风险。

从威胁信息发布时机和流程上看，如果信息发布从发现、上报到公开没有给原厂商、相关资产管理运维方，以及主管部门、应急响应部门留有足够的处置和协调响应时间，这种不加以约束和限制的发布可能会加剧风险。少数严重漏洞，机理并不复杂，即使没有披露细节，一旦存在线索提示，就很容易被猜测找到。如果不能给原厂商留有足够的制作和发布补丁的时间，不能给主管部门和应急机构留有足够的响应修复的时间，漏洞信息披露就可能产生负面效果。不但没有起到发布信息本身原有的缓解漏洞的初衷，反而还可能加速了漏洞被多方攻击者利用的过程。还有一些设备和系统陈旧的关键信息基础设施，存在一些机理性的漏洞，修复代价成本极大，甚至不全面替换就无法修复，如果此类威胁信息大面积公开，就会触发较为严重的连锁问题。此次公布的《办法》，对威胁信息的发布流程，按照区域、行业领域分门别类予以规范，尤其是兼顾各方合法利益，对涉及具体网络和信息系统存在的风险、脆弱性情况如何发布做出了具体规定，在一定程度上降低了威胁信息发布带来的关联性和次生性灾害的可能性。

从影响方面看，部分安全威胁披露，经过带有商业目的的传播和媒体的炒作后，威胁风险或实际威胁后果被夸大，容易引起无谓的恐慌，加大了社会成本消耗，而且反复下去，容易引发“狼来了”的效应，导致企业和个人对威胁信息的重视程度反而下降。例如早在 1992 年初，就有类似情况出现，“米开朗基罗”（Michelangelo）病毒开始传播，一家美国公司声称 3 月 6 日病毒爆发时，将有超过 500 万台电脑上的数据被破坏，一时间造成了公众恐慌，但实际上感染“米开朗基罗”病毒的电脑大概只有 1 万台左右。类似事件影响了公众对威胁信息披露的信任。《办法》对此也做出明确规定，要求发布信息“应坚持客观、真实、审慎、负责的原则，不利用网络安全威胁信息进行炒作、牟取不正当利益或从事不正当商业竞争”。受该原则约束，在发布网络安全威胁信息时，不能使用带倾向性的语言，不能夸大威胁的影响范围、影响程度，不能出于商业竞争目的，发布不利于竞争对手的信息。此外，《办法》还对“预警”一词使用做出了明文规定：“未经政府部门批准和授权，任何企业、社会组织和个人发布网络安全威胁信息时，标题中不得含有‘预警’字样”。这一规定并非不允许各方发布风险提示，而是限定不得随意使用“预警”两字。事实上，网信办早在 2017 年出台《国家网络安全事件应急预案》文件，已对网络安全事件“预警”的级别、监测、研判、发布和响应做出了明确规定，从中可以看出网络威胁“预警”是一种严肃的国家行政行为，而不应是任何企业、组织和个人可以随意使用甚至用于炒作的概念。

在国家相关部门授权机制下，形成威胁信息发布的规范机制，加强管理，提高网络安全防护水平，是各国的普遍作法。美国已出台了一系列威胁信息披露管理法案，英国也有一整套的“披露漏洞公平裁决策略和流程”。网信办此次出台的《办法》，是希望对威胁信息发布工作形成明确的导向和指引，确保威胁信息发布真实准确，确保信息发布者对内容负责，确保威胁信息发布能达成良好的初衷，保证网络和信

（下转第三版）

每周安全事件

类 型	内 容
中文标题	黑客组织利用暴露的 API 端点劫持 Docker 系统
英文标题	A hacking group is hijacking Docker systems with exposed API endpoints
作者及单位	Catalin Cimpanu for Zero Day
内容概述	研究人员发现自 11 月 24 日开始，一个黑客组织正在互联网上进行大规模扫描，来寻找暴露的 API 端点劫持 Docker 系统。黑客组织使用 Alpine Linux 映像创建了一个容器，通过扫描向 Docker 实例发送命令，以在公司的 Docker 实例上部署加密货币挖矿恶意软件，从而获取资金。该黑客组织目前正在扫描的数量已超过 59,000 个 IP 网络。
链接地址	https://www.zdnet.com/article/a-hacking-group-is-hijacking-docker-systems-with-exposed-api-endpoints/

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.yingzi.b[prv,spy] 2019-11-25	高	该应用程序是一款间谍软件，运行后隐藏图标，后台窃取用户短信、联系人、通话记录、地理位置、以及 QQ 和微信聊天记录、手机固件信息，私自截屏、通话录音、拨打电话、监听用户短信和通话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。
		Trojan/Android.huanji.b[exp,rog] 2019-11-26	中	该应用程序包含恶意代码，运行联网获取主流杀毒软件列表，逃避检测、实现免杀，后台发送大量网络请求、恶意刷量并联网统计感染设备数量，造成用户资费消耗，建议卸载。
		G-Ware/Android.jianmo.dc[rog,lck] 2019-11-27	低	该应用程序是一款勒索软件，运行后要求用户添加指定 QQ 解除，影响用户手机的正常使用，建议不要使用。
	较为活跃样本	Trojan/Android.konni.a[prv,rmt,spy]	中	该应用程序是一款间谍软件，运行后隐藏图标，接收远程控制指令，窃取用户短信、联系人、通话记录、键盘记录、应用安装信息、SD 卡目录，私自录音、截屏、下载安装其他软件、发送短信、删除文件和短信。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。
		Trojan/Android.Rootnik.ao[exp,sys,rtt]	中	该应用程序包含风险代码，运行私自下载恶意子包动态加载，联网下载提权文件私自提权，会造成用户流量资费损耗，请卸载。
		Trojan/Android.EvilInvisible.b[exp,rog]	中	该应用程序内嵌恶意代码，私自下载恶意子包动态加载。模拟点击广告，恶意刷量，会造成用户资费损耗，请卸载。
		Trojan/Android.FakeCJ.b[pay,fra]	中	该应用程序伪装游戏刷券应用，诱导用户充值购买和分享，会造成用户财产损失，请卸载。
		RiskWare/Android.linkedfunbocai.a[rog]	低	该应用程序是线上博彩游戏，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。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Windows Media Foundation 远程代码执行漏洞（CVE-2019-1430）	高	当 Windows Media Foundation 不正确地分析经特殊设计的 QuickTime 媒体文件时，会触发远程执行代码漏洞。成功利用此漏洞的攻击者会获得与本地用户相同的用户权限，若要利用该漏洞，攻击者必须向用户发送一个经特殊设计的 QuickTime 文件，然后诱使用户打开该文件，QuickTime 文件将在目标系统上执行攻击者设计的恶意代码。
	较为活跃样本	Trojan[Ransom]/Win32.Crusis	中	此威胁是一个勒索软件家族。该家族的样本在执行后会加密系统中的文档，并将用户的唯一标识码传送到 C&C 服务器，随后改变用户的桌面并留下勒索信，以解密数据为由勒索比特币。
		Trojan[Exploit]/Win32.UACSkip	中	此威胁是一类木马家族。该类家族的样本具有同样的特征，即利用了跳过 UAC 的机制来入侵系统，执行后续的恶意行为。
		Trojan/Win32.Brodcom	中	此威胁是一类木马家族。该家族的样本在运行后在后台收集数据、处理并发送给远程控制服务器，并接受远程服务器的控制。
		Trojan/Win32.AntiAV	中	此威胁是一个木马家族。该家族的样本在执行后会按照硬编码的列表和特征破坏系统中的杀毒软件，使得杀毒软件无法正常运行。
		Trojan/Win32.Remtas	低	此威胁是一种木马类程序。该家族样本添加开机自启，拖慢计算机速度。

（上接第一版）

息系统的脆弱性得到及时修复，减少发生关联性和次生性灾害的可能性，具有十分重要的现实价值和意义。《办法》在起草过程中，组织了广泛的讨论，对于安全研究者和安全厂商担心的，是否会影响威胁信息发布的及时性、全面性，影响安全研究的积极性以及相关边界难以把握等问题也进行了一定的完善和修订。经过调研、讨论和调整，在总体上兼顾了威胁发布的需求以及潜在风险问题，考虑了多方面意见，从而进入到发布征求意见稿，更广泛征集公开意见阶段，可以获得更多的修订意见和相关的反馈，对于其中可能存在争议点，特别是关于细节披露尺度和时间周期规定的合理性，各方也有机会进行进一步的研讨，从而推动《办法》的进一步完善和细化。同时也需要看到，网络安全威胁信息发布涉及到法律、技术、道德、产业、竞争等诸多方面，相关机制建立很难一蹴而就，还需要在今后实践中进一步细化、磨合与改进。

微信扫描二维码阅读原文

网络安全威胁信息发布管理办法（征求意见稿）

第一条 为规范网络安全威胁信息发布行为，有效应对网络安全威胁和风险，保障网络运行安全，依据《中华人民共和国网络安全法》等相关法律法规，制定本办法。

第二条 发布网络安全威胁信息，应以维护网络安全、促进网络安全意识提升、交流网络安全防护技术知识为目的，不得危害国家安全和社会公共利益，不得侵犯公民、法人和其他组织的合法权益。

第三条 发布网络安全威胁信息，应坚持客观、真实、审慎、负责的原则，不利用网络安全威胁信息进行炒作、牟取不正当利益或从事不正当商业竞争。

第四条 发布的网络安全威胁信息不得包含下列内容：

（一）计算机病毒、木马、勒索软件等恶意程序的源代码和制作方法；

（二）专门用于从事侵入网络、干扰网络正常功能、破坏网络防护措施或窃取网络数据等危害网络活动的程序、工具；

（三）能够完整复现网络攻击、网络侵入过程的细节信息；

（四）数据泄露事件中泄露的数据内容本身；

（五）具体网络的规划设计、拓扑结构、资产信息、软件源代码，单元或设备选型、配置、软件等的属性信息；

（六）具体网络和信息系统的网络安全风险评估、检测认证报告，安全防护计划和策略方案；

（七）其他可能被直接用于危害网络正常运行的内容。

第五条 发布网络和信息系统被攻击破坏、非法侵入等网络安全事件信息前，应向该事件发生所在地地市级以上公安机关报告。各级公安机关应及时将相关情况报同级网信部门和上级公安机关。

第六条 任何企业、社会组织和个人发布地区性的网络安全攻击、事件、风险、脆弱性综合分析报告时，应事先向所涉及地区地市级以上网信部门和公安机关报告；

发布涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的网络安全攻击、事件、风险、脆弱性综合分析报告时，应事先向行业主管部门报告；

发布全国性或跨地区、跨行业领域的综合分析报告时，应事先向国家网信部门和国务院公安部门报告。

第七条 未经政府部门批准和授权，任何企业、社会组织和个人发布网络安全威胁信息时，标题中不得含有“预警”字样。

第八条 发布具体网络和信息系统存在风险、脆弱性情况，应事先征求网络和信息系统运营者书面意见，以下情况除外：

（一）相关风险、脆弱性已被消除或修复；

（二）已提前 30 日向网信、电信、公安或相关行业主管部门举报。

第九条 通过下列平台发布信息的，平台运营者、主办单位接到有关部门通报、用户举报，或自行发现平台上存在违反本办法的发布行为和发布内容的，应当立即停止发布、采取消除等处置措施，防止违规内容扩散，保存有关记录，并向地市级以上网信部门、公安机关报告。

1. 报刊、广播电视、出版物；
2. 互联网站、论坛、博客、微博、公众账号、即时通信工具、互联网直播、互联网视听节目、应用程序、网络硬盘等；
3. 公开举行的会议、论坛、讲座；
4. 公开举办的网络安全竞赛；
5. 其他公共平台。

第十条 违反本办法规定发布网络安全威胁信息的，由网信部门、公安机关根据《中华人民共和国网络安全法》的规定予以处理。

第十一条 涉及国家秘密、涉密网络的网络安全威胁信息发布活动，按照国家有关规定执行。

第十二条 本办法所称网络安全威胁信息，包括：

（一）对可能威胁网络正常运行的行为，用于描述其意图、方法、工具、过程、结果等的信息。如：计算机病毒、网络攻击、网络侵入、网络安全事件等。

（二）可能暴露网络脆弱性的信息。如：系统漏洞，网络和信息系统存在风险、脆弱性的情况，网络的规划设计、拓扑结构、资产信息、软件源代码，单元或设备选型、配置、软件等的属性信息，网络安全风险评估、检测认证报告，安全防护计划和策略方案等。

第十三条 本办法自发布之日起实施。

（来源：中国网信网）