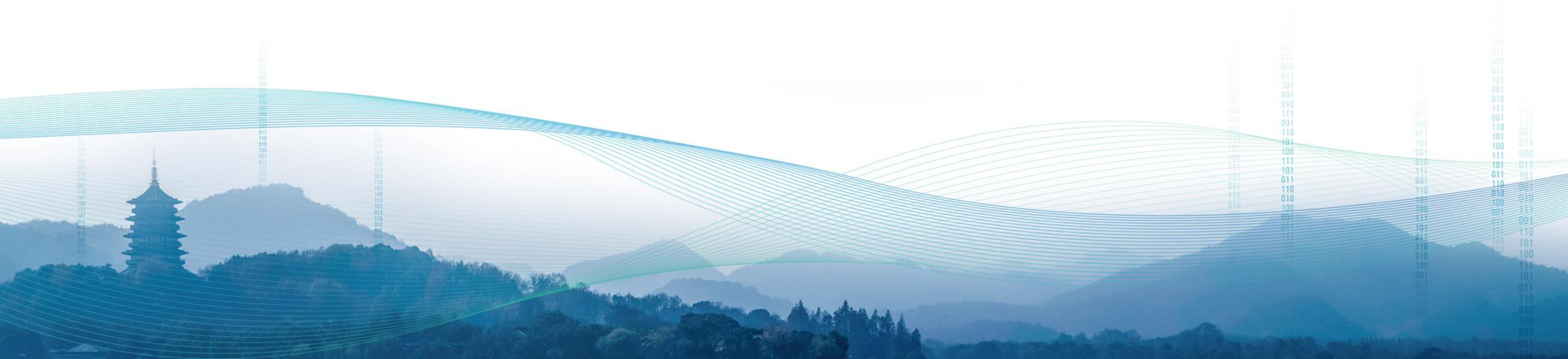
2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

2018威胁态势回顾与2019展望

卡巴斯基 董岩

2018年重大网络攻击回顾



2018年初冬季奥运会

后果严重

- 50台服务器被破坏
- 超过300台服务器受影响
- Wi-Fi, IPTV, Email 等系统瘫痪
- 4大类52种服务被迫停止

及时响应

- 距离开幕仅剩12小时
- 恢复应急设施
- 从灾难恢复中心恢复了数据
- 12小时内成功恢复

嫁祸于人

National Security

Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say

The PyeongChang 2018 Winter Olympics opened with a dazzling ceremony Feb. 9. (Pawel Kopczynski/Reuters)

By Ellen Nakashima February 24 Email the author

顶尖APT组织——Sofacy/Zebracy

2018年新动向：

- Gamefish 恶意软件
- 新版DealersChoice

新框架：

- Computrace/LoJack
- Cannon木马
- Zebracy高度活跃

顶尖APT组织——Lazarus/BlueNoroff

Lazarus/BlueNoroff以直接经济收益为目标积极攻击不同的金融组织，如加密货币交易所和赌场，目标地区包括土耳其、亚洲与南美洲。

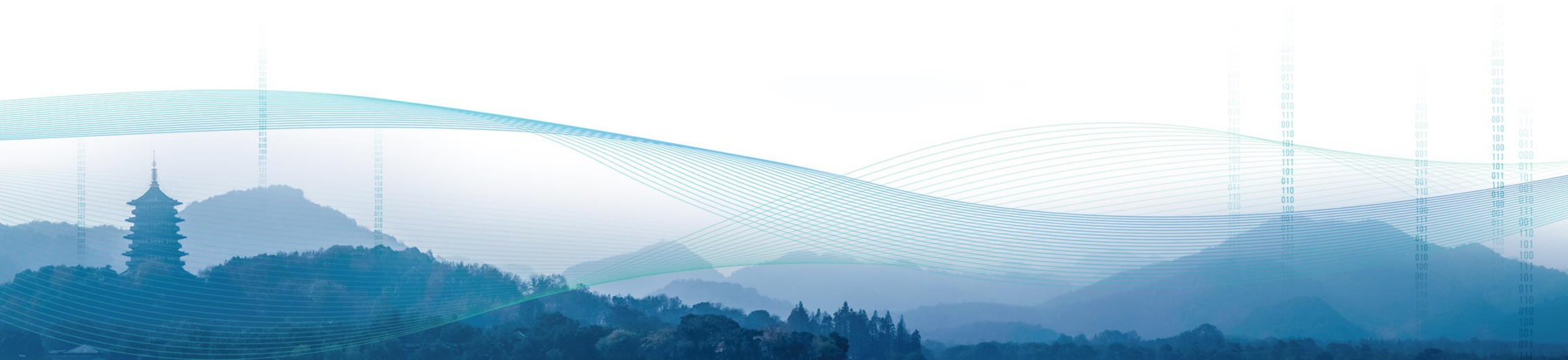
其新部署的恶意软件被称为ThreatNeedle。

重回视线 —— 亚洲篇

Scarcruft 针对三星手机用户部署0日Android恶意软件以及一个叫做PoorWeb的后门

DarkHotel 积极攻击高价值目标。我们分析认为 DarkHotel和Konni/NOKKI可能存在联系

OceanLotus海莲花针对南亚高价值目标积极部署水坑攻击



不止这些！

去年亚洲是APT攻击热点地区。许多新的（或已不太新）的攻击组织都很活跃。他们的攻击行动复杂程度不一，但通常较为低端：

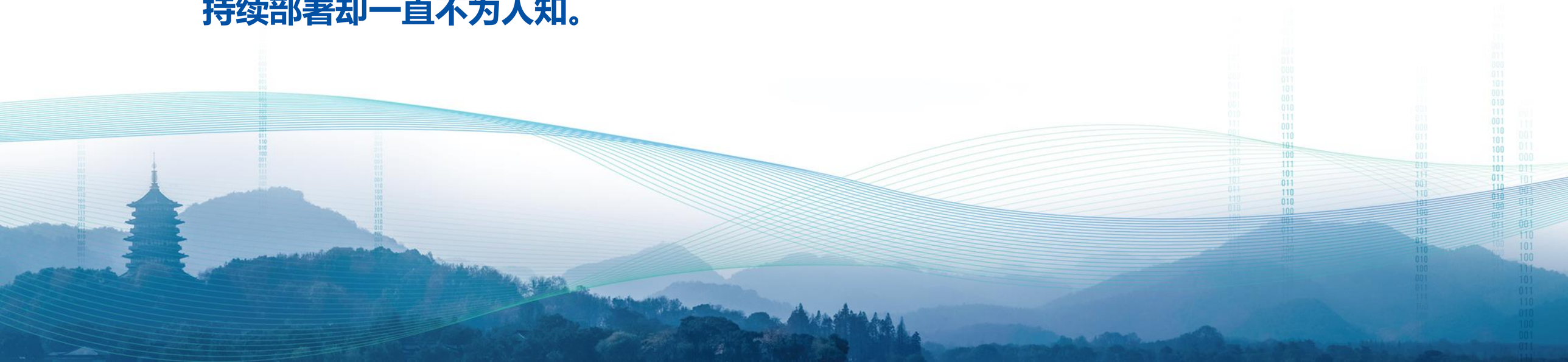
- ShaggyPanther
- Sidewinder
- CardinalLizard
- TropicTrooper
- DroppingElephant
- Rancor
- Tick group
- NineBlog
- Flyfox
- CactusPete

其它重大安全事件

VPNFilter：以网络硬件作为攻击目标，许多攻击者也在开发部署此类攻击

对金融行业的攻击没有太大变化。Carbanak组织成员的被捕对FIN7或CobaltGoblin的攻击行动没有产生影响

工控系统相关恶意软件与攻击也时有发生。去年发现的Triton/Trisis就可能在持续部署却一直不为人知。



国内勒索软件活跃

春节刚过黑客就开工了？勒索病毒入侵儿童医院 系统瘫痪看病难

2018-02-27 18:00　　勒索病毒

春节假期回归工作可是没有工作状态？要知道黑客们过完年可是马上就投入工作中

据微博网友爆料，国内一家省级儿童医院24日出现系统瘫痪的情况。近期儿童流感
儿童医院人满为患，系统瘫痪导致许多患者无法正常就医，影响极大。

高危预警！多地发生GlobeImposter勒索病毒“投毒”攻击

2018年08月23日17:35　来源：中国经济网　　分享到：

```
Windows Microsoft Microsoft Help Windows App Certification Kit Windows Defe
Windows Phone Kits Windows Phone Silverlight Kits Windows Photo Viewer Windows Portable Devices
ee Avira spytech software sysconfig Avast Dr.Web Symantec Symantec_Client_Security system volume
YandexBrowser ntldr Wsus ProgramData .Ser..4db..4dd..4d..4mp,.a .helpdcrpt@cock.
log dll lnk sys C:\Users\root\Desktop\vlad_len@exploit.im\patch.tmp
```

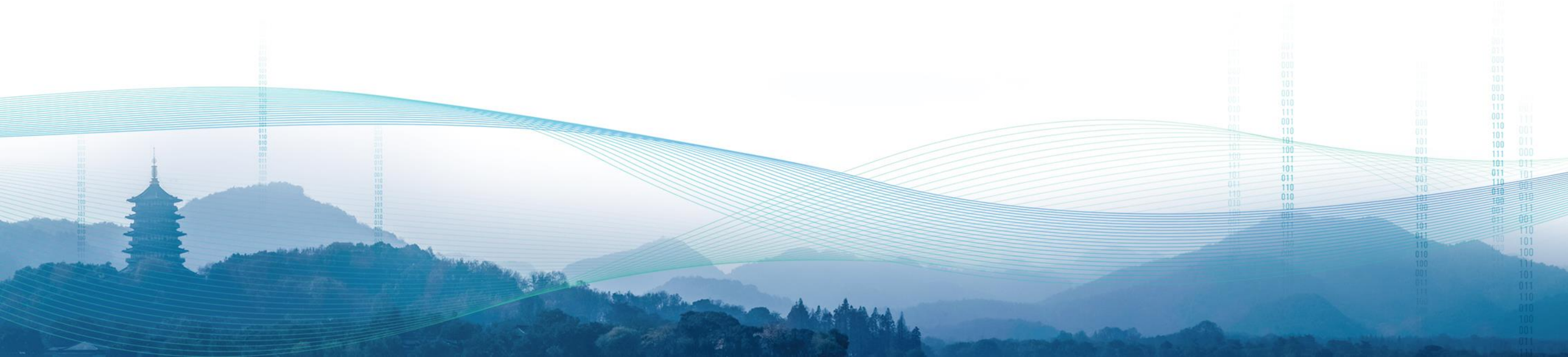
!logs	KPortScan 3.0	mimikatz
passrecpk	PH new	PHx86
!start.cmd	chinapass.txt	credentials.txt
good.txt	Java.exe	KPortScan 3.0.exe
m101.exe	NetworkShare_local_range.exe	nl.exe
pass.exe	Passwords.txt	PCHunter64.exe
results.txt	servers.txt	settings.ini
usr.txt		

Посл. активность: 10.01.19
Регистрация: 17.04.18
Сообщения: 4
JID: vlad_len@exploit.im
Telegram: VLADLEN_L
Покупки через Гарант-сервис: 0
Продажи через Гарант-сервис: 0

- **RDP Brute + RDP Recognizer** by z668
  Брут по логинам, паролям; Recognizer
  Тема: https://forum.exploit.in/index.php?showtopic=101024
- **RDP PortScanner** (Coded by z668)
  Консольный софт для проверки списка IP на наличие протокола RDP на порту.
  Тема: https://forum.exploit.in/index.php?showtopic=125001
- **NetworkShare.exe**
  Подсоединяет к дедику все диски с локальных машин.
- **Эффективные логины/пароли** для брута (собственноручно составленые).

Внимание! Я не просто привяжу софт к вашему железу, а **передам вам права владельца на софт**. То есть, я попрошу z668@exploit.im передать права собственника на софт вам. перепривязывать софт или продать софт другому человеку.

展望2019



1 不再有大型APT

典型的大型APT都进行了重构

溯源不再是首要问题

部署在盲区领域

顶级攻击者会利用外部资源和人才

顶级APT攻击者转入新思维模式

2 网络硬件

攻击难以检测和监控，已经在发生！

主要攻击组织都在开发自己的工具

威胁基础网络硬件

日益增长的IoT僵尸网络

网络硬件层面的攻击收效甚好，不能忽略

3 曝光示众与政治游戏

如何回击网络攻击?

公开私人信息、指控

后果令攻击者三思并打消后来者念头

美国网战司令部公布恶意软件IoC

公开APT攻击细节将被用于外交战

4 出现新APT攻击组织

想做网络间谍? 门槛从未如此之低

APT攻击者的两极：超牛的老手 vs 饥饿的新手

新来者有自己的方法入侵，而受害者也在提升防御手段

新来者使用公开的工具/框架与大型 APT组织争食

5 零环之内

去年发现的CPU漏洞打开了新的攻击之门，而现有安全机制几乎无法发现

攻击SMM的PoC早已存在。可能已经有SMM的漏洞被利用而我们尚未发现?

同理于虚拟化或UEFI恶意软件

贴近硬件层面的攻击极难检测

6 感染途径

渔叉式钓鱼仍然是主要的初始感染途径

大型社交网络泄露出的信息已经进入地下市场

而泄露的信息可以提升渔叉式钓鱼攻击的效果

我们相信渔叉式钓鱼仍将是最主要的感染途径

7 破坏性恶意软件

对于许多攻击组织来说破坏性恶意软件属于标配

既用于地缘战略攻击也用于销毁痕迹

也许已经有关键基础设施被植入，只等攻击者一声令下?

此类攻击将更为精准且在大规模冲突种作为备选

8 还有移动设备...

有钱的去高价购买iOS零日漏洞

没钱的就去搞rogue MDM服务器

iOS 泄漏的iBoot代码可能能帮助攻击者找到新的漏洞

我们仍然能够看到入侵移动设备的新方式

总结

大型APT组织转入新思维模式

新的APT攻击者则使用公开的工具/框架

恶意软件隐藏于（网络）硬件

曝光网络攻击用于外事交锋

THANK YOU

谢　　谢　　观　　看