网络安全技术及产业发展新趋势

中国电子科技集团公司第三十研究所 饶志宏

CETC

内容大纲

Table of Contents

CETC

PART 01

网络空间安全威胁
四新特点

四新特点

定向性

持续性

复杂性

破坏性

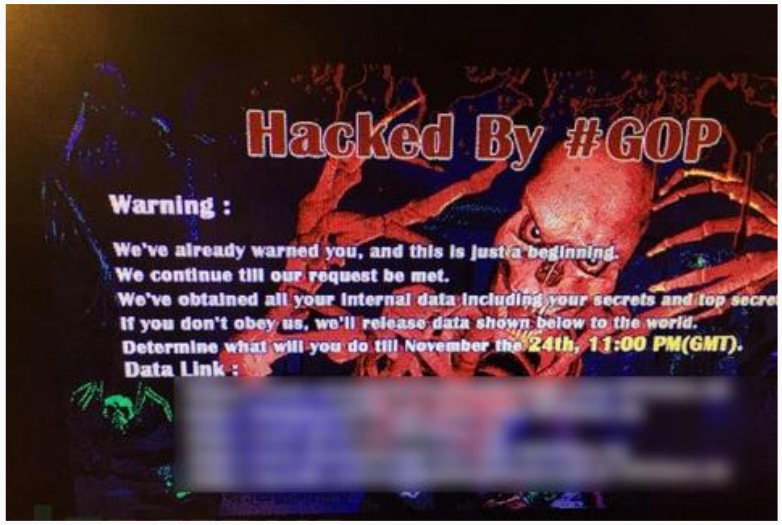
定向性

2014年11月 Regin病毒惊现网络

对于首款网络攻击平台Regin经卡巴斯基调查显示，攻击者的主要目标为电信运营商、政府、金融机构、研究组织、跨国政治团体以及从事高级数学/解密研究的个人。

2014年12月 索尼公司遭黑客攻击

日本电子巨头索尼公司位于美国加州的索尼电影娱乐公司遭到黑客袭击，内部计算机系统遭破坏，大量资料遭泄露。这是美国大型企业历史上遭遇过的最大规模网络攻击。



持续性

APT(Advanced Persistent Threat)

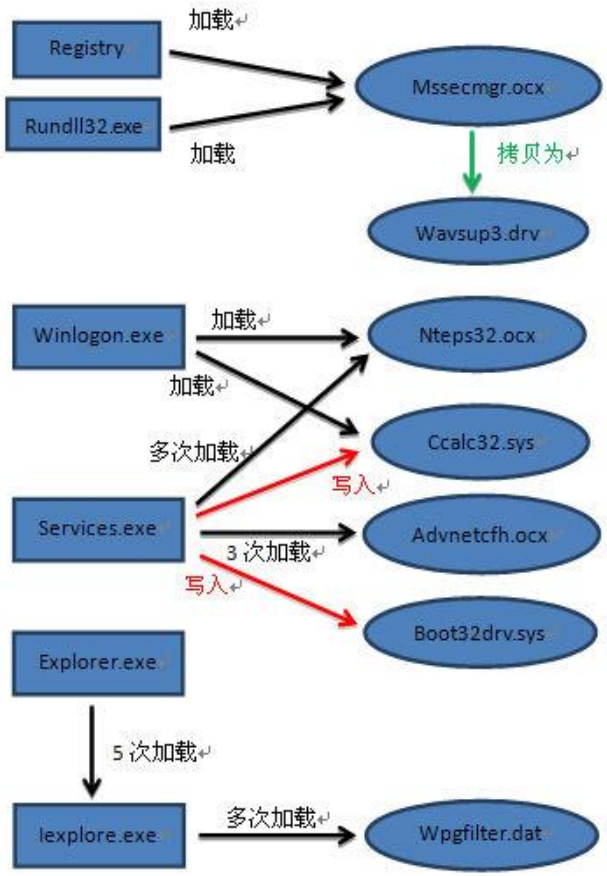
Flame | Duqu | Gauss | Stuxnet

病毒名称	释放时间	发现时间
Stuxnet	2009年6月	2010年7月
Duqu	2007年或2008年？	2011年8月
Flame	2007年12月之前？	2012年5月

CETC

复杂性

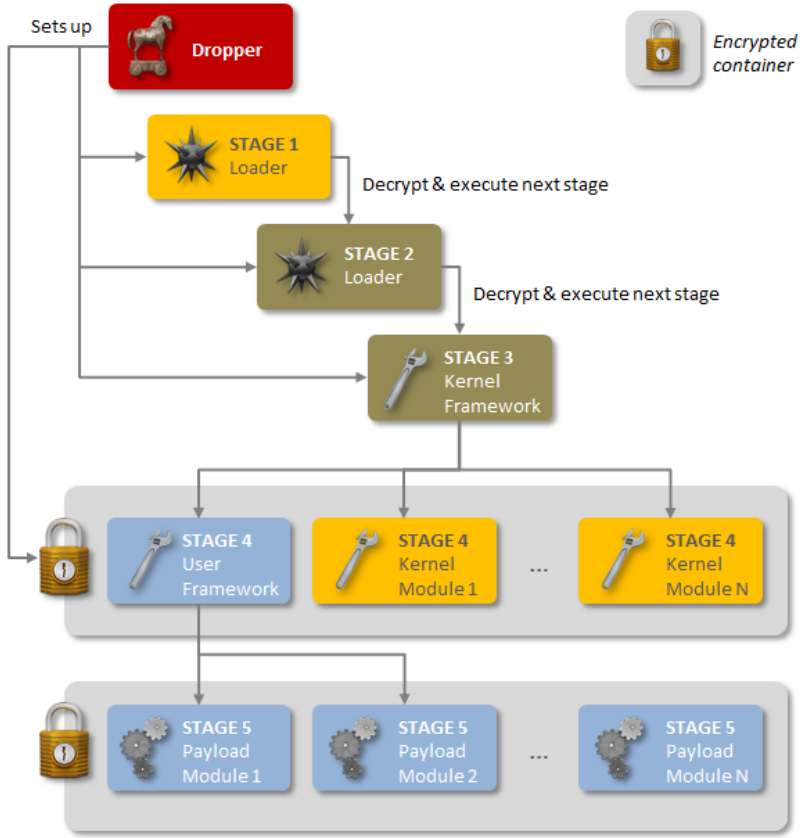
Flame



我们将需要几年的时间去完全明白Flame 20MB大小的文件。

——卡巴斯基《Flame病毒问答》

Regin



Regin 成为历史上最复杂的恶意代码。

（来源：赛门铁克）

破坏性

震网被检测

2010年6月，据德国媒体报道震网（Stuxnet）病毒已感染了全球超过 45000个网络，其中60%的受害主机位于伊朗境内，该病毒可以破坏世界各国的化工、发电和电力传输企业所使用的核心生产控制电脑软件。

索尼被攻击

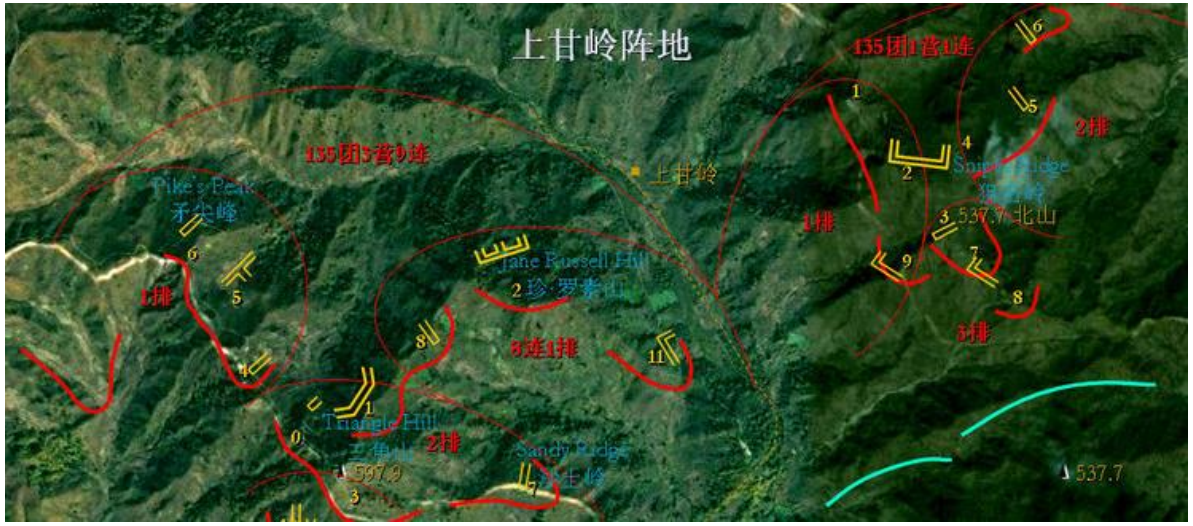
据美国媒体报道，索尼影业娱乐公司泄露的文件包括了超过4.7万索尼当前和前职员的社会安全码（SSN，相当于中国的身份证号码），其中就包括多位名人的社会安全码。

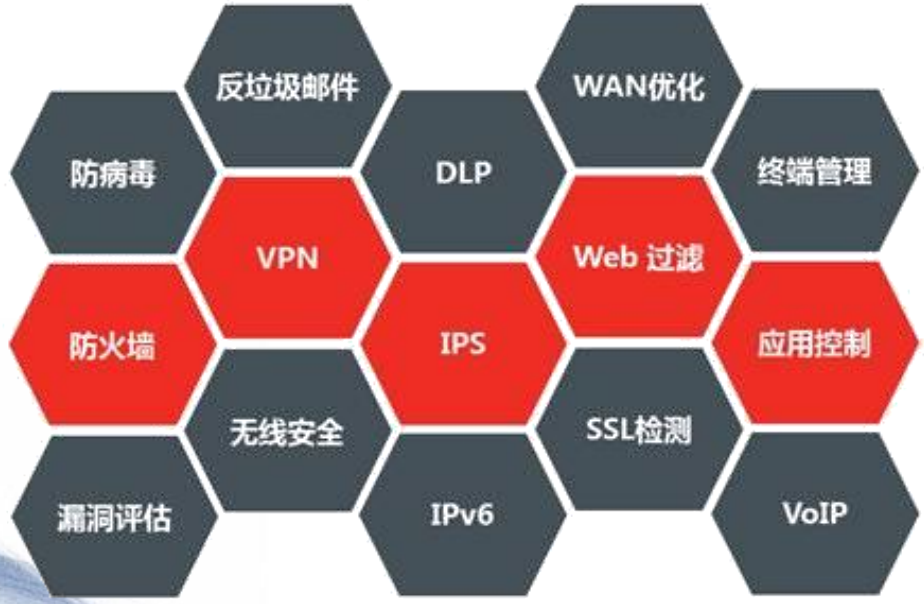
PART 02

网络安全技术
四防御

四防御

体系防御

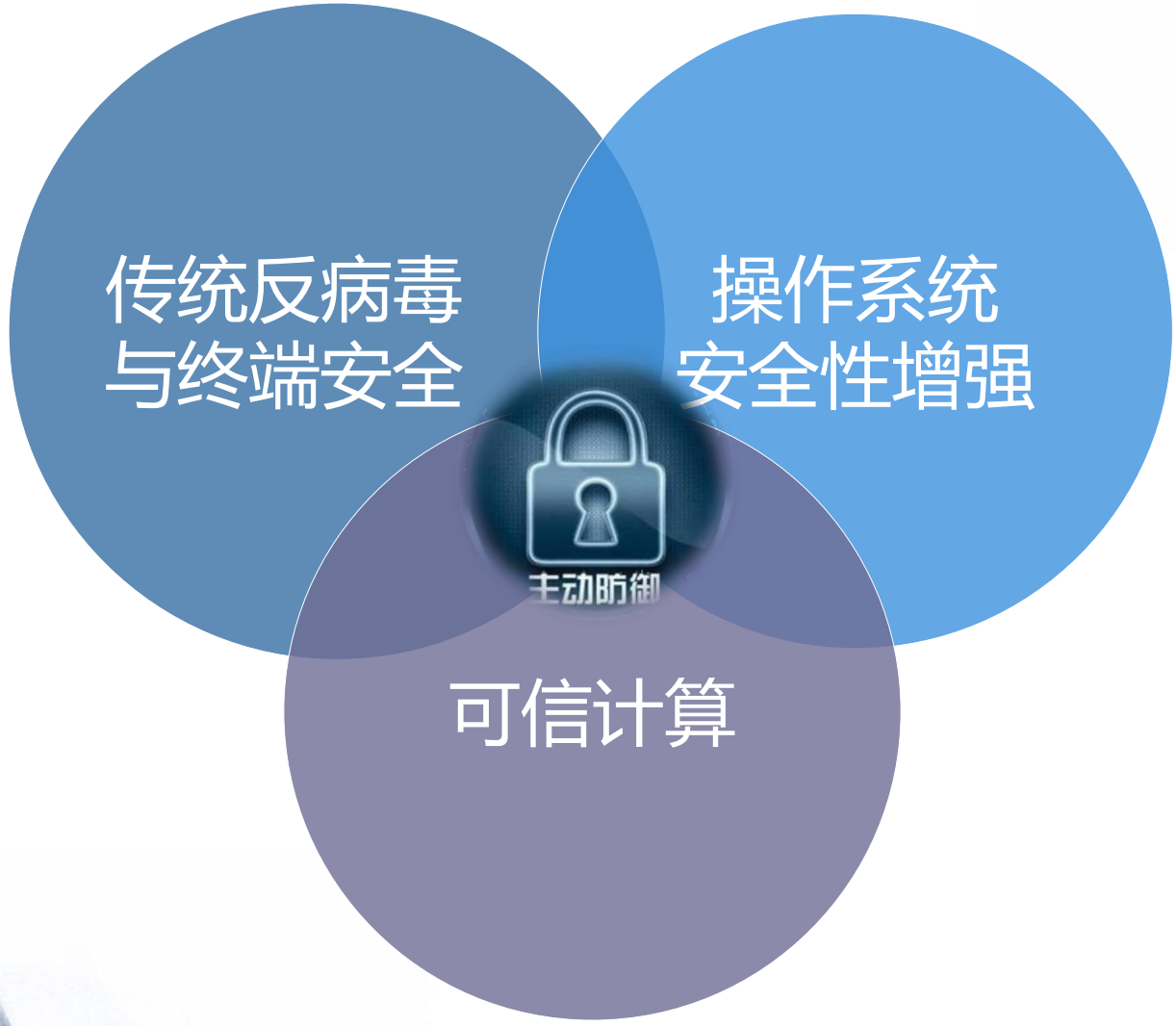




从环节拼凑到纵深防御

CETC

主动防御



各安全层面都在改善主动防御能力

CETC

协同云防御

中国

CETC

360 www.360.cn

金山安全 Kingsoft Security

ANTIY 安天

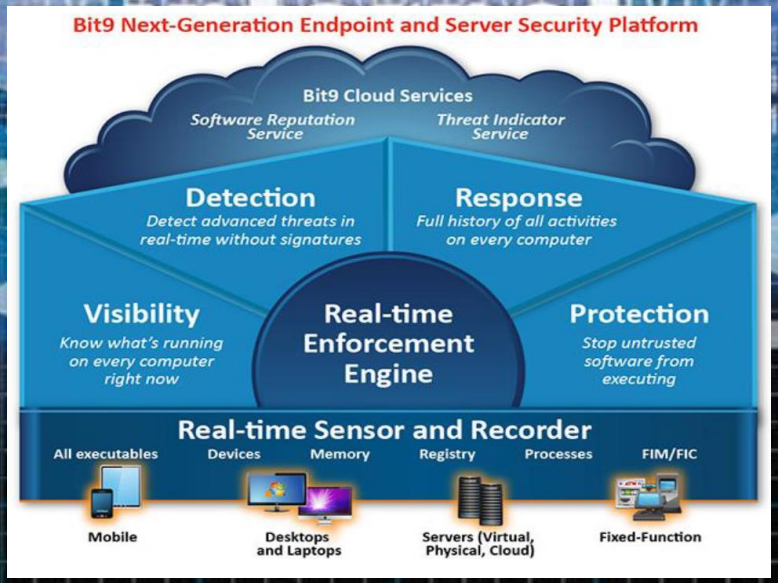
.....

美国

FireEye

Bit9

.....



白名单+安全基线
私有云鉴定
终端防护

CETC

大数据防御

大数据即是需要安全保护的对象，也是安全的方法。

CETC

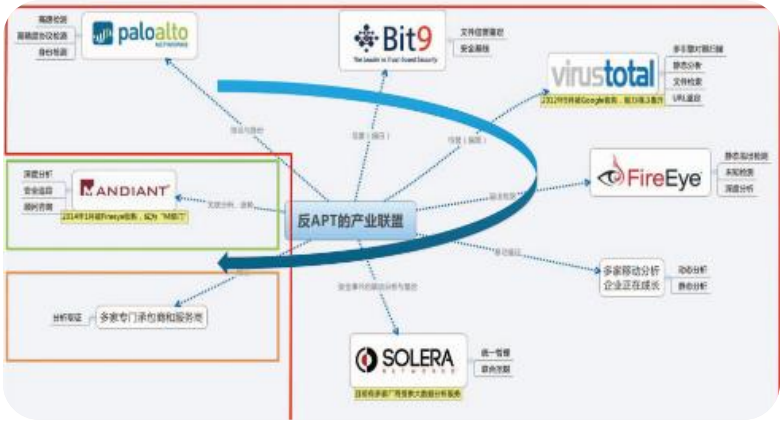
PART 03

网络安全企业新四化

新四化

联盟化

美国



美国的安全厂商已经形成了一个应对APT的产业资源体系和事实上的利益同盟。

注：图引自《大战略基石-美国信息安全产业格局的解析》。

中国

- 操作系统联盟
- 可信计算联盟
- 中关村企业联盟
- ……

联盟化已经成为全球化趋势，国内企业也已逐渐在各行业领域形成了大量同盟组织。

CETC

自主可控化

建立屏障

- 反病毒引擎
- 防火墙
- 入侵检测
- VPN
- ……

形成基础

- 操作系统
- CPU
- 服务器
- 交换机
- ……

CETC

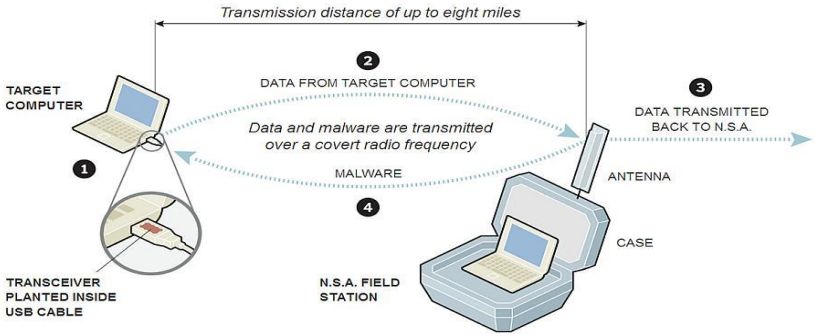
攻防兼备化

攻

防

How the N.S.A. Uses Radio Frequencies to Penetrate Computers

The N.S.A. and the Pentagon's Cyber Command have implanted nearly 100,000 "computer network exploits" around the world, but the hardest problem is getting inside machines isolated from outside communications.



1. Tiny transceivers are built into USB plugs and inserted into target computers. Small circuit boards may be placed in the computers themselves.

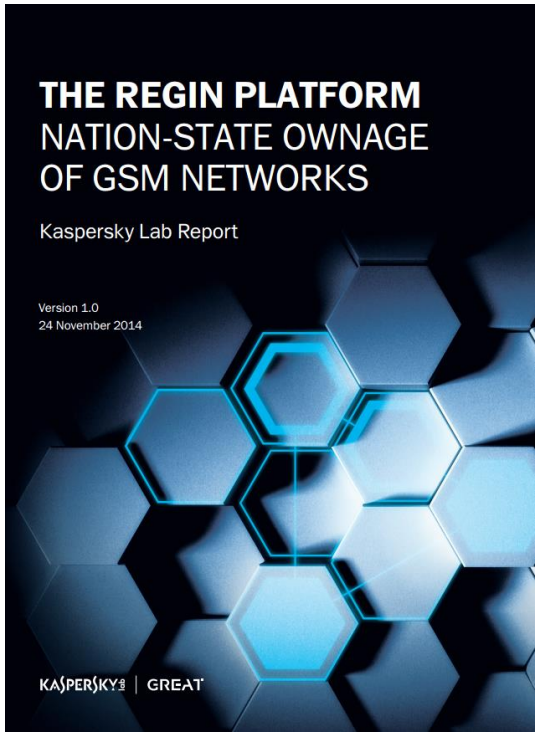
2. The transceivers communicate with a briefcase- size N.S.A. field station, or hidden relay station, up to eight miles away.

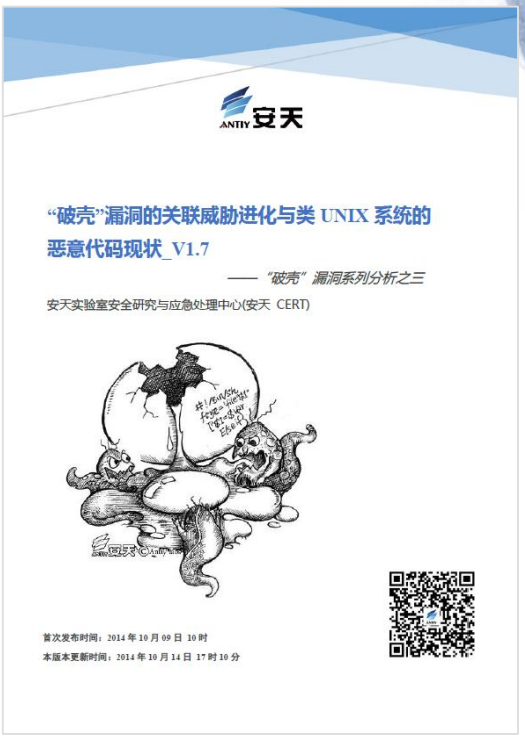
3. The field station communicates back to the N.S.A.'s Remote Operations Center.

4. It can also transmit malware, including the kind used in attacks against Iran's nuclear facilities.

CETC

体贴服务化





个性化、定制化、以人为核心的分析、响应对抗能力。

CETC

PART 04

中国网安未来新发展

CETC

结束语

THANKS

13608184980 China_rao charao@tom.com