全球关键信息基础设施网络安全状况分析报告（2017）

360 威胁情报中心

2018.1.12

目　　录

导　　语

关键基础设施的网络安全威胁已成为全球各个国家网络空间最为关注的课题之一。各个国家纷纷出台保护关键信息基础设施的政策和战略，通过研究美国、德国、英国、俄罗斯以及中国的相关政策，可以发现不同国家对关键信息基础设施的理解和界定，各不相同，但重点保护、全力保障关键信息基础设施安全的目标是一致的。通过大量公开资料及报道，我们发现全球关键信息基础设施已经或正在遭遇大量来外部、内部的网络攻击，或者因存在管理漏洞等问题而埋下诸多潜在隐患。本报告以金融、能源、通信、工业系统、教育、交通、医疗卫生等关键领域为例，给出这些关键信息基础设施遭遇安全攻击的实际案例，并简要分析，以期对我国关键信息基础设施防御与保护工作提供借鉴参考。

第一章　各国对关键信息基础设施的界定

关键信息基础设施关系国计民生，也是各国网络安全保障的首要目标。不过，世界各国的经济发展水平不同，网络状况、网络经济发展程度存在差异，因此各国对关键信息基础设施的定义和界定也存在很大的不同，侧重保护的重点领域也不尽相同。例如美国政府规定了 16 类关键基础设施，从民用领域到军事领域，涵盖非常广泛。而德国在联邦政府层面划定了 9 类关键基础设施，和美国相比，德国更加聚焦民生领域，而且增加了传媒与文化领域。本章将主要就中国、美国、俄罗斯、德国、英国这 5 个国家的政府部门对关键信息基础设施界定异同进行比较。以此来了解世界各国在关键信息基础设施保护方面的政策特点。

特别说明，世界各国对于某些关键信息基础设施的命名方法和职能限定有一定区别，比如，同样是应急响应部门，有的国家称之为应急服务，而有的国家则称之为灾害响应。出于横向对比方便的考虑，在本报告中，我们尽可能的对各国职能类似的基础设施采用相同的翻译名称。其中某些细微之处可能存在偏差。

一、 中国

《中华人民共和国网络安全法》中给出了关键信息基础设施的大致范围，可分为七类：公共通信和信息服务、能源、交通、水利、金融、公共服务（水、电、食品、卫生）、电子政务。

而《网络空间安全战略》中的规定的关键信息基础设施包括：1 张基础网络、11 个重要信息系统和 1 类重要互联网应用系统，共 13 项。

2017 年 7 月发布的关键信息基础设施安全保护条例（征求意见稿）在《网络安全法》和《国家网络空间安全战略》的基础上，再次增加了环境保护，和国防科工、大型装备、化工、食品

药品等领域的基础设施。

总结起来，目前国内相关政策法规中圈定的关键信息基础设施共含 17 个领域，具体包括：1、提供公共通信，广播电视传输等服务的基础信息网络；2、能源；3、金融；4、交通；5、教育；6、科研；7、水利；8、工业制造；9、医疗卫生；10、社会保障；11、公用事业；12、国家机关；13、重要互联网应用系统；14、国防科工；15、大型装备；16、化学工业；17、食品药品。

二、 美国

奥巴马政府将以下 16 个领域纳入为关键基础设施保护对象。并出台一系列政府文件和总统行政指令加以优先保护。这 16 个领域具体包括：

1、化学工业；2、商业设施、3、通信；4、关键制造；5、水利；6、国防；7、应急响应部门；8、能源；9、金融；10、食品和农业；11、政府部门；12、医疗卫生；13、信息技术；14、核设施；15、交通运输；16、供水及污水处理系统。

三、 俄罗斯

2009 年俄罗斯的信息安全政策文件中描述的关键部门，主要指科技、国防、通信、司法、应急响应部门等。

2013 年的出台的《俄联邦关键网络基础设施安全》规定：对入侵交通、市政等国家关键部门信息系统的黑客最高可处以 10 年监禁。这事实上是将交通、政府等纳入国家关键网络基础设施。

另外，俄罗斯政治研究中心网络安全问题专家奥列格•杰米多夫（Oleg Demidov）指出，俄罗斯的信息安全战略更多强调在内容层面的管控，非常重视互联网信息传播对传统文化、公民德道和价值观带来的影响，而在基础设施层面，则几乎没有特别具

体的描述，只是概括性地表示保护关键信息基础设施。

总结起来，俄罗斯政府部门明确或隐含界定的关键信息基础设施有 7 类：

1、科技；2、国防；3、通信；4、司法；5、应急响应部门；6、交通运输；7、政府部门。

四、 德国

德国网络空间战略（2011 年）中指出，关键基础设施是指各类非常重要的公共物资或资源相关的组织或机构，他们一旦遭到攻击或破坏，将导致供应紧缺或中断，严重危害公共安全利益，或者其他严重影响。

德国在联邦层面把关键基础设施定义为以下 9 种：

1、能源；2、信息技术与通信；3、交通；4、医疗卫生；5、水利；6、食品；7、金融；8、政府部门；9、传媒与文化。

五、 英国

2016 年英国公布的国家网络安全战略（2016-2021）中对 CNI（关键国家基础设施）做了界定，主要包括以下 5 个方面：

1、重要企业：已取得极大成功且在研发或知识产权具备很强优势的企业；

2、个人信息数据拥有者：不仅包括大规模数据的拥有者，还包括一些弱势群体信息数据的所有者；

3、高威胁目标：如媒体；

4、顶级数字经济提供商：数字经济的试金石；

5、保险、投资、监管、专业咨询组织等：对改善网络经济领

域网络安全状况有影响的组织机构。

英国对关键国家基础设施（CNI）的界定方法，打破了美国一直以来按照行业特征和部门属性划分关键信息基础设施的常规，从数字经济影响力、数据资源特性等维度，将英国关键基础设施划分为五类。特别值得注意的是，英国甚至把某些专业咨询组织或机构也纳入 CNI 的范围，前提为其对整个经济领域改善网络安全状况有一定影响。

六、 五国对比

中国、美国、俄罗斯、德国、英国这 5 个国家基本上可以代表欧美亚三大经济体中，互联网发展最为活跃的国家。下面我们就从界定领域的角度来横向对比一下这五个国家对于关键信息基础设施政策的异同。

首先，如果不考虑某些领域的界定可能内涵十分丰富的问题，单就各国界定的关键信息基础设施数量来看：美国最多，16 类；中国次之，13 类；接下来是德国 9 类，俄罗斯 7 类，英国 5 类。

国家	中国	美国	俄罗斯	德国	英国
CII 类别数量	17	16	7	9	5

五国划分的关键基础设施（CII）类别数量

值得指出的是，英国对关键信息基础设施的定义方式与众不同，既不是某一类具体的企业或机构，也不是某一种具体的基础设施，而几乎是完全抽象的、概念化的界定基础设施。

除了英国以外，中、美、俄、德四国对于关键信息基础设施的界定方式比较接近。而从关键信息基础设施的界定范围看，中国、美国和德国也极为接近。政府部门、通信和交通运输最受关

注，同时被中、美、俄、德四国圈定。而中、美、德三个国家共同圈定的领域有 7 个，分别是政府部门、通信、交通运输、能源、金融、水利、医疗卫生。此外，中国、美国和俄罗斯均将国防系统也圈定为关键信息基础设施。

下表给出了中、美、俄、德四国界定的关键信息基础设施对比情况。由于英国的界定方式比较特殊，未在下表中列出。

基础设施	中国	美国	俄罗斯	德国
政府部门	✓	✓	✓	✓
通信	✓	✓	✓	✓
交通运输	✓	✓	✓	✓
能源	✓	✓		✓
金融	✓	✓		✓
水利	✓	✓		✓
医疗卫生	✓	✓		✓
公用事业/服务	✓	✓		
工业制造	✓	✓		
科技/科研	✓		✓	
食品、药品和农业	✓	✓		✓
应急响应		✓	✓	
国防	✓	✓	✓	
教育	✓			
社会保障	✓			
重要互联网应用	✓			
化学工业	✓	✓		
商业设施		✓		
信息技术		✓		
核设施		✓		
司法			✓	
传媒与文化				✓
大型装备	✓			

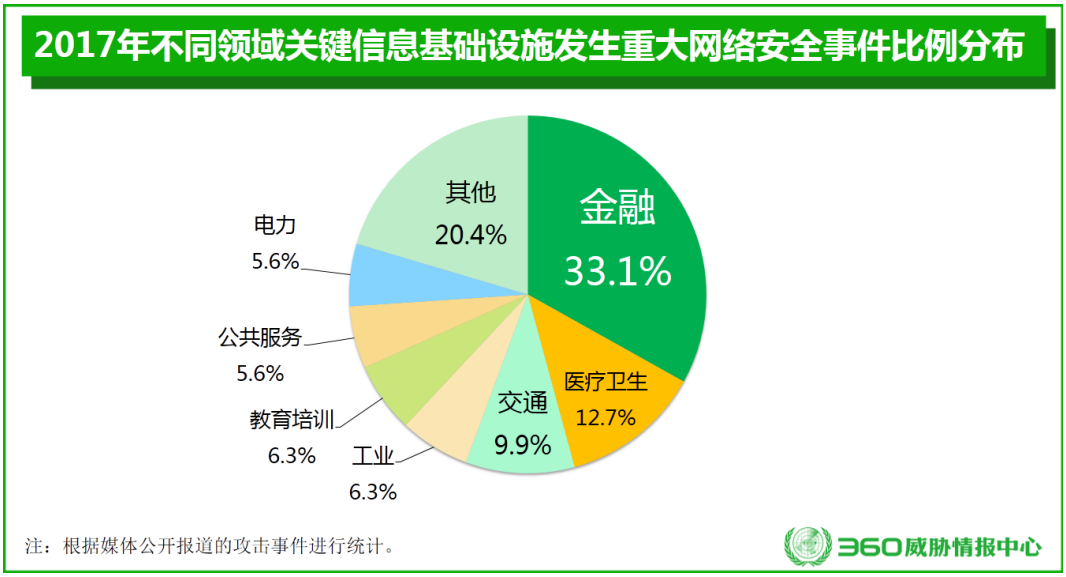
中美俄德四国界定的关键信息基础设施对比

第二章　关键信息基础设施面临的安全威胁

本章将主要参照国际上划分关键信息基础设施的主流类别，即从金融、能源、通信、工业系统、教育、交通、医疗卫生等七个领域分析全球关键信息基础设施面临的安全威胁。首先对全球关键信息基础设施发生的网络安全事件进行综述分析；其次，对七大领域的网络安全威胁分别加以介绍。

一、 综述

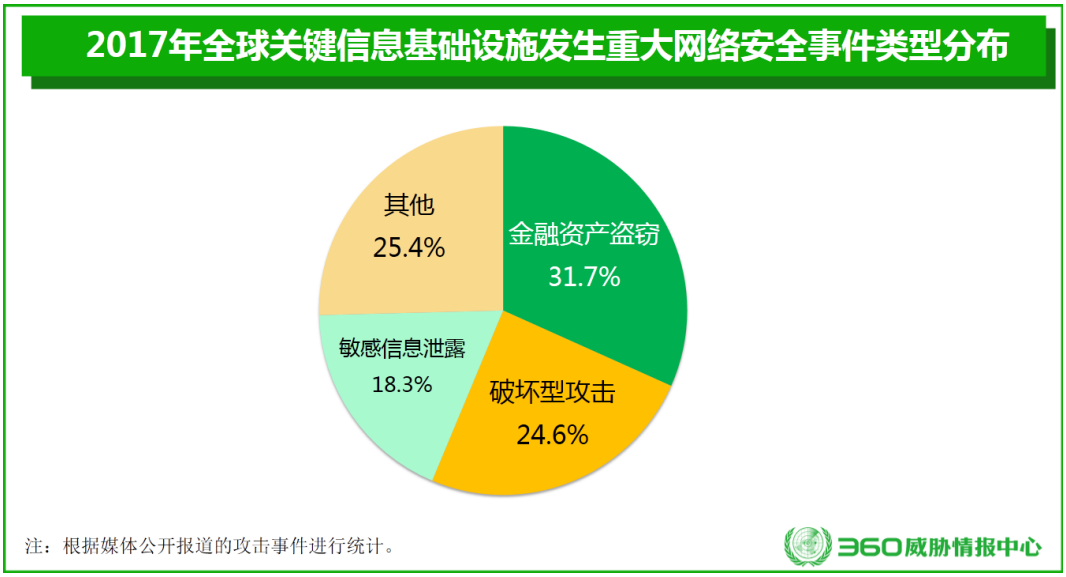
根据 360 威胁情报中心对 2017 年全球关键信息基础设施重大网络安全事件的公开信息监测数据分析，在各类不同的关键信息基础设施中，金融、交通、能源等领域最容易遭受网络攻击，其中金融（33.1%）、医疗卫生（12.7%）、交通（9.9%）、工业（6.3%）等领域信息基础设施发生的重大网络安全事件最多，具体见下图。



注：本章收录的各种典型案例，主要来自于公开渠道收集的各种资讯、新闻报道等，而并不代表全球关键基础设施实际遭遇攻击的规模和频率，因为还有很多中小烈度的网络攻击没有进入我们的研究视野，或者部分关键基础设施遭受的攻击事件没有被公开报道。

根据公开资料统计，全球信息基础设施发生重大网络安全事件的类型主要有敏感信息泄露、系统破坏、金融资产盗窃等。从共性上看，不同领域关键信息基础设施一般都会遭遇敏感信息泄露问题，例如金融、教育、交通、医疗卫生、能源等都发生过许多重大信息泄露事件；同时，不同领域也呈现一定的特点，例如金融领域的窃取金融资产的事件明显偏多；通信、能源领域的系统破坏事件较多，而教育行业领域网站遭篡改的事件明显多于其他领域。

根据 360 威胁情报中心 2017 年的监测数据，金融资产盗窃所占比例最高，占 31.7%，其次是破坏型攻击（24.6%）、敏感信息泄露 18.3%），三者之和约占总数的 3/4。具体见下图。



此外，一般认为发达国家的信息基础设施比较发达，且拥有更多的信息系统直接连接在互联网上，理论上遭遇网络攻击的可能性更高。但根据 360 威胁情报中心的监测数据，以英国、美国、德国为代表的发达国家关键信息基础设施发生的安全事件占比与发展中国家基本持平，分别占 48.6%和 51.4%。这表明以中国、印度、巴西、乌克兰、波兰、孟加拉、越南等为代表的发展中国家，同样面临着关键信息基础设施被攻击的极大可能性。尽管发

展中国家的信息基础设施较薄弱，接入互联网的基础设施也比较少，但并不说明遭遇到的网络攻击因此而减少。同时，在综合防护能力，应急响应能力等方面，发展中国家也远远落后于发达国家，所以网络安全问题对发展中国家的威胁比对发达国家来说更加严重。

二、 金融

2016 和 2017 年，均堪称是金融机构的网络灾害年。大量针对金融机构的攻击给全球各国的金融机构造成了巨大的财产损失。

从攻击者的攻击特点及事发原因来看，在 2017 年，金融机构主要面临以下几类高危风险：SWIFT 攻击、ATM 攻击、信息泄露、恶意软件、网络诈骗、系统故障和 DNS 攻击。

（一）SWIFT 攻击

利用 SWIFT 系统(Society for Worldwide Interbank Financial Telecommunication，既指环球银行金融电信协会，也指该协会运营的世界级金融电文网络）存在的潜在安全漏洞发动网络攻击或借此掩盖罪行的事件。

http://www.aqniu.com/learn/24785.html

就在 2016 年，还只有极少数人听说过环球银行金融电信协会(SWIFT)。该组织的标准化信息格式，被采纳为银行间金融转账的全球标准；相关软件和消息网络，驱动着今天大多数的国际银行转账，每年产生的金融消息超 50 亿条。然而，这并不是大多数人听闻 SWIFT 的原因所在。

2016 年，孟加拉央行和纽约联邦储蓄银行便涉入一场净值 1.01 亿美元的网络劫案——其中大多数资金都未追回。若非其

中一笔交易出现拼写错误引发质疑，另外 8.5 亿美元恐怕也会被盗。随后，对 SWIFT 网络的攻击此起彼伏，越南、厄瓜多尔、乌克兰都发生了此类事件，不过大多数受影响银行和国家都未公开事件。

现在，攻击者开始改变策略，从对用户终端的攻击，转变到对驱动银行系统本身的应用和网络的攻击。直到最近，安置各种 SWIFT 组件的最佳实践，都还是将它们都放到防火墙后面，但这依然阻挡不了同区域内与其他工作负载的自由通信，而且提供不了第 4 层之上的可见性与控制。

2017 年度，全球十余个国家的多家银行机构使用的 SWIFT（银行结算系统）陆续遭到网络攻击，此类系统正是全球金融生态系统的基础。攻击者能够利用金融机构内部的恶意软件操纵处理跨境交易的应用程序，之后可在全球任意金融机构处提取资金。

http://news.xinhuanet.com/2017-04/15/c_1120817020.htm

2017 年 4 月 1 5 日，黑客组织“影子中间人”１４日在推特等社交媒体上爆料说，美国国家安全局曾入侵国际银行系统，以监控一些中东和拉丁美洲银行之间的资金流动。

“影子中间人”发布的文件显示，美国国家安全局利用计算机代码入侵ＳＷＩＦＴ（环球银行间金融通信协会）服务器，并监控ＳＷＩＦＴ信息。文件还曝光了多个入侵ＳＷＩＦＴ系统的计算机代码和监控工具。

（二）ATM 机与 POS 机攻击

作为一种典型的瘦终端产品，银行 ATM 机器在运维管理与升级更新方面也普遍存在着诸多的安全隐患。2017 年就发生了多起针对 ATM 机的重大网络攻击事件。

为了实施各种网络犯罪活动，攻击者们倾向于采用成熟的货币化网络入侵手段。除了攻击 SWIFT（银行结算系统）之外，网络犯罪分子们还一直在积极利用 ATM 感染（包括金融机构内部网络中的 ATM 设备），远程银行系统、PoS 终端网络以及变更银行数据库内余额数据等方法。

2017 年 2 月，34 岁土耳其黑客 Ercan Findikoglu 因盗窃 ATM 机被美国联邦法院判处 8 年的徒刑。这名黑客带领一支跨国网络犯罪团伙入侵 ATM 发卡机构，并伪造卡进行欺诈，2011 年以来累计盗取 5500 万美元。起诉书显示，他于 2011 年至 2013 年间三次未经授权访问发卡机构的 IT 网络。2013 年 2 月，在第三次攻击中（也是最后一次攻击），该团伙仅仅用了 10 个小时在 24 个不同国家提款 3.6 万笔，共提取约 4000 万美元。其中近 3000 笔共计 240 万美元的提款发生在美国纽约市。

2017 年 3 月，趋势科技发现了一种新的 POS 机恶意软件，并将其命名为 MajikPOS。2013 年 1 月底，研究人员第一次发现这款恶意软件。其主要攻击目标是北美和加拿大用户。

https://item.btime.com/03or1860iuuinsl6gpvqd4j5kc5

2017 年 4 月，一群黑客将目标瞄准了俄罗斯的至少 8 台 ATM，一夜之间就窃取了 80 万美元。今年 2 月，黑客使用"无文件病毒"成功攻击了 140 家企业，包括银行、电信和政府组织，范围包括美国、欧洲等地区，不过攻击的细节没有做过多披露。研究人员称，攻击银行时所用的是一种无文件的病毒，它能够存在内存

中，而非像传统恶意程序那样驻足在硬盘中。这款被命名为ATMitch的恶意软件之前在哈萨克斯坦和俄罗斯被发现，病毒通过远程管理模块远程安装和执行的。黑客可以通过SSH隧道部署恶意软件并发送指令给ATM，从而获取现金。

（三）信息泄露

金融信息的泄露往往伴随着大量的用户实名制信息的泄露，同时也会严重威胁到用户金融账户本身的安全。研究表明，金融机构的数据已经成为黑产竞相争夺的重要资源。

https://www.easyaq.com/news/1408747933.shtml

2017年3月20日，亚美尼亚国家安全局成功捣毁了一个犯罪集团。根据初步数据，该犯罪集团成员以酒店与餐厅经营等借口在Armenia 3贸易组织中进行注册，并借此获取终端收银机。在此之后，他们得以通过输入银行卡数据进行非现金交易，而不再需要获得持卡人及其银行卡的详细信息。这个由俄罗斯与亚美尼亚公民组建的网络犯罪集团于2016年8月至12月期间利用计算机技术从澳大利亚多家银行的客户帐户当中总计窃取得8500万德拉姆资金。

2017年4月，英国知名的发薪日贷款（Payday Loan）公司Wonga确定其遭遇数据泄露,并之后发表声明通知客户联系银行。Wonga在声明中指出，黑客可能非法访问了数十万账户的个人信息，关系到预计总计高达27万客户数量的个人信息。本次泄露的信息可能包括：客户姓名、电子邮箱、家庭住址、电话号码、银行卡的后四位数、银行卡账号和银行代码。

https://www.easyaq.com/news/311631939.shtml

https://www.easyaq.com/news/441519587.shtml

2017 年 5 月，根据印度互联网与社会中心（简称 CIS）的一项调查结果，此次经由 4 个印度政府门户站点泄露的 Aadhaar 公民身份信息总量或高达 1.35 亿条，除此之外，还有 1 亿银行帐户也不慎曝光。

http://finance.ce.cn/rolling/201706/02/t20170602_23383458.shtml?lx-oauth=true&fileName=null

2017 年 4 月份，招商银行遭客户质疑信息泄露。中国江西网报道，南昌市民杨先生因接了一个对方自称是招商银行客服人员的电话，一天内就被骗走了 13 万。电话交谈中，对方准确的说出杨先生的个人账单信息、流水记录，还告诉他要一笔欠款要还。

2017 年 5 月，招商银行被曝网银出现严重漏洞，个人信息可被修改。有网友指出，当他登录招商银行专业版网银，进入了修改联系信息页面，弹出了“系统 LU 层异常”的对话框，同时，页面显示了他人的所有详细信息，包括“性别、电子邮箱、常住地址、单位名称、单位地址、单位邮编、单位电话，和部分打了码的银行预留手机号”。

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-7edc07f0-872e-49e8-9c30-ba4f1c0d7929&itemId=869197da-5dc8-4cdb-b726-f1cbd5e9dda6&timestamp=1500946699168&nonce=01447292-4830-4a29-83c0-1b13e4d26a12&sessionId=118405&signature=15e4818fda5a0c0af2dba4071edc11b8b1c99a82

2017 年 7 月，富国银行意外地向一名前理财顾问发送了 1.4GB 包含 5 万名高净值客户信息的数据。这名前理财顾问加里·辛德布兰德（Gary Sinderbrand）正在对富国银行一名员工

提起诽谤诉讼。他原本会收到与本案相关的电子邮件和其他文件，然而富国银行却将数万客户的机密信息，包括姓名、财务信息，以及社会安全号码发给了他。报道称，受影响客户的投资资产达到数百亿美元。

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-50f730eb-5cbc-45d1-9c66-56c3f64f8e92&itemId=38429fd3-55d7-4d3d-b891-fb65e5a5f2a1&timestamp=1512526391023&nonce=3f6ac402-1475-4b38-aaee-88cbb8e640fe&sessionId=264315&signature=9e734e7e02a22234b48052c57120cfb9a9f8fa4b

PayPal 在 12 月 1 日晚些时候发布的新闻稿中表示，该公司在今年早些收购的支付管理公司 TIO Networks 遭遇了网络安全事件，在此期间，攻击者似乎访问了为 160 万用户存储信息的服务器。

（四）恶意软件

银行类木马或网银类木马一直是恶意软件中比较活跃的一种类型。此类木马主要通过窃取用户帐号，劫持支付资金，转移支付对象等手段盗刷用户银行卡或网银帐号。2017 年，各国安全公司都截获了大量新型的高危网银木马。下面给出一些比较典型的新案例。

2017 年 2 月，安全专家已经发布了 Marcher Android 银行木马程序的详细分析，这是自 2013 年底以来一直存在的威胁。恶意软件的第一个变种是为了欺骗用户使用仿冒 Google Play 的钓鱼页面提交支付卡的详细信息。2014 年 3 月，Marcher 被视为

针对德国的银行客户。在 2016 年下半年，该恶意程序威胁到包括美国，英国，澳大利亚，法国，波兰，土耳其和西班牙等在内的多个国家的数十个组织或机构。

2017 年 2 月，英国网络安全企业 BAE Systems 公司的研究人员最近获得并分析了几份针对全球范围内 31 个国家的 104 家机构（其中多数为银行）发起攻击的恶意软件样本。这些样本的攻击复杂度极高，而且黑客组织还在其恶意软件当中故意插入俄文单词与命令，希望借此对调查人员进行误导。

https://www.easyaq.com/news/74723209.shtml

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-ddc73260-9db0-49a1-b09a-1f9953e448e2&itemId=139321b1-0f1d-4d78-a5fa-fc1b2cd062f8&timestamp=1501034916104&nonce=6aa5ae41-0d30-408c-a576-5ae39964a85b&sessionId=119930&signature=3515c1c5b090b4448362cbda3a892d5e454f3a95

2017 年 7 月 TrickBot 银行木马背后的黑客正在对美国银行发起新一轮攻击。有僵尸网络 Necurs 助力，TrickBot 新一轮攻击活动也针对欧洲、加拿大、新西兰、新加坡等国的金融机构。

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-72c892c3-d8be-450d-9ed8-792f01fe077a&itemId=5b140b75-2a87-40b1-ba81-672829d01d76&timestamp=1509413619985&nonce=7c388ccc-426c-466f-b5c2-fd0bc7733950&sessionId=216102&signature=5f6a876dd9222538d5a24296e95a8d47ea966b18

据 IBM X-Force 的研究人员透露，从 2017 年 9 月开始，网络罪犯分子就开始通过垃圾邮件传播一个臭名昭着的银行木马

——Ursnif。Ursnif，也被称为 a.k.a Gozi，是由 Gozi 银行木马经历了多年的更新演变而来。曾是 2016 年金融行业里最活跃的银行木马之一，并一直持续到今年。在先前的活动中，Ursnif 主要针对日本、北美、欧洲和澳大利亚。现在，Ursnif 的开发者已经增强了其逃避安全检测的能力，并将目标集中在了日本。

（五）网络诈骗

金融机构一直是网络诈骗犯罪的瞄准对象，各种新型网络骗术也是层出不穷。

2017 年 4 月份，中国江西网报道，南昌市民杨先生因接了一个对方自称是招商银行客服人员的电话，一天内就被骗走了 13 万。电话交谈中，对方准确的说出杨先生的个人账单信息、流水记录，还告诉他要一笔欠款要还。

2017 年 4 月，据媒体报道，美国国税局（IRS）大学生贷款工具被黑客利用盗走 3000 万美金。出自 IRS 的数据检索工具被黑客利用后，近 10 万人陷于身份盗窃风险之中。该工具是家长用来给使用联邦助学金免费申请表（FAFSA）的孩子传输财务信息用的。仅 2015 年，就有 1700 万学生使用 FAFSA 申请助学金。

虚假报税日渐成为 IRS 面临的一大问题，因为黑客找出了更复杂的方法在线盗取财务文档。仅 2013 年一年，IRS 便向以他人名义申请退税的小偷放出了 58 亿美元退税款。该骗局针对学校、医院和餐馆，大学生是最新一批受害者。

http://www.4hou.com/info/news/5256.html?lx-oauth=true&fileName=null

据美国宾夕法尼亚州总检察长 Josh Shapiro 于 2017 年 6 月 6 日发布的新闻稿表示，Facebook 所有的照片共享应用程序 Instagram 正被犯罪分子用作吸引人们加入银行诈骗活动的招募工具。已经有三名男子成功地使用 Instagram 从多家金融机构窃取了超过 50,000 美元。

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-cee5529a-41a1-4772-84ae-39dc19f5e7c1&itemId=04156557-6dd1-4b20-b57e-d35e55a9bd96&timestamp=1503536938064&nonce=281cc4a4-bda1-4ee8-839d-c1f4958aecdd&sessionId=149387&signature=2ce9ec9293be8c7849a16fb66fa9f582b5bda28a

2017 年 8 月，网络安全公司 Netcraft 发现黑客使用.fish 域名网站来骗取法国银行客户，他们发现一个采用.fish 域名的网站伪装成法国银行网站来对客户进行钓鱼攻击。当有人访问 parser.fish 时，他们将被重定向到一个越南网站，伪装成法国银行 BRED，同时试图盗取用户的银行证书。

（六）DNS 劫持

http://www.cnbeta.com/articles/tech/595229.htm

2017 年 3 月 22 日，俄罗斯第一大私人商业银行阿尔法银行（Alfa）通过新闻公告宣布，阿尔法的网络基础设施遭遇大规模 DNS 僵尸网络攻击。黑客似乎是为了制造假象，让人以为该银行与特朗普团队之间一直有联系。阿尔法目前正请求美国方面的协助，希望通过合作找出罪魁祸首。

（七）DDOS 攻击

2017 年 3 月 22 日讯 Necurs 是全球最大的僵尸网络之一。Necurs 刚开始只针对俄罗斯约会网站和股票网站，后来改变策略，传播各种致命病毒。这个臭名昭著的僵尸网络之前通过发送垃圾邮件散布 Locky 勒索软件。去年六月，该僵尸网络突然消失，没了踪影。而最近，Cisco Talos 团队发现 Necurs 网络犯罪分子卷土重来，这次重操旧业，将被感染的设备作为渠道发送垃圾邮件。

（八）勒索软件

https://www.chinanews.com/gj/2017/06-23/8258964.shtml

2017 年 6 月 23 日 据英国《金融时报》报道，韩国有关部门已进入“紧急状态”，忙于防范黑客组织威胁要对该国最大几家银行发起的网络攻击。

被称为“无敌舰队组织”(Armada Collective)的黑客组织 21 日表示，韩国 7 家主要银行如果未能用虚拟货币比特币(Bitcoin)支付赎金，将对其发起分布式拒绝服务(DDoS)攻击。

这一威胁出炉的一个月前，地标性的“想哭”(WannaCry)网络攻击感染了包括韩国在内的 150 个国家的数十万台计算机。

（九）其他网络攻击

2017 年 2 月，经波兰几家银行证实，在他们的工作人员访问了波兰金融监督管理局后，他们的系统感染了恶意软件。有趣的是，骗子实际上使用波兰金融监管机构——波兰金融监管局（KNF）的网站来传播恶意软件。

2017 年 3 月，360 威胁情报中心在其发布的《中国高级持续性威胁（APT）研究报告》中，披露了一个持续攻击国内多个商业机构、旨在窃取金融交易敏感信息的 APT 组织——“黄金眼”，这也是国内披露的首个针对商业机构的国内 APT 组织。

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-93c17ec4-9ac2-455c-a45e-198f54eca299&itemId=d2d72c77-780a-403c-8849-53180bdd07ce&timestamp=1502416664251&nonce=cfcbbac9-4a15-43f6-9f65-834b3e4041f5&sessionId=136091&signature=f3d995f4aaa84134acd119e077f3978f4b51b24c

2017 年 8 月匈牙利国家银行（National Bank of Hungary）于 8 日表示，黑客通过一系列网络钓鱼企图攻击匈牙利三家主要银行，但国家银行并未提及遭遇攻击的金融机构或实体的名称。

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-f0699e63-9671-4b97-b9ed-8732312b0012&itemId=5af1f050-31f6-45ed-8082-89f97769fb9f&timestamp=1511919597722&nonce=6e743ff0-5dd2-4e23-8016-9f8fff05a043&sessionId=251315&signature=75b9f07d54127aa74d1d0de4eeee822e7a274cf7

2017 年 11 月，网络安全公司 Reversing Lab 研究人员最新发现黑客组织 Cobalt 正通过微软近期披露的 Offic 漏洞（CVE-2017-11882）针对全球银行等金融机构展开网络钓鱼攻击。

2017 年 12 月，英国伯明翰大学安全研究人员公布了移动银行 App 中的安全缺陷，该缺陷可致数百万用户面临被黑风险升高。

包括汇丰银行、英国西敏寺银行和 Co-op 银行提供的 App，还有美国银行的 Health 账户 App，都出现由于“证书锁定”安全机制带来的严重缺陷，数百万用户面临中间人攻击的风险；

（十）内鬼

2017 年 4 月，一名曾在华尔街一家市值数十亿美元的金融服务公司(KCG 控股公司)工作的某高级系统管理员被 FBI 指控，原因是这名男子开发恶意软件窃取了有价值的源代码和加密密钥，而且直接访问了该公司核心业务的数据文件。

他被指控窃取超过 300 万个机密和专有文件，而这些文件是 KCG 业务的核心，这些文件帮助该公司在 2016 年赚取超过 14 亿美元的收入。据了解，该男子还曾在 KCG 控股公司的圣何塞办事处工作长达 7 年之久。

三、 能源

能源企业的生产安全直接关系国计民生，一旦遭遇网络攻击，就有可能造成大规模的断电、断油、断气等重大生产安全事故；同时还有可能造成基础设施信息、地质勘探信息、甚至是军事情报信息等国家核心敏感数据情报资源的泄露。特别的，有大量证据表明，在全球范围内，有多个高级攻击组织，长期将能源企业作为重点攻击目标，有组织、有计划、有目的地进行机密信息窃取和生产系统破坏活动。

在最近三年中，能源行业发生的重大网络安全事件及被曝光的重大网络安全隐患主要体现在以下四个方面：信息泄露问题、破坏性攻击、扰乱性攻击和智能电网风险。下面逐一举例进行说

明。

（一）信息泄露

2017 年 2 月，有一位美国研究者发文披露，美国维德路特公司制造的油品液位仪，存在安全漏洞，导致攻击者可以其错误配置的 telnet 端口获取到该类仪器的油品监测和库存管理系统信息，从而造成加油站信息的泄露，并且有可能通过串口线对加油管理设备直接进行物理设置或控制。

（二）破坏性攻击

2017 年 1 月初开始，土耳其伊斯坦布尔和土耳其其他地区一直在停电。土耳其能源部长表示：最近在土耳其的断电是由于地下电力线路的破坏和源自美国的网络攻击造成的。

2017 年 6 月 27 日讯，美国宾夕法尼亚 Bala Cynwyd 的亚当弗拉纳根（42 岁）因破坏美国东海岸多个供水设施提供商的 IT 网络被判 1 年零 1 天的监禁。弗拉纳根于 2007 年 11 月至 2013 年 11 月在某智能水电气设备制造商担任工程师。2013 年 11 月 16 日，该公司以非公开理由解雇了弗拉纳根。弗拉纳根此后决定报复公司，从而关闭了 TGB，使该公司客户的供水设施网络陷入瘫痪，之后他用攻击性的语言修改了某些 TGB 上的密码。供水设施提供商不得不派遣员工到客户家中手工抄写每月的用水量。

2017 年 6 月，欧洲某具有智能化控制系统的工业化学品石化工厂，称本地控制系统遭遇攻击，所有计算机系统陷入瘫痪并显示错误信息。经 Reddit 用户“C10H15N1”（一名化学工程师，某公司编程逻辑控制器专家）分析，此次勒索软件入侵该公司系统是由于第三方运维单位缺乏安全意识，咖啡机安装人员将咖啡

机连接到了内部控制室的网络，之后安装人员发现咖啡机无法联网又将其连接到了独立的 WiFi 网络。而咖啡机被勒索软件感染，后传播到了工厂内，导致内网系统大面积瘫痪。

结果水落石出，错误出在管理咖啡机的外部公司身上。从此事可以看出，设备安装哪怕出现一点小疏忽，而会铸成大错。设备安装人员应仔细查看设备连接的网络。

2017 年 12 月，全球最大石油运输公司 —— 俄罗斯管道巨头 Transneft 周五（12 月 15 日）证实，其计算机系统感染了秘密挖掘加密货币 monero 的恶意软件。目前尚未知晓有多少设备受到影响，Transneft 官方也暂未透露更多细节。

（三）扰乱性攻击

扰乱性攻击泛指一切非破坏性攻击。

2017 年 9 月 8 日，赛门铁克安全研究员找到证据显示，美国、土耳其和瑞士的数百电网遭到大规模黑客攻击。该公司为此次攻击命名 Dragonfly 2.0。赛门铁克警告道，黑客如今手握全球多个电网登录凭证，有制造断电事件的潜力。

（四）智能电网风险

2017 年 1 月，在德国汉堡进行的一次通信领域专业学术会议上，Vaultra 公司（一家专门为智能硬件提供安全解决方案的公司）的创始人 Netanel Rubin 指出：智能电表存在严重漏洞，已对消费者构成安全风险。

2017 年 4 月，根据堪培拉大学网络安全中心的 Nigel Phair 发表的论文（PDF），黑客完全能够入侵你家的智能电表，监控你家的用电情况已经确认你家多长时间处于闲置状态。

四、 通信

在所有关键信息基础设施中，通信系统的信息资源是最为丰富的，一旦遭到攻击，很容易泄露大量的用户个人信息。同时，通信系统的安全性也是整个网络系统安全性的基础。当通信系统遭到破坏时，其他关键信息基础设施的安全往往无法保障。

从 2017 年的情况来看，通信系统面临最大的安全威胁主要来自两个方面，一个是由网络攻击造成的断网威胁，一个是电信系统的信息泄露风险。

（一）断网威胁

2016 年，因通信系统被攻击而引发的灾难性事故，最为让人印象深刻就是美国断网事件和德国断网事件。2017 年，此类事故仍然引起大家的广泛关注。

1） 美国断网事件

2017 年 11 月，美国又遭遇了一场大范围的断网。从西海岸的加利福尼亚、到东边的纽约，多家互联网服务提供商（ISP）均受到了影响。DownDetector.com 给出的最新信息显示，康卡斯特（Comcast）在山景城、丹佛、纽约、波特兰、芝加哥、西雅图、休斯顿、旧金山、以及明尼阿波利斯等地的节点受影响较大。

据 Wired 报道，本次事件由一次“路由泄露”（route leak）意外引发。当 Autonomous Systems 公司在自家网络上分配了不正确的 IP 地址信息之后，导致 ISP 的路由效率低下和失效。

2） 委内瑞拉遭遇网络攻击 700 万手机通讯瘫痪

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-671f2c76-da3c-46a7-8ebe-f265450aa630&itemId=bd364453-

f498-482f-8893-250efa05cd88&timestamp=1502759338740&nonce=d048ec4e-cf6b-42e6-bff0-c001aea83167&sessionId=139225&signature=a2724e580a094dce55cdcb34e9bab1751e2f3590

2017 年 8 月，委内瑞拉政府表示，政府网站本周早些时候遭遇大规模网络攻击，导致 700 万手机用户无法使用通信服务。

一支自称“The Binary Guardians”的组织宣称对此负责。攻击使委内瑞拉政府、最高法院和国会的网站关闭。

（二）信息泄露

1） 英国最大移动运营商 Three 再陷“数据泄露”风波

https://www.easyaq.com/news/1459681288.shtml

2017 年 3 月，随着互联网和大数据不断发展，人们对数据安全的关注度越来越高。目前在全球范围内，英国的数据泄露仅次于美国。近日，英国移动运营商 Three 客户数据再次被泄，这次是因技术问题导致客户的个人信息被泄。

2） 西班牙电信德国子公司证实，黑客利用 SS7 漏洞窃取验证码，将客户账上的资金洗劫一空

2017 年 5 月 8 日，西班牙电信德国子公司 02 证实，该公司客户的银行账户遭到 SS7 漏洞利用攻击。

盗贼利用 SS7 窃听发送给网银客户的双因子验证码，然后借之将账户上的资金搜刮一空。多个消息来源印证，盗窃案在过去几个月里时有发生。黑客先向受害者电脑植入恶意软件，收集银行账户余额信息、登录信息和账户口令，以及手机号码。然后他

们购得流氓电信提供商访问权，将受害者手机号重定向到自己掌控的另一部手机，登陆受害者网银账户，将钱转走。

3） 黑客攻击马来西亚 12 家电信公司 政府服务器和数据库遭劫

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-7c004d2e-f0ee-4c43-be9a-494f7fa58947&itemId=034a5cd7-a489-4318-a46f-b175684ea58e&timestamp=1509932646672&nonce=840d6ef3-7b79-4c5b-9439-729723564d1c&sessionId=224695&signature=19e6dc09cc4cd5ad5635b27073a88b531d0dfae5

2017 年 11 月，黑客袭击政府服务器和数据库，马来西亚 12 家电信公司遭劫，4620 万被盗账户，成千上万条医疗记录，被骗子放到了网上售卖，马来西亚几乎每个人的数据被黑客扫荡一空。

4） 美国运营商 AT&T 的电视网关被爆 0day 漏洞，可远程 ROOT 设备

https://mp.weixin.qq.com/s/JShw6WpOwZLSgyOqjvDdQg?lx-oauth=false&&fileName=null&pubExponent=10001&pubModulus=99f11cb10cb7a3b3eac32597338325e2396602630b85dbfe29715afe77f7689b899177a08eb9242fe7b3ab2f9844534f20e09b39ac1b3155e3bfb8d9052733efb234d3fda01957b20a88fcbeb03337782f6865ccb5b9174cc9acfebfb86f284520747cfb5eaed33f3125b0e91b00d1d93c8a437336088bd150097faff011dacb

趋势科技安全研究人员 RickyLawshae 公开了 AT&T DirecTV WVB 设备组件中存在易于利用的 0day 漏洞（编号 CVE-2017-17411），黑客利用该漏洞可以获取 root 权限，从而完全控制该设备，数百万注册 DirecTV 服务的用户将面临风险。

五、 工业系统

工业系统本身并不是一种独立的关键信息基础设施类型。但能源、水利、工业制造等关键信息基础设施中，往往都会大量使用工业系统或工控系统。故此，我们在针对关键信息基础设施的网络安全分析中，也特别把工业系统作为一个子类来进行讨论。

（一）黑客攻击

2016 年以来，针对工业系统的木马病毒层出不穷，并先后引发了多起重大安全事故。

2017 年 3 月，工业网络安全公司 Dragos 发布报告称，一款针对工业系统的恶意软件伪装成西门子固件进行传播，全球范围内，已经至少有 10 家工厂(其中 7 家位于美国)中招，并且已经感染了多种工业设备。

据 Dragos 的披露，早在 2013 年，美国一个 ICS 机构就提交了西门子 PLC 控制软件的样本。最开始，各家杀毒软件厂商都将其标为误报，但最终呈现出来的确是实实在在的恶意软件。调查发现：过去 4 年中，该恶意软件围绕西门子设备所做的变种翻了 10 倍，最近一次截获的该恶意软件的新变种是在 2017 年 3 月。

https://www.easyaq.com/news/1029984171.shtml?lx-oauth=true&fileName=null

2017 年 6 月， 位于斯洛伐克反病毒厂商 ESET 和美国马里兰州工业网络安全企业 Dragos Inc.的安全研究人员们表示，他们发现了一种对关键的工业控制系统存在威胁并能够导致停电的恶意程序。ESET 该恶意软件命名为“Industroyer”，Dragos 将该恶意软件命名为“Crashoverride”，将威胁攻击者称为“ELECTRUM”。安全研究人员们认为，这套被称为“Crashoverride”或者“Industroyer”的恶意程序框架正是去年 12 月导致乌克兰基辅北部地区停电数小时的罪魁祸首。

https://www.easyaq.com/news/362319310.shtml?lx-oauth=true&fileName=null

2017 年 6 月，卡巴斯基实验室 15 日发布的报告指出，此前一波针对世界各地工业企业的恶意活动被初步确认为由尼日利亚网络犯罪分子所组织之网络钓鱼攻击。

黑客在一系列攻击活动中使用的恶意软件已经帮助黑客窃取到大量可实现商务邮件违规（简称 BEC）攻击的数据——具体来讲，攻击者可以借此冒充业务合作伙伴或者客户，从而诱使目标企业内的工作人员转出大笔资金。

2017 年 9 月，赛门铁克宣称，一年来美国、土耳其和瑞士的数百电网遭到大规模攻击，掌握电网登录凭证的黑客有可能具备制造断电事件的能力。

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-e5f528fd-8bce-4c26-80e3-21257b46d75e&itemId=dd3209f4-7cf1-4edd-bca0-05bd7e79fafa&timestamp=1513561696125&nonce=de23dd0a-51d6-4048-9338-a53fdab2864f&sessionId=273648&signature=4f145908a0435c8137562ad08438dd3ae58ebde6

2017 年 12 月，根据网络安全研究人员的推断，为国家工作的黑客组织攻击了一个属于关键基础设施的安全系统，导致该系统终止了运营。使用复杂的恶意软件，黑客可以对工作站进行远程控制，并关闭系统。Fireeye 和赛门铁克的报告均表示攻击者利用了工控恶意软件 TRITON，攻击了施耐德电气公司 Triconex 安全仪表系统（Triconex Safety Instrumented System，SIS）

（二）安全漏洞

工业企业同样饱受安全漏洞的困扰，特别是工业控制系统的

安全漏洞，修复难度很大，因为通常情况下，我们必须保证在不中断生产的情况下修补漏洞，同时还必须保证漏洞修复后不会影响生产。

https://www.easyaq.com/news/1441429343.shtml

人们一般会认为关键基础设施厂商会十分注意安全，就算不是真的在乎，那也会假装很在意。2017 年 4 月，工控行业的安全漏洞引发多方关注，法国施耐德电气（Schneider Electric）过去就曾被披露存在安全漏洞，并且被提醒：电气开发人员切勿使用硬编码密码！

六、 教育

从 2017 年以来的情况看，教育机构在全球范围遭遇的网络攻击以信息窃取为首要目的；另有部分教育机构也会遭到网站被黑、被恶意篡改攻击。此外，由于教育往往与科研密不可分，因此也成为很多以窃取科技情报为目的 APT 攻击者的重点攻击目标。

（一）信息泄露

2017 年，全球多所知名高校都遭遇了重大的信息泄露事件。

2017 年 3 月，美国福赛斯公立学校上周末（周五或周六）遭遇恶意软件攻击，给学校教师、学生、家长和地区行政人员造成影响。

2017 年 12 月，罗格斯大学的官员证实，1700 名罗格斯学生的学术信息在 11 月 8 日和 9 日的数据安全事件中遭到了在线暴露。罗格斯大学发言人 Neal Buccino 强调，暴露的数据不包括任何人的社会安全号码（Social Security number，SSN）、家庭

住址或财务信息。

（二）网站篡改

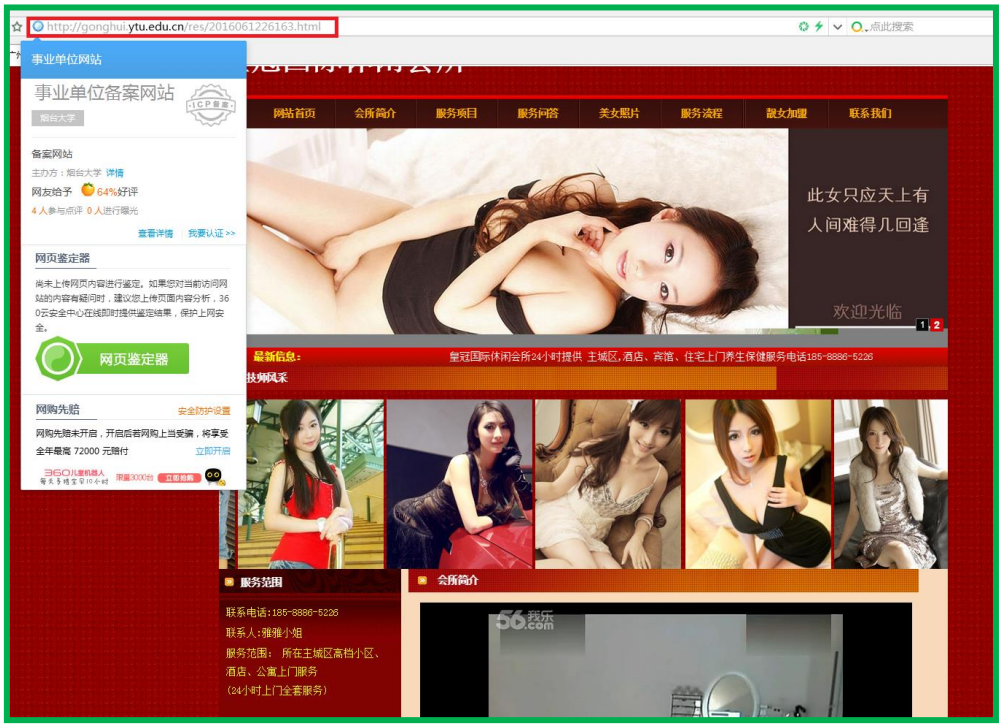
2017 年 5 月，Facebook 首席执行官马克·扎克伯格（Mark Zuckerberg）参加了哈佛今年的毕业典礼并做演讲。著名的哈佛校园媒体《哈佛深红报》(The Harvard Crimson)也对此进行大篇幅报道。 然而《哈佛深红报》随后却发现自己的网站发生了变化， 扎克伯格照片被 PS，而他的名字也变成 “Mork Zinkletink”。

事实上，360 互联网安全中心每年在国内截获的高校网站被篡改案例也很常见。下面给出的就是近两年截获的部分教育高校网站被篡改的具体实例。

1） 网站域名：ytu.edu.cn，网站（备案）名称：烟台大学

网站首页：

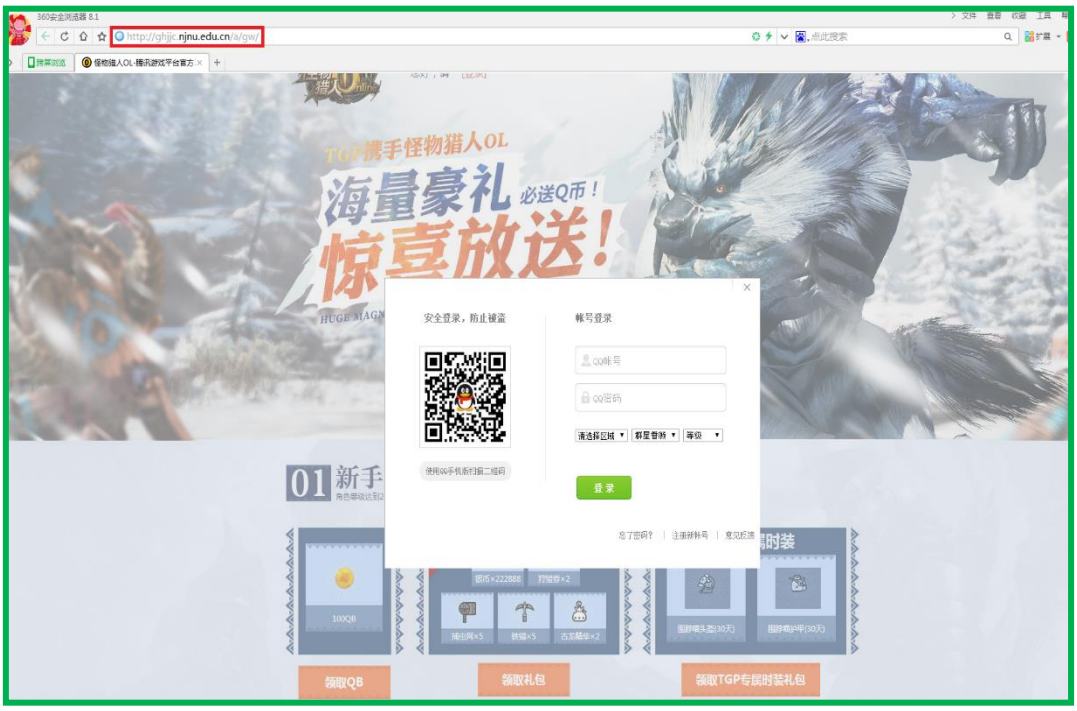
被植入的非法网页：



2） 网站域名：njnu.edu.cn，网站（备案）名称：南京师范大学

网站首页：

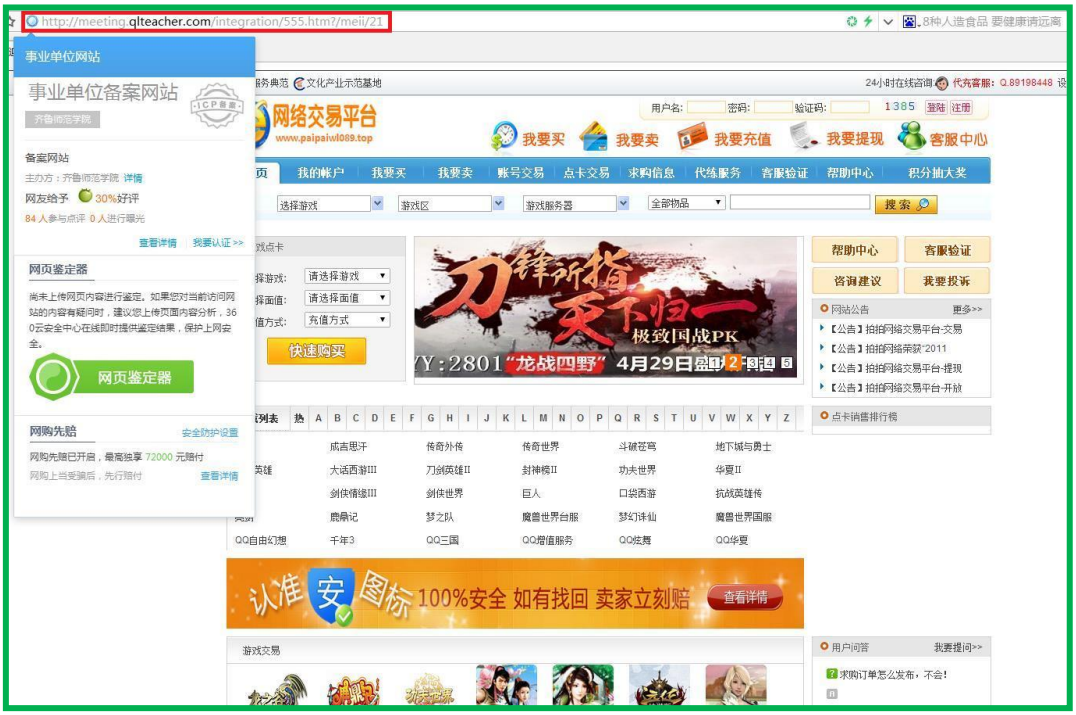
被植入的钓鱼网页：



3） 网站域名：qlteacher.com，网站（备案）名称：齐鲁师范学院

网站首页：

被植入的钓鱼网页：



（三）DDOS 攻击

专门针对教育机构发动 DDOS 攻击的情况并不太常见。但随着 DDoS 攻击本身的泛滥化，教育机构也难以幸免。

2017 年 2 月，美国一所不知名的大学遭到 5000 余台校园物联网设备的 DDoS 攻击。此次攻击是威瑞森公司在其《2017 年数据泄露文摘》的前瞻报告中详细描述了这起校园 DDoS 攻击。遭到攻击初期，大批学生表示网速极慢。经校方人员调查后发现，发起 DDoS 攻击的正是校园周围 5000 多台 IoT（物联网）设备构成的僵尸网络。在这些受感染 IoT 设备中，大多竟然是校园内的自动售货机。

七、 交通

给交通系统带来最大网络安全挑战的可能是智慧交通本身。作为关键信息基础设施，交通领域涵盖的范围比较广泛。民航、铁路、公交、公路、海运、汽车等都属于交通范畴。但是，不同形式的交通系统，其面临的网络安全威胁也有很大的区别。因此，

本小节将选几种从不同类型的交通系统为例，分析其目前所面临的网络安全威胁。

（一）民航（航空）

2017 年以来，全球民航系统因遭遇网络攻击而导致的重大安全事故就持续不断。其主要危害形式表现为以下几个方面：大范围航班延误；旅客信息泄露；巨额商业诈骗。下面我们就逐一展开并通过典型案例进行分析。

1）网络攻击或系统故障导致大范围航班延误

- 英航网络瘫痪不是黑客所为，只是工程师拔错电源

http://tech.sina.com.cn/i/2017-06-06/doc-ifyfuzny3649857.shtml?lx-oauth=true&fileName=null

2017 年 5 月，英国航空公司的计算机网络出现严重故障，导致上千个航班被取消，约 7.5 万名乘客受到影响。英国航空当时表示，这起事故是电力故障所致，而不是遭遇黑客攻击，但具体的原因仍在调查中。6 月 6 日，英国航空母公司国际航空集团(IAG)CEO 威利·沃尔什(Willie Walsh)向记者证实，这是一起人为事件。沃尔什称，当时位于伦敦希思罗机场(Heathrow)附近的一个数据中心的电源被一名工程师错误地拔掉。

综上所述，不论是网络攻击还是系统故障引发的民航系统停飞或航班延误事件，都充分表明了民航系统在网络安全方面的脆弱性。而且攻击者想要破坏民航系统，并不需要对民航系统业务特别了解，而仅仅是进行诸如数据清除或系统破坏之类的攻击，就足以造成巨大的经济损失和社会影响，甚至可能引发飞行事故。

2） 黑客攻击导致的大量民航用户数据泄露问题

a) 民航网信安全管理:不得收集与服务无关旅客信息

http://news.youth.cn/jsxw/201702/t20170221_9147796.htm

2017 年 2 月，国务院法制办就《民航网络信息安全管理规定(暂行)(征求意见稿)》公开征求意见。《征求意见稿》要求民航各单位制定旅客信息保护制度,对在提供服务过程中收集、使用的旅客信息,应当采取相应措施严格保护,不得泄露、篡改或者毁损,不得出售或者非法向他人提供。

与多数公共服务系统类似，各国民航系统也都储存了大量的用户实名制信息。这也是大量网络黑客瞄准民航系统进行攻击的主要原因之一。被盗取的实名制信息、乘坐航班信息等，都可被用于从事网络诈骗活动，并且这种现象在国内尤为猖獗。此外，很多实名制信息还与里程积分等可变现资源相关联，黑客盗取用户信息后，盗刷用户里程积分的事情也屡见不鲜。

b) 澳大利亚曝光一起黑客入侵波斯国际机场计算机系统，盗取高度敏感数据的事件

澳大利亚珀斯国际机场于 2016 年发现一名越南籍黑客 Le Duc Hoang Hai 入侵其内部计算机系统，窃取了机场敏感安全细节和建设计划。。

通过调查，警方发现该名男子于去年 3 月使用第三方承包商的资质进入珀斯国际机场的计算机系统窃取了大量与机场相关的数据，此外，调查发现 Le Duc Hoang Hai 曾还攻击过越南基础设施和网站，包括银行、电信和在线军事报纸等。

根据当地联邦警方收集的证据，Le Duc Hoang Hai 非法访问计算机系统的目的主要是进行信用卡盗窃 ，并试图盗取支付

卡数据。该名男子最终于 2016 年因非法入侵珀斯国际机场计算机系统被越南军方法院判刑四年。

事件发生后，珀斯国际机场增加了 200 万美元的额外安全措施。同时珀斯国际机场表示，机场及其工作人员、乘客或合作伙伴的安全从未受到任何损害，并且确信被窃取的数据不会对旅游公众造成任何威胁。

3） 针对航空企业的金融盗窃与商业诈骗造成巨大损失

2017 年 6 月丹麦航运公司马士基遭遇 Petya 勒索软件，业务损失超过 2 亿美元。据马士基集团官方确认，马士基集团旗下多个网址遭受黑客袭击，并导致系统瘫痪，几乎影响到马士基旗下的所有业务板块。马士基集团确认：包括旗下的集装箱海运业务、港口、拖船、油气、钻探以及油轮公司纷纷受到影响。

4）其他值得警惕的民航系统安全漏洞

2017 年 1 月，第 33 届混沌通信大会（Chaos Communications Congress）上，知名黑客 Karsten Nohl 和 Nemanja Nikodijevic 演示证明了最近的国际航空订票系统在设计上是存在严重的安全漏洞。利用这些漏洞，攻击者可以轻易取消、修改航班预约，甚至可以轻易的猜测到具有高级权限的航空机构管理员的账户密码，登陆系统并进行任意操作。

2017 年 11 月，在一个安全会议上，一名美国国土安全部（DHS）官员透露，其专家团队一年前在大西洋城机场，远程渗透进一架波音 757 的无线通讯系统。他表示， DHS 于 2016 年 9 月 19 日购得这架飞机，两天之后，他们成功实施远程、非合作式的渗透

入侵。Hickey 表示实验期间无人触碰过这架飞机，也就意味着不存在内部威胁一说。他们使用特别的设备绕过安全机制，并进入飞机的系统。

（二）铁路

a）瑞典交通机构遭受 DDOS 攻击

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-570fed0d-e4db-4934-9f30-9cf54f4db704&itemId=73bbc28d-13f6-4388-98e6-10c23e2efb4c&timestamp=1508376948193&nonce=959526e0-744a-41b8-a932-e1edc83538ed&sessionId=202873&signature=52efdb01470d59e2631859335341b2584ce861e1

据外媒报道，瑞典三家交通机构的 IT 系统于 2017 年 10 月 11 日、12 日分别遭到黑客 DDoS 攻击，导致官网服务掉线、列车运行延误。

调查显示，黑客于 10 月 11 日针对瑞典运输管理局（Trafikverket）展开 DDoS 攻击，导致该机构负责管理列车订单的 IT 系统瘫痪，以及电子邮件系统与网站宕机，从而影响了旅客预定或修改订单的情况。不过，该机构随后通过 Facebook 向旅客提供了有关情况的最新信息。

b）新加坡发生地铁相撞事故

https://www.lx.b.360.cn/pc/richMedia/displaySecondM

sg.do?lx-oauth=true&code=WWW-6e22b6d1-76d5-42a4-b97a-0e0760a4eea3&itemId=bc96e066-d579-4fbe-b67d-b96247491930&timestamp=1510882612631&nonce=dace4ec7-fac6-4600-9723-081dabbba881&sessionId=240366&signature=ba9b5dcb0f19dcab0c6f9e9d61dd78faad0b7509

当地时间15日早上8点多,新加坡发生两辆地铁相撞事故,一辆列车在裕群站附近撞上另一辆停在轨道上的列车,当时后车时速约16km/h,目前造成29名乘客受伤,大部分人只是受轻伤。初步显示与防护系统被移除有关

（三）智能汽车

严格的说,智能汽车本身还构不成关键信息基础设施。但是,智能汽车、车联网、电动汽车在近年来的快速发展已经对交通运输领域产生了深刻的影响。所以，本小节也把智能汽车的网络安全性问题作为交通领域网络安全的一个分析点。

1） 勒索攻击

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-f48d46b4-403b-42f7-ade2-f6bf3e63fd21&itemId=879033cb-c2fe-4290-9f25-0da995a0dacb&timestamp=1510624599785&nonce=b695807e-b39b-4ab6-82db-e2a2c60b3513&sessionId=235539&signature=0b000af006e5aa2daa5f30c02c85455a5033b4f4

2017年11月，美国通用汽车制造中心遭勒索软件攻击，众多城市服务被中断。

2） 安全漏洞

无论是专家还是公众，对于智能汽车最大的担忧无过于不断被发现的新的安全漏洞。2016 年，智能汽车及车联网又有一系列重大的安全漏洞被曝出。

2017 年 2 月，俄罗斯安全公司卡巴斯基的一组研究人员对 9 辆互联网汽车的 Android 应用（来自 7 家公司）进行了测试，这些应用的下载量已经超过几十万，甚至部分超过了 100 万。但这些应用却连最基础的软件保护都没有提供，更别说帮助车主保护这个重要的宝贵财产之一。研究人员表示，通过 Root 目标设备，欺骗用户安装恶意代码，黑客能够使所有 7 款应用来定位车辆位置，解锁车门，甚至能够在某种情况下点火启动。

2017 年 8 月 3 日，三位安全研究员发现，宝马、福特、英菲尼迪以及日产车辆当中使用的远程信息处理控制单元(简称 TCU)存在安全漏洞。目前在全球范围内有近 1.12 亿的互联网汽车，汽车网络安全的全球市场预计将成倍增长，至 2024 年收入将接近 50 亿美元。

3） 数据泄露

https://www.easyaq.com/news/1871049058.shtml?lx-oauth=true&fileName=null

a）1000 万辆汽车 VIN 识别码数据被泄

2017 年 6 月，在已经发现一个汽车数据库被泄露至网络当中，数据库囊括美国本土出售的上千万辆汽车以及相关购买者的个人信息。受这起泄露影响的汽车经销商包括 Acura(讴歌)、BMW（宝马）、 Chrysler（克莱斯勒）、Honda（本田）、 Hyundai（现代）、 Infiniti（英菲尼迪）、 Jeep（吉普）、 Kia（起亚）、 Mini（迷你）、 Mitsubishi（三菱）、Nissan（尼桑）、Porsche（保时捷） 和 Toyota（丰田）。

b）东风日产加拿大遭黑客入侵，113 万客户信息或已泄露

https://mp.weixin.qq.com/s/1UVCMxDoe8aedu3bvUqLNA?lx-oauth=false&&fileName=null&pubExponent=10001&pubModulus=99f11cb10cb7a3b3eac32597338325e2396602630b85dbfe29715afe77f7689b899177a08eb9242fe7b3ab2f9844534f20e09b39ac1b3155e3bfb8d9052733efb234d3fda01957b20a88fcbeb03337782f6865ccb5b9174cc9acfebfb86f284520747cfb5eaed33f3125b0e91b00d1d93c8a437336088bd150097faff011dacb

2017 年 12 月 11 日，东风日产加拿大发现自己似乎成为了数据泄露的受害者。目前，该公司正在通过电子邮件通知客户关于这起事件。虽然目前还不清楚究竟有多少客户受到数据泄露的影响，但出于安全考虑，该公司已经与所有现有和以前的客户（大约 113 万人）进行了联系。

（四）海事

a）丹麦航运公司马士基遭遇勒索

2017 年 6 月丹麦航运公司马士基遭遇 Petya 勒索软件，业务损失超过 2 亿美元。据马士基集团官方确认，马士基集团旗下多个网址遭受黑客袭击，并导致系统瘫痪，几乎影响到马士基旗下的所有业务板块。马士基集团确认：包括旗下的集装箱海运业务、港口、拖船、油气、钻探以及油轮公司纷纷受到影响。

b) 英最新航母被曝：电脑系统是微软公司一款已经停止支持的软件

http://news.163.com/17/0627/20/CNVBA7I7000187VE.html

2017 年 6 月，据外媒报道，英国海军最新航空母舰“伊丽莎白女王号”(HMS Queen Elizabeth)正式试航。不过，有英国媒体发现，这艘造价高达 35 亿英镑的航母，其控制室使用的计算机系统，是微软公司一款已经停止支持的软件 Windows XP。鉴于今年 5 月有黑客发动大规模攻击的目标之一，正是 Windows XP，外界担心航母的“铜皮铁骨”之下，计算机系统会不堪一击。

c) 英国海军称将把黑客攻击视为美国军舰撞船事件可能原因之一。

2017 年 8 月，美国军舰约翰·S·麦凯恩号与利比里亚油轮在新加坡附近相撞后，美国海军作战部长约翰·理查德森上将下

令，在海军调查相撞原因期间暂停舰队行动，而可能的调查方向包括了网络攻击。

一名美国海军官员向CNN透露，该军舰在靠近马六甲海峡时发生了“操舵失灵”，导致与该商业油轮相撞。“该官员称，尚不清楚为什么船员未能使用备用操舵系统保持控制的原因。”

CNN补充道，另一名海军官员称，“有迹象表明该驱逐舰就在相撞前失去了对船舵的控制，但操舵系统在之后又恢复了。”

前以色列情报机构网络战部门员工伊泰·格里克称，麦凯恩号撞船事件可能是黑客攻击的结果。

八、 医疗卫生

治病救人的医疗卫生机构也会成为网络攻击的目标。2016年12月，TrapX Security发布研究报告称：2016年以来，全球至少有93个网络攻击事件发生在医疗机构，而全年医疗保健行业的攻击增加了63%。

医疗卫生系统面临的网络安全威胁主要分为两类，一类是医疗机构及病人资料的泄漏，一类是医疗系统或医疗设备存在漏洞可能被入侵和破坏。

（一）信息泄露

a）黑客入侵英国国家医疗服务体系 NHS，窃取数千医疗人员资料

http://www.zdnet.com/article/hackers-steal-personal-data-of-thousands-of-hospital-staff/

2017 年 3 月，黑客窃取了数千名 NHS 医疗专业人员的信息。网络攻击者渗透到由 IT 供应商 Landauer 运营的数据服务器中，窃取了工作人员的姓名，出生日期，辐射剂量以及使用 X 射线工作的国民保险人员数量。

b）黑客入侵医疗信息系统 7 亿个人信息泄露被倒卖

http://news.163.com/17/0416/13/CI59FGDC00018AOP.html

2017 年 4 月，浙江松阳警方侦破一起特大侵犯公民个人信息案件，查获非法获取的各类公民个人信息 7 亿余条，共 370 余 G 的电子数据，抓获犯罪嫌疑人 20 名，其中查获 2 名入侵相关信息系统的网络黑客。

警方发现，这是一个完整的贩卖公民个人信息产业链，最底下的购买者是电信诈骗团伙，上家是贩卖信息中介，而源头就是网络黑客。

c）美国最大医疗保险公司同意为 2015 年数据泄露诉讼案赔偿 1.15 亿美元

http://fanyi.youdao.com/WebpageTranslate?url=http://securityaffairs.co/wordpress/60464/data-breach/anthem-115m-settlement.html&type=AUTO&action=%E7%BF%BB%E8%AF%91&keyfrom=360se

2017 年 6 月，美国最大医疗保险公司 Anthem，同意为 2015 年数据泄露集体诉讼案赔偿 1.15 亿美元。对 Anthem 的袭击揭露了 7880 万条记录，据调查此案的专家说，这可能不是一次骇人听闻的袭击，而是几个月内持续低调的信息。这次袭击是为了保持低于公司的 IT 和安全团队的警觉，利用机器人感染将数据泄露出组织。记录包括姓名，出生日期，地址和医疗身份证号码，财务和医疗记录没有暴露。

d）美最大医保公司再遭数据泄露事件，1.8 万用户受影响

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-92320a72-cc73-4101-9713-c5f7e1da95c0&itemId=560ab451-7a62-4a14-9fd9-df1726229ae4&timestamp=1501724093949&nonce=211487f2-b5f5-4fd9-9a3e-807de87ecf0e&sessionId=127912&signature=7a4d2acc48c018afac7092e4685c242d1756a88d

Anthem 在 2017 年 7 月 24 日向美国卫生和公共服务办公室报告了数据泄露事件，该办公室根据 2009 年颁布的 HITECH 法案追踪数据泄露事件。

Anthem 表示，这次数据泄露衍生自第三方公司 LaunchPoint Ventures 在 2016 年发生的数据泄露事件，该公司向 Anthem 提供保险调解服务。LaunchPoint 上周表示 2016 年 7 月 8 日，一名员工向自己的个人邮箱发送了一份文件，里面包含 Anthem 会员的个人信息。LaunchPoint 直到今年 4 月份也就是事件发生 10 个月之后才知晓此事。该公司表示这名员工随后被解雇并被送进监狱，目前正在调查一起不相关事件，他“可能跟身份盗窃活动有关”。LaunchPoint 了解到这名员工牵涉了 4 月份的偷盗活动并且在一个月后知悉，某些非 Anthem 数据可能在他任职期间被恶意使用。

e) 黑客入侵英国顶级整形医院数据库

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-873bbf68-65c3-4a89-bb70-6a41b358fd4b&itemId=a3751885-7321-4f5a-a4b1-f2b74bd0f153&timestamp=1508981898273&nonce=f7e3efa0-6d2a-4414-a4cd-9f33471ee94c&sessionId=211061&signature=09ded46507f113b50d683584e2a64c533e73f4db

2017 年 10 月，黑客组织 Dark Overlord 入侵英国顶级整形美容医院 London Bridge Plastic Surgery (LBPS) 的数据库，获取了大量的隐秘信息。

这些资料中包含有病人的名字、住址，更关键的是还有很多生殖整形、丰胸等手术的私照，其中除了普通人，还有英皇室成员和明星艺人，容量高达 TB 级。

（二）设备漏洞

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-df339140-eff6-4385-a44e-11392b04eec2&itemId=503b0373-f8e4-41f3-aaa9-64569f6805ac&timestamp=1504489925607&nonce=6f10c588-0239-4b81-a657-946188d5f691&sessionId=159909&signature=cb3f4702eed31a0a36cabb49d24f1d8ce4c3010d

2017 年 9 月，美国国土安全部的 CERT 团队宣布了一条惊人的消息，雅培公司生产的 100 万个心脏起搏器有近一半极易遭到黑客攻击。这些设备通常被植入到胸部皮肤下面，通过电线进入心脏以保持它的正常跳动。这已经是雅培起搏器遭遇的第三次重大漏洞事故了。起搏器附近的黑客可以利用该漏洞非法访问心脏起搏器，并允许他们发出命令，改变设置并干扰起搏器的功能。

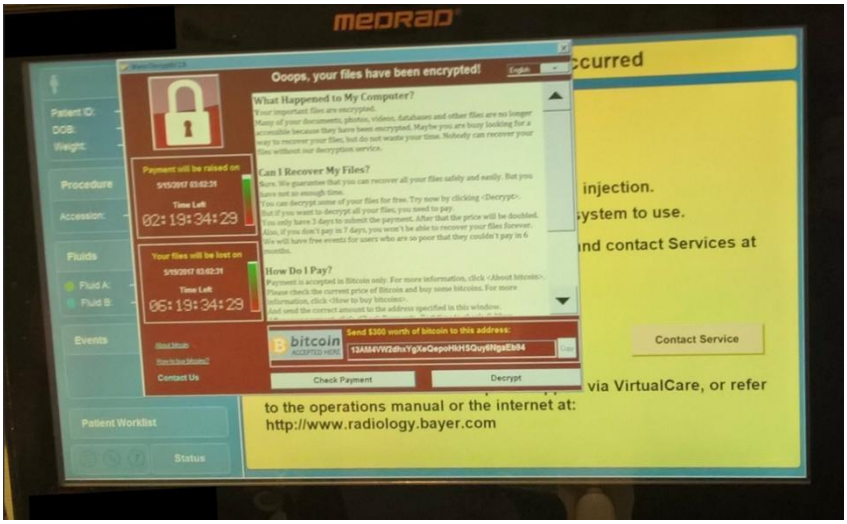
起搏器本来是提供电脉冲以缓解缓慢，不规则或停止的心脏。而干扰则可能导致使用的人立即死亡。

。

（三）恶意程序

http://securityaffairs.co/wordpress/59299/breaking-news/wannacry-ransomware-hospitals.html

2017 年 5 月，WannaCry 在 150 个国家感染了 20 万台计算机，据安全专家报告，WannaCry 感染了至少两家美国医院的医疗设备。医疗行业的一位消息人士通过福布斯在美国一家医院传播了感染拜耳 Medrad 设备的照片。消息来源并没有说明哪家医院受到影响，也不能确认拜耳模型是否被黑客攻击。但是，这似乎是放射科的设备，旨在帮助提高成像。”声明福布斯“。更具体地说，它是用于监测什么在业内被称为‘设备高压注射器，’这有助于提供一个‘造影剂’的患者。这类药物由改善磁共振成像（MRI）扫描质量的化学物质组成。



https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-c531af90-9bd5-4932-893f-0aed24efbc55&itemId=74d10670-7c18-4fbd-bf5d-c0986f62abca&timestamp=1509500059448&nonce=4ce0c109-3bf5-465d-94bd-0d1131778005&sessionId=219530&signature=4ebca32f4e6d8643b5a66dcececaf3cde762100e

自 2017 年 6 月以来持续受到 NotPetya 网络攻击影响，美国医药巨头默克集团(Merck)在销售方面的损失超过 1.35 亿美元，而其他损失超过 1.75 亿美元。事实上 NotPetya 网络所造成的危害不仅仅如此，FedEx 公司的系统直到今年 9 月份才恢复正常，导致公司损失 3 亿美元。货运公司 Maersk 由于受到该恶意程序攻击导致系统受感染损失 2 亿美元。自然在本次恶意攻击中，受灾最为严重的就是乌克兰，超过 1500 人和机构报告受到该恶意程序攻击。作为回应，NATO 宣布为乌克兰网络提供安全援助。

第三章　针对关键信息基础设施的 APT 攻击

关键信息基础设施历来是 APT 攻击重点。而从 2017 年的实际情况看，针对工业系统（涵盖多个基础设施领域）和金融系统的 APT 攻击最为多见。因此，本章将以工业系统和金融系统为例，简要介绍针对关键信息基础设施进行的 APT 攻击。

一、 针对能源系统的破坏

从全球范围内的 APT 攻击事件监控与研究情况来看，绝大多

数的 APT 攻击主要目的是窃取机密信息，而具有显著破坏性的 APT 攻击并不多见。但 2016 年末至 2017 年以来，在世界范围内却先后发生了数起引起全球关注的，具有显著破坏性的 APT 攻击事件。其中尤以针对能源系统的破坏性攻击最为引人关注。

（一）Patchwork 事件

据媒体报道，最近，一个与东南亚和中国南海问题相关的 APT 攻击被发现，该 APT 攻击以包括美国在内的各国政府和公司为目标 。经安全专家分析，该 APT 攻击所使用的全部工具代码都是通过 复制-粘贴 互联网公开代码组合而成，相对于其它 APT 特有的攻击工具而言，比较独特。

该 APT 攻击于今年 5 月在针对欧洲政府部门的一起钓鱼活动中被发现，攻击目标为一个中国政策研究机构的工作人员，其以 PPT 文档为诱饵发起网络攻击，文档内容为中国在南海的一系列活动。

Patchwork 现如今的攻击目标有了极大范围的扩展，不过主要还是针对公共部门和企业。近期 Patchwork 的一些攻击针对的行业包括：航空、广播、能源、金融、非政府组织、制药、公有企业、出版、软件。

攻击目标的地理位置则也扩展到了美国之外，虽然大约有半数攻击仍然针对美国，但其余攻击针对的国家地区则相对已经比较分散了，包括中国、日本、东南亚、英国等。而其攻击方式看来并没有太大变化，仍然是向目标发出时事新闻邮件。邮件中会包含攻击者的网站链接，这些网站的内容主要都是中国相关。

（二）全球企业依然面临 APT32（海莲花）间谍组织的威胁

https://www.anquanke.com/post/id/86101

（三）越南黑客组织 APT32 瞄准亚洲国家，成为威胁领域“最先进” 网络犯罪团伙之一

https://www.lx.b.360.cn/pc/richMedia/displaySecondMsg.do?lx-oauth=true&code=WWW-3818e488-3d91-449b-a552-b57b6ed52f54&itemId=d18758e3-1c7d-419c-bfa6-164c795f72ec&timestamp=1510278713459&nonce=394cf61e-813a-466b-a9c8-db5fa4045224&sessionId=229655&signature=e2614e3030d73c3bf5998df607c851af48ea2b30

二、 针对金融系统的犯罪

持续窃取金融交易信息 中国披露首个针对金融机构的国内 APT 组织。长期以来，APT 组织的网络攻击主要以窃取与政治、军事和科研有关的信息为主，不过近年来，以直接窃取钱财为目的的 APT 攻击事件频发。在这些攻击中，我们可以看到，即便是在理论上隔离的，防护级别极高的金融系统中，网络攻击依然可以发生，而且危害巨大。

（一）FIN7 的攻击再次遭受重创

http://blog.morphisec.com/fin7-attacks-restaurant-industry

2017 年 6 月 7 日，Morphisec 实验室发现了针对美国各地餐厅的新型高度复杂的无档案攻击。正在进行的活动使黑客能够抓住系统控制，并随意安装后门窃取财务信息。它包含了一些从未见过的回避技术，可以绕过大多数安全解决方案 - 基于签名和行为。

除了这些更新的技术，Morphisec 的调查显示 FIN7 攻击方法几乎完美匹配。过去对银行，证券交易委员会人员，大型餐饮连锁店和酒店组织的高度成功和破坏性的攻击都归功于财务激

励的 FIN7 集团。与卡巴纳克（Carbanak）团伙有关的 FIN7 必须被视为当今运作的主要威胁演员团体之一

2017 年度，全球十余个国家的多家银行机构使用的 SWIFT（银行结算系统）陆续遭到网络攻击，此类系统正是全球金融生态系统的基础。攻击者能够利用金融机构内部的恶意软件操纵处理跨境交易的应用程序，之后可在全球任意金融机构处提取资金。

http://news.xinhuanet.com/2017-04/15/c_1120817020.htm

2017 年 4 月 1 5 日电　黑客组织“影子中间人”１４日在推特等社交媒体上爆料说，美国国家安全局曾入侵国际银行系统，以监控一些中东和拉丁美洲银行之间的资金流动。

“影子中间人”发布的文件显示，美国国家安全局利用计算机代码入侵ＳＷＩＦＴ（环球银行间金融通信协会）服务器，并监控ＳＷＩＦＴ信息。文件还曝光了多个入侵ＳＷＩＦＴ系统的计算机代码和监控工具。

另外，SWIFT 方面的负责人在案件被报道之前却对此毫不知情。相关人士称，SWIFT 确实会核验系统发送信息中的密码来确保信息来自银行用户的终端设备。但是一旦网络盗窃者获取了密码和证书，SWIFT 就无法判断操作者是不是真正的账户持有人了。而黑客正是钻了这个空子，盗取了一名银行雇员的 SWIFT 证书，进而盗走了巨额资金。

从攻击战术或攻击流程来看，攻击者的攻击过程主要由三个环节组成：获得 SWIFT 权限，利用 SWIFT 发送转账指令，最终清

除证据掩盖事实。下面就来分别展开分析一下。

a） 获得目标银行 SWIFT 权限

攻击者首先需要获得目标银行的 SWIFT 系统操作权限。从相关报道来看，在索纳莉银行和厄瓜多尔银行攻击事件中，攻击者均是通过网络黑客技术来获得相关权限。特别是索纳莉银行攻击事件中，可以确定 SWIFT 相关登录帐号和密码是被植入的恶意程序所监控窃取。

可以看出，攻击者要获得 SWIFT 操作权限，并不一定需要与银行内部系统进行物理接触，完全可以通过网络攻击来完成。而目前尚未有报道明确指出孟加拉国央行的 SWIFT 系统权限是如何被盗取的，但调查孟加拉央行事件的研究人员则表示，应该是黑客利用网络攻击获得了相关登录凭证。而越南先锋银行的情况略有不同。该银行系统本身并没有被攻击，问题出在其第三方服务商（提供 SWIFT 服务）身上，但目前尚不清楚攻击者是否是通过网络攻击的方式获得了相关 SWIFT 操作权限的。越南先锋银行表示之后要改为直接连接 SWIFT 系统。

b） 向其他银行（代理帐户）发送转账指令

攻击者在获得 SWIFT 权限之后，最核心的目的就是要利用 SWIFT 发送转账指令。我们推测攻击者发送的应该是 SWIFT MT 报文中的第一类报文，如 MT103（单笔客户汇款）。除索纳莉银行以外，我们发现攻击者均向存在目标银行代理帐户的银行发送了转账指令，如美国 Wells Forga 银行设有厄瓜多尔银行的代理帐户；大华银行等其他 7 家银行设有越南先锋银行的代理帐户；纽约联邦储备银行设有孟加拉国央行的代理帐户。通俗来讲也就是孟加拉国央行等这几个目标银行存在其他银行上的钱被冒名转走了。

（二）ATM 机盗窃事件

与前述的利用 SWIFT 机制进行跨国银行盗窃的攻击手法相比，针对 ATM 机的攻击，风险则要大了很多。因为攻击者最终必须现身于 ATM 机前提取现金款。这也就给警方侦破案件，抓捕犯罪分子留下了更多的机会。

https://item.btime.com/03or1860iuuinsl6gpvqd4j5kc5

1） 2017 年 4 月，一群黑客将目标瞄准了俄罗斯的至少 8 台 ATM，一夜之间就窃取了 80 万美元。

今年 2 月，黑客使用"无文件病毒"成功攻击了 140 家企业，包括银行、电信和政府组织，范围包括美国、欧洲等地区，不过攻击的细节没有做过多披露。研究人员称，攻击银行时所用的是一种无文件的病毒，它能够存在内存中，而非像传统恶意程序那样驻足在硬盘中。这款被命名为 ATMitch 的恶意软件之前在哈萨克斯坦和俄罗斯被发现，病毒通过远程管理模块远程安装和执行的。黑客可以通过 SSH 隧道部署恶意软件并发送指令给 ATM，从而获取现金。

2） 针对 ATM 机的各种攻击

由于 ATM 机通常是处于一个相对隔离的网络环境中，因此，在对 ATM 机发动攻击时，如何植入恶意代码就成为了一个关键问题。目前已知的主要攻击手法有以下两类：

✧ 入侵银行内部网络，获得 ATM 机控制权限

✧ 通过光驱、USB 接口等直接对 ATM 机进行操作

另外，攻击 APT 机器的恶意程序也不一定只是让机器吐钞，也有一些恶意程序会通过 ATM 机暗中收集银行卡持卡人的数据信息。

下表给出了部分专门攻击 ATM 机的恶意程序的攻击方式对比。

出现时间	恶意程序名称	植入需要的媒介	ATM 机接口	攻击目标	目的	物理接触
2009	Skimer	特制的银行卡	读卡器	银行持卡人	盗取现金、银行卡数据	是
2013	Ploutus	手机	USB	银行持卡人	盗取现金、银行卡数据	是
2013	Anunak Carbanak	攻陷银行网络		银行	盗取现金	否
2014	Tyupkin Padpin	可引导光盘	光驱	银行	盗取现金	是
2015	Green Dispenser	内部人员植入		银行	盗取现金	是
2015	SUCEFUL	未知		持卡人	盗取现金、银行卡数据	未知
2016	Ripper	攻陷银行网络		银行	盗取现金	是

部分针对 ATM 机的恶意程序的攻击方式对比

（三）BlueNoroff/Lazarus：银行劫案的演变

针对波兰银行的大规模水坑攻击于 2017 年 2 月 3 日被公开披露。攻击者在波兰金融监管机构的网站上植入了一种病毒，然后等待银行在访问该网站期间不经意地下载它。

攻击者对银行展开的就是所谓的水坑攻击——得名于攻击者在目标经常出没之处进行伏击的做法；这个案例中，“水坑”是金融监管机构的网站。当名单上的银行访问该网站时，它们会被重定向至会试图下载恶意软件的软件。除了波兰银行，攻击者也对墨西哥财政部门采取了非常类似的战术，虽然没有其他受害

者被公开披露出来，但是有可能更多的银行也受到了同样的影响。

据悉，在目标名单上，波兰银行的数量最多，紧随其后的则是美国的银行，其中包括德意志银行美国分行。为农业和农村项目提供贷款的 CoBank 也被列为攻击目标。俄罗斯、委内瑞拉、墨西哥、智利和捷克的央行都在名单上。唯一一个与中国有关的目标，是中国银行在香港和美国的分支机构。

我们分析发现这些攻击事件与 Lazarus 旗下代号为 Bluenoroff 的黑客组织有关，他们专门从事金融犯罪，包括著名的孟加拉国银行大劫案，攻击目标遍及全球十余个国家的银行、赌场、加密货币公司。此次针对全球金融机构的水坑攻击中虽然没有使用任何零日漏洞，但是 Flash Player 和 Silverlight 漏洞已经足够瓦解银行机构运行的过时软件。

事实上，我们从很久以前就开始跟踪 BlueNoroff 组织。刚开始，该组织主要针对东南亚地区的银行机构，后来进行重新分组并转战至新的国家，选取目标主要为贫穷、较不发达地区，因为这些目标显然更容易得手。

BlueNoroff 开发了一套可以在目标组织内部横向移动的定制工具，并通过篡改 SWIFT 系统来实现攻击。这种技术与去年的孟加拉国央行劫案存在很大联系，当时攻击者试图从中窃取 9 亿美元。在 2 月份的“波兰劫案”中，我们发现该组织重新利用这些已知的横向移动工具，发动了新一轮的金融攻击。这让我们相信，这些攻击事件与 Bluenoroff 黑客组织有关。

有趣的是，BlueNoroff 组织在代码中种植了俄语词汇，扰乱了研究人员的方向。据悉，该代码中包含的俄语存在以俄语为母语的开发者不会犯的语法错误，怀疑可能是使用了在线翻译工具处理的句子。

目前，我们认为 BlueNoroff 可能是对全球银行机构最严重的威胁。

http://www.freebuf.com/articles/paper/133851.html