ISC 2019 第七届互联网安全大会

追踪NSA网络武器的那些年

郑文彬

360集团首席安全技术官、伏尔甘团队创始人

小鹅助理

扫码添加小鹅助理，与数万科技圈人士分享重量级活动PPT、干货培训课程、高端会议免费门票

追踪NSA网络武器的那些年

Years of Tracking NSA Cyber Weapons

郑文彬 | 360集团首席安全技术官

关于我（@mj0011sec）

360集团首席安全技术官

360三名创始工程师之一，在网络安全领域14年+

360Vulcan Team 创始人

2016~2018 PwnFest / Pwn2own / 天府杯 世界总冠军

国家信息安全漏洞库特聘专家

首届十名国家网络安全优秀人才

关于360威胁情报中心

360威胁情报中心（@360CoreSec）– 高级威胁应对小组（ATA Team）

中国最强的高级威胁对抗、网络战攻防精英

360安全数据海

十年安全ML & AI 积累

独门技术：终端威胁探针 / 高级漏洞侦测 / 零日漏洞库

高级威胁情报和追踪积累

议程

关于我 / 关于360威胁情报中心

NSA网络武器：背景

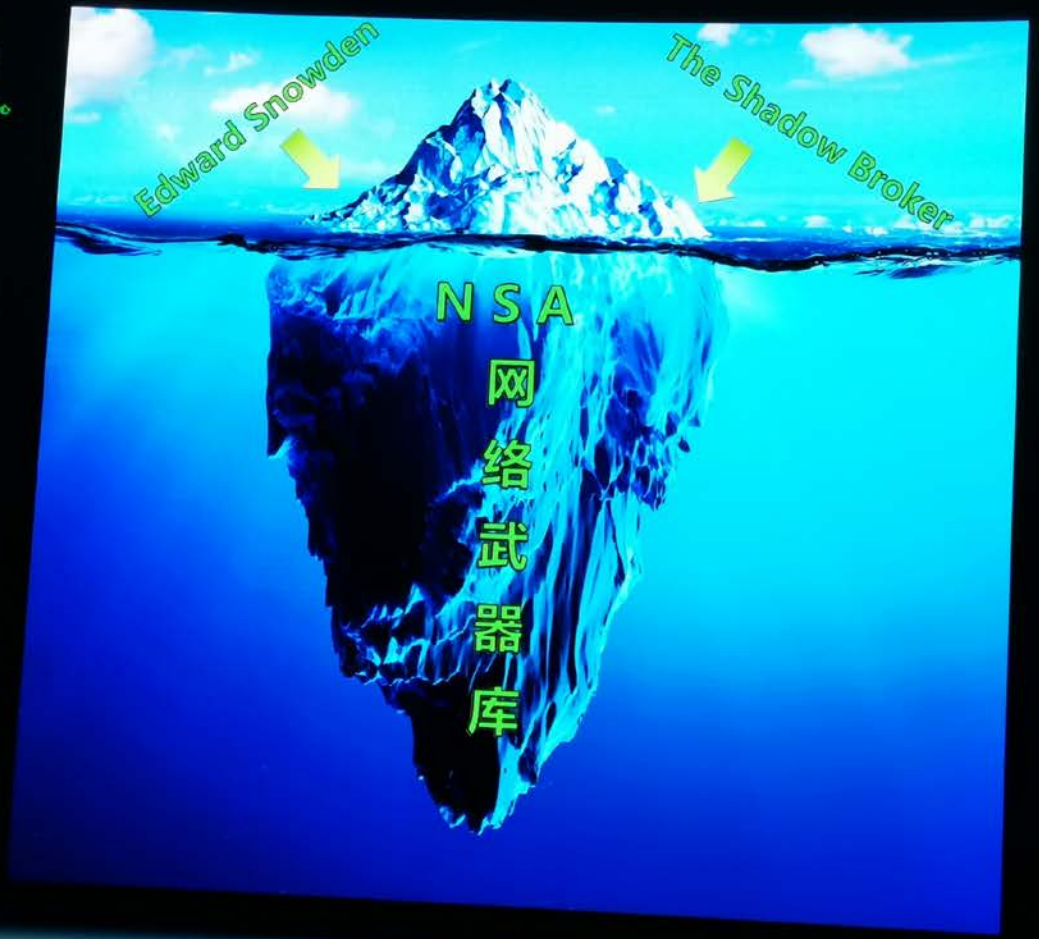
追踪NSA网络武器

追踪永恒之蓝

第七届互联网安全大会

360万联网安全中心

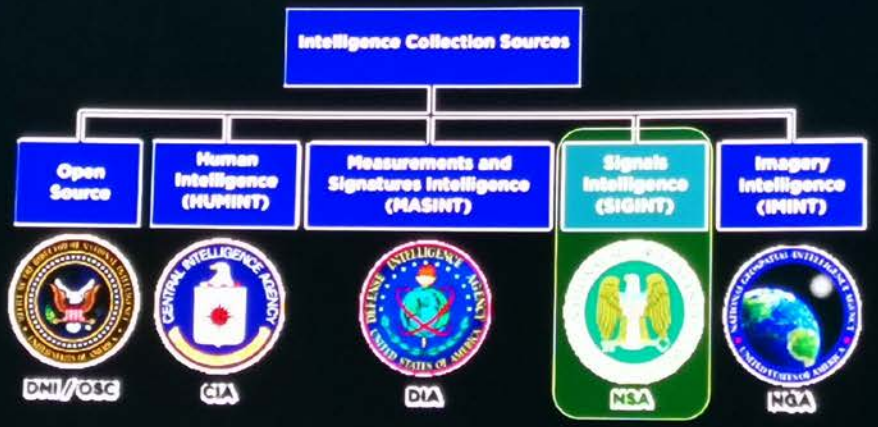
冰川法则



一开始的演讲计划


讨论后决定演讲的内容
Edwar
w Broker
N S A

美国情报机构分工



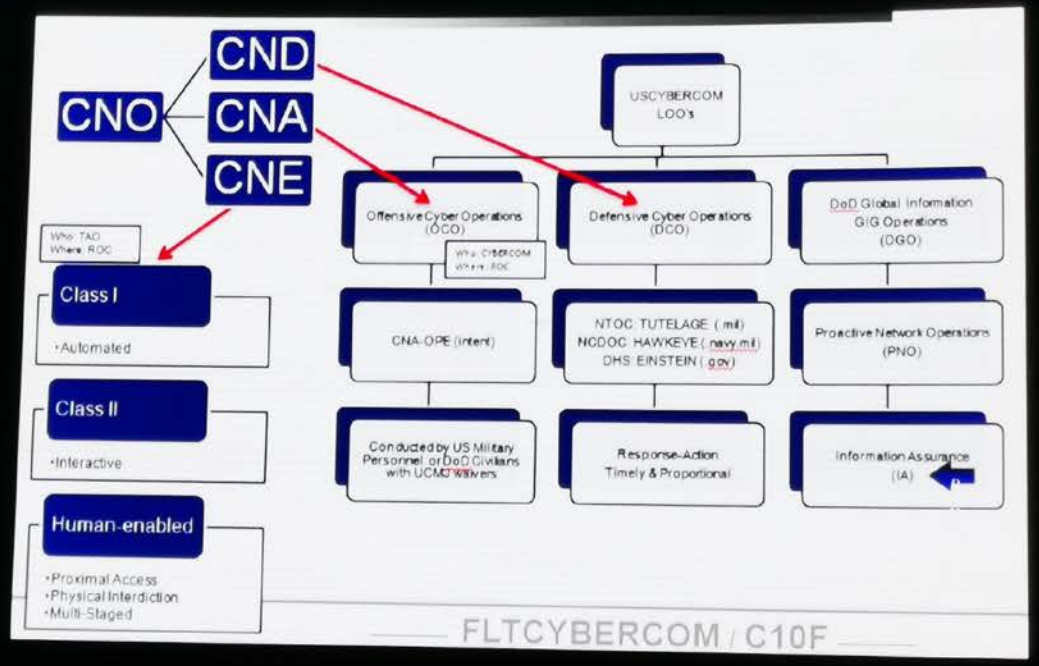
致力于电子情报(SIGINT)收集和分析

全世界单独雇佣最多数学博士、计算机博士和语言学家的机构，每年花费超过100亿美元

不惜成本、不择手段进行情报能力布局：1000万美元收买RSA公司植入算法后门(2004)

Source: https://xmmc.lhgu4dm.com/c.php?g=4541208p=3381428

美国网战司令部（USCYBERCOM）– 作战方案



Source: NICO MARYLAND ADVANCED COMPUTER NETWORK OPERATIONS COURSE

TAO（Tailored Access Operations）

|

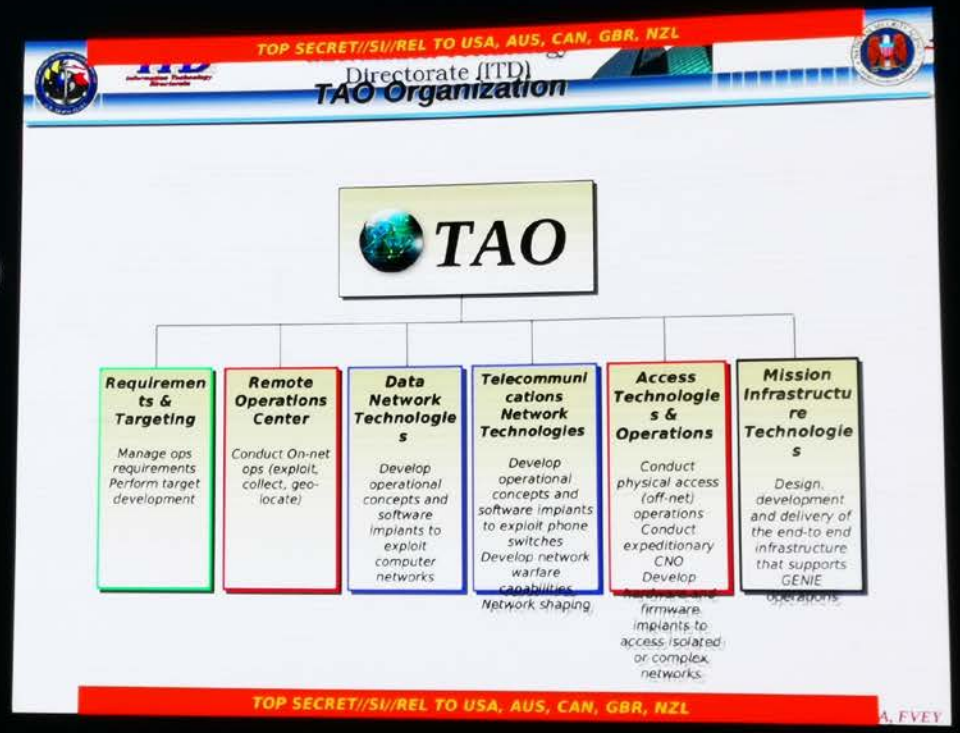
ROC（Remote Operations Center）

核心网战能力输出

+

ATO（Access Technologies & Operations）

核心技术和能力研发

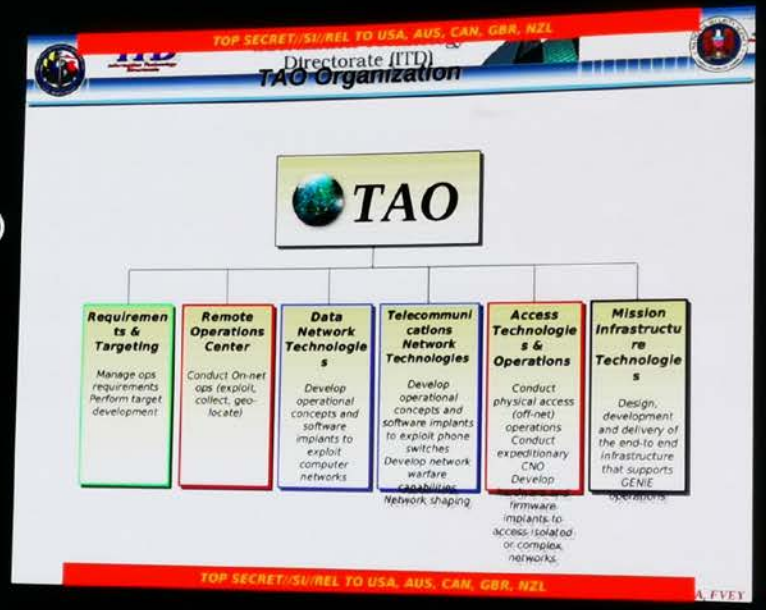


Source: NICO MARYLA[illegible]ANCED COMPUTER NETWORK OPERATIONS COURSE

TAO（Tailored Access Operations）
|
ROC（Remote Operations Center）
核心网战能力输出
+
ATO（Access Technologies & Operations）
核心技术和能力研发

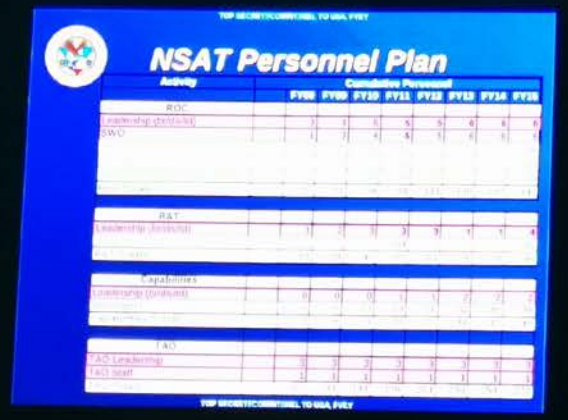
Target Sets - R&T Analysts

- China
- Russia
- Iran
- Afghanistan
- Pakistan
- India
- Iraq
- Counterterrorism
- Cyber Counterintelligence (CCI)



Source: NICO MARYLAND ADVANCED COMPUTER NETWORK OPERATIONS COURSE

TAO: ~2007年从小团队开始



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

NSAT Personnel Plan

Activity	Cumulative Personnel							
	FY08	FY09	FY10	FY11	FY12	FY13	FY14	FY15
ROC								
Leadership (contractor)	2	2	5	5	5	6	6	7
SWO	1	2	4	5	5	5	5	5
R&T								
Leadership (contractor)	1	1	2	3	3	3	4	4
Capabilities								
Leadership (contractor)	1	0	0	0	1	2	2	1
TAO								
TAO Leadership	2	2	2	2	2	2	2	2
TAO staff	3	3	3	3	3	3	3	3

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

Source: Tailored Access Operations

TAO: ~2007年从小团队开始

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

NSAT Personnel Plan

Activity	Cumulative Personnel FY08	FY09	FY10	FY11	FY12	FY13	FY14	FY15
ROC								
Leadership (brilliant)	2	2	2	6	6	6	6	6
SWO	1	3	4	6	6	6	6	6
Interactive Operators	8	25	40	52	65	79	93	96
Production Operators	10	16	19	20	21	22	23	23
Network Response (NWO/NIO)	6	7	11	13	15	17	19	20
ROC Totals	37	55	79	95	111	130	137	141
R&T								
Leadership (brilliant)	1	2	3	3	3	4	4	4
Analysts	12	27	44	54	59	67	72	81
R&T Totals	13	29	47	57	62	71	76	85
Capabilities								
Leadership (brilliant)	0	0	0	1	1	2	2	2
Developers	3	6	13	19	26	32	35	38
Capabilities Totals	3	6	13	20	27	34	37	40
TAO								
TAO Leadership	3	3	3	3	3	3	3	3
TAO Staff	1	1	1	1	1	1	1	1
TAO Totals	57	94	143	176	204	239	254	270

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

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

TAO - Space

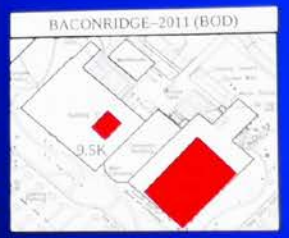
- **Status of Room 137**
  - 13 Racks installed, powered, in use
  - CDR Operational
  - Next installation in November 2008 for FREEZEPOST & DOCKETDICTATE
- **Schedule for Space A & B**
  - Operational - 27 NOV
  - Currently, TAO - 60 persons occupying 39 desks
  - Space management enabled by TDYs, Training, Integrees, Shift-Work, Details
  - End of 2008, potential for 13 more personnel

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

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

BACONRIDGE

AREAS	TEXAS
Personnel #s	270
Workstations	210
Workstation Area SqFt TX=100sqft vs GA/MI=72sqft	21,000
Operations Floor	1881
Ops Breakout Rooms	11
Large 350 sq ft	5
Medium 250 sq ft	4
Small 150 sq ft	2
Ops Breakout Rooms Total	3109
ROC Training Lab (RTL)	996
Technical Demonstration Center (TDC)	732
Maintenance Lab	~700
Data Closet	600
Conference Room	732
Caves	(8) ~ 85 = 680
Break/Locker area	~850
Data Center Racks/sqft	200 / 9,450
Total Sq Ft	*42000



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

Source: Tailored Access Operations(ES Leaking)

TAO: ~2007年从小团队开始

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

NSAT Personnel Plan

Activity	Cumulative Personnel FY08	FY09	FY10	FY11	FY12	FY13	FY14	FY15
ROC								
Leadership (brilliv/d)	3	4	5	5	5	6	6	6
SWO	3	3	4	5	5	6	6	6
Interactive Computers	0	25	40	62	65	70	83	90
Production Computers	19	18	19	20	21	22	23	2[illegible]
Network Response (NWO/NIO)	0	-	11	13	15	17	19	2[illegible]
ROC Totals	37	55	79	85	111	130	137	14[illegible]
R&T								
Leadership (brilliv/d)	1	2	3	3	3	4	4	4
Analysts	12	27	44	54	59	67	72	8[illegible]
R&T Totals	13	29	47	57	62	71	76	8[illegible]
Capabilities								
Leadership (brilliv/d)	0	0	0	1	1	2	2	2
Developers	3	6	13	19	26	32	35	3[illegible]
Capabilities Totals	3	6	13	20	27	34	37	4[illegible]
TAO								
TAO Leadership	3	3	3	3	3	3	3	3
TAO Staff	1	1	1	1	1	1	1	1
TAO Totals	57	94	143	176	204	239	254	27[illegible]

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

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

TAO - Space

- Status of Room 137
  - 13 Racks installed, powered, in use

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

Production Operations (POD)

	FY07	FY08
Olympus Tickets	6,360	9,126
SHARPFOCUS (SF2)	320	1940
PARCHDUSK (PD)	340	366
FOXACID Messages	12	17
sent to	2396	3446
called back	419	672
exploited	154	262

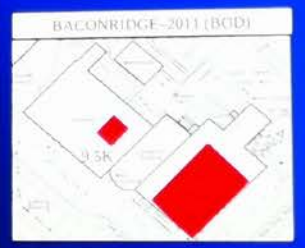
Iraq
Afghanistan

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

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

BACONRIDGE

AREAS	TEXAS
Personnel #s	270
Workstations	210
Workstation Area SqFt TX=100sqft vs GA/HI=72sqft	21,000
Operations Floor	1881
Ops Breakout Rooms	11
Large 350 sq ft	5
Medium 250 sq ft	4
Small 150 sq ft	2
Ops Breakout Rooms Total	3109
ROC Training Lab (RTL)	996
Technical Demonstration Center (TDC)	732
Maintenance Lab	~700
Data Closet	800
Conference Room	732
Caves	(8) ~ 85 = 680
Break/Locker area	~850
Data Center Racks/sqft	200 / 9,450
Total Sq Ft	*42000



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

Source: Tailored Access Operations(ES Leaking)

TAO 量子（QUANTUM）系列攻防平台
量子理论：主动&被动协议注入技术
量子植入（QI）：高度成功
量子饼干（QB）
量子短剑（QD）

TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

TOP SECRET//COMINT//REL USA, FVEY

(U) There is More Than One Way to QUANTUM

TS//SI//REL

Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other means)
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets (that are behind) large proxies, lack predictable source addresses, and have insufficient unique web activity	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (BISCUIT uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable's passive coverage to use as covert infrastructure	Oct 2010	Live Tested	**N/A**
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption	Dec 2008	Live Tested	**N/A**
CND				
QUANTUMSMACKDOWN	Prevents target from downloading implants to DoD computers while capturing malicious payload for analysis.	Oct 2010	Live Tested	**N/A**

TS//SI//REL

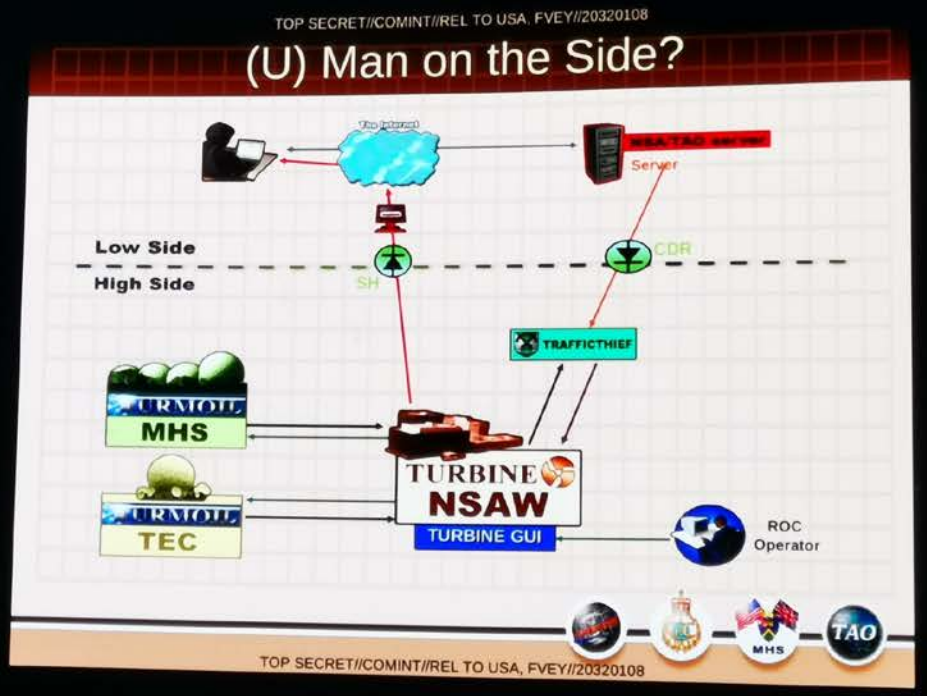
TOP SECRET//COMINT//REL USA, FVEY

1

Source: Case Studies of Integrated Cyber Operation Techniques
Source2: NSA QUANTUM Tasking Techniques for the R&T Analyst

MtoS（Man on the Side）会话劫持和注入

MHS: Menwith Hill Station



Source: QUANTUMTHEORY

FOXACID：酸狐狸零日漏洞攻击平台

在劫持流量、钓鱼邮件或XSS中植入攻击代码
获得目标系统控制权

VALIDATOR：初始化验证和轻量后门

用于初步探明目标环境
进一步安装复杂后门系统如欧林巴斯、联合耙等

TOP SECRET//COMINT//NOFORN

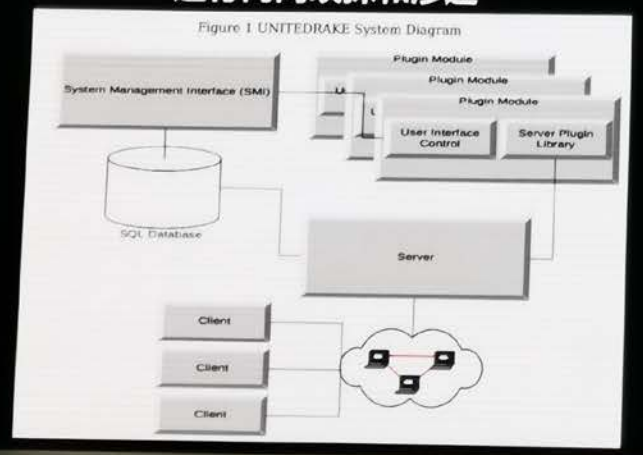
VALIDATOR

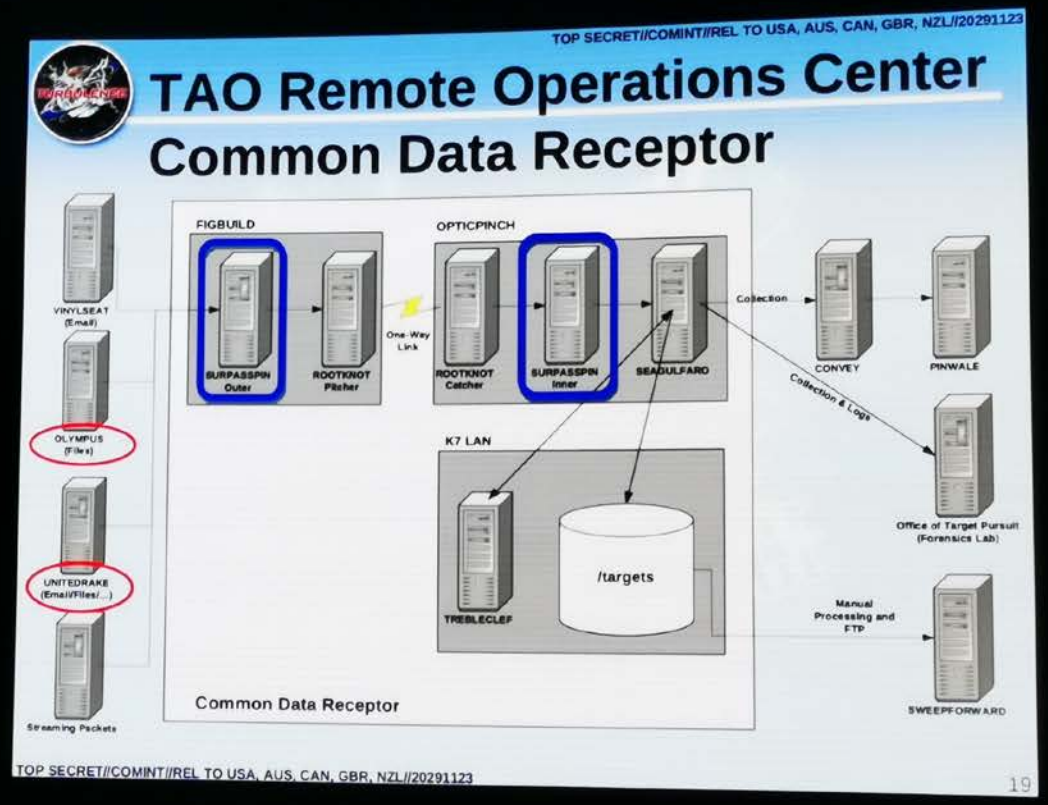
- VALIDATOR is a program that is designed for installation on target computers in a variety of ways.
- Its main function is to serve as a download agent for the Olympus installer, but it has other features that make it useable as an implant with exfiltration capabilities.
- These features include uploading/downloading files to/from a target, obtaining limited system information, finding a path out of the target (either dialup or direct connect).
- VALIDATOR can also delete itself via command or by built-in timer.

Source: FOXACID

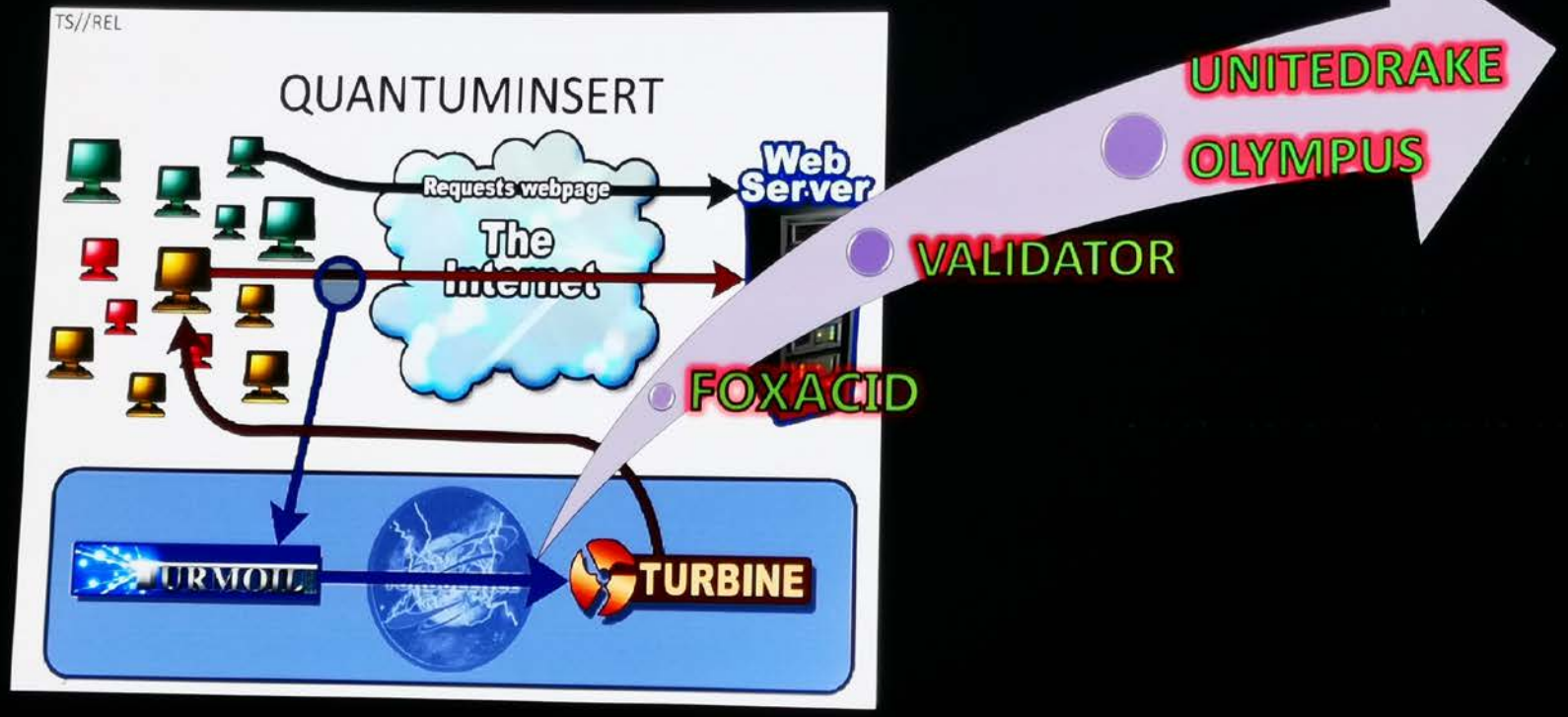
高复杂特种木马：
欧林巴斯（OLYMPUS）&
联合耙（UNITEDRAKE）

由VALIDATOR分发
高度复杂、插件化
高度隐蔽，持久驻留，无文件（Fileless）
深度收集目标系统信息
进行内网嗅探和渗透





Source1: APEX Active/Passive Exfiltration
Source2: https://assets.documentcloud.org/documents/3987443/The-Shaow-Brokers-UNITEDRAKE-Manual.pdf


TS//REL
QUANTUMINSERT
Requests webpage
Web Server
The Internet
TURMOIL
TURBINE
UNITEDRAKE
OLYMPUS
VALIDATOR
FOXACID


追踪NSA网络武器
震网：自2013
方程式：自2015
追踪：FOXACID / VAILDATOR / UNITEDRAKE

追踪FOXACID - VAILDATOR

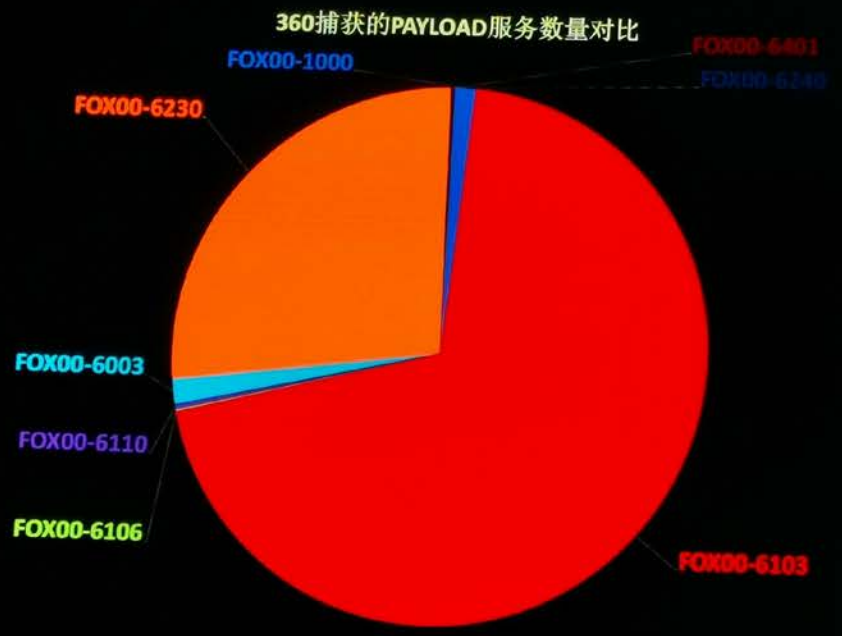
Payload ID命名规则

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
D R A F T

Once the new server is received, follow the below process to have MIT build the FOXACID Server.

- Request CDR Keys and domains for new server
- Create filters and directory in Clearcase for the new server
- Update the fa_install (located in Clearcase) with new server information
- Submit a RocHelp ticket for MIT to install Software in the following order: Server ***Plugins***Payloads***Val ID
- Install "keys" into C:\main\keys\
- Edit C:\main\config\server.xml
  - Updates include: CDR info (Verify IP and port, TA_ID, TE_ID, and IN_ID), list begin, list ends, set log forwarding to false
- Verify C:\main\config\deployment_types.xml
- Edit each payload config file
- Update C:\main\payloads\config\ids\[PAYLOAD_ID].txt (Ex. Server FOX00-6001 payload id = 600100000:600199999)
- Run fa_build_ops_disk.pl from Clearcase to upload new filters to thumbdrive. Then load updates on RAISEBED/WAITAUTO. If you're logging on to RAISEBED, upload from

Source: FOXACID-Server-SOP-Redacted



3.3.(TS//SI) FOXACID SERVERS AND SUPPORTED MISSIONS

Server	Mission	
XS10	YachtShop	
XS11	GCHQ MITM	英国GCHQ
FOX00-6000	*Test Server (Spam)*	
FOX00-6001	CT Spam	反恐
FOX00-6002	ME Spam	中东
FOX00-6003	AA Spam	亚太
FOX00-6004	RU Spam	俄罗斯
FOX00-6005	EU Spam	欧洲
FOX00-6100	*Test Server (MITM)*	
FOX00-6101	CT MITM	反恐
FOX00-6102	ME MITM	中东
FOX00-6103	AA MITM	亚太
FOX00-6104	RU MITM	俄罗斯
FOX00-6105	EU MITM	欧洲
FOX00-6106	CT-MAC	反恐
FOX00-6300	*Test Server (Enchanted)*	
FOX00-6401	CCNE China	中国
FOX00-6402	CCNE Russia	俄罗斯
FOX00-6403	CCNE Other	

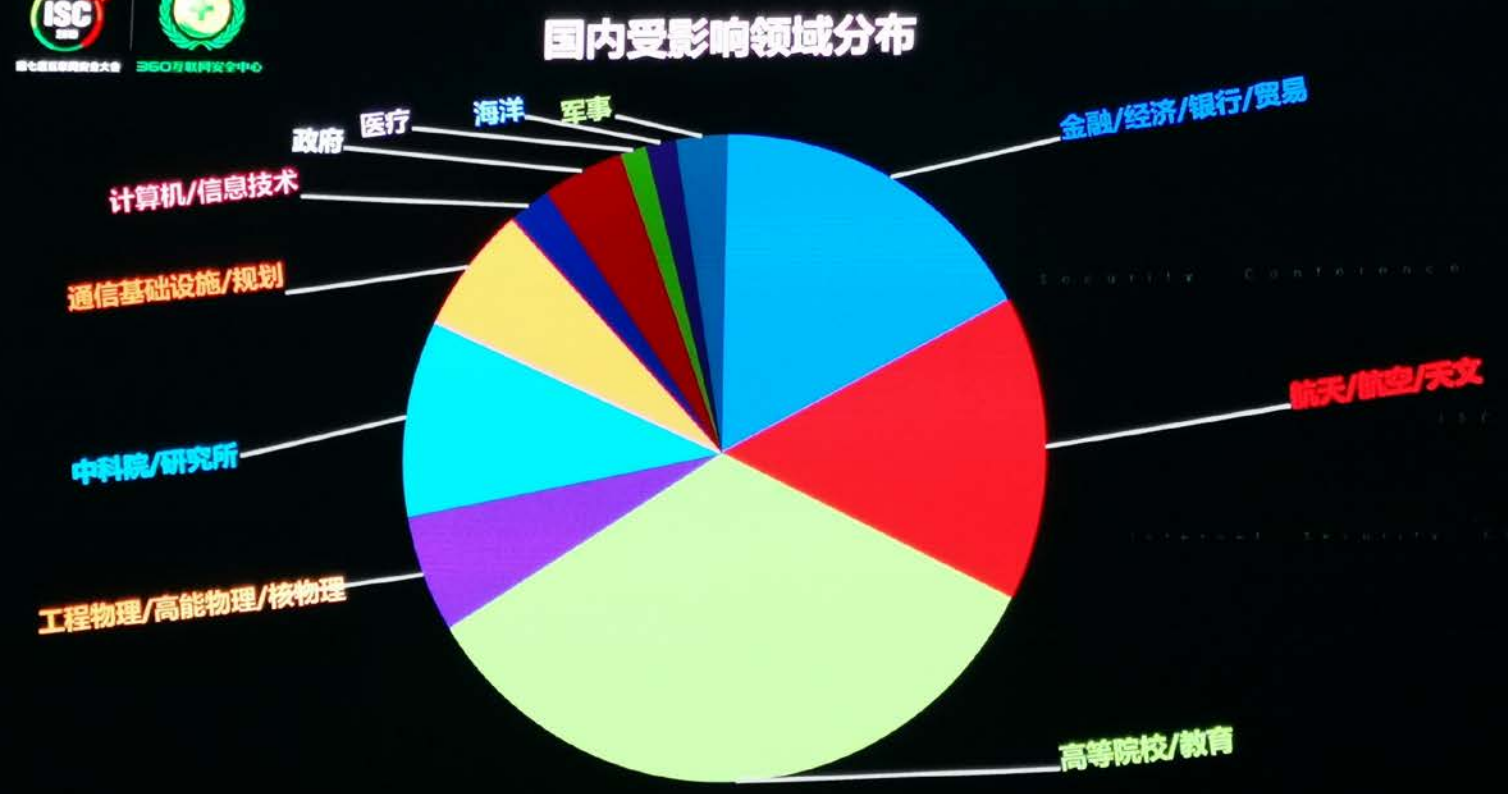
*****ENCHANTED Operations have been ceased as of week of 20100118*****

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
D R A F T

Source: FOXACID-Server-SOP-Redacted

国内受影响地域分布


北京 59.58%
陕西 21.74%
四川 6.51%
江苏 6.38%
上海 1.65%
辽宁 1.18%
广东 0.94%
天津 0.55%
浙江 0.31%
山东 0.24%
湖北 0.16%
贵州 0.16%
黑龙江 0.08%
内蒙古 0.08%
福建 0.08%
云南 0.08%
澳门 0.08%
吉林 0.08%
江西 0.08%
河北 0.08%
新疆
西藏
青海
甘肃
宁夏
内蒙古
黑龙江
吉林
辽宁
山西
河北
天津
山东
陕西
河南
安徽
江苏
上海
四川
重庆
湖北
浙江
湖南
江西
贵州
福建
云南
广东
广西
澳门
香港
海南
台湾
南海诸岛


国内受影响领域分布
金融/经济/银行/贸易
临天/航空/天文
高等院校/教育
工程物理/高能物理/核物理
中科院/研究所
通信基础设施/规划
计算机/信息技术
政府
医疗
海洋
军事

Payload ID差值分析法

FOXACID Server ID	ID最大值	ID最小值	ID差值
1000	1000-41952	1000-28269	13684
6003	6003-01160	6003-00217	944
6103	6103-13384	6103-01240	12145
6106	6106-04105	6106-04105	1
6110	6110-01791	6110-01414	378
6230	6230-003069	6230-000005	3065
6240	6240-001827	6240-000909	919
6401	6401-00000	6401-00000	1
TOTAL	N/A	N/A	31137

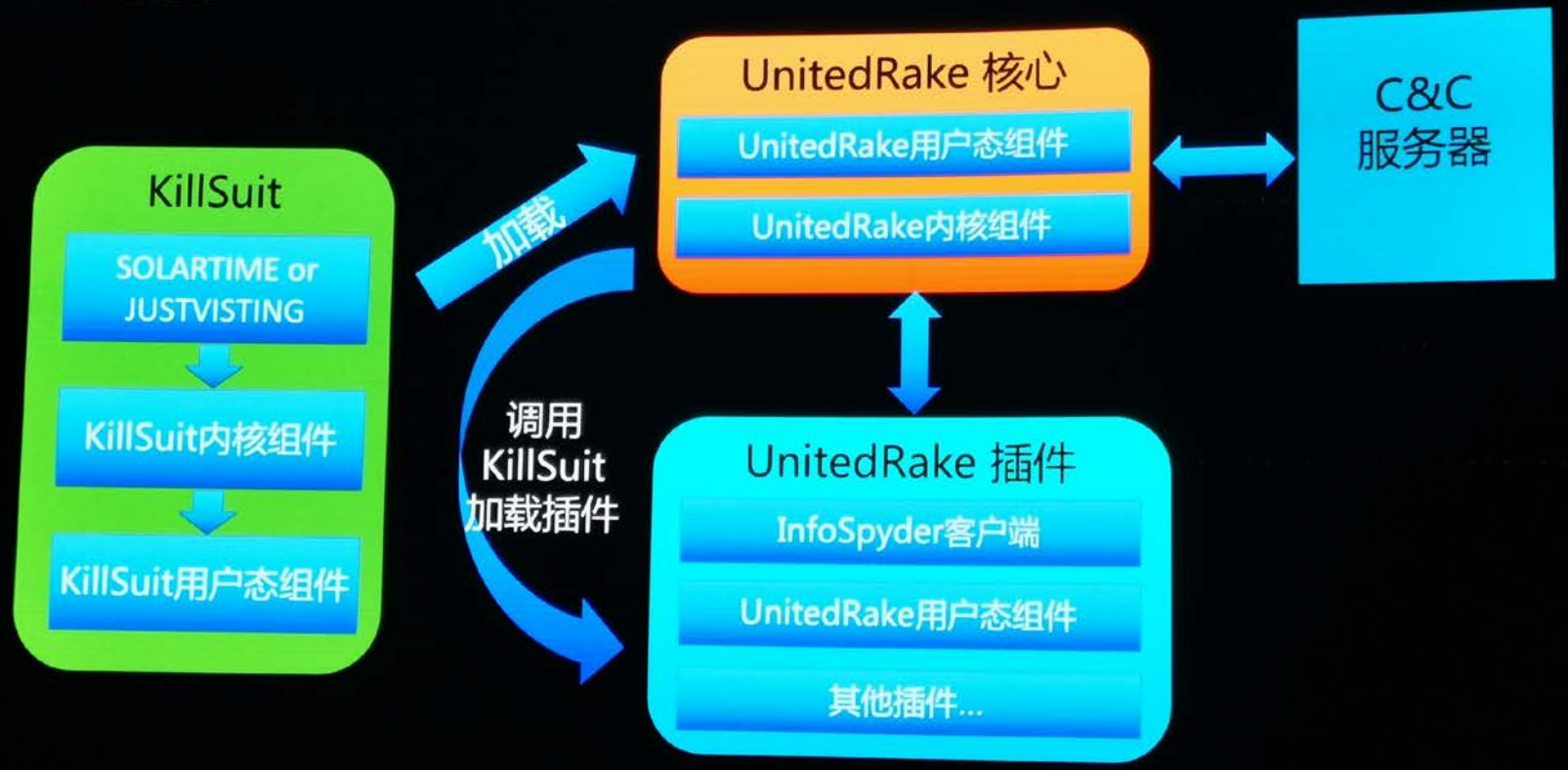
追踪UNITEDRAKE

TOP SECRET//COMINT//REL USA, FVEY

Bot Herding 101 – It's a Business

- Used Extensively for Illicit Means
  - Distributed Denial of Service (DDoS)
  - SPAM Operations
  - Financial Fraud
  - Intelligence Collection (Brazil, Russia, China, etc)
- Three Modes of Control
  - Phase 1 - IRC
  - Phase 2 - HTTP (OLYMPUS/UNITEDRAKE are Bots)
  - Phase 3 - Peer-to-Peer

追踪UNITEDRAKE

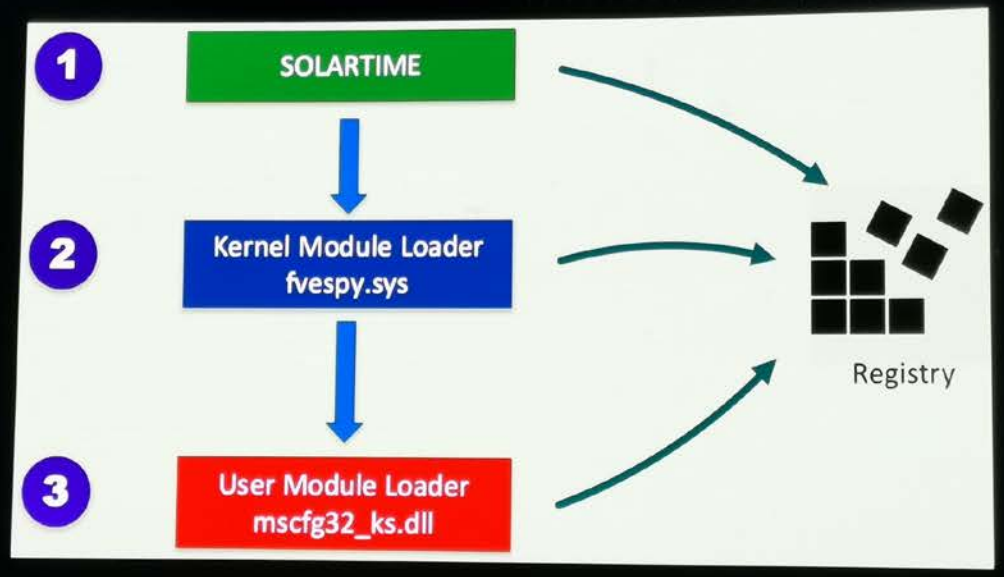


追踪UNITEDRAKE：KillSuit

持久化和权限维持框架

恶意程序加密存储和无文件加载

SOLARTIME: VBR Bootkit



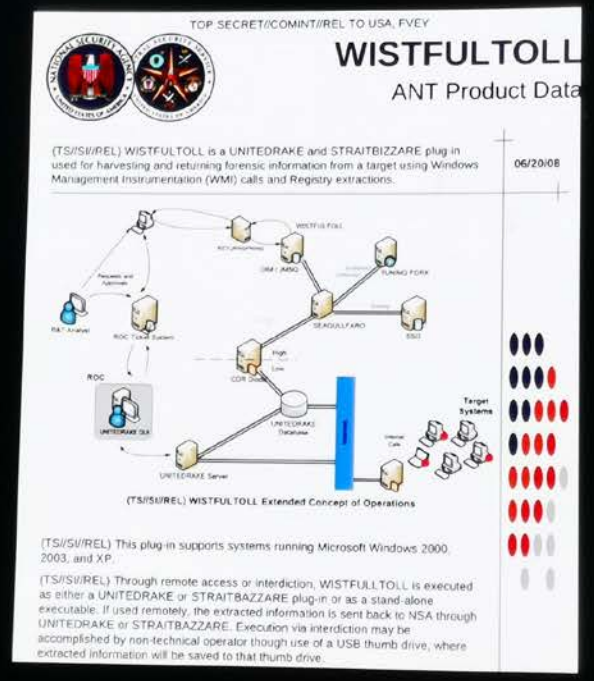
追踪UNITEDRAKE：组件

UnitedRake核心	模块ID	作用
MSCFG32_KS	0x4000	植入程序
ATMDKDRV	0x4001	核心通信控制驱动
LANGINFO32	0x4003	加载器

KillSuit组件	模块ID	作用
MPDKG32	0x7F32	用户态加载器
DRMKFLT	0x7F33	BH驱动
FVESPY	0x7F34	内核态加载器

UnitedRake插件	模块ID	作用
KHLP680W	0x8022	WhiteSpyder 文件和进程访问
CMIB158W	0x8024	InfoSpyder系统基本信息搜集
CMIB456W	0x8034	KrispyKreme VFS管理
KHLP807W	0x8040	NetSpyder 内网嗅探
KHLP760W	0x8050	DaytonSunday VFS加解密管理
KHLP733W	0x8058	WistfulToll 深度信息搜集和嗅探
KHLP866W	0x808A	SquashChunky2 压缩算法
VNETAPI	0x80BE	HTTP2通信
WEBMGR	0x80C6	ThermalDiffusion 浏览器信息搜集
WSHAPI	0x80CA	使用Winsocket通信

追踪UNITEDRAKE：WISTFULTOLL



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

WISTFULTOLL

ANT Product Data

(TS//SI//REL) WISTFULTOLL is a UNITEDRAKE and STRAITBIZZARE plug in used for harvesting and returning forensic information from a target using Windows Management Instrumentation (WMI) calls and Registry extractions.

06/20/08

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

(TS//SI//REL) This plug-in supports systems running Microsoft Windows 2000, 2003, and XP.

(TS//SI//REL) Through remote access or interdiction, WISTFULLTOLL is executed as either a UNITEDRAKE or STRAITBAZZARE plug-in or as a stand-alone executable. If used remotely, the extracted information is sent back to NSA through UNITEDRAKE or STRAITBAZZARE. Execution via interdiction may be accomplished by non-technical operator though use of a USB thumb drive, where extracted information will be saved to that thumb drive.

Source: ANT Product Data

追踪UNITEDRAKE：LCG算法

LCG（线性同余法）朴素的伪随机数生成算法

$$N_{j+1} = (A \times N_j + C) \bmod M$$

UNITEDRAKE常用的A/C值

A	C	
0x19660D	0x3C6EF35F	常用
0x1B0F6733	0x3501BF01	360独立发现
0x6033A96D	0xDD483B8F	安天分析GrayFish

Source: Analysis on the Encryption Techniques of EQUATION Components, Antiy

唯一困扰TAO的安全公司？

IRATEMONK

可感染西数、希捷、迈拓、三星、松下等硬盘固件的NSA武器

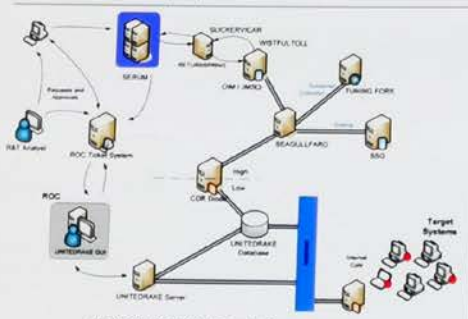
进行持久驻留，即使格式化整盘也无法清除

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



(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

[edit] (U//FOUO) CASTLECRASHER

(TS//SI//REL) CASTLECRASHER is the primary technique used in executing DNT Windows payloads from all payload persistence techniques (i.e. IRATEMONK and SIERRAMISTFREE). It is all Windows native mode code built using Visual Studio. CASTLECRASHER has many advanced techniques in it including thread injection and anti-stack backtracing. In many cases, CASTLECRASHER is closer to the DNT style kernel work than it is to traditional Persistence work. While the current version is quite robust, there are several features that need to be added:

- (TS//SI//REL) Currently CASTLECRASHER doesn't work against systems with 360 Safe installed. We need to find a way around this even if it involves using the older Windows service method of execution. This

6

/InternProjects - WikiInfo

will more than likely require a refactoring of how the configuration data of CASTLECRASHER is stored.

Source1: ANT Product Data
Source2: S3285/Intern Projects


ATIP（360高级威胁情报平台）
高级威胁情报
预警
未知高级攻击探测
高级攻击实时防护
...
360安全大脑

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票