安全加社区

公益
译文
项目

2017

（非保密）
美国本土面临的网络威胁

2016 年 10 月

（非保密）美国本土面临的网络威胁

2016 年 10 月

本简报的总体分类是：

非保密（U）// 仅供官方使用（FOUO）

（非保密）警告：本产品可能包含必要的美国人信息，以便目标接收方了解、评估或根据所提供的信息采取行动。美国人信息用“USPER”标签突出显示，应根据宪法要求以及联邦与各州的隐私与公民自由法予以保护。

文档信息			
原文名称	(UNCLASSIFIED) Cyber Threats to the Homeland		
原文作者		原文发布日期	2016 年 10 月
作者简介			
原文发布单位			
原文出处			
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

免责声明

- 本文原文来自于互联网的公共方式，由“安全加”社区出于学习交流的目的进行翻译，而无任何商业利益的考虑和利用，“安全加”社区已经尽可能地对作者和来源进行了通告，但不保证能够穷尽，如您主张相关权利，请及时与“安全加”社区联系。
- “安全加”社区不对翻译版本的准确性、可靠性作任何保证，也不为由翻译不准确所导致的直接或间接损失承担责任。在使用翻译版本中所包含的技术信息时，用户同意“安全加”社区对可能出现的翻译不完整、或不准确导致的全部或部分损失不承担任何责任。用户亦保证不用做商业用途，也不以任何方式修改本译文，基于上述问题产生侵权行为的，法律责任由用户自负。

“安全加”社区　　小蜜蜂公益翻译组

威胁

能力 x 意图 = 威胁

- 能力 – 可成功发动攻击的资源
  - 人 – 是否训练有素、是单一源起方还是团队、是否受国家支持
  - 工具 – 恶意软件、硬件、基础设施
  - 战术 – 已有、成熟、新兴还是鲜为人知的技术
- 意图 – 进行攻击的意愿
  - 目标
  - 意欲达到的效果
  - 原则 / 红线

若两者均为“0”，则为零威胁。许多恐怖分子集团有攻击意图但无能力。一些友好的国家、高校、研究与国家实验室有能力却无攻击意图。

《+》
安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

威胁源起国

- **极其活跃、危险、能力高超的网络攻击者**
  - 高级攻击手段与技术专长
  - 自主开发的漏洞利用工具
  - 资源充足
  - 社会工程（鱼叉式钓鱼）、广泛调查与目标分析、DDoS 攻击
- **漏洞利用支持与政治、军事、经济战略规划及情报收集**
  - 持续入侵、访问及数据泄露
  - 针对新兴技术的工业间谍
  - 在贸易谈判与企业合并中的竞争优势
  - 有些国家已将网络行动融入军事理论

采用综合、成熟的战术对各网络进行大范围持续入侵。

《+》
安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

网络犯罪分子

长期的网络威胁

- 攻击能力强
- 一些组织严密的犯罪集团能力高超，许多威胁源起国都无法与之匹敌
- 与破坏性相比，工具开发更看重漏洞利用

利益是唯一驱动因素

- 恶意软件商品化与漏洞利用工具降低了实施犯罪活动的技术门槛
- 获取目标漏洞系统（如 POS 机、ATM 机）的敏感信息
  - 采用勒索软件敲诈受害人
  - 窃取个人身份信息（PII），非法获利

安全加社区
公益译文项目
2017

试图利用网络获取经济利益，而不是为了进行破坏而发动攻击。由于地下黑市的繁荣与不断开发的新型工具，威胁会越来越多。

UNCLASSIFIED//FOR OFFICIAL USE ONLY

黑客犯罪分子

中低级能力

- 命令与控制弱，能力不一
- 缺乏资金与资源

通过犯罪活动，推动政治或意识形态事件发展

- 目的是宣传和暴露攻击目标等
- 对实际行动仅产生短期影响
  - 网页篡改
  - DDoS 攻击
  - 恶意散布个人信息（Doxing）

（U//FOUO）高调行动，小打小闹，效果有限。攻击源无法预测，几乎不可能发动破坏性攻击。

《+》
安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

恐怖分子

攻击能力最低的网络威胁源起方

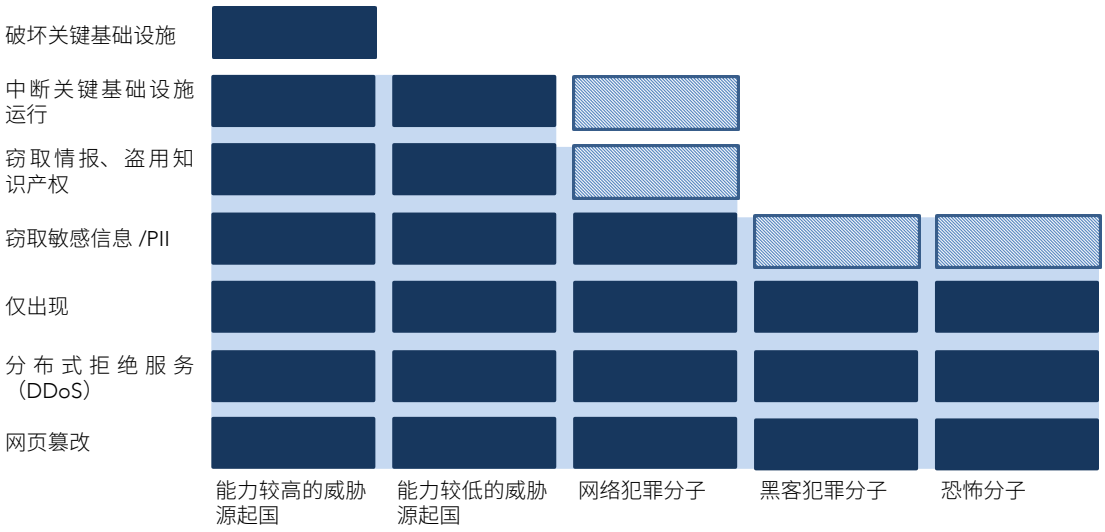
- 自身能力有限
- 使用网络进行招募与宣传
- 使用简单的在线工具窃取 PII，恶意散布个人信息
- 随机选取目标，目标不固定
- 宣扬暴力极端主义

《+》
安全加社区
公益
译文
项目
2017

恐怖分子发动影响力大的网络攻击的可能性较小，因为对相关知识仅有初步了解。不过，潜在的机会目标可能会诱发引人注目的攻击事件。

UNCLASSIFIED//FOR OFFICIAL USE ONLY

评估网络攻击源能力



动机与资源促使网络能力不断提升。

安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

州立、本地与私营部门近期面临的威胁

勒索软件

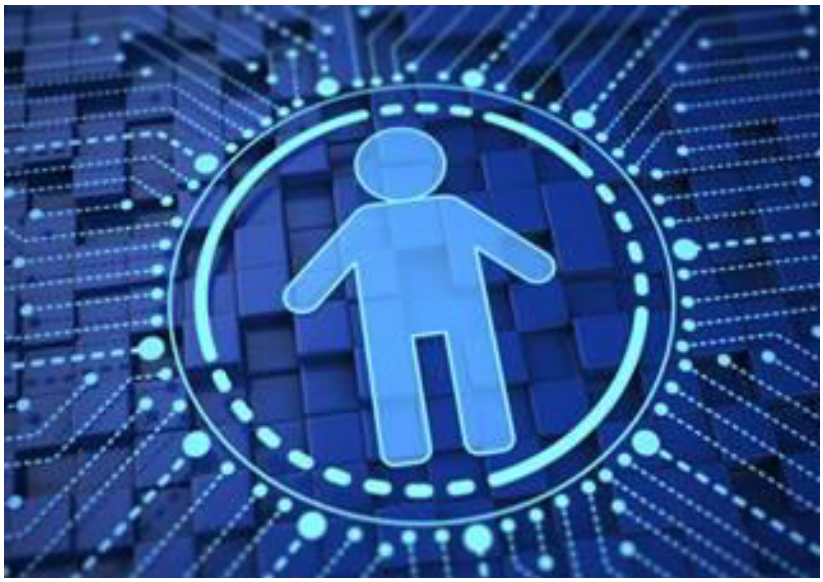
- 与网络犯罪分子相关
- 约始于 2005 年
- 加密系统及 / 或密钥文件
- 索要赎金，解密文件
- 感染媒介：钓鱼、网站入侵、其他恶意软件
- 有能力攻击任何计算机
- 改进版病毒与变种广泛传播
- 近期大事件：
  - 病毒通过互联医疗机构在 3 个州进行传播
  - 短期内针对马萨诸塞州政府发动了 71 次攻击

UNCLASSIFIED//FOR OFFICIAL USE ONLY

应关注的漏洞

物联网

- 终端设备越来越多
- 终端设备保护不力
  - 医疗设备
  - 儿童玩具
  - 厨房用具
  - 婴儿监视器与摄像头
- 近期大事件：
  - 2.5 万多台联网闭路电视（CCTV）设备被入侵，用于僵尸网络 DDoS 攻击
  - 12 所高校的打印机受人操控，打印种族主义与反犹太言论



安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

北卡罗来纳州近期面临威胁

扫描与侦测

- 准备活动
- 高度活跃，威胁程度低

攻击企图

- 针对公共网站的 SQL 注入攻击
- 暴力密码猜测

较成功事件

- 州立机构感染勒索软件
- 北卡立法机构遭 DDoS 攻击
- 利用假冒 CEO 邮件进行转账
- 网络钓鱼 / 鱼叉式钓鱼

安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

重点总结与资源

SLTT 网络与数据面临的威胁

- 最理想情况：低级别破坏与小打小闹（网页篡改、拒绝服务等）
- 最糟糕情况：意图破坏 SLTT 与 CI 网络，使其性能严重下降，拒绝服务
- 大概率事件：泄露并对外发布数据（PII），小动作不断，伺机发动攻击

资源 – 缓解 / 恢复 / 信息共享、调查、最佳实践

- 缓解 / 恢复 / 信息共享
  - 国家网络安全与通信集成中心（NCCIC）：NCCIC@hq.dhs.gov
  - 美国计算机紧急响应小组（US-CERT）：SOC@us-cert.gov
  - 跨州信息共享与分析中心：info@msisac.org
- 刑事调查：美国特勤局（USSS）及美国移民与海关执法局（ICE）
- 最佳实践：国家标准与技术研究院（NIST）网络安全框架
  - 网络安全自评工具：波多里奇卓越网络安全构建工具（Baldrige Cybersecurity Excellence Builder）

安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

SLTT 执法网络事件上报

组织	上报内容
国家保护和计划司（NPPD）	
国家网络安全与通信集成中心（NCCIC）（http://www.dhs.gov/about-nationalcybersecuritycommunications-integration-center） NCCIC@hq.dhs.gov or (888) 282-0870	可能会影响关键基础设施并需要进行技术响应与缓解协助的疑似或确认网络安全事件
美国特勤局（USSS）	
特勤局办事处 (http://www.secretservice.gov/field_offices.shtml) 电子犯罪特遣队（ECTFs） (http://www.secretservice.gov/ectf.shtml)	网络犯罪，包括计算机入侵或攻击、发送恶意代码、密码交易、窃取支付卡或其他金融支付信息
移民与海关执法局国土安全调查处（ICE HSI）	
ICE HSI 办事处（http://www.ice.gov/contact/inv/） ICE HSI 网络犯罪中心（http://www.ice.gov/cyber-crimes/）	基于网络的国内外跨境犯罪，包括剥削儿童、洗钱、走私及对知识产权的侵犯
联邦调查局（FBI）	
FBI 办事处（http://www.fbi.gov/contact-us/field） 网络特遣队（http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nationscybersecurity-1） 在线执法门户（https://www.cjis.gov/CJISEAI/EAIController）或 (888) 334-4536	网络犯罪，包括计算机入侵或攻击、欺诈、知识产权盗用、身份冒用、窃取商业机密、黑客犯罪行为、恐怖活动、间谍、蓄意破坏或其他国外情报活动

安全加社区
公益译文项目
2017

UNCLASSIFIED//FOR OFFICIAL USE ONLY

问答环节

本简报的总体分类是：

非保密（U）// 仅供官方使用（FOUO）

（非保密）警告：本产品可能包含必要的美国人信息，以便目标接收方了解、评估或根据所提供的信息采取行动。美国人信息用“USPER”标签突出显示，应根据宪法要求以及联邦与各州的隐私与公民自由法予以保护。

（非保密）

美国本土面临的网络威胁

安全加社区

公益译文项目

2017

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。