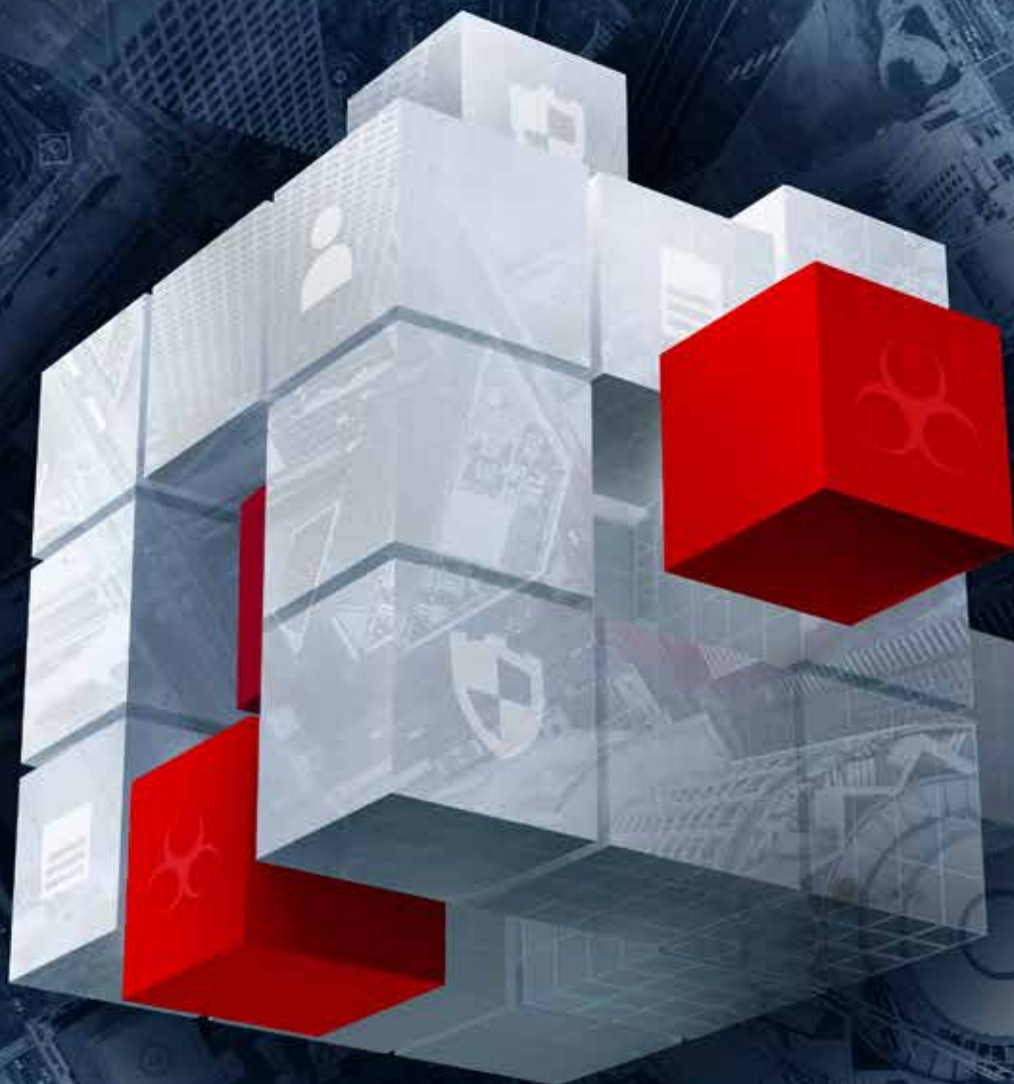


思科

2017 年年度网络安全报告



目录

执行摘要和主要研究结果	3	防御者行为	42
简介	8	2016 年漏洞数呈下降趋势	42
受攻击面的扩大	10	中间件：攻击者在未打补丁软件中寻找机会	44
攻击者行为	13	修补时间：缩短恢复时间	45
 侦测阶段	13	思科 2017 年安全能力基准研究	49
Web 攻击方法：“短尾”威胁帮助攻击者为攻击活动奠定基础	13	观点：安全专业人员对自己的工具信心十足，但不太确定对这些工具的利用是否有效	49
 武器化阶段	15	限制：时间、人才和资金影响应对威胁的能力	51
Web 攻击媒介：Flash 面临逐步淘汰，但用户必须保持警惕	15	影响：越来越多的组织因漏洞而蒙受损失	55
应用安全性：管理应用大爆发期间的开放式身份验证连接风险	16	结果：增强监管将有利于改善安全性	58
 传输阶段	20	信任与成本：购买安全产品的驱动因素是什么？	61
漏洞攻击包巨头的消失为其他规模较小的漏洞攻击包和新型漏洞攻击包提供了机会	20	小结：该基准研究揭示了什么	62
恶意广告：攻击者使用代理来提高行动速度和敏捷性	22	行业	64
调查发现 75% 的组织受到广告软件感染影响	23	价值链安全：全数字化世界的成功取决于第三方风险的缓解	64
全球垃圾邮件日益剧增，恶意附件的比例也越来越高	25	地缘政治最新动态：加密、信任以及对透明度的呼吁	65
 安装阶段	30	高速加密：用于保护传输中数据的可扩展解决方案	66
Web 攻击方法：“长尾”快照揭示用户可轻松避免的威胁	30	网络性能和采用与安全成熟度	67
垂直行业遭受恶意软件攻击的风险：攻击者无孔不入，牟取利益	31	总结	71
Web 阻止活动的地区概况	32	组织受攻击面迅速扩大，需要一个互联的集成安全方法 ...	71
检测时间：衡量防御者进展的基本指标	33	主要目标：减少攻击者的行动空间	73
演进时间：对于某些威胁，变化持续不断	34	关于思科	74
		思科《2017 年度网络安全报告》参与者	75
		附录	78