2017 上半年
网络安全观察

绿盟科技威胁情报中心

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，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。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易。

股票简称：绿盟科技　股票代码：300369

目录

01.

执行摘要

执行摘要

安全事件已经成为新闻头版的常客。今年以来，连续爆发WannaCry，Petya，NotPetya等重大网络安全事件，各种社会经济活动、IT和安全团队都备经战火洗礼。值得关注的是，分析师们开始把网络攻击事件和严重级别的飓风相提并论，全球造成的经济损失可能高达500多亿美元。在各种新技术快速演化、威胁环境快速演化的大背景下，不断重新审视网络安全业界的各种实践、技术和系统组态、生态环境等无疑是非常有意义、有必要的。

万物互联之下，已经没有可以独善其身的安全孤岛，只有相对安全和不安全的各种子生态。防御方可以接受某种程度上的渗透和泄露，只需要把风险控制于可接受水平之下，避免出现破窗效应，否则任何安全措施的效果都会大打折扣，进入“死环”。防御方必须利用各种因素使己方的漏洞、漏洞的利用、被利用后的踪迹处于可视、收敛和受控状态，如此防御方处于“生环”状态，安全态势逐渐向好的方向发展。信任体系、安全策略和实践、产品设计都应该评估并考虑目标系统所处的生态的安全水平。而威胁情报，就像名字所传递的意味，可以帮助管理层和运营团队判断所处态势、掌握威胁方动向、动态调整策略、架构、行动计划等。

IP地址是互联网的基石信息，恶意IP是指该IP地址被监控发现和某些恶意行为有关，例如拒绝服务攻击、入侵、扫描、发送垃圾邮件等等。这些IP地址往往是某些僵尸网络和犯罪团伙的成员。数万、数十万IP节点构成的大型“僵尸网络”不仅仅对大部分互联网业务具备摧毁性的破坏力量，并且可以完成各种复杂的协同性攻击入侵行为。在人工智能和机器学习的语境下，攻防双方将会展开新层面的情报和反情报、欺骗和反欺骗的对抗。掌握互联网范围的恶意IP的分布、演化、动态特点对于关键基础设施和大型组织的安全防护非常重要。

绿盟科技威胁情报中心[1]的监测数据表明，全球60%的恶意IP集中在GDP排名前十的国家中，其中以美国、中国、印度、日本为恶意IP占比最高的四个国家；另一方面，恶意IP地址占比（即恶意IP数和该国家总IP地址数的比例）和国家人均GDP展现出相当明显的线性关系，也即发达国家的互联网环境比发展中国家更为安全。和犯罪率类似，恶意IP率将会成为一个国家、地区、运营商重要的治理和运营指标。

[1] 绿盟科技威胁情报中心 https://nti.nsfocus.com/

Gartner在其今年的华盛顿安全峰会上分享的数据表明，今年来每年新出现的恶意软件已经达到令人惊讶的三亿多个，但这么多恶意软件所利用的漏洞却集中在几十个上面。我们上半年的监控数据表明，TOP10漏洞的利用占到了检测到的所有漏洞利用次数的50.8%。而WannaCry、Petya、NotPetya勒索事件三连发使得方程式漏洞利用的次数呈现爆发态势。

Struts2依靠连续5个漏洞成为今年上半年的一个焦点。在S2-045爆发的一周内，绿盟科技威胁情报中心监测到19,396次针对该漏洞的攻击尝试。针对Struts2利用的攻击次数超过所有框架及应用漏洞攻击总次数的80%。当有关键业务运行于Struts2框架之上时，24x7的漏洞监视、小时级的通报响应机制变得尤其重要。

反射放大型攻击依然占据了拒绝服务攻击类型的主流位置。 反射放大器成为网络生态中的不定时“炸弹”，成为攻击者手中低成本、低风险的强大火力。 本文呼吁，基础设施运营商和监管治理执法机构有必要以治理垃圾邮件的力度来治理反射放大器。

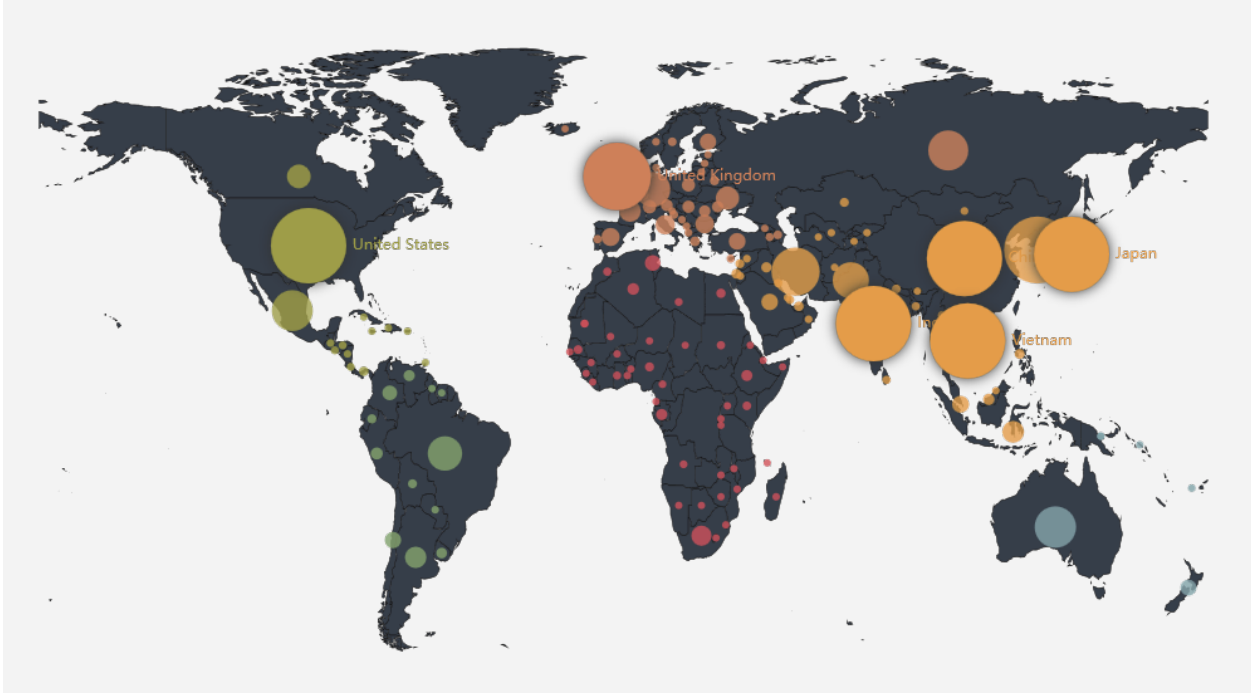
勒索软件成本低、收效快、ARPU值高、风险小的特点使其在黑产中增长迅猛，而勒索软件的持续爆发又似乎是比特币价格上涨的战鼓，一年内，比特币的价格从650美元飙升到2654美元。值得关注的是，勒索者展现出灵活的“商业”应变能力，按照文件数量、受害者所在地区的消费水平，提供不同层次的“价格套餐”，并且有详细的指引步骤，对受害者十分“友好”。随着物联网、智能汽车、智能家居、智慧城市等的快速推进，勒索软件及其各种不同形式，例如DDoS勒索、数据库勒索等，将会持续成为安全团队的攻防焦点，以及媒体的曝光焦点。

知己知彼百战不殆，已经成为全球网络安全产业界的新座右铭。威胁情报也成为安全防护各个环节中不可或缺的基础性能力。

02.

攻击源概览

图 2-1 攻击源国家地区分布图



数据来源：绿盟科技威胁情报中心（NTI）

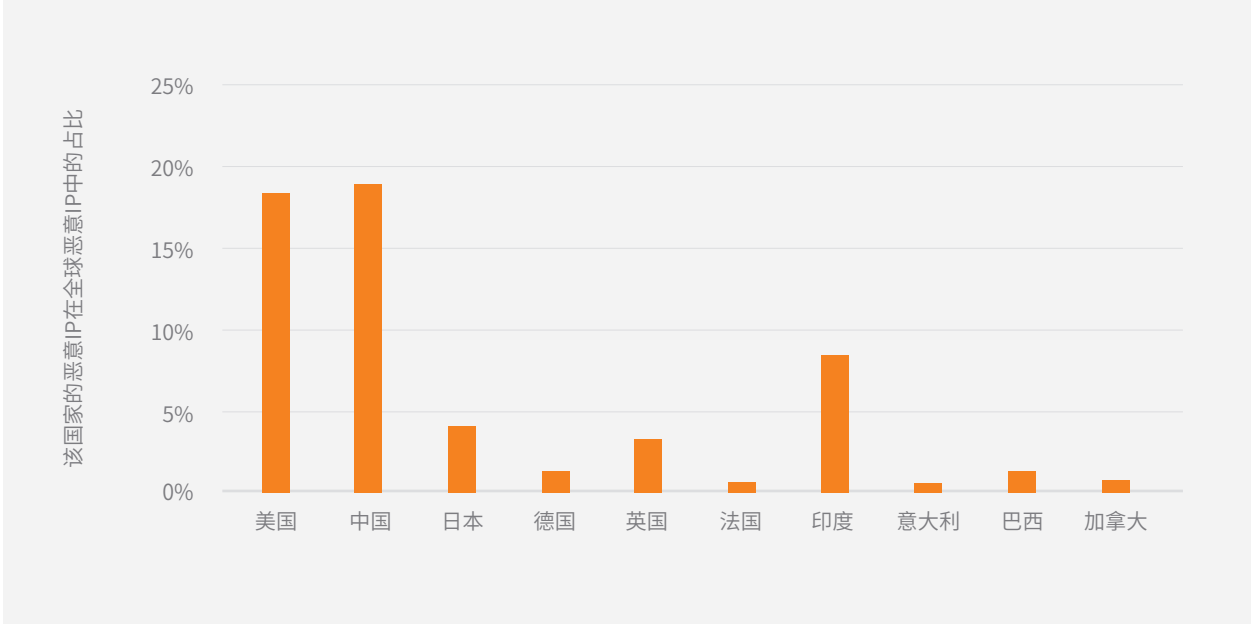
2017年上半年，绿盟科技威胁情报中心监控的数据显示，全球60%的恶意IP集中在GDP排名前十的国家中，其中以美国、中国、印度、日本为恶意IP占比最高的四个国家。

表 2-1 恶意IP在GDP排名前10的国家分布

国家	GDP排名	在所有恶意IP中的占比
美国	1	18.52%
中国	2	19.20%
日本	3	4.18%
德国	4	1.57%
英国	5	3.40%
法国	6	0.80%
印度	7	8.53%
意大利	8	0.69%
巴西	9	1.52%
加拿大	10	0.92%

数据来源：绿盟科技威胁情报中心（NTI）

图 2-2 恶意IP在GDP排名前十国家中的分布



数据来源：绿盟科技威胁情报中心（NTI）

03.

漏洞观察

在网络安全领域，漏洞发现和利用始终是安全团队至关重要的研究方向，绿盟科技威胁情报中心对各大厂商和流行的开源产品漏洞情况进行了密切监控和分析，发现如下：

1. 近年来，每年新公开的漏洞数量均呈上升趋势；仅2017年上半年，新公开的漏洞总数已达4144个。从增速来看，权限、特权与访问控制类漏洞（CWE-264）逐年上升，尤其在2016年以后，该类型的漏洞增长更为快速。从漏洞风险等级分类来看，高危漏洞的占比下降，中危漏洞占比上升。从危害来看，缓冲区溢出类漏洞（CWE-119）从2015年开始，增速加快，此种类型的漏洞由于能够造成拒绝服务、代码远程执行等攻击效果，会对业务系统产生很大的危害，因此备受攻击者青睐。

2. 2017年上半年，漏洞总体数量明显高于往年同期水平，与去年同期相比，增长率高达50%，尤其是中危漏洞的数量增长最为快速。上半年中，权限、特权与访问控制类漏洞（CWE-264）数量最多，增速也最快。

3. 2017年上半年，热度最高、最值得关注的漏洞为：

   1）Struts2依靠连续5个漏洞（S2-045—S2-049）成为今年上半年的一个焦点。在S2-045爆发的一周内，绿盟科技威胁情报中心监测到19,396次针对该漏洞的攻击尝试。

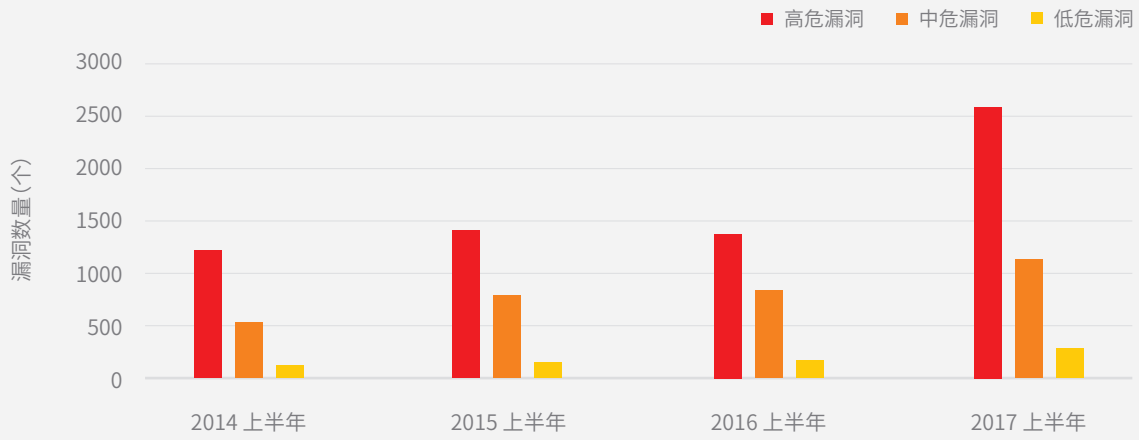
   2）Windows SMB 远程代码执行漏洞（MS17-010）因方程式组织的利用而成为今年上半年的另一个焦点，5月席卷全球的WannaCry勒索软件利用此漏洞进行大量传播。

4. 虽然每年被公开的漏洞数量众多，但被大规模利用的漏洞其实非常有限，且很多被利用的漏洞已有官方补丁，说明机构和个人及时更新官方补丁的安全意识还有待提高。

3.1 漏洞发展趋势

近三年来，每年新公开的漏洞数量均呈上升趋势。2017年上半年新公开漏洞数量大幅度上升，与2016年同期相比，增长率高达50%。2017年1-6月，新公开漏洞总数达到4144个，其中高危漏洞2561个，中危漏洞1254个，低危漏洞329个。从总数上看，涨幅最大的是中危漏洞，从比例上来看，高危漏洞的占比下降，中危漏洞占比上升。

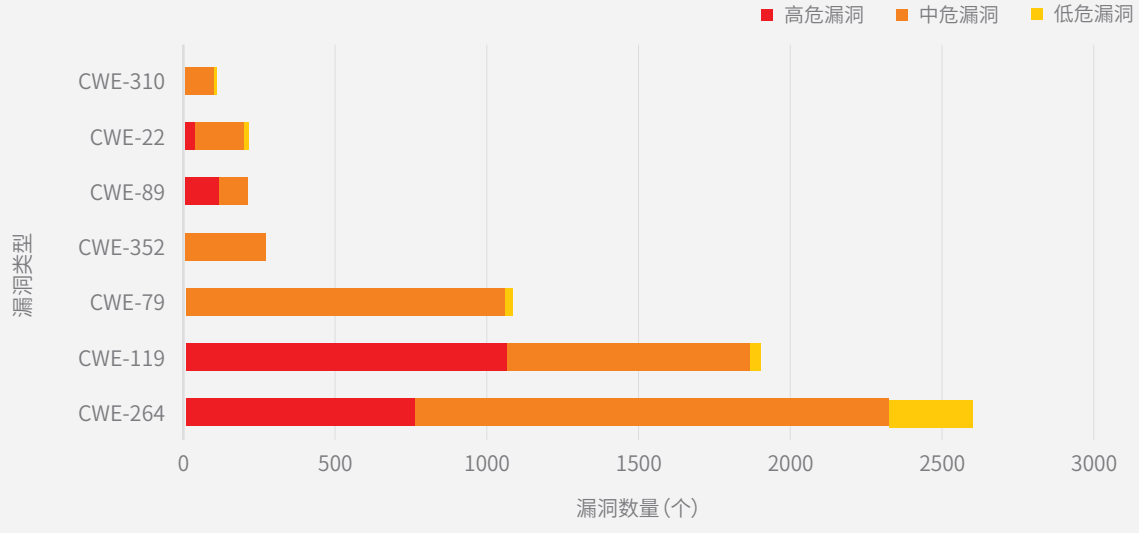
图 3-1 2014 ~ 2017 同期漏洞数量变化趋势



数据来源：绿盟科技威胁情报中心（NTI）

2017年上半年，从总体数量来看，权限、特权与访问控制类漏洞（CWE-264）数量最多，主要以中、高危漏洞组成。其次是缓冲区溢出类漏洞（CWE-119），该部分漏洞中，高危漏洞占比超过55.7%。此外XSS漏洞（CWE-79）、CSRF漏洞（CWE-352）、SQL注入漏洞（CWE-89）、路径遍历漏洞（CWE-22）、密码学安全问题（CWE-310）也是今年漏洞数量最为集中的类别。

图 3-2 热门漏洞类型及漏洞数量分布

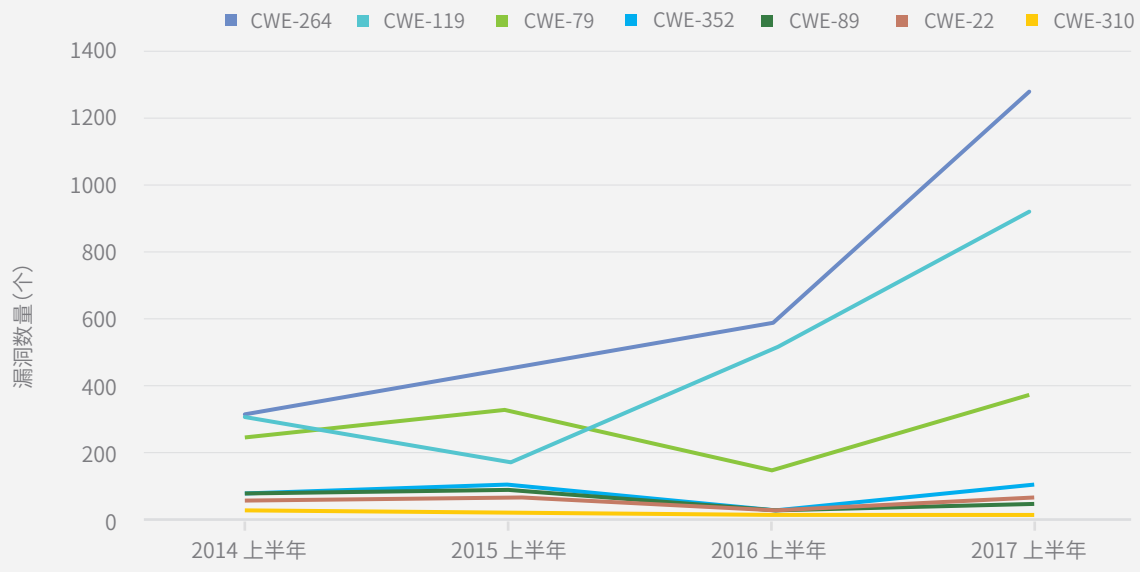


数据来源：绿盟科技威胁情报中心（NTI）

近年来，数量增长TOP3的漏洞类型为：权限、特权与访问控制类漏洞（CWE-264）、缓冲区溢出漏洞(CWE-119)和跨站脚本漏洞（CWE-79），其他类型的漏洞数量增速不大。

权限、特权与访问控制类漏洞（CWE-264）增速最快，尤其是2016年之后，数量显著增长。缓冲区溢出漏洞(CWE-119)从2015年开始，增速也开始加快，此种类型的漏洞由于能够造成拒绝服务、代码远程执行等攻击效果，会对业务系统产生很大的危害，因此也备受攻击者青睐。

图 3-3 2014 ~ 2017 各大类型漏洞数量变化趋势



数据来源：绿盟科技威胁情报中心（NTI）

漏洞分类简介：

表 3-1 CWE漏洞分类中英文名称对照[2]

漏洞分类ID	漏洞分类（中文）	漏洞分类（英文）
CWE - 264	权限、特权与访问控制	Permissions, Privileges, and Access Control
CWE - 119	缓冲区溢出（内存缓冲区边界内操作的限制不恰当）	Buffer Errors
CWE - 79	跨站脚本	Cross-Site Scripting (XSS)
CWE - 89	SQL注入	SQL Injection
CWE -352	跨站请求伪造	Cross-Site Request Forgery (CSRF)
CWE - 22	路径遍历	Path Traversal
CWE -310	密码学安全问题	Cryptographic Issues

[2] CWE是一种对漏洞类型的标准描述，相关介绍请参考http://cwe.mitre.org/、https://nvd.nist.gov/vuln/categories、http://wiki.scap.org.cn/cwe/cn/

3.2 漏洞攻击及利用

从监控数据中发现，很多公布时间较早的漏洞仍然活跃，最早的漏洞甚至可以追溯到2002年（CVE-2002-0649）。大部分的漏洞利用集中在少数几个知名且影响度较高的漏洞上。Gartner在其今年的华盛顿安全峰会[3]上分享的数据表明，尽管每年新出现的恶意软件已经达到令人惊讶的三亿多个，但这些恶意软件所利用的漏洞却集中在几十个上面。这和我们监控到的数据是一致的。该情况表明，机构和个人用户在漏洞修补中应该采取一定的优先措施，及时修补那些高危且容易被攻击和利用的漏洞。

表 3-2 监控中TOP10漏洞利用及攻击占比

漏洞名称和编号	漏洞利用占比
Microsoft Windows ASP.NET拒绝服务攻击(CVE-2009-1536)	12.10%
Microsoft SQL Server 2000 Resolution服务远程堆破坏拒绝服务攻击（CVE-2002-0649）	8.80%
Microsoft Network Policy Server RADIUS拒绝服务漏洞(CVE-2016-0050)(MS16-021)	8.30%
Microsoft Internet Explorer ASLR安全限制绕过漏洞(CVE-2015-0051)(MS15-009)	3.80%
OpenSSl SSLv2弱加密通信方式易受DROWN攻击(CVE-2016-0800)	3.50%
Apache Struts远程命令执行漏洞（s2-008）	3.40%
Microsoft mshtml.dll库GIF图象处理远程拒绝服务漏洞（MS04-025）	3.00%
Struts2远程命令执行漏洞(s2-045)(s2-046)(CVE-2017-5638)	2.70%
Squid Proxy DNS域名解析器远程拒绝服务漏洞(CVE-2005-0446)	2.70%
GNU Bash 环境变量远程命令执行漏洞(CVE-2014-6271)	2.50%

数据来源：绿盟科技威胁情报中心（NTI）

3.3 热点漏洞监控

今年4月，Shadow Brokers 组织公布了此前窃取的部分方程式组织（Equation Group）的机密文件。这部分被公开的文件曾经被Shadow Brokers组织以数亿美金拍卖，因为这部分文件包含了数个令人震撼的黑客工具，用来攻击包括 Windows 在内的多个系统漏洞。此次泄漏的文件包括三部分： Windows，Swift 以及 Odd。其中 Windows 目录下的黑客工具包含了IIS 6.0 远程漏洞的利用；SMB1的重量级利用，可以用来攻击开放了445端口的Windows系统并且提权；RDP服务远程漏洞的利用，可以攻击开放了3389端口的Windows机器等等。开放了135，445，3389等端口的Windows服务器有很大概率受到攻击。上半年曝光的漏洞相关信息以及影响的产品如下表：

表 3-3 方程式组织（Equation Group）泄露的漏洞利用[4]

漏洞编号	漏洞来源	影响产品
CVE-2017-3881	Vault 7	Cisco Cluster Management Protocol
CVE-2017-0143	ETERNALBLUE	SMBV1 Server
CVE-2017-0144	ETERNALBLUE	SMBV1 Server
CVE-2017-0145	ETERNALBLUE	SMBV1 Server

[3] LawsonCraig. (2017). To the Point:Doing the Simple Things Well Means the Hard. Garner安全峰会, (页 11-15).

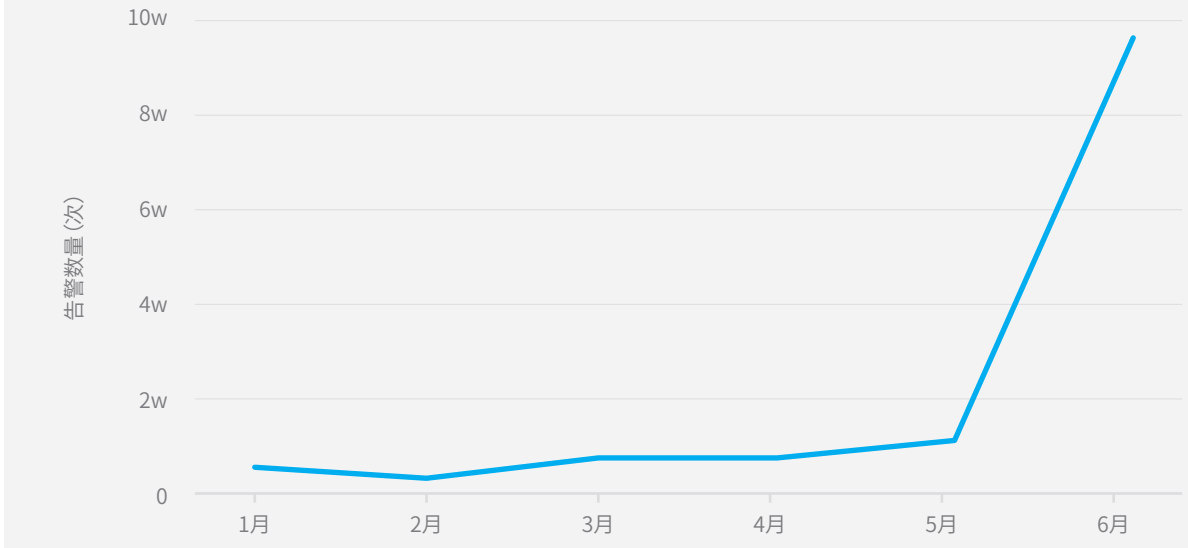
表 3-3续 方程式组织（Equation Group）泄露的漏洞利用[4]

漏洞编号	漏洞来源	影响产品
CVE-2017-0146	ETERNALBLUE	SMBV1 Server
CVE-2017-0147	ETERNALBLUE	SMBV1 Server
CVE-2017-0148	ETERNALBLUE	SMBV1 Server
CVE-2017-8487	ENGLISHMANSDENTIST	OLE
CVE-2017-0176	ESTEEMAUDIT	RDP
CVE-2017-7269	EXPLODINGCAN	IIS6.0

数据来源：绿盟科技威胁情报中心（NTI）

从绿盟科技威胁情报中心监测到的攻击情况来看，5-6月利用方程式漏洞进行的攻击次数呈现爆发态势，我们认为这与WannaCry和NotPetya勒索蠕虫的传播有着直接的关系。

图 3-4 方程式组织（Equation Group）泄露的相关漏洞告警



数据来源：绿盟科技威胁情报中心（NTI）

[4] 备注：ETERNALBLUE、ENGLISHMANSDENTIST、ESTEEMAUDIT、EXPLODINGCAN是方程式组织（Equation Group）开发的工具包名称。

04.

网站安全观察

从绿盟科技对网站安全的的防护监测中，我们得出下述四个关键发现：

- 网站攻击非常活跃
- SQL注入仍是最常见的攻击手段
- Web服务器中，针对老旧漏洞的攻击占据80%以上的攻击次数
- Struts2代码执行漏洞仍居Web框架和应用的漏洞首位

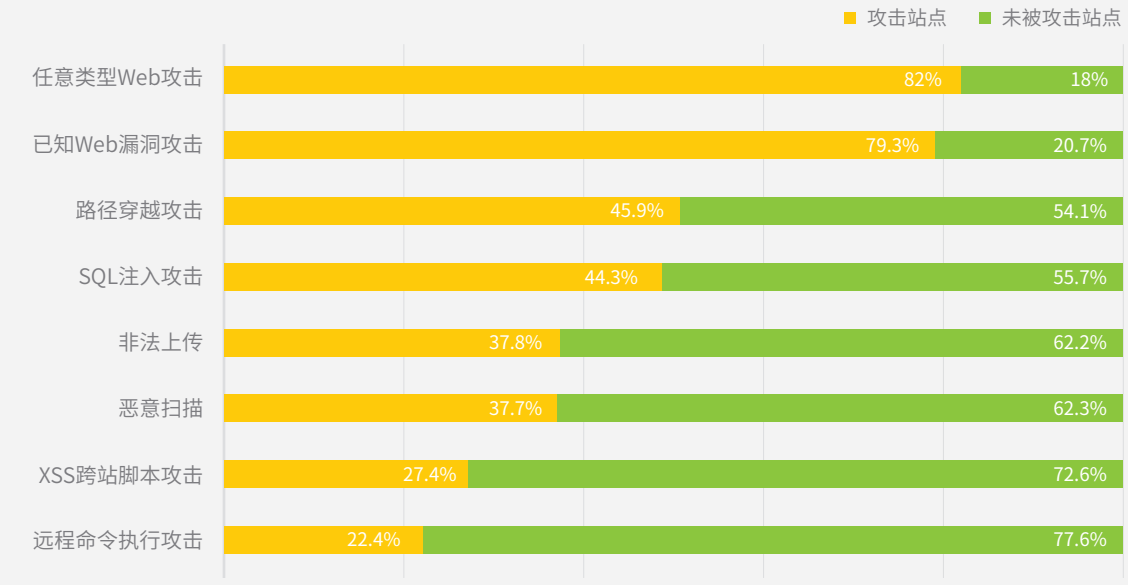
这些关键发现的具体内容如下：

4.1 网站攻击分布

从2017年上半年网站安全态势的监控数据来看，针对网站的攻击是非常活跃的。主要的攻击手段包括SQL注入、已知漏洞利用、路径穿越、跨站脚本、非法上传、远程命令执行等。

从监控的网站分布来看，82%的网站都遭遇过不同程度的网络攻击，79.3%的网站遭遇过针对已知的Web漏洞的攻击，45.9%和44.3%的网站分别遭遇过路径穿越攻击和SQL注入攻击。具体分布见图 4-1：

图 4-1 2017年上半年网站受攻击情况分布图



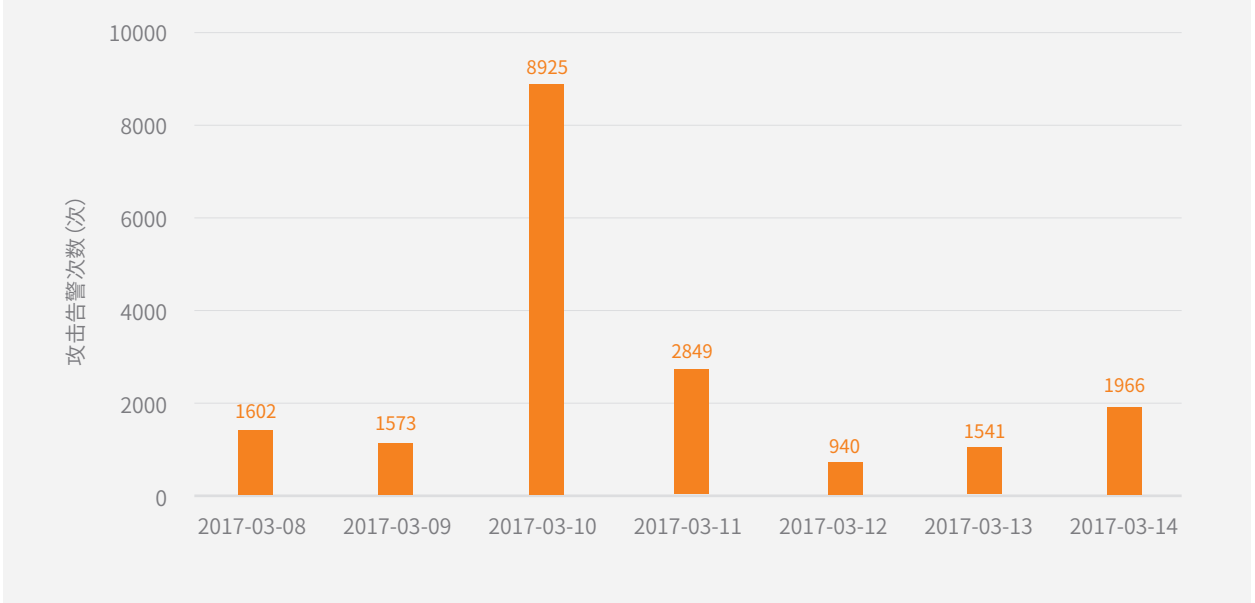
数据来源：绿盟科技可管理安全服务（MSS）

我们发现，攻击者的攻击集中在几个最常用的漏洞和探测方式上，这个现象与Web攻击本身的特点有密切关系。一方面Web攻击的难度和成本较低，另一方面基础的攻击手法和漏洞利用已经固化和集成到一些流行的攻击工具中，例如中国菜刀、sqlmap等，上述因素使得Web攻击入侵尝试变得非常容易。

网站Web服务对于攻击者来说是很重要的攻击目标，提供网站服务的主机，需要架设基础的Web服务系统组件，并且往往有一套运行在这个服务之上的各类Web应用程序，复杂的软件架构极易导致出现各种漏洞。同时，网站间技术同质化程度很高，导致每一种攻击手段都会批量地影响全球的网站服务。对于新增的漏洞，网络上的脚本小子们会第一时间通过Google等搜索引擎进行批量的匹配和尝试，在很短的时间内就可以获取到数量可观的webshell，加之现在有了类似Shodan这类开放的全网扫描引擎，攻击者针对Web服务漏洞可以更快地展开针对的攻击行动。

以最流行的Java Web服务器框架之一Apache Struts2为例，短短半年时间就曝出5个漏洞（S2-045—S2-049），影响了Struts2.3到Struts2.5的广大版本。其中以3月份爆发的S2-045（CVE-2017-5638）最为严重。在这个漏洞中Apache Struts2的Jakarta Multipart parser插件存在远程代码执行漏洞，攻击者可以在使用该插件上传文件时，修改HTTP请求头中的 Content-Type 值来触发该漏洞，导致远程执行代码。从该漏洞爆发时的监控数据来看，全球范围部署有大量的包含该漏洞的Web站点，其中以美国、中国、日本、欧洲等经济发达地区最为普遍。根据受监控网站的数据（见图4-2），在漏洞发布的一周内共发生19,396次针对该漏洞的攻击尝试，平均每天2,771次，其中以3月10日为攻击高发期，共发生8,925次。我们甚至发现，有攻击者利用S2-045漏洞进行勒索，获益可能超过84BTC ($100,000)。

图 4-2 Struts2（S2-045）爆发一周内受监控网站遭受攻击情况

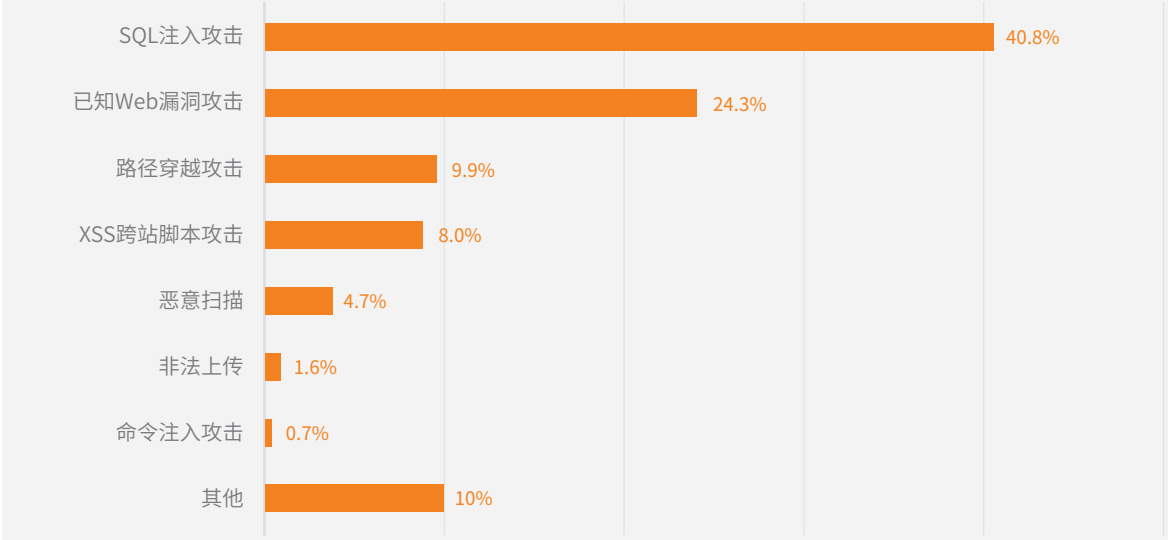


数据来源：绿盟科技可管理安全服务（MSS）

4.2 Web攻击类型分布

从攻击类型来看，SQL注入仍然是最常见的攻击手段，占总攻击量的40.8%。SQL注入攻击虽然历史悠久，但仍然是最常用也是最容易的攻击手段。

图 4-3 2017年上半年Web攻击类型分布情况



数据来源：绿盟科技可管理安全服务（MSS）

4.3 Web漏洞利用情况

从漏洞利用的角度看，在各种扫描和利用尝试中占比高的还是很早前公布的老旧漏洞，其中利用占比Top10的漏洞就占了总攻击的60%以上。该情况再次印证了前述我们提到的需要建立漏洞补丁修补优先级别的重要性。

表 4-1 被攻击的web服务器漏洞TOP10

漏洞名称	发布时间	攻击比例
Tomcat目录遍历漏洞（CVE-2008-2938）	2008 年	21.70%
IIS文件上传漏洞（CVE-2009-4445,CVE-2009-4444）	2009 年	13.90%
lighttpd 源代码暴露漏洞(CVE-2006-0814)	2006 年	6.00%
nginx 文件遍历漏洞（CVE-2009-3898)	2009 年	5.40%
IIS CGI程序名解析错误导致文件执行漏洞（CVE-2000-0886）	2000 年	5.40%
IIS文件扩展名解析错误导致ASP代码泄露(CVE-1999-0253)	1999 年	2.60%

表 4-1续 被攻击的web服务器漏洞TOP10

漏洞名称	发布时间	攻击比例
Tomcat目录遍历漏洞（CVE-2008-5515）	2008 年	2.40%
Apache头部数据长度异常导致服务器资源耗尽(CVE-2011-3192)	2011 年	2.10%
IIS脚本文件名解析漏洞（CVE-2009-4444）	2009 年	1.80%
IIS中Unicode字符解码错误导致远程命令执行（CVE-2000-0884）	2000 年	1.50%

数据来源：绿盟科技可管理安全服务（MSS）

在针对Web框架或者应用的漏洞中，Struts2代码执行漏洞的利用仍然高居漏洞榜首，占据超过所有框架及应用漏洞攻击次数的80%，这些漏洞包括：

漏洞名称	发布时间	攻击比例
Struts2远程命令执行(CVE-2013-1966)	2013 年	48.70%
Struts2远程命令执行(CVE-2013-2251)	2013 年	26.90%
Struts2 Jakata插件远程命令执行(CVE-2017-5638)	2017 年	5.90%
Struts2 ClassLoader操作漏洞(CVE-2014-0094)	2014 年	2.90%
Struts2恶意Ognl表达式导致远程代码执行（CVE-2016-3081）	2016 年	2.70%
Struts2 REST插件远程代码执行漏洞（CVE-2016-4438）	2016 年	2.40%

数据来源：绿盟科技可管理安全服务（MSS）

此外，下面几个漏洞也是利用率较高的网站应用漏洞：

漏洞名称	发布时间	攻击比例
ElasticSearch 沙盒绕过导致远程代码执行(CVE-2015-1427)	2015 年	2.70%
PHPCMS2008 pagesize参数校验不严导致命令注入	2011 年	2.00%
ThinkPHP lite模式下任意代码执行漏洞	2013 年	1.20%
DedeCMS 5.7版本SQL注入漏洞	2013 年	0.60%
Phpcms V9.1.9及以下版本的plugin.php对传入的id参数检查不严密造成本地文件包含漏洞	2013 年	0.20%
PHPCMS V9版本任意文件读取漏洞	2012 年	0.10%

数据来源：绿盟科技可管理安全服务（MSS）

05.

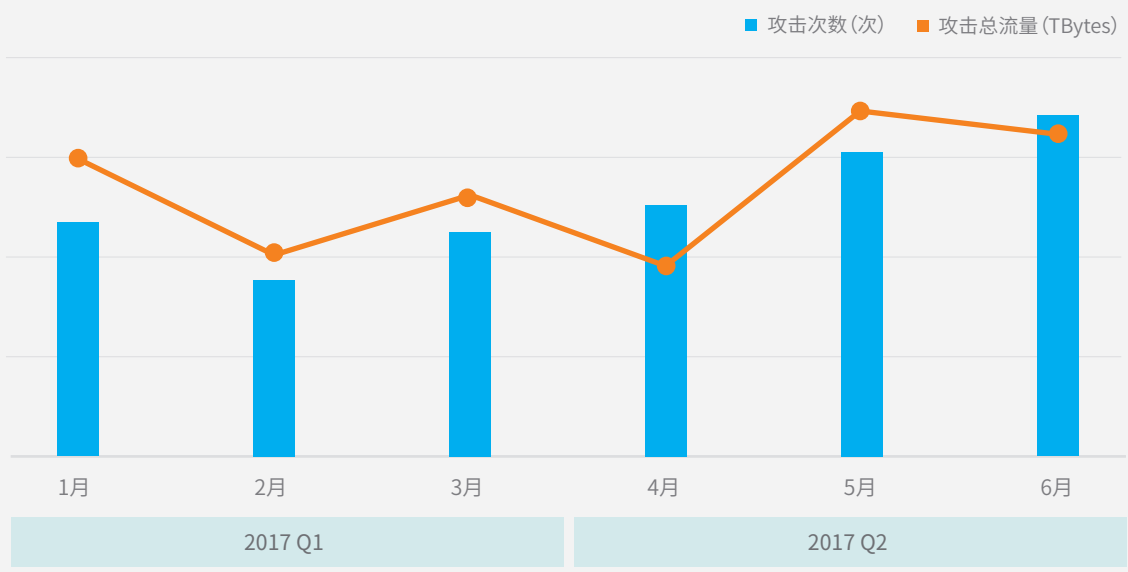
DDoS观察

5.1 DDoS攻击总次数和攻击总流量

2017年上半年，我们监控到DDoS攻击约10万次，相比2016年下半年下降30%；攻击总流量约1.6万TBytes，相比2016年下半年下降38.4%，我们认为，这与今年年初开始反射攻击活动减少有关。

2017上半年相比2016年整体攻击趋势放缓，2017 Q2季度有回升的趋势。Q2季度环比Q1季度总攻击次数增长39.3%，总流量增长10.3%。这符合以往的“年初DDoS攻击放缓，年中攻击活跃”的趋势。

图 5-1 各月份攻击次数和流量图



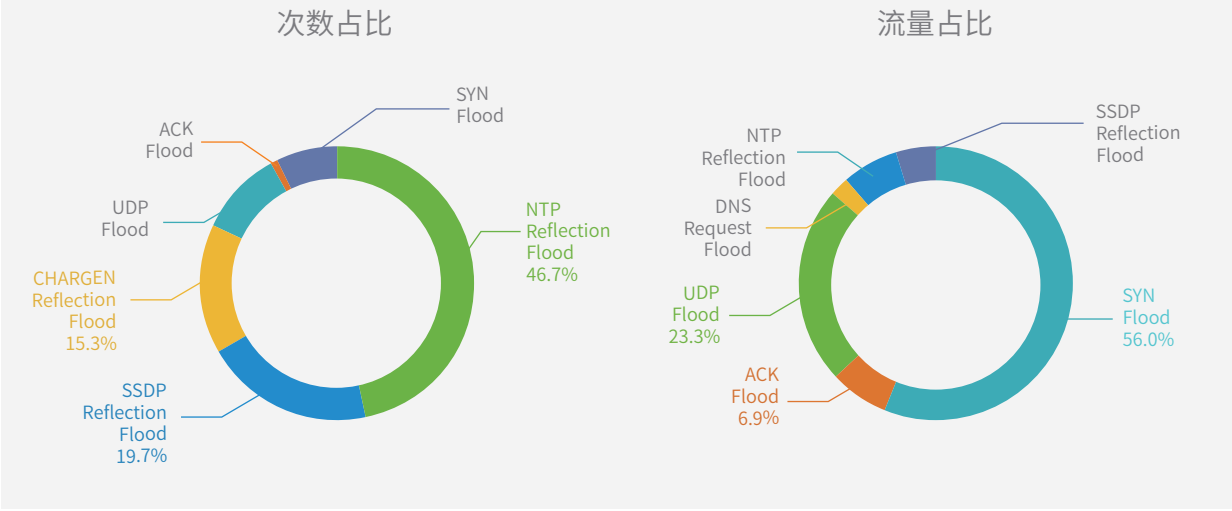
数据来源：绿盟科技全球DDoS态势感知系统（ATM）

5.2 DDoS各攻击类型次数和流量占比

2017上半年，Top 3（按攻击次数统计）DDoS攻击类型分别为NTP Reflection Flood、SSDP Reflection Flood和CHARGEN Reflection Flood，均为反射类型，Top 3合计占比达 81.7%。但反射攻击整体活动有所放缓，详见报告具体分析。

从各类攻击流量大小占比来看，SYN Flood和UDP Flood依然是流量最大的两种攻击类型，SYN Flood流量占比达56%，UDP Flood流量占比为23.3%。与2016年相比，SYN Flood流量占比明显增多，上升7个百分点，UDP Flood流量占比明显减少，下降6.3个百分点。这一趋势在大流量攻击中体现尤其明显，详见报告具体分析。

图 5-2 按DDoS攻击总次数/总流量统计各类型占比图

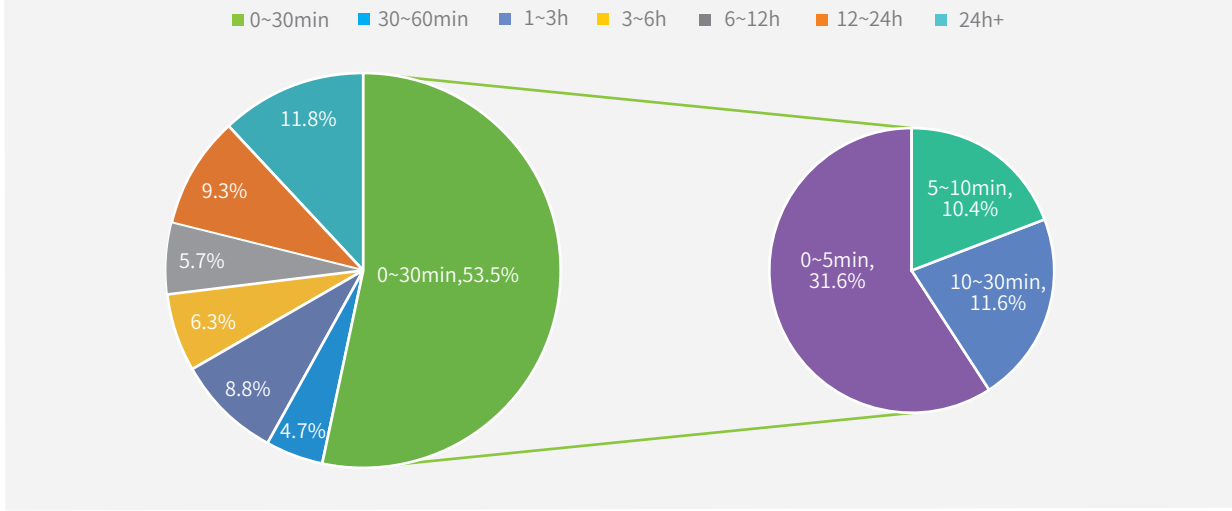


数据来源：绿盟科技全球DDoS态势感知系统（ATM）

5.3 DDoS攻击持续时间占比

2017上半年，长时攻击增多，短时攻击略有下降，但仍然占主导地位。攻击时长在30分钟以内的DDoS攻击占全部攻击的一半以上，占53.5%，相比2016下半年下降8.9个百分点；攻击时长超过3小时的攻击呈增长趋势，总体占比33%，相比2016下半年增长5.7个百分点。

图 5-3 攻击持续时间占比图

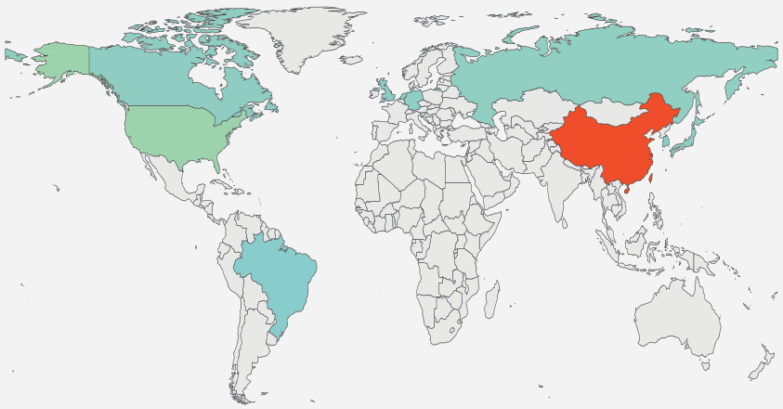


数据来源：绿盟科技全球DDoS态势感知系统（ATM）

5.4 全球DDoS攻击源国家分布

2017上半年，中国依然是DDoS攻击受控攻击源最多的国家，发起攻击次数占全部的46.6%，其次是美国和俄罗斯，分别占3.0%和2.0%。

图 5-4 全球DDoS攻击源国家分布图及TOP 10



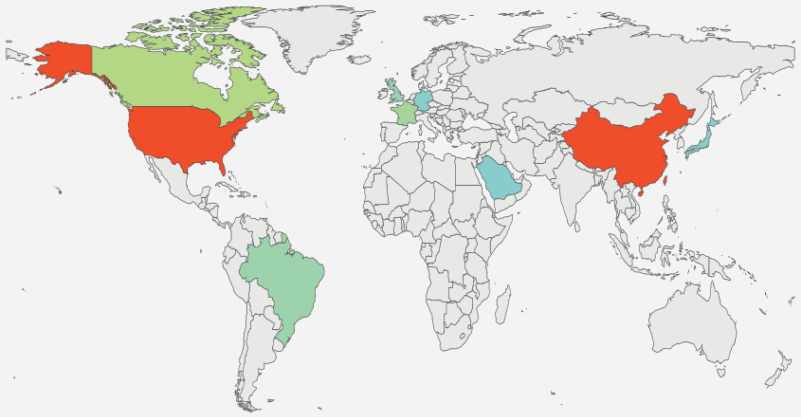
源国家	占比
中国	46.6%
美国	3.0%
俄罗斯	2.0%
加拿大	1.9%
日本	1.9%
德国	1.8%
英国	1.7%
荷兰	1.6%
巴西	1.5%
韩国	1.5%
其它	36.5%

数据来源：绿盟科技全球DDoS态势感知系统（ATM）

5.5 全球DDoS攻击目标国家分布

2017上半年，受攻击最严重的国家是中国，攻击次数占全部被攻击国家的64.6%，其次是美国和加拿大，分别占18.1%、2.5%。

图 5-5 全球DDos攻击目标国家分布图及TOP 10



目标国家	占比
中国	64.6%
美国	18.1%
加拿大	2.5%
法国	1.9%
英国	1.3%
巴西	1.0%
亚太地区	0.9%
德国	0.8%
日本	0.7%
沙特阿拉伯	0.7%
其它	7.5%

数据来源：绿盟科技全球DDoS态势感知系统（ATM）

更多精彩内容和分析请见即将发布的《NSFOCUS 2017 H1 DDoS与Web应用攻击态势报告》，敬请期待。

06.

勒索事件

网络勒索是2017年上半年最为火热的网络犯罪活动，根据对各种勒索活动的监测和分析，有如下发现：

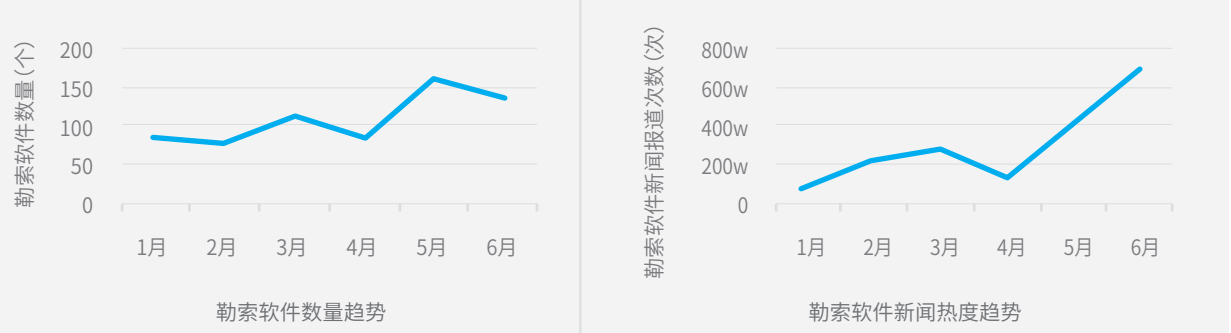
- 勒索软件数量持续增长，技术能力提升明显
- 勒索软件趋向于利用系统漏洞进行自动传播，针对Mac和Linux的漏洞开始频繁出现
- 勒索软件产业日趋成熟，威胁将长期存在
- DDoS勒索和数据库勒索频繁出现，或将成为新的热点

6.1 勒索软件

从技术上看，勒索软件本身并不新颖。但由于其加密行为，可导致数据丢失和关键服务失效，受害者承受的后果更为严重，使其成为当前广大网民和安全行业最为关注的网络犯罪行为。

2017年上半年，不仅出现了WannaCry、Petya/NotPetya等严重的勒索事件，新增勒索软件的数量也明显上升（截止6月30日，共新增勒索软件649个，分布见图6-1），几乎每周都有多起勒索软件的报道出现（主要勒索软件出现情况见图6-2）。其中部分为之前勒索软件的升级版本或者经过简单重组的版本，部分却利用了新的技术进行了全新的开发。

图 6-1 2017上半年勒索软件数量和新闻热度趋势图

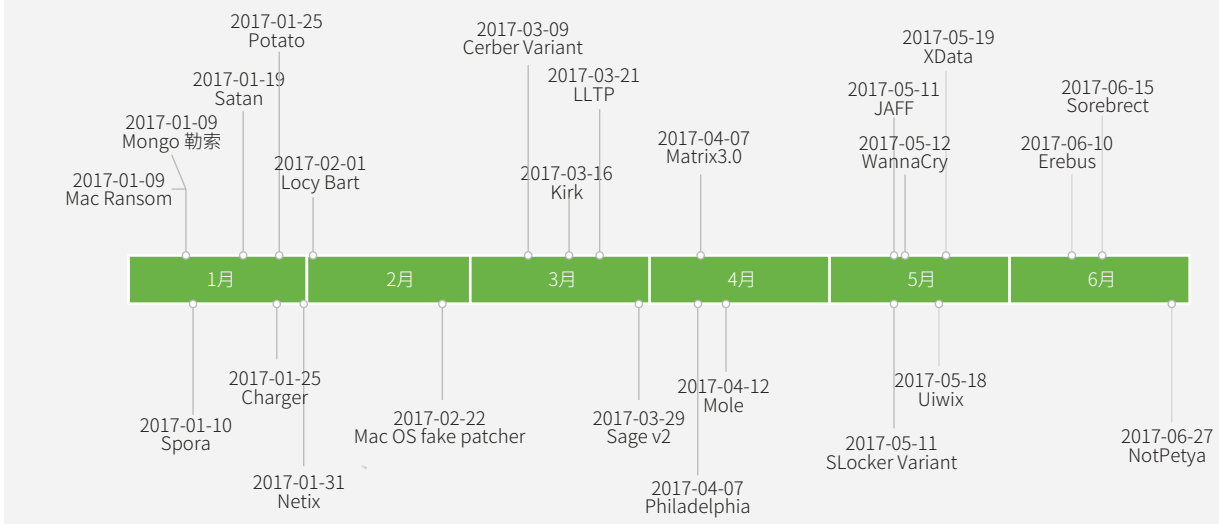


数据来源：绿盟科技威胁情报中心（NTI）

针对2017年上半年出现的勒索软件进行技术分析，我们发现：

- 为逃避检测，曾经流行过的勒索软件正在不断升级，以变种的新形式出现在网络中；开源勒索软件的出现使得勒索软件开发变得更加容易
- 勒索软件编写质量和加密机制日趋成熟，软件存在设计上的缺陷明显减少，被破解解密的可能性变得越来越小
- 从软件逆向分析结果上看，有的恶意软件根本不具备解密能力，即使受害者按照要求支付了赎金也无法解密数据。这类软件往往伪装成勒索软件，实际上却擦除或者不可逆的破坏了用户的文件，而且还可能开出一个高得离谱的赎金来恐吓受害者

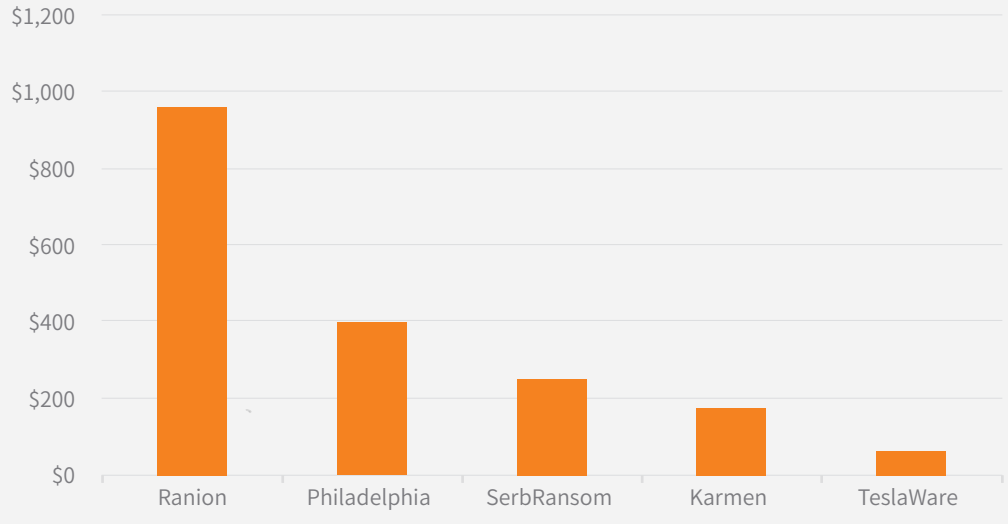
图 6-2 2017年上半年主要勒索软件报道时序图[5]



数据来源：绿盟科技威胁情报中心（NTI）

从传播方式角度看，大部分勒索软件通过邮件附件、网页挂马的方式诱骗用户进行触发操作，但也开始出现高级勒索软件，会对Office、Adobe、本地提权等漏洞进行利用，也会使用弱密码及其他远程执行漏洞进行传播，这类勒索软件对企业和普通用户来说是更为严重的危害。最为瞩目的WannaCry和Petya/NotPetya两款勒索软件，就在蠕虫中使用了微软SMB中存在的漏洞进行传播，一时间导致全球范围内数以万计的主机被感染。同时，使用洋葱路由作为通信保护成为勒索软件常见的技术手段。

图 6-3 勒索服务购买单价排名



数据来源：BleepingComputer

[5] 备注：图中时间坐标指勒索软件在新闻报道中出现的时间，而非该勒索软件首次被发现的时间

从勒索对象看，目前勒索软件主要针对Windows用户，但是针对Mac和Linux用户的勒索软件也开始频繁出现，其中包括Android Charger、SLocker、Lockdroid、Netix、MacRansom、Erebus、KillDisk等。

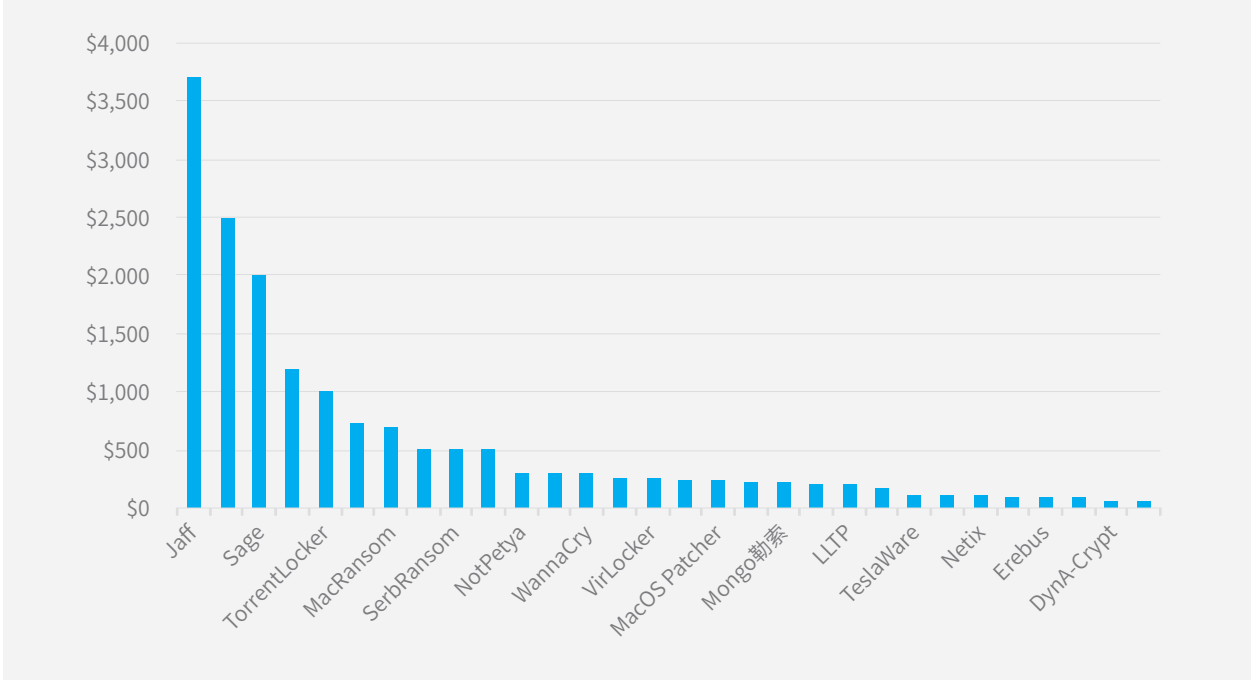
值得引起注意的是，从观察到的售卖情况来看，其已经形成了某种黑产商业，通过售卖短期、永久的证书提供Ransomware as a Service。售卖者通过收取一次性购买款或者提成的方式盈利，甚至有的勒索软件还制作了非常详尽的宣传广告，提供不同版本、不同价位的勒索服务。其中最便宜的商用Ransomeware仅售$60。很多脚本小子，只需要通过一个生成器进行简单的配置，就可以产生不同版本的勒索程序，然后结合传统的邮件、挂马、诱骗下载等方式进行扩散。

比特币产业的成熟也是助推勒索软件兴起的原因之一，匿名的特性使其成为最受勒索者青睐的支付方式。 通过比特币的汇率换算，受害者需要为每台主机向勒索者支付几十到上千美元不等的赎金，一个高级的勒索病毒能够迫使一个企业向黑客支付几十万到上百万的赎金，对于黑产来说，可以获得极大的现金回报。据观察发现：

- 大部分勒索软件的赎金在$100-$500美元之间，但也有要价较高的，例如Sage，Kirf，Jaff，Cerber等，赎金都超过1000美元，其中Jaff甚至高达$3700美元
- 从媒体中曝光的企业来看，企业需要交纳的总金额最高达到1百万美元（韩国Nayana公司）
- 勒索软件提供更加“人性化”的服务，按照文件数量、受害者所在地区的消费水平，提供不同层次的“价格套餐”，并且有详细的指引步骤，对受害者十分“友好”；由此看，勒索软件成本低、收效快、风险小的特点使其在黑产中增长迅猛，用户受到勒索的概率将会越来越高

产业化的发展趋势不难预测：勒索软件必将是未来一段时期内的主要网络犯罪活动之一。

图 6-4 2017上半年新增勒索软件赎金支付单价排名



数据来源：BleepingComputer

6.2 DDoS勒索

DDoS攻击是当前另一种主要的勒索变现的手法，主要通过对受害者的网络服务进行DDoS攻击来勒索赎金。除了部分勒索软件集成的DDoS攻击功能（ 例如FireCrypt ），更多的是通过僵尸网络对勒索对象进行DDos攻击（ 例如 Mirai 、Imeij、Hajime 、DeltaCharlie、Necurs、Amnesia、Rakos等 ）。由于目前基于僵尸网络发动DDoS攻击的黑色产业已经比较成熟，且已存在DDoS as a Service的购买模式，为DDoS勒索营造出日趋完善的商业模式，发动一次攻击非常方便且廉价。可以预见DDoS勒索还将有进一步发展的趋势。

下面梳理了2017年上半年发生的重大的DDoS勒索事件：

时间	DDoS勒索事件
2017-01-23	Lloyds Banking Group 收到一封要价100比特币（£ 75,000 / $94,000）的DDoS勒索
2017-04-26	XMR组织发动一起针对德国企业的DDoS攻击，并向受害者收取€250 ($275) “测试费用”
2017-06-26	继Nayana遭到勒索之后，自称“Armada Collective”的黑客向多家银行收到勒索信息，要求支付$315,000来避免遭受DDoS攻击

数据来源：绿盟科技威胁情报中心（NTI）

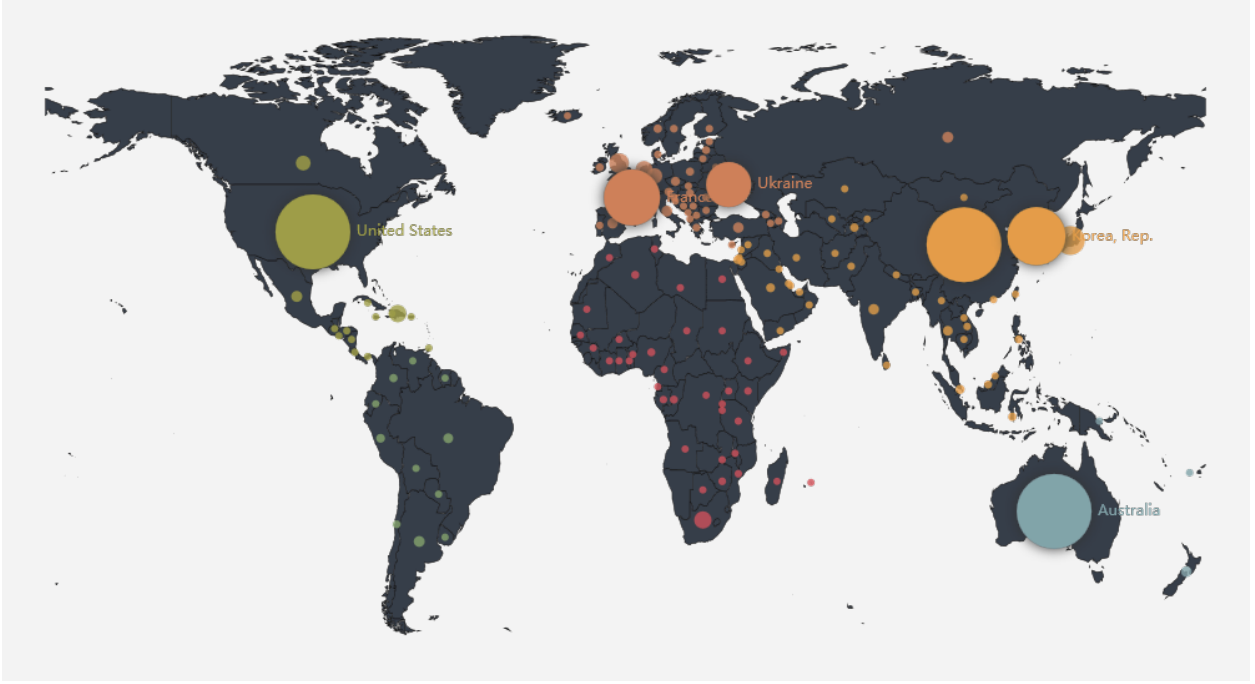
6.3 数据库勒索

很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。数据库勒索主要通过黑客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。今年年初，数据库勒索一度成为一个热门的话题。

时间	数据库勒索事件
2017-01-03	名为“Harak1r1”的黑客通过没有未经严格配置的MongoDB窃取并替换库中数据，并要求受害者支付0.2比特币（约$200）。刚开始仅仅是一个小的突发事件，但是随后更多的攻击者参与进来，其中包括一个专门进行勒索的组织Kraken（从公开信息上看，该组织至少成功攻击了21600个数据库，获利超过$7700）。截止1月15日，据不完全统计，超过32380个数据库、21个黑客组织参与此次勒索。 据观察，事发时暴露在互联网上的MongoDB数据库共计1,994,422个（地域分布见图6-5），如此大量的设备为此类攻击提供了巨大的空间。
2017-01-13	继MongoDB事件之后，ElasticSearch服务器也成为了黑客攻击的目标，攻击者在攻击中向受害者收取0.2BTC（约$200）
2017-01-18	CouchDB与Hadoop相继也出现数据被删除的受害事件
2017-01-24	白帽黑客发现暴露在互联网上的Cassandra数据库也可以成为攻击目标
2017-02-25	MySQL数据库遭遇到勒索事件，攻击者要求支付0.2BTC

数据来源：绿盟科技威胁情报中心（NTI）

图 6-5 2017年1月互联网暴露的Mongo数据库分布图



数据来源：绿盟科技威胁情报中心（NTI）

07.

热门事件监控

2017年上半年，信息窃取与泄露事件频发，热门事件监控如下：

时间	事件
2017年2月	一种新 Android 银行木马 Marcher 出现，通过短信或彩信进行网络钓鱼攻击诱骗用户下载恶意软件，获取权限、收集数十家银行账户数据。重要的是，国内外二十多款杀毒软件拿它没办法，无法查杀卸载
2017年3月	国外安全团队发现了Dridex银行木马的升级版本，该版本被称为Dridexv4
2017年4月	英国知名的发薪日贷款（Payday Loan）公司确定遭遇数据泄露，之后发表声明通知客户联系银行
2017年4月	卡巴斯基发现新型ATM恶意软件“ATMitch”
2017年5月	银行木马 TrickBot 推动了新一轮网络攻击，瞄准英国、澳大利亚与德国的私人银行、私人财富管理企业、投资银行、养老保险与年金管理机构
2017年5月	一个称为”Cron”的组织通过恶意软件Cron感染了俄罗斯100多万部 Android 手机，并盗取了银行客户超过5000多万卢布（约合人民币609万）
2017年5月	德国的O2-Telefonica公司通过《南德意志报》证实，其公司的部分客户遭受到利用SS7漏洞的网络劫持者攻击，攻击者利用7号信令（SS7）中的漏洞从德国银行偷取钱财
2017年6月	安全研究员发现了一款名为“Rufus”的ATM恶意软件
2017年6月	印度外包公司塔塔（Tata）的工作人员将一大批金融机构的源代码和内部文件上传到了GitHub的公共代码库上，造成代码泄露
2017年6月	McAfee Labs 安全研究人员发现一款新型银行恶意软件Pinkslipbot（又名：QakBot/QBot）可使用复杂多级代理通过“HTTPS 控制服务器”通信

数据来源：绿盟科技威胁情报中心（NTI）

总结

网络安全归根也是一种社会经济活动。随着我国互联网应用和用户的日益增加、网络通信设施的改善以及GDP的增长，我国已成为全球主要的网络攻击源头和被攻击的对象。因此机构和个人需要提高警惕，增加安全投入，提升安全防护水平和能力。在网络安全建设中，攻击者总是不断的寻找低难度、高回报的攻击目标，而互联网上那些开放的应用服务、缺省配置、缺少防护措施的节点如同一座座不设防的城市，首当其冲地被攻击者捕获而成为“帮凶”。在攻击中，那些少数能够造成严重危害且攻击成本较低的高危漏洞以及常规的攻击技术手段往往得到攻击者青睐。针对这样的情况，机构和个人需要对安全威胁进行评估，识别并跟踪关键资产的运行状态，分析判断漏洞修补的优先和重要级别，并采取适当的手段以获得防御的优势。此外，一些IT新技术和新业务的应用与开展，在某种程度上也为攻击者提供一定的便利，网络勒索正是这样的一个体现并且渐渐成为一种新的安全威胁趋势。因此，机构和个人有必要增强安全意识，增加对未知威胁的识别检测和防御能力以应对此类威胁。

总体而言，网络安全是一个攻防博弈，动态发展变化的过程，而威胁情报可以帮助安全团队有针对性的制定安全防护策略和执行计划，缩减暴露时间窗口，最大化防御方的投入回报。在此过程中绿盟科技愿意携手包括监管治理机构、安全界厂商、组织和企业用户及个人在内的社会各界资源共同应对网络威胁，构建一个安全的网络空间。

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，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。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com