网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

2021年网络安全威胁回顾

——安天2021年网络安全年报（预发布版）内容提要

安天 | 安天副总工 / 李柏松

01 APT

APT攻击活动阴谋涌动、阳谋尽显；

利用移动设备攻击成常态，中东、南亚演绎高级威胁；

松散的情报引用使得更多的归因结果不严谨或不可靠。

全球APT攻击行动、组织归属地理位置分布图

中东地区
- Urpage
- EmpireMonkey
- Bahamut
- Group WITRE
- Molerats/灵猫

哈萨克斯坦
- 黄金雕/APT-C-34
- 毒针/APT-C-31

俄罗斯
- TRITON（海渊）
- Dukes
- GreyEnergy
- BlackEnergy（黑色能量）
- WhiteBear（白熊）
- Inception Framework
- Gamaredon Group
- FIN7
- Sednit
- Turla（图拉）
- DustSquad
- Gamaredon Group
- APT-28
- SandWorm（沙虫）
- Earworm
- Grim Spider
- BuhTrap
- Cobalt group
- TA505
- Wizard Spider
- Lunar Spider
- RTM
- SaintBear
- hades
- Evil Corp
- APT-29
- Callisto
- UNC1151

美国
- 方程式
- Unit 8200
- Pizzo Spider
- Project Sauron
- Lamberts

墨西哥
- leetMX

未知
- REvil
- TeamTnT
- UNC2452
- TA800
- Kek Security
- FIN8
- Mirrorthief
- TA551
- HEXANE
- Evilnum
- UNC1945
- Indra
- Molerats
- LuminousMoth
- Cyrus
- Muhstik
- LOREC53
- TH-261
- CloudFall
- FIN12
- Harvester
- Chimera
- TOOHASH
- Kasablanka
- TA511
- 利刃鹰
- APT-Q-42
- UNC2546
- UNC2198
- MKLG行动
- Zebra2104
- UNC2628
- UNC2529
- 恶流行动-EvilFlow
- DarkOxide
- Earth Wendiao
- LazyScripter
- Metamorfo
- ReconHellcat
- TA2722
- TA543
- MysterySnail
- GOLD WINTER
- Ferocious Kitten
- Operation ElectroRAT
- ChamelGang
- 艾叶豹组织(Snow leopard)
- Operation 'Harvest'
- FamousSparrow
- 金睛兽
- Hydro Jlin campaign
- TA544
- Operation Spalax
- BazaLoader campaign
- Praying Mantis
- SilverFish
- 幻鼠
- DarkSide
- UNC2465
- Operation TunnelSnake
- Operation Kremlin
- wastedLoader Campaign
- Aurora campaign
- Operation NightScout
- TA575
- EICAR Group
- Operation WildPressure
- UNC2447
- Operation Eagle Eye
- Operation Overtrap
- TA2721
- IndigoZebra
- Operation FakeGuard
- Operation "Armor Piercer"
- PuzzleMaker
- 金眼狗/GoldenEyeDog
- SparklingGoblin
- Magecart Group 12
- OPERATION MASKFACE
- Water Pamola
- Roaming Mantis
- Void Balaur
- MosesStaff
- Mummy Spider
- EGoManiac
- Tardigrade
- BackdoorDiplomacy

法国
- Animal Farm(动物农场)
- JIIN

乌克兰
- Operation Groundbait Project Sauron
- Operation Poison Needles
- Volodya
- 鲸鹭行动
- 卢甘斯克组织

西班牙
- The Mask

东亚地区
- 莱琼洞/APT-C-59

白俄罗斯
- Andromeda Spider
- UNC1151

意大利
- Anon Italia
- LulzSec Italia
- Operation Poisoned News
- Operation Pistacchietto
- Docless Vietnam
- Hacking Team

朝鲜
- Kim Soo-ki
- Honeybee
- TA406
- Crafty Panda
- Stolen Pencil
- 洋葱狗/OnionDog
- Lazarus Group(拉撒路)
- 危险密码/DangerousPassword
- FASTCash
- APT-37
- TA406
- Kimsuky
- Kulak
- APT-Q-12（伪猎者）

突尼斯
- Corsair Jackal
- Fallaga Team

中国台湾地区
- 绿斑（毒云藤）
- 蓝宝菇（APT-C-12）

韩国
- 黑店/DarkHotel
- Konni
- 虎水榴(DarkHotel)

利比亚
- Libyan Scorpions

阿尔及利亚
- 北菲狐

巴勒斯坦
- Molerats（灵猫）

以色列
- SandCat
- Flowershop

罗马尼亚
- FIN4

越南
- 海莲花

马来西亚
- DragonForce Malaysia

印度尼西亚
- Habil Moonz

菲律宾
- CyberGhost404
- Pinoy LulzSec

黎巴嫩
- Dark Caracal
- Reuse team

沙特阿拉伯
- OurMine
- 黄金鼠/APT-C-27

伊朗
- APT35
- APT39
- 潜盗者
- Flying Kitten
- Clever Kitten
- 污水/MuddyWater
- APT34
- Agrius
- LazyMeerkat
- Leafminer
- xHunt
- Domestic Kitten
- Hexane
- TA456
- ITG18
- PIONEER KITTEN
- DEV-0343
- Boss Spider
- Shamoon
- Cobalt Dickens
- DEV-0343
- 美人鱼/APT-C-07
- Group 42
- Leafminer
- MalKamak

巴基斯坦
- Gnosticplayers
- APT-36
- Stealth Mango and Tangelo
- Gorgon
- SideCopy
- 三边行动

阿根廷
- Anonymous Argentina

尼日利亚
- london blue
- SWEED
- SilverTerrier
- 尼日利亚黑客组织
- Operation Layover

土耳其
- StrongPity
- 图兰军

印度
- APT_CNC
- 幼象
- 苦象/BITTER
- 孔夫子/Confucius
- CNC（APT-C-48）
- Trianguium
- 猎天行动
- 肚脑虫/APT-C-35
- 响尾蛇/SideWinder
- Operation Vikrant
- Bahamut
- 腾云蛇
- APT-Q-42
- 白象

巴西
- DEMONSAD
- Poseidon Group
- NEWSEC GROUP
- Pryzraky Group
- Guildma
- Sprek3rsSec

阿拉伯联合酋长国
- FruityArmor
- Vikingdom

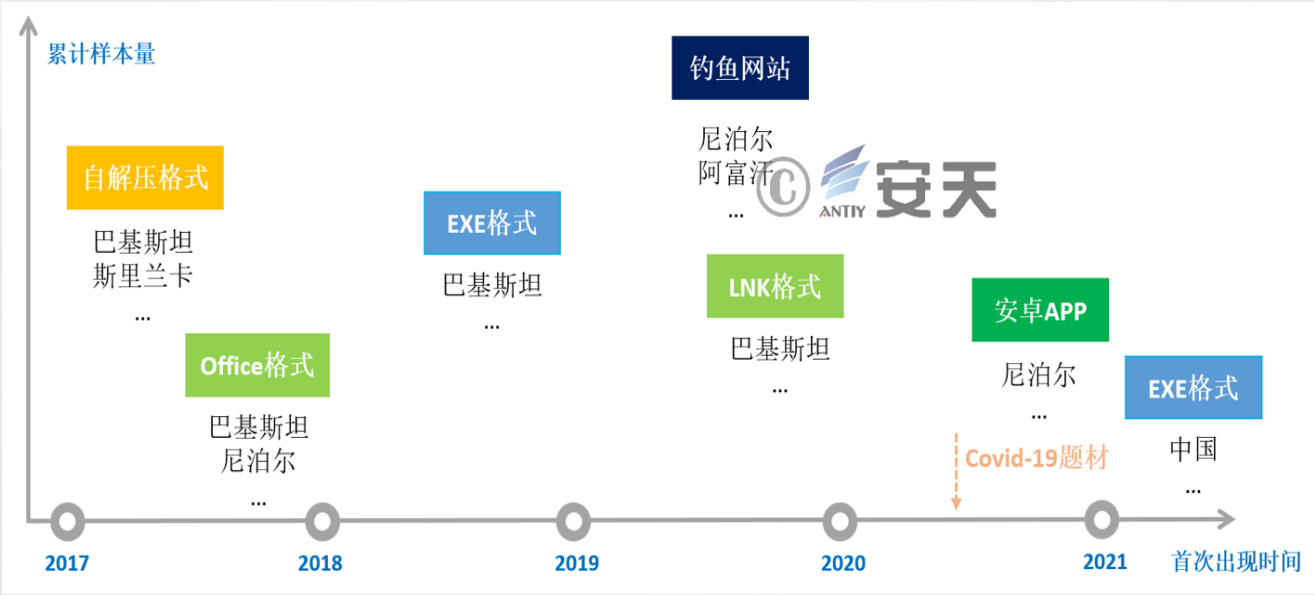
叙利亚
- 拍拍熊/APT-C-37
- Syrian Malware Team

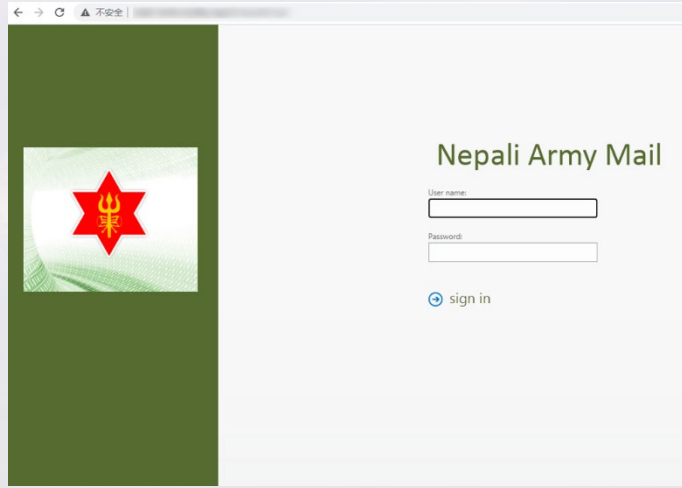
黄色的字是2021年活动的攻击组织　● APT组织

2021年网络安全威胁回顾 - APT

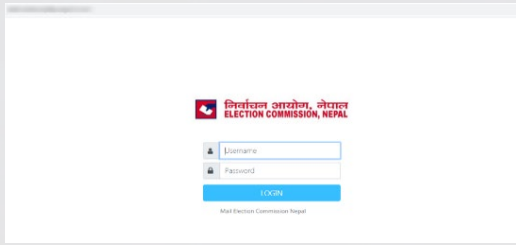
利用移动设备攻击成常态，中东、南亚演绎高级威胁

——“幼象”组织在南亚地区的网络攻击活动分析





仿冒尼泊尔军队邮件系统



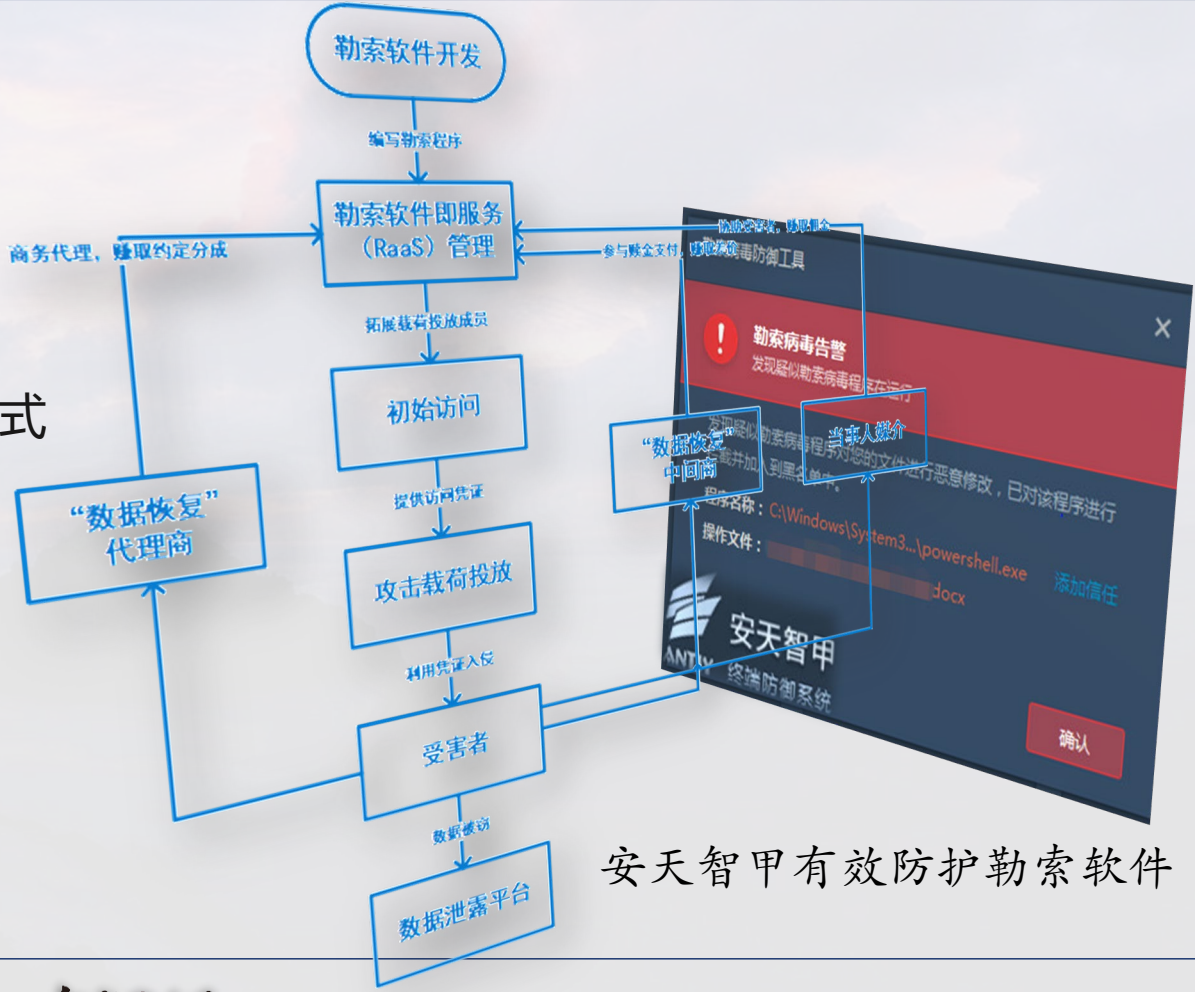
仿冒尼泊尔武装警察部队邮件系统
仿冒尼泊尔海关邮件系统
仿冒尼泊尔选举委员会邮件系统

02 勒索软件

勒索软件攻击仍然保持广撒网与定向攻击并存，
定向勒索攻击能力已达“APT”水平。

2021年网络安全威胁回顾 - 勒索软件

- 定向勒索攻击能力已达“APT”水平
- 勒索软件组织改头换面，卷土重来
- “三重勒索”模式的出现
- “破坏式”勒索软件再现
- 少量勒索软件采用“不加密只勒索”模式
- 勒索软件呈现组织化，攻击流程链条化



安天智甲有效防护勒索软件

03 挖矿木马

我国大力开展整治虚拟货币“挖矿”活动，已有显著成效。

由于挖矿木马的多功能集成性，结合目前云市场的规模和发展，攻击者针对云主机的挖矿活动将持续增长，利用威胁情报有助于快速发现并处置挖矿木马。

2021年网络安全威胁回顾 - 挖矿木马

随着虚拟货币的价值不断攀升，近年来不断有黑客团伙通过非法入侵控制互联网上的计算机，并植入木马从事挖矿活动，牟取暴利。造成大量能源消耗，并使受害主机无法正常工作。

近几年，越来越多的企业业务开始向云上迁移，随之而来的是攻击者针对云主机的挖矿活动频繁发生。

04 钓鱼邮件

在定制化钓鱼活动攻击过程中，其针对性和威胁性都呈现了递进特征，诱惑性更强，攻击成功率相对更高。邮箱的“邮件自动转发”功能成为隐蔽性高的泄密渠道。

2021年网络安全威胁回顾 - 钓鱼邮件

- 针对性的递进式钓鱼活动诱惑性更强
- 邮件自动转发功能成为隐蔽泄密渠道
- 邮件中的钓鱼网站标识载体有所变化

第一层	广撒网式批量钓鱼
第二层	针对重点人员钓鱼
第三层	仿冒重点人员邮件
第四层	诱导访问钓鱼网站
第五层	……

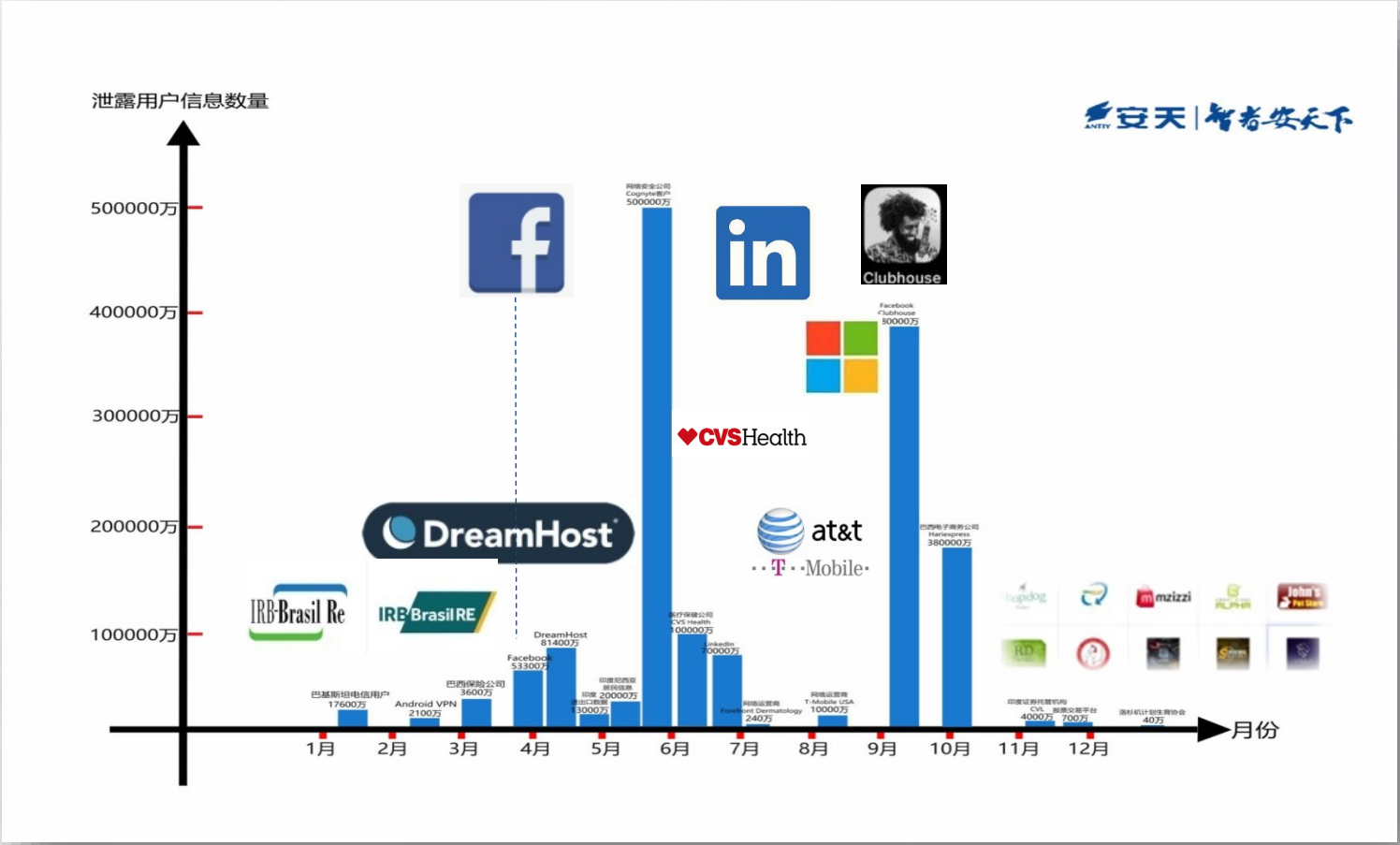
05 数据泄露

针对医疗机构的网络攻击“阴云不散”；泄露事件、泄露数据与泄露信息呈现“三高”趋势；立法与打击治理并行，为隐私保护提供有力保障。

2021年网络安全威胁回顾 - 数据泄露

保护数据信息安全不能抱有侥幸心理。

应在数据安全风险来临之前及时发现薄弱点，为薄弱环节增加防护策略和手段，以降低数据泄露的可能性。



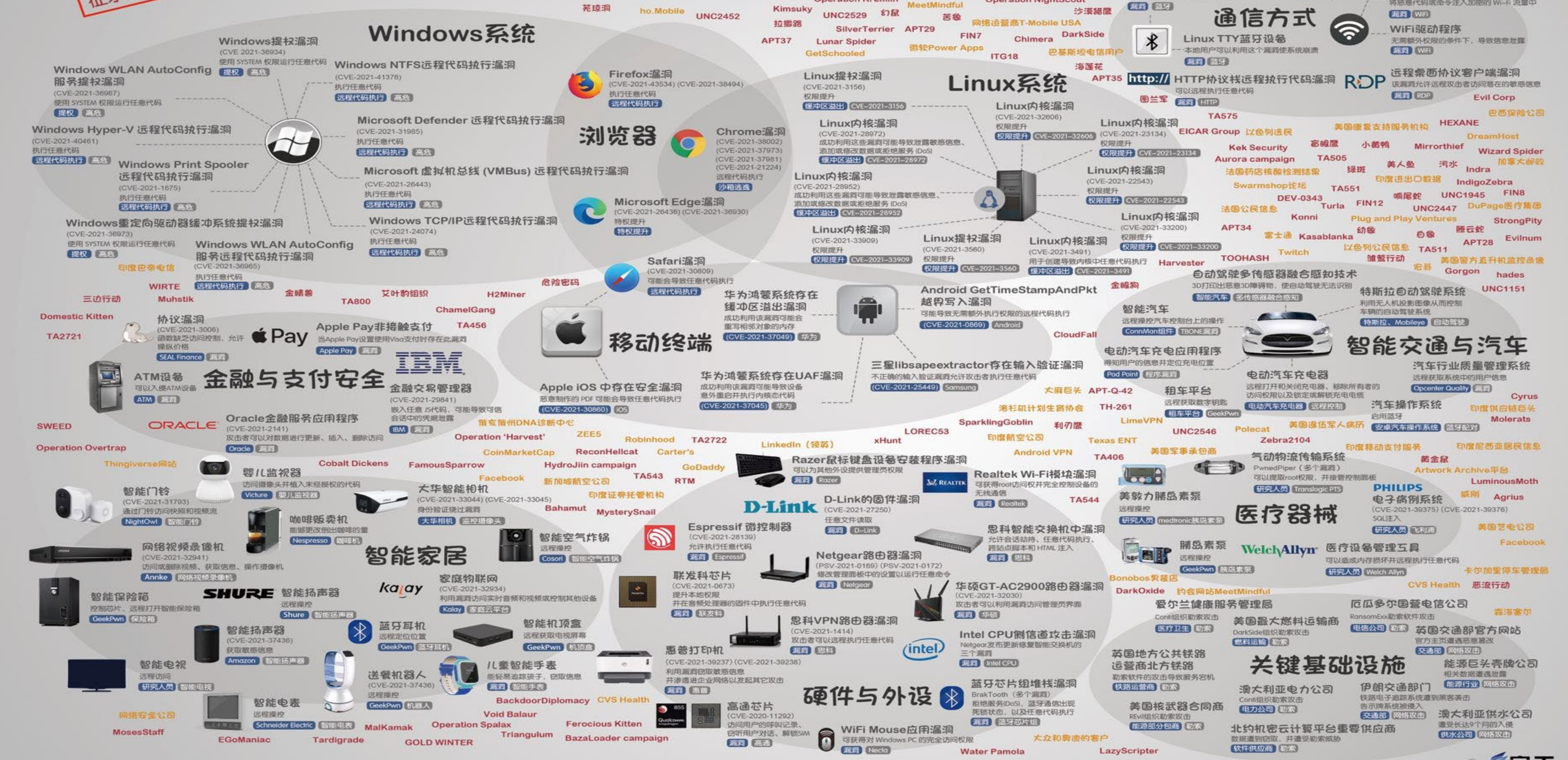
2021年影响力较大的文件数据泄露事件

06 威胁泛化

智能终端的多样性和脆弱性，一直是攻击者寻找短板的目标。

2021网络安全威胁泛化与分布

征求意见稿



本图引自《安天实验室2021网络安全年报》 安天

感谢聆听

安天冬训营 wtc.antiy.cn