安天发布《Maze 勒索病毒变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Maze 勒索病毒的变种，该变种病毒名叫 ChaCha 勒索病毒，最早出现于 2019 年 5 月，擅长使用 FalloutEK 漏洞利用工具通过网页挂马等方式传播，被挂马的网页，多用于黄赌毒以及某些软件内嵌的广告页面等。

Maze 勒索病毒通过大量混淆代码来对抗静态分析，并且使用 RSA+Salsa20 方式加密文件，加密完成后对文件添加随机扩展后缀，被加密后的文件包含以下三部分内容：被加密内容 + 被加密的文件密钥之后创建名为 DECRYPT-FILES.html 的勒索信，勒索信的内容告诉受害者文件被加密，并且留下了作者的电子邮箱，提供付款指南等，勒索信的最后是一个 Base64 编码的字符串，其中包含加密的私有解密密钥和受感染计算机的信息，勒索信指明，在发送电子邮件给勒索软件作者时，必须发送此文本，值得一提的是 Maze 变种与其它勒索病毒不同的是解密赎金额度取决于被感染电脑的重要程度（个人电脑，办公电脑，服务器），这意味着高价值系统受攻击后解密付出的代价也会相应的更高，目前被加密的文件在未得到密钥时暂无法解密。勒索病毒给企业和个人的数据安全带来了严重的威胁，一旦主机被入侵，主机中的文件都有可能被加密，而且被加密文件将难以恢复，因此防护显得极为重要。安天建议广大用户，不要将数据安全立足于加密后的数据恢复，应该安装杀毒、防毒软件（参考安天智甲工具）并及时升级系统和修补设备漏洞；对重要的数据文件进行备份，避免弱口令的使用，避免使用统一的密码。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。

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、文件来源信息鉴定器、数字证书鉴定器、文件元数据鉴定器、动态(Win7 x86) 鉴定器、反病毒引擎鉴定器、动态(WinXP) 鉴定器、聚美分析鉴定器、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	9d86beb9d4b07dec9db6a692362ac3fce2275065194a3bda739fe1d1f4d9afc7
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	351 KB
MD5	A0DC59B0F4FDF6D46569468654 33BCCE
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Fuerboos
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/_lk/details.html?hash=A0DC59B0F4FDF6D4656946865433BCCE

◆ 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

◆危险行为

行为描述	危险等级
延时	★★★
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
枚举进程	★
获取计算机名	★
获取驱动器类型	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
创建特定窗体	★
创建挂起进程	★★
访问文件尾部	★
获得计算机用户名	★
文档篡改	★★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 06 月 17 日 (总第 187 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

ICT 供应链安全，我国该如何管理？

安天研究院院长 陈晓桦

当今世界，不仅是国防军事武器系统，几乎所有的涉及国计民生的关键基础设施对微电子、计算机、通信等信息通信技术（以下简称 ICT）的依赖程度越来越高。在 ICT 采购全球化的态势下，ICT 供应链安全与国家安全的关系愈发密切，可以认为，ICT 供应链是所有供应链的基础，是“供应链的供应链”。供应链涉及的不仅仅是 ICT 的公共技术，石油、矿产、粮食、以及衣食住行都存在全球资源的配置问题。供应链安全早在几十年前就已经在国外被提出，当时西方国家对矿产、石油、粮食跨境的海陆空运输和进出口都实行了精细化的控制，而近年尤其是美国对我国中兴、华为等公司的“断供事件”又使得对 ICT 供应链的安全问题的关注逐渐增多，但大多数讨论都集中在供应链断供的严重性方面。

鉴于国家关键基础设施和重要资源 (Critical Infrastructure and Key Resources, CIKR) 对 ICT 技术的依赖，通过国家安全审查识别和控制 ICT 供应链风险成为保障国家安全的重要手段。国外的做法通常是利用与外国投资相关的国家安全审查手段，我国则是利用网络安全审查的方式，这在我国的《国家安全法》中有所提及，网络安全审查是国家安全审查在关键信息基础设施保护方面的延伸。

一、 ICT 供应链的概念

ICT 供应链，按照我国的国家标准 GB/T36637-2018 定义，即 ICT 产品和服务的供应链，是指“为满足供应关系通过资源和过程将需方、供方相互连接的网链结构，可用于将信息通信技术的产品、服务提供给需方。”而 MITRE 公司向美国防部（DoD）提出的供应链安全战略咨询的定义是指“从开发到将产品或服务从供应商交付给客户所涉及的组织、人员、活动、信息和资源系统。供应链‘活动’或‘运营’涉及：将原材料、组件和知识产权转化为产品，交付给最终客户；与供应商、中间人和第三方服务提供商进行必要的协调和协作。”

2019 年 5 月 2 日，32 个国家的代表在布拉格召开了 5G 安全准则讨论会

从对供应链安全管理的认识上看，美国很多的技术标准内容要比我国的更加丰富和全面。供应链结构通常是多级的，一般来说供应链有四大特点，分别是全球分布性、全生命周期、产品服务复杂和供应商多样性，其中全生命周期十分复杂，涵盖了设计与开发阶段、传统供应阶段和服务运维阶段。例如设计、开发、采购、生产、仓储、物流、销售、维护、召回等，而每个环节都有可能被篡改或控制，因此供应链安全问题是全世界很多国家都非常重视的。2019 年 5 月初，包括欧盟和北约成员国在内的 30 多个国家代表在布拉格举行 5G 网络安全会议，并达成“布拉格提案”，表示希望与会各方找到保障 5G 网络安全的办法。该提案中就提到了供应链安全问题，认为“所有利益相关方的共同责任应该推动供应链安全。通信基础设施的运营商通常依赖于其他供应商的技术，主要的安全风险来自提供 ICT 设备的日益全球化的供应链的跨境复杂性。应根据相关信息将这些风险视为风险评估的一部分，并设法防止受损设备的扩散以及恶意代码和功能的使用。”这里也专门提到了 ICT 供应链的全球化和跨境复杂性。

二、 ICT 供应链安全风险

ICT 供应链面临的安全风险主要来源于安全威胁和安全脆弱性。首先，安全风险主要包括恶意篡改、假冒伪劣、供应中断、信息泄露、违规操作和其他方面的威胁。例如恶意篡改带来的危机，是指在 ICT 供应链的设计、开发、采购、生产、仓储、物流、销售、维护、召回等某一环节，对 ICT 产品或上游组件进行恶意篡改、植入、替换等，以嵌入包含恶意逻辑的软件或硬件，具体威胁有恶意程序、硬件木马、外来组件被篡改、未经授权的配置、供应信息篡改等等。而在设计之初，是设计者留有后门还是系统存在漏洞，则比较难以区分。再比如假冒伪劣，不合格产品往往会带来严重的后果，当年美国的“挑战者号”载人航天飞船就因为隔热装备的垫圈质量不过关而燃烧坠落。供应中断是指由于人为或自然的原因，造成 ICT 产品或服务的供应量或质量下降，甚至出现 ICT 供应链中断或终止的情况。

其次，安全脆弱性主要包含供应链生命周期的脆弱性和供应链基础设施的脆弱性。供应链生命周期的脆弱性包括开发阶段、供应阶段和运维阶段三个阶段的脆弱性子集，开发阶段的脆弱性体现在如未遵循安全开发流程，没有建立完善的配置管理控制产品或组件的变更等等。供应阶段的脆弱性会来源于采购时无法识别被篡改或伪造的组件，生产环境的物理安全访问控制不严，采用了不可靠或不安全的仓储商，运输时产品被植入、篡改或替换，经销商未经授权私自预装程序等。近期华为被断供一事可以理解为是供应阶段的脆弱性表现，像华为这样的厂商，其供应链涉及的厂家往往会有近千家，一旦供应链上游厂家的供应出现问题，都会对自身的供应链以及其下游供应链或客户造成影响。

三、 国外 ICT 供应链安全管理

国外 ICT 供应链安全管理可以从战略地

（下转第三版）

每周安全事件

类 型	内 容
中文标题	垃圾邮件活动针对意大利分发 Ursnif 变种
英文标题	How Ursnif Evolves to Keep Threatening Italy
作者及单位	ZLAB-YOROI
内容概述	Yoroi 检测到 Ursnif 变种针对意大利的新攻击活动，Ursnif 通过对国家检查和大量代码混淆，提高了对目标的选择能力及其反分析能力。攻击者仍使用垃圾邮件附件的恶意 Excel 文档启用感染链，启用宏后将检索包含 Base64 编码脚本的单元格，然后开启执行一系列多层混淆的 Powershell 脚本阶段。首先对 Windows 版本进行目标选择，分为 Windows 10 和其它。对于多数 windows 版本，将下载使用 LSB 隐写技术隐藏 powershell 代码的图像，检查意大利语环境，分别执行接下来的四层加密混淆 Powershell，最终释放 Ursnif 银行木马。Windows 10 版本与其它不同的是，图片隐写命令由 Powershell 直接调用，进行两次国家检查，依次执行六层的混淆 powershell 阶段，最终释放相同载荷。
链接地址	https://blog.yoroi.company/research/how-ursnif-evolves-to-keep-threatening-italy/

每周值得关注的恶意代码信息

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.spymax.a[prv,rmt,spy] 2019-06-09	高	该应用程序是一款间谍软件，运行后隐藏图标，联网私自下载恶意间谍子包，窃取用户地理位置、wifi 信息、私自拍照、录像。造成用户隐私泄露，建议立即卸载。
		Trojan/Android.PlaytubeSpy.a[prv,rmt,spy] 2019-06-10	高	该应用程序伪装其他应用，无实际功能，程序运行会隐藏图标，监听短信拦截短信并联网上传，监听来电设置静音拦截来电并删除通话记录；连接到远程服务器获取指令执行窃取用户短信、通讯录、通话记录、位置信息、拍照截图、录音、上传下载文件等行为，造成用户隐私泄露和资费消耗。建议立即卸载。
		Trojan/Android.KotlinHrx.b[prv,exp,rmt] 2019-06-11	高	该应用程序包含风险代码，运行上传用户手机信息，接收网络远程指令，上传用户服务提供商的信息、登录信息、验证码图片，获取订阅信息并私自订阅，造成用户隐私泄露和资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.rtpkg.b[exp,rog]	中	该应用程序包含风险代码，运行后上传用户应用安装信息，加载未知子包，私自加载网页脚本，模拟点击网页广告。造成用户流量消耗，建议卸载。
		Trojan/Android.FakeSystem.be[exp,rog]	中	该应用程序伪装成系统应用，安装无图标，联网获取广告数据，后台推送广告，造成用户资费损耗，建议卸载。
		Tool/Android.rackcontroller.a[rmt,exp]	中	该应用程序是远控机架设备相关工具，程序运行会监听短信拦截指定短信，获取远控短信指令操作机架设备，私自发送短信，建议谨慎使用避免造成资费消耗。
		G-Ware/Android.Clicker.z[rog,exp]	中	该应用程序伪装游戏应用，无实际功能，运行激活设备管理器，跳转至比特币网址进行推广，会造成用户流量资费损耗，建议卸载。
		RiskWare/Android.jsgjclub.a[rog]	低	该应用程序为对虚拟货币 USDT 投资相关的应用，需要邀请码注册，可能给用户的财产带来一定风险，且难以保障财产权益，建议谨慎使用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows Office 访问连接引擎远程代码执行漏洞（CVE-2019-0945）	高	当 Windows Office 访问连接引擎未能正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。
	较为活跃样本	Trojan[Downloader]/JS.Gumblar	高	该病毒家族是一种可以下载其他恶意代码的木马家族。该家族样本通过 JS 脚本语言编写。Gumblar 最早被安全界认知是由于其利用 Adobe Flash/PDF 的漏洞传播恶意软件。该木马家族会下载恶意软件到感染者计算机上并且寻找本地 FTP 账号试图继续传播。
		Trojan[Downloader]/HTA.Agent	中	该病毒家族是一种下载者木马类程序，其格式是 HTA，HTA 是 HTML Application 的缩写（HTML 应用程序）。该家族主要目的是下载其他恶意代码到本机运行。
		Trojan[Downloader]/Win32.Walta	中	该病毒家族是一种下载广告软件的木马家族。该家族样本运行后，会在电脑中下载恶意程序并运行。该家族会修改注册表、添加启动项，以达到随系统启动的目的。
		GrayWare[AdWare]/Win32.Fourthrem	低	该病毒家族是一种有广告行为的灰色软件类程序。该家族软件运行后会在感染者的计算机的浏览器中显示广告。该家族会安装自动更新程序来获取自身的最新版本。
		GrayWare[Porn-Dialer]/Win32.AdultBrowser	低	该病毒家族是一种可以静默使用户计算机拨号导致用户付费的灰色软件家族。它可以通过用户的电话连接色情网站，这些网站一般都是付费的，以此来获取利益。

（上接第一版）

位、国际标准、ICT SCRM 项目、软硬件供应链安全、采购安全五个方面展开。

首先，国外对 ICT 供应链安全管理的战略定位很高。以美国为例，2008 年布什政府提出国家网络安全综合计划（CNCI），提出建立全方位的方法来实施全球供应链风险管理。到 2009 年，奥巴马政府指出不应局限于仅谴责国外产品和服务供应商，新的供应链风险管理方法势在必行。2011 年美国发布《网络空间国际战略》，将“与工业部门磋商，加强高科技供应链的安全性”作为保护网络空间安全的优先政策。俄罗斯方面，在中俄提交联合国的《信息安全国际行为准则》中，双方强调“应当努力确保信息技术产品和服务供应链的安全，防止他国利用自身资源、关键设施、核心技术及其他优势，削弱落后国家对信息技术的自主控制权，或威胁其政治、经济和社会安全。”欧盟方面，提出了《供应链完整性》报告，指出 ICT 供应链完整性是国家经济发展的关键因素，提高供应链完整度对公私部门的意义重大。

其次，目前在国际标准方面已经有很多关于 ICT 供应链安全的标准。比如早期的 ISO 28000 系列标准，还有 ISO/IEC 27002、ISO/IEC 27036、ISO/IEC 15026、ISO/IEC 22O43 等等。其中 ISO 28000 系列标准将 ICT 供应链安全的风险要素划分为安全计划、资产安全、人员安全、信息安全以及货物及运输工具安全等，安全威胁来源于入侵或控制供应链中的资产、供应链走私、信息破坏、货物完整性、非授权使用等，另外 ISO 28000 系列标准也关联了其他指南，包括 ISO 28001《供应链安全、评估和计划的最佳实践—需求和指南》、ISO 28002《供应链恢复能力的开发 -- 要求及使用指南》等内容。

再者，2008 年为响应国家网络安全综合计划 CNCI#11 “建立全方位的方法来实施全球供应链风险管理”，布什政府启动了非国家安全信息系统供应链风险管理实践开发计划，即 ICT SCRM 项目。CNCI#11 为美国联邦机构信息系统的供应链风险管理提供了全面的方法。CNCI#11 第二工作组（WG2）通过提供与采购决策相关的威胁、漏洞和后果的高度认识，开发协作工具，识别能减轻整个产品和服务生命周期中风险的资源，来促进 SCRM。

在软硬件供应链安全方面，硬件供应链安全与其他类型供应链相似，是指 ICT 硬件采购、设计、制造、组装、维护到处理的一系列过程，其风险来源于 ICT 硬件供应链系统与外部环境发生资源交换，以及在与供应链成员进行协调与合作过程中，存在着各种内部不确定性和外部不确定性的风险因素。通常由外部风险方面的自然灾害、恐怖事件、突发事件等和内部的供应中断，如攻击者中断制造和交付、错误的运输路线或延误交货、错误的订单（如数量或项目错误）、质量等风险。软件供应链安全方面，从棱镜门事件到 XcodeGhost，再从惠普驱动键盘记录后门事件，到 Xshell 后门、python pip 源欺骗性污染、VSCODE 插件钓鱼。软件供应链安全事件频发，且具有威胁对象种类多、极端隐蔽、涉及维度广、攻击成本低回报高、检测困难等特性。软件供应链可影响已交付的系统的所有方面，无论何时，只要供应链参与者能接触最终的软件代码或系统，危及软件供应链安全的风险都是存在的。

最后是采购安全。美国方面已经制定了一系列的政府规章。1998 年克林顿发布的第 63 号总统令中指出要确定大型采购任务中与其相关的信息安全，2002 年布什政府起草的国家安全战略中详细阐述了采购的步骤和过程，以及相关的标准。2008 年美国战略与国际问题研究中心（CSIS）发布了《在第 44 任总统任期内保护网络空间安全》的咨询报告，向奥巴马总统提出了若干重要建议，其中包括“通过采购规则提高安全性”，该条建议希望政府能与工业界合作，共同制定和执行 ICT 产品（软件居首要位置）采购安全指南。具体而言，美国政府的国防采购，美国国防部的 ICT 采购实行国防部统一领导与军种分散实施相结合的管理模式。所谓统一领导，是指在国防部设置专门的采购、技术与后勤副国防部长一职，统管全军 ICT 研发及采购事务。而分散实施，是按 ICT 项目的重要性及费用多少实行分类和分级管理。对于不同类别的 ICT 采购项目，负责采购、技术和后勤的副部长指派相应级别的决策当局进行监管。

今年 5 月 15 日，美国总统特朗普正式签署《确保信息通信技术与服务供应链安全》行政令，禁止交易、使用可能对美国国家安全、外交政策和经济构成特殊威胁的外国信息技术和服务。虽然没有点名华为公司，但大家都知道它目前主要是针对华为公司的。

四、 国内 ICT 供应链安全管理

2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上指出，“互联网核心技术是我们最大的‘命门’，核心技术受制于人是我们最大的隐患。一个互联网企业即便规模再大、市值再高，如果核心元器件严重依赖外国，供应链的‘命门’掌握在别人手里，那就好比在别人的墙基上砌房子，再大再漂亮也可能经不起风雨，甚至会不堪一击。”

从战略层面，2016 年我国发布了《国家网络空间安全战略》中，明确提出“建立实施网络安全审查制度，加强供应链安全管理，对党政机关、重点行业采购使用的重要信息技术产品和服务开展安全审查，提高产品和服务的安全性和可控性，防止产品服务提供者和其他组织利用信息技术优势实施不正当竞争或损害用户利益。”另外，我国也制定了 ICT 供应链安全的相关标准，如 GB/T 24420-2009 供应链风险管理指南、GB/T 31168-2014 云计算服务安全能力要求、GB/T 32921-2016 信息技术产品供应方行为安全准则、GB/T 22239-2008 信息系统安全等级保护基本要求、GB/T 29245-2012 政府部门信息安全管理基本要求。2019 年 5 月 1 日正式实施的 GB/T 36637-2018《信息安全技术 ICT 供应链安全风险管理指南》，正是在完整性、保密性、可用性、可控性的原则指导下制定的指南，目标使用者包括了 ICT 产品、服务的采购方——党政部门、重点行业、关键信息基础设施。

在经济全球化时代，信息通信技术供应链存在产品和服务复杂、涉及全生命周期、供应商跨境的特点。没有 ICT 供应链安全，就没有国家安全。为此，应当加强我国 ICT 供应链安全管理，防止他国利用自身资源、关键基础设施、核心技术及其他优势，削弱我国对 ICT 技术的自主控制权，威胁我国的政治、经济和社会安全。

为此，我们提出以下建议：

1、我国应尽快制定专门的 ICT 供应链安全管理相关法律法规，明确各方在 ICT 供应链安全管理中应当承担的责任和义务。在今后修订《网络安全法》的时候，增加对 ICT 供应链安全管理的条款。并且，供应链管理也应该覆盖上下游，通过与进出口许可管理制度、负面清单、不可靠实体清单等制度配合，发挥保障我国军事、外交、以及经济安全等方面更大的作用。

2、建立 ICT 供应链安全管理制度，实施国家 ICT 供应链全方位安全管理。建立供应链安全管理制度已成为国际通行做法，也是国际社会所接受的保障国家网络安全的正当措施。

3、促进相关标准的研究制定，加大支持研究 ICT 供应链安全管理相关核心技术的力度。