邮件安全的威胁认知与防御关口设置

安天安全服务中心

威胁框架：细粒度对抗

長纓待展

CONTENTS

目 录

01 邮件系统业务现状

电子邮件系统历史

1965年
- 首个电子邮件系统

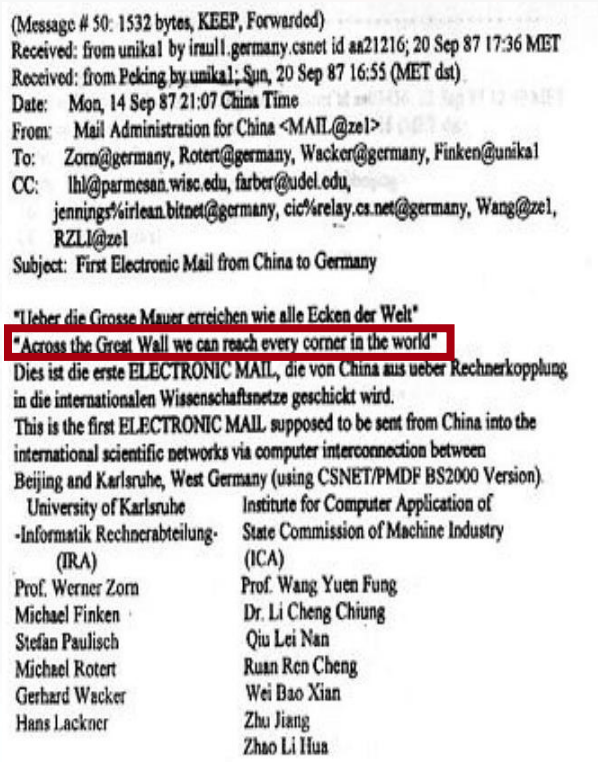
1971年
- 首封跨主机电子邮件

1987年
- 中国首封电子邮件

1965年：麻省理工学院开发MAILBOX电子邮件系统，仅能发送到同一主机不同用户

1971年：Ray Tomlinson首次使用 @ 分开用户名与主机名，发送人类历史第一封真正意义的电子邮件

1987年：中国首封电子邮件，主题“Across the Great Wall we can reach every corner in the world“(跨越长城，我们可以到达世界的任何角落)。通过国际互联网发送到西德卡尔斯鲁厄大学，这预示着互联网时代悄然叩响了中国的大门



(Message # 50: 1532 bytes, KEEP, Forwarded)
Received: from unika1 by irau1.germany.csnet id aa21216; 20 Sep 87 17:36 MET
Received: from Peking by unika1; Sun, 20 Sep 87 16:55 (MET dst)
Date: Mon, 14 Sep 87 21:07 China Time
From: Mail Administration for China <MAIL@ze1>
To: Zorn@germany, Rotert@germany, Wacker@germany, Finken@unika1
CC: lhl@parmesan.wisc.edu, farber@udel.edu,
jennings%irlean.bitnet@germany, cic%relay.cs.net@germany, Wang@ze1,
RZLI@ze1
Subject: First Electronic Mail from China to Germany

"Ueber die Grosse Mauer erreichen wie alle Ecken der Welt"
"Across the Great Wall we can reach every corner in the world"
Dies ist die erste ELECTRONIC MAIL, die von China aus ueber Rechnerkopplung in die internationalen Wissenschaftsnetze geschickt wird.
This is the first ELECTRONIC MAIL supposed to be sent from China into the international scientific networks via computer interconnection between Beijing and Karlsruhe, West Germany (using CSNET/PMDF BS2000 Version)

University of Karlsruhe
-Informatik Rechnerabteilung-
(IRA)
Prof. Werner Zorn
Michael Finken
Stefan Paulisch
Michael Rotert
Gerhard Wacker
Hans Lackner

Institute for Computer Application of
State Commission of Machine Industry
(ICA)
Prof. Wang Yuen Fung
Dr. Li Cheng Chiung
Qiu Lei Nan
Ruan Ren Cheng
Wei Bao Xian
Zhu Jiang
Zhao Li Hua

中国首封电子邮件

邮件系统供应链现状

自建邮件系统

- Exchange server
- Daemon
- Domino
- Coremail
- 时代亿信…

免费邮箱

- 网易163、126
- 腾讯QQ…

云服务

- 阿里云企业邮箱
- 华为云企业邮箱
- 腾讯云企业邮箱…

电子邮件业务现状

2021年1月

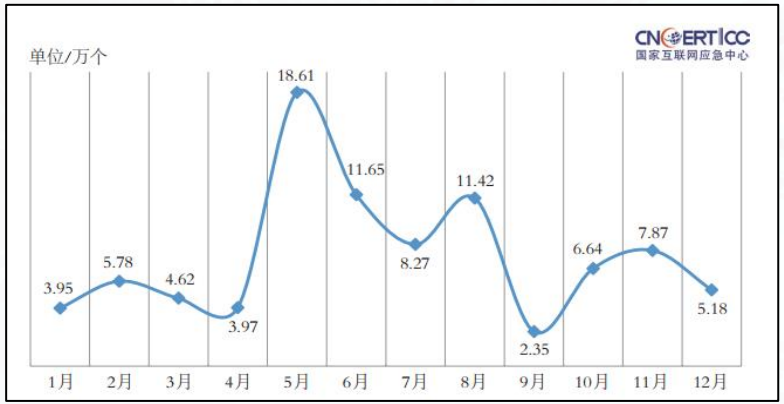
中国公网开放的邮件系统约**68027个**①

2019年度

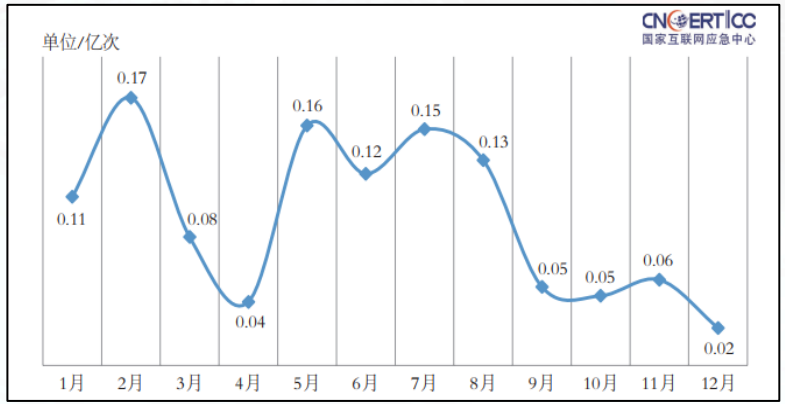
CNCERT/CC捕获与监测②

通过电子邮件传播的恶意代码**79.2万余个**，全年恶意电子邮件传播次数**1.148亿余次**

重要党政机关部门遭受钓鱼邮件攻击数量达**56万多次**，月均**4.6万余次**



2019 年通过电子邮件传播的恶意程序数量按月度统计



2019 年恶意电子邮件传播次数按月度统计

注： ① 引自shodan ② 引自CNCERT发布《2019年我国互联网网络安全态势综述》报告

02 邮件安全的威胁认知

新冠疫情期间，邮件安全事件频发

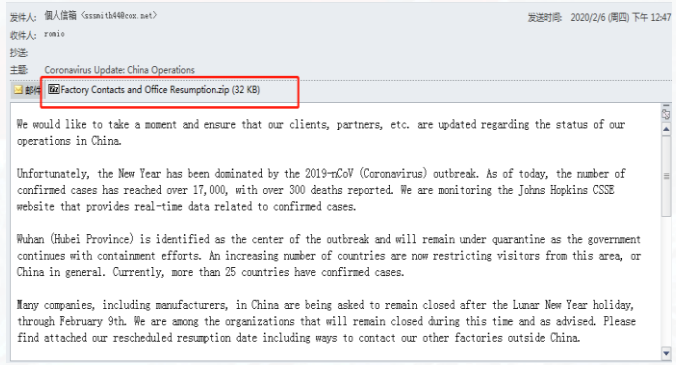
新冠疫情无疑使企业加强远程办公，同时对信息化安全是挑战，钓鱼事件有所频发

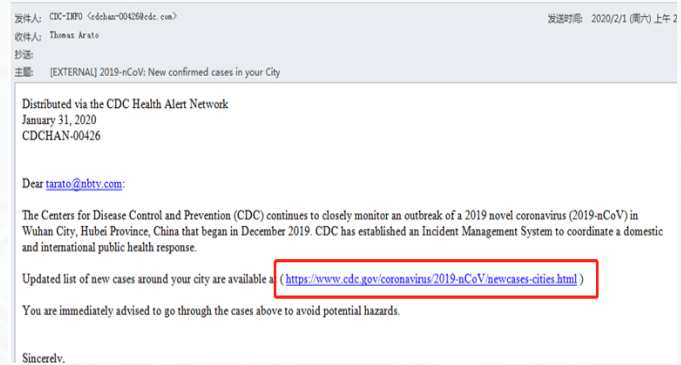
2020年02月12日，CNCERT发布《防范网络不法分子利用新型肺炎相关主题进行钓鱼邮件入侵的预警通报》

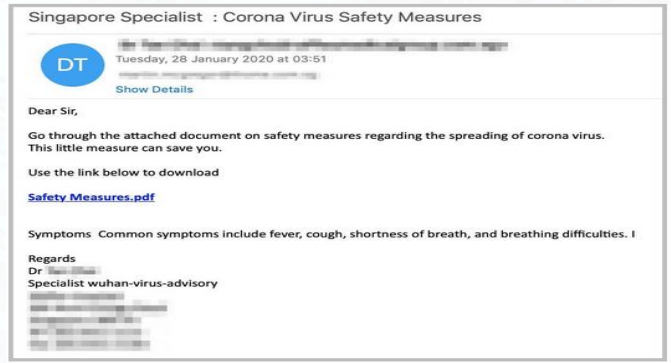
新冠疫情期间，安天捕获多起邮件社工事件

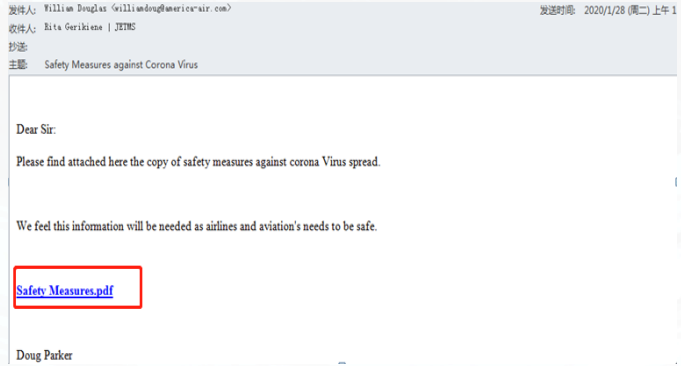
安天CERT监测到多起恶意代码的事件，利用新型冠状病毒肺炎疫情相关热词，诱导用户点击

- 恶意代码文件名
  - 冠状病毒
  - 菲律宾各大楼冠状肺炎名单
  - 新型冠状病毒肺炎病例全国已5名患者死亡；警惕！！
- 诱饵形态
  - 可执行文件
  - 钓鱼邮件携带恶意链接
  - 传播恶意PDF









新冠疫情期间，安天捕获邮件社工事件案例

安天捕获Ryuk勒索软件事件。攻击者通过垃圾邮件传播Emotet银行木马，Emotet木马下载TrickBot僵尸网络，TrickBot僵尸网络开启反向shell，通过shell来投放Ryuk勒索软件

勒索软件执行流程

（1） 释放衍生文件、注入进程

Ryuk勒索软件样本执行后释放衍生文件，执行后注入特定进程

（2）获取系统信息、生成密钥并对密钥进行加密

获取系统版本信息，根据不同系统版本，设置不同写入密钥文件路径。

（3）排除特定目录并生成勒索信息文件

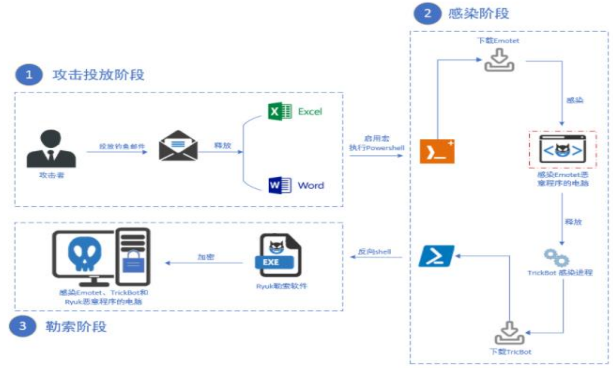
排除系统目录外，加密其余目录下的文件，并生成勒索信息文件。

（4）排除特定后缀名文件并进行加密

检索系统中文件，排除指定后缀名文件，对其余后缀名文件进行加密。

（5）根据文件大小采取不同方式进行加密

通过对样本的分析，发现样本针对不同大小文件采取不同加密流程。



病毒名称	Trojan[Ransom]/Win32.Ryuk
原始文件名	lx356.exe
MD5	EA0351560415B60AA010A2E9FED8B65B
处理器架构	Intel 386 or later, and compatibles
文件大小	323.50 KB (331,264 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2020-02-03 17:16:45
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++
VT首次上传时间	2020-02-13 10:16:46
VT检测结果	59 / 72

常态化邮件安全事件

2020年11月1日~2020年12月31日，安天《每日安全简讯》提及13起与邮件安全相关事件，天数占比21.3%

① 攻击者正在劫持普渡大学等热门高校的电子邮件账户

② 攻击者利用Rackspace托管电子邮件服务进行网络钓鱼

③ 英国国会议员每月收到近3百万次电子邮件攻击

④ Xbox Live 漏洞可导致电子邮件地址泄露

⑤ 黑客正在出售数百名高管的电子邮件账户密码

⑥ 黑客入侵赛百味营销系统给客户发送恶意邮件

⑦ 钓鱼邮件冒充eFax等企业窃取用户Office365凭证

⑧ Facebook漏洞暴露Instagram用户邮件地址

⑨ SolarWind黑客入侵美国财政部官员的电子邮件账户

⑩ 钓鱼邮件冒充美国邮政服务窃取用户信用卡凭证

⑪ 假冒亚马逊礼品卡电子邮件分发Dridex恶意软件

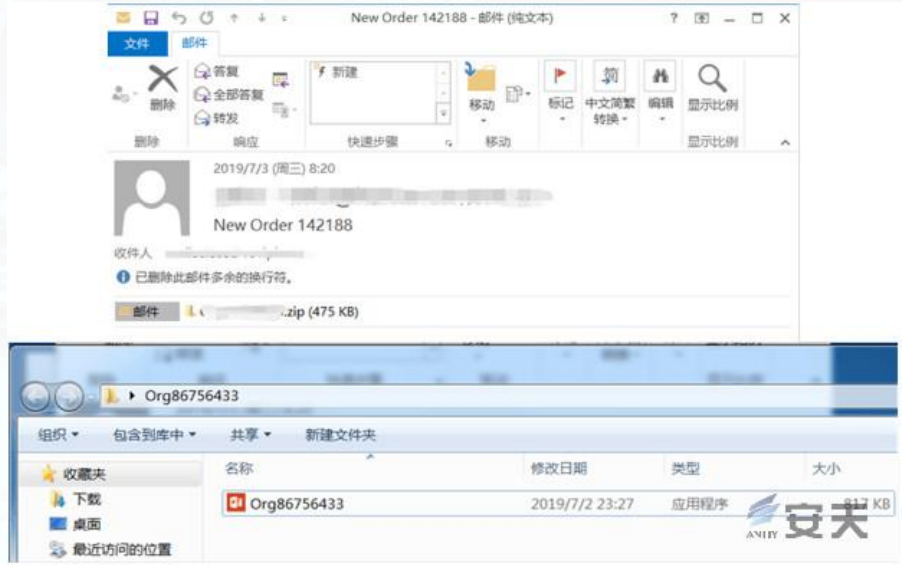
⑫ 芬兰称黑客访问了部分议员的电子邮件账户

⑬ 钓鱼邮件冒充Chase的安全通知窃取用户凭证

常态化邮件安全事件：安天曝光KPOT恶意代码窃密事件

2019年8月，安天CERT监测到了多起利用KPOT木马进行窃密的事件，判定此类事件是由Magecart第五小组发起攻击者利用KPOT窃取用户加密货币钱包信息、应用账户信息以及浏览器cookies等多种信息。攻击者主要利用了**垃圾邮件**以及**RIG和Fallout漏洞利用工具包**来传播木马。

- **步骤一：**攻击者通过公开收集、自动生成等方法，获取邮件地址
- **步骤二：**攻击者发送大量带有恶意附件的垃圾邮件。
- **步骤三：**攻击者将KPOT木马制作成压缩包添加在邮件附件中，将KPOT木马伪装成PPT等正常文件；或构造漏洞利用文档，文档被打开时，下载KPOT
- **步骤四：**当用户双击打开该伪装PPT时，就会运行KPOT木马，被窃取各种信息。



安天曝光APT“折纸行动：针对南亚多国军政机构的网络攻击”

2020年01月15日，安天发布报告《“折纸行动：针对南亚多国军政机构的网络攻击”》，披露2019年度多起南亚网络攻击事件

邮件主题

- “中印峰会期间的关键讨论要点”
- “巴基斯坦MOFA（外交部）官员的工资”
- “2019年11月9日卡塔普尔走廊的就职典礼”
- “Cyber Policy 2019”和“NDU国外学习之旅（FST）-2020”等。

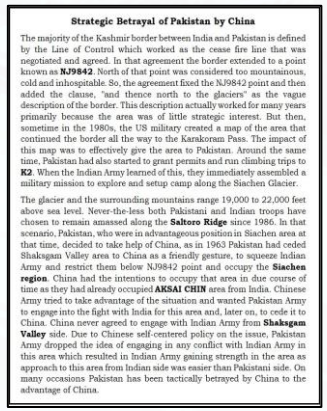
邮件发件人

- dgpr.paknavy.gov.pk@email.com”
- arif9945@baf.mil.bd”
- 收件人都位于巴基斯坦境内

诱饵文件类型

- 快捷方式
- 伪装成PDF的程序
- 宏文档

攻击时间	至少始于2017年7月-2020年1月，保持活跃
攻击意图	窃密、刺探
针对目标	集中于巴基斯坦，其他少量分布在孟加拉国、斯里兰卡等南亚国家
针对行业/领域	政府、军事、国防、外交、核能、金融、教育、电信等
攻击手法	鱼叉邮件、钓鱼网站
涉及平台	Windows、Linux
攻击技术	纯脚本载荷、恶意宏、图标伪装、后缀名伪装、域名伪装
诱饵类型	图标伪装EXE、PDF图标自解压、Office文档、快捷方式等
使用漏洞	CVE-2017-11882、CVE-2018-0802
开发语言	C++、Python、PowerShell、HTML和Go语言
武器装备	Empire框架、Exploit Pack平台、自研C++、Python木马



Strategic Betrayal of Pakistan by China

The majority of the Kashmir border between India and Pakistan is defined by the Line of Control which worked as the cease fire line that was negotiated and agreed. In that agreement the border extended to a point known as **NJ9842**. North of that point was considered too mountainous, cold and inhospitable. So, the agreement fixed the NJ9842 point and then added the clause, "and thence north to the glaciers" as the vague description of the border. This description actually worked for many years primarily because the area was of little strategic interest. But then, sometime in the 1980s, the US military created a map of the area that continued the border all the way to the Karakoram Pass. The impact of this map was to effectively give the area to Pakistan. Around the same time, Pakistan had also started to grant permits and run climbing trips to **K2**. When the Indian Army learned of this, they immediately assembled a military mission to explore and setup camp along the Siachen Glacier.

The glacier and the surrounding mountains range 19,000 to 22,000 feet above sea level. Never-the-less both Pakistani and Indian troops have chosen to remain amassed along the **Saltoro Ridge** since 1986. In that scenario, Pakistan, who were in advantageous position in Siachen area at that time, decided to take help of China, as in 1963 Pakistan had ceded Shaksgam Valley area to China as a friendly gesture, to squeeze Indian Army and restrict them below NJ9842 point and occupy the **Siachen region**. China had the intentions to occupy that area in due course of time as they had already occupied **AKSAI CHIN** area from India. Chinese Army tried to take advantage of the situation and wanted Pakistan Army to engage into the fight with India for this area and, later on, to cede it to China. China never agreed to engage with Indian Army from **Shaksgam Valley** side. Due to Chinese self-centered policy on the issue, Pakistan Army dropped the idea of engaging in any conflict with Indian Army in this area which resulted in Indian Army gaining strength in the area as approach to this area from Indian side was easier than Pakistani side. On many occasions Pakistan has been tactically betrayed by China to the advantage of China.

Turkey's response to ISI help

Turkey has trained Pakistani officers and supplied a wide variety of military hardware, including Ozmk MRTP-33 fast attack craft, AH-1 Cobra helicopter parts and artillery simulators. Turkish Aerospace Industries has also upgraded Pakistan's F-16A/B Block 15s and promoted its T-129 attack helicopter as an AH-1F Cobra replacement. SSB, Turkey and TAI has also entered into contract with Pakistan Aeronautical Complex, Board, Kamra to buy Super Mushak Training planes.

M/s Havelsan agreement on simulation and training

Turkey's Havelsan software and systems integration company signed a memorandum of understanding with the Pakistan Armed Forces regarding simulation and training. Mr. Sadik Yamac, General Manager, CEO of Havelsan, informed that three agreements are in play. These cover Research and Development, the Pakistan Armed Force's C4I (Command, Control, Communications, Computers, and Intelligence) and **simulators for the Pakistan Air Force and Army, including flight, driving and possibly artillery simulators**.

Projects that will benefit from the agreements include **the JF-17 Thunder, F-16 Fighting Falcon, C-130 Hercules, Mil Mi-17 and Super Mushak**. Pakistan's **Military Vehicle Research and Development Establishment (MVRDE)** in particular will benefit from the agreements. The latter has developed a tank artillery simulator.

Havelsan has performed work for the Pakistan Armed Forces, having delivered Artillery Forward Observer Simulators, an Electronic Warfare Test and Training Range (**EWTTR**) and battle management and information systems. Havelsan received order for its Genesis combat management system for the Pakistan Navy's Oliver Hazard Perry class frigate, **PNS Alamgir**.

Is ISI capable to fetch China's discreet help to Pakistan for its nuclear weapons campaign?

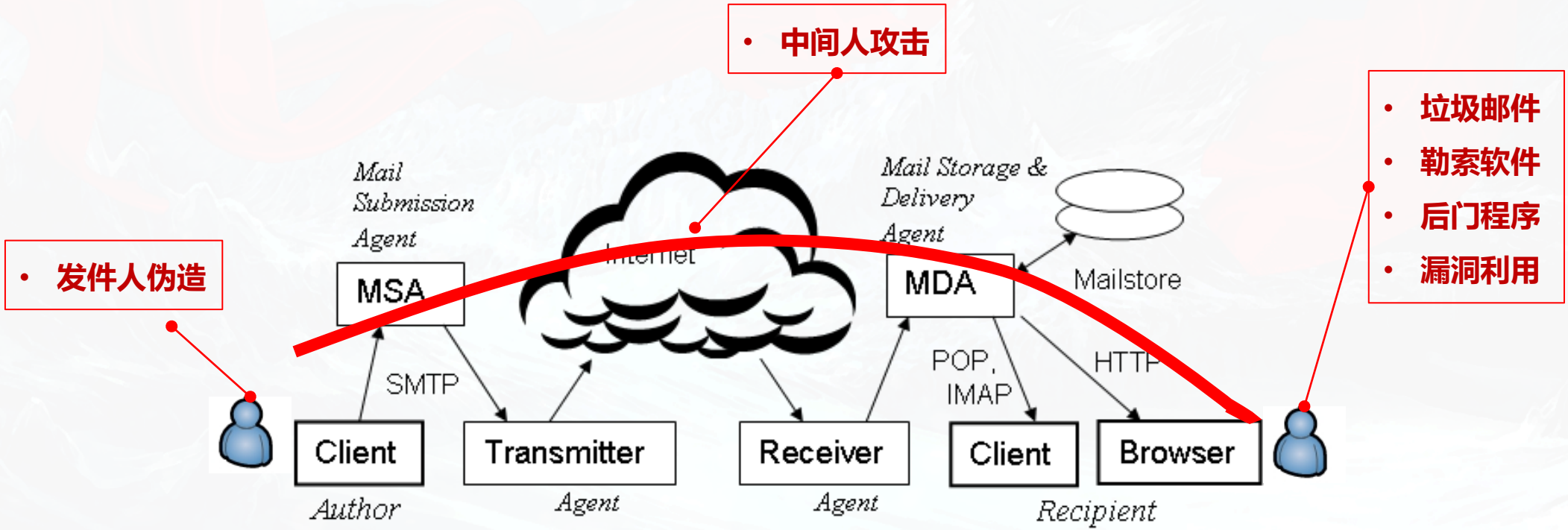
In order to deter its traditional rival India, **ISI's** efforts to get Chinese support to achieve its nuclear weapon campaign, is a success or failure? ISI extended full support to its' campaign to achieve nuclear weaponry – installation at **Fateh Jung**. The recent visit, of ISI chief to Beijing along with Army Chief to finalize the modalities of future course of action, has resulted into signing of a new deal. The visit was never publicized in the Press to keep it very secret. The deals in past were modified to suit their requirement.

Chinese signing of deal to build new nuclear reactor in Pakistan served as the main document for the meeting. China had signed a deal to build a third large nuclear reactor in Pakistan, which wants to get a fifth of its electricity from nuclear by 2030. **China National Nuclear Corporation (CNNC)** and **the Pakistan Atomic Energy Commission (PAEC)** had signed a cooperation agreement for the construction of a 1,000 Megawatt (MW) HPR1000 "**Hualong-One**" reactor at the **Chashma nuclear power plant in Punjab**. Pakistan generates five percent of its electricity from four small 300 MW Chinese reactors at the **Chashma plant** and wants to boost nuclear capacity to 8,800 MW, or about 20 percent of power generation capacity, by 2030. China has already building two **Hualong-One** reactors with a capacity of 1100 MW each near the port city of Karachi, which are expected to become operational in 2020 and 2021 respectively.

The Sino-Pakistani deal is different from the Indo-U.S. agreement. In the Indian case, the agreement went through the various procedural steps, whether at the IAEA, the NSG or the legislatures of the **United States and India**, and only then was it implemented through specific deals with various suppliers. In the Sino-Pakistani case, the parties did not seek formal approval from the NSG, and China preferred to "grandfather" the reactor transaction despite earlier commitments to desist from doing so. Moreover, attempts by China and Pakistan to conclude a nuclear deal that would add to the **Chashma 1 and 2** reactors predate the Indo-U.S. nuclear agreement by several years; preparations for this deal were already made when the Indo-U.S. deal was announced.

Lt Col (Retd) Raza Abbas Ghazi
razaghazi@mail.com

邮件安全部分威胁认知


• 中间人攻击
• 发件人伪造
• 垃圾邮件
• 勒索软件
• 后门程序
• 漏洞利用
Mail Submission Agent
MSA
Internet
Mail Storage & Delivery Agent
MDA
Mailstore
SMTP
POP, IMAP
HTTP
Client
Transmitter
Receiver
Client
Browser
Author
Agent
Agent
Recipient

社工邮件关联的ATT&CK技战术

侦察	资源开发	初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	数据渗出	影响
主动扫描	获取基础设施	水坑攻击	利用命令和脚本解释器	操纵账户	滥用提升控制权限机制	滥用提升控制权限机制	暴力破解	发现账户	利用远程服务	压缩/加密收集的数据	使用应用层协议	自动渗出数据	删除账户权限
搜集受害者主机信息	入侵账户	利用面向公众的应用程序	利用主机软件漏洞执行	利用BITS服务	操纵访问令牌	操纵访问令牌	获取密码存储中的凭证	发现应用程序窗口	执行内部鱼叉式钓鱼攻击	捕获音频	通过可移动介质通信	限制传输数据大小	损毁数据
搜集受害者身份信息	入侵基础设施	利用外部远程服务	利用进程间通信	利用自动启动执行引导或登录	利用自动启动执行引导或登录	利用BITS服务	利用凭证访问漏洞	发现浏览器书签	横向传输文件或工具	自动收集	数据	使用非C2协议回传	造成恶劣影响的数据加密
搜集受害者网络信息	能力开发	添加硬件	利用API	利用初始化脚本引导或登录	利用初始化脚本引导或登录	反混淆/解码文件或信息	强制认证	云服务仪表板	远程服务会话劫持	收集剪贴板数据	混淆数据	使用C2信道回传	操纵数据
搜集受害者组织信息	建立账户	鱼叉式钓鱼邮件	利用计划任务/工作	添加浏览器扩展插件	创建或修改系统进程	直接访问卷	输入捕捉	云服务发现	利用远程服务	来自云存储对象的数据	使用动态参数	使用其他网络介质回传	篡改可见内容
通过网络钓鱼搜集信息	能力开发	鱼叉式钓鱼链接	利用客户端执行	篡改客户端软件	事件触发执行	执行范围保护	利用中间人攻击（MITM）	发现域信任	通过可移动介质复制	收集信息库数据	使用加密信道	使用物理介质回传	擦除磁盘
从非公开源搜集信息	获取基础设施	入侵供应链	利用第三方软件部署工具	创建账户	利用漏洞提权	利用漏洞规避防御	修改身份验证过程	发现文件和目录	利用第三方软件部署工具	收集本地系统数据	使用备用信道	使用Web服务回传	端点侧拒绝服务（DoS）
从公开技术数据库搜集信息	获取受害者资产	利用受信关系	利用系统服务	创建或修改系统进程	利用组策略修改	修改文件和目录权限	网络嗅探	扫描网络服务	污染共享内容	收集网络共享驱动数据	使用入口工具传输	定时传输	破坏固件
搜集公开网站/域	获取受害者网络资产	利用有效账户	诱导用户执行	事件触发执行	执行流程劫持	修改组策略	操作系统凭证转储	发现网络共享	使用备用身份验证材料	收集可移动介质数据	创建多级信道	将数据转移到云账户	禁止系统恢复
搜索受害者自有网站	获取受害者组织资产		利用Windows管理规范（WMI）	利用外部远程服务	进程注入	隐藏行为	窃取应用程序访问令牌	网络嗅探		数据暂存	使用标准非应用层协议		网络侧拒绝服务（DoS）
				执行流程劫持	利用计划任务/工作	执行流程劫持	窃取或伪造Kerberos 凭证	发现密码策略		收集电子邮件	使用非标准端口		资源劫持
				植入容器映像	利用有效账户	削弱防御机制	窃取Web会话Cookie	发现主机接入设备		输入捕捉	使用协议隧道		禁用服务
				启动Office应用程序		删除主机中的信标	双因子认证拦截	发现权限组		浏览器中间人攻击（MitB）	使用代理		系统关机/重启
				在操作系统前启动		间接执行命令	未受保护凭证	发现进程		利用中间人攻击（MITM）	利用远程访问软件		
				利用计划任务/工作						获取屏幕截图	使用流量信令		
				利用服务器软件组件						捕获视频	利用合法Web服务		
				使用流量信令									
				利用有效账户									
						在操作系统前启动		发现系统网络连接					
						进程注入		发现系统所有者/用户					
						注册恶意域控制器		发现系统服务					
						使用Rootkit		发现系统时间					
						执行签名的二进制文件代理		虚拟化/沙箱逃逸					
						执行签名的脚本代理							
						损坏信任控制							
						模板注入							
						使用流量信令							
						利用受信的开发工具执行							
						未使用/不受支持的云区域							
						使用备用身份验证材料							
						利用有效账户							
						虚拟化/沙箱逃逸							
						利用XSL文件执行							

钓鱼邮件

获取内网桥头堡
支撑下一步作业

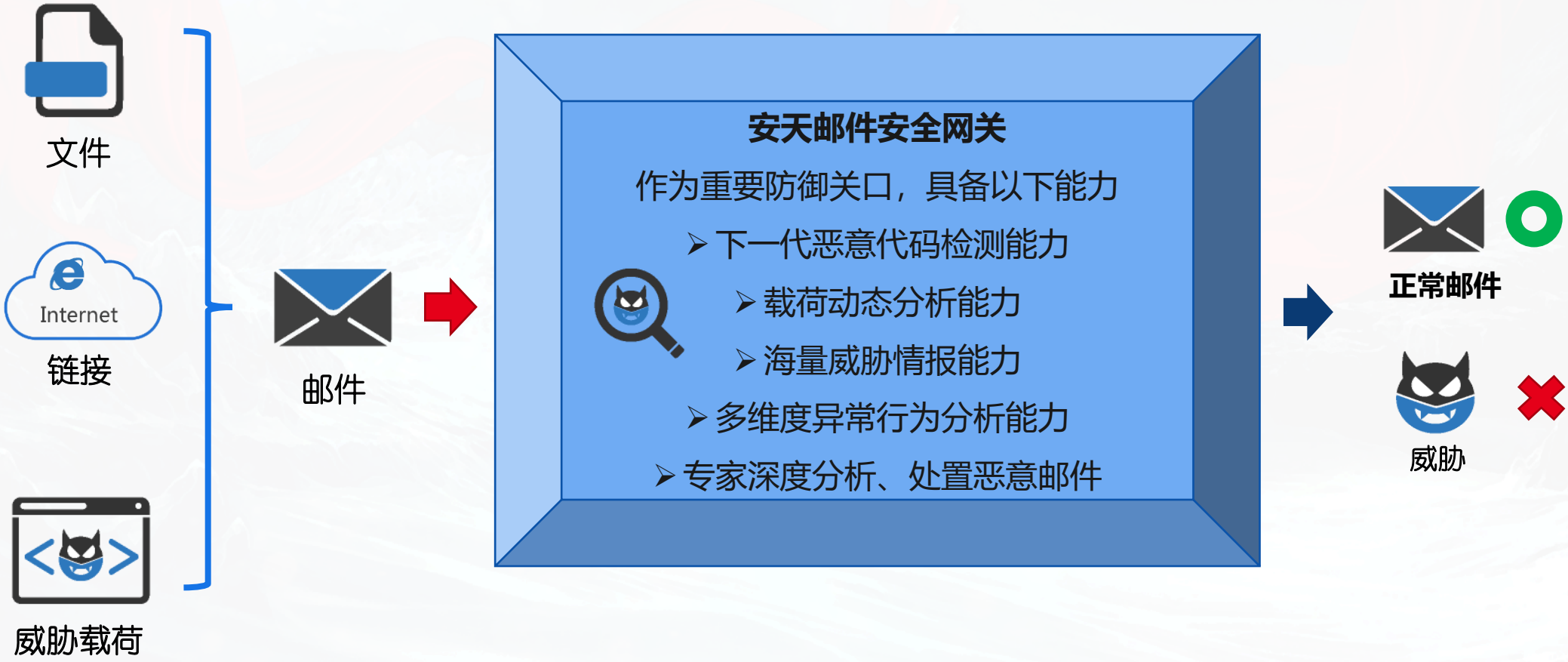
03 邮件安全防御关口设置

邮件系统传统防御手段

传统防御手段：SPF、DKIM、DMARC、邮件系统内置杀毒模块…

- **SPF**是一种以IP地址认证电子邮件发件人身份的技术。接收邮件方会首先检查域名的SPF记录，SPF可以防止别人伪造你来发邮件，可以一定程度上防止别人假冒你的域名发邮件。 ⟷ **合法凭证对抗**
- **DKIM**是一种防范电子邮件欺诈的验证技术，通过消息加密认证的方式对邮件发送域名进行验证。从而确认在邮件发送的过程中，防止邮件被恶意篡改，保证邮件内容的完整性。 ⟷ **合法凭证对抗**
- **DMARC**是一种基于现有的SPF和DKIM协议的可扩展电子邮件认证协议，便于邮件发送方和邮件接收方共同对域名的管理进行完善和监督。DMARC能够有效识别并拦截欺诈邮件和钓鱼邮件，保障用户个人信息安全。 ⟷ **合法凭证对抗**
- **邮件系统杀毒能力，邮件系统厂商内置杀毒模块（如clamAV…）** ⟷ **免杀文件对抗**

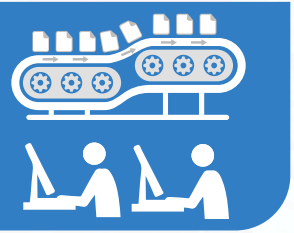
邮件场景——防御关口设置


文件
Internet
链接
威胁载荷
邮件
安天邮件安全网关
作为重要防御关口，具备以下能力
➢ 下一代恶意代码检测能力
➢ 载荷动态分析能力
➢ 海量威胁情报能力
➢ 多维度异常行为分析能力
➢ 专家深度分析、处置恶意邮件
正常邮件
威胁

邮件场景——安天下一代恶意代码检测能力

病毒捕获

病毒分析



情报共享

知识体系

8大分类

5万家族

1000万独立变种

超308种文件签名格式

检测能力 | 识别能力 | 适配能力 | 检测能力

AVL SDK

Since 2000

Windows

Linux

国产操作系统

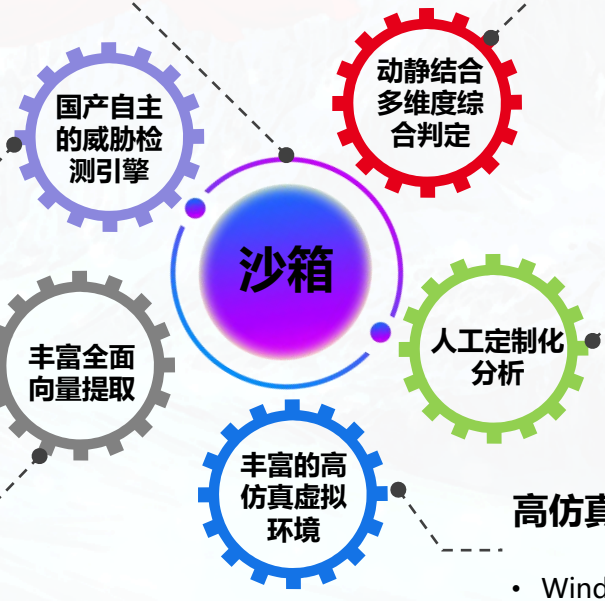
4,300万高质量检测规则

超过1000万可检测恶意代码种类

智者安天下

威胁框架：细粒度对抗

邮件场景——安天载荷动态分析能力



覆盖企业、移动场景的动态载荷分析能力，应对多场景威胁载荷

- PE/APK/ELF类文件等综合分析，深度判定恶意
- 触发并捕获0day漏洞利用
- 绕开多种对抗手段，如代码加密、混淆等

国产自主、领先的AVL威胁检测引擎为威胁分析提供精准线索

- 海量已知威胁快速精准判定
- 最及时的威胁响应速度
- 输出丰富威胁线索和关注点

丰富全面向量提取，细粒度向量拆解，支撑威胁情报生产

- 文档说明：标题、主题、类别、备注...
- 文档内容：附带文件，宏代码...
- 动态：服务、权限、窗口、进程、网络.....

动静结合综合分析，全方位揭示威胁行为

- 静态分析与动态触发相互结合验证
- 已知威胁进行快速识别
- 未知威胁具备检出能力

分析过程灵活可控

- 优先分析
- 强制动态
- 干预分析
- 自定义规则

高仿真环境，丰富环境按需定制

- Windows 、Linux、国产操作系统...
- WPS、Office、Adobe沙箱环境...
- 户操作模拟、网络模拟、移动介质模拟等高仿真模拟

邮件场景——安天海量威胁情报能力

- 支持域名当前解析记录和历史解析记录。
- 支持域名WHOIS记录和历史解析记录。
- 数据量超过20亿，每日更新10万。

- 支持md5、sha1、sha256查询文件信誉。
- 支持输出静态/动态执行信息、多引擎扫描结果。
- 数据量超过30亿，每日新增百万。

- 涵盖操作系统的常见注册表键值。
- 支持输出使用注册表的样本。
- 规则数量超过万条。

- 收集APT报告数量超过700份
- 跟踪组织或行动超过180个，涉及14个国家和三个地区

- 涵盖CVE、CNNVD编号查询。
- 支持资产(CPE)搜索受影响的漏洞。
- 漏洞数据量超过10万个，每天更新

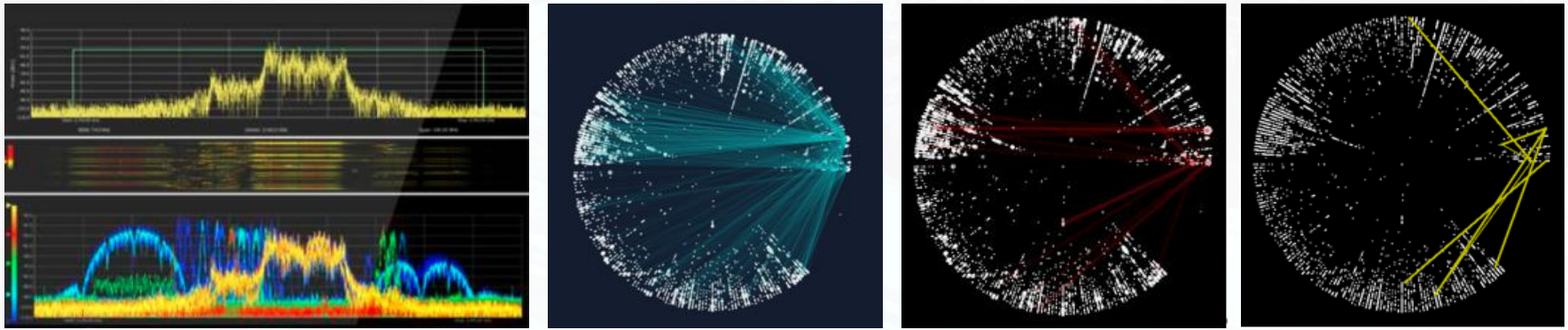
- 支持查询地理位置、ASN归属、开放端口、服务、应用等信息。
- 支持当前IP反向解析域名和历史解析记录。
- 数据量涵盖全部IPv4,每日更新十万。

- 支持输出URL关联的通讯样本，从URL下载样本、样本静态分析出的URL
- 数据量超过10亿，每日更新10万

邮件场景——安天多维度异常发现能力

安天多维度异常分析，利用关注图谱、图算法、时序频谱和神经网络等技术与异常监测结合，其目标是构建以知识为中心的异常检测。分析仿冒邮件场景，对**发件异常、收件异常、账户破解、IP多地登陆**等进行告警，可**自定义异常场景的检测条件**。

智能化异常检测



邮件异常分析

邮件场景——安天专家深度分析、处置事件

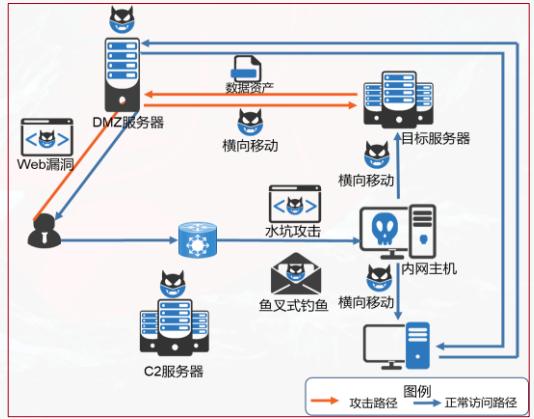
根据捕获的社工邮件事件，安全专家深度分析恶意载荷，拓展威胁线索，协助处置事件

专家深度分析

以“事前防御、事中处置、事后追溯”为目标，

深度剖析围绕邮件系统、被攻击对象的攻击事件

- 二进制分析人员逆向分析恶意载荷
- 利用安天威胁情报能力拓展恶意载荷，追踪溯源
- 协助安全事件取证、根除，关键信息留存

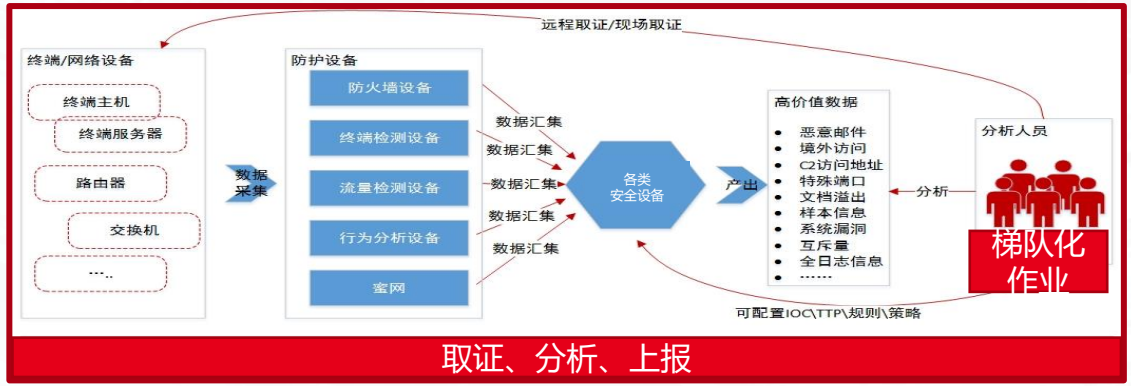


安天优势

1、国内顶尖APT分析处置团队，一流且丰富的实战经验

2、以敌情想定为基本前提，展开邮件场景威胁对抗

3、分析团队梯队化作业模式，节节阻击高烈度网空行动



安天曾捕获白象组织行动案例：检测、溯源、排查、处置

组织名称:白象

别名:Monsoon、摩诃草、Patchwork、Dropping Elephant

归属国家:南亚某国

组织性质:一般能力国家/地区行为体

攻击意图:窃取敏感数据

攻击手法:鱼叉式钓鱼、水坑攻击、0day漏洞利用、社会工程学等

影响平台:Windows、Android、macOS等

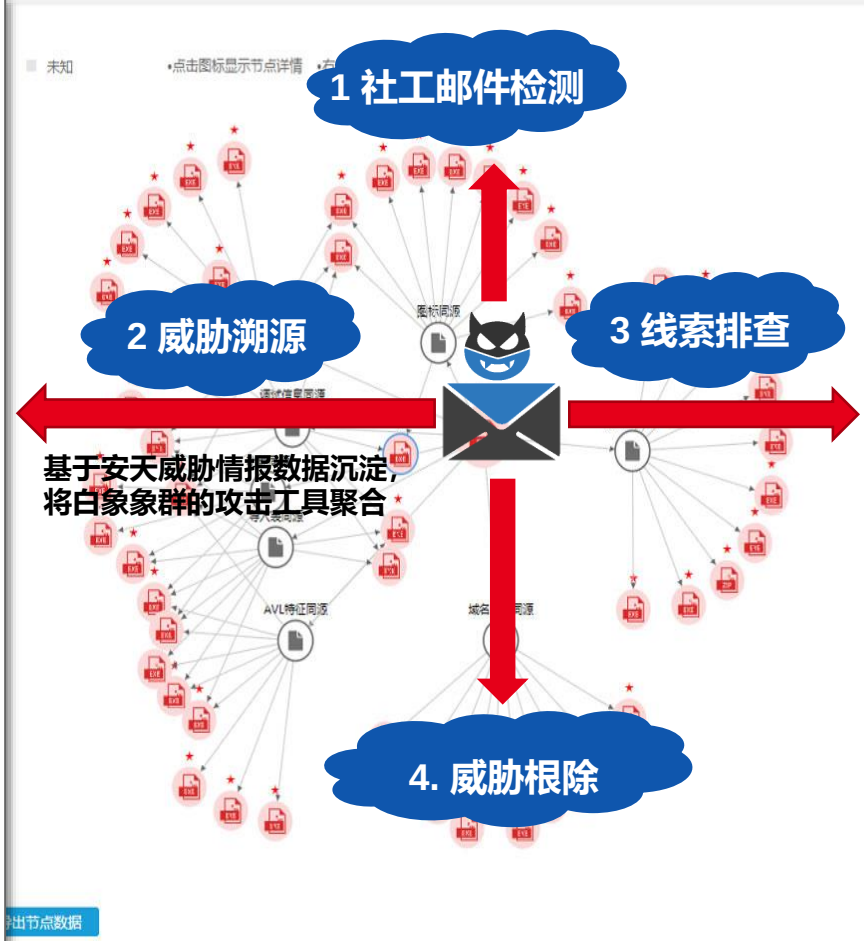
目标国家/地区:中国、巴基斯坦等

目标行业:政府、军事、教育等

利用漏洞:CVE-2017-0199、CVE-2017-8570等

攻击装备: HangOver、 DarkCometRAT、Quasar RAT、 Badnews等

IOC信息:1000+恶意样本、200+恶意URL



情报拓展威胁线索，指导排查

- 恶意HASH值
  - 00a0a6071c335f78c161cb4a3dcdc435
  - 00bd9447c13afbbb7140bef94e24b535
  - 0128f683e508c807ec76d5092eaaf22c
  - 01774e34e8a444685b1499eef3406cd0
  - 01a7af987d7b2f6f355e37c8580cb45a
  - 01adea2d3707a343f5a6d149565c7ec5
- 恶意URL
  - activetalk.org
  - add-on-update.com
  - addon-updates.com
  - adminassistance.net

专家跟进威胁及其线索，协助处置事件

谢谢大家