全球关键信息基础设施网络安全状况分析报告

360 互联网安全中心

360 威胁情报中心

2017. 4. 21

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，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。

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	13	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，美国和俄罗斯均将应急响应（如抗洪办）与国防系统也圈定为关键信息基础设施，值得我国借鉴。

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				✓

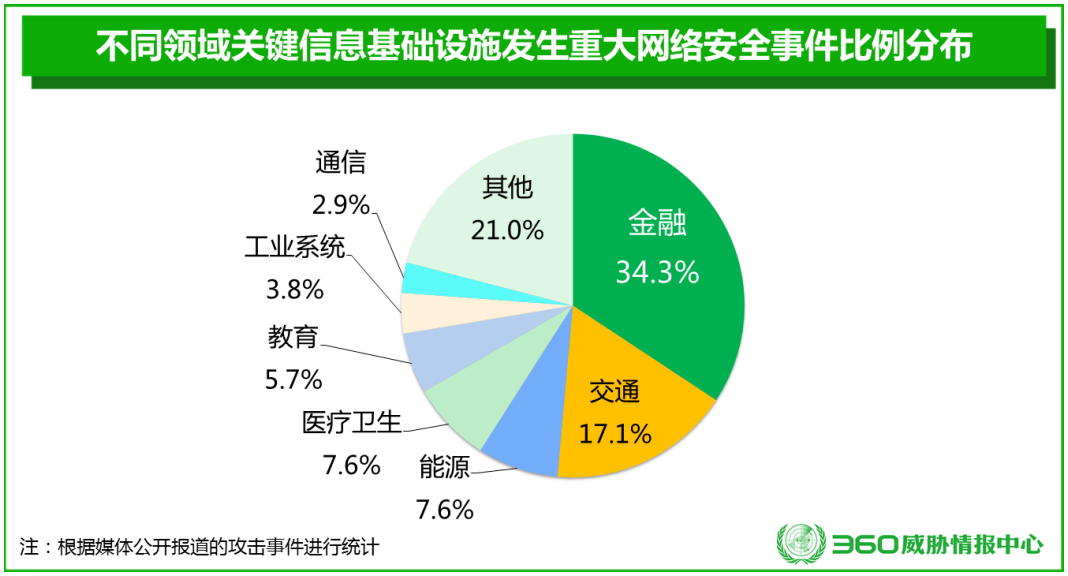
中美俄德四国界定的关键信息基础设施对比

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

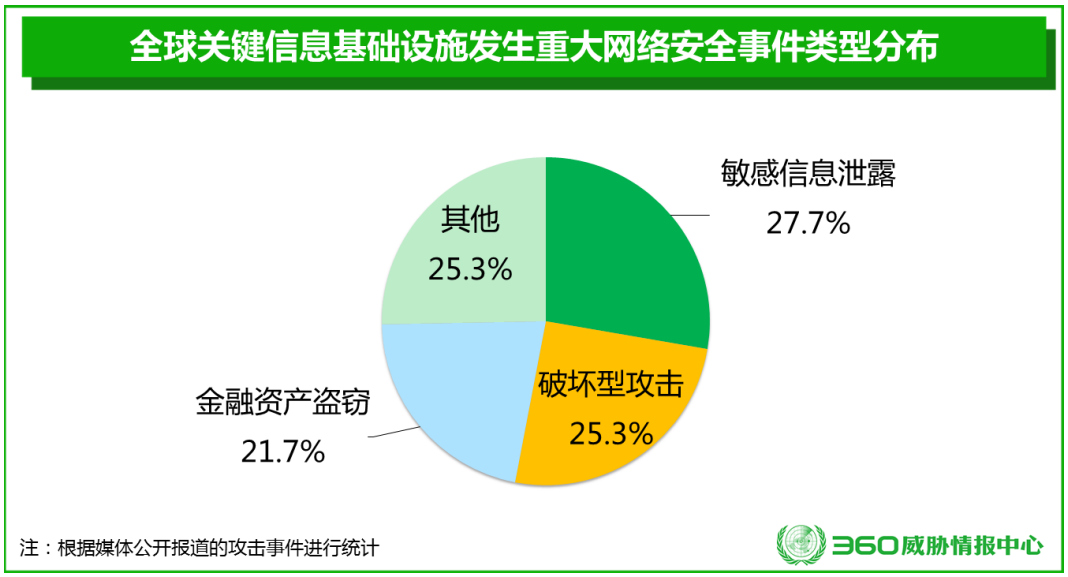
根据 360 威胁情报中心对全球关键信息基础设施重大网络安全事件的公开信息监测数据分析，在各类不同的关键信息基础设施中，金融、交通、能源等领域最容易遭受网络攻击，其中金融（34.3%）、交通（17.1%）、能源（7.6%）、医疗卫生（7.6%）等领域信息基础设施发生的重大网络安全事件最多，具体见下图。



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 威胁情报中心的监测数据，敏感信息泄露所占比例最高，约占 27.7%，其次是破坏型攻击（25.3%）、金融资产盗窃（21.7%），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 51.6%和 48.4%。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。

2016 年 11 月，美国托管信托结算公司（DTCC）进行的第三季度研究显示，22%的受访者将网络风险列为单一最大风险，56%的受访者将其列为全球金融体系的前五大风险。

从攻击者的攻击特点及事发原因来看，在 2016 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，在 2016 年多次发生，并引起了人们的关注。

2016 年 2 月 5 日，孟加拉国央行被黑客攻击导致 8100 万美元被窃取。攻击者通过网络攻击或者其他方式获得了孟加拉国央行 SWIFT 系统操作权限，随后，攻击者向纽约联邦储备银行发送虚假的 SWIFT 转账指令，而孟加拉国央行在纽约联邦储备银行上

设有代理帐户。纽约联邦储备银行总共收到 35 笔，总价值 9.51 亿美元的转账要求，其中 30 笔被拒绝，另外 5 笔总价值 1.01 亿美元的交易被通过。而这其中又有 2000 万美元因为拼写错误被中间行发觉而被找回，而另外 8100 万美元则被成功转走盗取。

2016 年 6 月，有报道称，黑客们从乌克兰银行手中偷走了 1000 万美元,并使用银行转账系统 SWIFT 来转移他们的战利品。

2016 年 12 月，环球银行金融电信协会(SWIFT 协会)近期向世界各地的银行警告称，自 2016 年 2 月黑客盗走孟加拉国中央银行的 8100 万美元存款以来，多起瞄准全球银行转账系统的黑客攻击已经成功盗走多笔资金。SWIFT 表示，如今黑客的手段已变得更加成熟，各家银行需对此提高警惕。这些攻击和新的黑客策略凸显出，SWIFT 的消息网络正面临着持续的威胁，这一网络每天处理的资金量高达数万亿美元。

（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。2016 年就发生了多起针对 ATM 机的重大网络攻击事件。

2016 年 7 月，台湾第一银行发生 ATM 机“自动吐钱”事件。紧接着，2016 年 8 月，来自东欧的网络犯罪团伙的黑客有从泰国的 21 台 ATM 机中偷走了超过 1200 万泰铢(约合 346,000 美元)。本报告将在下一章“针对关键信息基础设施的 APT 攻击”中，将会对这两起攻击事件进行详细分析。

2016 年 8 月，在拉斯维加斯举行的黑帽会议上，网络安全公司 Rapid7 的高级安全顾问 Weston Hecker 展示了 ATM 机的安全性如何被绕过，允许犯罪分子在 15 分钟内从一台机器中获得高达 5 万美元的收益。这一展示表明，尽管芯片和 PIN 系统的设

计旨在防止犯罪分子执行这种活动，但是最新一代自动取款机仍然存在安全漏洞可以被利用，使他们能够获得数以万计的现金。

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。

2017 年 4 月，有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。但是攻击者使用的方法却非常奇幻。监控显示一个黑客走向 ATM 机，甚至都没有触碰机器就把现金取了出来。

（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。

2016 年 7 月，来自全球各地的，超过 105000 个用户的 324000 张卡详细信息被黑客以 0x2Taylor 的名义泄露至互联网。数据包含浏览器用户代理详细信息，IP 地址，信用卡 CVV，部分信用卡数据，电子邮件地址，姓名，电话号码，实际地址以及购买和金融交易清单。

2016 年 7 月，信息巨头 Thomson Reuters 承认，其保管的一份全球银行业使用的恐怖嫌疑人数据库被泄露。这个数据库中存储的一些高风险个人和组织的数据库，其中一些被认为涉及金融犯罪，腐败和恐怖主义。数据库包含 220 万个人和公司名称。该数据库可追溯到 2014 年中期，其中包含从执法记录，政治信息，文章，博客文章和社交媒体等收集的名称，日期，出生地点和其他敏感信息。

2016 年 9 月，某自称黑暗霸主的黑客或黑客组织入侵了洛杉矶投资银行，并且从银行系统内部窃取了包括演示文稿，非公开协议，内部报告和合同等大量机密资料。随后，黑暗霸主对洛杉矶投资银行进行了敲诈勒索，要求银行为泄密资料支付赎金。但该银行 CEO 断然拒绝了黑暗霸主的要求，随后，黑暗霸主将窃密的资料公开在了互联网上。

2016 年 11 月，英国乐购网上银行的 4000 个网上银行账户被攻破，其中一半的账户中的钱被窃走。目前银行方面已经宣称将全额赔付被窃用户的损失。

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。

（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。2016 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。

2016 年 7 月 Proofpoint 研究人员发布警告称，过去几个月来，多个银行木马在加拿大处于活跃状态。这些木马主要属于六个不同的银行木马家族，即 Dridex，Vawtrak，Kronos，Zeus，Gootkit 和 Ursnif。

2016 年 7 月，有境外研究机构称，截获了 Retefe 银行木马的新变种，主要针对英国的银行客户。Retefe 通常通过网络钓鱼邮件传播。该电子邮件包含一个嵌入恶意 JavaScript 的文档，并需要用户交互来激活该木马。

2016 年 8 月，卡巴斯基宣布截获了一种新的银行木马 Trojan-Proxy.PowerShell.Agent.a,这种木马会使用 Microsoft PowerShell 来更改计算机的本地代理设置，以便在尝试访问银行门户时将用户重定向到错误的服务器。

2016 年 8 月,IBM 研究人员透露,经过八个月的暂停,Ramnit Trojan 已经重新出现了两个新的实时攻击服务器和一个新的命令和控制（C&C）服务器。该木马曾经一度曾瞄准了英国六大银行。

2016 年 8 月,IBM 的 X-Force 安全团队发现了高端银行木马 Zeus Sphinx 和 Zeus Panda。并且这些木马主要瞄准了巴西金融机构的用户。这种木马感染计算机后，会等待用户访问他们的网上银行或支付账户，然后在用户交易过程中实施拦截通信，修改网站，窃取凭据并重定向付款等攻击。

2016 年 8 月，IBM X-Force 的研究人员表示，当年 4 月截获一种新的木马 GozNym,主要针对 13 家德国银行及其本地子公司。

2016 年 9 月，卡巴斯基安全研究人员宣称截获一款利用社会工程学手法进行传播的银行木马，该木马会通过欺骗性的安装提示诱骗用户点击安装。该木马家族在 2015 年底首次出现，目前在俄罗斯非常活跃，其中有 93%的受害者居住在该国。

2016 年 11 月，Fortinet 安全研究人员在德国截获了一系列新的 Android 银行木马，该木马甚至可以阻止安全应用程序启动。这一系列的木马，旨在从德国银行的 15 种不同手机银行应用的用户窃取银行信息。

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。

（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。

2016 年 6 月，安全研究人员 Akamai 披露，其在当年 2 月的一个星期中，监测到有网络诈骗犯罪分子使用 993,547 个不同的 IP 来尝试登陆 427,444,261 个金融帐户。这一发现使人们更清

楚的认识到网上撞库活动的可怕规模和先进技术。

2016 年 11 月底，有黑客成功入侵了列支敦士登银行，盗取了部分疑似海外逃税者的银行账户，如国外政治家，演员或其他富人等。但与其他的攻击者不同，这名黑客并没有直接去盗刷这些有钱人账户，而是威胁这些用户，必须用比特币向其支付赎金，额度为用户账户余额的 10%，否则就会将这些人的海外账户和存款金额等信息发布给当局和媒体。

2016 年下半年，一种基于移动终端自动贷款业务网络诈骗形式开始在国内流行，并在 2017 年初形成快速增长态势。这种诈骗的实质是利用手机银行或手机支付工具的快速在线贷款功能，首先诱骗受害者自己用手机从银行贷款，之后再诱骗用户将钱转账给骗子的一种诈骗手法。受害者损失少则数万元，多则数十万至上百万元。这种新型诈骗打破了“没有钱就不可能被骗”传统安全思维。

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。

（六）系统故障

系统故障对于金融机构来说往往是灾难性的。由于电脑或网络系统故障引发的金融网络安全事件，在 2016 年也有发生。

2016 年 9 月，由于交易系统的数据库硬件故障，导致澳大利亚股市一天内两次关闭，阻碍了大部分时间的交易。据悉，ASX 系统管理员当天花费了两个小时才恢复约 75%的证券交易服务，最终在当地时间下午 1:00 恢复了所有业务的服务。

（七）DNS 劫持

2016 年 10 月 22 日，一伙犯罪分子在 3 个月的精心准备之下，成功控制一家巴西银行所有业务长达 5 个小时。该银行的 36 个域名，企业邮箱和 DNS 全体沦陷。这家建立于 20 世纪早期的银行在巴西、美国、阿根廷和大开曼拥有 500 个分行 ，总计拥有 500 万用户和 250 亿美元资产。

卡巴斯基实验室的研究人员 Fabio Assolini 和 Dmitry Bestuzhev 发现，这伙网络犯罪分子已经将同样的手段炮制到全球范围内的另九家银行，但他们并未透露是哪家银行遭遇了攻击。

此次攻击看上去就是普通的网站劫持，但是实际上没有这么简单。他们认为犯罪分子使用的攻击很复杂，并不只是单纯的钓鱼。攻击者用上了有效的 SSL 数据证书，并且还用 Google Cloud 来提供欺诈银行服务支持。

在这 5 小时的时间里，仿冒网站会向所有访问者提供恶意软件，可能有数万甚至上百万全球范围内的用户受到了这种攻击。该恶意软件是一个隐藏在.zip 文件中的 JAVA 文件，伪装成了银行安全插件应用 Trusteer，加载在索引文件中。这款恶意程序的作用是禁用受害者电脑中的安全产品，而且还能窃取登录凭证、邮箱联系人列表、邮件和 FTP 身份凭证。

此外，在这 5 个小时的时间内，据说还有一些特定的银行客户收到了钓鱼邮件。随着研究的深入，研究员发现，当时银行的主页展示了 Let’s Encrypt（一家免费的凭证管理中心）颁发

的有效 SSL 证书——这其实也是现在很多钓鱼网站会用的方案。

在本次事件中，这家银行的 36 个域名全部被攻击者控制，包括线上、移动、销售点、融资和并购等功能的域名。除此之外，攻击者还控制了企业邮箱设施，为了防止银行方面通知受攻击用户、注册主管和 DNS 供应商，攻击者关闭了邮箱服务。值得一提的是，另外巴西银行没有启用 Registro.br 的双重认证方案，这会导致钓鱼成功率大大提高。

（八）DDOS 攻击

2016 年 11 月，俄罗斯五家大型银行同时遭受了 DDoS 攻击，攻击时间长达 2 天之久。调查显示，这次 DDoS 攻击的源头是来自 30 个国家 2.4 万台计算机构成的僵尸网络. 此次攻击十分强大，并且每起攻击的强度都在不断增强。按照卡巴斯基实验室提供的分析，超过一半的僵尸网络位于以色列、台湾、印度和美国。每波攻击持续至少一个小时，最长的不间断持续超过 12 个小时。攻击的强度达到每秒发送 66 万次请求。

（九）其他网络攻击

2016 年 10 月，印度第三大私人银行 Axis 宣布，其网络系统遭到了黑客入侵 ，但在黑客窃取客户账户资金之前，银行已经设法阻止入侵。

2016 年 12 月，俄罗斯央行遭受黑客攻击 损失 3100 万美元。中央银行官员 Artyom Sychyov 也证实了这一事件，并补充说黑客企图窃取更多的约 50 亿卢布。

2016 年 12 月，有攻击者利用家用路由器组成的僵尸网络对俄罗斯五大金融机构发起分布式拒绝服务攻击。

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。

Verifone 为美国领先的信用卡终端提供商，业务范围遍布全球 150 多个国家。2017 年 1 月，Verifone 在得知其网络遭到了有限入侵后，高级副总裁兼首席信息官 Steve Horan 立即向所有员工和承包商发送了一封紧急电子邮件，提醒他们在 24 小时内修改所有密码。

邮件还提醒，Verifone 的员工不能在公司手提电脑和 PC 上安装任何软件。这就表明，这起入侵事件可能因下载恶意软件所致。在 Verifone 发送上述电子邮件的前几天，信用卡公司 Mastercard 和 Visa 向 Verifone 通知了这起事件。

2017 年 3 底，俄罗斯与亚美尼亚黑客联手从澳大利亚多家银行窃取约 18 万美元 。该犯罪组建于 2016 年 8 月至 12 月期，他们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 8500 万德拉姆资金。

（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。

2016 年 5 月，七国集团能源部长发表联合声明，宣布承诺“推进包括电力，天然气和石油在内的弹性能源系统，以有效应对新出现的网络威胁并保持关键功能”。

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

1） 灰色业务引发的信息泄露

2016 年 12 月，有国内媒体报道，在国家电网大力推广“掌上电力”等便民服务 APP 时，淘宝上却出现了一大批提供“掌上电力绑定”服务的灰色产业。这一灰色产业可能已经导致海量电力用户的个人信息被泄露。

这种提供“绑定”服务的店铺，主要是帮助各地电力系统的 APP 推广人员进行虚假的用户绑定：只要买家向店长提供电力用户的相关个人信息，店长们就会使用一批手机号，冒充真实用户下载安装“掌上电力”APP，并绑定手机号，从而为推广人员制

造虚假的业绩。

而这一灰色服务给电力用户带来的巨大风险就是个人信息的泄露：用户的个人信息从电力企业流入了淘宝，随后则有可能通过各种非法交易，最终流入黑市。

2） 安全漏洞引发的信息泄露

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

近年发生的，针对能源系统破坏性攻击，最为典型的例子就是乌克兰停电事件。同时，这也是一起典型的 APT 攻击事件。关于乌克兰大停电事件的分析，将在下一章“针对关键信息基础设施的 APT 攻击”进行详细分析。

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。

（三）扰乱性攻击

扰乱性攻击泛指一切非破坏性攻击。2016 年 10 月，国际原子能机构(IAEA)的主任 Yukiya Amano 证实，两到三年前，德国的一座核电站受到了扰乱性的网络攻击。幸运的是，这次网络攻击所造成的损失不算严重，不至于迫使运营商关闭这座核电站，但他们还是采取了一些额外的预防措施。

实际上，近三年来，还有另外三场针对核电站的攻击也值得

关注：2014 年，日本 Monju 核电厂控制室被入侵，部分数据被泄露；2014 年，韩国水力核电厂计算机系统被入侵，内部资料外泄；2016 年 4 月，德国 Gundremmingen 核电站的计算机系统，在常规安全检测中发现了 Conficker 和 Ramnit 恶意软件，核电站被迫关闭了发电厂。

（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。

Rubin 的研究发现，在欧洲和北美，智能电表所使用的通信标准包括 ZigBee 和 GSM，ZigBee 主要负责用户家中的智能设备通信，而 GSM 负责处理智能电表和电力设施之间的通信。但是，ZigBee 和 GSM 系统是已知存在很多严重的安全漏洞协议系统，这就使得攻击者可能利用这些系统的漏洞入侵智能家电和智能电表等设备。

事实上，在欧美国家，当地智能电网可能存在的安全隐患已经引起了人们的普遍担忧。2016 年 10 月，国外安全公司 Tripwire 就曾发布报告称，98%的受访者认为智慧城市存在网络攻击的危险，而 38%的受访者认为智能电网面临的安全风险将会比其他的智慧城市服务的安全风险更大。

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 2016 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。这两起断网事件的技术成因虽然完全不同，但却都是由一个臭名昭著的僵尸网络 mirai 的攻击所导致的。

mirai 是一种主要感染 IoT（物联网）设备（比如智能摄像头等）的恶意程序，而被 mirai 感染并控制的网路，就是 mirai 僵尸网络。自 2016 年 8 月 1 日被首次发现以来，mirai 僵尸网络不断通过针对 IoT 设备的扫描活动来扩充自己僵尸军团的规模。截止 2017 年 2 月 4 日，可以确信已经被 mirai 僵尸网络控制的各类 IoT 设备总数至少 194.8 万台（数据来源 http://data.netlab.360.com/mirai-scanner），形成了规模庞大的僵尸网络。2016 年的美国断网事件和德国断网事件都是由 mirai 僵尸网络发动的攻击所造成的，但这两次攻击事件的事故成因却又有很大的不同。

1） 美国断网事件

mirai 僵尸网络在 2016 年制造的最为知名的网络灾难事件就是 2016 年 10 月 21 日晚间发生的美国大面积断网事件。在该事件中，Twitter、亚马逊、华尔街日报等数百个重要网站无法访问，美国主要公共服务、社交平台、民众网络服务瘫痪。

360 威胁情报中心的监测显示，此次事件发生在 2016 年 10 月 21 日 19：00～22：50 之间，事件原因是攻击者对美国互联网域名解析服务商 DYN 进行了 DDoS 攻击，峰值流量达到日常互联

网流量的 20 倍。而在这次 DDoS 攻击的流量构成中，mirai 僵尸网络当时已经操控的全球约 89 万台智能设备（其中还包括中国境内超过 9 万台正在使用的智能设备）所发动的攻击，就是最重要的组成部分之一。在这次灾难中，仅 DYN 一家公司的直接损失就超过了 1.1 亿美元。

2） 德国断网事件

2016 年 11 月 26 日,360 威胁情报中心截获了一个新的 mirai 变种，该变种利用了独立安全研究员 Kenzo 通过博客发布的家用路由器设备 TR-069/TR-064 的一个新的安全漏洞，对全网范围内的 7547 端口进行了大规模的扫描。而不幸的是，这种扫描活动本身就有可能导致该特定型号路由器的死机或崩溃，从而导致使用该型号路由器的家庭无法正常上网。

根据事后德国电信发布的数据显示：德国境内使用的 TR-069/TR-064 家用路由器数量约为 2000 万台，其中约有 90 万台路由器因 mirai 的扫描活动和死机，无法上网，约占所有受影响设备的 4%-5%。

特别值得注意的是，在此次事件中，断网事件本身可能还不是 mirai 扫描活动给德国用户，甚至是全球互联网用户造成的最大危害。因为绝大多数情况下，路由器死机反而意味着 mirai 恶意程序的植入过程可能没有完成或没有成功。而其余那些没有发生任何异常迹象的路由器，反而很有可能是已经被成功植入了 mirai 恶意程序。由约 2000 万台可能已经被恶意程序控制的，家用路由器组成的僵尸网络，将是一颗多么可怕的定时炸弹？从美国断网事件的经验来看，这样一个规模庞大的僵尸网络，完全有能力使任何一个国家的网络系统随时陷入瘫痪。

不过，好在德国电信进行了有效的应急处理，紧急联系了路

由器的设备供应商，连夜制作了补丁包并在全网下发，及时修复了相关问题，否则后果不堪设想！

（二）信息泄露

根据海外媒体报道，2016 年 7 月，有一名化名 Pravy 的乌克兰黑客入侵了波兰 NETIA SA 电信公司，并将窃取的大量数据信息发布在一个地下论坛上。据悉，NETIA SA 电信公司是波兰第二大电信公司。

据悉，NETIA SA 电信公司此次泄露的数据包括大量的客户个人信息,如全名、电子邮件地址、家庭地址,街道地址,城市,区号,电话号码,和 IP 地址等。其中，仅各大门户网站用户的电子邮件地址就多达 615 万余个。

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。

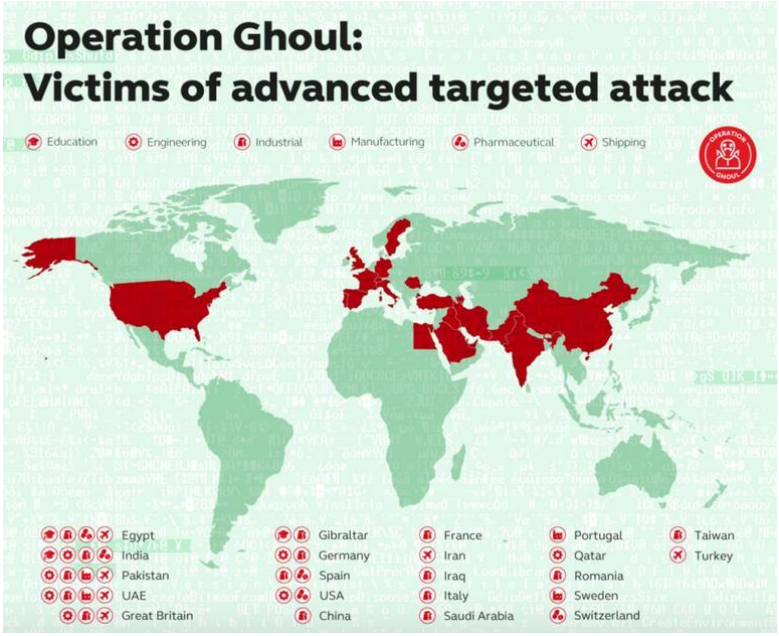
（一）黑客攻击

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。

2016 年 3 月，美国司法部公开指责 7 名伊朗黑客入侵了纽约鲍曼水坝（Bowman Avenue Dam）的一个小型防洪控制系统。幸运的是，经执法部门后期调查确认，黑客还没有完全获得整个大坝计算机系统的控制权，仅只是进行了一些信息获取和攻击尝试。这些伊朗黑客可能为伊朗伊斯兰革命卫队服务，他们还涉嫌攻击了包括摩根大通、美国银行、纽约证券交易所在内的 46 家

金融机构。

2016 年 8 月，卡巴斯基发布报告称，食尸鬼行动对超过全球 30 多个国家 130 家公司进行了工业间谍活动 。报告显示，食尸鬼行动的主要攻击目标是中东地区工业系统的工程师和管理员。但实际攻击范围已经扩散到全球。包括中国、美国、欧洲部分国家都有受害者。



食尸鬼行动的主要攻击手段是鱼叉邮件，用户一旦中招，恶意程序就会开始监视用户并收集数据，主要包括密码、击键和屏幕截图等。卡巴斯基的报告认为，食尸鬼行动的大多数受害者是中小企业，其主要目的赚钱：要么是盗刷受害者网银账户，要么是出售受害者的知识产权。

2016 年 8 月，伊朗最高国家网络空间委员会在调查一起化工厂火灾事件时，在该化工厂的电脑系统中发现一款恶意软件，但该恶意程序本身在火灾发生时处于不活跃的状态，目前没有证据表明其与火灾之间有直接的关系。但当局仍然担心国家的工业系统有可能再次遭到类似震网病毒的攻击。

2016 年 12 月，德国重工业巨头蒂森克虏伯对外表示，其遭到了黑客攻击，攻击者的目的是窃取公司的商业和技术机密，但没有成功。初步调查认为，攻击者来自东南亚地区。

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。

（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。

从 2016 年的情况来看，工业系统被报告的重大漏洞不在少数，而且修复率很低。

2016 年 6 月，德国西门子公司告知用户，由于其 ICS（工业控制系统）设备存在安全漏洞，暂时不要进行联网使用。美国工控系统计算机事故应急小组(ICS-CERT)在西门子公司的 SIMATIC WinCC(视窗控制中心)系统中发现，由于该系统缺乏必要的安全验证，使得黑客能够轻易地远程控制设备，进而实施攻击。

2016 年 7 月，西门子电力自动化系统中被发现两个漏洞。

其中，一个漏洞(CVE-2016-5848)会导致用户密码设置得不到有效保护，而另一个漏洞(CVE-2016-5849)则可能被黑客访问敏感的配置数据。

2016 年 10 月，工业安全公司研究员 CyberX 在 ICS 网络安全会议上报告称，总部位于法国的施耐德生产的一款专业工业防火墙发现一个安全漏洞 该漏洞允许远程执行代码，攻击者可以利用该漏洞实现修改防火墙规则，窃听网络流量，注入恶意数据包，扰乱通讯等攻击。

2016 年 11 月，研究人员在 Moxa 工业以太网产品中发现了几个严重的漏洞。这些漏洞允许攻击者在服务器上执行任意操作系统命令。

系统有漏洞其实并不可怕，关键在于是否能够得到及时的修复。2016 年 8 月，美国安全公司 FireEye 发布报告称：33%的工业控制系统漏洞（共 1552 个）长期未能得到修复，其主要原因是没有供应商来修复这些漏洞。这就给企业带来了巨大的潜在风险。

六、 教育

从 2016 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；其次是 DDOS 攻击；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

2016 年，全球多所知名高校都遭遇了重大的信息泄露事件。

2016 年 6 月，英国格林威治大学遭到一名疑似因被学校开

除而心怀不满的黑客的报复式攻击。攻击者窃取了学校网站的整个数据库并公布在互联网上，相关文件大小约为 2.74GB，其中包含该校学生与工作人员的大量敏感信息：如全名、电子邮件地址、密码、考试成绩，病假申请等信息。此外，这名黑客还用自己的网页替换了学校官网的首页。

2016 年 10 月，黑客 Mys7erioN 在网上宣布，他成功的入侵密歇根州立大学数据库，并将相关数据泄露在了网上。被泄露的数据信息包括：姓名，网站登录名，电话号码，已发布的电子邮件和加密密码等。2016 年 11 月，该所大学证实，约有 40 万条该校学生和雇员记录的数据库被窃取。据悉，这不是密西根州立大学第一次遭到黑客入侵，在 2012 年，黑客 DARWINARE 就曾在网上发布了该学校的约 1500 个人的名字，电子邮件地址，加密密码，用户 ID 和邮寄地址等信息。

2016 年 8 月，山东地区接连发生两起因学生个人信息泄露导致的网络诈骗并致人死亡的恶性事件，举国震惊。特别是 18 岁临沂女孩徐玉玉被骗致死案，也引起了人们对相关教育机构泄露学生助学金信息的质疑。而记者的进一步调查发现，在山东约有 20 万高考考生的个人信息已经遭到泄露，所有数据一起打包出售仅需 6000 元！

（二）网站篡改

2016 年 8 月，罗马尼亚大学网站被黑，攻击者在网站上植入了恶意代码，一旦有用户访问了含有恶意代码的页面，电脑就会感染敲诈者病毒（也称勒索软件），电脑上的所有办公文件、照片和视频文件都会被强行加密，受害者只有按照攻击者的指示用比特币支付赎金后才能解密自己的文件。

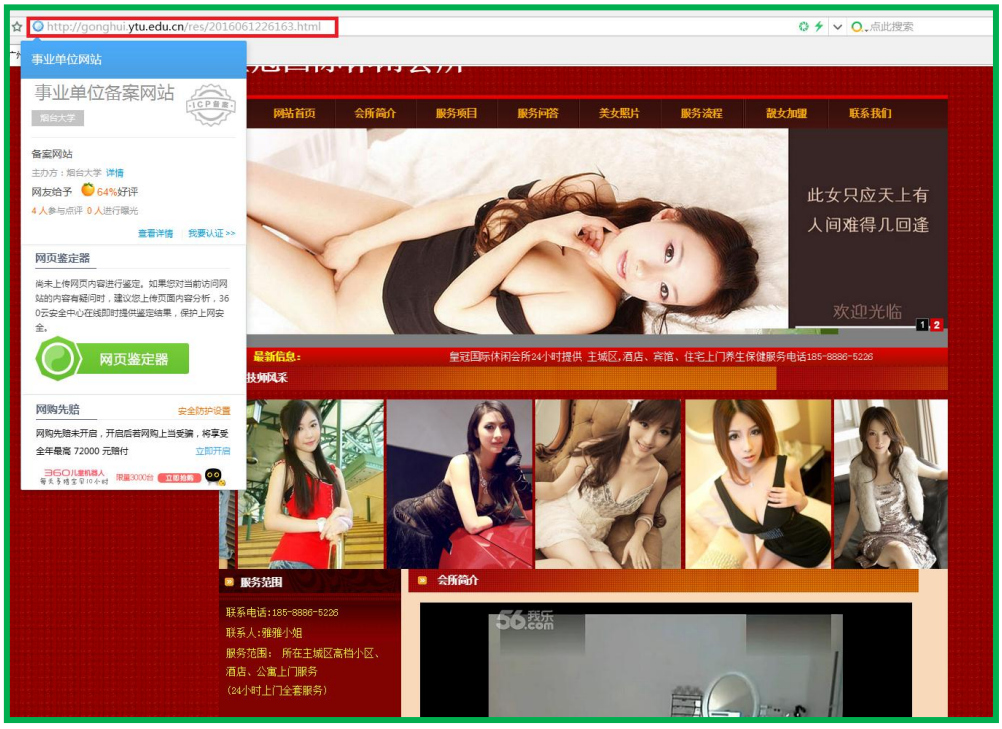
事实上，360 互联网安全中心每年在国内截获的高校网站被

篡改案例也很常见。下面给出的就是 2016 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：

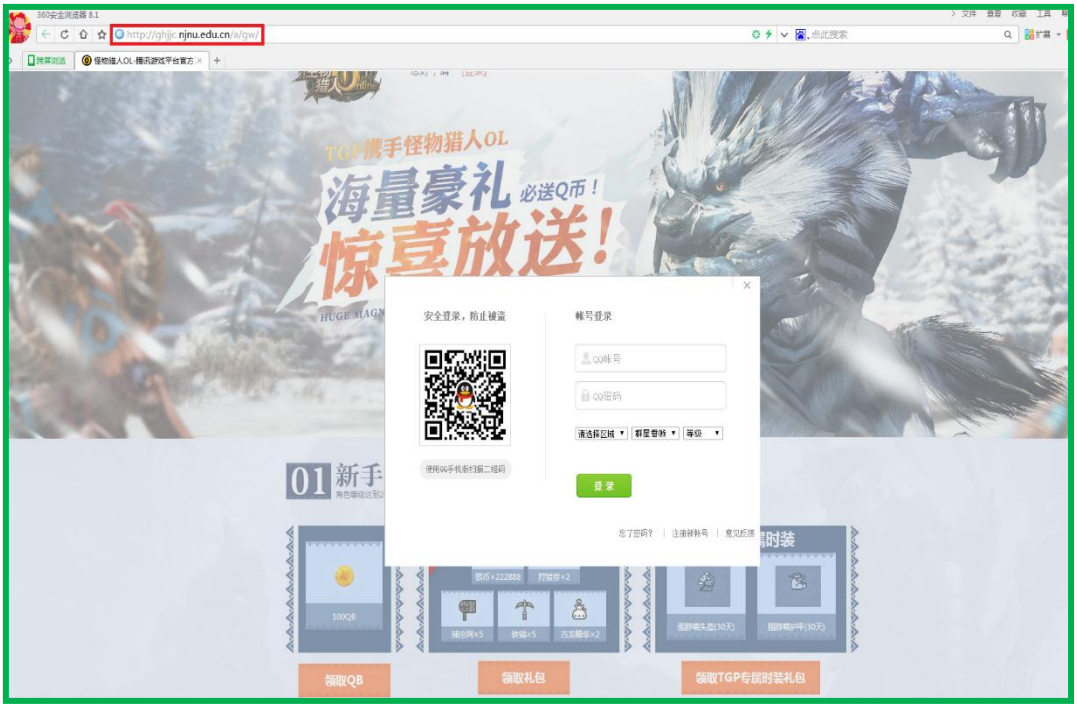
被植入的非法网页：



2） 网站域名：njnu.edu.cn，网站（备案）名称：南京师范大学

网站首页：

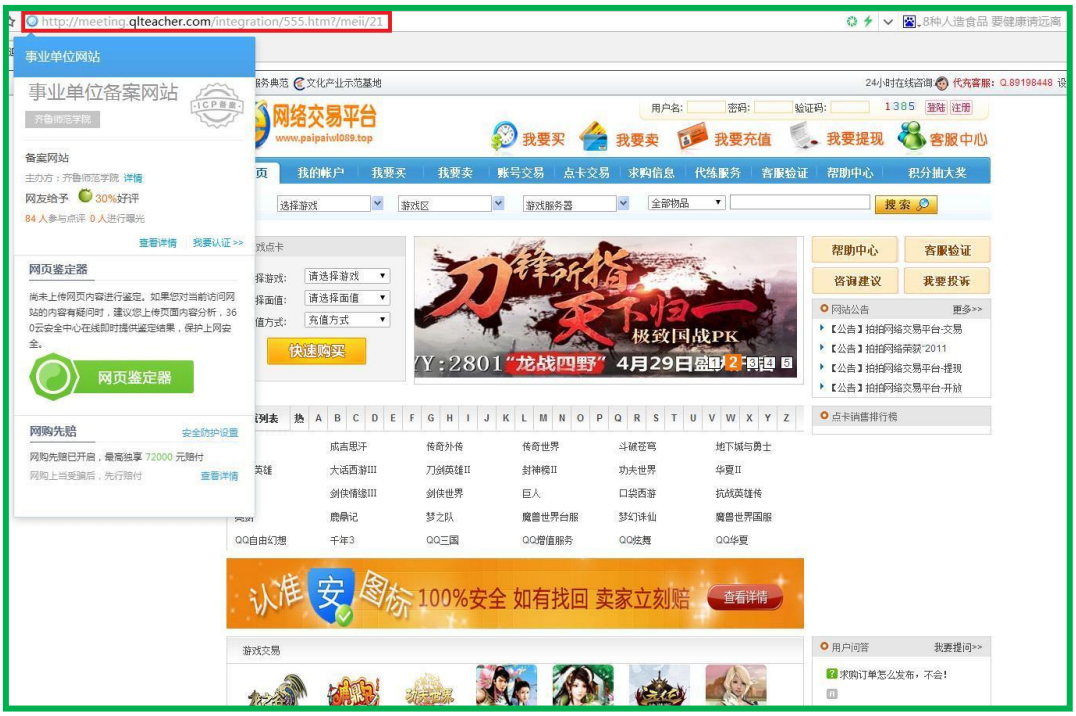
被植入的钓鱼网页：



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。

2016 年 7 月，总部设在马萨诸塞州剑桥的内容交付网络和云服务提供商 Akamai 发布的一项威胁咨询表示，攻击者在当年头六个月针对麻省理工学院服务器发动 35 次 DDOS 攻击。其中最大的一次 DDOS 攻击持续了近一天，峰值攻击带宽为 295 Gbps。Akamai 认为这次攻击是由 Kaiten 恶意软件控制的僵尸网络所发动的。

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。例如，2016 年 11 月，英国交通系统技术发展中心发布报告说：随着技术快速发展，英国交通运输业面临越来越大的网络安全威胁，有必要投入更多资源加强防范。报告认为：目前全球正逐渐形成新兴的“智能运输”市场，以自动驾驶车辆、物联网等新技术为特征，并越来越多地利用个人数据提供定制服务，这给“本身脆弱的”交通运输网络增添了复杂性，带来新的网络安全威胁。

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

2015 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四个方面：大范围航班延误；旅客信息泄露；散播政治言论；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

a） 英国航电脑系统故障至数百航班延误事件

2015 年 2 月，有英国媒体报道称，英国国家航空服务公司（NATS）在去年 12 月份发生一起严重事故。由于其两条系统航班服务器通道均发生故障，导致数百架航班无法起飞。据一份内部报告显示，此次混乱共造成 120 架航班被取消，500 架航班被耽搁了 45 分钟，总共影响约 10000 万名旅客。这也是英国航空史上最严重的大混乱。

此次事故的发生是一台运行航班数据处理系统的 IBM S/390 主机宕机造成的。内部报告显示，在 14 点 44 分，一台为航空指挥控制人员提供数据的计算机发生故障；14 点 45 分，所有离开伦敦机场的航班被叫停；15 点整，整个欧洲所有计划经过英国领空的航班被叫停。在当天的 20 点 10 分，系统才恢复正常。

b） 波兰国家航空公司 LOT 的地面计算机系统遭攻击事件

2015 年 6 月，波兰国家航空公司 LOT 的地面计算机系统遭受网络攻击，导致无法安排飞行计划，最终造成至少 10 个航班被取消，超过 1400 位乘客被迫滞留在华沙 Okecie 机场。

这场攻击发生在当地时间下午 4 点左右，并在当晚 9 点得到解决。LOT 发言人 Adrian Kubicki 说道：“这是针对航空公司网络攻击的首次案例”。

c） 美联航电脑系统故障至数百航班停飞事件

2015 年 7 月，美国联合航空公司发生了因电脑系统故障而停飞数百架次航班的事件。有专家称，这不过是业务越来越自动化的航空公司未来可能面临状况的一次预演，而技术故障带来的冲击将会越来越大。

d） 土耳其黑客 DDoS 维也纳机场

2016 年 9 月，有土耳其黑客因政治动机扬言要对维也纳机场网站发动 DDoS 攻击。奥地利当局立即对此展开了调查。这名黑客自称是以阿斯兰•内费勒•蒂姆（Aslan Neferler Tim）的名义（由土耳其人译为狮子士兵队）进行攻击。

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） 英国航空公司数万乘客账户被窃

2015 年 3 月，英国航空公司证实其电脑系统存在安全隐患，有数万个乘客账户被未经授权访问，但并不清楚未经授权的攻击来源。该航空公司发言人表示，攻击者似乎使用的是撞库攻击，通过互联网上已经泄露的一些密码信息，批量自动化入侵了这些账户。

b） 全球四大航空公司网站移动版未使用 HTTPS

2015 年 12 月，有研究机构发布报告称，全球 16 家大型公司（其中包括 4 家航空公司）的公司网站移动版并未使用 HTTPS 加密,可能导致用户信用卡数据遭泄露。发布报告的公司 Wandera 表示，研究人员在测试过程中可轻易获取个人可识别信息，甚至可以通过移动版网站或手机 APP 中进行的交易获取到客户信用卡卡号。

与此项研究相关的 4 家航空公司分别是：爱尔兰航空、加拿大航空、亚航、易捷航空（英国航空公司）。

c） 伪造电子登机牌免费进入航空公司的休息室

2016 年 8 月，一位来自波兰计算机紧急响应小组的安全专家 Przemek Jaroszewski 宣称，通过伪造的电子登机牌，他可以进入欧洲各地任何一个机场的休息室。据 Jaroszewski 介绍，他在各个航空公司休息室使用的计算机系统中发现了一个漏洞,并基于该漏洞开发了一款 Android 应用,来产生虚假的电子登机牌。Jaroszewski 通过其伪造的电子登机牌“数十次”进入欧洲各地机场的休息室。这些电子登机牌未经任何中央数据库验证，航空公司休息室的工作人员在扫描二维码后，并未发现异常。

d） 纽约机场 750GB 数据遭泄露

2017 年 2 月,纽约斯图尔特国际机场被曝 750G 数据遭泄露，大量敏感数据被恶意人士所随意窃取。调查发现，此次攻击活动至少自去年 3 月就已经开始。被泄露的数据中包含电子邮件、密码与政府文件,还包括包含某些机场设备的密码和机场员工的社会服务号码。MacKeeper 公司安全研究人员克里斯•维克里指出，此次泄露事件标志着纽约机场的网络完整性“彻底崩溃”。

e）波音公司 36000 名员工信息泄露

2017 年 2 月，波音公司向 3.6 万名员工通告了他们个人信息的意外泄漏。事件的起因是一名公司员工去年年底不经意间通过电子邮件将公司电子表格发送给了他在该公司工作的配偶。

该文件共享的文件包含 36,000 名波音员工的敏感，个人身份信息，包括姓名，出生地点，BEMSID 或员工身份证号码以及会计部门代码等信息。

尽管该名雇员及其配偶都向公司证实，他们没有分发或使用任何信息。但公司仍然判定这是一起信息泄露事件，并向相关员工进行了通报。

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。

3） 黑客通过攻击机场网站或广告牌散播政治言论

a） 澳大利亚机场网站遭支持 IS 组织黑客攻击

2015 年 4 月，据外媒报道，澳大利亚霍巴特国际机场的网站遭到黑客攻击。据报道，实施攻击的黑客是极端组织“伊斯兰国”（IS）的支持者，这些黑客在机场网站上留下了支持“伊斯兰国”的声明。澳大利亚警方称，黑客似乎是攻击了霍巴特国际机场网站的主机，并在网站上公布了一份支持“伊斯兰国”的声明，不过此次攻击并没有造成直接威胁。

b） 越南机场遭疑似中国黑客攻击

2016 年 7 月，据外媒报道，越南河内和胡志明市三个主要机场的电脑系统遭疑似中国黑客入侵，机场显示屏上出现批评菲律宾和越南对南海主权的留言，广播系统播出的内容也声称南海属于中国。越南民航局在声明中表示，黑客攻击打扰了机场的电子登机系统，不得不手动为乘客办票，造成多个航班延误。

越南《青年报》（Toui Tre）上载了一段在其中一个机场拍摄的视频，机场内正播放着一段以英语念出的录音:“这是从中国 1937CN 团队发出的警告，南海是中国固有的领土。”

不过，“1937CN”事后发表声明称，该组织坚持南海诸岛自古以来属于中国的立场，但对越南机场事件“不参与，不执行，不接受，不承认”。

同时，越南航空（Vietnam Airline）网站同样遭黑客入侵，登入者会被转移到一个海外的网站，其网站页面也展示了同一个黑客组织发出的类似警告。此外，该航空公司还声明说，有部分飞行乘客的资料被放上网。外泄的数据达 100 兆字节，大约为 4 万名乘客的资料。

在上述两个典型案例中，我们都能看出黑客对机场系统或航空公司网站发动的政治性网络攻击的巨大危害。特别的，机场是城市中人流密集，国际化程度较高的地区，因此攻击机场系统并散布政治言论，其影响力也会被明显放大。这种危险情况值得各国民航机构高度警惕。

4) 针对航空企业的金融盗窃与商业诈骗造成巨大损失

a) 爱尔兰航空公司银行账户遭黑客盗刷 500 万美元

2015 年 4 月，黑客洗劫了爱尔兰航空公司旗下的子公司瑞安航空银行账户，盗走 500 万美元（折合 460 万欧元）。这个银

行账户是瑞安航空用来为旗下飞机支付加油款项的加油基金账户，并且没有设置立即报警功能。安全人员在调查中发现，攻击者在这次盗窃中使用了专门的恶意软件，这类恶意软件问世以来已经从各家企业账户当中盗走超过 100 万美元。

瑞安航空在一份简短的声明当中表示，瑞安航空公司发现被盗走的资金已经通过一家中国的银行进行了电子汇款。爱尔兰当局现正调查此事。

b） FACC CEO 遭邮件诈骗 5000 万欧元

2015 年 12 月到 2016 年 1 月，被中航工业集团收购的奥地利飞机零部件制造商（FACC）陆续向多个海外账户汇出 5000 万欧元。这是典型的身份造假诈骗，也被称为“商务电子邮件攻击”。攻击者冒充其他员工或合作伙伴，给首席执行官发送电子邮件，要求紧急汇款。2016 年 5 月，FACC 公司 CEO 沃尔特•史蒂芬（Walter Stephan）因此被解雇。

尽管 FACC 公司已设法追回了被盗的 1090 万欧元，但其余的资金仍然不翼而飞，或分布于斯洛伐克和亚洲各地的银行中。

客观的说，黑客盗刷和商业诈骗活动一般不会仅仅针对航空公司进行。但航空公司的账户被轻易盗刷，CEO 成为诈骗的直接对象，这些事件也客观表明了航空公司工作人员在在安全管理措施和安全防范意识等方面都有明显的缺欠和不足。境外民航企业发生的类似安全事件值得国内民航企业引以为戒。

5）其他值得警惕的民航系统安全漏洞

2016 年 12 月，OActive 的研究人员披露了松下航空电子飞行娱乐系统（IFE）中的几个漏洞。利用这些漏洞，攻击者可以干扰飞行操作并窃取敏感信息。根据松下公司提供的数据，他们

已经为主要航空公司提供了 8000 多个飞行中的 IFE 和通信系统以及 1300 个飞行连接解决方案。

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。

（二）铁路

2016 年 7 月，有国外媒体援引安全公司 Darktrace 介绍，英国的铁路系统在过去的十二个月内先后遭到了四次网络攻击。所幸这些攻击只是进行了基本的侦察操作，可能只是想要检测网络的内部结构，并收集未来攻击的信息。当然，也不排除这些入侵是偶然的。而此前一年的冬天，也有安全人员在乌克兰监测到了一次针对铁路系统的攻击。

（三）公交

2016 年 11 月，美国旧金山的 Muni 交通系统遭到敲诈者病毒攻击，从而导致公交系统员工电脑上的办公文档、照片和视频等文件被全部加密。攻击者最终只留下“你被黑客入侵，全部数据加密”的信息。由于整个公交办公系统被加密锁定，导致所有工作人员无法正常办公。最终，当地交通部门做出决定：当地所有的公交线路当日搭乘均可免费。

（四）公路

2016 年 12 月，两段盗刷 ETC 卡的黑客演示视频在网上疯传。其中一段视频中，一名男子拿着 POS 机走过来，隔着挡风玻璃对

准车上的 ETC 设备轻轻一碰，“滴滴”几声后 POS 机显示 100 元扣款已成功。而在另一段视频中，男子手持 POS 机靠近自己车辆的 ETC 卡,POS 机提示输入交易金额。该男子首先输入了 400 元，交易提示要求输入密码。随后，该男子再次刷了一下 ETC 卡，输入交易金额 300 元，POS 机提示交易成功，并打出流水单。在单据下方标明，这是小额免密支付。

对此，粤通卡客户服务网站发布通知，称所谓盗刷是利用了银联卡小额支付免密免签交易的功能，车主可咨询发卡行关闭“小额免密免签”服务。而北京速通科技有限公司则表示，目前北京发行的 ETC 卡不具备闪付功能，因此不会被盗刷。

（五）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） 特斯拉自动驾驶碰撞案

2016 年 5 月 7 日，Joshua 驾驶一辆特斯拉 Model S 在佛罗里达的一个交叉路口与一辆拖挂车发生了剧烈碰撞,导致其不幸丧生。调查显示，两辆车在碰撞发生时，这辆特斯拉轿车正处于自动驾驶模式下，而驾驶员也没有做出任何规避动作,。

随后美国国家公路交通安全管理局(NHTSA)介入了这场事故的调查，在经过历时 7 个月的漫长调查之后，2017 年 1 月 NHTSA 公布了对特斯拉自动辅助驾驶系统(Autopilot)的调查结果：未检测到特斯拉自动紧急制动系统与自动辅助驾驶系统中存在任何设计与表现的缺陷。与此同时，NHTSA 还表示：没有必要对该问题进行进一步审查。

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。

2016 年 6 月，研究人员发现，黑客可以利用 Wi-Fi 远程关闭三菱欧蓝德汽车防盗报警器。其主要安全问题在于：三菱将 Wi-Fi 预共享密钥写在了用户手册中,而且格式十分简短。因此，研究人员仅用了 4 天时间就使用暴力破解技术破解了该密钥。

2016 年 7 月，研究人员发现宝马 ConnectedDrive 门户网站包含一个 0day 漏洞，可能会导致注册信息或有效的车辆识别号

码被泄露，同时，黑客还有可能利用这个漏洞在网站上篡改汽车信息。

2016 年 8 月，著名的汽车网络安全专家查理•米勒和克里斯•瓦拉斯克在美国黑帽大会期间向人们展示了如何远程劫持 Jeep 汽车的转向、制动和加速。这两位安全专家自 2013 年就开始破解各种智能汽车，包括福特、丰田、切诺基等品牌的智能汽车，都曾被他们远程破解和入侵。

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。

3） 汽车盗抢

2016 年 8 月，美国休斯敦警方抓获了两名黑客汽车大盗。这两名黑客使用安装了盗版软件的笔记本电脑先后偷了 100 多辆汽车。被逮捕的两名罪犯分别是 Michael Arce 和 Jesse Zelaya，并被指控将盗版软件用于汽车盗窃。据称二人使用在笔记本电脑上运行的软件来重新编程目标车辆的电子安全系统,这样他们可以使用他们自己的钥匙来访问车辆并窃取。据调查案件的当局说，两名黑客在攻击过程中，可能利用某些系统漏洞。

2016 年 11 月，挪威互联网安全公司 Promon 指出：特斯拉专属应用的安全性不够高，很可能导致用户的 Model S 或 Model X 被盗。据悉，特斯拉为其电动汽车定制的智能手机应用能为车主提供诸多方便，如查看汽车剩余电量、在拥挤的停车场寻找爱

车，甚至在无钥匙情况下远程打开车门等。

2016 年 12 月，美国国家保险犯罪局（NICB），发现了一个新工具，可以允许盗贼解锁配备“无钥匙进入”功能的汽车，启动引擎并且开走汽车。关于这个“神秘设备”的信息目前外界还所知不多，但是由保险公司组成的非营利组织 NICB 表示，他们从海外的第三方安全专家那里获得了一个。该机构表示，该设备在欧洲使用，很少在美国使用，同时也没有警察官方报告确定该设备是汽车盗窃设备。

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

2016 年 6 月，一名黑客在网上声称窃取了近 1000 万病人的记录，内容包括数据包括姓名，地址，出生日期和社会保险号码等。而这些病人的记录在网上的销售额已达 820,000 美元。这名自称 thedarkoverlord 的黑客还同时发布了自己在网上黑市 TheRealDeal 上的交易记录。

2016 年 7 月，布鲁金斯学会的一项研究显示，自 2009 年底，已经累计有超过 1.55 亿美国人的医疗信息被泄露。

2016 年 8 月，一名黑客攻击了美国俄亥俄州卫生系统，超过 10 万内部医疗记录文档被盗，其中包括许多有关患者个人健康信息的文件。一名乌克兰黑客在 Twitter 上声称是自己进行的攻击，并且给出了几十个名字、地址、出生日期和诊断截图。这名黑客总共上传了超过 156GB 的数据到 Google 云端硬盘。

2016 年 8 月，美国最大的非营利性医疗保健组织 Banner Health 向其服务的 370 万患者、食品及饮料客户、内部员工发出安全警告，他们的个人资料可能已经被盗。事件的起因是，该组织监测发现有攻击者访问了其旗下商店支付卡数据的系统；进一步调查又发现攻击者进入过存储患者信息的系统，可能被攻击者窃取的信息包括姓名，出生日期、地址、医生姓名、服务日期、索赔信息、以及健康保险信息和社会保障号码。

2016 年 9 月，匿名者黑客组织攻击了意大利四个医疗机构。具体发动攻击的是匿名者意大利和 AntiSec 意大利这两个匿名者黑客组织的分支组织。他们发动攻击的目的是抗议政府对 ADHD（注意力缺陷/多动症）的立场。黑客破坏了这些医疗机构服务器，污染了公共网站，并在 Facebook 和 Twitter 上泄露了其中两家医疗机构（那不勒斯和都灵的诊所）的大量内部文件，包括内部通信，库存凭证和员工简历等。

事实上，相关黑客组织早在 2016 年 3 月就曾发起过针对卫生部，高等院校和当地卫生部门的 DDoS 攻击活动。意大利红十字会也遭到过这些黑客组织的攻击。

2016 年 10 月，澳大利亚红十字会的 120 万份血液捐献记录被不慎泄漏，这些记录共约 1.74GB 大小，涉及约 550000 位献血者的个人信息，具体包括的姓名、性别、电子邮件地址、家庭住址、电话号码、出生日期、出生国、血型，以及是否曾经献过血，

献血日期、献血种类（血浆，血浆、血小板、单采血小板、全血）和献血者的调查问题答案等。

泄露这 120 万份血液捐献记录的网站 Have I Been Pwned 的创始人 Troy Hunt 称，造成此次泄露的是一个数据库备份文件，该文件被发布在一个可公开访问的 Web 目录中。发布者是在偶然间将文件发给 Hunt 的，当他发现事情结果后，立即告诉了澳大利亚红十字会血液部有关情况。

2017 年 3 月，有黑客入侵了英国国家医疗服务体系 NHS 并窃取数千医疗人员的信息。内容包括名称，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。

（二）设备漏洞

2016 年 7 月 18 日，有研究人员报告称，已经确定了飞利浦医疗设备中的数百种高危安全漏洞，而供应商方面也已经发布了解决问题的软件更新。受影响的产品主要是飞利浦 Xper 信息管理系统，这种医疗信息系统主要在美国和欧洲使用。ICS-CERT 发布的一项研究成果也显示，Xper Connect 1.5.12 版本和 Windows XP 以前的运行版本，受到总共 460 个漏洞的影响，其中许多漏洞可能导致攻击者破坏系统。

2016 年 10 月，胰岛素给药系统公司 Animas 的产品胰岛素泵被曝存在安全漏洞，攻击者利用这些漏洞可以操控设备并给病人注入非法剂量胰岛素。有趣的是，这些漏洞是被 Rapid7 公司一名身患 I 型糖尿病且正使用该胰岛素泵的安全研究员发现的。

2017 年 1 月，美国食品药物管理局(FDA)证实，圣犹达医疗公司出品的心脏移植设备存有可供黑客访问的漏洞。一旦入侵发生，黑客可以耗尽设备的电量、设置错误的跳动节奏和震击。

（三）恶意程序

2016 年 8 月，美国安全公司 FireEye 发出警告：敲诈者病毒（勒索软件）已经开始瞄准美国和日本医疗行业 。据 FireEye 研究员 Ronghwa Chong 透露，敲诈者病毒正在向美国和日本的医院发动“大量”袭击事件。已经有越来越多的医疗卫生部门遭到携带 Locky 病毒（敲诈者病毒的一个家族）网络钓鱼邮件攻击。

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 2016 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、 针对工业系统的破坏

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 2015 年末至 2016 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。其中尤以针对工业系统的破坏性攻击最为引人关注。

2015 年 12 月 23 日，也就是在圣诞节的前夕，乌克兰遭遇了大规模停电事件，数万“灾民”不得不在严寒中煎熬；而在 2016 年 11 月 17 日晚，也就是伊斯兰教的大赦之夜，沙特阿拉伯又遭遇了 Shamoon2.0 的攻击，包括沙特国家民航总局在内的 6 个重要机构的计算机系统遭到严重破坏。似乎每到年末的时候，针对工业系统的网络攻击就会悄然来袭，使那些可怜的受害者们无法“安心过年”。

（一）乌克兰圣诞大停电事件

2015 年 12 月 23 日，也就是 2015 年的圣诞节前夕，乌克兰一家电力公司的办公电脑和 SCADA 系统（Supervisory Control And Data Acquisition 系统，即数据采集与监视控制系统，一般用来代指工业控制系统）遭受到第三方非法入侵。事故导致伊万诺•弗兰科夫斯克地区将近一半的家庭经历了数小时的电力中断。起初，电力公司估计约 8 万名左右的用户受灾，后发现共有三种不同配电站的能源公司遭受攻击，造成约 22.5 万名用户的

电力中断。

攻击事件发生后不久，乌克兰政府官员声称电力中断是由网络攻击引起的，并指责俄罗斯国家安全部门应为此事负责。美国政府，以及许多的当地私营企业均对乌克兰的政府调查人员施以援手，协助乌克兰政府对攻击事件进行分析，以确定故障的根本原因。

2016 年 1 月 3 日，安全公司 ESET 最早披露了本次事件中的相关恶意代码，并发表文章称：乌克兰电力部门感染的恶意代码为 BlackEnergy。BlackEnergy 是一种后门程序，攻击者能够利用它来远程访问并操控电力控制系统；此外，在乌克兰境内的多家配电公司设备中还检测出了恶意程序 KillDisk，其主要作用是破坏系统数据以延缓系统的恢复过程。再者，研究人员还在电力系统的其他服务器上发现了一个被添加后门的 SSH 服务端程序，攻击者可以根据内置密码随时连入受感染的主机。

事实上，恶意程序 BlackEnergy 对乌克兰以及电力控制系统的攻击并不是第一次了。自 2007 年被首次披露以来，BlackEnergy 已经经历了多次的变种和升级，并且对乌克兰电力系统进行多轮次的“狂轰滥炸”。国外安全机构发布的研究资料还显示，2016 年，BlackEnergy 还在继续对乌克兰境内的多个工业系统发动攻击，并且在 2016 年的 12 月，又再次造成了乌克兰某电力企业的一次小规模停电事故。下表给出了 BlackEnergy 发展的简要历程。

年份	事件概要
2007	Arbor 公司首次披露一个在 DDoS 攻击中被用来创建僵尸网络的工具 BlackEnergy，该版本一般被称之为“BlackEnergy 1”
2008	俄格冲突期间，一些身份不明的黑客针对格鲁吉亚的网络系统发动了 DDoS 攻击，BlackEnergy 被用于创建僵尸网络
2009	有黑客利用 BlackEnergy 盗取美国 Citibank 数千万美元
2010	戴尔旗下安全公司 SecureWorks 发布配备 Rootkit 的 BlackEnergy 变种，该版本一般称之为“BlackEnergy 2”
2011 年 7 月	ESET virusradar 研究显示，BlackEnergy 在全球活动达到高峰
2013 年 10 月	BlackEnergy 支持 64 位操作系统
2014 年 9 月	F-Secure 发现了为乌克兰政府量身打造的 BlackEnergy 新变种，该版本一般被称之为“BlackEnergy 3”
2014 年 10 月	有报道称，BlackEnergy 开发团队，疑似沙虫组织，针对北约、乌克兰和波兰政府、欧洲各重要工业系统进行了攻击
2014 年 10 月	ICS-CERT 警告 ICS 和 SCADA 中存在高危漏洞，并发现攻击者使用 BlackEnergy 2 攻击 SCADA HMI（人机接口）系统
2014 年 11 月	卡巴斯基称，BlackEnergy2 已经可以对路由器、Linux 系统、Windows 系统发起攻击，且能够攻击 Cisco 思科设备和 ARM 及 MIPS 平台
2015 年 11 月	乌克兰一家矿业公司和一家大型铁路公司的系统中发现感染了 BlackEnergy 和 KillDisk
2015 年 11 月	CERT-UA 首次将 BlackEnergy 和 KillDisk 关联在一起。当时正值 2015 乌克兰大选，多家新闻媒体公司被攻击，许多视频和文档资料被毁
2015 年 12 月	乌克兰电网被攻击，引发大规模停电事件，引发关注
2016 年 1 月	CERT-UA 通报称乌克兰最大机场基辅鲍里斯波尔机场遭受 BlackEnergy 攻击
2016 年 1 月	卡巴斯基研究人员发现新型针对乌克兰的 BlackEnergy 文档类攻击，使用 Word 攻击乌克兰电视台 STB
2016 年 12 月	乌克兰的国家电力部门疑似被网络攻击，导致其发生了又一次的大规模的停电事件，本次停电持续了大约 30 分钟。此次停电事件疑似由“外部干扰”所导致的，恶意攻击者通过网络对公司电力系统进行了非法操作。

BlackEnergy 的发展历程

乌克兰电力系统遭到的持续攻击，引起了世界各国安全行业和政府的高度重视。实际上，全球几乎所有的电力公司所使用的工业控制系统都十分类似，操作系统也都以 Windows 居多，底层的硬件更是垄断在为数不多的几个大公司手中，因此，我们预期类似的攻击很有可能会在其他国家和地区重现。

（二）沙特大赦之夜攻击事件

据媒体报道，2016 年 11 月 17 日晚，也就是伊斯兰教的大赦之夜（Lailat al Qadr），包括 GACA（沙特国家民航总局）在内的至少 6 家沙特重要机构遭到了严重的网络攻击。受害者的电脑系统中大量文件和数据被损毁，代之以一张 2015 年 9 月 2 号溺水的叙利亚难民男孩 Alan Kurdi 的照片。

研究者们将此次攻击行动调查中截获的恶意程序样本命名为 Shamoon2.0，同时也将此次攻击行动命名为 Shamoon2.0，因为研究人员们发现，被截获的攻击样本实际上是 2012 年被发现的 Shamoon 程序的一个变种。

2012 年 8 月 15 号，在针对沙特石油巨头 Saudi Ameraco 的网络攻击中，Shamoon 恶意程序首次现身。攻击发动的时候，正值该公司员工休假期间，该公司大约 3 万多台电脑上的文件都遭到损毁。事后，有一个自称 Cutting Sword of Justice 的组织宣布为此次事件负责，但是根据当时多家安全机构的分析，此次攻击应该是一个来自伊朗的有国家背景的黑客组织所为。

所以，尽管媒体在报道 2016 年 11 月发生的这次网络攻击事件中，并未详细报道更多受害者的具体信息，也未对受害者遭受的具体损失做详细的说明，但参考 2012 年的 Shamoon 攻击事件以及 Shamoon2.0 与 Shamoon 的相似性，我们大致可以猜测出：此次攻击事件中的主要受害者应该是沙特的工业系统或工业部门，而受害者的主要损失就是大量系统文件与系统数据被恶意删除，致使工业系统无法正常运行。

Shamoon，又称 Disttrack，是一款模块化恶意程序，具有很强的毁坏性，能够导致目标网络完全瘫痪。此前共发生了两次由 Shamoon 引起的网络攻击事件（其中一次为疑似案例），而攻

击目标都是沙特。

Shamoon 使用的模块程序分为三类:分别是投放器(Dropper)、通讯组件(Communications)和擦除组件(Wiper components)。Shamoon 不仅仅会对目标进行数据的收集，还具有很强的破坏性——即程序内部存在定时器，当系统时间超过设定的时间，Shamoon 就会用无用的数据，例如特定的 JPEG 图片，来覆盖磁盘（包括 MBR、分区表和分区），导致磁盘数据的损毁和被攻击系统的瘫痪。

实际上，Shamoon 在 2012 年和 Shamoon2.0 在 2016 年的攻击中都用了 JPEG 方法：2012 年的攻击中使用的是燃烧着的美国国旗，而 2016 年的攻击中出现的图片是 2015 年 9 月 2 号溺水的叙利亚难民男孩 Alan Kurdi。

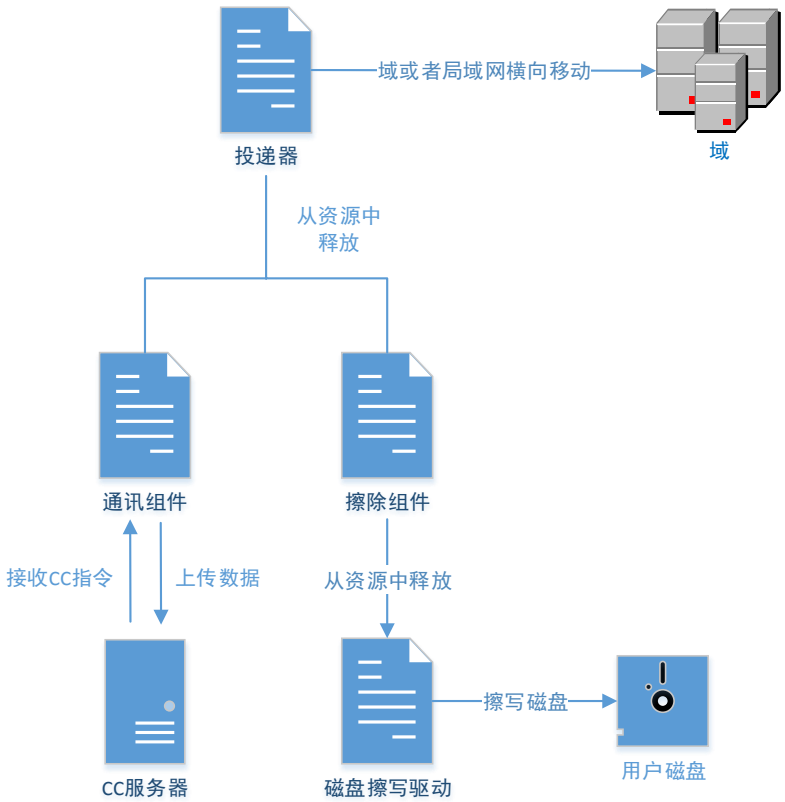
两次攻击的恶意程序编写方式也十分相似，使用了同一个 RawDisk 设备驱动（临时的证书密钥都一样），投递器在释放恶意程序组件时，会从资源中的特定位置读取字节数并且用 Base64 编码的密钥来解密，在与从资源中获取的 Byte 串进行异或操作，拼接后获取完整的程序。

Shamoon 本身还会尝试通过当前的权限来访问当前系统的活动目录，相同域及局域网上的其他主机，进行横向移动。Shamoon 的横向移动可能导致的最严重情况是整个目标网络的大规模瘫痪。

特别值得一提的是，Shamoon2.0 的恶意破坏性要比 Shamoon 更加明显。在先前的 Shamoon 攻击中，恶意样本会首先窃取用户数据并上传到 C&C 服务器上之后，才会执行文件删除或覆盖操作，这就使我们在理论上有可能通过阻断网络或限制 IP 访问等方法来阻止 Shamoon 的破坏行为。但 Shamoon2.0 的攻击者却在程序

中填写了一个完全不可达的 C&C 服务器地址，并在程序中编码了定时器时间为 2016 年 11 月 17 日晚 8:45。这就使得 Shamoon2.0 俨然成为了一颗“定时炸弹”，一旦成功投放，就几乎一定会“爆炸”。

下图给出了 Shamoon 的基本攻击原理。可以看到，投递器投递成功后，通讯组件被释放并且执行后开始与 C&C 服务器进行通讯，其通信过程使用的是 HTTP 协议。但 Shamoon2.0 与之前的版本存在区别，之前的 Shamoon 是将用户的数据上传到 C&C 服务器当中；但是 Shamoon2.0 中，C&C 服务器的地址却被填写成一个不可达的地址：1.1.1.1:8080。



总体而言，Shamoon 与 Shamoon2.0 具有很强的相似性，不仅是攻击的目标国家相似，选取的攻击时间点存在共性（休假期间），而且具体实现技术和攻击原理也都十分相似。因此，多数研究者认为，Shamoon 与 Shamoon2.0 的攻击应为同一黑客攻击

组织。

二、 针对金融系统的犯罪

2016 年上半年接连发生了以孟加拉国央行为代表的银行被盗事件，受害者损失高达数千万美元。随后，下半年又接连发生了以台湾第一银行ATM吐钞事件为代表的一系列ATM机攻击事件。而一个以合法软件开发企业为伪装的，以不当盈利为目的的，长期从事敏感金融交易信息窃取活动的境内 APT 组织“黄金眼”，也在 2015 年底至 2016 年初被截获。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）多国银行被盗事件

2016 年初，媒体陆续曝出了孟加拉、厄瓜多尔、越南、菲律宾等多个国家的银行系统曾经遭遇黑客攻击的消息。尽管这些攻击事件的发生时间不尽相同，但它们都有一个共同特点，就是攻击者都瞄准了 SWIFT 银行间转账系统，并利用这一系统存在的某些“特点”来发动攻击并销毁证据。下表给出了部分攻击事件的发生时间和损失情况。

攻击时间	被攻击银行	计划窃取	实际损失
2013 年	索纳莉银行（Sonali Bank）	未知	25 万美元
2015 年 1 月	厄瓜多尔银行（Banco del Austro）	未知	1200 万美元
2015 年 10 月	疑似菲律宾某银行	未知	未知
2015 年 12 月	越南先锋银行（Tien Phong Bank）	120 万欧元	无
2016 年 2 月	孟加拉国央行（Bangladesh Central Bank）	9.51 亿美元	8100 万美元
未知	疑似香港某银行	未知	未知
未知	疑似菲律宾、新西兰某银行和其他 10 多家金融机构	未知	未知

BlackEnergy 的发展历程

1） 孟加拉国央行（Bangladesh Central Bank）

2016 年 2 月 5 日，孟加拉国央行被黑客攻击导致 8100 万美元被窃取。攻击者通过网络攻击或者其他方式获得了孟加拉国央行 SWIFT 系统操作权限，随后，攻击者向纽约联邦储备银行（Federal Reserve Bank of New York）发送虚假的 SWIFT 转账指令，而孟加拉国央行在纽约联邦储备银行上设有代理帐户。纽约联邦储备银行总共收到 35 笔，总价值 9.51 亿美元的转账要求，其中 30 笔被拒绝，另外 5 笔总价值 1.01 亿美元的交易被通过。而这其中又有 2000 万美元因为拼写错误被中间行发觉而被找回，而另外 8100 万美元则被成功转走盗取。

而我们捕获到的这次网络攻击所使用的恶意代码，其功能是篡改 SWIFT 报文和删除相关数据信息以掩饰其非法转账的痕迹。其中攻击者通过修改 SWIFT 的 Alliance Access 客户端软件的数据有效性验证指令，绕过相关验证。

2） 越南先锋银行（Tien Phong Bank）

2015 年 12 月 8 日，越南先锋银行遭黑客攻击，其攻击手法与孟加拉央行遭到的攻击类似。攻击者最终从越南先锋银行盗走了约 120 万欧元。

360 追日团队也捕获了攻击越南先锋银行的恶意程序样本。相关恶意代码内置了 8 家银行的 SWIFT CODE，越南银行均在这些银行中设有代理帐户。目前看到的 Fake PDF Reader 样本的目的并不是攻击列表中的这些银行，而是用来删除越南先锋银行与其他家银行间的转帐确认消息（篡改 MT950 对帐单）。这样银行的监测系统就不会发现这种不当交易了。

关于针对越南先锋银行攻击的详细分析，可以参见 360 追日团队此前发布的报告：《SWIFT 之殇——针对越南先锋银行的黑客攻击技术初探》。

3） 厄瓜多尔银行（Banco del Austro）

据路透社报道，2015 年 1 月 12 日，在一条来自厄瓜多尔银行系统信息的指引下，位于旧金山的 Wells Forga 美国银行向某个香港的银行账户进行了转账。并且在接连 10 天内，至少有 12 笔厄瓜多尔银行资金通过 SWIFT 系统被转走，总金额高达 1200 万美金。厄瓜多尔银行已就该事件将 Wells Frago 告上了纽约法庭，理由是 Wells Forgo 美国银行本应该将这些交易标记为可疑交易。然而从诉讼资料看，双方银行都相信这些资金是被匿名黑客盗走的。

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。

4） 索纳莉银行（Sonali Bank）

据路透社报道，2013 年孟加拉国的索纳莉银行（Sonali Bank）也发生了类似孟加拉央行的攻击事件。在索纳莉事件中，攻击者共盗取了 25 万美金的银行资金。银行 IT 运营部的高级官员称，在索纳莉银行劫案中，黑客们在一台电脑上安装 keylogger 来窃取其他系统的密码，然后使用 SWIFT 系统发送伪造的转账申请。

5） 攻击事件的相似性分析

通过分析从2013年的索纳莉银行到2016年的孟加拉国央行这4起攻击银行的事件，不难看出相关攻击事件之间有很多的相似性。

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。

3） 篡改 MT9XX 报文清除证据

由于我们暂未捕获到针对索纳莉和厄瓜多尔银行进行攻击的恶意样本，这里主要分析对越南先锋银行和孟加拉国央行攻击事件的追踪。

首先，攻击者都是对 MT9XX 报文进行了劫持：对越南先锋银行的攻击是劫持 MT950 对帐单，对孟加拉国央行的攻击则是劫持了 MT900 借记证实。

其次，两次攻击事件中，攻击者都对相关报文进行了篡改，目的是删除相关转帐记录，进行平帐。而两次攻击事件的区别是：孟加拉国央行事件中是对相关报文篡改后直接发送给打印机打印出来；而越南先锋银行事件中则是对 MT950 的电子版 PDF 文件进行篡改，然后再把 PDF 文件发给打印机打印。但不论怎样，攻击者最终目的就是篡改报告，另外删除其他一些数据信息，从而抹去相关证据线索。

另外，我们还发现，在越南先锋银行事件和孟加拉国央行事件中，攻击者所使用的恶意代码，都存在一个特殊的安全删除函数，这也更进一步证明了这两次攻击事件的同源性，它们并不是孤立的，两者之间有一定联系。

（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。

1） 台湾第一银行（First Bank）

2016 年 7 月 12 日，台湾第一银行发布公告《第一银行 ATM 遭异常盗领客户权益不受影响》表示“第一银行部分分行 ATM 提款机遭异常盗领，作案过程约 5-10 分钟，交易集中在 7 月 9 日和 7 月 10 日，共计遭盗取的金额约 7000 多万新台币，20 家分行共 34 台 ATM 发生异常……可能遭植入恶意软件驱动吐钞模块执行吐钞”。

后经第一银行清算核实，全台共有 41 台 ATM 遭到盗领，被盗金额 8327 余万元。这是台湾首宗银行遭跨境黑客盗领案。后经台湾警方侦破追捕，抓获罗马尼亚籍和摩尔多瓦籍共犯各一人，追回赃款 6050 万元。后续调查还显示，此次攻击中，攻击者是通过攻击补丁更新服务器，向 ATM 机下发恶意程序的，这些恶意程序会开启 ATM 远程控制服务(Telnet Service)，使藏身在海外的幕后操控者可以操控 ATM 机“吐钞”。

此次事件中遭攻击的 ATM 机，全部是来自德利多富(Wincor)公司的同一款机型（pro cash1500 机型），目前该款机型已全面暂停服务。据了解，德利多富（Wincor）的产品涉及银行业及零售业，提供包括现金类自助设备和非现金类自助服务终端及其解决方案，代表硬件产品包括自动取款机、存取款一体机、多媒体服务终端、存折打印机等，业务遍及 130 多个国家。

在对相关攻击事件的分析中，我们发现攻击者并没有使用银行卡和对 ATM 机操作等，即攻击者无需物理接触 ATM 机，就能实现 ATM 机自动吐钞目的。这点攻击现象引起了我们的注意，以往

攻击 ATM 的事件并不少见，但能达到不进行物理接触而使 ATM 吐钞的攻击，还是比较少见的。

2） Anunak 组织（即 Carbanak）

不过，在台湾第一银行 ATM 机吐钞事件之前，也有其他攻击组织曾经实施过这种针对 ATM 机的非接触式攻击。其中最为著名的 APT 组织就是 Anunak（即 Carbanak）。

Anunak 组织的攻击活动始于 2013 年，该犯罪团伙总计向全球约 30 个国家和地区的 100 家银行、电子支付系统和其他金融机构发动了攻击，相关攻击活动还很活跃。在《2015 年中国高级持续性威胁（APT）研究报告》中我们也提到了 Anunak。通过研究分析该组织相关攻击手法和意图，我们将该组织视为针对金融行业的 APT 组织。

Anunak 组织攻击的一般过程是：首先，通过极具针对性的攻击手法，入侵金融机构员工的计算机或银行网络；随后，通过内部网络，对计算机进行视频监控，从而查看和记录负责资金转账系统的银行员工的屏幕；最后，当攻击者了解到银行相关员工工作的全部详情后，就会模仿银行员工的行为进行恶意操作，盗取银行资金。

另外该组织还可以控制银行的 ATM 机，命令这些机器在指定的时间吐出现金。当到支付时间时，该组织会派人在 ATM 机旁边等待，以取走机器“主动”吐出的现金。

通过将 Anunak 的攻击手法与台湾第一银行吐钞事件进行对比，我们发现，二者之间有很多相似的地方，具体如下表所示：

	台湾第一银行	Anunak（即 Carbanak）
幕后组织	攻击者来自俄罗斯	攻击者来自俄罗斯
攻击方式	利用恶意程序	利用恶意程序
植入方式	攻击补丁更新服务器	攻陷银行内网，到获得 ATM 权限
ATM 品牌	Wincor	Wincor
吐钞方式	突破取款上限，连续吐钞	突破取款上限，连续吐钞
取现方式	指定时间，无需物理接触	指定时间，无需物理接触
攻击规模	40 台 ATM	52 台 ATM
窃取金额	8000 万新台币	5000 万卢布

台湾第一银行吐钞事件与 Anunak 攻击特点的对比

3） 泰国邮政储蓄银行

2016 年 8 月，泰国政府储蓄银行发现，从当月的 1 日至 8 日，全国共有 21 台 ATM 机中的现金被盗。这些被盗的 ATM 机分别分布在曼谷、 普吉岛、 春蓬、 巴蜀、 碧武里和素叻他尼等地。获悉此事后，泰国中央银行（Central Bank of Thailand ，BoT）向全国的商业银行发出安全警告，关闭了全国约 3300 台 ATM 提款机。

通过对 ATM 机内部摄像头捕获信息的分析，泰国警方确认此次事件中的犯罪团伙属于外籍人士。随后，泰国警方逮捕了三名犯罪嫌疑人，据这些犯罪嫌疑人交代，他们组织大约有三十名东欧人，其中大部分人都在 ATM 机领域有多年的工作经验，同时，组织内部还有三名俄罗斯人。

该犯罪团伙的主要攻击手法是：通过插入特别制造的 ATM 卡（带有 EMV 芯片），将恶意程序 Ripper 植入到 ATM 机中。恶意程序一方面会让 ATM 机每次吐钞 4000 泰铢，另一方面会使 ATM 机与银行网络断开，从而使 ATM 机在吐钞时不会被发现。

据调查,该犯罪组织通常是在深夜集体出动,相互配合作案。在 8 月的 1 日-8 日期间，该组织累计从泰国各地的 ATM 机上取走了大约 1229 万泰铢（约合 346,000 美元)。

4） 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：

1） 入侵银行内部网络，获得 ATM 机控制权限

2） 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）黄金眼行动事件

2015 年 12 月，360 安全服务团队基于日常的应急响应记录结合云端大数据，发现一系列针对金融机构的定向攻击事件，360 安全服务团队联合 360 追日团队对此事件展开了深入调查。

调查结果显示，攻击者是一个以合法软件开发企业为伪装的，以不当盈利为目的的，长期从事敏感金融交易信息窃取活动的境内 APT 组织。其攻击水平和反侦察能力均达到了国家级水平，甚至超出了很多境外的 APT 组织。该组织的活动时间至少长达 12 年以上，遭到该组织长期攻击的金融机构涉及多家。

鉴于该组织是一个专门针对金融系统发动攻击的 APT 组织，我们将该组织及其发动的攻击行动命名为“黄金眼”，组织及行动编号 APT-C-19。

调查显示，黄金眼行动最早可以追溯到 2004 年，相关攻击活动分别在 2012 年和 2014 年呈现两次高峰，且 2014 年的攻击强度远远超过 2012 年。其主要攻击对象为：基金、证券、保险、理财和资产管理等多种类型的境内金融机构，还包括一部分的个人股民。

黄金眼行动使用了一整套恶意代码对目标系统实施入侵和控制，并可跨越所有 Windows 平台发动攻击。相关攻击工具经过了长期不断的版本升级和功能演化。黄金眼行动还具有极强的反侦察能力，相关攻击代码在被释放出来之前也做了必要的清理。

黄金眼行动的恶意代码，其架构之复杂，功能之完善，反侦察能力之强大，以及持续改进的繁多版本，显示出该组织开发运维的高度专业性。

此外，我们也发现，即便仅仅从对金融业务的熟悉程度来看，

黄金眼行动也具有高度的专业性。我们有理由认为，该 APT 组织实际上是由一群计算机专家和熟悉金融业务的人员共同组成。

从攻击目的来看，黄金眼行动主要是通过恶意程序窃取其他金融机构的敏感交易信息，进而将这些交易信息作为投资情报，用于不当的投资活动并赚取非法超额利润。