XDef 2019

对话·交流·合作　前沿·实用·人才

第八届全国网络与信息安全防护峰会

从内容安全到行为安全

---历史辩证论的新视角看网络空间安全

周琳娜

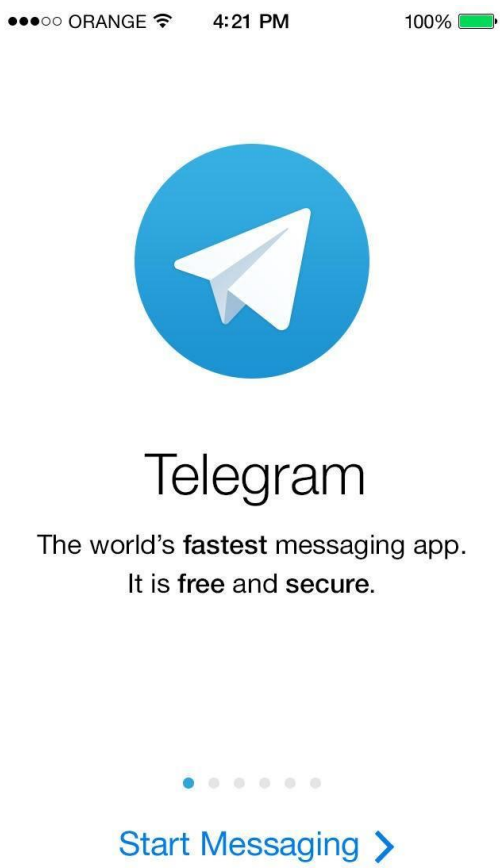
北京邮电大学　2019年12月13日

一张照片背后的故事

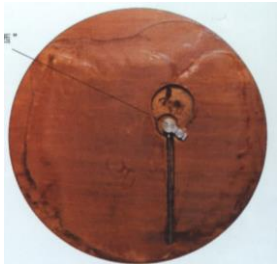
铁人王进喜

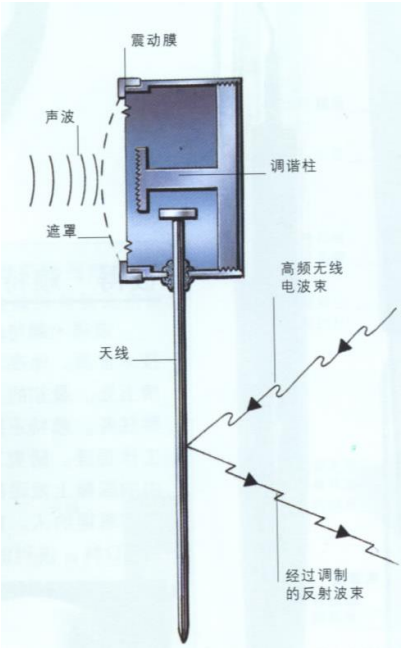
闻名全球的“电报”

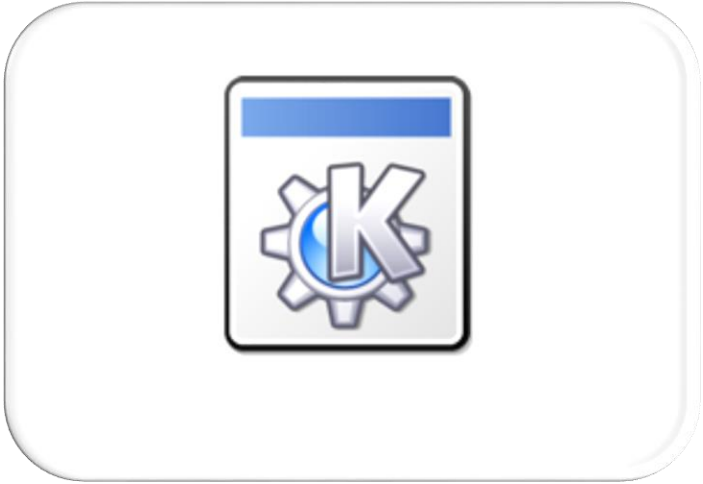
- Telegram messenger
  - 非盈利，不流氓，轻量级
  - 想用就用，不用就删
  - 不留任何用户信息（包括通信内容和身份信息）
  - 不捆绑任何应用
  - Pavle兄弟开发（俄罗斯的扎克伯格）
  - 加密通信 认证算法RSA2048，加密算法AES256
  - 吸引大量恐怖分子和不干好事的人使用



“金唇”窃听器

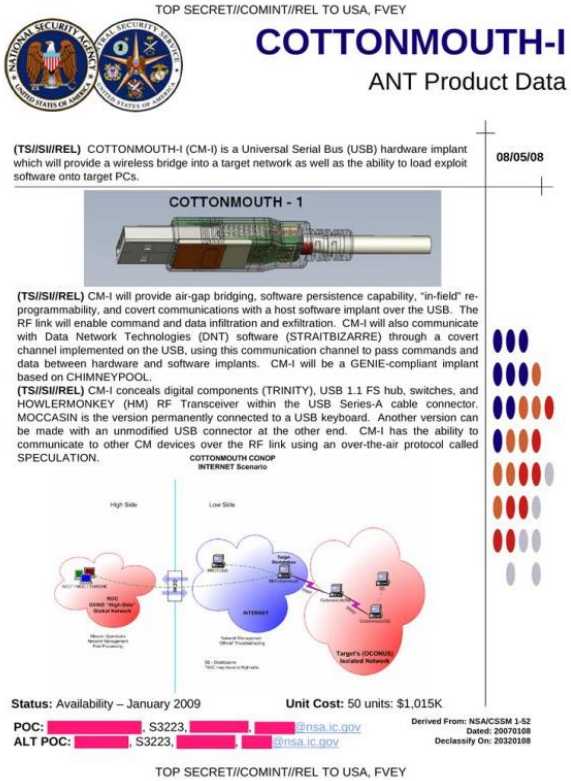






再来看看他们的厉害工具

警惕——看看NSA的工具



TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HOWLERMONKEY (HM) RF Transceiver within the USB Series-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP
INTERNET Scenario

High Side | Low Side

INTERNET

Target's (DCONUS) Isolated Network

Status: Availability – January 2009 **Unit Cost:** 50 units: $1,015K

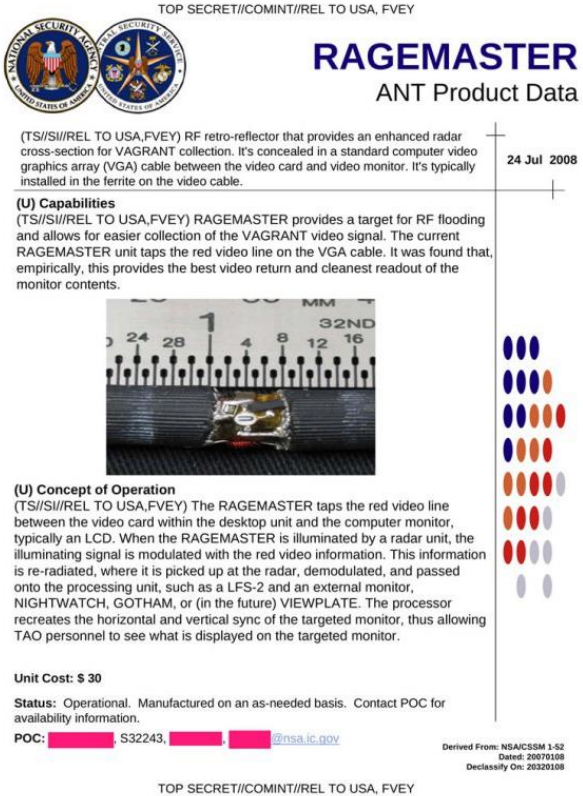
POC: [redacted], S3223, [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- COTTONMOUTH-I
- 水蝮蛇一代
- 一种USB硬件植入，它能通过USB与主机植入的数据网络技术（DNT）软件进行通信，将命令和数据导入或导出。

警惕——看看NSA的工具



TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER

ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

Status: Operational. Manufactured on an as-needed basis. Contact POC for availability information.

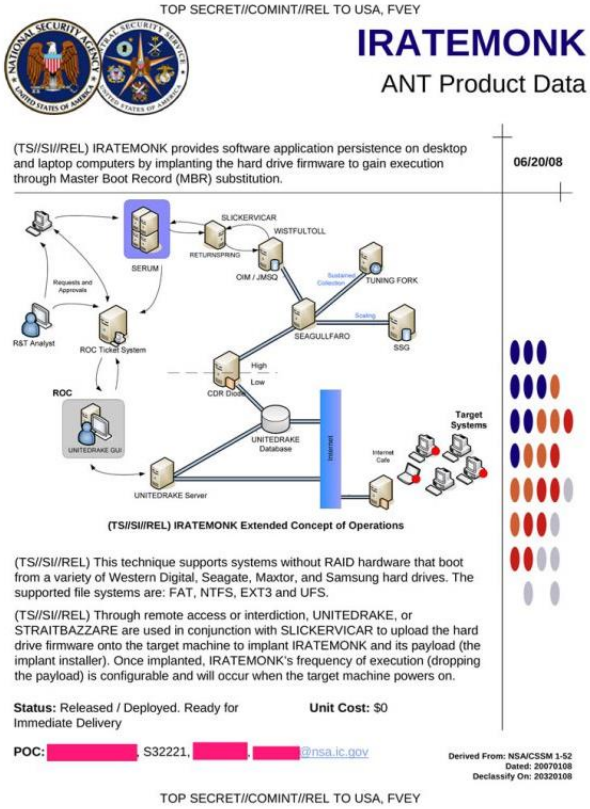
POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- RAGEMASTER
- 狂暴大师
- 一种射频回复反射器，安装在VGA连线上，可以截取显卡到显示器的信号，并通过NIGHTSTAND等技术手段中继传输到远程。

警惕——看看NSA的工具



TOP SECRET//COMINT//REL TO USA, FVEY

IRATEMONK

ANT Product Data

(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

06/20/08

SLICKERVICAR
WISTFULTOLL
RETURNSPRING
SERUM
OIM / JMSQ
TUNING FORK
Requests and Approvals
R&T Analyst
ROC Ticket System
SEAGULLFARO
SSG
High
Low
CDR Disks
ROC
UNITEDRAKE GUI
UNITEDRAKE Database
Internet
Target Systems
Internet Cafe
UNITEDRAKE Server

(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

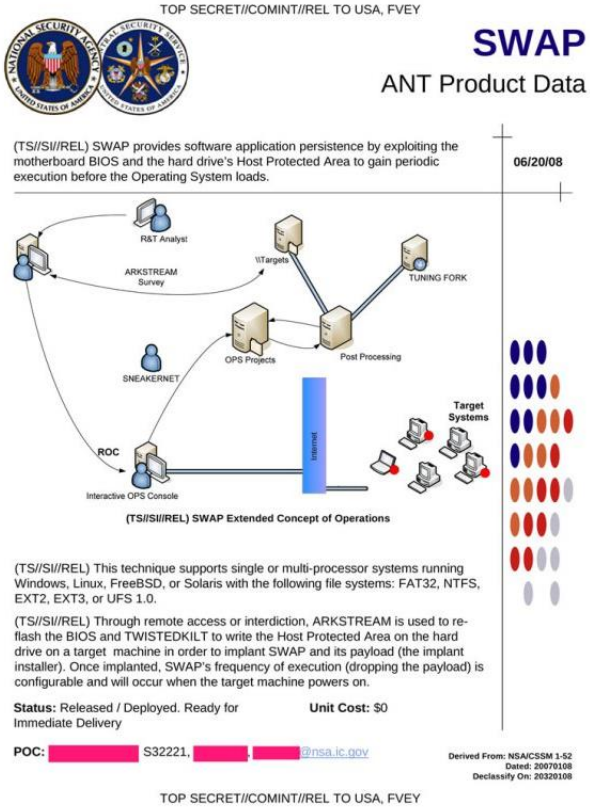
POC: [redacted], S32221, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- IRATEMONK
- 发怒僧侣
- 一种恶意软件，可通过硬盘主引导记录（MBR）替换植入硬盘固件，进而达到常驻系统内存的目的。

警惕——看看NSA的工具


TOP SECRET//COMINT//REL TO USA, FVEY

SWAP

ANT Product Data

(TS//SI//REL) SWAP provides software application persistence by exploiting the motherboard BIOS and the hard drive's Host Protected Area to gain periodic execution before the Operating System loads.

06/20/08

R&T Analyst
ARKSTREAM Survey
\\Targets
TUNING FORK
OPS Projects
Post Processing
SNEAKERNET
ROC
Interactive OPS Console
Internet
Target Systems

(TS//SI//REL) SWAP Extended Concept of Operations

(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS and TWISTEDKILT to write the Host Protected Area on the hard drive on a target machine in order to implant SWAP and its payload (the implant installer). Once implanted, SWAP's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

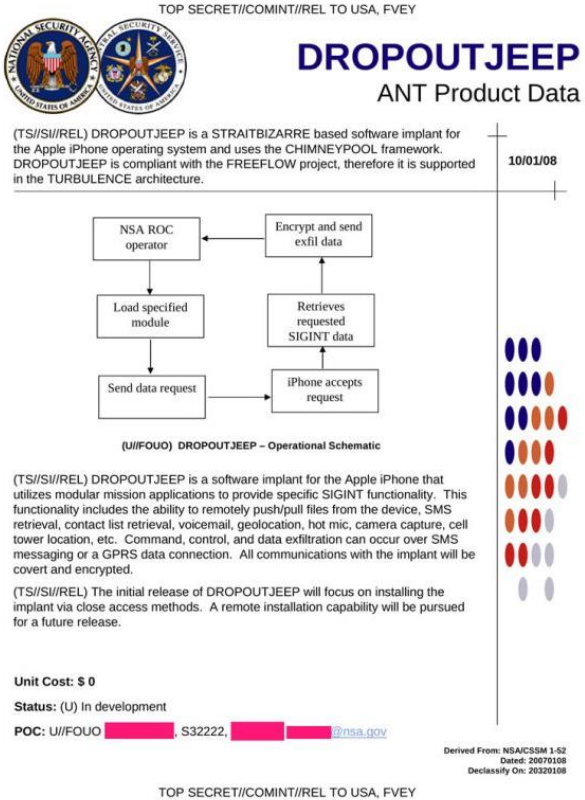
POC: [redacted] S32221, [redacted] [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- SWAP
- 交换
- 一种针对BIOS的恶意软件，可绕过操作系统保护修改BIOS内容，以保护受害计算机上恶意软件持续运行。

警惕——看看NSA的工具



TOP SECRET//COMINT//REL TO USA, FVEY

DROPOUTJEEP

ANT Product Data

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08

(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Unit Cost: $ 0

Status: (U) In development

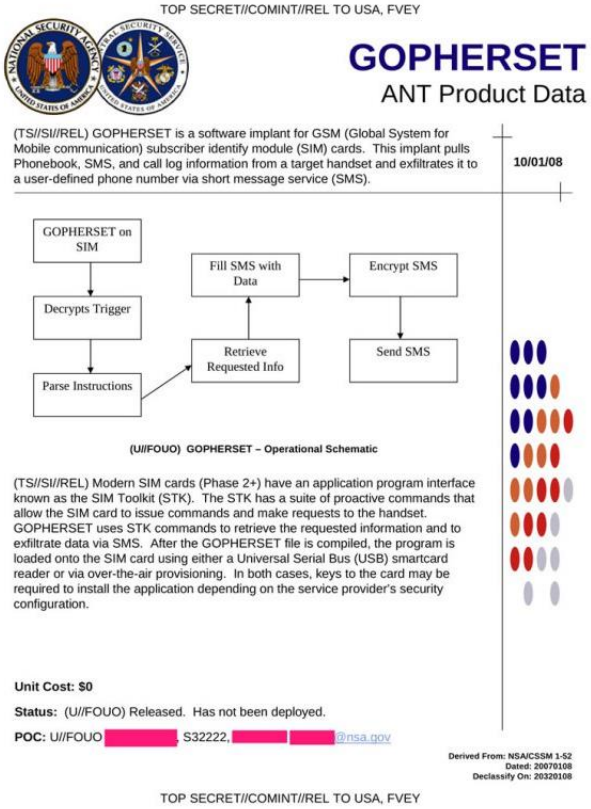
POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- DROPOUTJEEP
- 出轨吉普
- 植入苹果iPhone的恶意软件，可提供专门的情报收集功能。

警惕——看看NSA的工具



TOP SECRET//COMINT//REL TO USA, FVEY

GOPHERSET

ANT Product Data

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08

(U//FOUO) GOPHERSET – Operational Schematic

(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. GOPHERSET uses STK commands to retrieve the requested information and to exfiltrate data via SMS. After the GOPHERSET file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration.

Unit Cost: $0

Status: (U//FOUO) Released. Has not been deployed.

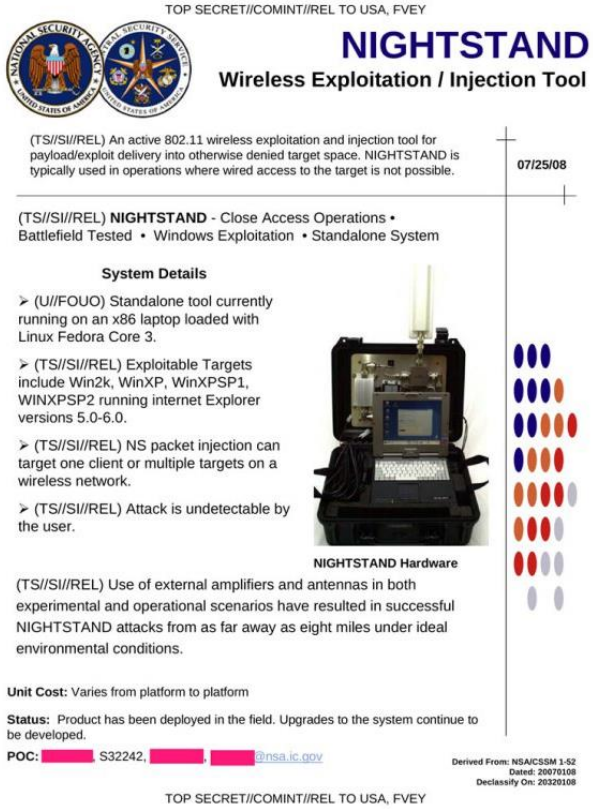
POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- GHOPHERSET
- 松鼠集
- 针对SIM卡实施攻击的工具集，可远程控制手机把手机通讯录、短信等信息发送到指定手机。

警惕——看看NSA的工具



TOP SECRET//COMINT//REL TO USA, FVEY

NIGHTSTAND

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

07/25/08

(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

NIGHTSTAND Hardware

(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.

Unit Cost: Varies from platform to platform

Status: Product has been deployed in the field. Upgrades to the system continue to be developed.

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

- NIGHTSTAND
- 床头柜
- 便携式无线破解工具箱，可实现无线破解、漏洞利用、远程传输、数据中继等功能。在放大器支持下，中继传输距离可达8km。

警惕——看看NSA的工具

- WannaCry
- 一种“蠕虫式”的勒索病毒软件
- 不法分子利用NSA（National Security Agency，美国国家安全局）泄露的危险漏洞“EternalBlue”（永恒之蓝）进行传播 。

再回想一下棱镜...

发酵

8月10日
向德《明镜》周刊曝光美国安局监视目标清单，中俄为最高监视目标

10月24日
向英《卫报》披露美国安局监听35个国家和地区领导人，包括德法等传统欧洲盟友

7月31日
再爆 美“X关键分”监控项目

8月1日
俄批准临时避难申请进入俄境内

……

7月12日
与俄杜马议员和国际人权组织代表、知名律师等会面

爆料

6月30-7月2日
向俄罗斯、玻利维亚等20余个国家提出避难申请

6月24日
爆料美国安局入侵并持续攻击我境内企业和相关机构网络

6月5日
向英国《卫报》曝光美“棱镜”监控项目

6月23 日
由香港前往莫斯科

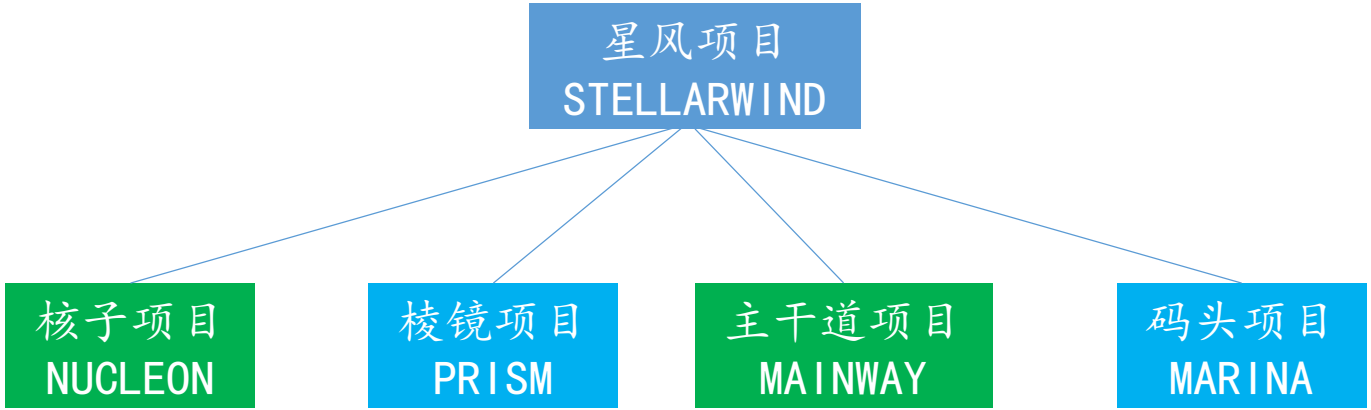
爆发

斯诺登的爆料要点

- 1、美国通过电信公司监控所有美国用户电话记录（元数据）
- 2、棱镜计划——与九大公司的监控合作
- 3、NSA曾攻击包括香港和我国等多个企业与电信运营商
- 4、NSA与GCHQ的合作，互相帮助提供监控
- 5、NSA曾监听多个外国领导人的电话
- 6、XKeyScore：能够“看到一个人在互联网上所作的一切”
- 7、NSA曾尝试破解加密算法，在安全协议中预置后门
- 8、NSA的黑客精英部队：TAO
- 9、NSA曾渗透攻击进入谷歌和雅虎的数据中心
- 10、监控全美短信数据，轻易破解手机通信
- 11、美国可监听巴哈马和阿富汗全国的所有电话
- 12、美国曾入侵SIM卡制造商金雅拓窃取密钥

监控能力

应建立多层次、全方位的网络空间监控能力



- “棱镜”和“核子”负责截取内容
- “核子” 截获电话通话者对话内容及关键词
- “棱镜” 用于监视互联网，从包括微软、谷歌、雅虎、Facebook、PalTalk、AOL、Skype、YouTube以及苹果等美国IT巨头的公司服务器上收集个人信息

- “主干道”和“码头” 对“元数据”进行存储和分析
- “主干道” 监视电话信息，包括通话或通信的时间、地点、使用设备、参与者，但不会窃听通话内容
- “码头” 监控电子邮件、网上聊天系统以及其他借助互联网交流的媒介

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

TOP SECRET//SI//ORCON//NOFORN

美国国家安全局（NSA）
——美国网络监听计划的执行者

- 1952年成立，隶属美国防部
- 总部雇员约3.8万人
- 年预算经费超100亿
- 有三个大型数据情报中心
- 80%美成品情报源自NSA

- “三叶草”、“塔尖”、梯队、“曼哈顿”、“星风”、“棱镜”
- NSA的监控触角已伸向全球信息化基础设施

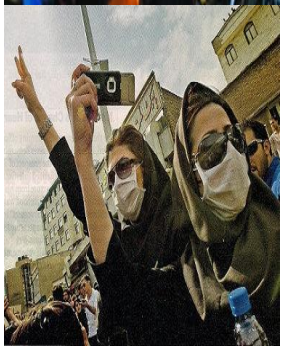
- NSA局长亚历山大兼任网络司令
- 网络司令部与NSA共享设施、人员、情报资源

美国中央情报局（CIA）

——引爆全球网络革命的颠覆者

- 成立于1947年
- 美国最大的、唯一的独立情报部门
- 行动司、情报司、科技司、行政管理与后勤司
- 共约20000人
- 总部位于维吉尼亚州

中亚“颜色革命”



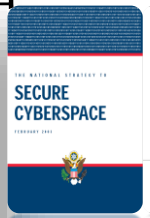
伊朗“推特革命”

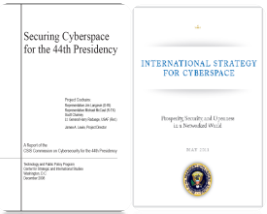
中东北非“茉莉花革命”

美国国土安全部（DHS）

——美国网络安全的捍卫者

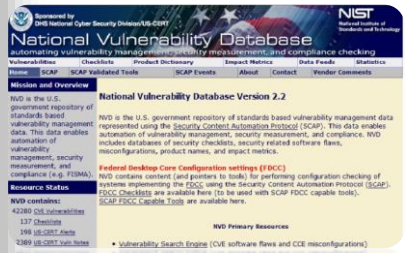
制订执行国家网络安全战略



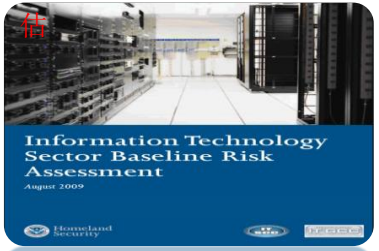


开展信息安全战略政策评估

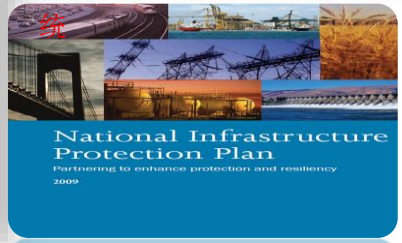
经营国家信息安全漏洞库



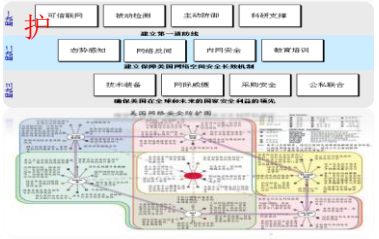
推进国家信息安全风险评估



运行国家信息安全防御系统



强化关键信息基础设施保护



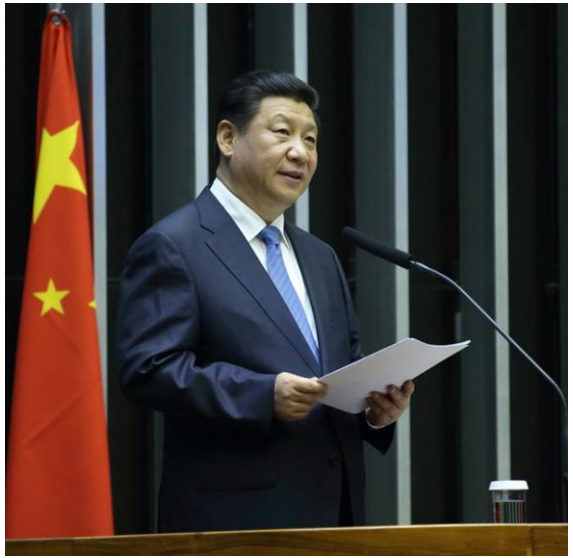
情报分析与行动能力

突袭本拉登

案例：本拉登和巴格达迪

那我们呢？？？

习近平总书记：加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势



----习近平主席的网络安全讲话

- **加快构建关键信息基础设施安全保障体系。金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。“物理隔离”防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。**
- **全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险。要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。要建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制。**

CII+态势感知

信息隐藏的发展历程

古希腊、古中国时代

蜡板传书、漏格传信等方法

巧妙地应用正常的物品及正常的行为隐藏秘密信息

54年在音乐中嵌入不可感知的信号来证明版权

二战时期

隐形墨水等技术的应用

83年Simmons提出了最初的形式化模型

89年在图像中嵌入秘密信息的论文发表

1996年，在英国剑桥牛顿研究所召开了第一届国际信息隐藏研讨会

第1届国际信息隐藏学术研讨会

98年Cachin《An Information Theoretic Model for Steganography》

1999年

第1届国内信息隐藏学术会议

1999年，在北京电子技术应用研究所召开了第一届全国信息隐藏研讨会，迄今为止已召开了15届(华侨大学 2019年10月)

98年左右，学术界开始了隐密分析技术的研究

2005年以后

隐密分析与数字取证

- 隐密技术
- 隐密分析技术
- 数字媒体水印
- 软件水印
- 匿名技术
- 非常规载体隐密技术
- 数字取证技术

对抗是

将军问：木兰，听说你出征前，东市买骏马，西市买鞍鞯，南市买辔头，北市买长鞭，你是女扮男装吧?木兰惊问:你怎么发现的?将军道:男人是不会为了买这点东西逛四个集市的...

对抗是信息安全发展的主旋律

三个层次的安全性对抗

现在看华为的商标，
越看越好看
几瓣几瓣的，
仔细想想才读懂
原来是把苹果给切了

所以 美国人急眼了

HUAWEI

对抗是信息安全发展的主旋律-以信息隐藏为例

三个层次的安全性对抗

破坏秘密信息（鲁棒性对抗）

发现秘密信息（隐蔽性对抗）

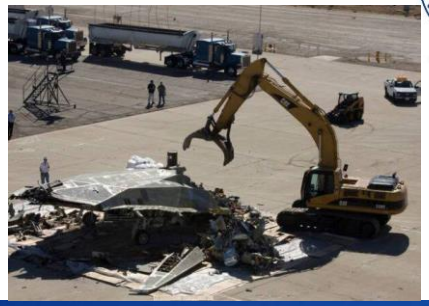
从内容安全
到行为安全

提取秘密信息（取证性对抗）

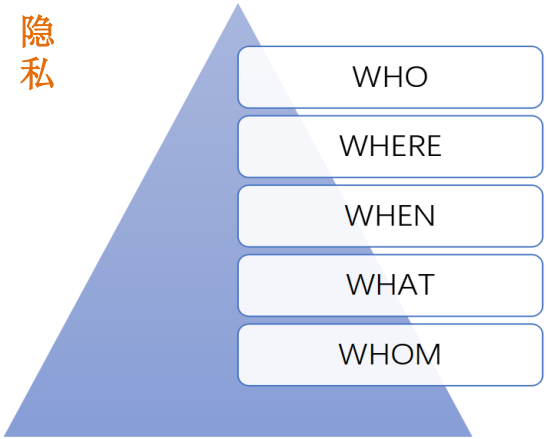
思想的与时俱进——物竞天择，适者生存

- 世界已然变化
- 多维度的来源
- 归一化的存储
- 关联分析

新的时代，新的意识，新的平台



AI来了，在大数据时代



如何隐身?

如何行动? 使用技术方法

运用法律武器	关键是切断三个维度和五个要素之间的映射和联系
运用技术方法	所谓“天时不如地利、地利不如人和”——掩藏身份最重要
运用社会工程学	在现代社会，与身份相关的信息很多，姓名、手机卡号和IMEI号、IP地址、信用卡、医疗保险卡、支付账号等等

怎么办?

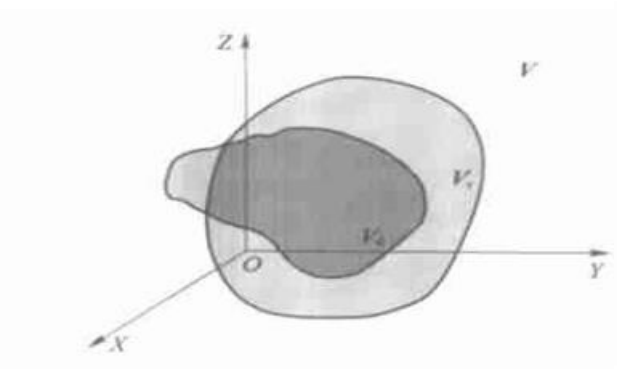


图 1　信息感知与信息记录子空间示意图

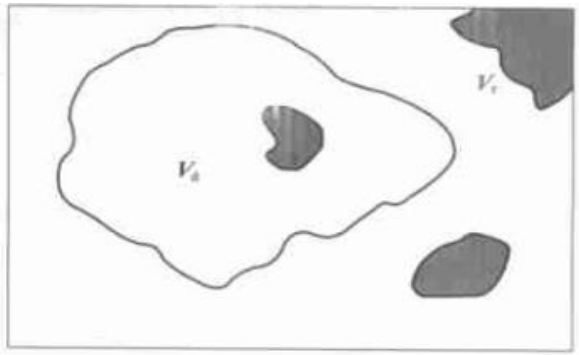


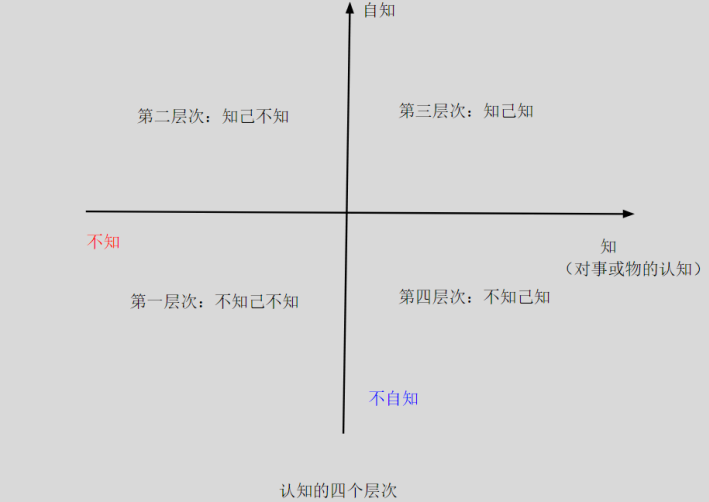
图 2　信息记录与信息感知区域的关系

广义信息隐藏技术的机理与模型

林代茂，　胡　岚，　郭云彪，　周琳娜
(北京电子技术应用研究所，北京 100091)

怎么办?

- 表象
- 认知的四个层面



→ 知己与知彼

AI对信息隐藏的影响

信息隐藏的安全可证需要借助外力

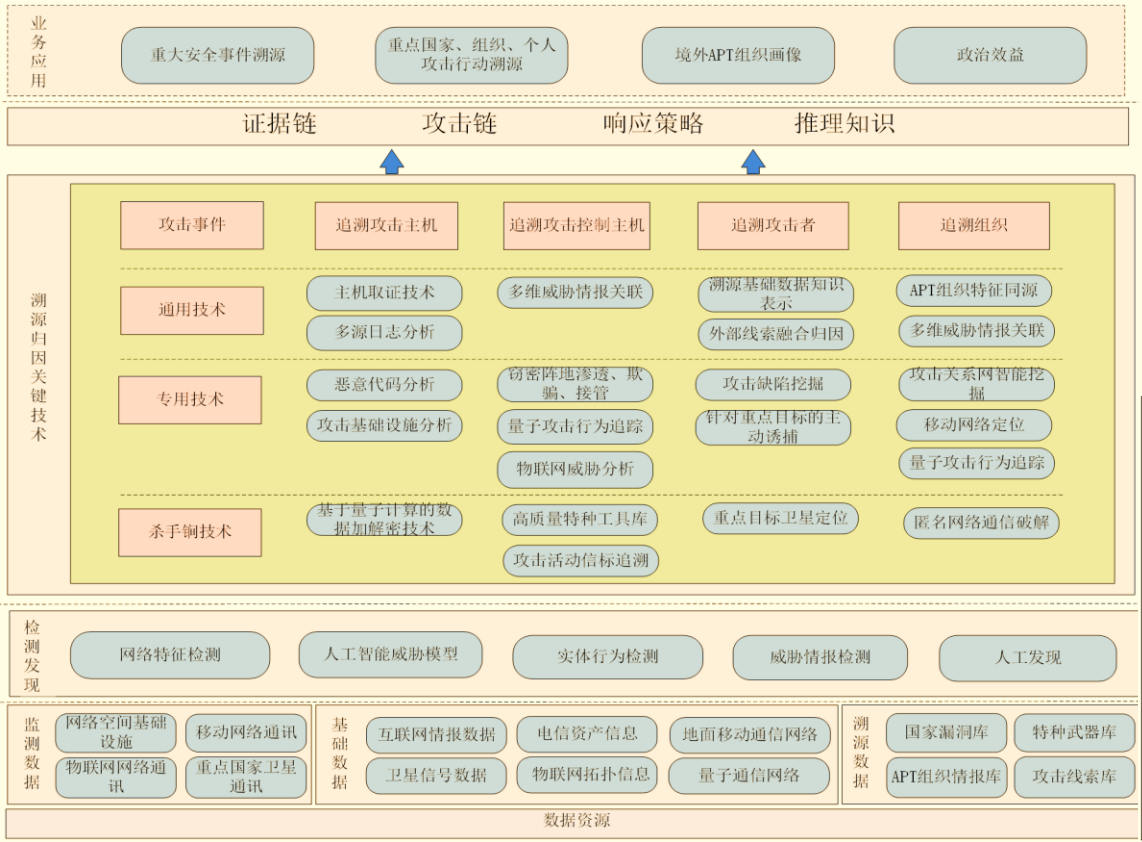
AI对信息隐藏的**赋能**效应

AI对网络攻防的影响

安全是一种伴生技术

AI对网络攻防的伴生效应:
新技术会带来新的安全问题，技术本身有安全问题，还会引发其他安全问题。

网络追踪溯源体系结构



被动溯源分析

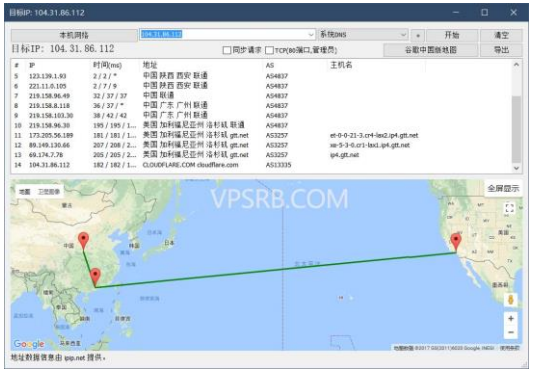
溯源基础数据知识表示 互联网数据、移动通信数据、物联网数据、卫星信号数据归一化	APT组织同源 恶意代码同源、攻击设施同源、TTP同源	多元数据融合归因 受害人分析、地缘政治归因、攻击意图分析、外部资源归因
IPV4/IPV6威胁情报关联 威胁模型构建、IPV6地理测绘、IPV6关系网挖掘	4G/5G移动互联网威胁定位 通信还原、信令分析、物理定位	攻击关系网挖掘 恶意代码关系网、IP域名关系网、攻击组织关系网
量子攻击行为追踪 量子计算威胁模型、量子攻击电子证据、攻击组织情报线索	量子计算数据加解密技术 窃密数据还原、攻击命令检测、危害定损	物联网威胁终端谱系分析 终端信息谱系化、僵尸网络控制接管

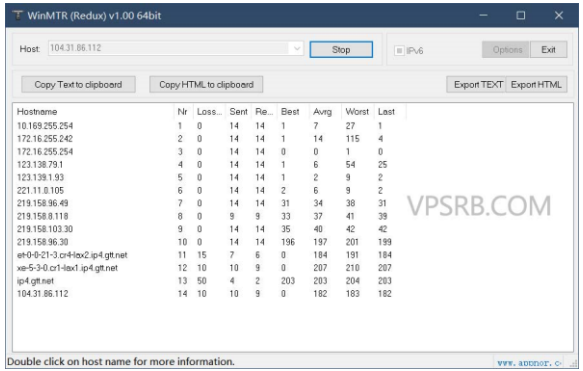
主动溯源分析

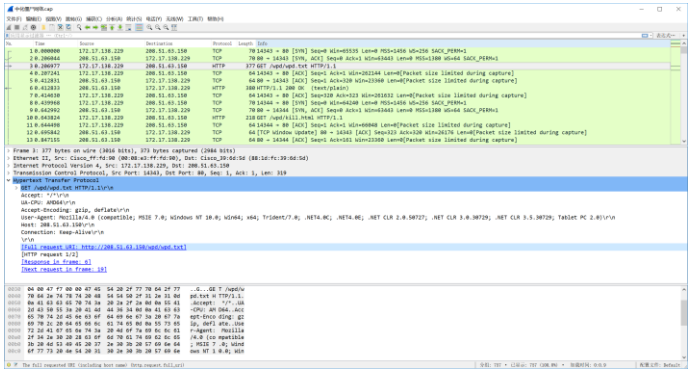
窃密阵地渗透、欺骗、接管 服务器渗透、web应用渗透、个人账户渗透	针对重点目标的主动诱捕 蜜罐追踪技术/基于社会工程学的溯源技术
攻击缺陷挖掘 攻击组织武器获取分析、漏洞利用溯源	匿名网络通信破解 攻击者跳板机追踪、真实攻击IP定位
攻击活动信标追溯 基于不同角色的信标制作技术、攻击流量信标嵌入技术	重点目标卫星定位 定位卫星部署、重点人物定位追踪

网络追踪溯源常用工具

- 磁盘和数据捕获工具
- 文件查看器
- 文件分析工具
- 注册表分析工具
- 互联网分析工具
- 电子邮件分析工具
- 移动设备分析工具
- 网络流量取证工具
- 数据库取证工具







湖畔大学五期学员名单

2019

戴　琨（优信集团）　韩树人（鲜丰水果）

胡彦斌（纽班文化）　黄源浩（奥比中光）

蒋晓莹（香飘飘）　李丹阳（年糕妈妈）

李华敏（时代天使）　李来斌（水星家纺）

李　娜（云锋新创）　李　想（车和家）

李一帆（禾赛科技）　林凯源（GOGOVAN）

刘梦媛（衣二三）　刘舒婷（超级猩猩）

刘　夜（作业盒子）　娄楠石（气味图书馆）

马瑞敏（地素时尚）　桑文锋（神策网络）

沈　鹏（水滴互助）　苏　峻（智米科技）

苏伟杰（诸葛找房）　王　宁（keep）

王　星（创客星球）　吴　群（鱼跃医疗）

夏海通（朴诚乳业）　夏玉洁（中鼎橡塑）

杨　冰（毒APP）　余　凯（地平线）

余玲兵（宋小菜）　俞　哲（婚礼纪）

张步镇（速道信息）　张世伟（凯京信达）

张天泽（零氪科技）　张以弛（校宝在线）

赵　璐（太美医疗）　郅　慧（DaDa英语）

朱海琴（云海肴）　朱　明（金螳螂）

竺兆江（传音控股）　邹小武（易点天下）

跨界生：潘江雪（真爱梦想）

当你老了，回顾一生，就会发觉：
什么时候出国读书，
什么时候决定做第一份职业，
何时选定了对象而恋爱，
什么时候结婚，
其实都是命运的巨变。

只是当时站在三岔路口，
眼见风云千樯，
你作出选择的那一日，
在日记上，
相当沉闷和平凡，
当时还以为是生命中普通的一天

XDef 2019

对话·交流·合作　前沿·实用·人才

Thanks

谢谢关注!