RISING 瑞星

# 2021

# 中国网络安全报告

北京瑞星网安技术股份有限公司
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
咨询：400-660-8866
网站：http://www.rising.com.cn

# 免责声明

本报告由北京瑞星网安技术股份有限公司发布，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的数据及资料进行收集和整理，针对中国 2021 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

# 报告摘要

- 2021 年瑞星“云安全”系统共截获病毒样本总量 1.19 亿个，病毒感染次数 2.59 亿次，病毒总体数量比 2020 年同期下降了 19.66%。广东省病毒感染人次为 2,614 万次，位列全国第一，其次为江苏省及山东省，分别为 1,870 万次及 1,835 万次。

- 2021 年瑞星“云安全”系统共截获勒索软件样本 32.22 万个，感染次数为 62.4 万次；挖矿病毒样本总体数量为 485.62 万个，感染次数为 184.11 万次。勒索软件感染人次按地域分析，广东省排名第一，为 5.79 万次；挖矿病毒感染人次按地域分析，新疆以 22.12 万次位列第一。

- 2021 年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 6,279 万个，其中挂马类网站 4,366 万个，钓鱼类网站 1,913 万个。在中国范围内排名第一位为河南省，总量为 31.53 万个，其次为北京市和广东省，分别为 17.76 万个和 17.35 万个。

- 2021 年瑞星“云安全”系统共截获手机病毒样本 275.6 万个，病毒类型以信息窃取、资费消耗、远程控制、流氓行为等类型为主，其中信息窃取类病毒占比 43.72%，位居第一。

- 2021 年重大企业安全事件包括：Incaseformat 蠕虫病毒爆发，致多数用户磁盘数据被删除；加拿大无线通信设备制造商 Sierra Wireless 遭勒索攻击，工厂中断生产；伊朗核设施遭遇网络攻击；美国最大成品油管道运营商遭勒索软件攻击；Apache Log4j2 惊现高危漏洞等。

- 2021 年 CVE 漏洞利用率 Top10 包括：CVE-2017-11882 Office 远程代码执行漏洞；CVE-2017-17215 HG532 远程命令执行漏洞；CVE-2017-0147 Windows SMB 协议漏洞 MS17-010 等；年度最热漏洞有 CVE-2021-44228 Apache log4j2 远程代码执行漏洞；CVE-2021-40444 MSHTML 远程代码执行漏洞；CVE-2021-26855 服务端请求伪造漏洞等。

- 2021 年全球 APT 攻击事件解读：威胁组织 Darkside；威胁组织 Patchwork；威胁组织 Lazarus Group；威胁组织 Transparent Tribe；威胁组织 SideWinder 和威胁组织 APT-C-23。

- 2021 年勒索软件分析：越来越多的威胁组织在勒索同时，采取文件窃取的方式来 “绑架”企业的隐私文件，以历史攻击事件梳理来看这确实卓有成效，大大提高了勒索软件敲诈赎金的成功几率。并且越来越多的攻击组织或不法分子选择运用勒索软件即服务（RaaS）这一模式进行攻击，这让不具备专业技术知识的犯罪分子可以轻而易举地发起网络敲诈活动。

- 趋势展望：APT 组织及攻击活动越来越多被披露；勒索软件持续危害企业安全；电子邮件依然是网络入侵的主要窗口；基础软件安全性备受关注，供应链“投毒”逐渐递增；高可利用性的漏洞备受攻击者青睐，“老”漏洞不会很快退出历史舞台；传统威胁检测手段进一步面临考验，人工智能技术应用增多。

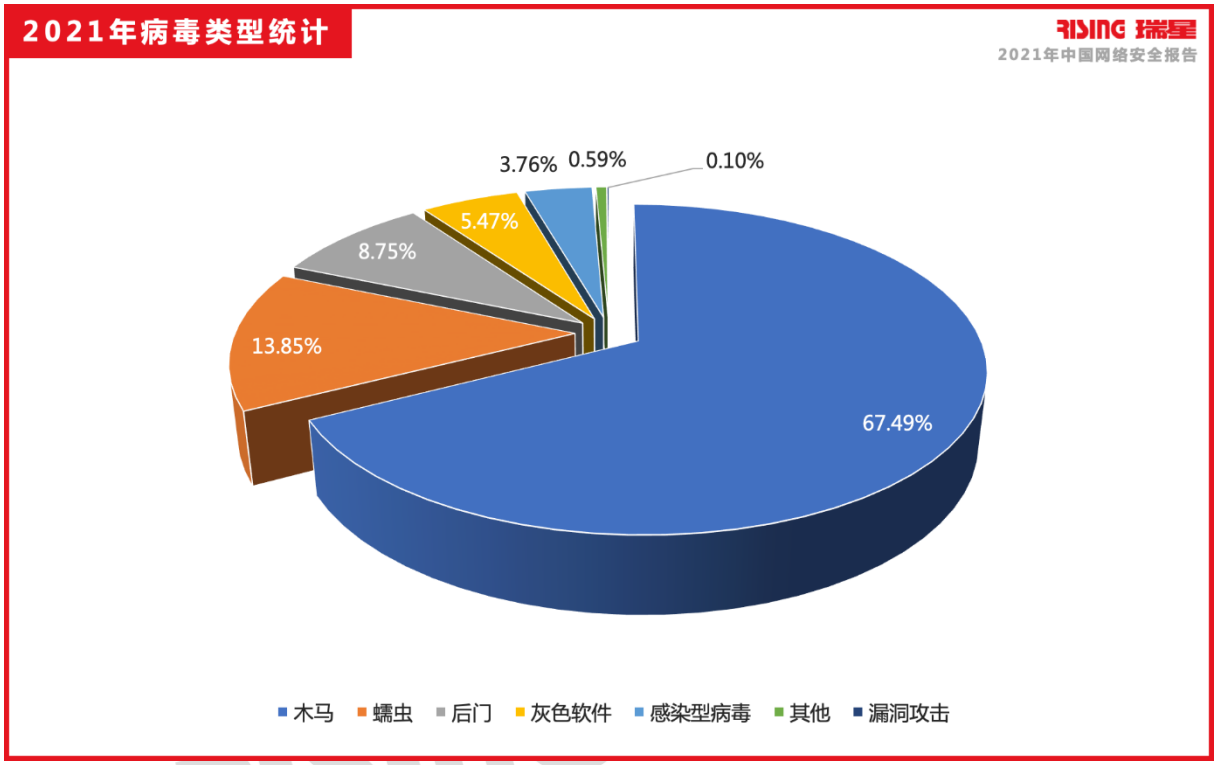
# 一、恶意软件与恶意网址

## （一）恶意软件

### 1. 2021 年病毒概述

**(1) 病毒疫情总体概述**

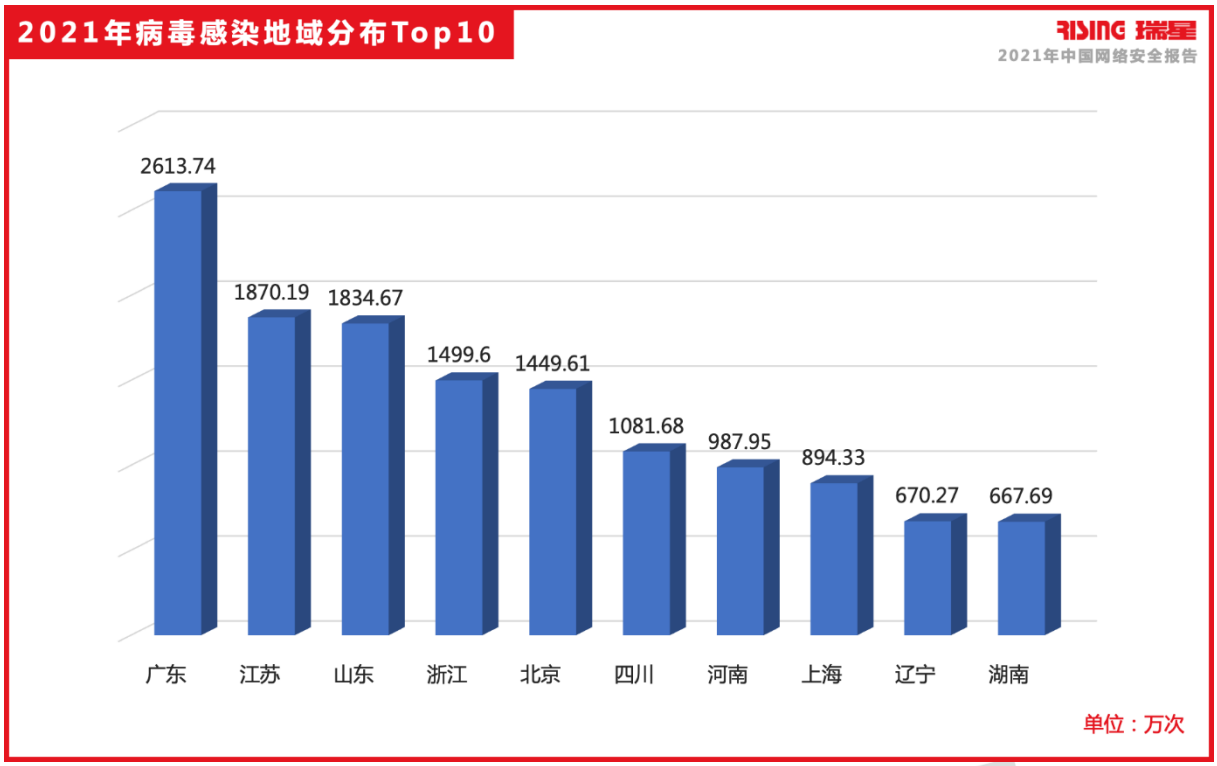
2021 年瑞星“云安全”系统共截获病毒样本总量 1.19 亿个，病毒感染次数 2.59 亿次，病毒总体数量比 2020 年同期下降了 19.66%。报告期内，新增木马病毒 8,050 万个，为第一大种类病毒，占到总体数量的 67.49%；排名第二的为蠕虫病毒，数量为 1,652 万个，占总体数量的 13.85%；后门、灰色软件、感染型病毒分别占到总体数量的 8.75%、5.47%和 3.76%，位列第三、第四和第五，除此以外还包括漏洞攻击和其他类型病毒。




图：2021 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 2,614 万次，位列全国第一，其次为江苏省及山东省，分别为 1,870 万次及 1,835 万次。




图：2021 年病毒感染地域分布 Top10

## 2. 2021 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 2021 年 1 至 12 月病毒 Top10：

2021年病毒Top10

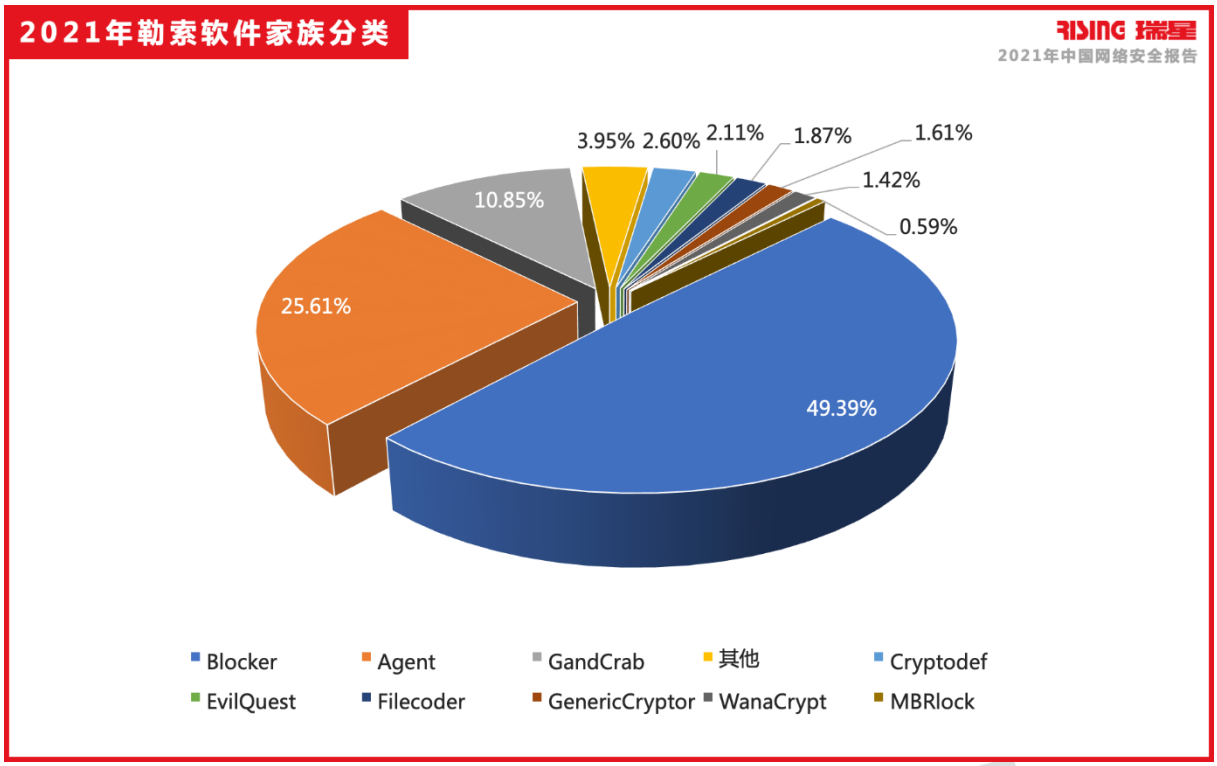
RISING 瑞星 2021年中国网络安全报告

| 排名 | 名称 | 描述 |
|---|---|---|
| 1 | Adware.Agent!1.C6F0 | 流氓软件，国内流氓软件使用的流氓模块，主要通过Web下载、共享软件等方式进行传播。 |
| 2 | Trojan.Agent!8.B1E | 木马病毒，目的通常为破坏系统、窃取用户隐私、下载其他木马，主要通过电子邮件附件、Web下载等方式进行传播。 |
| 3 | Trojan.ShadowBrokers!8.B976 | 方程式小组的黑客工具套件，该工具被病毒广泛用于传播蠕虫病毒，主要通过共享软件、免费软件等方式传播。 |
| 4 | Exploit.UAC!8.107CD | 漏洞利用程序，该程序可利用系统漏洞绕过UAC（用户账户控制），主要通过Web下载、共享软件等方式进行传播。 |
| 5 | Trojan.Zpevdo!8.F912 | 木马病毒，目的通常为破坏系统、窃取用户隐私、下载其他木马，主要通过电子邮件附件、共享软件等方式进行传播。 |
| 6 | Trojan.Vools!1.B1FA | 方程式小组的黑客工具套件，该工具释放并调用永恒之蓝等病毒进行攻击，主要通过漏洞、免费软件、下载站、共享软件等方式进行传播。 |
| 7 | Trojan.Inject!8.103 | 注入型木马病毒，该病毒会将恶意代码注入进其他程序运行，主要通过Web下载、共享软件等方式进行传播。 |
| 8 | Dropper.Generic!8.35E | 释放型木马病毒，该病毒会释放其他具有恶意行为的木马，主要通过电子邮件附件、下载站、共享软件等方式进行传播。 |
| 9 | Worm.Win32.Undef.oa | 蠕虫病毒，感染系统文件并自动传播，主要通过受感染文件、漏洞、U盘、共享软件、Web下载等方式进行传播。 |
| 10 | Trojan.Kryptik!8.8 | 恶意Crypter打包程序，通常用于保护后门、木马及间谍软件，达到逃避安全软件检测目的，主要通过电子邮件附件、Web下载等方式进行传播。 |

## 3. 勒索软件和挖矿病毒

勒索软件和挖矿病毒在 2021 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 32.22 万个，感染次数为 62.4 万次；挖矿病毒样本总体数量为 485.62 万个，感染次数为 184.11 万次。

瑞星通过对捕获的勒索软件样本进行分析后发现，Blocker 家族占比 49.39%，成为第一大类勒索软件，其次是 Agent 家族，占到总量的 25.61%，第三是 GandCrab 家族，占到总量的 10.85%。

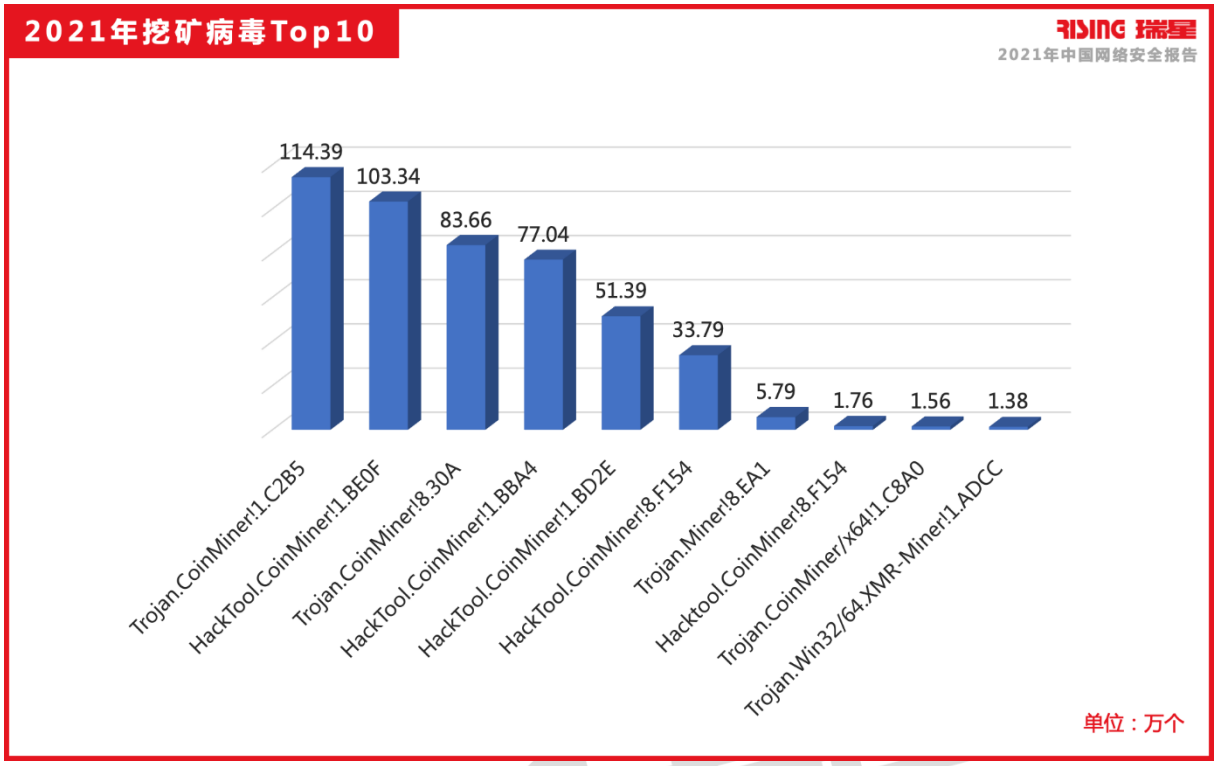



图：2021 年勒索软件家族分类

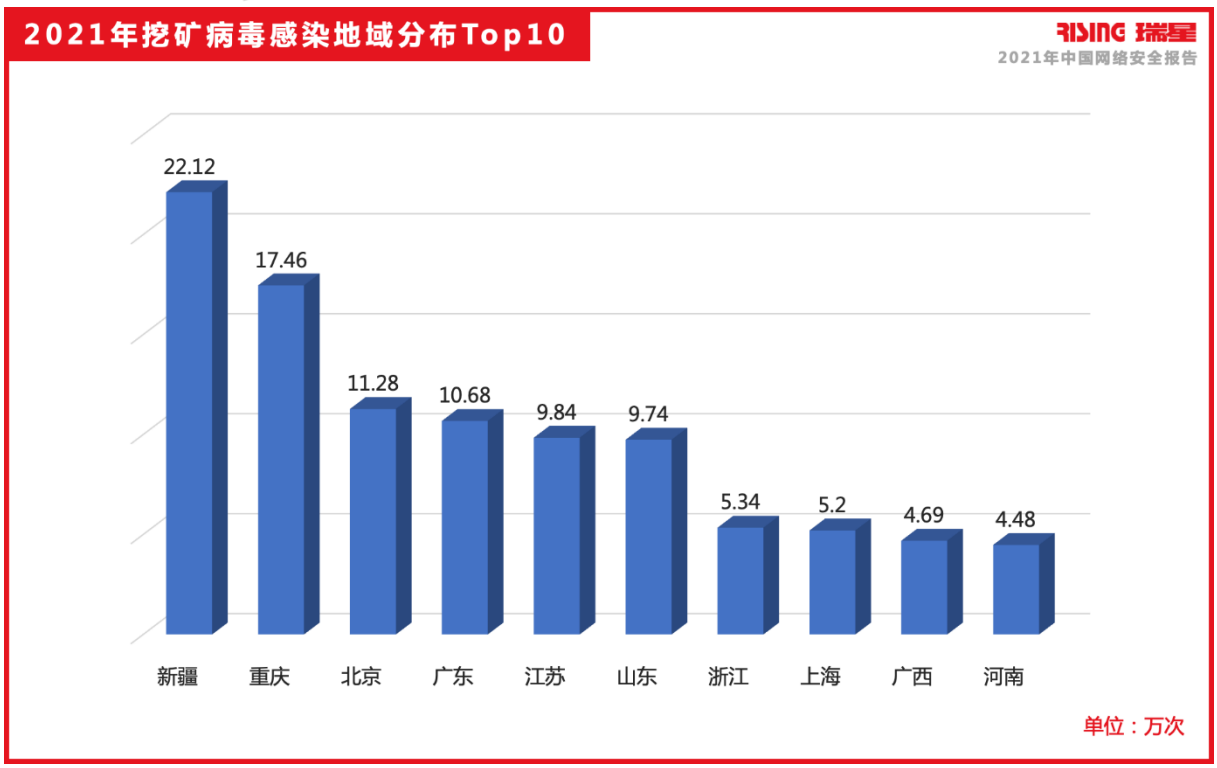
勒索软件感染人次按地域分析，广东省排名第一，为 5.79 万次，第二为江苏省 5.5 万次，第三为山东省 5.27 万次。


图：2021 年勒索软件感染地域分布 Top10

挖矿病毒在 2021 年依然活跃，瑞星根据病毒行为进行统计，评出 2021 年挖矿病毒 Top10：




挖矿病毒感染人次按地域分析，新疆以 22.12 万次位列第一，重庆市和北京市分别位列二、三位，为 17.46 万次和 11.28 万次。

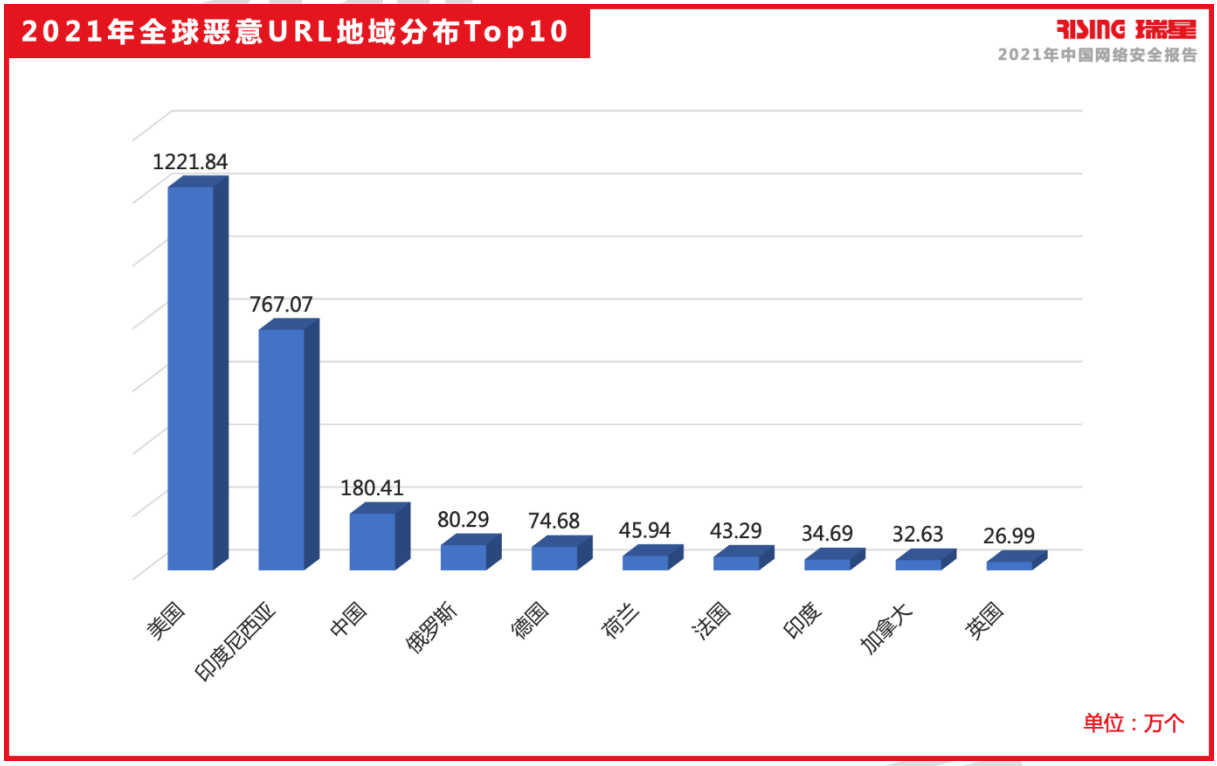


图：2021 年挖矿病毒感染地域分布 Top10

## （二）恶意网址

### 1. 2021 年全球恶意网址概述

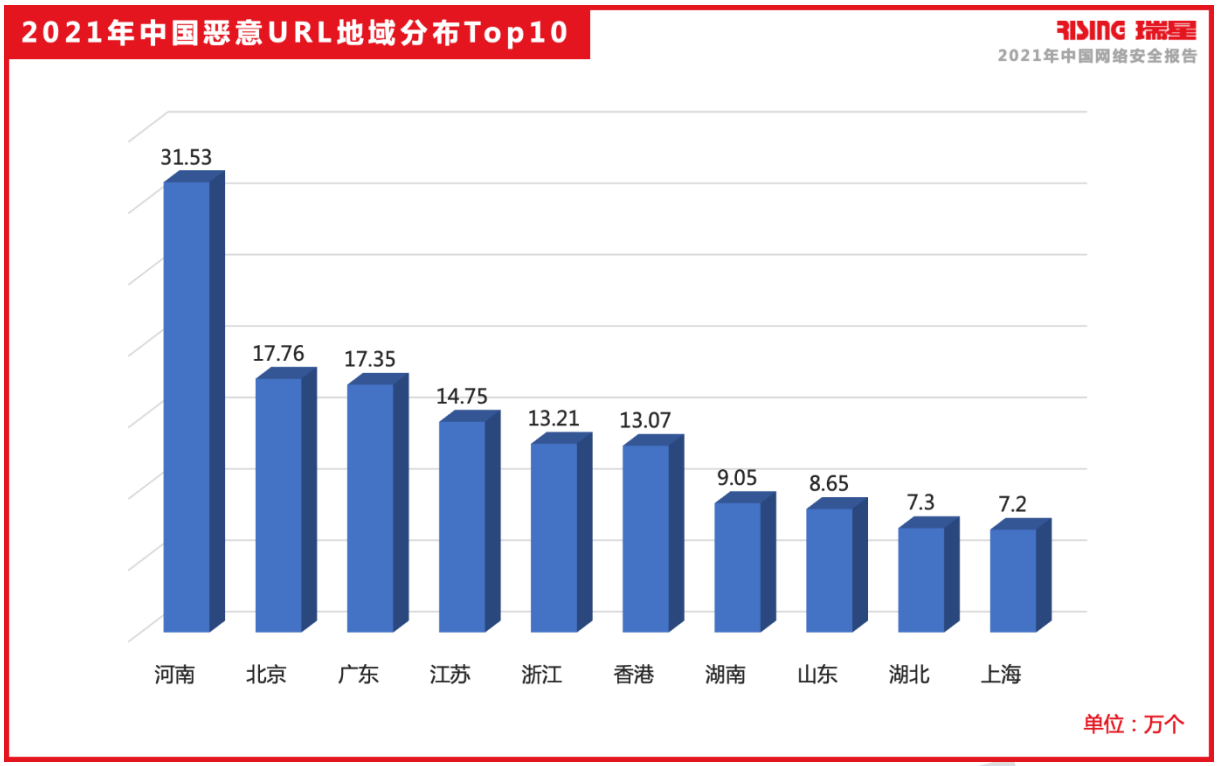
2021 年瑞星“云安全”系统在全球范围内共截获恶意网址（URL）总量 6,279 万个，其中挂马类网站 4,366 万个，钓鱼类网站 1,913 万个。美国恶意 URL 总量为 1,222 万个，位列全球第一，其次是印度尼西亚 767.07 万个和中国 180.41 万个，分别排在二、三位。




图：2021 年全球恶意 URL 地域分布 Top10

### 2. 2021 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，第一位为河南省，总量为 31.53 万个，其次为北京市和广东省，分别为 17.76 万个和 17.35 万个。

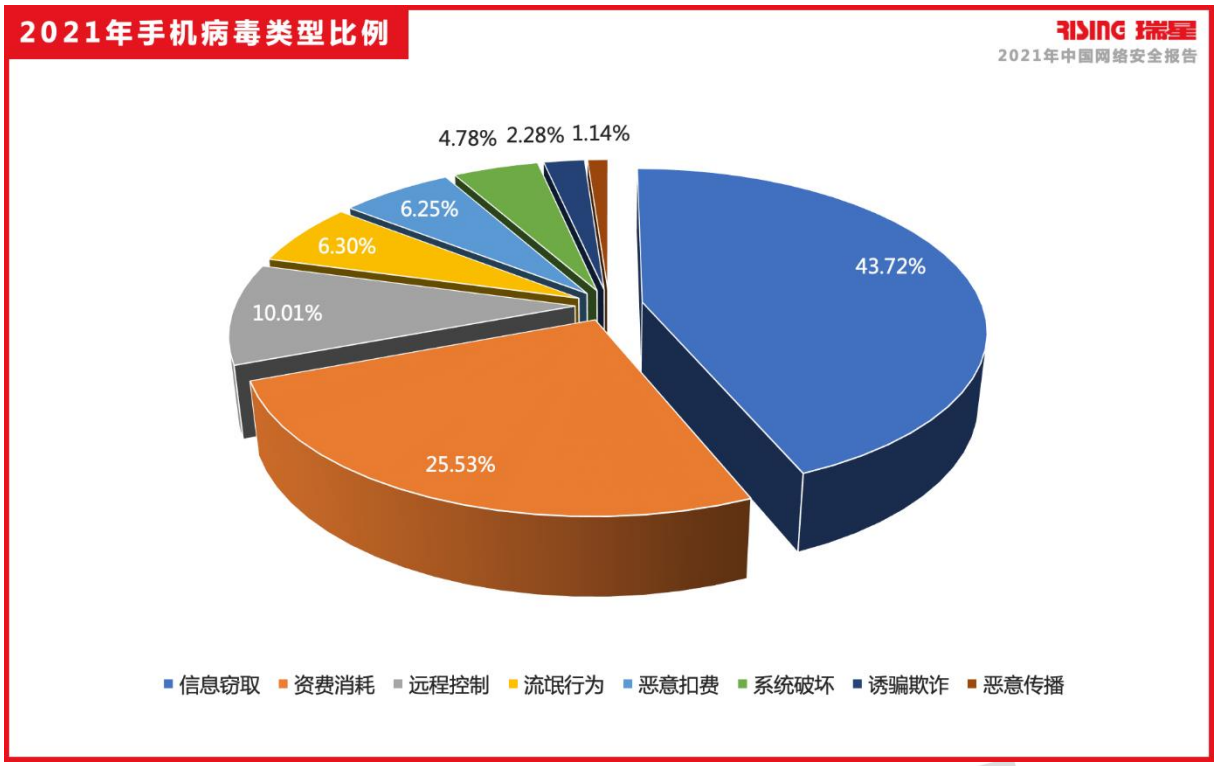



图：2021 年中国恶意 URL 地域分布 Top10

# 二、移动安全

## （一）2021 年手机病毒概述

2021 年瑞星“云安全”系统共截获手机病毒样本 275.6 万个，病毒类型以信息窃取、资费消耗、远程控制、流氓行为等类型为主，其中信息窃取类病毒占比 43.72%，位居第一；其次是资费消耗类病毒占比 25.53%，第三名是远程控制类病毒占比 10.01%。




图：2021 年手机病毒类型比例

## （二）2021 年 1 至 12 月手机病毒 Top5


| 排名 | 名称 | 描述 |
|---|---|---|
| 1 | 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，主要通过免费软件、下载站、共享软件等方式进行传播。 |
| 2 | Adware.Mobby/Android!8.A0FC | 广告软件，包含Mobby广告SDK的软件，该软件主要通过Web下载、共享软件等方式进行传播。 |
| 3 | Dropper.Agent/Android!8.37E | 释放型木马病毒，该病毒会释放其他木马并运行，主要通过下载站、共享软件等方式进行传播。 |
| 4 | Trojan.Obfus/Android!8.3F7 | 带混淆的木马病毒，该病毒常使用混淆工具规避安全软件检测，主要通过免费软件、Web下载等方式进行传播。 |
| 5 | Trojan.Agent/Android!8.358 | 安卓木马病毒，目的通常为破坏系统、窃取用户隐私、下载其他木马，主要通过免费软件、下载站、共享软件等方式进行传播。 |

## （三）2021 年手机漏洞 Top5

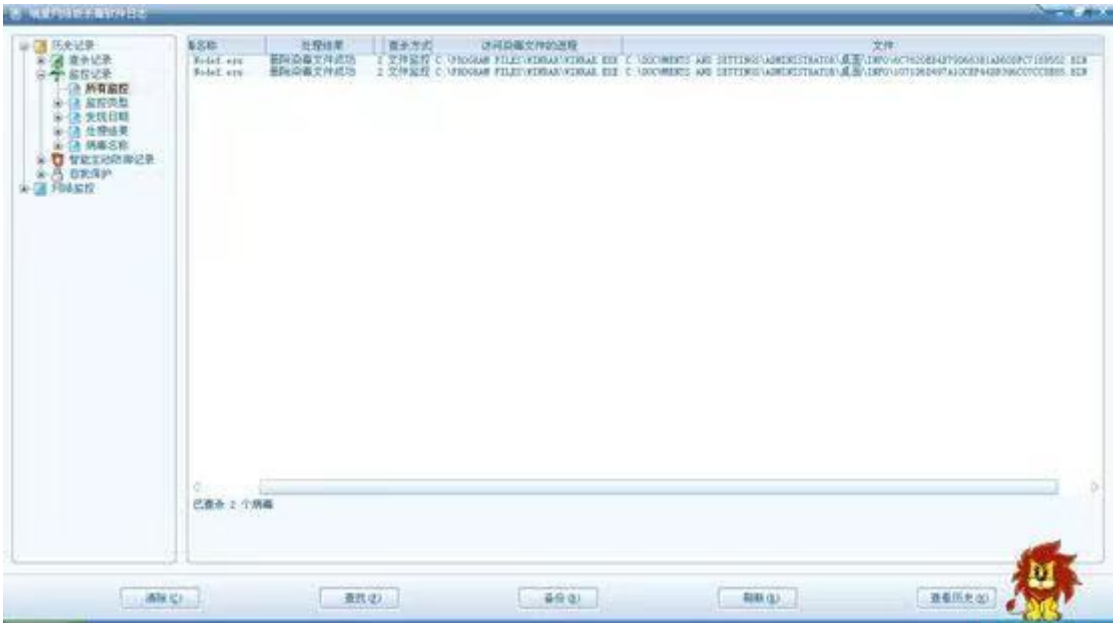

| 排名 | 名称 | 描述 |
|---|---|---|
| 1 | 多款 Samsung 产品缓冲区错误漏洞 CVE-2021-22492 | 该漏洞因为蓝牙UART驱动程序有缓冲区溢出，使得Samsung mobile devices O(8.x)、Samsung mobile devices P(9.0)和Samsung mobile devices Q(10.0)(Broadcom蓝牙芯片组)软件存在缓冲区错误漏洞，远程攻击者可利用该漏洞执行任意代码。 |
| 2 | Google Android 缓冲区错误漏洞 CVE-2021-0515 | 该漏洞存于Android-8.1，Android-9，Android-10和Android-11中，源于在factory.cc的Factory::CreateStrictFunctionMap中边界错误，这可能导致发生越界写入。攻击者可利用该漏洞在目标系统上执行任意代码。 |
| 3 | Amazon AWS SDK for Android安全漏洞CVE-2021-40527 | 该漏洞影响了com.onepeloton.erlich移动应用程序（包括版本 1.7.22），源于受影响产品将敏感信息暴露给未经授权的参与者。攻击者可利用该漏洞读取移动应用程序中以纯文本形式存储的凭证，来访问存储在 AWS S3存储桶中的开发人员文件。 |
| 4 | Apple iOS 缓冲区错误漏洞 CVE-2021-30666 | 该漏洞存于Apple iOS 12.5到12.0系统中，由于Safari浏览器引擎WebKit中的边界错误，使得该系统存在了缓冲区错误漏洞，远程攻击者可利用该漏洞执行任意命令。 |
| 5 | MediaTek 芯片 资源管理错误漏洞 CVE-2021-0670 | 多款MediaTek芯片存在安全漏洞，源于在apusys 中由于use-after-free可能导致内存损坏，这可能导致本地权限提升，攻击者可利用该漏洞在特权进程的上下文中执行任意代码。漏洞利用不需要用户交互。 |

# 三、企业安全

## （一）2021 年重大企业网络安全事件

### 1. Incaseformat 蠕虫病毒爆发，致多数用户磁盘数据被删除

2021 年 1 月 13 日，Incaseformat 蠕虫病毒爆发。瑞星公司接到大量用户求助，这些用户电脑非系统盘中的所有文件均被删除。根据瑞星安全研究院分析发现，这是一个名为 Incaseformat 的蠕虫病毒所致，该蠕虫病毒主要通过 U 盘等方式进行传播，当其感染 U 盘后，U 盘下的原文件夹将被隐藏，病毒会伪装成原文件夹。一旦用户再插入受感染 U 盘就会误以为真，点击运行后，病毒就会感染除 C 盘之外其他磁盘上的文件夹，并在指定时间段内删除系统中 C 盘之外磁盘上的所有数据。经过分析，这并不是一个新病毒，瑞星杀毒软件在 2013 年就可以查杀，本次突然发作是因为病毒内存在时间开关。



图：瑞星拦截查杀 Incaseformat 蠕虫病毒

## 2. 新加坡电信巨头近 13 万客户信息遭泄露，涉身份证号等

2021 年 2 月 17 日，新加坡知名电信公司新电信（Singtel）在其官网发布消息称，由第三方供应商 Accellion 提供的名为 FTA 的第三方文件共享系统受到不明身份黑客的非法攻击，导致数据泄露。此次遭泄露的数据包括：约 129000 名新电信客户的个人信息，含姓名、身份证号（National Registration Identity Card，NRIC）、出生日期、手机号码、地址等隐私信息。

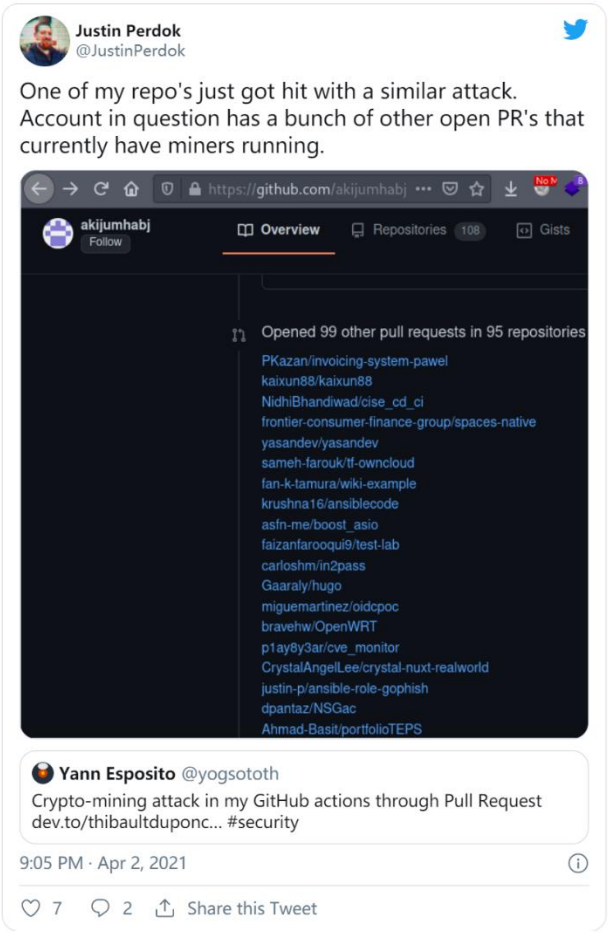

图：新电信公司公告

## 3. 加拿大无线通信设备制造商 Sierra Wireless 遭勒索攻击，工厂中断生产

2021 年 3 月 20 日，加拿大 Sierra Wireless 无线设备制造公司的 IT 系统遭到勒索软件攻击，勒索软件对 Sierra 的内部 IT 网络进行了加密，阻止员工访问与制造和计划相关的内部文档和系统，该事件导致公司在全球各地的生产基地停产。

## 4. 攻击者利用 GitHub Action 在 GitHub 服务器上挖矿

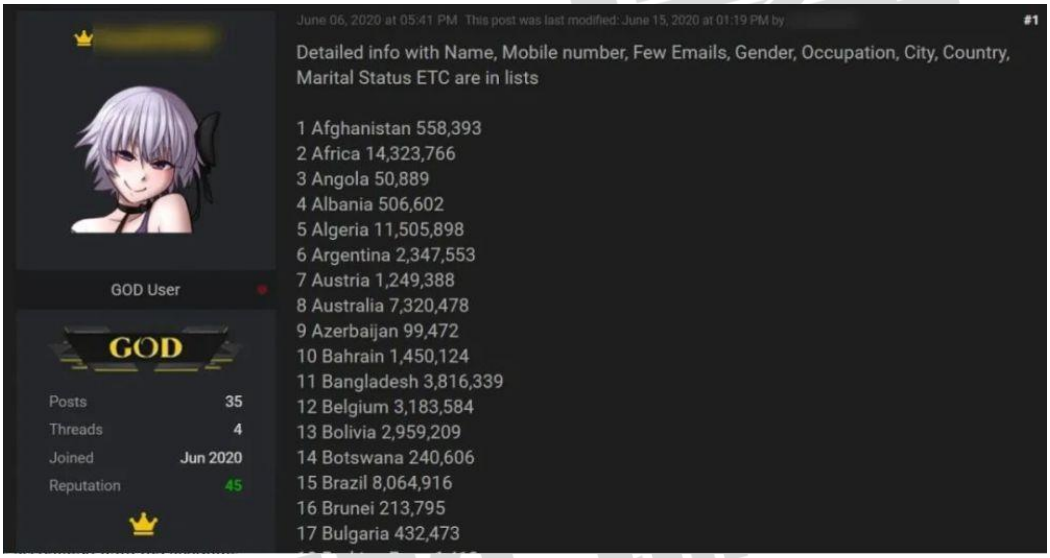
2021 年 4 月 3 日，有开发者发现，黑客滥用 GitHub Actions 功能在 GitHub 服务器上植入挖矿软件，利用 GitHub 资源来开采加密货币。据悉，自 2020 年 11 月开始，攻击者就发现了 GitHub Actions 的一个 Bug：提交含有恶意代码的 Pull Request 时，无需项目原作者同意即可运行恶意代码。一旦这些恶意 Pull Request 被提交，GitHub 系统就会读取这些代码并启动一个虚拟机，而该虚拟机就会在 GitHub 的基础架构上下载并运行加密货币挖掘软件。




图：荷兰安全工程师 Justin Perdok 分享的屏幕截图

## 5. Facebook5.33 亿用户数据被发布

2021 年 4 月 7 日，国外有媒体爆料称，5.33 亿 Facebook 用户的数据，包括电话号码、Facebook ID、全名、出生日期和其他信息都被发布在网上。安全公司哈德逊洛克（hudsonrock）的首席技术官阿隆•加尔在推特上发布了这个数据。加尔公布了受影响用户的国家名单，根据他的名单，美国有 3230 万受影响用户，英国有 1150 万。Facebook 解释，公司无法判断是哪些用户的信息被泄露，无法通知到个人，并表示用户自身也解决不了问题，没有告知的必要。



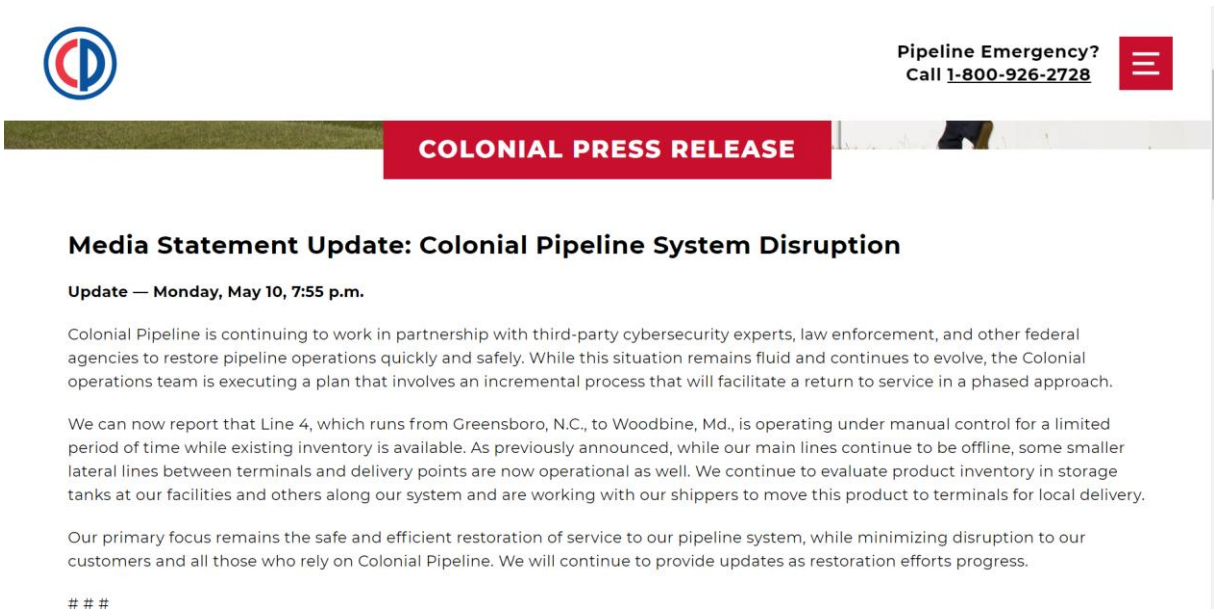

图：某黑客论坛公布了超过 5.33 亿 Facebook 用户数据

## 6. 伊朗核设施遭遇网络攻击

2021 年 4 月 13 日，据国外媒体报道，位于德黑兰以南的伊朗核设施遭到了网络攻击。伊朗负责核安全的相关负责人 Ali Akbar Salehi 称，此次网络攻击的目标为 Natanz 核设施，在此次袭击发生的前两天，伊朗刚刚发布新的浓缩铀设备。由于该设备不仅可以用于浓缩核电使用的铀原料，亦可以用于生产武器级浓缩铀，美国科学家联合会表示此离心机可能引起非常严重的核武器扩散问题。有关于此次网络攻击事件，Salehi 认为这是针对伊朗正常核计划的“恐怖袭击”。

## 7. 美国最大成品油管道运营商遭勒索软件攻击

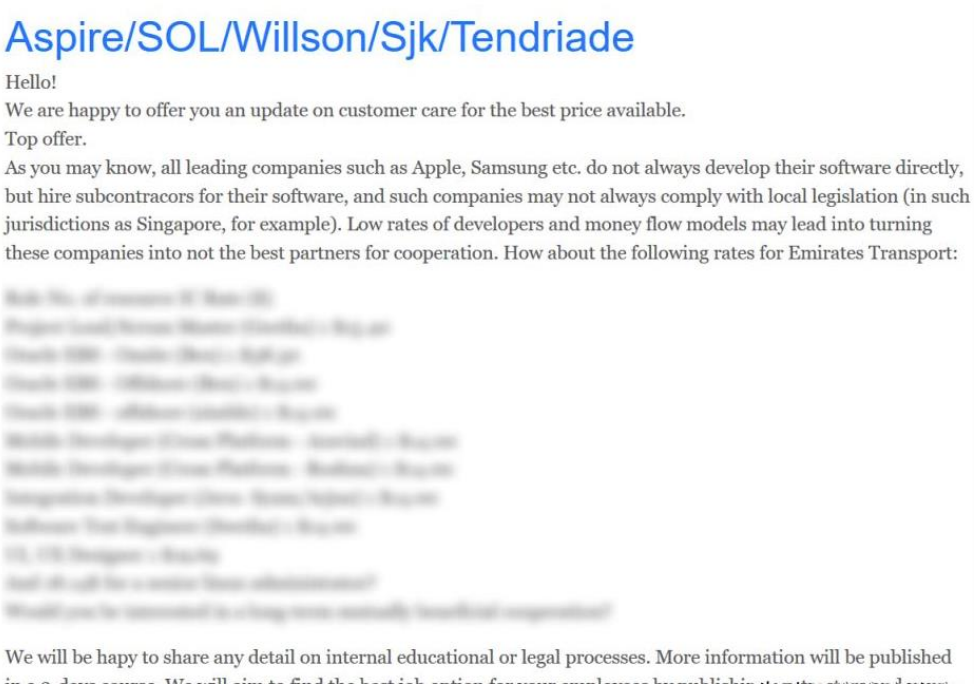
2021 年 5 月 7 日，美国最大成品油管道运营商 Colonial Pipeline 公司的工业控制系统遭到攻击组织 DarkSide 的网络攻击，该事件导致 Colonial Pipeline 公司被迫中断了东部沿海主要城市输送油气的管道系统运营。而后，该公司向负责该事件的 DarkSide 网络攻击组织支付了 500 万美元的赎金，此次攻击影响让长达 5500 英里的管道所服务的许多市场出现燃料短缺。




图：Colonial Pipeline 公司官方声明

# 8. 美国核武器承包商 Sol Oriens 遭 REvil 勒索软件攻击

2021 年 6 月初，有消息披露，美国能源部(DOE)分包商与国家核安全局(NNSA)合作开发核武系统的 Sol Oriens 公司遭到了 REvil 勒索软件攻击，该公司称其主要协助国防部、能源部、航空航天承包商和技术公司开展复杂的项目。REvil 团伙正在拍卖攻击期间窃取的数据，其中包括业务数据和员工信息，例如员工社会安全号码、招聘概览文件、工资单文件和工资报告等。Sols Oriens 也证实了其在 2021 年 5 月遭到了网络攻击，可能已经泄露部分数据。



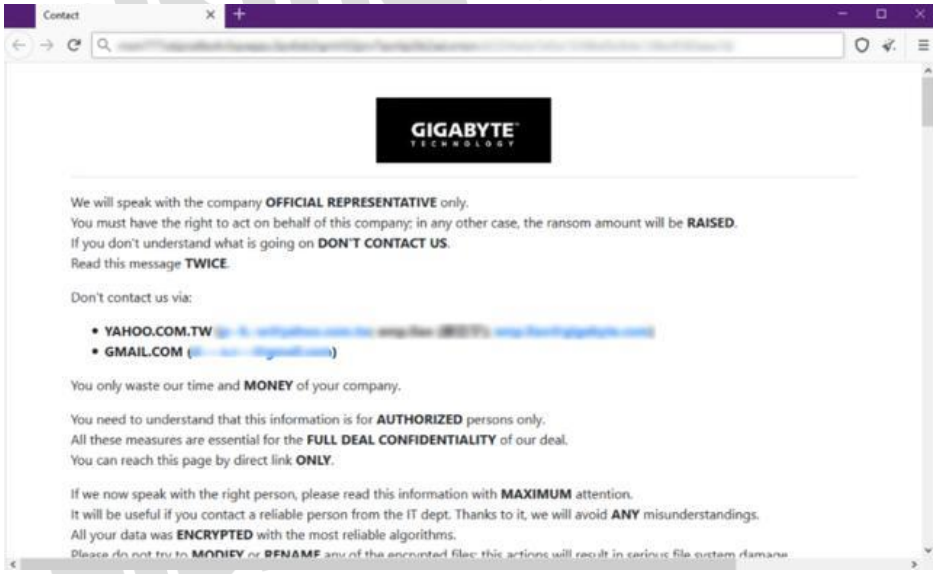

图：REvil 勒索软件的暗网数据网站中 Sol Oriens 公司被盗数据的信息

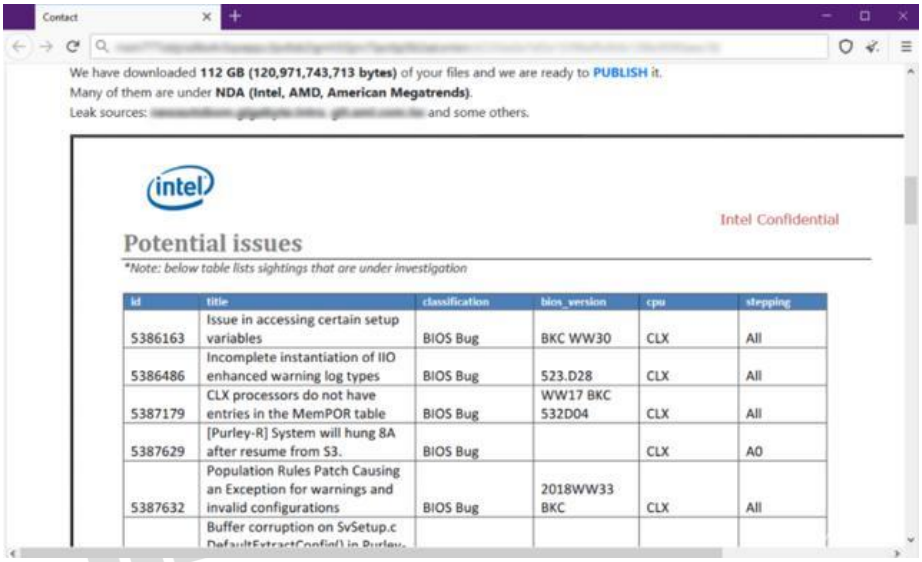
## 9. 伊朗交通部门连续遭到网络攻击

2021 年 7 月 10 日，伊朗道路和城市发展部遭到网络攻击，门户网站无法运行。此前一天，伊朗铁路公司也遭到网络攻击。网络安全公司 SentinelOne 的研究人员在一份新报告中重建了对伊朗火车系统的网络攻击并发现了一种新的威胁因素，他们将其命名为 MeteorExpress，这是一种以前从未见过的 wiper。据报道，wiper 可以更改所有用户的密码、禁用屏幕保护程序、基于目标进程列表终止进程、安装屏幕锁、禁用恢复模式、更改启动策略错误处理、创建计划任务、注销本地会话、删除影子副本、更改锁定屏幕图像和执行要求。

## 10. 技嘉遭勒索软件攻击 黑客威胁称不支付赎金就公开 112GB 内部数据

2021 年 8 月 7 日消息，硬件厂商技嘉表示，公司于本周二晚上遭到勒索软件攻击，但没有对生产系统产生影响，因为攻击的目标是位于总部的少量内部服务器。技嘉表示由于安全团队的迅速行动，服务器已从备份中恢复并重新上线，但事件远未结束。援引外媒 The Record 报道，勒索软件团伙 RansomExx 对本次攻击负责，该团伙声称拥有 112GB 的数据，其中包括技嘉和 Intel、AMD 和 American Megatrends 的机密通信。该组织威胁要公开所有内容，除非技嘉愿意支付赎金。






图：黑客威胁要在暗网上发布超过 112GB 的商业数据

## 11. T-Mobile 遭黑客入侵致用户资料外泄，受影响人数增至 5300 万

2021 年 8 月 16 日，美国移动通信运营商 T-Mobile US 披露，因黑客入侵导致用户资料外泄，受影响人数增至 5300 万。T-Mobile 指出，美国联邦通信委员会（FCC）已经就该事件展开调查。T-Mobile 本周较早时估计，资料外泄用户数量超过 4000 万个，其中包括 780 万名现有客户。外泄的资料包括用户姓名、出生日期、电话号码，但信用卡等个人财务资料则没有外泄。

## 12. 南非司法部网络系统遭到黑客攻击陷入瘫痪

2021 年 9 月 6 日，勒索软件攻击并加密了南非司法和宪法发展部所有系统，导致内部和公众无法使用所有电子服务。南非司法和宪法发展部发言人 Steve Mahlangu 表示：“（攻击）导致所有信息系统被加密，内部员工以及公众都无法使用。因此，该部门提供的所有电子服务都受到影响，包括签发授权书、保释服务、电子邮件和部门网站。” Mahlangu 表示，该部的 IT 专家已经发现“没有数据泄露的迹象”。到目前为止，还没有任何一个拥有数据泄露网站的团伙声称对这次攻击负责。

the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

MEDIA ADVISORY

09 September 2021

THE DEPARTMENT OF JUSTICE'S IT SYSTEM ATTACKED BY RANSOMWARE

The department of Justice and Constitutional Development has established that its Information Technology systems have been interrupted due to a security breach. The breach was affected through ransomware on the evening of 6 September 2021.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

图：南非司法部官方说明

## 13. 欧洲呼叫中心巨头分部遭勒索软件攻击，多个关基组织客服中断

2021 年 9 月，欧洲规模最大客户服务与呼叫中心供应商之一 Covisian 公司的西班牙与南美洲分部 GSS 遭遇勒索软件攻击，其大部分 IT 系统瘫痪，面向西班牙语区客户群体的呼叫中心应声沦陷。一位了解内情的消息人士表示，受到影响的呼叫中心用户包括移动运营商西班牙沃达丰、电信运营商 MasMovil、马德里市供水公司、多家电视台及私营企业。母公司 Covisian 的一位发言人表示，此次攻击出自 Conti 勒索软件团伙之手。

## 14. 加拿大多省医疗卫生系统因网络攻击而中断

2021 年 10 月 30 日，加拿大纽芬兰省和拉布拉多省均遭受网络攻击，导致中央卫生局、东部卫生局、西部卫生局和拉布拉多-格伦费尔地区卫生局等多地医疗卫生系统发生严重的网络中断，数千个医疗预约被迫取消。受网络中断影响，医生无法访问医疗中心数据库，只能采取纸质化方式办公；受影响的医疗中心也被迫取消了化疗、X 光扫描、手术和其他专科医疗服务的预约，仅保留了疫苗接种和急危重症患者收治服务通道。此外，网络中断还引发了多地通讯瘫痪，有患者称无法打通医疗急救中心电话。

## 15. 美国 FBI 服务器遭黑客入侵！超 10 万人收到虚假邮件

2021 年 11 月 13 日，隶属于美国司法部的情报机构，美国联邦调查局（FBI）邮件系统遭到黑客入侵。黑客使用 FBI 的电邮账号发送了超过 10 万封虚假电子邮件，并警告可能将发生网络攻击事件。FBI 指出，发送虚假邮件的电子邮箱域名看上去似乎是 FBI 的官方邮箱，且邮件的署名为美国国土安全部。FBI 表示，黑客攻击造成的软件漏洞目前已被修复。


图：联邦调查局就虚假电子邮件事件发表声明

## 16. Apache Log4j2 惊现高危漏洞

2021 年 11 月 24 日，阿里云安全团队向 Apache 官方报告了 Apache Log4j2 远程代码执行漏洞。Apache Log4j2 是一个基于 Java 的日志记录工具，该工具重写了 Log4j 框架，并且引入了大量丰富的特性，Apache Log4j-2 是 Log4j 的升级版，这个日志框架被大量用于业务系统开发，用来记录日志信息。在大多数情况下，开发者可能会将用户输入导致的错误信息写入日志中，而攻击者则可以利用此特性通过该漏洞构造特殊的数据请求包，最终触发远程代码执行。

## 17. 战网遭受 DDoS 攻击 暴雪表示服务已恢复正常

2021 年 11 月 25 日，暴雪表示旗下战网服务正遭到 DDoS 攻击。在推特上，官方说此次攻击会导致玩家遇到高延迟或是断线，并表示正在尽全力缓解问题。宣布遭受攻击 1 小时后，官方发推称正在试图缓解的 DDoS 攻击已经结束，玩家应该可以再次正常登录战网。在服务器检测网站 DownDetector 上，动视暴雪的许多服务和产品都出现了服务器断线报告，有数千人报告战网掉线，同时也有数百人表示部分暴雪游戏服务断线。


图：暴雪官方公告

## 18. IT 服务商 Inetum 遭 Blackcat 勒索软件攻击

2021 年 12 月下旬，法国 IT 服务商 Inetum Group 遭勒索软件攻击，官方声明攻击并不涉及大型基础设施，只影响了法国的部分业务，且公司立刻采取行动保护敏感数据，未出现数据泄露。官方声明没有提及遭哪个勒索软件组织攻击，但法国出版物 LeMagIt 的主编透露此次攻击为之前报告的今年最复杂勒索软件 Blackcat 组织所为。

# （二）2021 年漏洞分析

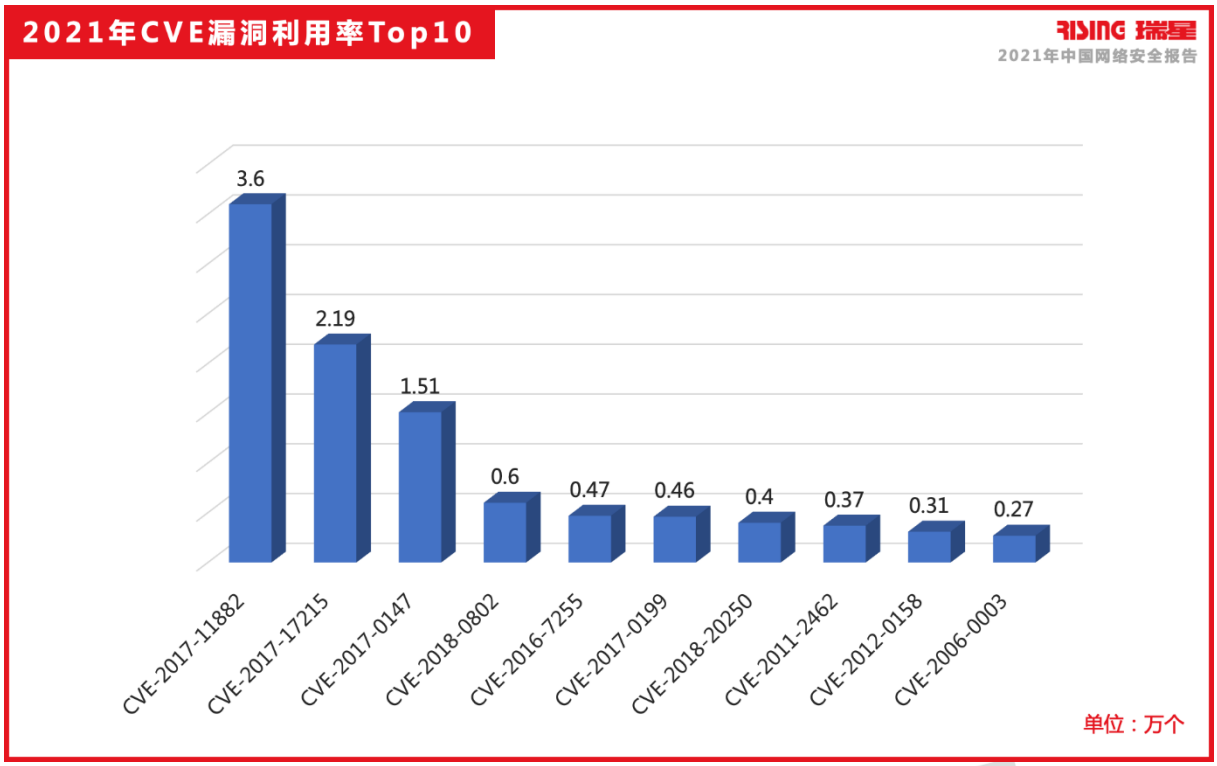
## 1. 2021 年 CVE 漏洞利用率 Top10

报告期内，从收集到的病毒样本分析来看，利用最多的漏洞依然是微软 Office 漏洞。CVE-2017-11882、CVE-2018-0802、CVE-2017-0199 得益于漏洞稳定性、易用性和用户群体广泛性一直是钓鱼邮件攻击者首选的利用漏洞。诸如 Patchwork、SideWinder、Donot 等 APT 组织以及 Emotet、AgentTesla 等间谍软件、银行木马也都十分善于利用这些 Office 漏洞实现对受害目标群体的广泛攻击。

CVE-2017-0147 Windows SMB 协议漏洞（MS17-010 永恒之蓝漏洞）在 2017 年爆发，至今已经过去 4 年时间，然而它仍是目前被病毒利用最多的安全漏洞之一。该漏洞之所以有着居高不下的利用率，也正是由于在大多数企业内网环境中依然存在大量的终端设备尚未修复该漏洞，进入内网环境的病毒程序仍可透过该漏洞轻松地在内网环境中传播。

Log4j2 远程代码执行漏洞(CVE-2021-44228)可以说是引爆 2021 年安全行业的重大事件。Apache Log4j2 是 Apache 开源的项目，是一款优秀的 Java 日志框架，用来记录日志信息，在各类 Java 项目中应用十分广泛。12 月 9 日晚 Log4j2 爆出严重漏洞，其相关利用被公开并迅速地在网络上扩散，引起各国高度重视，一时间全球近一半企业与之相关的业务均受到该漏洞的影响，同时也出现了诸如比利时国防部被不法分子利用 Log4j 漏洞进行攻击等事件。

瑞星根据漏洞被黑客利用程度进行分析，评选出 2021 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-2017-17215 HG532 远程命令执行漏洞

2017 年 11 月份 Check Point 团队报告了国内某产品的远程命令执行漏洞(CVE-2017-17215),漏洞原理是利用 upnp 服务器中的注入漏洞来实现远程执行任意代码，已发现的针对该漏洞的攻击利用是 Mirai 的升级变种。

## 1.3 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，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。

## 1.4 CVE-2018-0802 公式编辑器漏洞

此漏洞与它的上一代 CVE-2017-11882 一脉相承，同属于 Microsoft Office 中的 EQNEDT32.EXE 公式编辑器的漏洞。该漏洞又被称为“噩梦公式”，源于对象在内存中的处理不当（微软 Office 内存破坏漏洞），当用户打开特制的嵌有公式编辑器对象的 Office 文档时会直接触发漏洞导致任意代码执行。

## 1.5 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。

## 1.6 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。

## 1.7 CVE-2018-20250 WinRAR 目录穿越漏洞

UNACE.DLL 是 WinRAR 所使用的一个陈旧的动态链接库，用于处理 ACE 格式的文件，该动态链接库在 2006 年被编译，没有任何防护措施。WinRAR 在解压处理 ACE 格式的文件的过程中存在一处目录穿越漏洞，该漏洞允许解压过程中向任意目录写入文件，利用该漏洞可以向开机启动目录中写入恶意文件导致机器开机时执行恶意代码。

## 1.8 CVE-2011-2462 远程代码执行漏洞

Windows 和 Mac OS X 上的 Adobe Reader 和 Acrobat 10.1.1 及更早版本以及 UNIX 上的 Adobe

Reader 9.x 至 9.4.6 中的 U3D 组件中存在未指定的漏洞，允许远程攻击者通过未知载体执行任意代码或导致拒绝服务(内存损坏)，正如在 2011 年 12 月被广泛利用的那样。

### 1.9 CVE-2012-0158 Microsoft Office 栈溢出漏洞

此漏洞主要是在 MSCOMCTL.OCX 模块中,一段内存拷贝代码由于逻辑错误导致栈缓冲区溢出的漏洞。该漏洞常在各类 APT 攻击活动中被利用，通过生成一个精心构造的恶意 RTF 文件可以使攻击者通过该漏洞在 RTF 文件被打开时执行任意代码。

### 1.10 CVE-2006-0003 RDS.Dataspace 远程代码执行漏洞

RDS.Dataspace ActiveX 控件中存在未指明的漏洞，它包含在 ActiveX 数据对象(ADO)中并分布在 Microsoft 数据访问组件(MDAC) 2.7 和 2.8 中，允许远程攻击者通过未知的攻击媒介执行任意代码。

## 2. 2021 年最热漏洞分析

### 2.1 CVE-2021-44228 Apache log4j2 远程代码执行漏洞

2021 年 12 月 9 日晚 Apache log4j2 被曝出远程代码执行漏洞。由于 Apache Log4j2 某些功能存在递归解析功能,攻击者可直接构造恶意请求,触发远程代码执行漏洞。该漏洞无需配置,且 Apache Struts2、Apache Solr、Apache Druid、Apache Flink 等均受影响。Apache Log4j2 是一款流行的 Java 日志记录工具，该工具重写了 Log4j 框架，并且引入了大量丰富的特性。该日志框架被大量用于业务系统开发，用来记录日志信息。大多数情况下，开发者可能会将用户输入导致的错误信息写入日志中。此次漏洞触发条件为只要外部用户输入的数据会被日志记录，即可造成远程代码执行。

### 2.2 CVE-2021-40444 MSHTML 远程代码执行漏洞

2021 年 9 月 7 日，微软发布了 Windows IE MSHTML 中的一个远程代码执行漏洞。攻击者可通过制作恶意的 ActiveX 控件供托管浏览器呈现引擎的 Microsoft Office 文档使用，成功诱导用户打开恶意文档后，可在目标系统上以该用户权限执行任意代码。微软称该漏洞可通过 Office 365 和 Office2019 在受影响的 windows 10 主机上下载和安装恶意软件。

### 2.3 CVE-2021-27065 Exchange 任意文件写入漏洞

2021 年 3 月微软官方发布了 Microsoft Exchange 安全更新修复了任意文件写入漏洞，攻击者

可结合 CVE-2021-26855 SSRF 漏洞，或提供正确的 administrator 凭证，构造恶意请求，在系统上写入任意文件。

## 2.4 CVE-2021-26855 服务端请求伪造漏洞

2021 年 3 月微软官方发布了 Microsoft Exchange 安全更新修复 Exchange 服务器端请求伪造（SSRF）漏洞，利用此漏洞的攻击者可构造恶意请求，发送任意 HTTP 请求并通过 Exchange Server 进行身份验证。

## 2.5 CVE-2021-1675 Windows 打印服务提权漏洞

2021 年 6 月初微软官方发布 Windows 打印服务(Windows Print Spooler)的提权漏洞。未经身份验证的远程攻击者可利用该漏洞以 SYSTEM 权限在域控制器上执行任意代码，从而获得整个域的控制权。

## 2.6 CVE-2021-41379 Windows Installer 权限提升漏洞

2021 年 11 月 9 日微软发布了 CVE-2021-41379 的安全补丁。该漏洞是 Windows 操作系统存在的一个特权提升漏洞，漏洞源于 Windows Installer 服务存在一些特定的缺陷，攻击者可以利用此漏洞在 SYSTEM 上下文中创建联结，提升当前账户的低级管理权限。

## 2.7 CVE-2021-34527 Windows 打印服务漏洞

2021 年 7 月初微软官方发布了一个存在于 Windows 打印服务(Windows Print Spooler)的高危漏洞。Windows Print Spooler 是 Windows 的打印机后台处理程序，利用该漏洞，攻击者可以使用一个低权限用户（包括 guest 用户）,对域控发起攻击，进而控制整个内网。

## 2.8 CVE-2021-36934 Windows 特权提升漏洞

2021 年 7 月由微软公开的 Windows 提权漏洞，该漏洞是由于对多个系统文件（包括安全帐户管理器(SAM)数据库的访问控制列表(ACL)过于宽松，存在特权提升漏洞。成功利用此漏洞的攻击者可以使用 SYSTEM 权限运行任意代码，然后攻击者可以安装程序，查看、更改或删除数据，或创建具有完全用户权限的新帐户。

### 2.9 CVE-2021-26858 Microsoft Exchange Server 远程代码执行漏洞

该漏洞主要来自 Exchange 中身份验证后的任意文件写入漏洞，攻击者通过 Exchange 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径，该漏洞可以配合 CVE-2021-26855 SSRF 漏洞进行组合攻击。

### 2.10 CVE-2021-1732 Microsoft Windows 本地提权漏洞

2021 年 2 月，微软每月的例行补丁包中修复了一个 Windows 系统本地提权漏洞，本地攻击者可以利用此漏洞提升到 System 权限，此漏洞可能被用于定向攻击活动。该漏洞主要由函数 win32kfull!xxxCreateWindowEx 对应用层回调返回数据校验不严导致，本地用户执行漏洞利用程序获取系统权限。

## （三）2021 年全球 APT 攻击事件解读

### 1. 威胁组织 Darkside

DarkSide 组织主要是通过投递 Darkside 勒索软件对目标进行攻击的，该团伙于 2020 年 8 月出现，据统计已经袭击了近百个受害者，从被 Darkside 团伙攻击过的行业来看，该团伙的攻击目标涉及了 IT、石油和天然气等多个领域。2021 年 DarskSide 先后对成品油管道运营商 Colonial Pipeline、东芝公司（Toshiba Tec Corp）、化学品分销集团 Brenntag 等企业进行了网络攻击。

攻击事件 1：2021 年 5 月 7 日，DarkSide 组织袭击了美国最大成品油管道运营商 Colonial Pipeline 公司的工业控制系统。该事件导致 Colonial Pipeline 公司被迫中断了东部沿海主要城市输送油气的管道系统运营，随后美国政府宣布进入紧急状态。据悉，Colonial Pipeline 是美国最大的成品油管道运营商，每天通过管道系统输送超过 1 亿加仑的燃料，该管道系统连接得克萨斯州休斯顿和新泽西州林登，跨度长达 5500 多英里，美国东海岸 45%的燃料都由该管道系统提供，受此事件影响，此次燃油管道关闭有可能导致油价攀升。

Pipeline Emergency?
Call 1-800-926-2728

COLONIAL PRESS RELEASE

**Media Statement Update: Colonial Pipeline System Disruption**

**Update — Monday, May 10, 7:55 p.m.**

Colonial Pipeline is continuing to work in partnership with third-party cybersecurity experts, law enforcement, and other federal agencies to restore pipeline operations quickly and safely. While this situation remains fluid and continues to evolve, the Colonial operations team is executing a plan that involves an incremental process that will facilitate a return to service in a phased approach.

We can now report that Line 4, which runs from Greensboro, N.C., to Woodbine, Md., is operating under manual control for a limited period of time while existing inventory is available. As previously announced, while our main lines continue to be offline, some smaller lateral lines between terminals and delivery points are now operational as well. We continue to evaluate product inventory in storage tanks at our facilities and others along our system and are working with our shippers to move this product to terminals for local delivery.

Our primary focus remains the safe and efficient restoration of service to our pipeline system, while minimizing disruption to our customers and all those who rely on Colonial Pipeline. We will continue to provide updates as restoration efforts progress.

# # #

图：Colonial Pipeline 公司官方声明

攻击事件 2：2021 年 5 月 14 日，DarkSide 组织对东芝集团（Toshiba Tec Corp）欧洲子公司进行了网络攻击，为了防止损害的扩散，东芝停止了在日本和欧洲之间以及在欧洲子公司之间运营的网络和系统，同时采取了恢复措施和数据备份。

TOSHIBA Toshiba Tec Corporation

Worldwide | Japanese | Sitemap | Contact Us

Search

Home | Products | Solutions | Services | Download & Videos | Corporate Data

**Cyber attack on European subsidiaries of the Toshiba Tec Group**

May 14, 2021
Toshiba Tec Corporation

It was confirmed that European subsidiaries of the Toshiba Tec Group companies suffered from the damage of cyber attack. ("the damage").

After discovering the damage, the Toshiba Tec Group ("the group") immediately reported to the authorities concerned in Europe. The group also took actions to stop the networks and systems operating between Japan and Europe as well as those operating among European subsidiaries with the aim of preventing the spread of damage while deploying recovery measures sequentially once effective data backup has been completed. In addition, the group is proceeding to identify the content and extent of the possible damage through conducting investigations by the outside specialized organization.

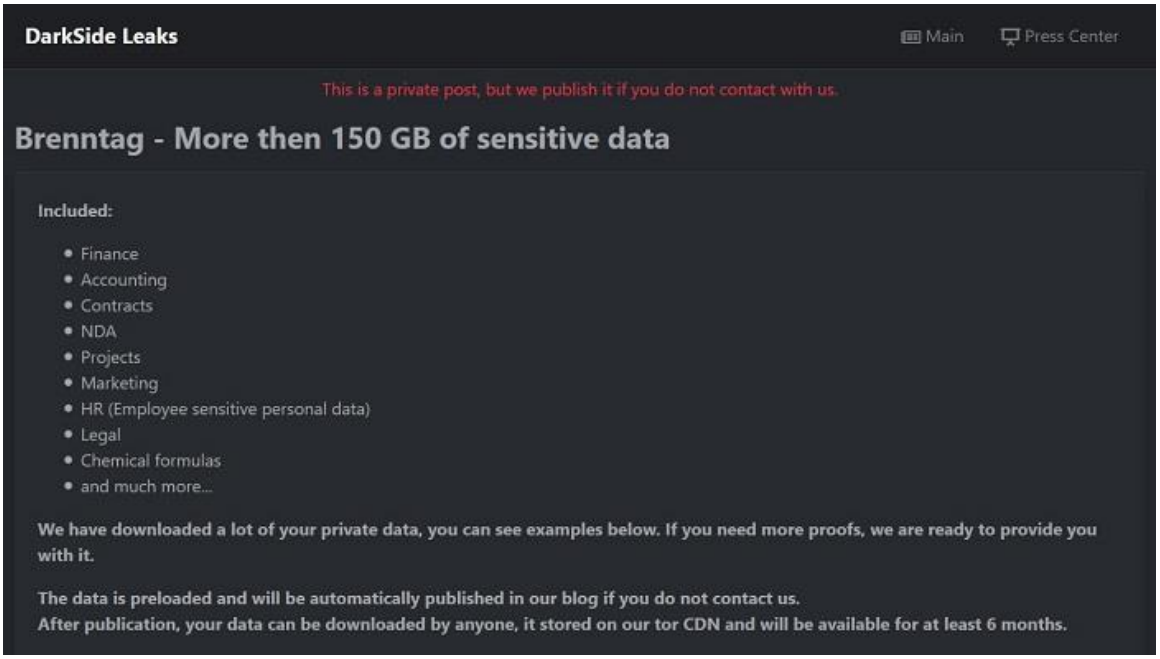
According to the investigation, the extent of impact has been limited to some regions in Europe and we have not yet confirmed a fact that customer related information was leaked externally.

As far as the investigation result shows, the group recognizes that it is possible that some information and data may have been leaked by the criminal gang, we will continue to conduct further investigation in cooperation with external specialized organization to grasp the details.

Although the group has been steadily implementing information security measures, the group will further enhance securtity measures to ensure protecting the information of our customers and employees. Going forward, the group is determined to resolve

图：东芝集团发布的声明

攻击事件 3：2021 年 5 月初，化学品分销巨头 Brenntag 遭受了网络攻击，网络犯罪分子不仅对该公司网络上的设备数据进行了加密，还窃取了大量未加密的文件。DarkSide 勒索软件组织声称在本次攻击期间窃取了 150GB 的数据。为了解救被网络攻击者加密的数据，并防止被盗数据的公开泄露，Brenntag 被迫向 DarkSide 勒索软件团伙支付了价值 440 万美元的比特币赎金。

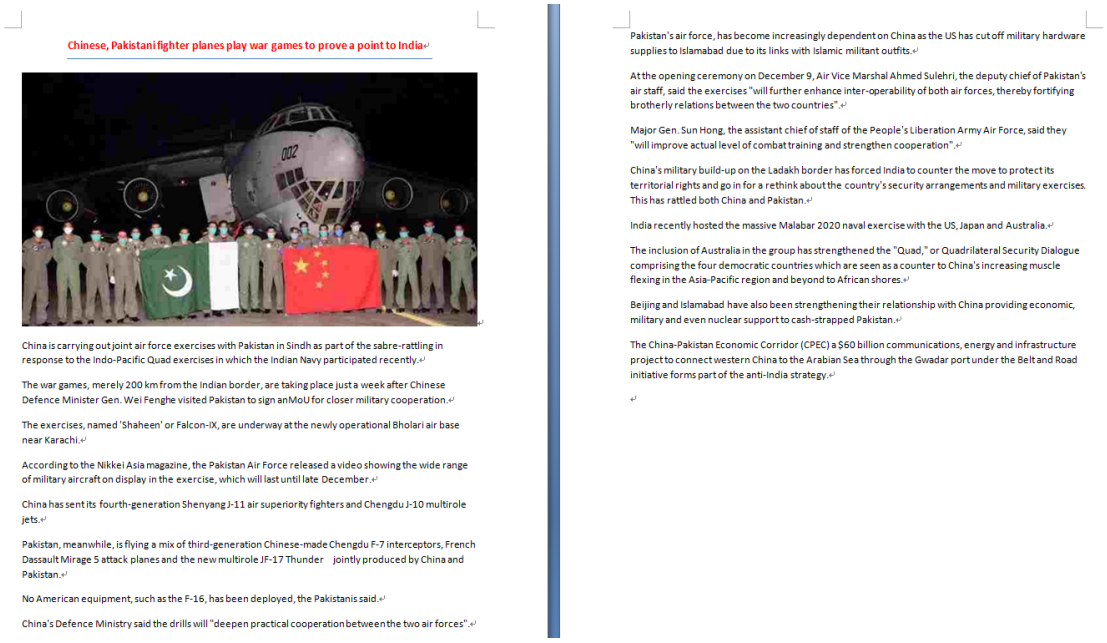



图：DarkSide 组织创建的私人数据泄露页面

## 2. 威胁组织 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 组织还有“摩诃草”、Dropping Elephant、Chinastrats、APT-C-09、Quilted Tiger 和 ATK 11 等称谓。该组织主要是从事信息窃取和间谍活动，其针对的目标包含了中国、巴基斯坦、日本、英国和美国等多个国家，涉及的目标行业多为航空、国防、能源、金融、IT 和政府等。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。2021 年瑞星捕获到了多起和其相关的安全事件。

攻击事件 1：2021 年 1 月，瑞星威胁情报平台捕获到一起涉及中国和巴基斯坦的样本，通过分析发现，该样本名为“Chinese_Pakistani_fighter_planes_play_war_games.docx.”，（译文：中国巴基斯坦战斗机参加战争游戏.docx）。该样本利用 esp 漏洞进行攻击，当用户点击执行 docx 文档后，该恶意样本便会通过文档目录“word/_rels/document.xml.rels”中的加载项加载“media/image1.eps”，利用 esp 释放同名诱饵文档以迷惑用户，诱饵文档内容则与中国和巴基斯坦的空军演习相关报道相关，同时还会释放 FakeJLI 后门病毒，以进行信息窃取等恶意操作。



Chinese, Pakistani fighter planes play war games to prove a point to India

China is carrying out joint air force exercises with Pakistan in Sindh as part of the sabre-rattling in response to the Indo-Pacific Quad exercises in which the Indian Navy participated recently.

The war games, merely 200 km from the Indian border, are taking place just a week after Chinese Defence Minister Gen. Wei Fenghe visited Pakistan to sign anMoU for closer military cooperation.

The exercises, named 'Shaheen' or Falcon-IX, are underway at the newly operational Bholari air base near Karachi.

According to the Nikkei Asia magazine, the Pakistan Air Force released a video showing the wide range of military aircraft on display in the exercise, which will last until late December.

China has sent its fourth-generation Shenyang J-11 air superiority fighters and Chengdu J-10 multirole jets.

Pakistan, meanwhile, is flying a mix of third-generation Chinese-made Chengdu F-7 interceptors, French Dassault Mirage 5 attack planes and the new multirole JF-17 Thunder jointly produced by China and Pakistan.

No American equipment, such as the F-16, has been deployed, the Pakistanis said.

China's Defence Ministry said the drills will "deepen practical cooperation between the two air forces".

Pakistan's air force, has become increasingly dependent on China as the US has cut off military hardware supplies to Islamabad due to its links with Islamic militant outfits.

At the opening ceremony on December 9, Air Vice Marshal Ahmed Sulehri, the deputy chief of Pakistan's air staff, said the exercises "will further enhance inter-operability of both air forces, thereby fortifying brotherly relations between the two countries".

Major Gen. Sun Hong, the assistant chief of staff of the People's Liberation Army Air Force, said they "will improve actual level of combat training and strengthen cooperation".

China's military build-up on the Ladakh border has forced India to counter the move to protect its territorial rights and go in for a rethink about the country's security arrangements and military exercises. This has rattled both China and Pakistan.

India recently hosted the massive Malabar 2020 naval exercise with the US, Japan and Australia.

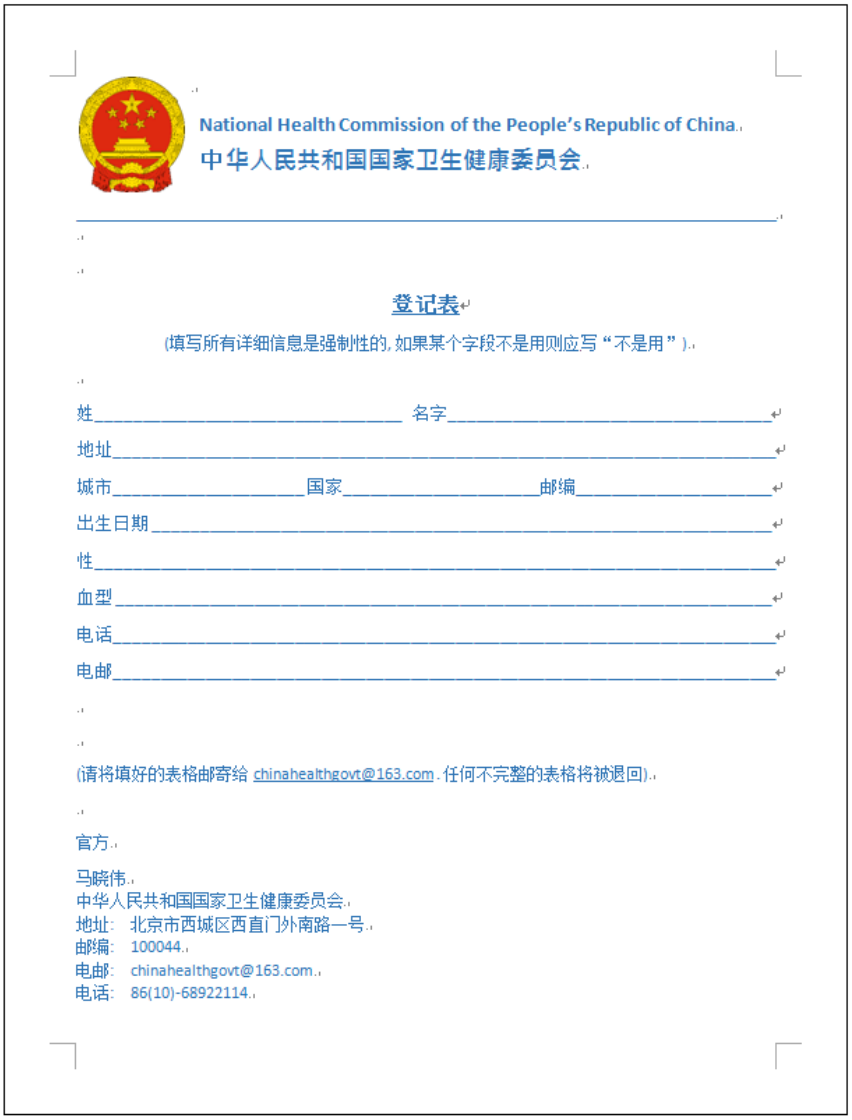
The inclusion of Australia in the group has strengthened the "Quad," or Quadrilateral Security Dialogue comprising the four democratic countries which are seen as a counter to China's increasing muscle flexing in the Asia-Pacific region and beyond to African shores.

Beijing and Islamabad have also been strengthening their relationship with China providing economic, military and even nuclear support to cash-strapped Pakistan.

The China-Pakistan Economic Corridor (CPEC) a $60 billion communications, energy and infrastructure project to connect western China to the Arabian Sea through the Gwadar port under the Belt and Road initiative forms part of the anti-India strategy.

图：攻击事件 1 中的诱饵文档

攻击事件 2：2021 年 12 月 21 日，瑞星威胁情报平台捕获了一起 Patchwork 组织对中国发起的攻击事件。该组织在此次攻击中利用了带有 CVE-2017-11882 漏洞的诱饵文档，伪装成《中华人民共和国国家卫生健康委员会登记表》进行攻击，登记表内需要填写的内容包含姓名、出生日期、地址、邮箱以及电话等隐私信息。一旦目标打开诱饵文档，攻击者就会利用文档漏洞执行一段 shellcode，从而在目标系统内隐秘释放远控木马。



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

登记表

(填写所有详细信息是强制性的,如果某个字段不是用则应写“不是用”)

姓_____ 名字_____

地址_____

城市_____国家_____邮编_____

出生日期_____

性_____

血型_____

电话_____

电邮_____

(请将填好的表格邮寄给 chinahealthgovt@163.com.任何不完整的表格将被退回)

官方

马晓伟
中华人民共和国国家卫生健康委员会
地址: 北京市西城区西直门外南路一号
邮编: 100044
电邮: chinahealthgovt@163.com
电话: 86(10)-68922114

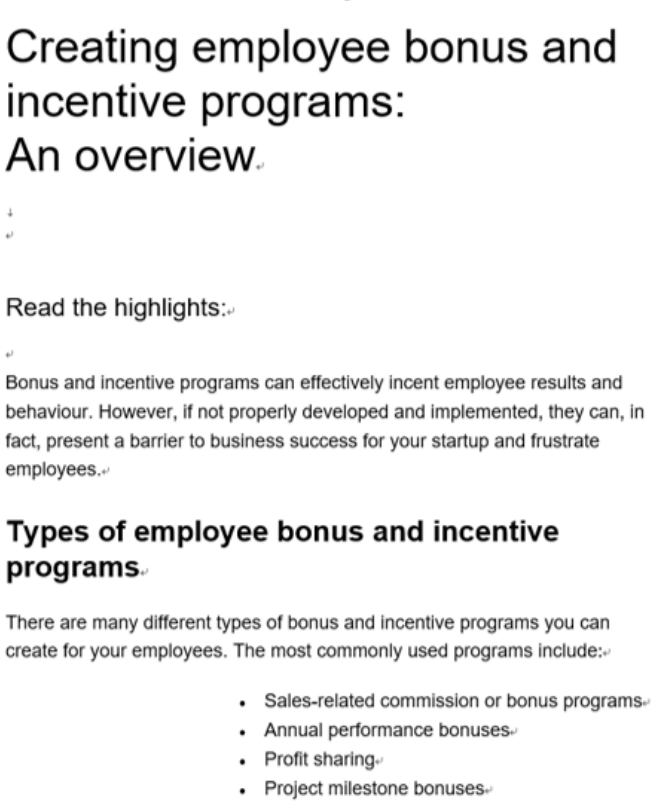
图：攻击事件 2 中的诱饵文档

## 3. 威胁组织 Lazarus Group

Lazarus Group 是一个自 2007 年就开始对目标进行网络攻击的威胁组织，该组织又被称为 Group 77、Hastati Group、Hidden Cobra、APT-C-26、T-APT-15、Zinc 和 Nickel Academy 等，是现今最活跃的威胁组织之一。该组织来自朝鲜，具有国家背景，除了擅长信息盗取、间谍活动外，还会通过蓄意破坏电脑系统以获取经济利益，攻击的国家包括中国、德国、澳大利亚、日本等，涉及的领域有航空航天、政府、医疗、金融和媒体等。2021 年瑞星捕获到的多起攻击事件都和其相关。

攻击事件 1：2021 年 5 月 11 日，瑞星威胁情报平台捕获到一起 Lazarus Group 组织的攻击事件。此攻击事件中，该组织使用的诱饵文档内容主要是关于创建员工奖金和激励计划，通过溯源得知该文章从加拿大 MaRS 网站上摘抄得来。在这起攻击事件中，攻击者利用钓鱼邮件等方式向目标投递名为“New Bonus Announcemnet.zip”压缩包，在压缩包内有两个文件：“New Bonus Announcemnet.docx”和“Password.txt.lnk”。因为文档“New Bonus Announcemnet.docx”被攻击者加密，所以需要目

标用户点击“Password.txt.lnk”获取密码进行解密操作，而“Password.txt.lnk”的快捷方式文件则指向一段恶意 JS 代码，所以目标用户在获取密码的同时也会被该 JS 代码所释放的恶意程序远程控制。


Creating employee bonus and incentive programs: An overview

Read the highlights:

Bonus and incentive programs can effectively incent employee results and behaviour. However, if not properly developed and implemented, they can, in fact, present a barrier to business success for your startup and frustrate employees.

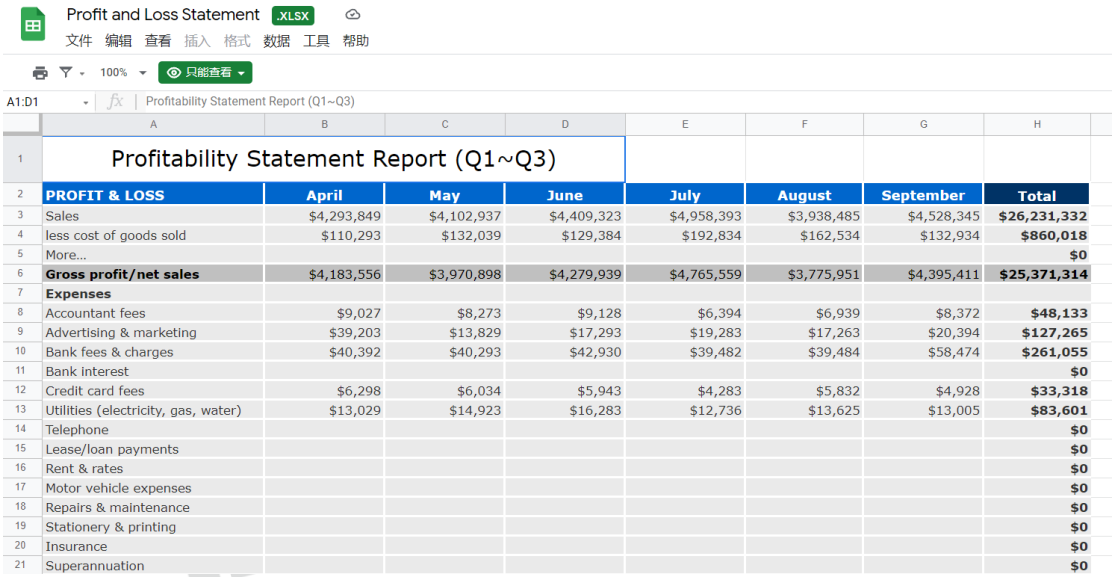
Types of employee bonus and incentive programs

There are many different types of bonus and incentive programs you can create for your employees. The most commonly used programs include:

- Sales-related commission or bonus programs
- Annual performance bonuses
- Profit sharing
- Project milestone bonuses

图：攻击事件 1 中的诱饵文档

攻击事件 2：2021 年 10 月 22 日，瑞星捕获到 Lazarus Group 组织另一起安全事件。此次攻击事件中，攻击者利用钓鱼邮件等方式向目标投递名为“Profitability Statement Report.zip”压缩包，当目标用户解压压缩包后会得到名为“Profit and Loss Statement.xlsx.lnk”的快捷方式文件，该快捷方式指向一段 JS 代码，攻击者利用这段 JS 代码打开诱饵文档迷惑用户，诱饵文档内容是一张盈利报表，里面记录了 4 到 9 月份期间销售盈利和各方面的花销等内容，同时还会释放恶意程序以达到对目标用户计算机进行远程控制的目的。



Profit and Loss Statement .XLSX

文件 编辑 查看 插入 格式 数据 工具 帮助

100% 只能查看

A1:D1 | Profitability Statement Report (Q1~Q3)

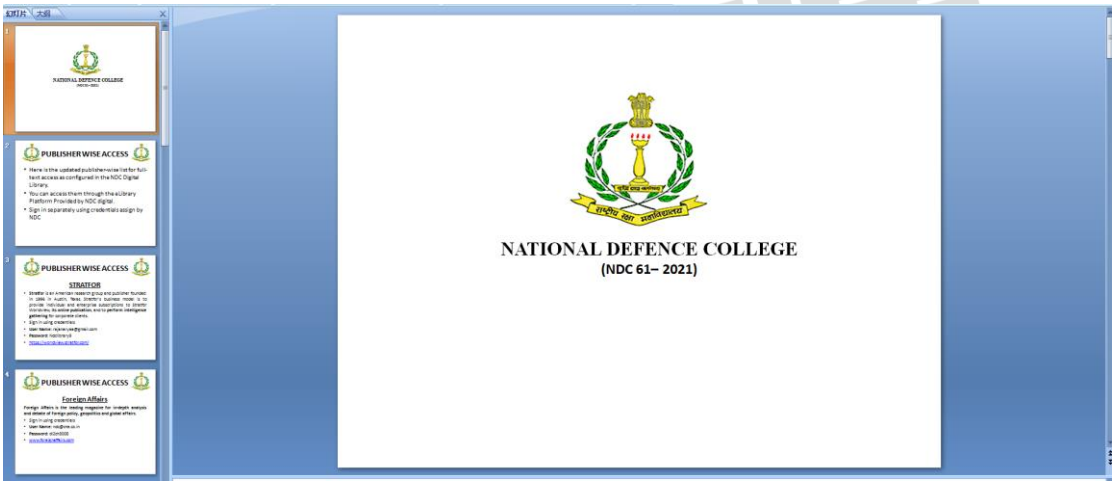
| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | Profitability Statement Report (Q1~Q3) | | | | | | | |
| 2 | **PROFIT & LOSS** | **April** | **May** | **June** | **July** | **August** | **September** | **Total** |
| 3 | Sales | $4,293,849 | $4,102,937 | $4,409,323 | $4,958,393 | $3,938,485 | $4,528,345 | **$26,231,332** |
| 4 | less cost of goods sold | $110,293 | $132,039 | $129,384 | $192,834 | $162,534 | $132,934 | **$860,018** |
| 5 | More... | | | | | | | **$0** |
| 6 | **Gross profit/net sales** | $4,183,556 | $3,970,898 | $4,279,939 | $4,765,559 | $3,775,951 | $4,395,411 | **$25,371,314** |
| 7 | **Expenses** | | | | | | | |
| 8 | Accountant fees | $9,027 | $8,273 | $9,128 | $6,394 | $6,939 | $8,372 | **$48,133** |
| 9 | Advertising & marketing | $39,203 | $13,829 | $17,293 | $19,283 | $17,263 | $20,394 | **$127,265** |
| 10 | Bank fees & charges | $40,392 | $40,293 | $42,930 | $39,482 | $39,484 | $58,474 | **$261,055** |
| 11 | Bank interest | | | | | | | **$0** |
| 12 | Credit card fees | $6,298 | $6,034 | $5,943 | $4,283 | $5,832 | $4,928 | **$33,318** |
| 13 | Utilities (electricity, gas, water) | $13,029 | $14,923 | $16,283 | $12,736 | $13,625 | $13,005 | **$83,601** |
| 14 | Telephone | | | | | | | **$0** |
| 15 | Lease/loan payments | | | | | | | **$0** |
| 16 | Rent & rates | | | | | | | **$0** |
| 17 | Motor vehicle expenses | | | | | | | **$0** |
| 18 | Repairs & maintenance | | | | | | | **$0** |
| 19 | Stationery & printing | | | | | | | **$0** |
| 20 | Insurance | | | | | | | **$0** |
| 21 | Superannuation | | | | | | | **$0** |

图：攻击事件 2 中的诱饵文档

# 4. 威胁组织 Transparent Tribe

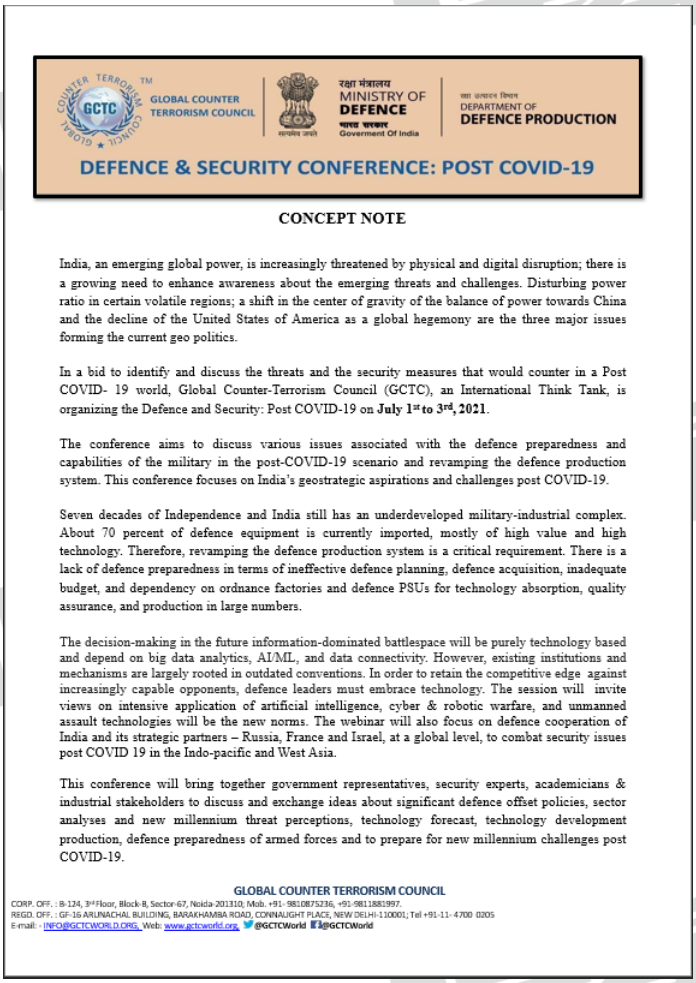
Transparent Tribe 是一个自 2013 年以来一直在活跃着的威胁组织。这个组织又被称为“透明部落”、APT 36、ProjectM、Mythic Leopard 和 EMP.Lapis，有信息表明该组织疑似为巴基斯坦背景，由国家支持，其主要目的是信息盗窃和间谍活动，攻击目标包括阿富汗、印度、哈萨克斯坦和沙特阿拉伯等国家，涉及行业多为教育、国防和政府等领域。2021 年瑞星捕获了多起和与 Transparent Tribe 组织相关的的攻击事件。

攻击事件 1：2021 年 4 月，瑞星威胁情报平台捕获到一起针对印度国防大学（NATIONAL DEFENCE COLLEGE（NDC））的攻击事件，攻击者投放的样本是个带宏文档的 PPT，名为“NDCUpdates.ppt”。当目标用户点击样本执行宏后，样本会在计算机上释放内容为印度国防大学（NATIONAL DEFENCE COLLEGE（NDC））的诱饵文档及 Crimson 远控木马，攻击者通过诱饵文档迷惑用户，并在后台执行 Crimson 远控木马进行信息窃取等恶意操作。




图：攻击事件 1 中的诱饵文档

攻击事件 2：2021 年 6 月 18 日，瑞星捕获 Transparent Tribe 威胁组织的另一起攻击事件。在这起攻击事件中，攻击者使用的诱饵文档为英文，内容为一个会议介绍及日程安排，会议讨论的内容是 COVID-19 疫情过去之后，印度如何改造自己的军事防御体系，并且会议将聚焦于印度的地缘战略抱负和挑战。根据其主要内容可以得知此次攻击目标为印度。在这起攻击事件中，攻击者疑似利用钓鱼邮件等方式投递名为“Defence and security Agenda Point.ppt”的宏文档，当用户打开这个 PPT 文档并启用宏后，宏代码会释放并打开诱饵文档以迷惑用户，同时还会释放并执行一个木马释放器，攻击者利用这个木马释放器释放并执行 Crimson 远控木马进行信息窃取及远控操作。



GLOBAL COUNTER TERRORISM COUNCIL

रक्षा मंत्रालय MINISTRY OF DEFENCE भारत सरकार Government Of India

DEPARTMENT OF DEFENCE PRODUCTION

**DEFENCE & SECURITY CONFERENCE: POST COVID-19**

**CONCEPT NOTE**

India, an emerging global power, is increasingly threatened by physical and digital disruption; there is a growing need to enhance awareness about the emerging threats and challenges. Disturbing power ratio in certain volatile regions; a shift in the center of gravity of the balance of power towards China and the decline of the United States of America as a global hegemony are the three major issues forming the current geo politics.

In a bid to identify and discuss the threats and the security measures that would counter in a Post COVID- 19 world, Global Counter-Terrorism Council (GCTC), an International Think Tank, is organizing the Defence and Security: Post COVID-19 on **July 1st to 3rd, 2021**.

The conference aims to discuss various issues associated with the defence preparedness and capabilities of the military in the post-COVID-19 scenario and revamping the defence production system. This conference focuses on India's geostrategic aspirations and challenges post COVID-19.

Seven decades of Independence and India still has an underdeveloped military-industrial complex. About 70 percent of defence equipment is currently imported, mostly of high value and high technology. Therefore, revamping the defence production system is a critical requirement. There is a lack of defence preparedness in terms of ineffective defence planning, defence acquisition, inadequate budget, and dependency on ordnance factories and defence PSUs for technology absorption, quality assurance, and production in large numbers.

The decision-making in the future information-dominated battlespace will be purely technology based and depend on big data analytics, AI/ML, and data connectivity. However, existing institutions and mechanisms are largely rooted in outdated conventions. In order to retain the competitive edge against increasingly capable opponents, defence leaders must embrace technology. The session will invite views on intensive application of artificial intelligence, cyber & robotic warfare, and unmanned assault technologies will be the new norms. The webinar will also focus on defence cooperation of India and its strategic partners – Russia, France and Israel, at a global level, to combat security issues post COVID 19 in the Indo-pacific and West Asia.

This conference will bring together government representatives, security experts, academicians & industrial stakeholders to discuss and exchange ideas about significant defence offset policies, sector analyses and new millennium threat perceptions, technology forecast, technology development production, defence preparedness of armed forces and to prepare for new millennium challenges post COVID-19.

GLOBAL COUNTER TERRORISM COUNCIL

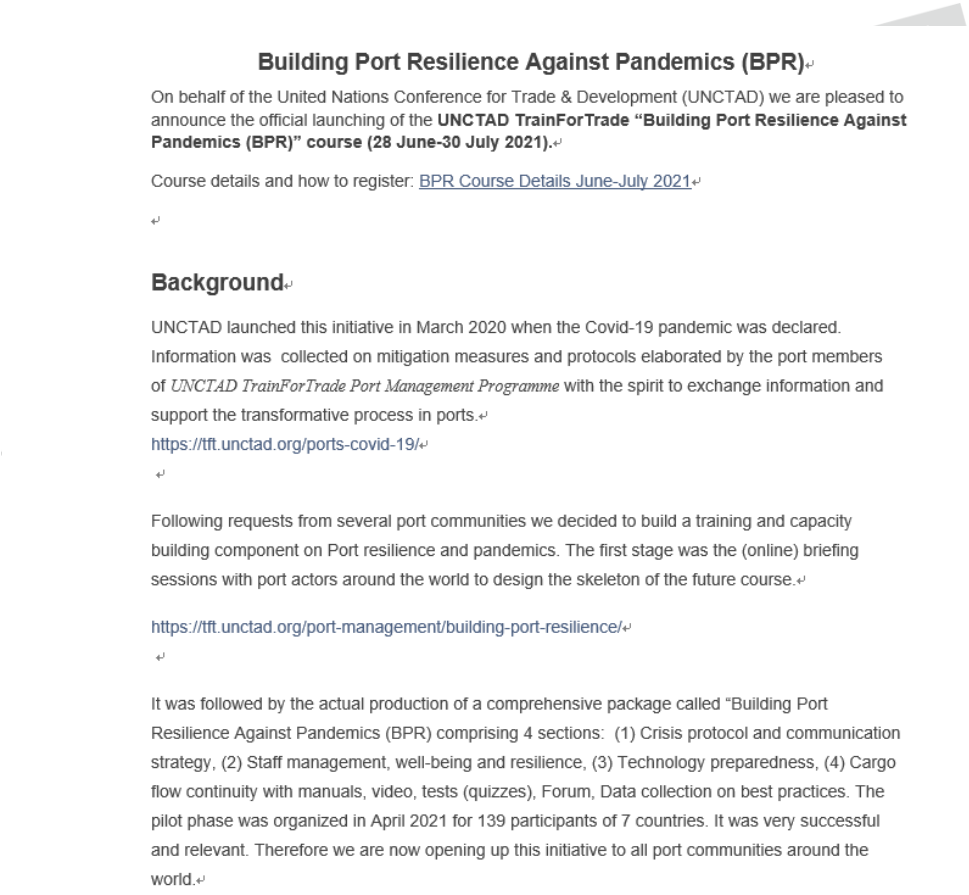
CORP. OFF. : B-124, 3rd Floor, Block-B, Sector-67, Noida-201310; Mob. +91- 9810875236, +91-9811881997.
REGD. OFF. : GF-16 ARUNACHAL BUILDING, BARAKHAMBA ROAD, CONNAUGHT PLACE, NEW DELHI-110001; Tel +91-11- 4700 0205
E-mail: - INFO@GCTCWORLD.ORG, Web: www.gctcworld.org, @GCTCWorld @GCTCWorld

图：攻击事件 2 中的诱饵文档

## 5. 威胁组织 SideWinder

SideWinder 是一个至少从 2012 年就开始进行网络攻击的威胁组织，疑似来自印度。这个 APT 组织又被称为“响尾蛇”、T-APT-04、Rattlesnake 和 APT-C-17，是现今最活跃的组织之一。该组织主要是从事信息窃取和间谍活动，大多数活动都集中在中国、巴基斯坦、阿富汗等国家，涉及的目标行业多为医疗、国防、政府和科技公司等，其攻击手法主要是利用钓鱼邮件等方式投递嵌入了恶意对象和 CVE-2017-11882 漏洞的文档，又或者向目标投递指向恶意链接的快捷方式等。2021 年瑞星捕获到了与其相关的攻击事件。

攻击事件：2021 年 5 月 24 日，瑞星捕获了和威胁组织 SideWinder 相关的攻击事件，此次攻击事件中该组织所使用的诱饵文档与联合国贸易和发展会议（UNCTAD）相关，文档内容关于 2021 年 6 月至 7 月的 “建立港口抗击流行病的能力（BPR）” 课程。攻击者利用钓鱼邮件等方式向目标投递嵌入了恶意对象和 CVE-2017-11882 漏洞的文档进行攻击，文档中被嵌入的恶意对象是个 JS 脚本文件，当目标用户运行文档后，JS 脚本文件便会被攻击者利用 CVE-2017-11882 漏洞执行起来，最终达到信息窃取等恶意操作的目的。



**Building Port Resilience Against Pandemics (BPR)**

On behalf of the United Nations Conference for Trade & Development (UNCTAD) we are pleased to announce the official launching of the **UNCTAD TrainForTrade "Building Port Resilience Against Pandemics (BPR)" course (28 June-30 July 2021).**

Course details and how to register: BPR Course Details June-July 2021

**Background**

UNCTAD launched this initiative in March 2020 when the Covid-19 pandemic was declared. Information was collected on mitigation measures and protocols elaborated by the port members of *UNCTAD TrainForTrade Port Management Programme* with the spirit to exchange information and support the transformative process in ports.
https://tft.unctad.org/ports-covid-19/

Following requests from several port communities we decided to build a training and capacity building component on Port resilience and pandemics. The first stage was the (online) briefing sessions with port actors around the world to design the skeleton of the future course.

https://tft.unctad.org/port-management/building-port-resilience/

It was followed by the actual production of a comprehensive package called "Building Port Resilience Against Pandemics (BPR) comprising 4 sections: (1) Crisis protocol and communication strategy, (2) Staff management, well-being and resilience, (3) Technology preparedness, (4) Cargo flow continuity with manuals, video, tests (quizzes), Forum, Data collection on best practices. The pilot phase was organized in April 2021 for 139 participants of 7 countries. It was very successful and relevant. Therefore we are now opening up this initiative to all port communities around the world.

图：攻击事件中的诱饵文档

# 6. 威胁组织 APT-C-23

APT-C-23 是一个至少从 2016 年开始对目标进行网络攻击的威胁组织。该组织又被称为 FrozenCell、AridViper、Micropsia、Desert Falcon 和 “双尾蝎”。APT-C-23 威胁组织主要目的是信息盗窃和间谍活动，具备针对 Windows 与 Android 双平台的攻击能力。该组织长期针对中东地区，特别是巴勒斯坦进行攻击，涉及行业多为政府、教育、军事等重要领域。2021 年瑞星捕获了多起与其相关的攻击事件。

攻击事件 1：2021 年 8 月 8 日，在瑞星捕获的这起攻击事件中，攻击者向目标投递伪装成 PDF 文档的可执行恶意程序，程序名为 “0001_دراغمة باسل المريض pdf.exe”，语言为阿拉伯语。该程序由 Delphi7 编写，带有隐藏窗口，窗口内含 6 个定时器和 8 个按钮，样本利用这些控件的消息响应函数来达到窃密和远控的目的。此次事件所投递的诱饵文档共有 5 页，文中内容由图片组成，文中页面顶部带有巴勒斯坦国徽，且文内大部分内容使用阿拉伯语编写，文档内还提到了巴勒斯坦卫生

部，因此猜测此次攻击事件的目标是巴勒斯坦，领域涉及巴勒斯坦卫生部。

State of Palestine
Governorate of Toubas & Northern valleys
Office of The Governor

دولة فلسطين
محافظة طوباس والأغوار الشمالية
مكتب المحافظ

دولة فلسطين
محافظة طوباس والأغوار الشمالية
07-07-2021
مكتب المحافظ
صادر

عطوفة الأخ موفق دراغمة حفظه الله
منسق شؤون المحافظات

تحية طيبة وبعد ،،

الموضوع : المريض باسل اسعد حسن دراغمة / طوباس
هوية رقم : 982672933

تهديكم محافظة طوباس والأغوار الشمالية أطيب تحياتها ،،
بالاشارة الى الموضوع اعلاه ، نامل من عطوفتكم مساعدة المواطن المذكور أعلاه حيث تقدم ذويه بطلب مساعدة من اجل تغطية التامين الصحي لدخوله مستشفى الرازي في جنين حيث تعرض لجلطة حادة استدعت تحويله بشكل عاجل من المستشفى التركي الى مستشفى الرازي وتم تجديد تأمينه باليوم التالي لدخوله بعد اجراء عملية شبكية مستعجلة .

وتفضلوا بقبول فائق الاحترام والتقدير،،،

طوباس في 2021/07/07

اللواء ركن يونس العاصي
محافظ محافظة طوباس والأغوار الشمالية

- مرفق الملفات اللازمة

فاكس 092571078
هاتف 092571075/6/7
Email: info@tubas.plo.ps
http://www.tubas.plo.ps

图：攻击事件 1 中的诱饵文档

攻击事件 2：2021 年 12 月 27 日，瑞星威胁情报平台捕获到一起针对中东地区阿拉伯语国家的攻击事件。通过分析发现，此次攻击事件的主谋是 APT-C-23 组织。该组织是利用了社交媒体或自建的钓鱼网站对目标进行攻击的。此次样本所释放的诱饵文档名为“Profit from the Internet.docx”，文档内文显示为阿拉伯文，因此可判定攻击目标为阿拉伯语国家。该文档内容主要是关于“如何通过互联网盈利”，以此来诱骗目标用户点击运行，一旦诱饵文档被打开，恶意程序便会在后台开展信息收集、远程服务器通信等恶意行为，从而达到窃取机密信息的目的。

ماذا يعني الربح من الإنترنت؟

الربح من الانترنت واحد من المصطلحات الحديثة التي أوجدها التقدم التكنولوجي الكبير الذي وصلنا إليه في عالمنا الحالي. وكان لظهور الإنترنت أول مرة والمزايا والخصائص التي يتمتع بها ويوفرها الدور الأكبر في انتشار هذا المصطلح بعدما أوجد المستخدمون طرقًا مُبتكرة لتوظيفه في تحقيق أموال وليس بهدف التصفح والاطلاع على ما يدور حول العالم فقط.

وواصل المصطلح انتشاره حول العالم مع دخول التكنولوجيا كل منزل وزيادة عدد مستخدمي شبكة الإنترنت؛ فكل ما يتطلبه الأمر من أي فرد _بغض النظر عن عمره أو مكانه_ أن يكون متوافر لديه جهاز متصل بشبكة الإنترنت ومن ثم يمكنه بعدة طرق تحقيق الربح من الانترنت بدون راس مال ولو بالقليل.

وما سهل أيضًا من انتشار هذا المفهوم وكما أكدنا بعيدًا عن رأس المال، فهو لا يحتاج كذلك إلى خبرات تقنية أو فنية؛ إذ يمكن لأي شخص مبتدئ لديه القدرة على التعامل مع الأجهزة اللوحية أو أجهزة سطح المكتب أو حتى الهواتف الذكية المتصلة بالإنترنت تحقيق الربح من الانترنت.

أثرت فضولك لتتعرف على طرق الربح السهلة والمضمونة هذه؟! إذا هيا بنا نتعرف سويًا إلى أفضل وأسهل هذه الطرق في الفقرة التالية.

أفضل طرق الربح من الانترنت بدون راس مال

دائمًا ما يكون رأس المال هو العقبة الأساسية في طريق بدء العمل الخاص وتحقيق الاستقلال المهني، لذا كان البحث عن طرق ذكية لتحقيق الربح دون أن يحتاج رائد الأعمال إلى رأس مال. من هنا جاء العمل على شبكة الإنترنت الذي أوجد حلًا سحريًا لبدء المشاريع الخاصة بدون راس مال على الإطلاق.

وإليك مجموعة من أفضل وأكثر طرق الربح من الانترنت بدون راس مال شيوعًا حول العالم:

从互联网中获利是什么意思?

互联网利润是我们在当今世界取得的巨大技术进步所创造的现代术语之一。互联网的第一次出现，以及它所享有和提供的优势和特点，在用户找到了创新的使用它赚钱的方式之后，对这个词的传播起到了最大的作用，而不仅仅是为了赚钱。浏览并查看世界各地正在发生的事情。

随着技术进入每个家庭以及互联网用户数量的增加，该术语继续在世界范围内传播；任何个人——无论他的年龄或位置——所需要的只是将设备连接到 Internet，然后他就可以通过多种方式从 Internet 中获利，甚至不需要一点资本。

促进这一概念传播的，正如我们所强调的，远非资本。它也不需要技术或技术专长；任何有能力处理连接到互联网的平板电脑、台式机甚至智能手机的新手都可以通过互联网赚钱。

激起你的好奇心来了解这些简单且有保障的盈利方式？！因此，让我们在下一段中一起了解这些方法中最好和最简单的方法。

无需资金即可从互联网中获利的最佳方式

资本一直是阻碍自己创业和实现职业独立的主要障碍，因此寻找不需要资本的创业者赚钱的聪明方法。从这里开始，互联网上的工作找到了一个神奇的解决方案，可以在没有任何资本的情况下启动私人项目。

图：攻击事件 2 中的诱饵文档及译文

# （四）2021 年勒索软件分析

## 1. 勒索软件概述

勒索软件在 2021 年依然主要针对政府及企业用户，而且在未来也将成为常态，随着大大小小攻击事件的逐年增长，相关利益产业链也会不断扩大。

2021 年，越来越多的威胁组织在勒索的同时，采取文件窃取的方式来“绑架”企业的隐私文件，以历史攻击事件梳理来看这确实卓有成效，大大提高了勒索软件敲诈赎金的成功几率。即使今年比特币面临各方打压依旧水涨船高，对比过去五年涨幅高达 10.353%，这也为勒索软件等黑色相关产业带来了信心。产业链的扩大使勒索软件更注重上下游供应链和分发攻击的模式，定制化的勒索服务也是那些勒索软件作者或团队的优化目标。

同时，越来越多的攻击组织或不法分子选择运用勒索软件即服务（RaaS）这一模式进行攻击，让不具备专业技术知识的犯罪分子可以轻而易举地发起网络敲诈活动，这就导致勒索软件市场规模不断扩大。勒索软件制作者或团队通过暗网出售可定制的勒索工具，购买者只需要根据生成工具提供的配置文件或者配置选项，即可在不编码的情况下生成定制化的勒索软件。

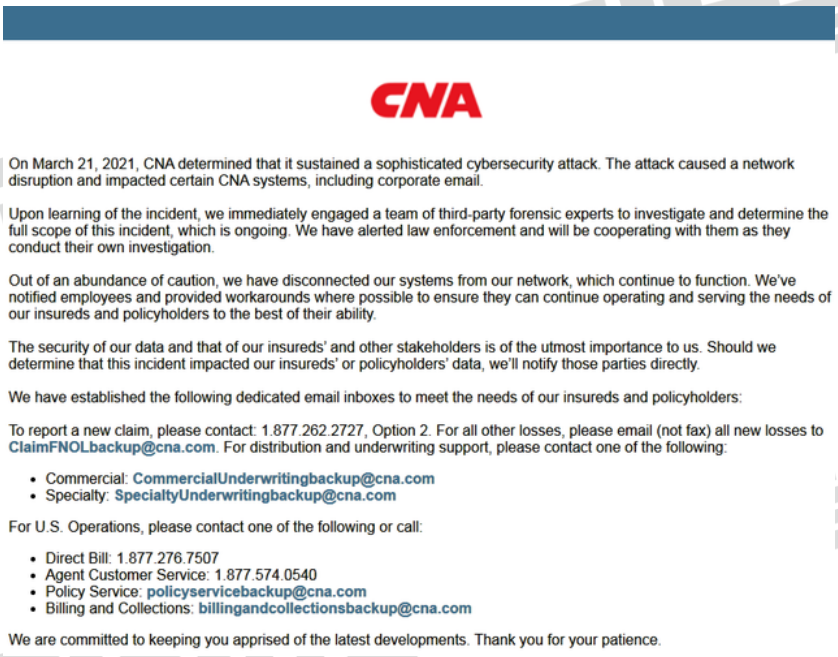
随着未来企业安全意识及安全厂商技术的不断提高，勒索软件制作者也会为其用户提供针对性更强、更多样化的黑客服务，从而攻击获利的机会也会变得更大，攻击行为也将会变得更加隐蔽，将有更多基建或能源企业面临勒索软件的威胁。

## 2. 勒索软件攻击事件

① 2021 年 2 月，一家位于波兰的流行视频游戏开发公司 CDProjekt Red 遭到 HelloKitty 团伙的

黑客攻击。黑客组织访问了开发中的游戏项目和加密设备的源代码，并以此胁迫获得赎金，然而 CDProjekt 拒绝支付赎金，使用备份恢复了丢失的数据。

② 2021 年 3 月初，大型保险公司 CNA 成为勒索软件攻击的受害者，该公司的系统感染的是 Phoenix Locker 勒索软件，该软件为 Hades 勒索软件的变种，是被称为 Evil Corp 的网络犯罪集团的武器库中的工具，其加密了该公司 15000 台设备。CNA 在 3 月底向黑客支付了 4000 万美元（2.5 亿人民币），以恢复对其系统的访问。



CNA

On March 21, 2021, CNA determined that it sustained a sophisticated cybersecurity attack. The attack caused a network disruption and impacted certain CNA systems, including corporate email.

Upon learning of the incident, we immediately engaged a team of third-party forensic experts to investigate and determine the full scope of this incident, which is ongoing. We have alerted law enforcement and will be cooperating with them as they conduct their own investigation.

Out of an abundance of caution, we have disconnected our systems from our network, which continue to function. We've notified employees and provided workarounds where possible to ensure they can continue operating and serving the needs of our insureds and policyholders to the best of their ability.

The security of our data and that of our insureds' and other stakeholders is of the utmost importance to us. Should we determine that this incident impacted our insureds' or policyholders' data, we'll notify those parties directly.

We have established the following dedicated email inboxes to meet the needs of our insureds and policyholders:

To report a new claim, please contact: 1.877.262.2727, Option 2. For all other losses, please email (not fax) all new losses to ClaimFNOLbackup@cna.com. For distribution and underwriting support, please contact one of the following:

- Commercial: CommercialUnderwritingbackup@cna.com
- Specialty: SpecialtyUnderwritingbackup@cna.com

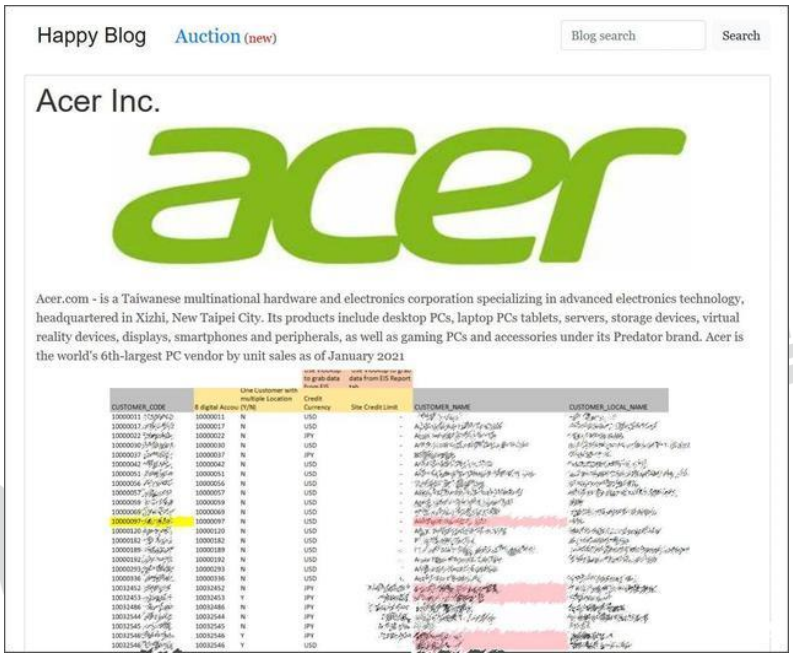
For U.S. Operations, please contact one of the following or call:

- Direct Bill: 1.877.276.7507
- Agent Customer Service: 1.877.574.0540
- Policy Service: policyservicebackup@cna.com
- Billing and Collections: billingandcollectionsbackup@cna.com

We are committed to keeping you apprised of the latest developments. Thank you for your patience.

图：CAN 公司发布公告

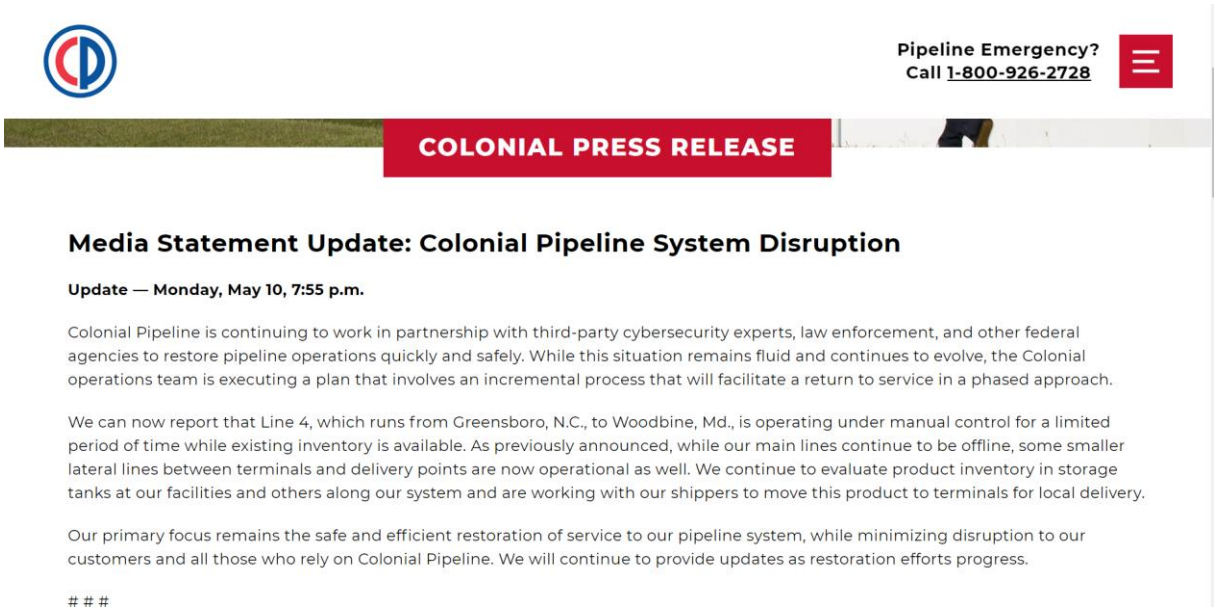
③ 2021 年 3 月，勒索软件黑客组织 REvil 宣称，他们攻击电脑大厂宏碁（Acer），并公布疑似内有窃得数据的屏幕截图，黑客向宏碁勒索 5 千万美元赎金，约相当於新台币 14 亿元。这些图片所透露的外泄内容，包含了财务报表、帐户余额，以及与银行之间往来的相关文件。




图：REvil 组织在网络上泄漏了 Acer 的信息数据

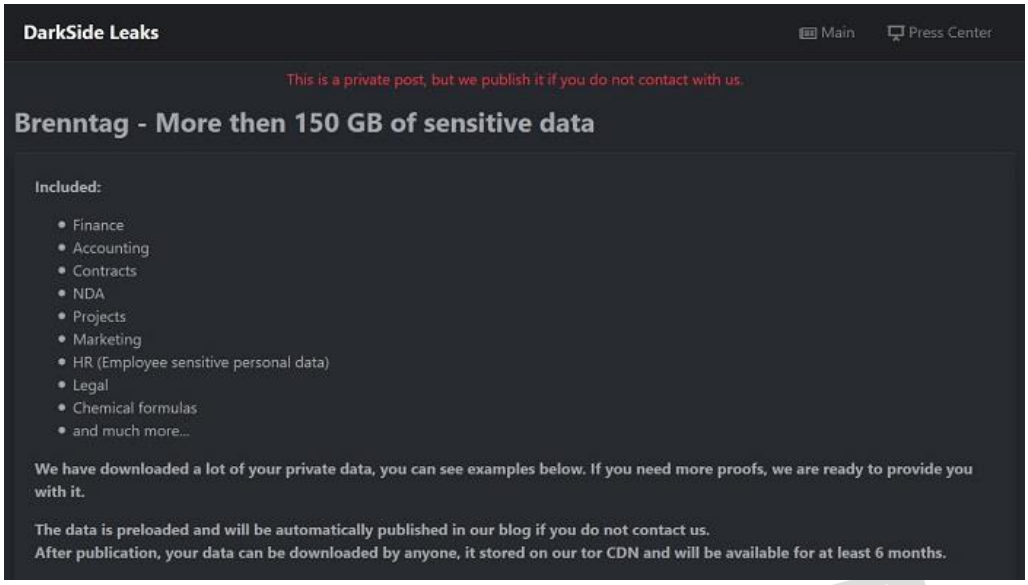
④ REvil 在 2021 年 4 月也向计算机制造商广达索要 5000 万美元的赎金，该公司是苹果的主要业务合作伙伴之一。在该公司拒绝与黑客组织谈判后，REvil 转而针对苹果公司。从泄露资料的广达手中获得了苹果产品蓝图后，他们威胁要发布更敏感的文件和数据，此次勒索攻击持续到 5 月份。

⑤ 2021 年 5 月初,DarkSide 团队把攻击瞄准向了 Colonial Pipeline,这是一家美国本土的燃油、燃气管道运营商。攻击针对了该公司的计费系统和内部业务网络，导致多个州的汽油短缺。为了避免进一步的损失,Colonial Pipeline 最终同意并向攻击组织支付了 440 万美元的比特币。




图：Colonial Pipeline 公司官方声明

⑥ 2021 年 5 月上旬，几乎是与之相同的时间点，全球领先、总部设在法国、在全球 670 个地区拥有 1.7 万余名员工的化学品分销公司 Brenntag 遭受了 DarkSide 的网络攻击，DarkSide 组织声称在本次攻击期间窃取了 150GB 的数据。为了解救被网络攻击者加密的数据、并防止被盗数据的公开泄露，Brenntag 被迫向 DarkSide 组织支付了价值 440 万美元的比特币赎金。




图：DarkSide 组织创建的私人数据泄露页面

⑦ 2021 年 7 月，活跃频频的 Revil 再次出现，对全球有名的远程管理解决方案提供商 Kaseya 发起攻击，Kaseya 首席执行官通告勒索软件团伙可能获得了对 Kaseya 后端基础设施的访问权限，并滥用它向在客户端运行的 VSA 服务器部署恶意更新。REvil 要求受害者支付 7000 万美元来解密在 Kaseya 攻击中被加密的系统。


图：Revil 在暗网博客中发布了攻击 Kaseya 的消息

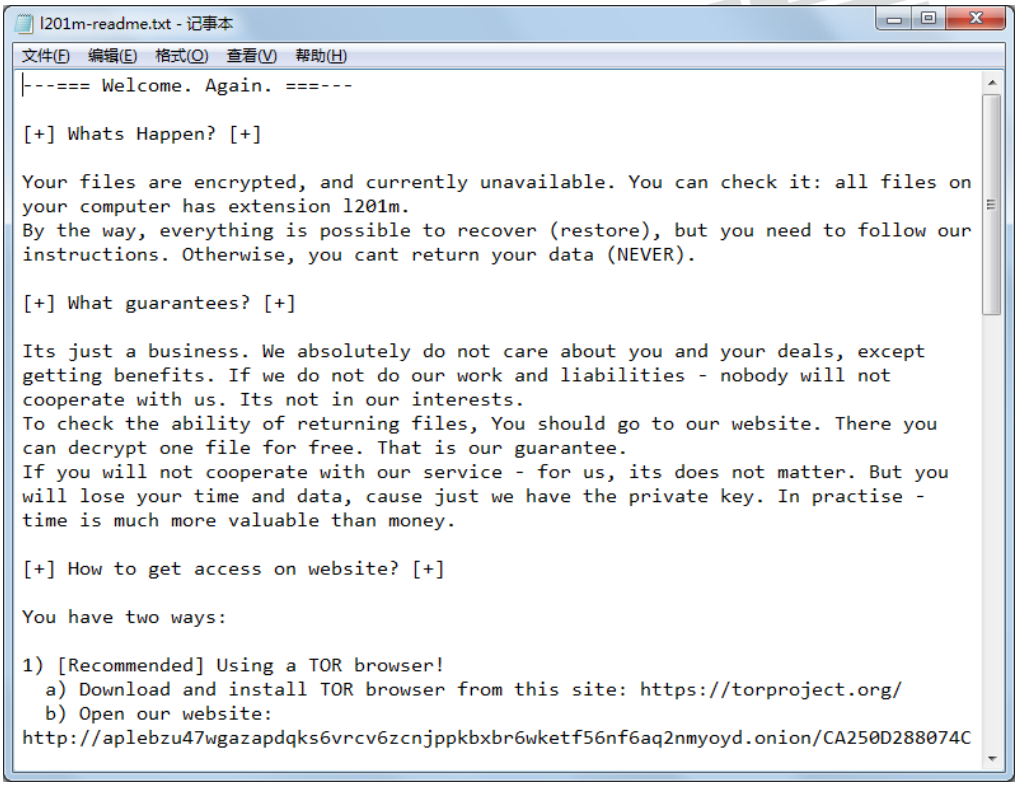
# 3. 2021 年 1 至 12 月勒索软件 Top3

在 2021 年期间出现了很多异常活跃的勒索软件，瑞星根据感染量、威胁性筛选出影响较大的年度 Top3 勒索软件进行概要性总结。

## 3.1 Sodinkibi 勒索软件

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，作为 CandCrab 退出视野以来的继任者，近两年频频活跃，2021 年更是制造了多起大型企业的攻击事件。Sodinokibi 以“勒索软件即服务”的方式分发，通过这一模式将勒索软件出售给其他犯罪团伙。

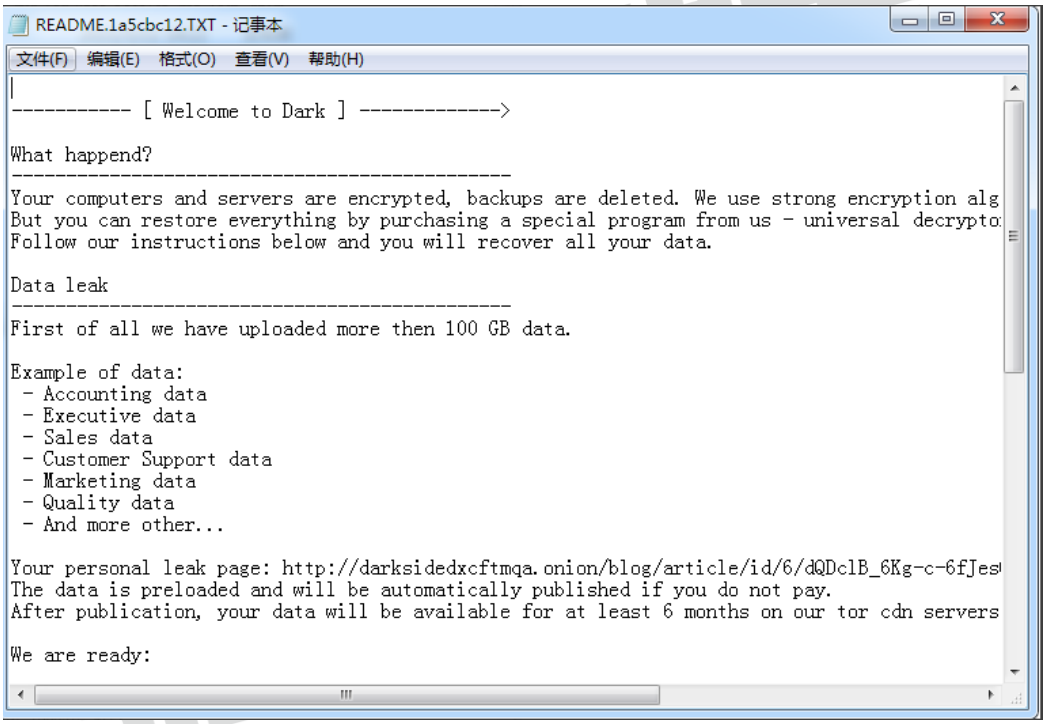
Sodinokibi 的攻击目标涉及领域较广，医疗机构、政府单位、大中型企业均有感染发生。Sodinokibi 采用椭圆曲线(ECC)非对称加密算法，运行后会使用一个配置文件来处理加密初期的参数配置工作，这可以使得 Sdoinkibi 的攻击十分灵活。它包含了加密公钥、排除扩展名、排除文件夹、排除目录，以及结束妨碍加密的进程，通过域名还能够窃取用户设备信息，其加密逻辑严谨，因此在没有攻击者私钥的情况下暂不能解密。




图：Sodinokibi 勒索信

## 3.2 Darkside 勒索软件

Darkside 勒索软件于 2020 年 8 月出现，源于俄罗斯的犯罪团伙“Darkside”，该勒索团伙已经袭击了近百个受害者，该团伙在 2021 年相当活跃，5 月期间同时攻击了多个大型企业，包括美国最大成品油管道运营商 Colonial Pipeline 公司的工业控制系统，以及化学分销公司 Brenntag，并窃取了大量数据，给以上企业造成了难以估量的损失。



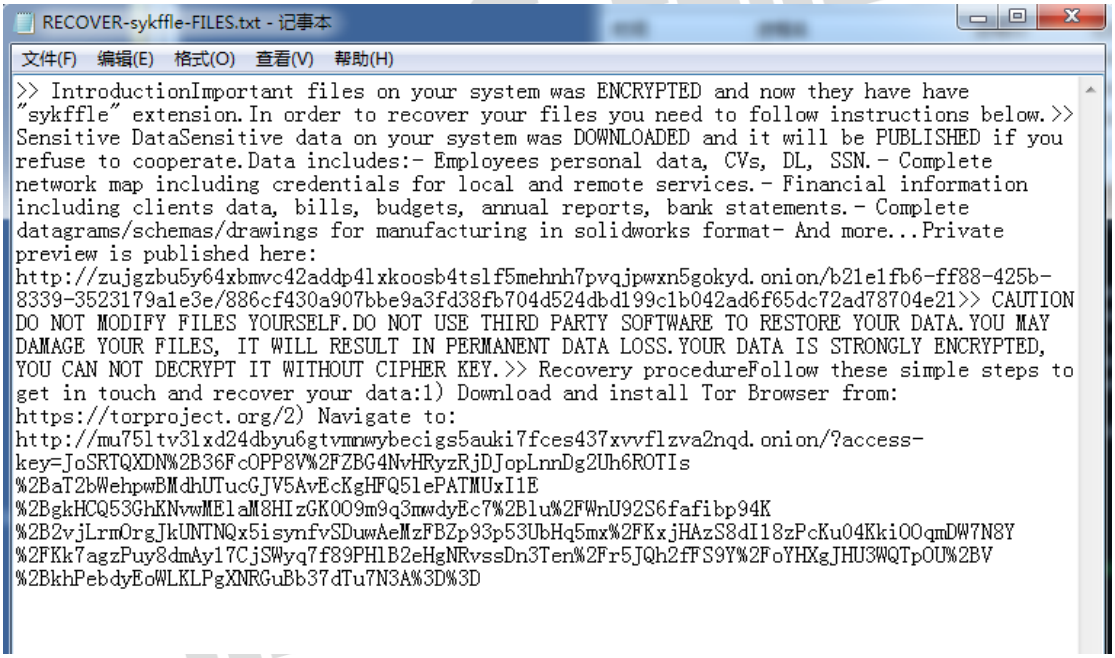

图：Darkside 勒索信

Darkside 在文件加密时，会排除系统文件、应用程序、快捷方式，以及一些公共信息的缓存文件格式，而加密其余所有其他格式，且追加新的文件后缀为 8 字节随机字母数字，同时勒索信的名称 README.[1a5cbc12].TXT 也将根据勒索的随机扩展生成相同的随机字母数字。


图：随机的勒索扩展名

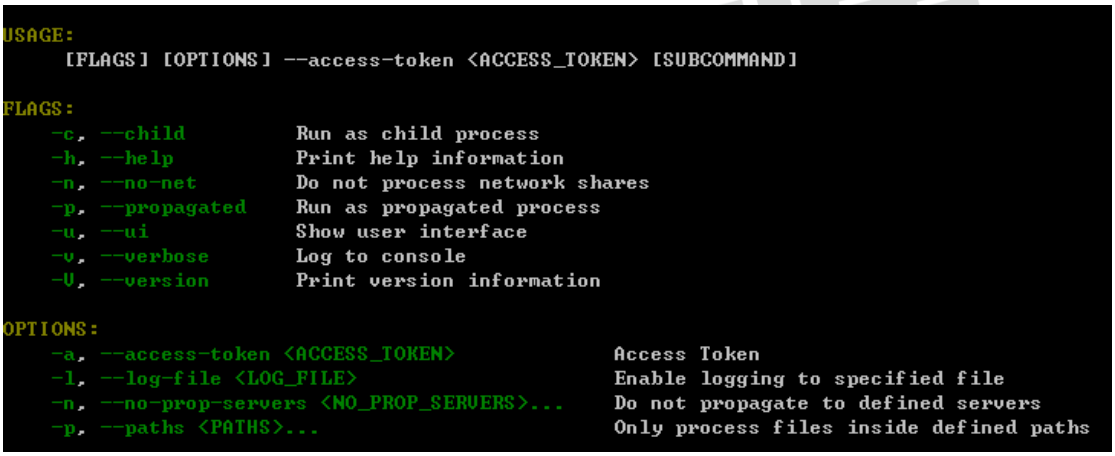
## 3.3 BlackCat 勒索软件

在 2021 年圣诞节前夕，法国 IT 服务商 Inetum Group 遭受到 BlackCat 勒索软件的攻击，所幸未造成严重损失。作为 2021 年的新增勒索组织，Blackcat 以年度最复杂勒索软件著称，其使用以安全开发著称的 Rust 语言编写，在俄语论坛进行过大肆推广，这也是为数不多的，可以进行灵活且全面攻击配置的勒索软件，有更为严谨的加密方案以供选择。




图：BlackCat 勒索信

BlackCat 不仅支持多种加密算法和加密模式，还通过命令行参数与配置文件一同实现针对性的勒索攻击。例如修改勒索信名称、内容，修改加密后缀名，文件加密的模式，以及加密的大小等。这些可能会迷惑勒索软件受害者，令他们难以辨认勒索攻击所属的相关家族。




图：勒索软件的参数化配置

# 四、趋势展望

## （一）APT 组织及攻击活动越来越多被披露

随着全球安全企业对 APT 攻击组织和 APT 攻击活动的持续关注，越来越多的国家级网络攻击被披露，从侧面反映出国家级 APT 攻击的活动频繁，通过捍卫网络安全来保护国家安全任重而道远。

## （二）勒索软件持续危害企业安全

勒索软件主要攻击目标由个人转向企业，全球众多企业、组织遭受到勒索软件攻击，金融、医疗、交通、能源、通信、制造、教育等诸多关键基础设施和重要行业领域无一幸免。一旦遭遇勒索软件攻击，轻则导致业务系统瘫痪、经济损失，重则带来社会性服务的停止，影响城市甚至国家正常运行。企业和组织的攻击面远大于个人，做好安全防护工作难度也远高于个人，通过持续的安全投入，建立网络安全综合治理体系，搭建多层防御系统，编织出一张严密的勒索攻击防御之网是企业和组织对抗勒索软件攻击的重要手段。

## （三）电子邮件依然是网络入侵的主要窗口

全球 90%左右的组织经历过鱼叉式网络攻击，钓鱼邮件是攻击组织进行环境侦察、获取凭据、投递恶意软件的重要手段，与时俱进地做好电子邮件安全成为企业远离一般性网络安全风险的重要手段。

## （四）基础软件安全性备受关注，供应链“投毒”逐渐递增

Apache Log4j2 漏洞是 2021 年最值得关注的基础软件漏洞。开源社区投毒事件屡屡发生，python/node.js 社区均有出现。软件开发者引用开源项目需要谨慎，建立事前源代码安全性审查、事后规范化的应急响应将成为软件开发企业必不可少的基础性安全工作。

## （五）高可利用性的漏洞备受攻击者青睐，“老”漏洞不会很快退出历史舞台

利用成功率极高的漏洞依然受到攻击者的青睐，与漏洞的新老程度无关。这种现象和使用者不积极更新存在漏洞的软件有关，大量没有更新的老旧软件会成为攻击者的首选利用目标。及时更新

或替换携带高危漏洞的老旧软件，有助于消灭企业安全隐患。

## （六）传统威胁检测手段进一步面临考验，人工智能技术应用增多

面对越来越多样性的攻击形式，传统检测手段疲态尽显，目前大多数主流的安全公司已经分领域研究和应用人工智能技术，在未来五年内，人工智能技术将取代传统的特征、规则技术，成为主流的网络安全事件检测和风险评估技术，而攻击者也将从传统的对抗技术，转向同人工智能技术的对抗。

# 附：2021 年国内重大网络安全政策法规

## 1.《工业互联网创新发展行动计划(2021-2023 年)》

2021 年 1 月 13 日，工业和信息化部印发《工业互联网创新发展行动计划(2021-2023 年)》，计划指出，我国工业互联网发展成效显著，2018-2020 年起步期的行动计划全部完成，部分重点任务和工程超预期，网络基础、平台中枢、数据要素、安全保障作用进一步显现。2021-2023 年是我国工业互联网的快速成长期。同时，计划提出工业互联网创新发展目标，其中包括新型基础设施进一步完善、融合应用成效进一步彰显、技术创新能力进一步提升、产业发展生态进一步健全和安全保障能力进一步增强。

## 2.《常见类型移动互联网应用程序必要个人信息范围规定》

2021 年 3 月 22 日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局近日联合印发《常见类型移动互联网应用程序必要个人信息范围规定》。规定指出，App 包括移动智能终端预置、下载安装的应用软件，基于应用软件开放平台接口开发的、用户无需安装即可使用的小程序。本规定所称必要个人信息，是指保障 App 基本功能服务正常运行所必需的个人信息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。规定强调，App 不得因为用户不同意提供非必要个人信息，而拒绝用户使用其基本功能服务。

## 3.《关于印发加强网络安全和数据保护工作指导意见的通知》

2021 年 4 月 6 日，国家医疗保障局发出《关于印发加强网络安全和数据保护工作指导意见的通知》，要求到 2022 年，基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。到“十四五”期末，医疗保障系统网络安全和数据安全保护制度体系

更加健全，智慧医保和安全医保建设达到新水平。

## 4. 《中华人民共和国数据安全法》

2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议通过了《中华人民共和国数据安全法》（简称“《数据安全法》”），自 2021 年 9 月 1 日起施行。该部法律体现了总体国家安全观的立法目标，聚焦数据安全领域的突出问题，确立了数据分类分级管理，建立了数据安全风险评估、监测预警、应急处置、数据安全审查等基本制度，并明确了相关主体的数据安全保护义务，这是我国首部数据安全领域的基础性立法。

## 5. 《IPv6 流量提升三年专项行动计划（2021-2023 年）》

2021 年 7 月 8 日，工信部、网信办联合发布《IPv6 流量提升三年专项行动计划（2021-2023 年）》，《专项行动计划》从基础设施、应用生态、终端、安全四个方面提出了 13 项工作要求和任务举措，重点强化基础设施 IPv6 承载能力，激发应用生态 IPv6 创新活力，提升终端设备 IPv6 支持能力。并要求电信运营商深化网络基础设施 IPv6 改造，千兆光网、5G 网络等新建网络同步部署 IPv6，新增互联网骨干直联点和新型交换中心应支持 IPv6，完成移动物联网 IPv6 改造，深化商业互联网网站和应用 IPv6 升级改造。

## 6. 《网络产品安全漏洞管理规定》

2021 年 7 月 12 日由工业和信息化部、国家互联网信息办公室、公安部三部门联合印发，自 2021 年 9 月 1 日起施行。此规定中规范了漏洞发现、报告、修补和发布等行为，明确网络产品提供者、网络运营者以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人的责任与义务，将推动网络产品安全漏洞管理工作的制度化、规范化、法治化，提高相关主体漏洞管理水平，引导建设规范有序、充满活力的漏洞收集和发布渠道，防范网络安全重大风险，保障国家网络安全。

## 7. 《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》

2021 年 7 月 12 日，工信部公开征求对《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》的意见。意见稿提出，到 2023 年，网络安全产业规模超过 2500 亿元，年复合增长率超过 15%，一批网络安全关键核心技术实现突破，达到先进水平。新兴技术与网络安全融合创新明显加快，网络安全产品、服务创新能力进一步增强。

## 8. 《关键信息基础设施安全保护条例》

2021 年 7 月 30 日，国务院总理李克强签署中华人民共和国国务院令第 745 号：《关键信息基础设施安全保护条例》，该《条例》于 8 月 17 日正式发布，自 2021 年 9 月 1 日起施行。该条例在《网络安全法》框架下，聚焦关键信息基础设施安全，建立专门保护制度，明确关键信息基础设施的认定原则和程序，压实关键信息基础设施运营者的义务和责任，对关键信息基础设施的网络安全提出明确的监管要求。

## 9. 《中华人民共和国个人信息保护法》

2021 年 8 月 20 日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，自 2021 年 11 月 1 日起施行。个人信息保护法借鉴国际经验并立足我国实际，确立了个人信息处理应遵循的原则，强调处理个人信息应当遵循合法、正当、必要和诚信原则，具有明确、合理的目的并与处理目的直接相关，采取对个人权益影响最小的方式，限于实现处理目的的最小范围，公开处理规则，保证信息质量，采取安全保护措施等。

## 10. 《关于加强互联网信息服务算法综合治理的指导意见》

2021 年 9 月 29 日，网信办、教育部、科技部等九部委联合发布《关于加强互联网信息服务算法综合治理的指导意见》，意见指出，坚持正确导向，强化科技伦理意识、安全意识和底线思维，充分发挥算法服务正能量传播作用，营造风清气正的网络空间；坚持依法治理，加强法律法规建设，创新技术监管模式，打击违法违规行为，建立健全多方参与的算法安全治理机制；坚持风险防控，推进算法分级分类安全管理，有效识别高风险类算法，实施精准治理；坚持权益保障，引导算法应用公平公正、透明可释，充分保障网民合法权益；坚持技术创新，大力推进我国算法创新研究工作，保护算法知识产权，强化自研算法的部署和推广，提升我国算法的核心竞争力。

## 11. 《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》

2021 年 9 月 30 日，工信部公开征求对《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》的意见，旨在贯彻落实《数据安全法》等法律法规，防范数据安全风险。《征求意见稿》提出应当坚持先分类后分级，定期梳理，根据行业要求、业务需求、数据来源和用途等因素对数据进行分类和标识，形成数据分类清单；工业和电信数据处理者应当对数据处理活动负安全主体责任；工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据；依照法律、行政法规要求重要数据在境内存储，若需向境外提供则应当依法依规进行数据出境安全评估，在确保安全的前提下进行数据出境。

## 12. 《网络数据安全管理条例（征求意见稿）》

2021 年 11 月 14 日，国家网信办发布《网络数据安全管理条例（征求意见稿）》，向社会公开征求意见。这是《网络安全法》、《数据安全法》和《个人信息保护法》三大数据法规在执行层面的重要的配套法规，其中《网络安全法》聚焦网络空间安全整体治理和数据保护，《数据安全法》针对数据处理活动的安全与开发利用，《个人信息保护法》负责网络环境下的信息或隐私，三者并行，成为网络治理和数据保护的“三驾马车”。而《意见稿》以规范网络数据处理活动，保障数据安全，保护个人、组织在网络空间的合法权益，维护国家安全、公共利益方面为目的，是对“三驾马车”的执行、细化和补充。

## 13. 《“十四五”信息通信行业发展规划》

2021 年 11 月 16 日，工业和信息化部发布《“十四五”信息通信行业发展规划》，明确提出，到 2025 年，信息通信行业整体规模进一步壮大，发展质量显著提升，基本建成高速泛在、集成互联、智能绿色、安全可靠的新型数字基础设施，创新能力大幅增强，新兴业态蓬勃发展，赋能经济社会数字化转型升级的能力全面提升，成为建设制造强国、网络强国、数字中国的坚强柱石。

## 14. 《网络安全审查办法》

2021 年 11 月 16 日，国家互联网信息办公室 2021 年第 20 次室务会议审议通过《网络安全审查办法》，网信办、发改委、工信部等十三部门联合修订发布《网络安全审查办法》，于 2022 年 1 月 4 日公布，自 2022 年 2 月 15 日起施行。《办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须向网络安全审查办公室申报网络安全审查。根据审查实际需要，增加证监会作为网络安全审查工作机制成员单位，同时完善了国家安全风险评估因素等内容。

## 15. 《国家安全战略（2021—2025 年）》

2021 年 11 月 18 日，中共中央政治局召开会议审议《国家安全战略（2021—2025 年）》。会议指出，新形势下维护国家安全，必须牢固树立总体国家安全观，加快构建新安全格局。必须坚持党的绝对领导，完善集中统一、高效权威的国家安全工作领导体制，实现政治安全、人民安全、国家利益至上相统一；坚持捍卫国家主权和领土完整，维护边疆、边境、周边安定有序；坚持安全发展，推动高质量发展和高水平安全动态平衡；坚持总体战，统筹传统安全和非传统安全；坚持走和平发展道路，促进自身安全和共同安全相协调。

## 16. 《“十四五”软件和信息技术服务业发展规划》

2021 年 11 月 30 日，工信部正式发布《“十四五”软件和信息技术服务业发展规划》，《规划》提出，“十四五”时期我国软件和信息技术服务业要实现“产业基础实现新提升，产业链达到新水平，生态培育获得新发展，产业发展取得新成效”的“四新”发展目标。到 2025 年，规模以上企业软件业务收入突破 14 万亿元，年均增长 12%以上，工业 APP 突破 100 万个，建设 2-3 个有国际影响力的开源社区，高水平建成 20 家中国软件名园。

## 17. 《“十四五”大数据产业发展规划》

2021 年 11 月 30 日，工信部正式发布《“十四五”大数据产业发展规划》，《规划》要求，到 2025 年，大数据产业测算规模突破 3 万亿元，年均复合增长率保持在 25%左右，创新力强、附加值高、自主可控的现代化大数据产业体系基本形成。数据要素价值评估体系初步建立，要素价格市场决定，数据流动自主有序，资源配置高效公平，培育一批较成熟的交易平台，市场机制基本形成。关键核心技术取得突破，标准引领作用显著增强，形成一批优质大数据开源项目，存储、计算、传输等基础设施达到国际先进水平。

## 18. 《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）（征求意见稿）》

2021 年 12 月 22 日，工业和信息化部研究起草《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）》，并面向社会公开征求意见。《工作指引》指出，风险信息报送，是指有关单位向工业和信息化部、地方工业和信息化主管部门、地方通信管理局报送数据安全风险信息的行为。风险信息共享，是指经工业和信息化部、地方工业和信息化主管部门、地方通信管理局审核、授权后，向有关部门、单位告知风险提示的行为。风险信息报送与共享工作坚持“及时、客观、准确、真实、完整”的原则，不得迟报、瞒报、谎报。

## 19. 《工业互联网综合标准化体系建设指南（2021 版）》

2021 年 12 月 24 日，工业和信息化部、国家标准化管理委员会联合印发《工业互联网综合标准化体系建设指南（2021 版）》。《指南》提出，明确到 2023 年，工业互联网标准体系持续完善。制定术语定义、通用需求、供应链/产业链、人才等基础共性标准 15 项以上，“5G+工业互联网”、信息模型、工业大数据、安全防护等关键技术标准 40 项以上，面向汽车、电子信息、钢铁、轻工（家电）、装备制造、航空航天、石油化工等重点行业领域的应用标准 25 项以上，推动标准优先在重点行业和领域率先应用，引导企业在研发、生产、管理等环节对标达标。到 2025 年，制定工业互联网关键技术、产品、管理及应用等标准 100 项以上，建成统一、融合、开放的工业互联网标准体系，形成标准广泛应用、与国际先进水平保持同步发展的良好局面。

## 20. 《“十四五”国家信息化规划》

2021 年 12 月 27 日，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》。《规划》提出，到 2025 年，数字中国建设取得决定性进展，信息化发展水平大幅跃升。数字基础设施体系更加完备，数字技术创新体系基本形成，数字经济发展质量效益达到世界领先水平，数字社会建设稳步推进，数字政府建设水平全面提升，数字民生保障能力显著增强，数字化发展环境日臻完善。

## 21. 《“十四五”智能制造发展规划》

2021 年 12 月 28 日，工业和信息化部等八部门联合印发了《“十四五”智能制造发展规划》。《规划》提出推进智能制造的总体路径是：立足制造本质，紧扣智能特征，以工艺、装备为核心，以数据为基础，依托制造单元、车间、工厂、供应链等载体，构建虚实融合、知识驱动、动态优化、安全高效、绿色低碳的智能制造系统，推动制造业实现数字化转型、网络化协同、智能化变革。未来 15 年通过“两步走”，加快推动生产方式变革：一是到 2025 年，规模以上制造业企业大部分实现数字化网络化，重点行业骨干企业初步应用智能化；二是到 2035 年，规模以上制造业企业全面普及数字化网络化，重点行业骨干企业基本实现智能化。

**北京瑞星网安技术股份有限公司**
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
咨询：400-660-8866
网站：http://www.rising.com.cn