平安金融安全研究院
PingAn Academy of Financial Security

NSFOCUS

2017
金融科技安全分析报告

平安金融安全研究院
PingAn Academy of Financial Security

平安金融安全研究院

是由平安集团旗下的全资子公司平安科技成立的业界首家综合性的金融安全研究及创新机构，为平安集团、各行业和国家提供强有力的金融安全技术支撑，为金融机构在互联网时代下的信息安全建设、业务安全风控、金融科技安全保障和国家金融安全作出技术贡献，努力推动和引领我国在金融安全方面的科学技术进步，打造金融安全品牌。

NSFOCUS

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技）

成立于 2000 年 4 月，国内外设有 40 多个分支机构，一直为各行业提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技在网络空间安全生态建设和威胁情报应用方面组建的专业性威胁情报研究中心。

《2017 中国企业金融科技安全调查问卷》

本报告部分数据来源于问卷调查。问卷由平安金融安全研究院和北京神州绿盟信息安全科技股份有限公司共同发起，共发出 1591 份，覆盖安全行业和金融行业，参与者主要为：安全架构师、安全咨询师、安全工程师，占比 40.3%；安全开发及运维人员，占比 15.7%；还包括首席执行官、首席信息官、信息安全官、IT 部门主管、业务部门主管等。

目 录

01 执行摘要

在 2017 年 8 月 22 日，世界经济论坛发布了报告《超越金融科技：全面评估金融服务的颠覆潜力》[1]。该报告涵盖了数百位金融、科技领域专家的访谈内容，旨在探索创新对全球金融生态系统的影响。报告对驱动 FinTech 创新的 8 大因素及其颠覆潜力进行了定义；同时总结出在 FinTech 冲击下，支付、信贷、财富管理、保险、数字银行等 7 大金融领域未来的创新模式和路径，以及每个领域所面临的风险和可能的终局。近年，依托云计算、大数据、人工智能、区块链等先进的计算机技术的发展，金融服务也趋于多样化、便利化、智能化。金融科技的出现频率正在高速增长，伴随其技术变革与创新加速，至今已经步入金融科技 3.0 时代。

天下熙熙皆为利来，天下攘攘皆为利往，逐利更是攻击者的天性。随着金融科技日渐成为金融产品的重要支撑手段，攻击者也在不断丰富其攻击目标和攻击手段，以图提升自身的攻击变现能力。一方面，攻击者对金融科技系统的渗透逐步深入，从网络服务、金融业务逐步深入到核心业务数据、用户财产和隐私。攻击者不再满足于危害金融系统的可用性，更青睐从贩卖数据和资产转移中直接获利。另一方面，攻击者不局限于传统针对信息系统的攻击，愈多从人员的角度迂回渗透，勾结内部人员进行数据倒卖。Loudhouse 曾发布的企业安全调查报告显示，如果价格到位，35% 的员工会倒卖包括公司专利、财务记录和客户信用卡等敏感数据。这一调查事实也侧面印证在网络安全、业务安全和数据安全之外，人员安全同样也需要重视。

对于以金融科技为目标的攻击者，获利是他们的核心诉求。那么对于金融科技安全从业者而言，在传统的以脆弱点和检测点为核心的防护方案之外，更应从获利点出发，逆向分析，进而组织自身的防护体系。

[1]《超越金融科技：全面评估金融服务的颠覆潜力》，世界经济论坛，2017 年 8 月 .

安全现状

1. 金融行业经大幅度互联网化，83.5% 的机构或企业都开展了互联网业务。金融行业约 60% 的机构使用了各类云服务，大部分使用的是私有云，也有超过 20% 的机构使用公有云或者混合云。金融行业使用云业务时最关心的风险除了数据及隐私保护外，也十分关注业务的访问权限控制。

2. 40% 金融行业机构对安全事件的处置可以在一天内完成，另外 40% 能在一周内完成，约 20% 对安全事件处置超过一周。同时，漏洞修补时间近半数超过一周。

3. 从问卷统计中，我们认为安全事件的最主要成因是安全意识淡薄和运维投入不足，这或许是安全管理各类问题的根源所在。缺乏基本的安全意识，安全投入自然不足，同时安全管理制度上也会不够完善，导致数据安全、隐私保护等方面出现问题。

4. 金融行业从业者最关心的安全问题集中在数据安全与隐私保护，而合规性要求也是企业关注安全问题的一个重要考量。但我们需要指出，安全措施是一个整体的规划，并不是一个方面或者某个领域的单一问题，需要从开发、管理、运维等各个生产环节进行规划，不是一台设备、一次巡检能够彻底解决的，为了更好的保护数据安全与隐私，需要有完善的配套管理流程、防护方案。

5. 对于安全服务，业务量最大的服务包括安全咨询、安全运维、应急响应服务，从问卷统计中我们认为，金融行业仍然普遍缺乏安全管理的知识和经验，在安全培训、人才储备上需要加强。

6. 我们看到企业均加强了对信息安全问题的关注。另外，大部分企业（71.3%）会加大预算的投入，但只有少部分（21%）企业打算扩招自己的安全团队。这应该是由于近年来互联网业务高速发展、企业业务复杂度大幅提升、新技术频出、攻击态势演变更加迅猛而促使企业采取应对举措。企业为了维护自身业务安全，需要技术、人员两方面的支持，不过大部分企业仍然倾向于通过业务外包来减轻自己管理规划的负担。

安全态势

1. 2017 年与 2016 年相比，DDoS 攻击总流量和攻击规模大幅上升，攻击总流量达 **64 万 TBytes**，增长 **79.4%**，单次攻击峰值高达 **1.4Tbps**，是 2016 年的近 **2 倍**。

2. 2017 年 Botnet 的数量和规模在不断扩大。其中，C&C（僵尸网络控制者）的数量持续不断增长，在进入 8 月份后增速明显，10 月份环比增长达到 **1.67%**。同时，全球受控主机的数量间歇性增长，8 月份的数量环比上月增长高达 **3** 倍（增长 **320%**）。

3. 网络勒索事件频发，“Opicarus2017”等多起事件利用勒索病毒进行攻击，危及大量金融机构的网站安全，并导致敏感数据泄露。

4. MySQL 的漏洞暴露情况最为严重，MySQL 和 PostgreSQL 在过去三年里的漏洞数量有着较快的增长。

5. 以 Web 应用为目标的攻击中，据统计，针对框架（例如 Struts、ThinkPHP）的攻击占比高达 **54%**，插件类（例如 ImageMgick 等）占比 **39%**，而针对具体 CMS 程序的攻击占比较低。

本报告将结合相关企业数据、行业报告和安全分析报告，从互联网的角度重点分析金融行业的网络安全现状。报告将简单介绍金融科技的发展历程和趋势，重点介绍典型的网络安全威胁、数据安全威胁和业务安全威胁，并结合各环节中的典型安全案例和《2017 中国企业金融科技安全调查问卷》，分析金融科技机构的安全现状及面临的安全趋势。金融行业要持续、健康地发展，必定不可忽视安全问题。作为报告的编纂方，平安金融安全研究院与绿盟科技希望本报告能为我国金融业从业机构提供一个可参考的安全视角，为我国金融业的健康发展贡献一份薄力。

02 金融科技

传统金融是只具备存款、贷款和结算三大传统业务的金融活动，传统金融机构在面对市场竞争时的应对能力明显不足。随着互联网的发展，互联网金融时期来临，金融业搭建在线业务平台，通过互联网渠道收集用户信息，完成业务处理。传统金融加科技服务，这是金融科技 1.0 阶段。金融科技 2.0 则是向服务金融科技转化，通过底层技术革新促使金融服务的方式发生变革，重塑金融产品的生成模式和定价模式，极大提升资产配置效率。其典型应用有智能投顾、智能信贷、供应链金融等。金融科技不断发展，同时也面临着越来越多的安全威胁，安全事件频发，对业务造成资金损失和极大的负面影响，关注金融安全将是金融科技 3.0 时代的重中之重。

金融科技涉及领域广泛，应用场景多元。大数据、人工智能、区块链和云计算作为金融科技核心技术，使金融服务更加高效、智能，已在许多场景展露头角。

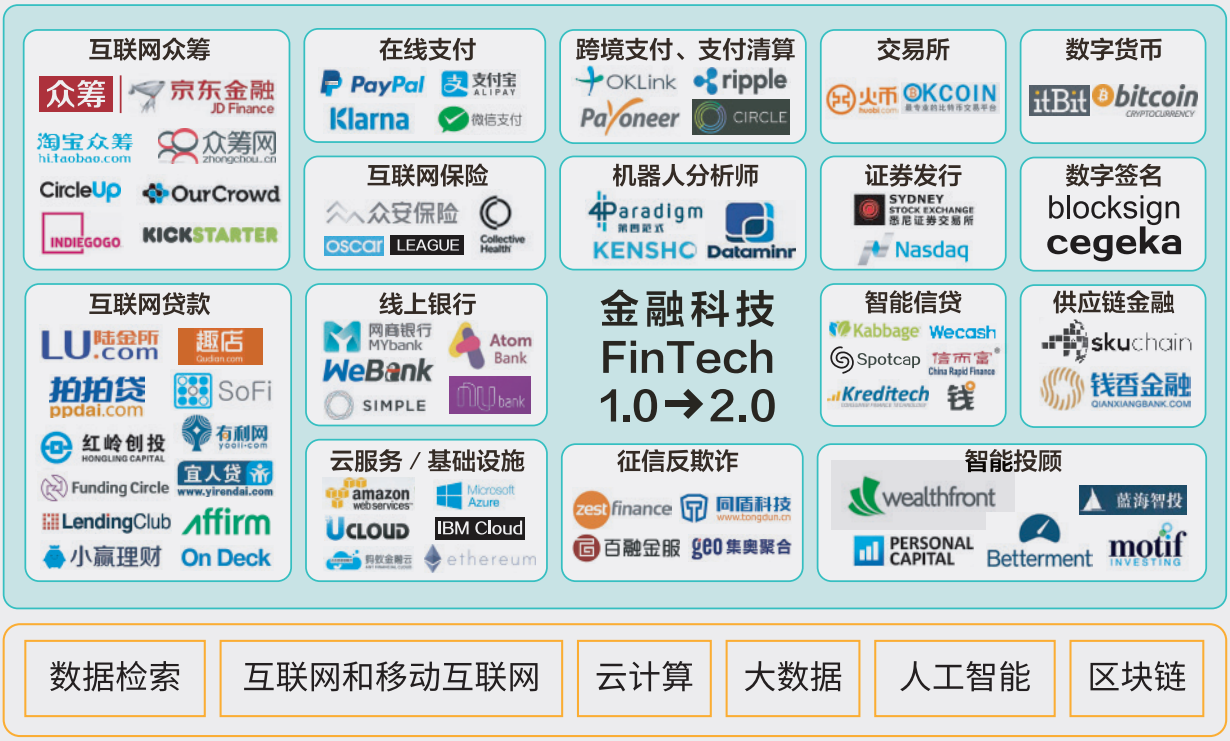

图 1 - 金融科技的应用场景 [2]

金融科技天生拥有创新基因，对行业、经济、民生是有益的，但插上科技翅膀的金融，具有更强、更广和更快的易破坏性，因而尤其需要引导和规范。在国际上，美国、英国、欧盟等相继发布金融科技监管文件，以平衡发展需求。而国内也已加快金融监管机构、法律法规等的建设，中国人民银行已成立金融科技（FinTech）委员会，旨在加强金融科技工作的研究规划和统筹协调。从总体上看，国家监管者对金融科技发展持开放态度，但同时对于金融科技风险的重视程度也逐年增强，预计未来几年，国内监管机构将采取更为主动积极的监管措施。

[2]《金融科技》，周伟，张健，梁国忠，2017 年 8 月 .

03 网络安全威胁介绍

金融科技技术的发展大力推动了金融服务领域的拓展和维度，其面临的安全威胁也与日俱增。《2017 年度网络犯罪报告》[3] 中指出：网络犯罪是当今世界上所有公司面临的最大威胁，也是人类面临的最大问题之一。根据这份报告，到 2021 年为止，网络犯罪的成本将从 2015 年的 3 万亿美元增加到 6 万亿美元。众所周知，金融行业是我国网络安全重点行业之一，因其行业特殊性金融机构一直是网络犯罪的主要目标。以下，我们将通过 2017 年金融行业的重大安全事件说明安全威胁可能造成影响及损失。

3.1 DDoS 攻击

分布式拒绝服务 (Distributed Denial of Service，DDoS) 攻击指借助于客户或者服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。

2017 年 6 月相继发生的“匿名者”和“无敌舰队”勒索事件，是对金融机构发起大规模 DDoS 攻击。显而易见，拒绝服务攻击已是当前金融领域极为常见的安全威胁，金融业作为对安全性和稳定性都要求极高的行业，一旦服务瘫痪，资产管理系统中断，将会造成难以弥补的损失。

攻击仍然频繁，共发生 20.7 万次攻击

2017 年同 2016 年相比，攻击发生次数基本保持平稳，共计发生 20.7 万次。但是从攻击总流量上来看有较为明显的波动，从年初到 5 月份前后，攻击总流量有非常显著的增长，而 5 月份之后攻击总流量回落至较为平稳的水平。与 2016 年相比，2017 攻击仍然频繁，攻击总流量大幅上升。

[3] “Cybercrime damages are predicted to cost the world $6 trillion annually by 2021”，PR Newswire，2017 年 10 月 19 日 .

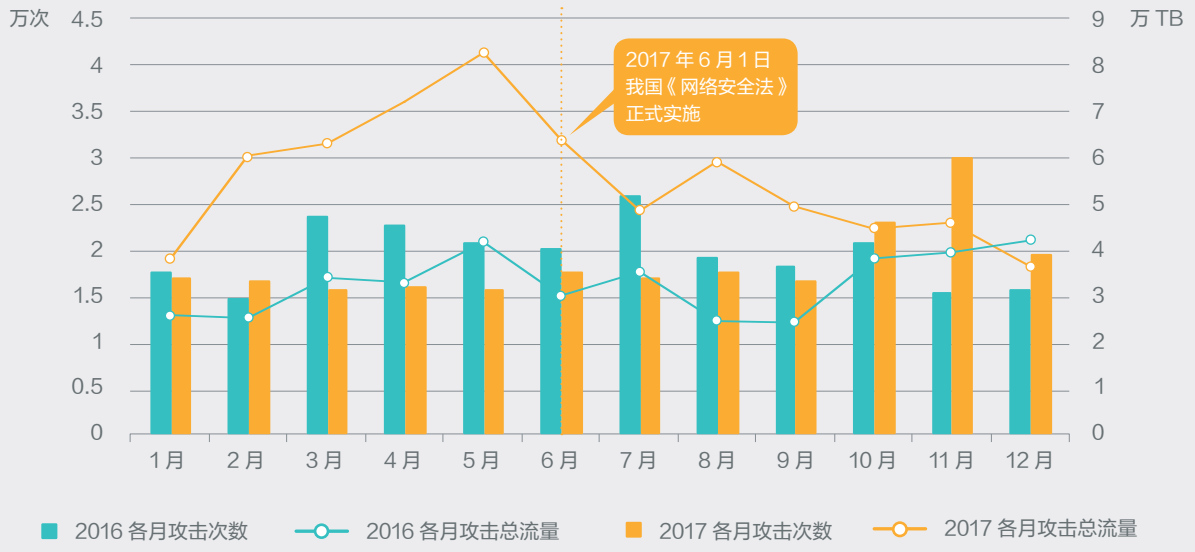

图 2 - 2016 vs 2017 各月份攻击次数和流量 [4]

从类型上看，2017 年攻击次数占比最高的攻击类型仍然为反射型攻击，实施这类攻击，黑客只需要拥有很少的带宽，就能以此放大产生显著的攻击流量。从攻击流量上看，SYN Flood 2017 年度占比突出超过 60%。综合 2017 年度网络环境分析，绿盟科技认为与物联网僵尸网络的扩张有较大的关系，互联网具有设备基数大、防护弱、在线时间长等特点，成为了发动 DDoS 攻击的温床。

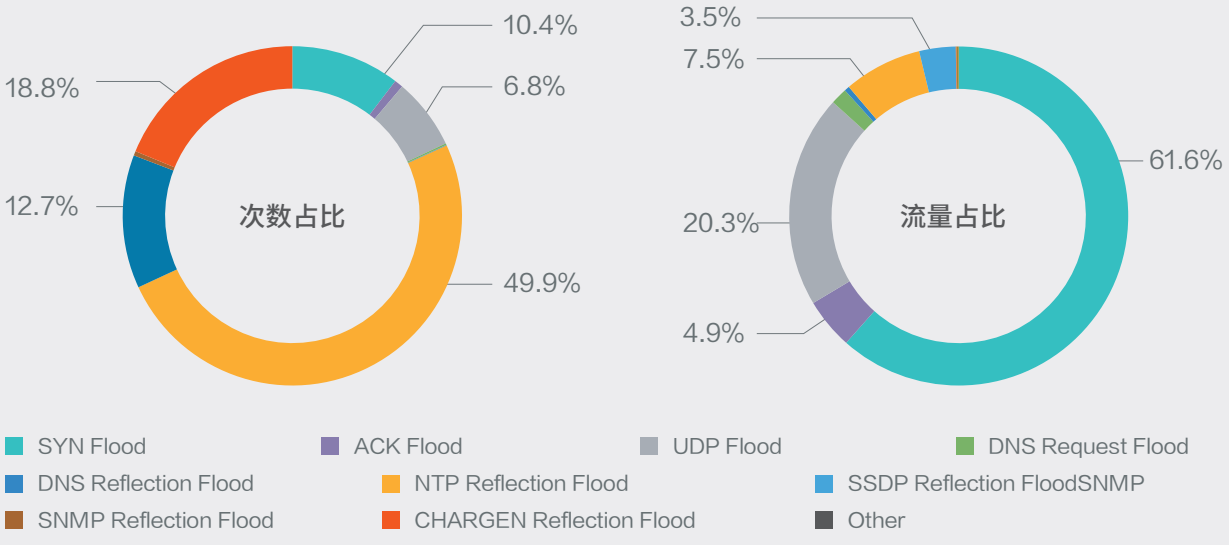

图 3 - DDoS 攻击类型分布

[4] 图 2 至 6、图 16 引用中国电信云堤与绿盟科技联合发布的《2017 年 DDoS 与 Web 应用攻击态势报告》.

流量再创新高，峰值高达 1.4Tbps

流量持续攀升似乎已经不是什么新的态势，从近两年的报告中都可以看到，每个月都会出现超过百 Gbps 的流量，最高的时候流量已经达到 Tbps 的级别，2017 年度攻击最频繁的是 5 月份，攻击最高的峰值更是达到了 1.4Tbps 的级别，这种“巨无霸”攻击，一次一次挑战着防御者的能力上限。

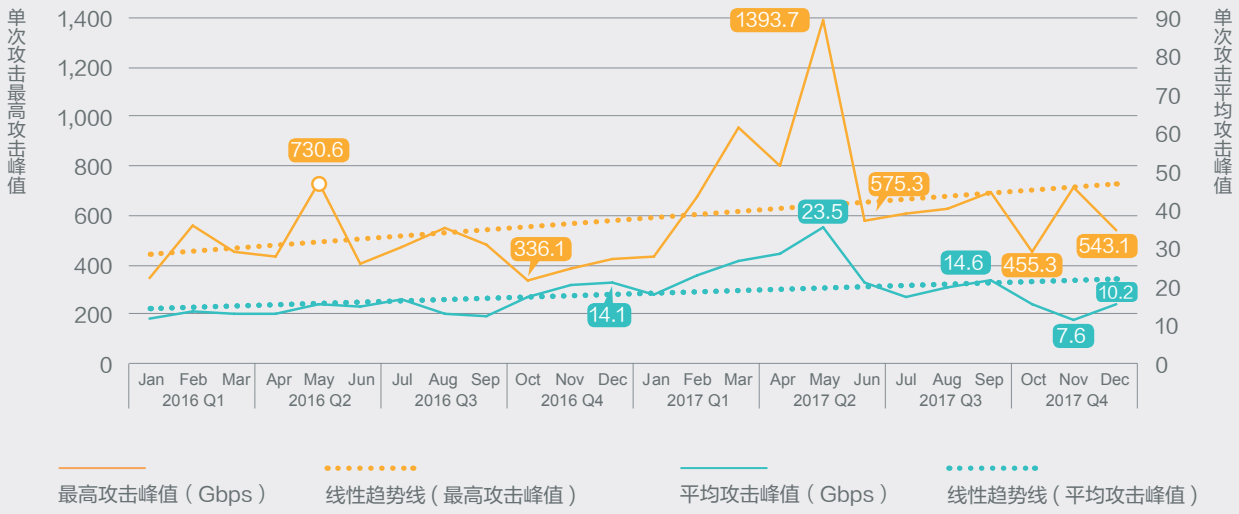

图 4 - 单次攻击最高攻击峰值与平均攻击峰值

另外，从流量的区间分布来看，大流量攻击明显增多，也是 2017 年度一个显著的趋势。

来自 IoT 设备的攻击比例达到 12%

在 2017 年的 DDoS 攻击中，攻击源中 IoT 设备的数量已经占据相当的比例，在或大或小规模的 DDoS 攻击中 IoT 设备都有显著的占比，已经成为 DDoS 网络环境中需要重点关注的一个类别。从网络总体态势来看，物联网迅猛发展的过程中必然伴随着安全技术的滞后，可预测 IoT 设备的威胁治理会进一步提上日程，而作为最易实施的攻击类型之一，IoT 遭受 DDoS 攻击的数量会进一步上涨。

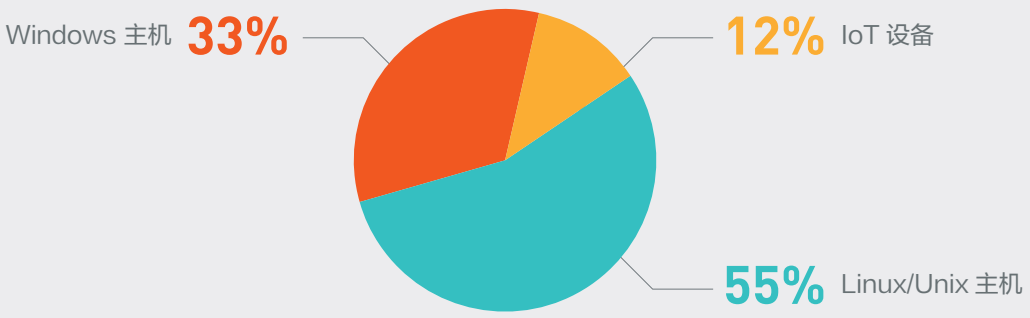

图 5 - DDoS 攻击源设备类型

在 IoT 设备参与 DDoS 的攻击中，路由器、摄像头是主要的设备类型。这与这两年 IoT 发展的情况基本是一致的，大量的路由器、网络摄像头被引入生产、生活环境，而安全配套措施尚未进一步完善，可以合理预期的是在物联网攻击这个领域会有更多的攻击形式出现。从数据统计上看，我们观察到，在属于物联网设备的 IP 中，恶意 IP 的比例是高于平均水平的，例如，在对公网摄像头 IP 进行统计时，我们发现这些 IP 中恶意 IP 的比例约 4.8%，而对于所有 IP（中国境内）而言，恶意 IP 的平均占比仅为 1.57%，也就是说，摄像头恶意 IP 比例是平均水平的 3 倍，物联网设备的风险明显是较高的。

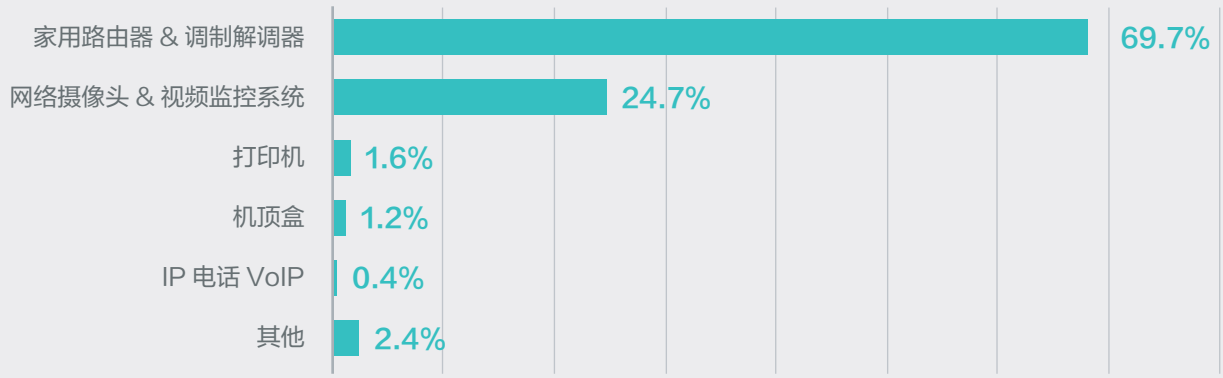

图 6 - DDoS 攻击源 IoT 设备

3.2 网络勒索

网络勒索（Cyberextortion）是一种犯罪行为，它对企业造成攻击事实或攻击威胁，同时向企业提出金钱要求来避免或停止攻击。近年，网络犯罪已经开发出可以用来加密受害人数据的勒索软件（Ransomware），

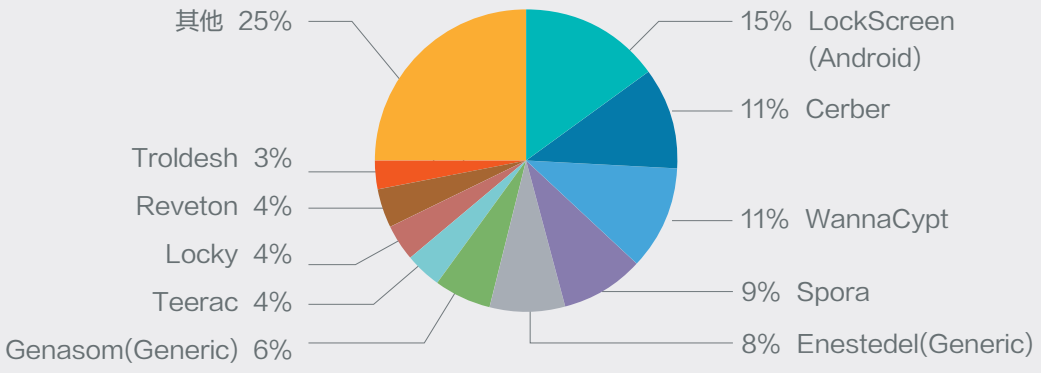

图 7 - 2017 年上半年最流行的勒索软件 [5]

[5] “Ransomware FAQ”， Microsoft.

然后攻击者利用解密密钥向受害人索取钱财。2017 年度，此类攻击事件数量占比靠前的勒索软件有 LockScreen、Cerber 和 Wannacrypt 等。其中，Wannacrypt 感染事件爆发，全球范围近百个国家遭到大规模网络攻击，攻击者利用 MS17-010 漏洞，向用户机器的 445 端口发送精心设计的网络数据包，实现远程代码执行，被攻击者电脑中大量文件被加密，被要求支付比特币以解密文件。

2017 年 6 月相继发生的“匿名者”和“无敌舰队”勒索事件，对企业发起攻击威胁来索要钱财。许多金融机构在此类事件中收到勒索邮件。“匿名者”向全球金融机构发起代号为“Opicarus2017”的攻击，中国人民银行、香港金融管理局等超过 140 个金融机构都在其攻击列表中，被要求支付 10 比特币（目前市值约 53 万人民币）作为保护费。

现今，对互联网服务的勒索攻击已经成为一种网络攻击趋势，平均每天有 4000 起勒索软件攻击。

3.3 僵尸网络

据绿盟科技监测的数据显示，2017 年 Botnet 活动仍然十分猖獗，尤其 Q2 季度更是 Botnet 活动的高发期。根据绿盟科技监控的僵尸网络 C&C 攻击指令数据，在 Botnet 活动最高峰时期，平均每天共发出 5187 次指令，单个 C&C 每天发出的指令最高达 114 次。

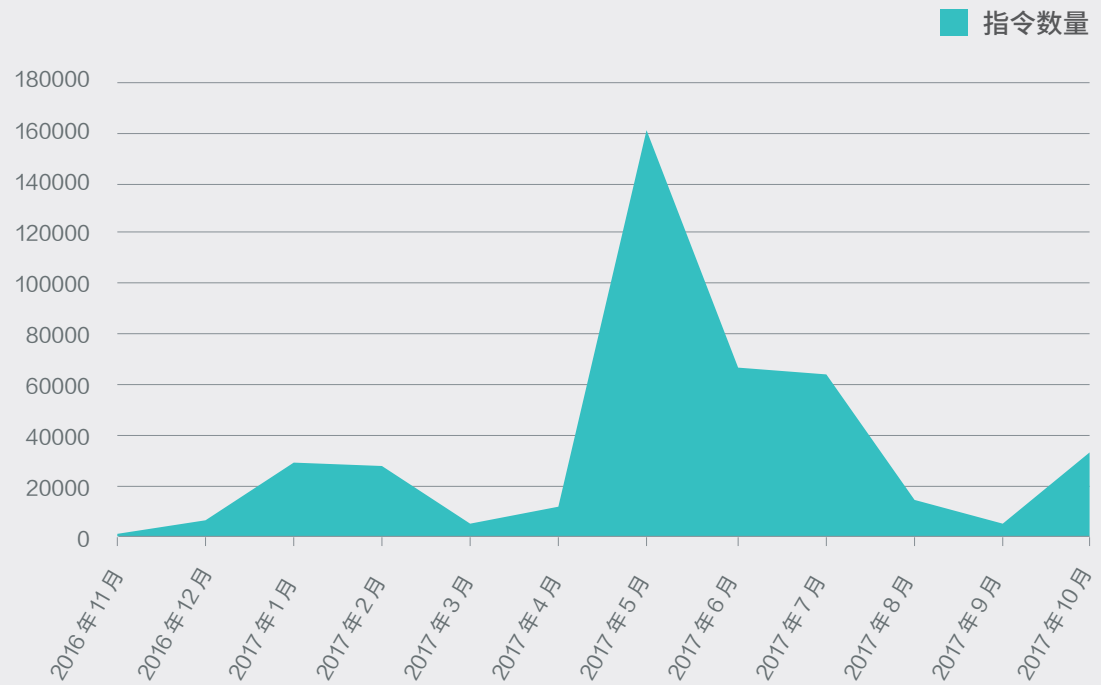

图 8 - 僵尸网络 C&C 攻击指令数据

2017 年 Botnet 的数量和规模在不断扩大。其中，C&C 的数量持续不断增长，进入 8 月份后增速明显，10 月份环比增长达到 1.67%。另一方面，全球受控主机的数量间歇性增长，8 月份的数量环比上月增长高达 3 倍（增长 320%）

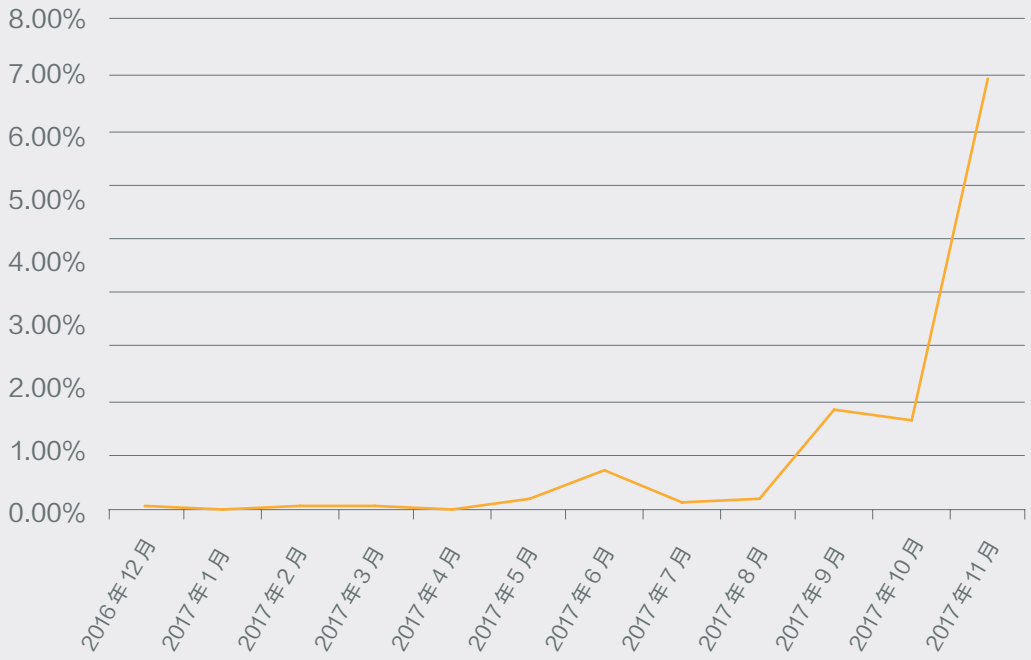

图 9 - C&C 数量增长率的变化趋势

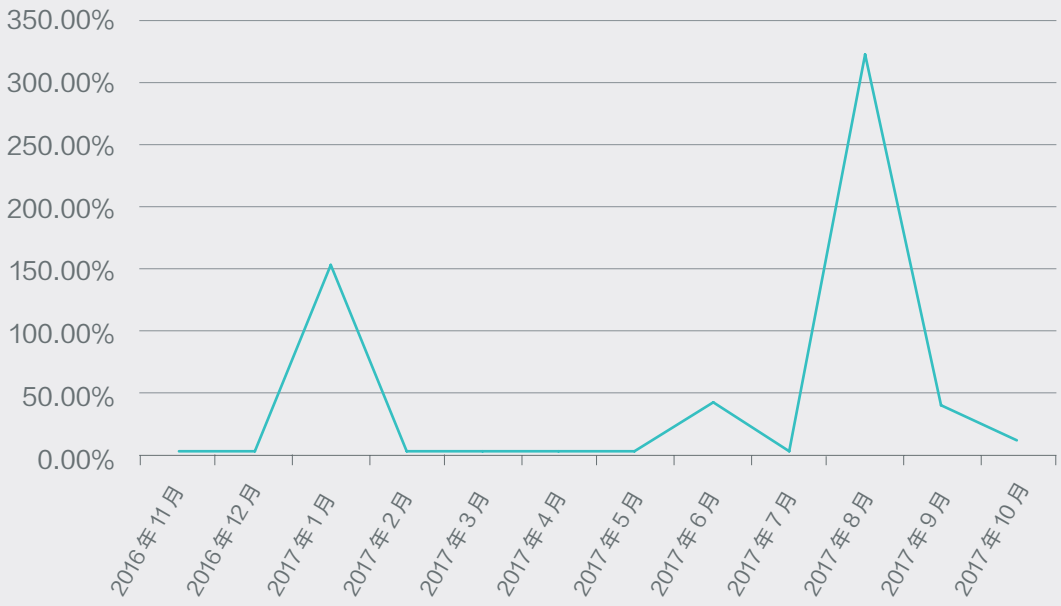

图 10 - 僵尸网络受控主机增长率

物联网和智能设备、移动设备构成的 Botnet 开始对 Botnet 战场的形势产生新的影响。在绿盟科技持续跟踪的 Botnet 中，至少存在 4% 的样本攻击目标为物联网设备。虽然 Botnet 形式还是以 Windows 平台的设备为主，但是近年来，随着 IoT 设备、智能设备、移动设备的入网，针对 IoT 或其他智能设备、移动设备的恶意样本也逐渐增多。

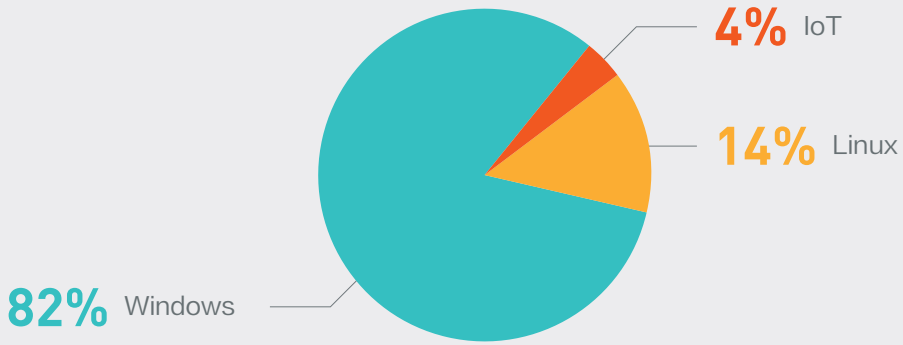

图 11 - 僵尸网络运行平台统计

对于 PC 用户，邮件、“水坑”站点或者在软件安装包中捆绑恶意代码都是很有效的入侵手段，而对于物联网设备来说，其在线时间长、数量规模大、用户普遍疏于升级和配置，导致黑客通过简单扫描就可以捕获大量存在漏洞的设备。2017 年 10 月绿盟科技发现并命名的机顶盒蠕虫 Rowdy，就是利用了机顶盒的脆弱性在国内互联网上大规模传播 [6]。另外，绿盟科技关注到一些 Botnet 家族攻击的目标是 Android 平台的设备，典型的家族包括：Dendroid、FlexiSpy、GMbot 等， Botnet 俨然是一个全平台存在的互联网威胁。

正如在前文提到的，Botnet 持续不断的追求规模的扩张，通过俘获大量设备提升自身攻击的能力，IoT 设备具有的脆弱性使其成为理想的切入点。但是贪婪的黑客们野心并未停止，我们观察到有的 Botnet 已经具备了跨平台的能力，在兼具自传播特点的同时能够根据设备类型，植入对应平台的程序来获取控制权限，进一步提升自己的传播能力。下面是几个典型的具有跨平台传播能力的 Botnet：

[6] “新型 IoT 机顶盒恶意软件 Rowdy 网络分析报告”，绿盟科技博客 .

Botnet 家族	运行平台
Rowdy	linux(x86/x86_64、arm、arm4、arm7、mips、mpsl 等)
Mirai	windows、linux (ARM、EABI4、MIPS、MIPS-I、PowerPC or cisco 4500、Renesas SH、SPARC、Intel 80386)
Gafgyt.bax	linux(x86/x86_64、ARM、Mips、PowerPC、SuperH 以及 Motorola 68000)
darkshell 族	Windows、linux(x86)
jRAT (远控)	依赖 java 环境实现跨平台，windows、linux、macos、freebsd 等

表 1 - 僵尸网络跨平台传播能力分析之运行平台

从 Botnet 采用的程序语言上，也可以发现跨平台的趋势。C 语言和脚本语言具有良好的跨平台能力，在 arm 架构的嵌入式系统和在 linux、Windows 系统中都有良好的适应能力。在此基础上构建的 Botnet 程序，具备跨平台传播运行的能力。

Botnet 家族	编写语言
Rowdy	C++
Gyddos	C++
LuaBot	Lua
Aldi_bot	Delphi
yi2.0	易语言

表 2 - 僵尸网络跨平台传播能力分析之编写语言

另外，脚本语言的编写相对比较容易，可以更加快速高效地实现一个新的 Botnet 程序。较低的门槛、快速的收益吸引着更多的黑客，使得网络中 Botnet 的威胁形势更加严峻。2017 年 9 月，众多网站发现其网页内嵌了挖矿 JavaScript 脚本，一旦用户进入网站，JS 脚本就会自动执行，占用大量机器资源挖取数字加密货币，导致电脑异常卡顿[7]。挖矿病毒就是僵尸网络的一种。

2017 年大规模爆发挖矿木马僵尸网络病毒，如“Bondnet”、“Adylkuzz”、“隐匿者”，其中很大一部分来自中国。金融、运营商及互联网等众多行业均有相关安全事件发生。2017 年 12 月底有安全公司发布预警称“知名激活工具 KMSpico 内含挖矿病毒”。据绿盟科技安全专家分析，原作者的官方版本并不含挖矿病毒，而是黑客利用搜索引擎排名假冒克隆 KMSpico 的网页，发布捆绑挖矿软件在内的多种病毒，诱导用户下载，进而窃取用户隐私信息或利用用户电脑挖矿谋取暴利[8]。

3.4 APT 攻击

高级长期威胁（Advanced Persistent Threat，APT），又称高级持续性威胁、先进持续性威胁等，是指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，仅针对特定的目标。其通常是出于商业或政治动机，针对特定组织或国家，并要求在长时间内保持高隐蔽性。

在过往的监控中，实现政治诉求的 APT 居多，例如伊朗“震网”事件、白俄罗斯军事通讯社事件，随着时间迁移，APT 概念和技术开始被行业熟知，各种层面的对抗也更加复杂。2017 年 NSA“方程式组织”与 CIA 网络情报机构的武器库泄露，为整个黑色产业链条提供了大量有价值的“弹药”，更多的组织和个人可以利用更加成熟的技术实施高级攻击。APT 攻击相较普通的攻击手法，实施难度和成本都更高，除了国家资助下政府间的对抗外，在巨大的利益驱使下，金融行业成为攻击者的首选目标，2017 年绿盟科技发现的境外 APT-C1 组织就是利用“互金大盗”恶意软件攻击我国某互金平台，窃取平台数字资产就是典型针对金融行业新型业务所采取的 APT 攻击事件。

金融行业与其他行业一样，都在面对技术的革新和升级，一方面带来了更多的便利性，另一方面势必诱发许多潜在的风险，但是与其他行业不同的是，金融行业的资产天生比其他行业具有更直接的价值，对于 APT 风险，金融行业需要特别关注。

[7] “腾讯安全 2017 年度互联网安全报告”，腾讯电脑管家，2018 年 1 月 17 日 .
[8] “激活工具 KMSpico 内含挖矿病毒事件的分析”，绿盟科技博客 .

04 数据安全威胁介绍

近年，大规模数据泄露事件激增，2017 年前 11 个月的数据泄露事件数量已比 2016 年全年总数量多出 10%[9]。美国知名信用机构 Equifax 在 9 月份透露，曾遭黑客袭击，导致 1.43 亿名用户的信息泄露 [10]；科技公司 Uber 则发现，5700 万名乘客和司机的信息在 2016 年一次大规模数据泄露事件中被黑客窃取。数据泄露的目标除了政府机构和金融机构，已经扩大到第三方承包商、数据集成商、以及安全厂商和解决方案提供商自身，企业和个人可能会因为敏感数据泄露而处于危险之中。

4.1 数据库漏洞与利用

许多数据库的读取接口直接暴露在互联网上，并且没有设置完整的访问控制策略，通过弱密码甚至空密码就可以直接获取数据库的控制权限。数据库勒索是黑客通过各种攻击手段获取数据库控制权，加密或破坏数据，以此要挟受害者支付赎金。

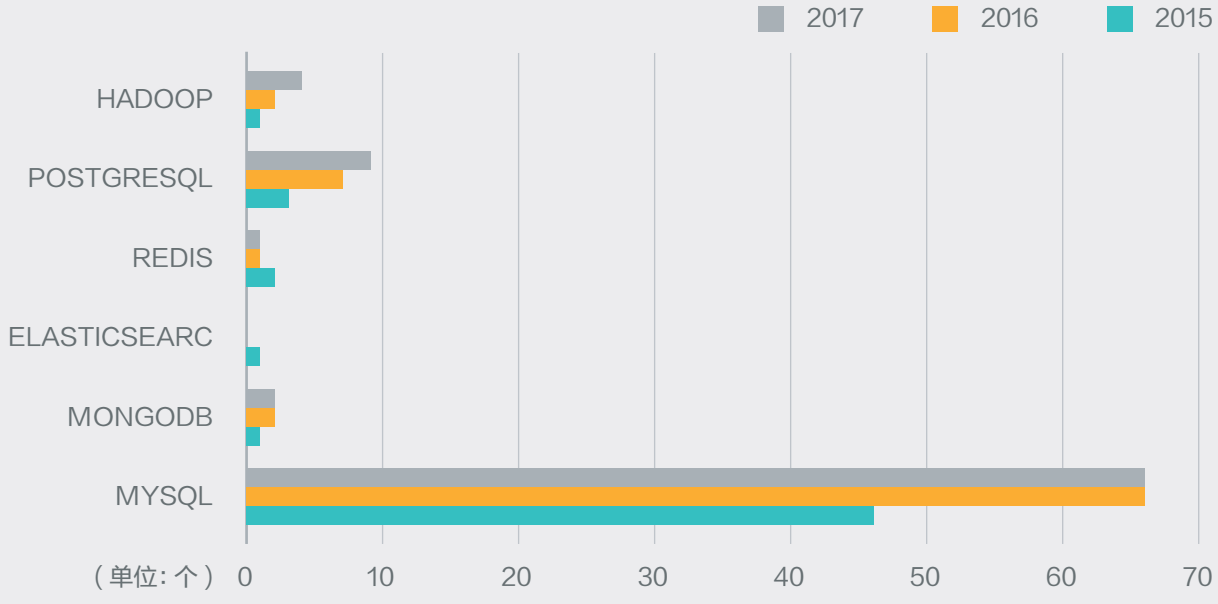

图 12 - 中危、高危漏洞统计

[9] “The 10 Biggest Data Breaches Of 2017”， CRN, 2017 年 12 月 .
[10] “An Offensive Defense: Lessons from the Equifax Breach”

数据库安全成为 2017 年的安全热点，我们针对勒索事件涉及到的数据库近三年来的中危、高危漏洞进行了统计。

其中 MySQL 的漏洞暴露最严重，从增速方面看，除了 MySQL，PostgreSQL 在过去三年里的漏洞也有较快的增长。相比之下，MongoDB、Elasticsearch、Redis、Hadoop 等数据库则相对安全，不过仍有一定程度的增长。从数据库漏洞的发展态势上看，数据库的安全问题也越来越受到关注。

4.2 内部人员数据倒卖

根据 Identity Theft Resource Center 和 CyberScout 发布的报告[11]，2017 年全年有多达 1500 起数据泄露事件发生，相比 2016 年发生的 1093 起增加 37%。 Loudhouse 曾发布的企业安全调查报告[12]也显示，如果价格到位，35% 的员工会倒卖包括公司专利、财务记录和客户信用卡等敏感数据。

2017 年 6 月，Verizon 证实有 600 万用户的数据被泄露，并表示此次数据泄漏是由该公司供应商的一名员工造成的，他因操作失误导致外部可进入云存储区域访问信息。同年，Verizon 发布数据泄露调查报告指出，已发生的数据泄露事件中，有 25% 是由内部人员造成的。因此，金融行业作为信息泄露高发的行业，应完善敏感信息保护措施，加强内部管理，建立必要的制度与控制机制。

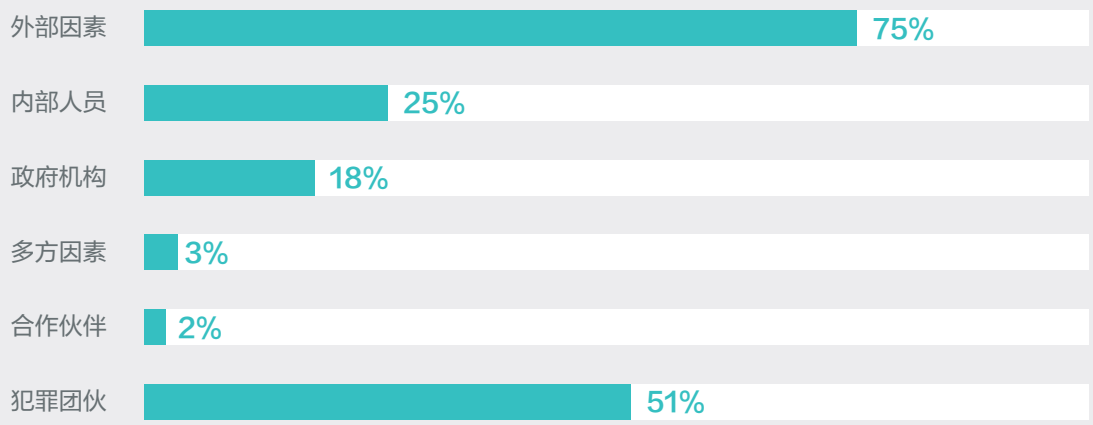

图 13 - 数据泄露成因[13]

[11] “At Mid-Year, U.S. Data Breaches Increase at Record Pace”， CyberScout, 2017 年 7 月 18 日 .
[12] “What's your employees' price?”, clearswift.
[13] “Mitigate the cyber risks with the Verizon 2017 Data Breach Investigations Report.”， Verizon.

4.3 云上数据窃取

2017 年中国私有云市场规模达预估已达 425 亿元左右，到 2020 年市场规模将达到 762.4 亿元[14]。而本次问卷调查显示，我国金融行业约 60% 的机构使用了云服务，大部分使用的是私有云，也有超过 20% 的机构使用公有云或者混合云。金融行业使用云业务最关注的安全风险是数据及隐私保护、业务的访问权限控制。

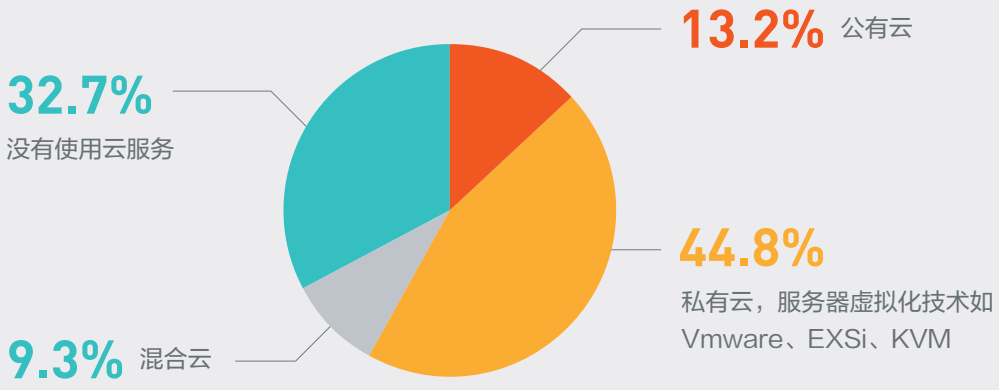

图 14 - 企业使用云计算服务比例

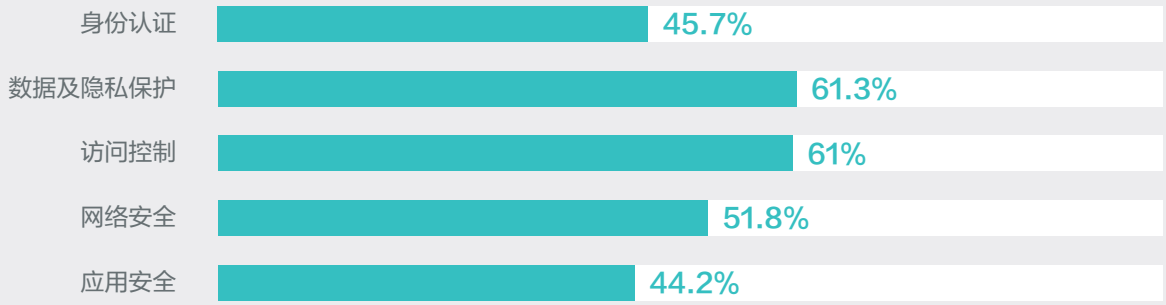

图 15 - 云计算服务安全风险点

个人数据及隐私安全不仅是企业自身的安全要求，也是国家监管机构越来越重视的方面。如欧盟颁布的《一般数据保护条例》，将于 2018 年 5 月 25 日起实施，要求加强对欧盟所有人的隐私权保护、物联网的隐私权保护，并简化数据保护的管理。而在国内，新颁布的《网络安全法》和正在制订的《个人信息保护法》也突出了国家对数据及隐私安全的重视。

[14]《2018-2024 年中国私有云行业运营态势及发展趋势研究报告》，智研咨询集团，2017 年 11 月 .

05 业务安全威胁介绍

业务安全威胁来源有很多，如使用不安全的函数或协议，集成了有缺陷的 SDK、Web 插件、服务器程序、或者业务流程上的逻辑缺陷等。

依据本次问卷收集数据统计，金融行业中，有 83.5% 的机构或企业都开展了互联网业务。在此次问卷调查中，企业机构对业务面临的互联网风险，最关注以下三个方面：

- 自身资产是否存在漏洞
- 自有资产开放高危端口与服务情况
- 是否存在信息泄露风险。

结合金融行业业务发展现状，业务安全威胁重点梳理了 Web 攻击、银行机构 ATM 与 SWIFT 攻击威胁、金融欺诈威胁、移动支付威胁、区块链安全威胁。

5.1 Web 攻击与代码缺陷

Web 攻击是常见的攻击类型。根据绿盟科技防护数据统计，73.6% 的网站遭遇过不同程度的 Web 类型的攻击，65.9% 的网站遭遇过利用特定程序漏洞进行的攻击。

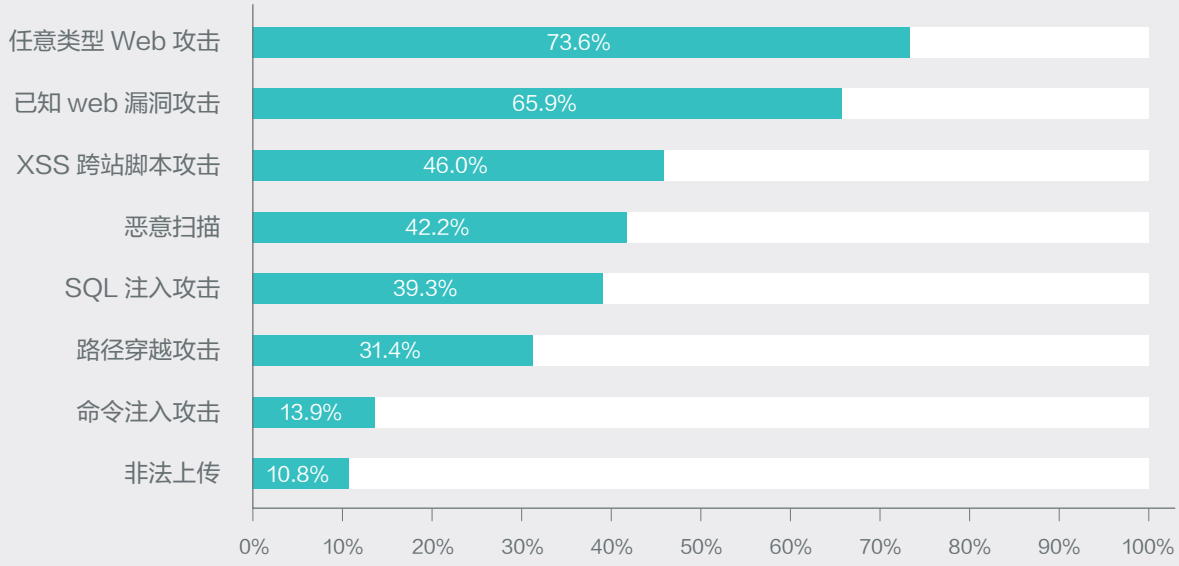

图 16 - 遭受 Web 应用攻击的站点占比

在金融行业中，针对 Web 服务器的攻击中，攻击次数最多的仍然是一些最常规的攻击手段，包括 SQL 注入、XPATH 注入、跨站、路径穿越、命令注入等，这部分攻击占比超过 60%。Web 攻击已经成为一个基本的攻击手段，也是各类攻击中相对容易实施的。此外针对特定的 Web 插件、服务器程序的攻击比例也相对较高，企业应该定期维护系统，升级相关的服务器应用。

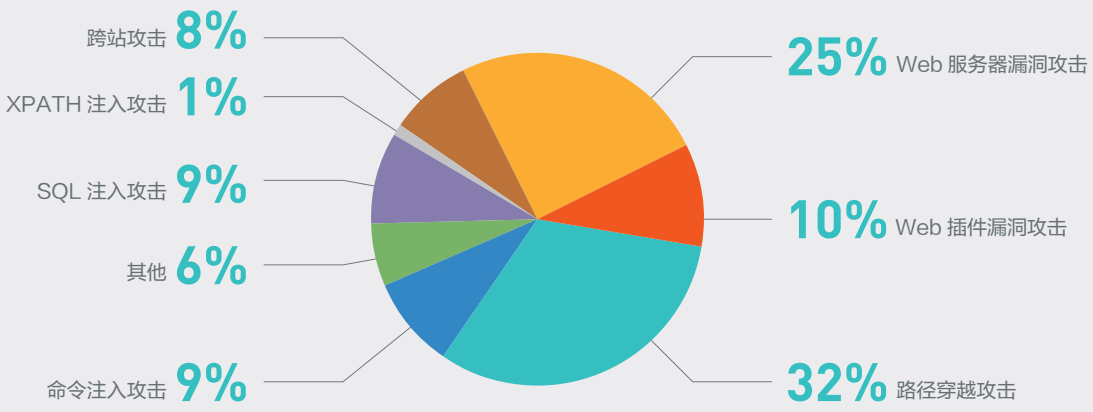

图 17 - Web 类攻击类型细分

从服务器类型上来看，在金融行业中 Nginx、IIS、Tomcat 服务器是遭受攻击最为频繁的资产类型，在使用这类服务器时应该仔细防护。

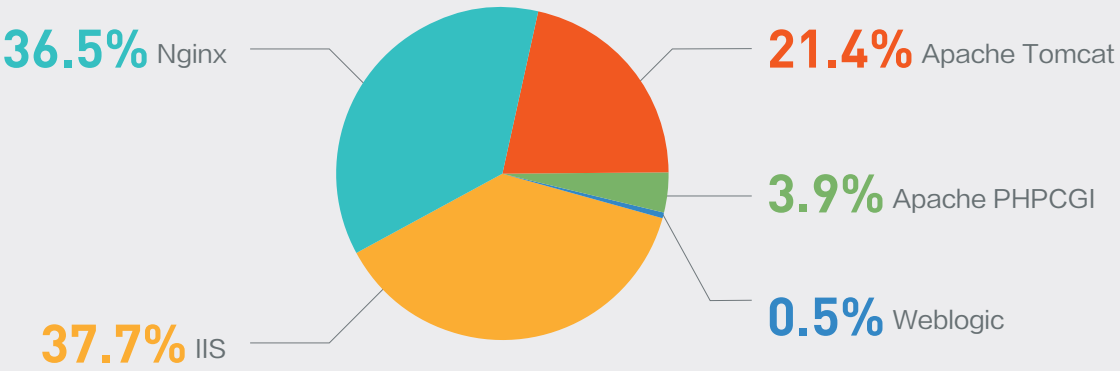

图 18 - 受攻击的 Web 服务器类型

从服务器系统应用程序的角度，针对金融行业的攻击中普遍利用的漏洞类型是关键信息泄露，这类漏洞通常是由于服务器软件配置上的错误造成，这些信息包括文件在服务器磁盘系统中的位置、系统版本号等。此外，文件类型过滤错误导致的文件执行也是经常出现的漏洞类型，这类攻击造成的危害更为严重，直接可以获取高权限 WebShell，为黑客提权控制创造了条件。

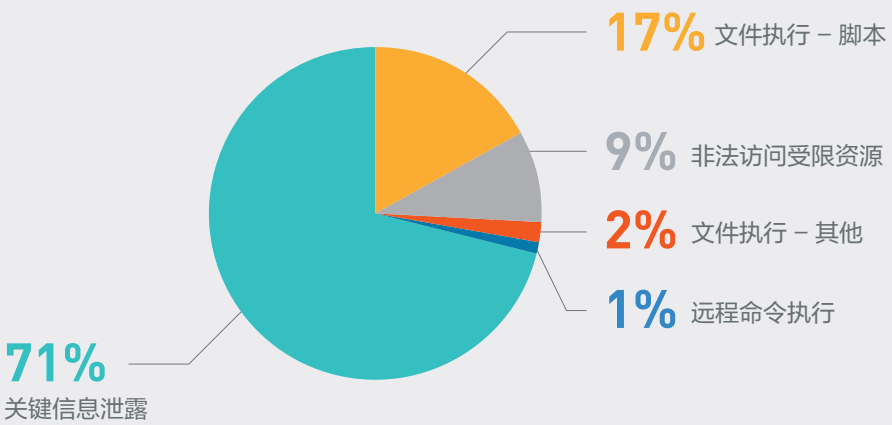

图 19 - Web 服务器最常被利用的漏洞类型分布

代码存在缺陷是 Web 攻击事件逐年增加的主因。参考 Fortify 官方的表述，根据代码缺陷形成的原因、被利用的可能性和表现出的安全问题等因素进行分析，将代码缺陷分为八类：

图 20 - 常见的代码缺陷分类

在金融行业的信息系统开发环节，仅有 32.9% 的机构采用 SDL 管理，而且调查显示，大部分安全管理工作集中在运维、上线、测试阶段，在需求、设计、编码阶段，对安全考虑十分欠缺。

5.2 业务欺诈

随着消费金融的快速发展，各类金融机构都面临着一个严峻的问题：欺诈。在《2017/18 年度全球反欺诈及风险报告》[15] 中，中国有 86% 的受访企业表示 2017 年曾遭受欺诈，较全球平均值的 84% 略高 2 个百分点。

《中国金融反欺诈技术应用报告》[16] 指出，2017 年第一季度，金融服务领域被拒绝的交易相较于 2016 年增长了 40%，相关僵尸攻击增长幅度为 180%；预计到 2020 年，在线支付欺诈将达 256 亿美元，而预计到 2019 年因数据泄露造成的经济损失在全球范围内将达到 2.1 万亿美元。金融欺诈涉及的业务环节多、手段多样、隐蔽性强，且金融欺诈移动化、组织化程度不断增加，新型金融科技公司愈渐成为欺诈者的目标。

[15] “Global Fraud & Risk Report”， Kroll.
[16]《中国金融反欺诈技术应用报告》，零壹智库，猛犸，2017 年 8 月 .

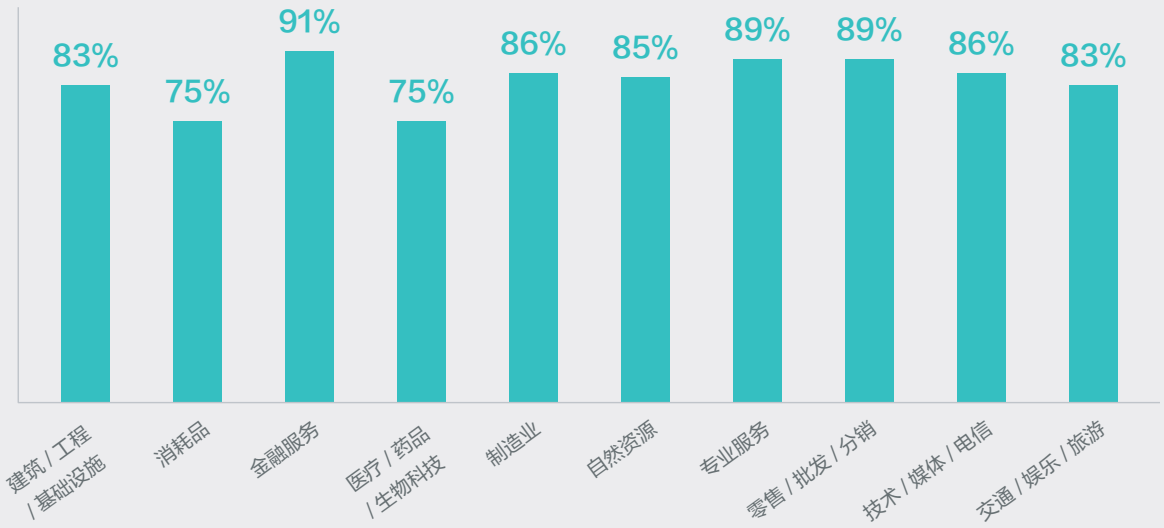

图 21 - 2017 年各行业发生欺诈事件比例 [17]

5.3 ATM 与 SWIFT 攻击

2017 年度，针对银行 ATM 设备的攻击方式有了新发展，利用红外插入式卡槽器展开网络攻击活动。据悉，插入式卡槽器是一款采用短距离红外通信技术的超薄微型设备，隐藏在 ATM 机卡槽内捕获信用卡数据并存储在嵌入式闪存中。虽然该设备构造简单，但主要通过天线将窃取的私人数据传输至隐藏在 ATM 机外部的微型摄像头中，进而收集信用卡或借记卡数据，之后极有可能被用于伪造信用卡或借记卡以便获取用户资金。

2017 年 10 月份，台湾远东银行 SWIFT 事件遭盗领 6000 万美元，警方介入追回大部分窃款，损失约 50 万美元。同期，尼泊尔 NIC 亚洲银行，在类似的 SWIFT 事件中损失约 500 万美元。而且，这并非银行机构首次遭受黑客攻击，充分说明银行业金融机构对于反复发生的此类安全事件没有足够重视，且没有有效的控制措施。信息安全管理不能只靠运气，建立健全的安全管理体系和有经验的安全团队才是降低风险的正确道路。

5.4 移动支付安全

在《2017 年移动支付用户调研报告》[18] 中：有 59.0% 用户担心移动支付安全问题。用户在使用生物识别技术进行移动支付和交易验证时，首要担心的问题是个人隐私泄露和相关安全隐患，占比分别为 77.1% 和 70.2%。

[17] 同脚注 15.
[18]《2017 年移动支付用户调研报告》，中国支付清算协会，2018 年 1 月 2 日 .

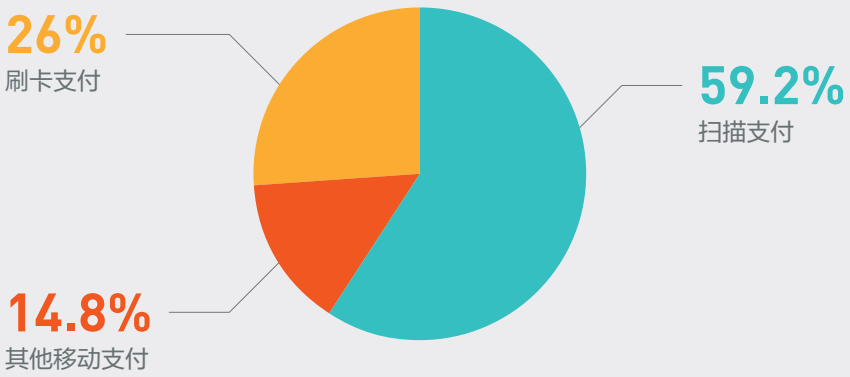

图 22 - 支付方式 [19]

根据《2017 移动互联网支付安全调查报告》[19]，移动支付安全存在的 5 大风险是：随意扫码；删除手机应用 APP 时不解除银行卡绑定；上网时如实填写各类支付信息；浏览有危险链接的短信或邮件；安装跳出来的不明文件。报告还指出，被调查者中，超过 6 成被访者在使用手机时，存在上述不安全行为，对个人信息或支付账号安全产生威胁。因此，作为移动支付的使用者，需要时刻提高警惕，防范各种支付风险。

5.5 区块链安全

区块链是一种分布式网络交易记账系统。它具有的开放性、全球性的特点，保证了交易活动可以在任何时间、任何地点进行，突破了传统贸易在时间和空间上的限制。因此被认为在金融、征信、物联网、经济贸易、结算、资产管理等众多领域都拥有广泛的应用前景。2017 年，随着国务院把区块链技术列入在“十三五”[20] 规划，中国的加密货币市场总值也增长了 30 倍。

在《Distributed Ledger Technology & Cybersecurity》报告中分析了区块链技术，同时也明示了它所带来的一些挑战：如密钥管理、隐私、智能合约等。报告指出，传统系统和区块链中使用的一些安全原则虽然是相同的，但是它仍然带来了新的挑战值得我们去关注，比如共识劫持和智能合约管理。

然而，在区块链不断得到研究、应用的同时，在技术层面和应用层面依旧存在一定的安全局限，在共识机制、私钥防盗等方面仍需提高安全意识和加强防范措施。2018 年 2 月，132 名投资者向日本加密交易所 Coincheck 提起诉讼，要求其赔偿 2.28 亿万日元（约 200 万美元）损失，原因是 Coincheck 在 1 月下旬曾遭受黑客重大攻击，导致价值超过 5.23 亿美元的 NEM 被盗。有投资者认为事件是 Coincheck 对“安全措施的忽视”造成的 。

[19] “中国银联发布 2017 移动支付安全调查分析报告”，2018 年 1 月 17 日 .
[20] “What’ s the future of blockchain in China?”， World Economic Forum, 2018 年 1 月 11 日 .

06 总结与展望

6.1 总结

金融科技是金融业务创新的一个模式，在这个模式中，通过科技的力量极大的改变和提升了金融业务在普惠性、便捷性、差异性、灵活性等方面的发展和建设程度。回顾人类的历史，科学技术通常带有创造和毁灭的两面性，对于金融业这样一个特殊的行业，必须时时保持对风险的警惕和防范控制。在 2017 年的“全国金融工作会议”上，习近平主席特别强调防控金融风险是当前的一项主要工作任务。因此在金融科技这样一个创新模式中，行业机构必须重视科技本身以及在其利用和使用过程中所携带的安全隐患。

本报告结合最新的案例和丰富的情报源，以金融科技所面临的网络安全威胁、数据安全威胁和业务安全威胁作为切入点，直观地分析了各类威胁的现状及趋势，在分析 DDoS、Web 类攻击和数据库漏洞利用等传统威胁的同时，更加着重对移动互联网、云计算、区块链等新技术所带来安全威胁进行分析。从分析中可见，金融科技要持续、健康地发展，安全问题必不可忽视，需要从安全意识教育、安全设备部署、安全服务引入、安全人才储备、安全预算投入等方面提升整体安全能力。

6.2 展望

按照 2017 年“全国金融工作会议“的要求，一切金融业务都要纳入监管，因此金融机构在发展和应用金融科技的同时必须严格遵循和满足国家监管要求，不能一味追求创新。金融科技的风险如报告分析所示，包括了诸多方面，既有传统网络安全威胁也有新型网络安全威胁。综合考虑这些风险的危害范围、危害程度以及金融机构的应对防护现状，我们认为针对金融科技风险，金融机构需要在未来关注以下六个方面：

- **新的监管合规要求**

  重视自身风险管控能力与风险之间的匹配和差距程度。

- **内部的安全培训**

  提高内部人员安全意识，加强开发安全标准、安全部署与管理等方面的意识和技能培养。

- **新技术应用风险**

  应对物联网、区块链、移动支付等潜在安全风险。

- **开发安全管控**

  系统地识别和消除各个阶段可能出现的由于人员知识和技能、开发环境、业务逻辑等所造成的信息安全风险。

- **高风险网络攻击**

  应对 DDoS 攻击、Web 攻击、有组织的 APT 攻击、欺诈与勒索等潜在安全威胁。

- **数据安全**

  一方面要切实遵循国内外数据及隐私安全监管条例，另一方面加强企业数据保护及防范数据倒卖风险的能力。

如需获取更多信息或解决方案，请关注：