2020年网络安全威胁回顾

——安天2020年网络安全年报（预发布版）内容提要

安天副总工 / 李柏松

威胁框架：细粒度对抗

長纓待展

CONTENTS

目 录

長纓待展

威胁框架：细粒度对抗

01 APT攻击

医疗卫生机构成为重点目标；突破物理隔离成为普遍能力

全球APT攻击行动、组织归属地理位置分布图

中东地区
- 双尾蝎（APT-C-23）
- 人面狮（APT-C-15）

巴基斯坦
- Gorgon group
- GravityRAT
- Stealth Mango
- Molerats
- Operation C-Major
- Operation Arachnophobia
- APT-36
- Gorgon

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

美国
- Slingshot
- DUQU（毒曲）
- Stuxnet（震网）
- Regin（瑞晶）
- Equation(方程式)
- Gauss(高斯)
- Flame（火焰）

未知
- Rancor
- Andariel
- FruityArmor
- VPNFilter
- StrongPity
- Hussarini
- Sowbug
- Wiper
- Hades
- Metamorfo
- Skygofree
- Kronos
- Potao
- DarkHydrus
- Tropic Trooper
- TA516
- Rocket Kitten
- Cobalt Gang
- BlackTech（黑凤梨）
- APT-C-35
- QUEDAGH
- BISKVIT
- RedOctober
- Tequila
- HeartBeat APT
- TA555
- Taidoor
- Big Bang
- Mirage
- Iron Group
- Moafee/DragonOK
- Gallmaker
- VERMIN Quasar
- Cobalt Group
- Musical Chairs
- Cedar Spyware
- TSCookie
- ComboJack
- Gamaredon Group
- Inception
- The White Company
- Parliament
- 利刃鹰
- FIN6
- Espionage Campaign
- WindShift
- THE RSA HACK
- SectorB06
- Careto / Mask APT （面具）
- 军刀狮
- MoneyTaker（赚钱者）
- Hexane
- OPERATION PROWLI
- SilverTerrier
- The TopHat Campaign
- Platinum
- operation cloudyomega
- KingSqlZ
- MageCart
- Mummy Spider
- Morpho（Wild Neutron、Jripbot）
- Operation Parliament
- SWEED
- FIN8
- Orangeworm
- Operation North Star
- Mirrorthief
- DangerousPassword（危险密码）

加沙地区
- Desert Falcon（沙漠猎鹰）

土耳其
- StrongPity

朝鲜
- Sun Team
- Kim Soo-ki
- APT38
- APT-37
- Lazarus（拉撒路、Hidden Cobra）
- Operation Honeybee
- Group123
- Reaper
- Kimsuky
- BabyShark

北美
- Longhorn

法国
- Animal Farm(动物农场)

黎巴嫩
- Dark Caracal
- volatile-cedar（爆炸雪松）

巴勒斯坦
- DustySky（灵猫）

南美
- 盲眼鹰

韩国
- DarkHotel（暗黑客栈、SANNY）
- Konni

尼日利亚
- Oil Tanker(幽灵的威胁)
- “折翼的雏鹰”

伊朗
- APT35
- AST
- Cobalt Dickens
- Infy
- APT33
- Chafer
- Charming Kitten
- MuddyWater
- 美人鱼（APT-C-07）
- TEMP.Zagro
- OilRig（人面马）
- APT34
- Thamar Reservoir（塔玛水库）
- Operation Cleaver（手术刀）
- Flying Kitten
- APT39
- MAGNALLIUM

印度
- Urpage
- SHAKTI（女神）
- HangOver
- ARX（阿克斯）
- Confucius(孔夫子)
- 响尾蛇
- BITTER（苦酒、蔓灵花）
- 白象（摩诃草、Patchwork、Dropping Elephant、MONSOON、Chinastrats、丰收行动）
- APT-C-35（肚脑虫）
- 幼象

中国台湾地区
- 绿斑（毒云藤）
- 蓝宝菇（APT-C-12）

沙特阿拉伯
- Gaza Cybergang
- APT-C-27 (黄金鼠)
- Desert Falcons（沙漠猎鹰）
- 拍拍熊

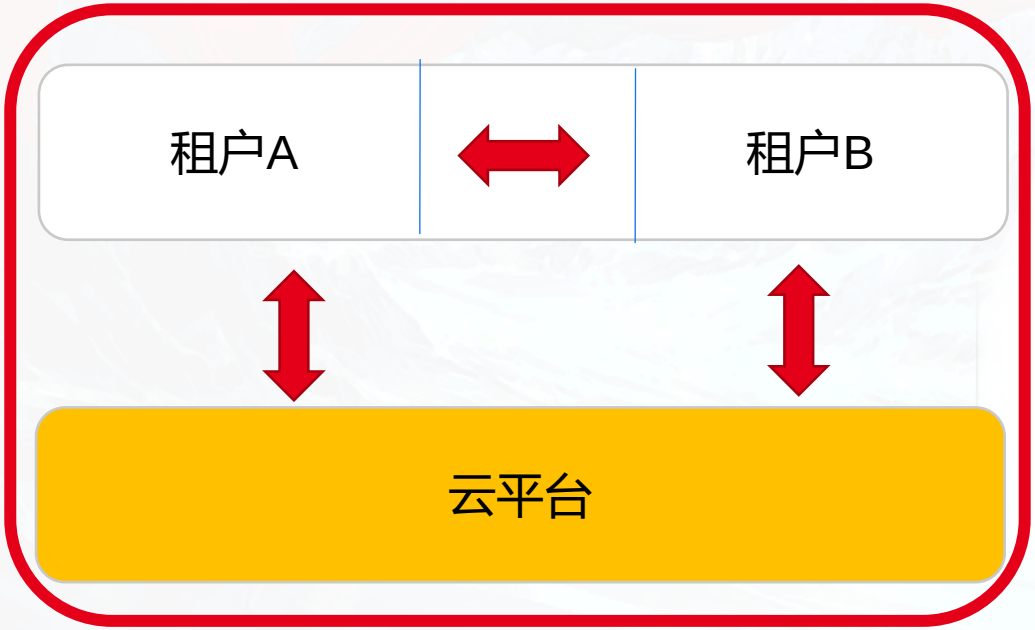
越南
- APT-TOCS(海莲花、OceanLotus、APT 32)

阿拉伯联合酋长国
- StealthFalcon

黄色的字是2020年活动的攻击行动、组织　● APT组织　▲ APT行动

2020年网络安全威胁回顾 - APT攻击

- 针对云平台、基础设施管理平台的高级威胁攻防对抗强度将会加剧




```
ar *user_input, char **ret_username)

    register char *ptr;
    register int index = 0;
    char username[PAM_MAX_RESP_SIZE];
/* ... */

    ptr = user_input;
/* ... */
     /*
      * username will be the first string we get from user_input
      * - we skip leading whitespaces and ignore trailing whitespaces
      */
    while (*ptr != '\0') {
          if ((*ptr == ' ') || (*ptr == '\t'))
                    break;
          else {
                    username[index] = *ptr;
                    index++;
                    ptr++;
          }
    }
     /* ret_username will be freed in pam_get_user(). */
    if ((*ret_username = malloc(index + 1)) == NULL)
          return (PAM_BUF_ERR);
    (void) strcpy(*ret_username, username);
    rn (PAM_SUCCESS);
```

2020年网络安全威胁回顾 - APT攻击

- 突破物理隔离网络已经成为高级威胁组织的普遍能力

扫描二维码查看报告

安天发布APT事件分析报告

《"折纸"行动：针对南亚多国军政机构的网络攻击》

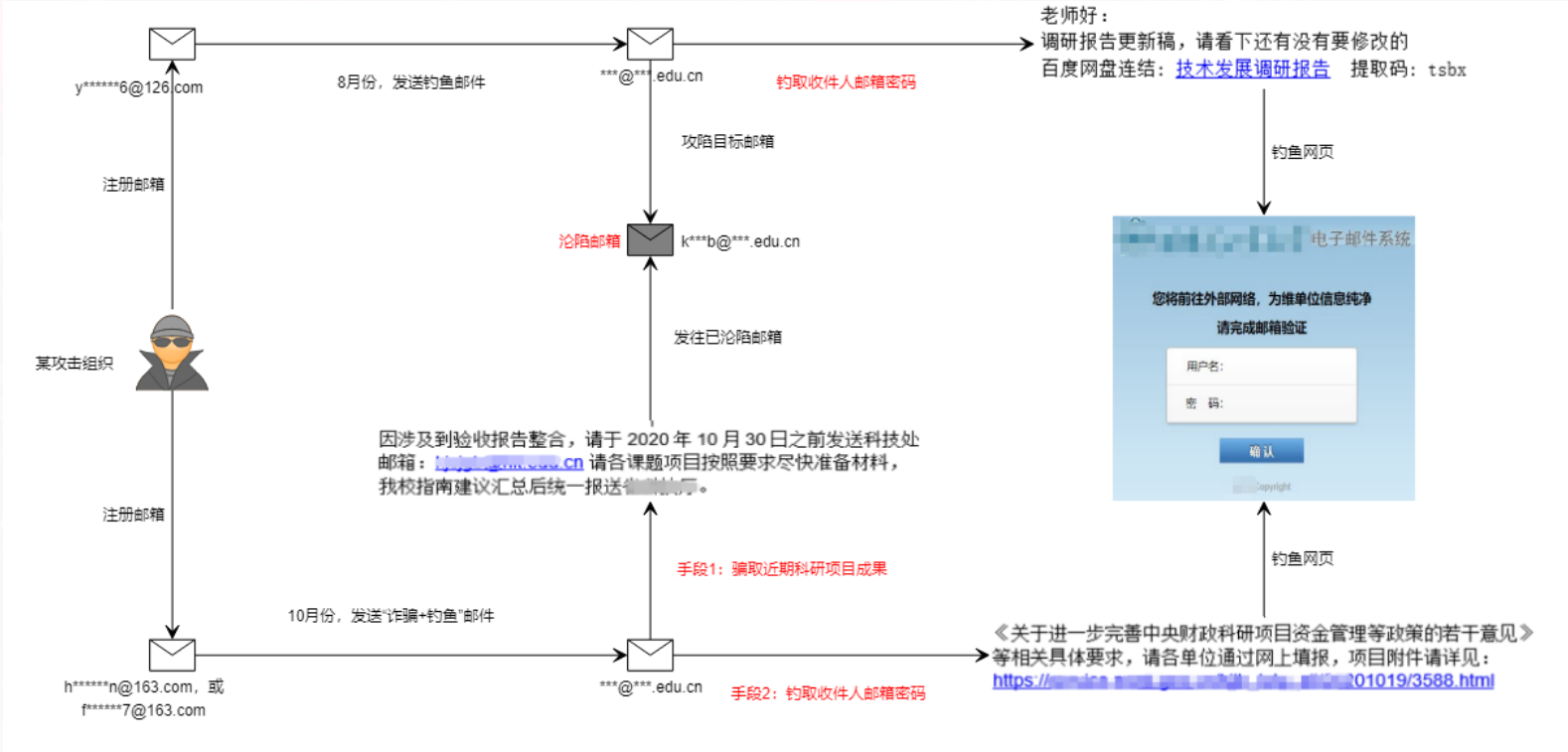
扫描二维码查看报告

安天发布APT事件分析报告

《Darkhotel组织渗透隔离网络的Ramsay组件分析》

2020年网络安全威胁回顾 - APT攻击

- 警惕利用社工手段的无载荷APT窃密攻击方式



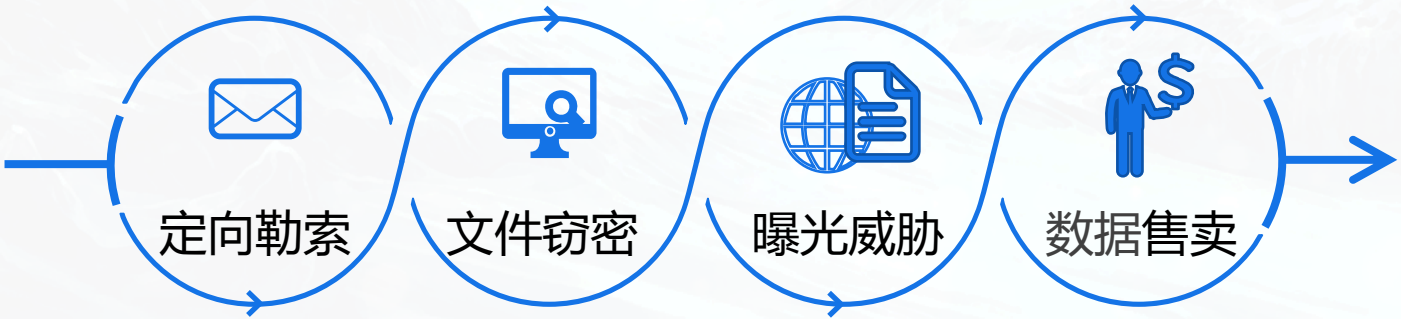
2020年8月，安天监测到多起针对我国高校、科研院所等机构的无载荷的APT攻击活动。

02 勒索软件

勒索软件攻击能力不断提高，已接近“APT”水平

2020年网络安全威胁回顾 - 勒索软件

- 勒索软件攻击能力不断提高，已接近“APT”水平
- 勒索软件对有价值的攻击目标进行定向勒索
- 勒索攻击呈现流程链条化模式
- 中间商假扮“数据恢复公司”



勒索软件攻击的作业模式

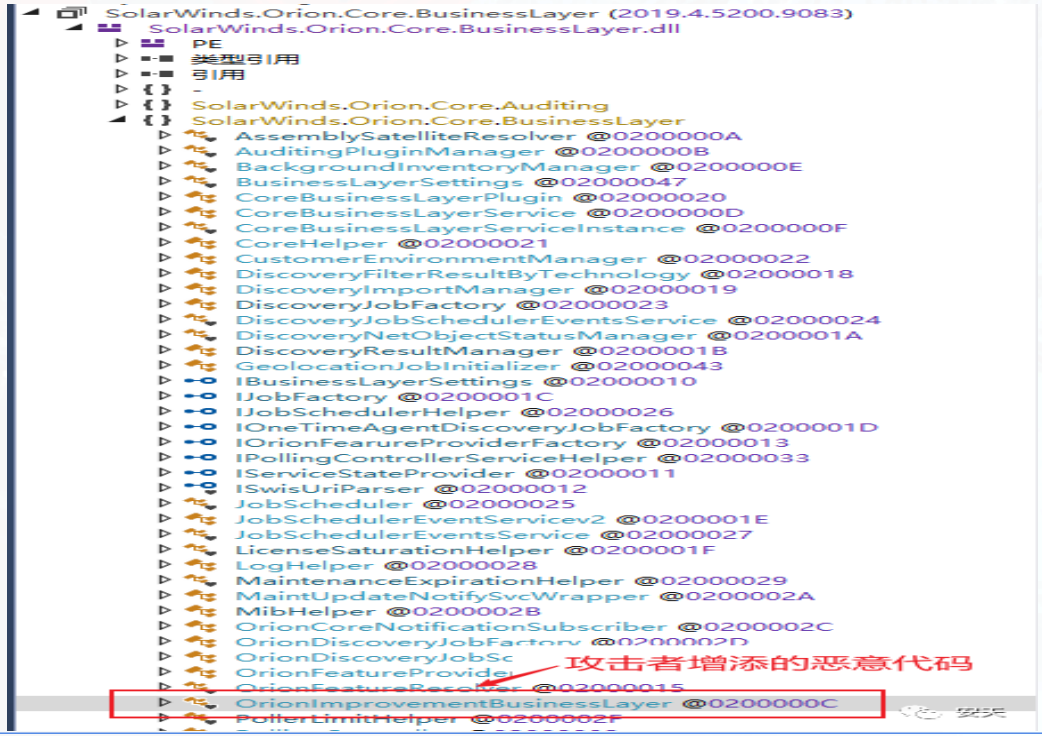
安天智甲有效防护勒索软件

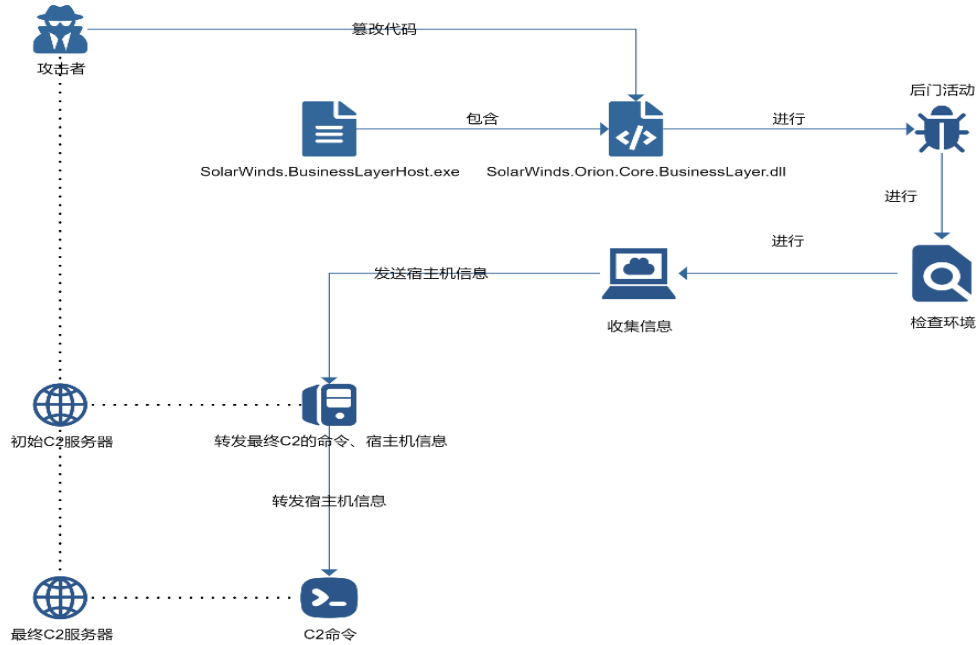
03 供应链安全

供应链上游环节面临威胁；供应链及其用户皆被卷入

2020年网络安全威胁回顾 - 供应链安全

- 网空威胁行为体不断加大供应链上游环节的攻击成本投入
- 将有更多行业领域供应链及其用户被卷入供应链战争





04 威胁泛化

物联网终端为攻击者开辟了更多的攻击入口

2020网络安全威胁泛化与分布

本图引自《安天实验室2020网络安全年报》© 安天

谢谢大家