B.15
工业信息安全事件技术分析

张晓菲　李耀兵　胡　彬*

摘　要： 2017 年，工业信息安全事件时有发生。“WannaCry”蠕虫病毒引发大规模勒索攻击，使网络勒索走进普通民众视线；供应链产品相关漏洞相继曝出，全球工业互联网安全形势愈加严峻；曼哈顿纽约机场机密文档泄露等事件表明，数据泄露现象十分严重；摄像头、路由器等智能终端漏洞频出，物联网设备愈发成为僵尸网络的“主力军”。

关键词： 网络安全　数据泄露　勒索病毒　工业互联网　物联网

一　网络勒索成为世界焦点

随着“WannaCry”病毒大规模感染等事件爆发，网络勒索事件逐渐成为网络安全领域的重大关注。勒索病毒“Petya”、勒索软件“Bad Rabbit”等引起的勒索事件接踵而来，给工业企业带来巨大影响。勒索病毒的攻击特点是，对系统文件或硬盘进行加密，要求用虚拟货币（例如比特币）等缴纳赎金，限定时期内不缴纳则赎金翻倍。同时，病毒利用系统开放的 445 端口进行感染传播，扩大影响范围。在攻击方式上，有的利用系统漏洞，例如

* 张晓菲，工程硕士，国家工业信息安全发展研究中心助理工程师，研究方向为信息安全；李耀兵，工程硕士，国家工业信息安全发展研究中心助理工程师，研究方向为信息安全；胡彬，国家工业信息安全发展研究中心工程师，研究方向为信息安全，长期从事网络安全运维管理及计算机与网络安全研究工作，具有扎实的理论基础与丰富的实践经验。

“WannaCry”勒索病毒，有的利用钓鱼攻击，例如“Bad Rabbit”勒索病毒。因此，勒索病毒的多样化亟须工业企业提高安全防范意识。

（一）全球 PC 灾难，“WannaCry”病毒爆发

2017 年 5 月 12 日，“WannaCry”勒索病毒在全球大范围爆发，导致 150 多个国家和地区受到影响，造成 100 多亿美元损失，成为有史以来影响力最大的病毒之一。西班牙电力公司 Iberdrola、天然气公司 Gas Natural、电信巨头 Telefonica、德国德累斯顿火车站、葡萄牙电信公司、联邦快递 FedEx、俄罗斯内政部及其第二大电信运营商 Megafon 等都是这轮攻击的受害者。我国众多行业受到感染，涉及能源、电力、交通、医疗、教育等重点行业领域，影响范围十分广泛，造成后果极其严重。受害人必须限时支付价值 300 美元的比特币赎金，否则超时翻倍，因此，该病毒又被称为“比特币病毒”。据悉，攻击者会先扫描公网 IP 端口 445，再利用 445 端口漏洞对该端口开放的系统进行攻击。进入局域网后，利用 Windows 系统的 SMB 远程提权漏洞（MS17 - 010 漏洞）发起攻击，并迅速蔓延至工业企业内网甚至工业控制网络，导致工业主机被加密锁定以至于无法正常运行，甚至造成整个工业企业内网瘫痪。在 Windows 操作系统中，445 端口主要提供局域网中的文件或打印机共享服务。SMB 协议则是 Microsoft Windows 中使用的一项 Microsoft 网络文件共享协议，在大部分 Windows 系统中默认开启，用于在计算机间共享文件、打印机等。

与以往不同的是，“WannaCry”病毒结合蠕虫的方式进行传播，攻击者与 445 端口建立请求连接，获得指定工业内网中的各类共享信息，同时通过该端口漏洞获取 Windows 系统权限，自动感染其他未打补丁的系统。该勒索病毒会加密系统中的图片、文档、压缩包、音频、视频、可执行程序等几乎所有类型的文件，被加密的文件后缀名被统一修改为“. WNCRY”。该勒索病毒的加密强度极大，暴力破解需要极高的运算量，如果没有密钥，几乎不可能解密。病毒会将自身复制到每个文件夹，并命名为“@ WanaDecryptor @. exe”，同时衍生大量语言配置等文件，在桌面弹出勒索对话框，提示受

害者支付价值数百美元的比特币。该病毒仅针对 Windows 系统的电脑，手机等终端不会遭受攻击，包括 Unix、Linux、Android 等系统也都不会受影响。10 月 12 日，Microsoft Windows SMB Server 远程代码执行漏洞（CVE－2017－11780）再次爆发，再一次对 Windows 系统造成冲击。攻击者依旧通过 445 端口或 139 端口对 Windows 服务器进行远程攻击，获取系统的控制权限。由于“WannaCry”的前车之鉴，这次并没有造成很大影响。

（二）勒索病毒“Petya”来袭，更具破坏性

2017 年 6 月，“WannaCry”病毒肆虐过后，全球多个国家遭新一轮勒索病毒“Petya”的攻击。乌克兰遭受的危害最严重，其政府部门、国有企业相继“中招”，我国也有用户受到影响。该勒索病毒最先攻击乌克兰，随后蔓延至欧洲、北美等多个国家和地区。“Petya”勒索病毒传播速度特别快，病毒爆发当天就已经实施约 2000 次攻击，90% 以上位于乌克兰和俄罗斯。在欧洲国家重灾区，该病毒的传播速度达到每 10 分钟感染 5000 余台电脑，多家运营商、石油公司、机场、ATM 机等企业和公共设施大量沦陷，甚至乌克兰副总理的电脑也遭到感染。“Petya”病毒利用已知的 Office/wordpad 远程执行代码漏洞（CVE－2017－0199），伪装成求职简历电子邮件进行传播，用户点击该邮件后释放可执行文件，病毒在成功感染本机后形成初始扩散源，再利用“永恒之蓝”漏洞在工业内网中扫描开放 445 端口的主机进行传播，使得病毒在短时间内呈爆发态势。“Petya”勒索病毒与“WannaCry”勒索病毒类似，传播时都利用了泄露的美国国家安全局网络“开锁工具”，但是该病毒会对 NTFS 分区加密、修改硬件主引导记录（MBR）、阻止机器正常启动，使计算机无法使用。

（三）新型勒索软件“Bad Rabbit”袭击东欧诸国

2017 年 10 月 24 日，在东欧和俄罗斯开始传播一种新的勒索病毒“坏兔子”（Bad Rabbit），影响了俄罗斯部分媒体组织、乌克兰的部分业务（包括基辅的公共交通系统和国家敖德萨机场）以及保加利亚和土耳其，并向

美国蔓延。该病毒通过水坑攻击将恶意代码植入合法网站，伪装成 Flash 升级提示，诱骗互联网用户主动下载并运行恶意程序。病毒带有伪造的 Symantec 数字签名，它不仅加密受害终端的文档，而且扫描内网 SMB 共享，使用弱口令和 Windows 密码工具获取登录凭证等手段，尝试登录和感染内网其他工业主机。该勒索病毒和“Petya”勒索病毒的相同之处是使用开源的加密软件 DiskCryptor，该软件用 RSA－2048 的方式对文档进行加密，并利用 SMB 共享端口感染其他工业内网主机。攻击者要求被“坏兔子”感染的受害者支付约 275 美元以解锁被加密文件，但缴纳赎金后不清楚是否可以解密电脑文件。

二　供应链安全风险凸显

传统的供应链是商品到达消费者手中之前各相关者的连接或业务的衔接，从采购原材料开始，制成中间产品以及最终产品，最后由销售网络把产品送到消费者手中的一个整体的供应链结构。传统商品的供应链同样适用于计算机软硬件，可简化成开发、交付、使用三个环节。显而易见，攻击者只要对上述某一环节进行攻击，最终的软件产品和整个使用场景的安全就可能受到影响。从多个现实案例分析发现，第三方支持库、开发工具、开发软硬件环境、到达用户的渠道、使用软硬件产品的过程等供应链相关安全风险，并不低于针对软件应用本身、相应操作系统的安全漏洞导致的安全风险。2017 年，针对供应链环节的攻击频率增长，网络安全形势令人担忧，各种供应链相关产品高危漏洞频频爆发，工业企业潜在安全威胁增多。

（一）Xshell 应用软件存在后门

2017 年 8 月，一款被广泛应用于服务器运维和管理的终端模拟器 Xshell 被曝出存在后门。Xshell 是一款支持 TELNET、SFTP、SSH 等远程协助操作的免费终端模拟软件，工业企业常将其用于远程连接工业主机。NetSarang 的 Xshell、Xlpd、Xftp 等产品被某安全公司发现存在恶意代码，这些恶意代

码存在于模块 nssock2. dll 中，其中已确认存在恶意代码的两个版本是 Xshell 5. 0. 1325 和 Xshell 5. 0. 1322。有安全企业分析发现，7 月 23 ~ 31 日，Xshell 等产品的命令与控制（C&C）存在 DNS 解析，且 DNS 服务器指向不正常，极有可能泄露用户信息。该后门程序通过 DGA 算法，根据系统时间、机器名等参数每月生成一个新的 C&C 域名，然后通过 DNS TXT 请求进行通信传递主机相关信息，并接收服务器指令，这种方式很难被检查出来。由于 Xshell 被广泛应用于服务器运维和管理，工控企业网站管理人员、技术运维人员在这次的网络威胁中首当其冲。

（二）主板厂商利用英特尔 UEFI BIOS 固件漏洞留门

2017 年 10 月，卡梅隆大学的 CERT/CC 小组发布信息称，统一可扩展固件接口（UEFI）系统和一些英特尔主板芯片的 BIOS 中存在三个固件漏洞。由于 UEFI 未限制对 EFI S3 启动脚本访问，攻击者可利用该漏洞绕过系统安全机制（Secure Boot），对启动设备的固件进行刷新或者在 SMRAM 中写入数据。该漏洞影响 Phoenix、英特尔和 American Megatrends 等厂商的 UEFI 系统，并可被用于安装底层勒索软件。固件源文件 FSVariable. c 中存在缓冲区漏洞，利用方法比较复杂，危害因 OEM 固件执行环境不同而不同，Insyde、戴尔、惠普、联想、索尼和东芝等产品都受影响，苹果、IBM、英特尔与 Phoenix 没有受到影响。BIOS 漏洞存在于英特尔固件中，该漏洞允许攻击者重写固件代码，利用条件苛刻，只有依靠 BIOS_ CNTL. BIOSWE 和 BIOS_ CNTL. BLE 二进制文件进行 BIOS 锁定的系统才存在此漏洞。

（三）恶意软件“TRITON”引发工业厂房安全事件

2017 年 12 月 14 日，网络安全公司火眼（FireEye）披露了一起工业厂房安全事件，这是首起直接发生在工业厂房的工控安全事件。该事件表明黑客针对工业控制系统等关键基础设施的攻击日趋严重。火眼公司安全团队 Mandiant 的事件调查结果显示，攻击者对一个关键基础设施的安全仪表系统（SIS）发起了网络攻击，获取了该系统的远程访问权限，并部署新型恶意软

件“TRITON”来远程控制和操纵 SIS 控制器，造成 SIS 进入故障状态，并自动关闭了工业过程，最终触发了安全警报而被发现。受攻击的系统为施耐德电气公司 Triconex 安全仪表系统，其作用是为用户发布网络入侵的安全警报，广泛应用于能源行业，包括石油天然气工厂、核设施等。

“TRITON”是一种针对工业控制系统的恶意软件，包括 trilog. exe 和 library. zip 两个主要模块。模块 trilog. exe 是调用和执行 libraries. zip 模块的可执行程序，而 library. zip 是与 SIS 控制器进行交互的自定义通信库。“TRITON”功能众多，包括读写独立功能、查询 SIS 控制器状态等。同时，“TRITON”具有与施耐德 Triconex SIS 控制器进行通信的能力，例如发送暂停、读取内容等特定命令，也可对 SIS 控制器进行远程重新编程并运行。

（四）英特尔等 CPU 惊现重大安全漏洞，工业企业相关操作系统、云服务平台、工业互联网平台等面临安全威胁

2018 年 1 月 3 日，美国谷歌（Google）公司安全团队 Project Zero 披露了 2 组共 3 个高危漏洞，分别是“熔断”（Meltdown，漏洞编号为 CVE－2017－5754）和“幽灵”（Spectre，漏洞编号为 CVE－2017－5753、CVE－2017－5715），该漏洞影响英特尔（Intel）、美国超微半导体公司（AMD）等厂商生产的主流中央处理器（CPU）并导致用户敏感信息泄露，工业控制系统、云服务平台及工业互联网平台可能受到这两组漏洞的影响。

“熔断”和“幽灵”漏洞利用了 CPU 芯片硬件层面乱序执行机制的缺陷，使得低权限的恶意访问者可以突破内存隔离，发动侧信道攻击。在未被许可的情况下读取同一系统中的其他进程或同一主机上其他虚拟机内存中的敏感信息，包括密码、账户信息、加密密钥或理论上存储在内核内存中的任何内容。该漏洞打破了云平台基于虚拟化隔离技术的所有安全假设，任何虚拟机的租户或者不法分子可以通过利用该漏洞跨账户、跨虚拟机窃取其他用户的资料，给全球云计算基础设施的安全性带来严重威胁。

三　全球数据泄露问题愈演愈烈

2017 年数据泄露事件持续增多，维基解密（WiKiLeaks）公布了数千份文件，并揭秘了美国中央情报局（CIA）关于黑客入侵技术的最高机密，信息涉及 iPhone 手机、Android 手机、智能电视，以及 Windows、Mac、Linux 等操作系统相关漏洞和利用工具；影子经纪人公开美国国家安全局（NSA）黑客武器库中的攻击工具，造成一系列工业信息安全事件；纽约机场陷入泄密危机，750G 数据被曝。

（一）国家级攻击工具泄露带来全球网络安全连锁影响

2017 年 3 月，维基解密披露了代号为“Vault 7”的 CIA 文件，其中“Year Zero”文件有 513MB，包含 8761 份秘密文件，涉及大量零日漏洞、病毒、恶意软件以及高度机密文件。该泄密文件描述了 CIA 在全球部署恶意软件的范围和目标，表明 CIA 拥有入侵 iPhone 手机、Android 手机、智能电视，以及 Windows、Mac 和 Linux 操作系统的强大能力。CIA 拥有比 NSA 更高的政治和财政预算的优先权，它在全球部署了自己的黑客武装力量，该机构的黑客不用向 NSA 披露自己的非授权入侵行为。2016 年底，CIA 的黑客部门归属网络智能中心（CCI），拥有约 5000 名员工，并开发了超过 1000 个网络攻击武器。

维基解密提供的信息表明，CIA 发现的产品安全漏洞并没有报送给相关厂商，而是利用这些漏洞入侵用户的软硬件产品，如 Android 手机等，而这些产品被全球数百万用户使用。安全领域的一些专家、企业对“Vault 7”的机密文档做了研究分析，指出针对移动端的攻击技术在 CIA 泄密文档中有所描述，文档记录了 iPhone 手机和 Android 手机相关入侵破解技术，利用这些技术不仅可以拿到目标设备的完整控制权，而且能够远程接管目标设备 idea 内核，即接管负责控制智能手机运行的操作系统核心部分。CIA 没有破解手机通信软件的加密算法，而是利用能够获取手机完整访问权限的黑客工

具以绕过手机本身的安全机制，从而远程访问目标手机。CIA 利用跨平台的恶意软件绕过计算机的监控服务，入侵 Linux、macOS 及 Windows 计算机。CIA 在开发自己的间谍软件的过程中，借鉴了当前流行的恶意软件代码，以满足其特殊需求。CIA 利用捆绑恶意的 App 监控目标，“Vault 7”中记录了名叫 Weeping Angel 的监控技术，CIA 利用这种技术能够渗透三星的智能电视，可以记录语音聊天信息。此次维基解密泄密事件虽没有斯诺登的泄密事件影响力大，但是依然波及较大范围，使美国公民的个人敏感信息置于风险之中。

2017 年 11 月，名为“Vault 8”新的一系列 CIA 网络武器被曝光，此次泄密文档中曝光的部分不涉及任何零日漏洞，因而没有造成较大安全影响，泄密文档中提及名为 HIVE（蜂巢）的 CIA 网络工具源码和开发日志，CIA 利用 HIVE 可以针对 Windows、Solaris、MikroTik（路由器 OS）、Linux 和 AVTech 网络视频监控等系统定制植入程序，实现针对平台植入任务的后台控制，进而以 HTTPS 协议和数据加密方式执行命令和窃取数据。该工具认证证书仿造了现实中存在的公司和组织，其中一个就是仿造俄罗斯网络安全公司卡巴斯基实验室的安全证书，以此来隐瞒电脑病毒的来源，它被 CIA 利用从其他组织或公司的电脑中窃取机密。

截至目前，维基解密已曝光“Vault 7”、“Vault 8”系列秘密文档和网络武器，其中涉及的网络武器已经引发了如“WannaCry”病毒勒索等大规模的网络安全事件，相关的零日漏洞和攻击代码给不法分子的恶意行为带来了便利，给工业互联网安全带来了巨大隐患。

（二）影子经纪人公开美 NSA 黑客武器库

2017 年 1 月，影子经纪人在网上公布多个 NSA 网络武器库中的程序截图，涉及微软 23 个系统漏洞的 12 种攻击工具，引发勒索病毒事件的“永恒之蓝”不过是其中之一。4 月，影子经纪人声称从“方程式组织”获取一份 300M 的秘密文档，在网上公开当时截图中的多个黑客武器和漏洞。据说美国政府正是利用这些工具入侵国际银行系统，侦查各国间资金

流向，监控中东和拉美国家银行间的资金往来情况。这些黑客工具包括恶意软件、私有的攻击框架及其他攻击工具，主要针对微软的 Windows 系统等。由于这个黑客团队制造的“武器”拥有超强的自毁能力，绝大多数进攻完成之后，不会留下任何痕迹。6 月，影子经纪人声称将提供“影子经纪人数据曝光月（The Shadow Brokers Data Dump of the Month）”服务，该项服务实行会员制度，制定月度订阅模式，逐月向会员提供曝光数据，这些数据涉及浏览器、手机等漏洞及相关工具、新的攻击行动、一些入侵数据，以及针对中国、俄罗斯、伊朗和朝鲜的导弹和核弹计划的内部网络数据。

（三）曼哈顿纽约机场机密文档泄露

2017 年 2 月，位于曼哈顿的纽约机场的内部敏感数据不断被暴露在互联网上，这些超过 750G 的文件没有采取任何加密措施。泄密文档中涵盖纽约机场人员的电子邮箱账户、人力资源文件、办公室备忘录、工资单数据、一套疑似财务追踪用途的大型数据库，以及其他核心基础设施的原理图与各类细节信息。此次泄密事件原因被认为是黑客使用了“Shadow Protect”的备份软件以及存在严重安全隐患的 Buffalo Terastation 的辅助备份设备。这些泄密文档被黑客利用可篡改登机牌及其他乘客信息，甚至可以影响机场运营，导致乘客滞留在地面。

四　物联网安全形势依然严峻

随着智能设备的普及，物联网设备日益增多，由物联网设备引发的安全事件逐渐增多。2016 年造成美国断网事件的“Mirai”物联网恶意软件变种升级为“Rowdy”，攻击对象由摄像头等视频监控系统转向机顶盒物联网设备，影响中国 2 亿多用户；变异僵尸网络“IoT_ reaper”利用物联网设备漏洞进行攻击传播，持续扩大僵尸网络范围；网络路由器、摄像头等设备不时曝出新漏洞，引发关注。物联网和工业互联网息息相关，这些物联网安全事

件的不断增加，表明物联网安全形势依然严峻，工业互联网受到威胁，亟须引起高度重视。

（一）20万国产 WiFi 摄像头曝漏洞，后门大开任由黑客进入

2017 年 3 月，有媒体曝出市面上超过 1250 款型号的摄像头存在漏洞，近 20 万台设备存在被黑客入侵的风险。存在漏洞的产品名称是 Wireless IP Camera（P2P）WiFiCAM，它是由中国厂商生产，并以贴牌产品的形式提供给多家摄像头厂商。该厂商提供的商品固件中存在多个安全漏洞，导致其他公司的产品也存在这些漏洞。其中，一个漏洞和 GoAhead 网页服务器相关，通过该服务器可在网页端中控台控制设备。此外，该厂商的产品被分析存在后门账号（任意用户可以通过默认账号密码访问登陆设备）、预授权信息与凭证泄露、未授权访问等漏洞，利用这些漏洞可绕过认证机制访问设备。这些设备具有 Cloud 管理功能，可以让用户通过网络管理设备，该功能使用明文 UDP 通道绕过 NAT 和防火墙，可被攻击者利用并发起蛮力攻击（brute-force attacks）猜测设备的凭证信息。拥有该功能的设备数量超过 100 万台，大幅度削弱了私有网络提供的各项保护措施。安全研究人员发现，利用这些漏洞可以对设备植入僵尸病毒“Persirai”，再通过设备存在的零日漏洞攻击其他的网络摄像头，最后，黑客会控制这些设备发动 DDoS 攻击。黑客还会利用这些漏洞入侵装置获取控制权，窃取用户的电子邮件账号资料，拦截被黑设备传回云端主机的资料。

（二）数十款 Linksys 路由器曝高危漏洞，可致远程命令执行及敏感信息泄露

2017 年 4 月，IOACTIVE 的研究人员发现 Linksys 智能 WiFi 路由器存在漏洞。该路由器属于 Belkin 公司旗下的一个品牌，在亚洲的市场占有率较小。研究人员通过逆向固件，发现从低危到高危共 10 个漏洞，其中 6 个漏洞可被利用执行远程攻击，两个漏洞可被利用进行 DoS 攻击。攻击者利用漏洞可绕过认证机制，获取路由器的技术资料、运行进程列表、读取

FTP 配置、获取 SMB 服务配置等敏感信息，甚至以 root 权限执行注入命令，创建后门账号长期控制路由器。研究人员发现 7000 多个易受攻击设备，其中约 69% 位于美国，其次是加拿大（10%）、中国香港（1.8%）、智利（1.5%）、荷兰（1.4%），中国内地、印度、英国等其他国家和地区占比都不到 1%。在这 7000 多台设备中，11% 存在默认密码，易被黑客入侵。

（三）“Mirai”变异升级继续感染物联网

2017 年 8 月，中国某安全厂商 DoS 态势感知平台监控到某用户被 DoS 攻击，通过溯源发现攻击是利用了物联网设备，攻击载体由摄像头变成电视机顶盒，而且攻击目标在中国，数量达 2 亿多台，攻击源头是名为“Rowdy”的恶意软件。“Rowdy”是造成美国断网事件的“Mirai”物联网恶意软件的变种，采用加壳措施进行自我保护，利用 Telnet 服务感染扩散，实现了从摄像头等视频监控系统向机顶盒物联网设备的跨越，大幅度扩展了其传播范围。“Rowdy”僵尸网络通过自动化扫描方式感染其他主机，利用内置用户名/口令字典，破解登录 Telnet 服务，支持 X86、ARM、MIPS 等多个平台，通过设备的 busybox 工具下载并执行恶意病毒程序。该僵尸网络能够发动 SYN Flood、DNS Flood、HTTP Flood、ACK Flood、VSE Flood 等多种 DoS 攻击，组成僵尸网络的设备都为上网出口设备，具备发起大规模、大流量 DoS 攻击的能力。针对该僵尸网络的 C&C 控制服务器溯源发现 IP 地址位于荷兰阿姆斯特丹，中国东南部沿海地区是重灾区。

2017 年 9 月，安全研究人员监测发现一款 IoT 设备新型恶意样本。随后，其恶意软件迅速感染全球大规模物联网设备，并形成物联网僵尸网络“IoT_ reaper”。该恶意软件的编译者不断更新代码，众多知名品牌的无线路由器遭到感染，包括 GoAhead、D-Link、TP-Link、AVTECH、NETGEAR、MikroTik、Linksys 及 Synology 等。截至目前，IoT_ reaper 集成漏洞信息如表 1 所示。

表 1　IoT_ reaper 集成漏洞信息

序号	设备类型	漏洞名称	可能受影响的设备型号
1	无线网络通用摄像头(P2)WiFiCAM	信息泄露	1250 + 不同型号 WIFICAM 摄像头
		远程命令执行	
2	D-Link 路由器	远程命令执行	DIR 850L/800 /600/300
		信息泄露	DIR 800/850L
		未授权访问	DIR - 645
		Cookie 溢出远程命令执行	DIR 850L
3	MVPower 等闭路数字录像机	默认密码	设备 web 服务器标志:JAWS/1.0
		Web 旁路绕过	
4	NETGEAR 网络设备	未授权命令执行	DGN 路由器
		远程命令执行	ReadyNAS 监控设备
		任意文件上传	ProSAFE NMS300 网络管理系统
		命令注入	R7000/6400、DGN2200 路由器
5	Avtech 设备	明文存储管理密码、CSRF、信息泄露等	所有型号设备
6	Linksys 设备	远程命令执行	E1500/E2500、WRT110 路由器
		管理界面 DoS 命令执行	WRH54G
7	Vacron 网络硬盘录像机	远程命令执行	Vacron NVR

资料来源：卡巴斯基实验室，国家工业信息安全发展研究中心综合分析。

被“IoT_ reaper”感染设备涉及的国家有中国、意大利、新加坡、美国、越南、土耳其、韩国、泰国、印度和伊朗等。“IoT_ reaper”具有感染速度快、攻击手段复杂、蔓延行为隐蔽等特点。“IoT_ reaper”恶意软件利用 IoT 设备漏洞，通过“自蔓延”感染方式建立僵尸网络，代码中集成 LUA 执行环境，支持使用 LUA 脚本编写复杂而高效的攻击指令，代码中存在多种 DDoS 攻击方式。“IoT_ reaper”恶意软件 C&C 服务器被完全重新设计，使用新的后台。所有与 DDoS 相关的功能都由 C&C 后台进行协调和管理，并作为单独的模块下载，降低了被安全研究者发现的风险，提升了僵尸网络扩张蔓延的程度。

五　安全漏洞频出，危及工业互联网

2017 年，CNVD 共收录网络安全漏洞信息 14000 余条，其中高危漏洞超 5000 个，Web 层面漏洞依旧频频曝出，使网络安全领域波涛起伏，网络安全相关人员心弦紧绷。Struts2 框架的 Apache Struts2 －045、Apache Struts2 －046、Apache Struts2 －052、Apache Struts2 －053 等漏洞相继曝出，给使用此架构的工业企业、政府、高校的网站带来巨大影响。常用 WPA2 无线协议和蓝牙协议存在漏洞、Tomcat 服务器存在远程代码执行等，给工业互联网用户带来了巨大困扰。

（一）常用无线协议存在多个漏洞

2017 年 9 月，物联网安全研究公司 Armis 发现蓝牙协议中存在多个零日漏洞，这些漏洞将影响 Windows、Linux、iOS、Android 等系统设备和使用短距离无线通信的物联网设备，影响全球设备数量多达 53 亿台。该安全公司在实验室进行了相关测试，利用 BlueBorne 攻击成功搭建了僵尸网络，并安装勒索软件。利用蓝牙协议漏洞能够在用户感知不到的情况下获取系统权限，实现任何恶意目的，比如数据窃取、网络间谍、勒索攻击等，甚至可以通过物联网设备搭建大型僵尸网络（如 Mirai 僵尸网络），或是利用移动设备创建僵尸网络（如 WireX 僵尸网络）。具备蓝牙功能的联网设备都有遭受到恶意攻击的可能，攻击者无需进行任何交互就能够远程控制设备。一旦攻击者利用该漏洞，可能会像可怕的蠕虫型勒索软件“WannaCry”一样迅速蔓延，对全球工业企业和组织造成难以估量的损害。

2017 年 10 月，安全研究人员发现在 WPA2 协议中存在多个漏洞，这些漏洞组合在一起形成了概念验证攻击 KRACK（代表 Key Reinstallation Attacks）。Wi-Fi Protected Access Ⅱ协议被广泛用来保护现有的 WiFi 网络已有 13 年之久。研究人员发现，Android、Linux、Apple 等任何使用 WPA2 协议的设备都会受到影响。攻击者可以利用 KRACK 攻击影响封包重送、解

密、TCP 连接绑架等内容，读取一些聊天信息、信用卡号、电子邮件等敏感信息，通过一些网络配置，可以实现注入和对数据处理等操作。例如，将 ransomware 等恶意软件注入到网站中。

（二）Struts2高危漏洞爆发趋势不减

2017 年 3 月、9 月 Struts－045/046、Struts－052/053 高危远程命令执行漏洞相继爆发，政府、企业、高校、科研院所等单位使用 Struts2 框架进行 Web 开发的业务系统均受到威胁，对其业务正常开展造成严重影响，市政、电力、航空航天、装备制造、水利等多个工业领域也受到影响。Struts2 是第二代基于 Model－View－Controller（模型）的 Java 企业级 Web 应用框架，是一款在我国金融、电力、交通、医疗等领域的关键信息基础设施中均有广泛应用的 Web 中间件，其中 Struts2－045 漏洞利用无任何条件限制，攻击者可绕过绝大多数防护设备的通用防护策略，在使用基于 Jakarta 插件的文件上传功能时，通过修改浏览器 HTTP 请求头中的 Content-Type 值可触发该漏洞，直接获取应用系统所在服务器的控制权限，执行系统命令。Apache Struts2－046 远程代码执行漏洞和 Apache Struts2－045 远程代码执行漏洞原理相同，仅使用了不同的攻击向量，攻击者通过发送恶意构造的 HTTP 数据包利用该漏洞，在受影响服务器上执行系统命令，进一步控制该服务器，导致拒绝服务、数据泄露、网站篡改等危害。对于工业企业，位于企业办公网的企业资源计划（ERP）系统、自动办公（OA）系统、生产运行管理系统等可能使用 Struts2 进行开发，攻击者可通过该漏洞远程执行代码，获取主机权限，然后利用上层信息系统，通过跳板渗透等手段影响内网工控系统安全。

（三）Tomcat 存在远程代码执行漏洞

2017 年 9 月，Tomcat 远程代码执行漏洞（CVE－2017－12615）在 Windows 平台运行的 Tomcat 上被发现。Tomcat 是一款比较流行的 Web 应用中间件，用于支持运行 Servlet/JSP 应用程序的容器。在启用 HTTP PUT 请求

方法的情况下，攻击者构造攻击请求向服务器上传包含任意代码的 JSP 文件。该 JSP 文件能被服务器执行，可获取服务器权限，对服务器站点造成严重影响，引发数据泄露、后门植入、沦为“肉鸡”等安全事件。

（四）PHP 存在缓冲区溢出漏洞，可执行任意代码

2017 年 11 月，PHP 脚本语言被曝存在缓冲区溢出漏洞（CVE－2017－16642），攻击者利用该漏洞可以执行高度特权的任意代码，获取服务器的控制权限，PHP5. 6. 32 版本之前、7. 0. 25 之前和 7. 1. 11 之前版本均受到影响。

（五）视频监控设备高危漏洞危及工控安全

2017 年 5 月，美国 ICS-CERT 披露中国两个安防监控设备制造商的产品存在 4 个高危工控漏洞。这充分表明，随着视频设备在工业领域的日益广泛应用，视频设备安全值得高度关注。

1. 较多视频设备开放远程登录协议，易被恶意控制发起网络攻击

当前，视频设备多存在开放远程登录（telnet）协议现象，易被黑客等不法分子通过远程登录获取控制权限，上传恶意程序对视频设备进行控制，甚至将其当成“肉鸡”构建僵尸网络，发动大规模分布式拒绝服务攻击。

2. 视频监控安全漏洞可对工业相关领域造成恶劣后果

视频监控能实时了解工业设备运行、工艺流程故障、人员操作等情况，是保障工业设备安全和人身安全的重要手段。一旦视频监控设备存在漏洞，被不法分子或攻击者利用，可能造成严重后果。一是可能导致视频设备失灵，造成无法及时掌握当前企业运行相关情况，影响工业生产甚至可能造成安全事故。二是不法分子通过控制视频设备可获取工业生产数据、工艺参数、地理位置等敏感信息，造成商业机密泄露，对工业企业造成重大经济损失。三是视频设备可被利用作为攻击工业系统的跳板，威胁工业生产安全；或者被黑客利用并构建僵尸网络，进而发起大规模 DDoS 攻击，造成工业系统瘫痪等严重后果。

参考文献

《CNCERT 互联网安全威胁报告》，2017。
“Strategic Principles for Securing the Internet Of Things”，2017。
《360 互联网安全杂志》，http：//zt. 360. cn/2015/reportlist. html? list =8，2015。
黄玲：《Struts2 框架技术研究》，重庆工程学院，2017。