总第3期

2021年6月

直击本月重点安全漏洞 回顾网络安全重大事件
掌握勒索病毒攻击态势 聚焦移动安全数据分析

网络安全月报

本期热点

Windows Print Spooler远程代码执行漏洞
用友NC BeanShell远程代码执行漏洞
谷歌Android应用程序中检测到安全漏洞
研究人员发现了针对韩国政府的黑客行动
奥迪、大众330万客户遭遇数据泄露
Ragnar Locker勒索团队公开ADATA 700G 敏感数据
西部数据NAS设备遭到网络攻击，硬盘遭遇格式化
APT组织Lazarus Group对中国发起攻击

官网链接：https://cert.360.cn
联系我们：g-cert-report@360.cn

360CERT
COMPUTER EMERGENCY READINESS TEAM

前言

当前，随着数字时代进程逐渐加快，网络空间博弈上升到全新高度。潜在的漏洞风险持续存在，全球各类高级威胁层出不穷。洞悉国内外网络安全形势，了解网络安全重要漏洞是建设好自身安全能力的重要基石。在此背景下，360CERT推出《网络安全月报》，分析本月国内外安全漏洞、网络安全重大事件、恶意软件攻击态势、移动安全情况等。每个章节中都具备总结性文字、重点罗列、图表分析等展现形式，方便读者了解本月网络安全态势。

团队介绍

360CERT 是高级威胁研究分析中心的尖兵团队，团队致力于维护计算机网络空间安全，是 360 基于 "协同联动，主动发现，快速响应 " 的指导原则，对全球重要网络安全事件进行快速预警、应急响应的安全协调中心。针对全球重大安全漏洞第一时间启动安全响应流程，发布权威报告，帮助用户进行预防处理，保护用户和互联网安全。

目录

2021 DIRECTORY

网络安全月报

网络安全月度综述

OVERVIEW

前言

本月度重点关注安全漏洞分析、网络安全重大事件、勒索病毒攻击态势、移动安全数据分析、样本分析等。

目录预览

综述

summary

一、安全漏洞

2021年6月，360CERT共收录66个漏洞，其中严重19个，高危34个，中危13个。主要包含代码执行漏洞、UAF漏洞、特权提升漏洞、拒绝服务漏洞、验证绕过漏洞、内存越界漏洞等。涉及的厂商主要是Windows、 用友NC、Apache、Adobe 、安卓、VMware、Chrome。Istio等。

二、安全事件

本月收录安全事件161项，话题集中在数据泄露、恶意程序、网络攻击方面，涉及的组织有：Microsoft、Google、Facebook、Youtube、Adobe、JBS、三星、华为等。涉及的行业主要包含IT服务业、政府机关及社会组织、制造业、卫生和社会工作、教育行业、金融业等。

三、恶意程序

勒索病毒传播至今，360反勒索服务已累计接收到上万勒索病毒感染求助。随着新型勒索病毒的快速蔓延，企业数据泄露风险不断上升，数百万甚至上亿赎金的勒索案件不断出现。勒索病毒给企业和个人带来的影响范围越来越广，危害性也越来越大。360安全大脑针对勒索病毒进行了全方位的监控与防御，为需要帮助的用户提供360反勒索服务。

2021年6月，全球新增的活跃勒索病毒家族有:Spyro、APISWiper 、ChupaCabra 、Vice Society 、Findnotfile、Red Epsilon，Hive等。其中Red Epsilon家族利用Microsoft Exchange服务器漏洞对网络上的机器进行攻击，在攻击成功后还会在被攻陷设备中部署远程控制木马（Remote Utilities）；采用RaaS运营模式的

HimalayA家族，仅需RaaS服务收费200美元便为其成员免费提供加密器，同时该团伙还宣称不会对医疗机构以及非盈利组织发动攻击；Hive家族采用双重勒索模式运营，目前为止该家族已在暗网发布了2个组织的数据。

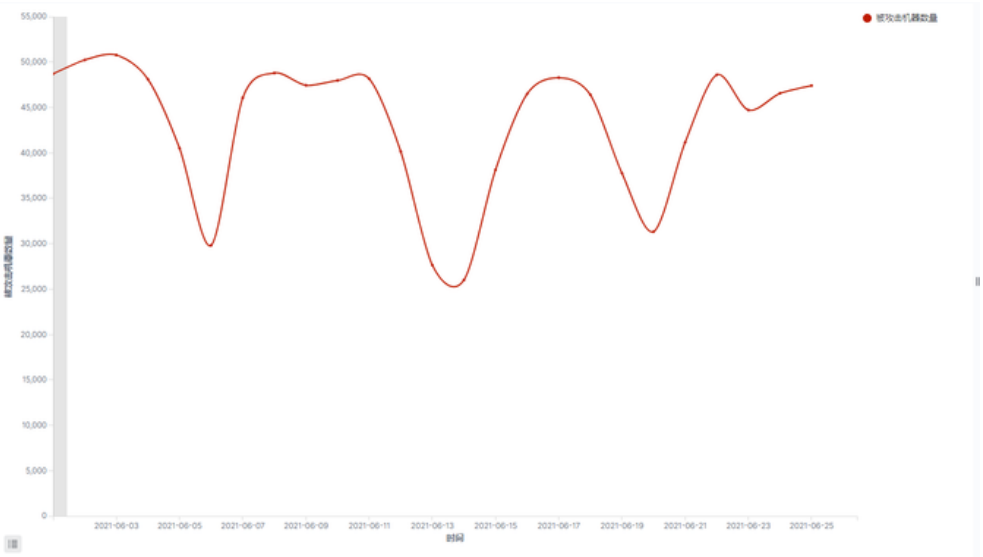
通过隐私窃取拦截量TOP10来看，上海、广东、福建这三个省份移动端隐私窃取数量占据前列，基本上可以体现人口越集中、经济越发达、移动设备使用数量越多的省份，软件恶意行为更加猖獗、恶意软件存活比例越大。

本月攻击态势

Attack situation analysis

一、僵尸网络攻击

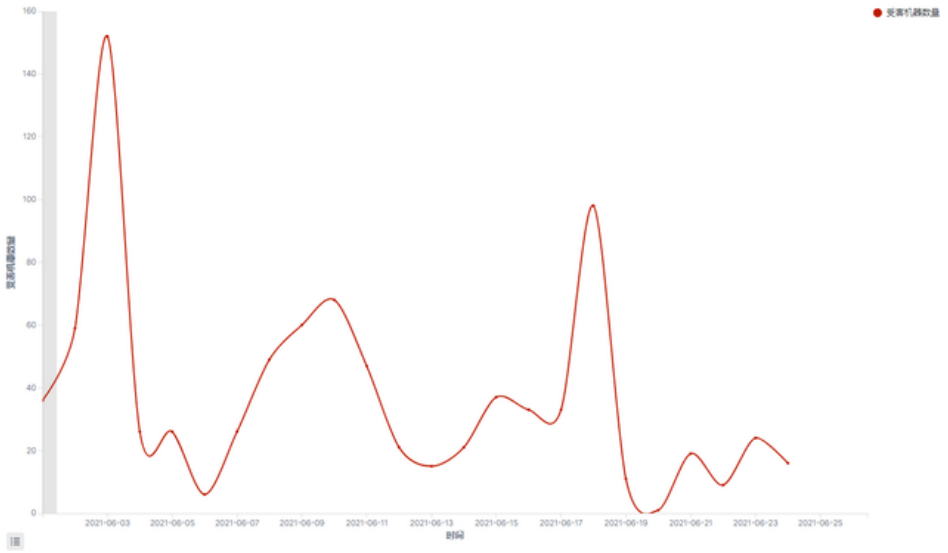
本月Windows终端下僵尸网络活动相对平稳，受害用户数量与上个月相比基本持平。经过一个月的“复苏”之后，“紫狐”挖矿僵尸网络的攻击趋势已基本稳定，目前每天超过10000台计算机被“紫狐”僵尸网络入侵。



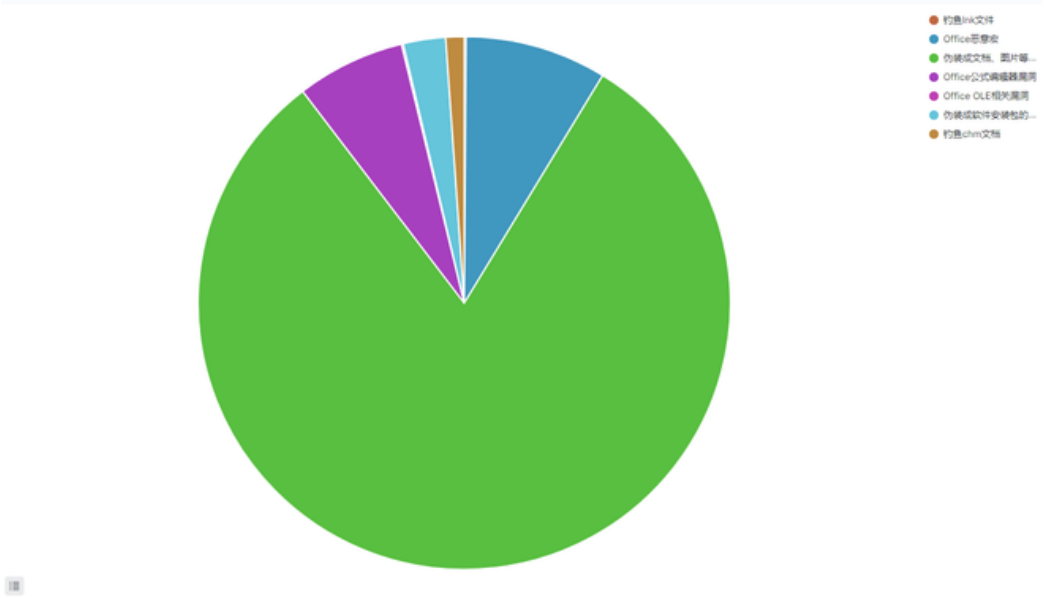
本月，另一大挖矿僵尸网络——“驱动人生”挖矿僵尸网络进行了小范围更新，此次更新中，“驱动人生”僵尸网络在其入侵的ExChange服务器中植入DDoS木马，意图在挖矿之外开辟新的牟利方式。此次更新仅针对小部分受害用户进行，这也符合“驱动人生”僵尸网络在进行功能更新时所使用的策略偏好。

二、钓鱼邮件攻击

本月钓鱼邮件攻击数量相比5月出现一定增长，增长的原因是省级、市级攻防演练中攻击队使用了大量钓鱼邮件。这类钓鱼邮件附件文件名一般具有迷惑性，例如：“单位人员缴费基数调整表.xls.exe”、“七一放假安排.docx.exe”，“打完疫苗注意以下几点不能做.png.exe”，诱导攻击目标双击运行。本月钓鱼邮件攻击趋势如下所示。

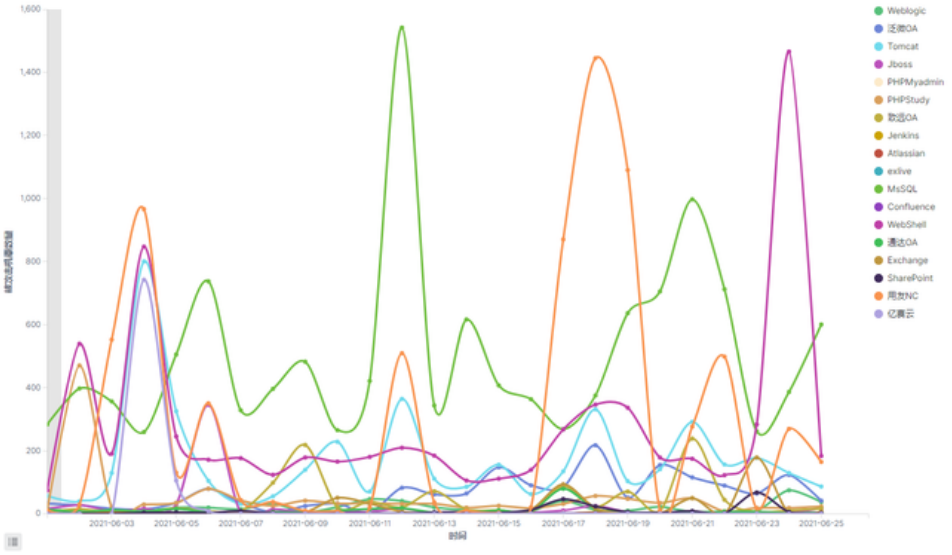


在攻击方式分布上，伪装成文档、图片等的可执行文件占比超80%，而恶意Office宏和公式编辑器漏洞这两种银行木马偏爱的攻击方式占比超16%。

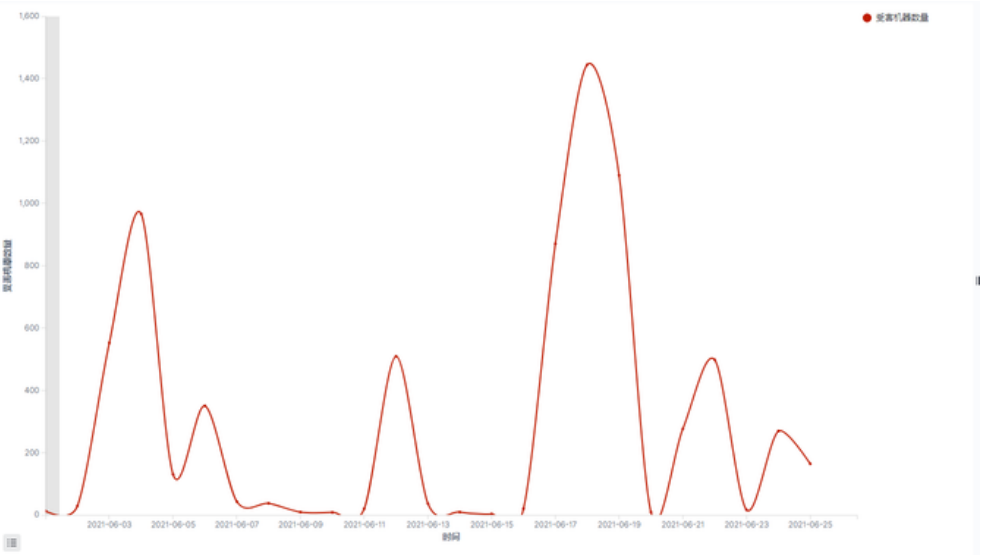


三、针对Web应用和数据库的攻击

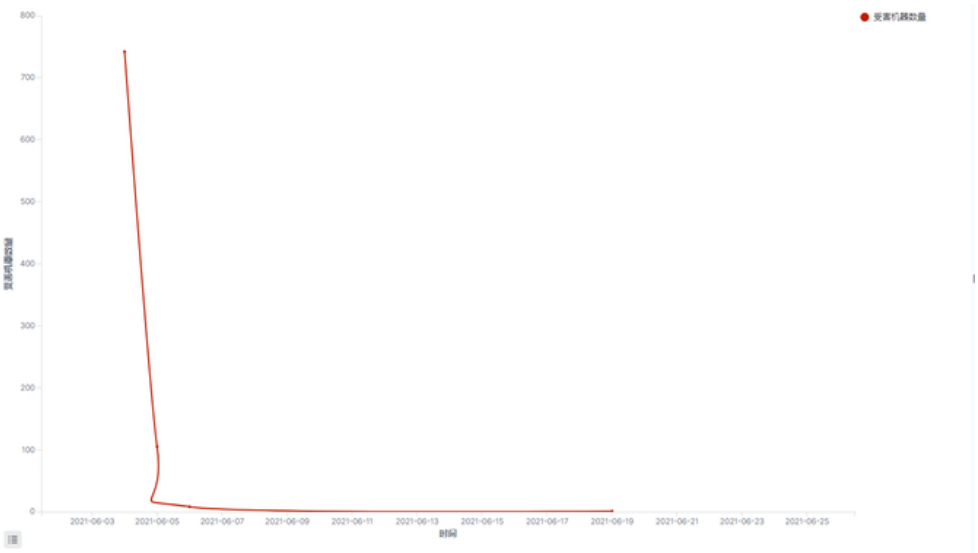
在今年5月针对Web应用和数据库的攻击中，针对用友NC平台、泛微OA、Weblogic等Web应用和OA系统的攻击出现大幅度增长。进入6月后，针对泛微OA和Weblogic的攻击有所减少，而针对用友NC平台的攻击有增无减。下图展示了6月份针对Web应用和数据库的攻击趋势。



不难看出，针对用友NC平台的攻击出现多个峰值，单日最高有将近1500台搭载用友NC的服务器遭到攻击。根据360安全大脑的监测数据，6月份有多个黑产团伙利用用友NC平台漏洞对互联网中开放的用友NC平台发起攻击，其中部分黑产团伙向受害机器植入挖矿木马，也有部分黑产团伙向目标机器写入WebShell以追求对目标机器的持续控制。下图展示了本月针对用友NC平台的攻击趋势。



除了用友NC外，本月有黑产组织对亿赛通电子文档安全管理系统发起攻击。该黑产团伙疑似利用互联网上公开的漏洞利用代码对网络上的亿赛通电子文档安全管理系统进行扫描和入侵，入侵成功后植入名为“Index_bk.jsp”的WebShell，除了亿赛通电子文档安全管理系统外，该团伙也会攻击用友NC平台。下图展示了本月针对亿赛通电子文档安全管理系统的攻击趋势。



安全漏洞

VULNERABILITIES

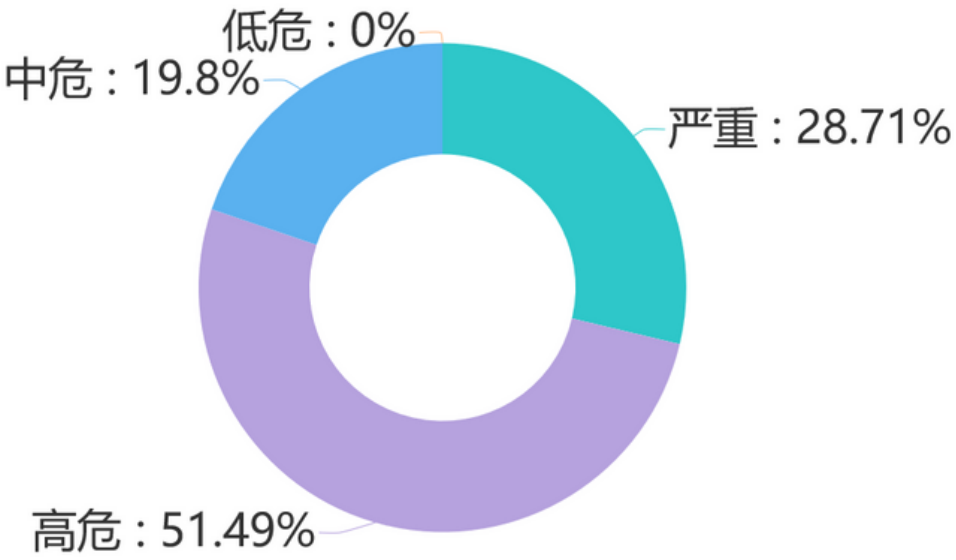
前言

2021年6月，360CERT共收录66个漏洞，其中严重19个，高危34个，中危13个。主要包含代码执行漏洞、UAF漏洞、特权提升漏洞、拒绝服务漏洞、验证绕过漏洞、内存越界漏洞等。涉及的厂商主要是Windows、用友NC、Apache、Adobe、安卓、VMware、Chrome、Istio等。

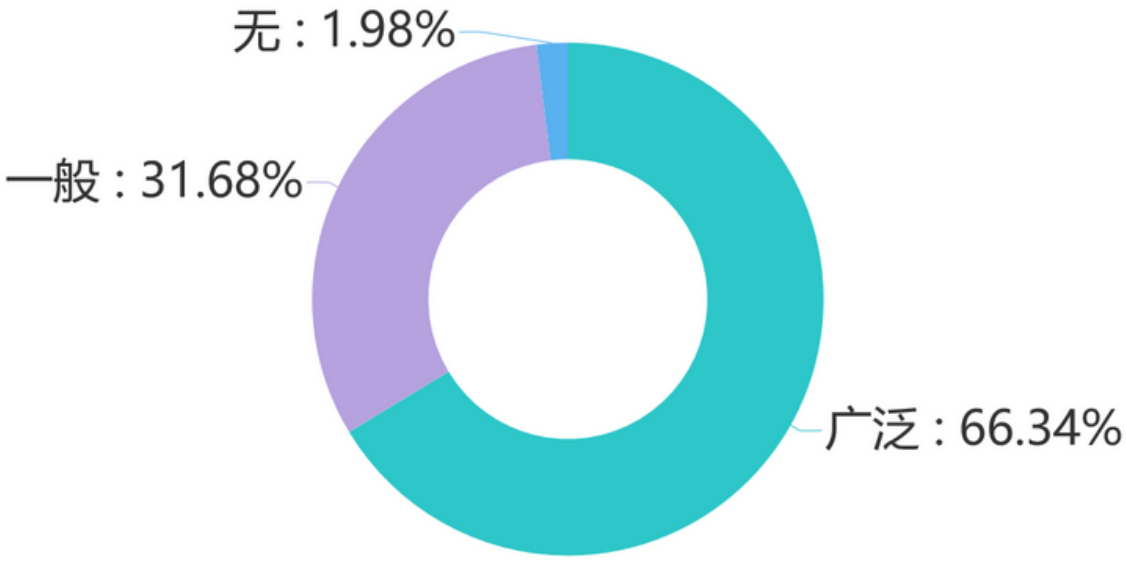
目录预览

漏洞图表

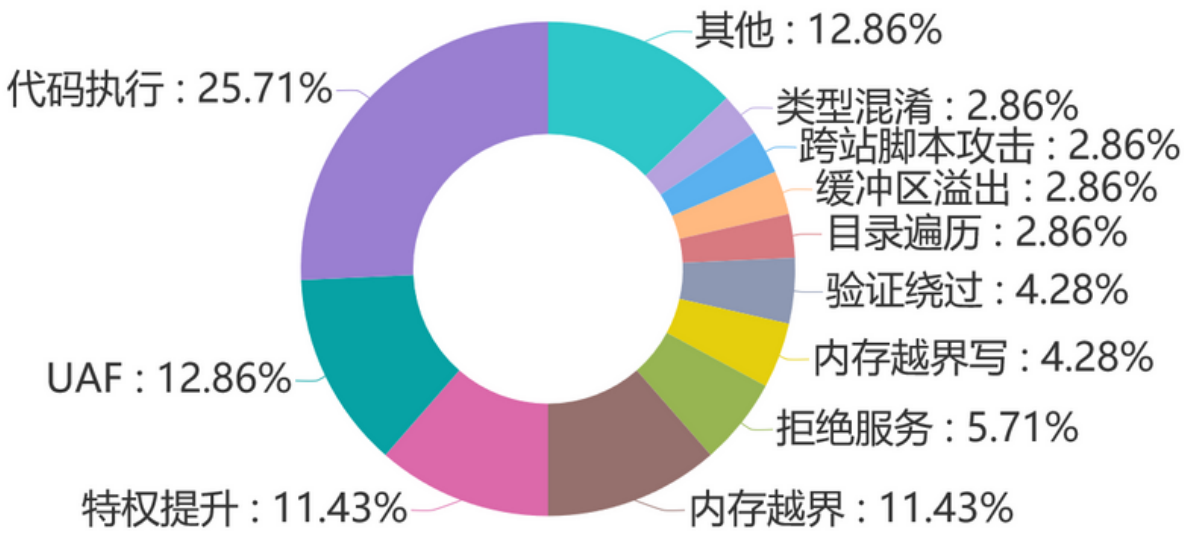
Charts Of Vulnerabilities



漏洞等级占比情况



漏洞影响范围占比情况



漏洞类型数量情况

Windows Print Spooler
用友NC
ForgeRock AM
Microsoft Defender
Microsoft SharePoint Server
Istio
Apache Dubbo
Adobe Acrobat Reader
Andriod
Chrome BFCache
VMware Carbon Black App Control
runc
Cortex XSOAR
AutoDesk

热门组件列表

重点漏洞回顾

Review Of Vulnerabilities

Windows Print Spooler远程代码执行漏洞 评分：7.8

2021年06月29日，360CERT监测发现安全研究人员在GitHub上公开了Windows Print Spooler远程代码执行漏洞的POC，漏洞编号为CVE-2021-1675。Windows Print Spooler是Windows的打印机后台处理程序，广泛的应用于各种内网中，攻击者可以通过该漏洞绕过PfcAddPrinterDriver的安全验证，并在打印服务器中安装恶意的驱动程序。若攻击者所控制的用户在域中，则攻击者可以连接到DC中的Spooler服务，并利用该漏洞在DC中安装恶意的驱动程序，完整的控制整个域环境。

用友NC BeanShell远程代码执行漏洞 评分：9.8

2021年06月03日，360CERT监测发现用友官方发布了用友BeanShell远程代码执行漏洞的风险通告，漏洞编号为CNVD-2021-30167。该漏洞是由于用友NC对外开放了BeanShell接口，攻击者可以在未授权的情况下直接访问该接口，构造恶意数据执行任意代码并获取服务器权限。

ForgeRock AM远程代码执行漏洞 评分：9.8

2021年06月30日，360CERT监测发现portswigger发布了ForgeRock AM远程代码执行漏洞的漏洞分析报告，漏洞编号为CVE-2021-35464。ForgeRock AM是一个开源的访问管理、权限控制平台，在大学、社会组织中存在广泛的应用。未经身份验证的攻击者可以通过构造特殊的请求远程执行任意代码，并接管运行ForgeRock AM的服务器。由于 ForgeRock AM本身的权限管理功能，攻击者在控制 ForgeRock AM的服务器的同时，还可以直接访问其他敏感服务，进行进一步的攻击。

Microsoft Defender远程命令执行漏洞 评分：7.8

2021年06月08日，360CERT监测发现微软发布了Microsoft Defender远程命令执行漏洞的通告，漏洞编号为CVE-2021-31985。Microsoft Defender是Windows内置的安全软件，默认安装，该漏洞可让攻击者绕过Defender的防御策略，构造特制的二进制程序并诱使用户打开，即可接管用户计算机。

Microsoft SharePoint Server远程代码执行漏洞 评分：7.1

2021年06月08日，360CERT监测发现微软发布了SharePoint Server远程命令执行漏洞的通告，漏洞编号为CVE-2021-31963。Microsoft SharePoint是微软公司开发的一个企业业务协作平台。该平台用于对业务信息进行整合，并能够实现共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息，是业界领先的技术解决方案，在全世界拥有大量客户。攻击者利用该漏洞可以构造特制的Http请求并发送至SharePoint Server完成远程代码执行。

Istio 敏感信息窃取漏洞 评分：9.1

2021年06月28日，360CERT监测发现Istio发布了SECURITY-2021-007的风险通告，漏洞编号为CVE-2021-34824。Istio是运行在 k8s 容器服务上的一套软件，是一种服务网格，是一种现代化的服务网络层，它提供了一种透明、独立于语言的方法，能够灵活且轻松地实现应用网络功能自动化。Istio 包含一个可远程利用漏洞，使用Istio的k8s集群内的机器有可能被攻击者越权访问到TLS证书和密钥，并借此接管k8s集群。

Apache Dubbo多个高危漏洞 评分：9.8

2021年06月24日，360CERT监测发现Github SecurityLab发布了Dubbo组件多个高危漏洞的风险通告，漏洞编号包括CVE-2021-25641等。Apache Dubbo是一款高性能、轻量级的开源Java RPC框架，它提供了三大核心功能：面向接口的远程方法调用，智能容错和负载均衡，以及服务自动注册和发现。攻击者可以构造恶意请求调用恶意方法从而造成任意代码执行。

Adobe Acrobat Reader多个严重漏洞 评分：9.8

2021年06月09日，360CERT监测发现Adobe发布了Adobe Acrobat Reader 安全更新的风险通告，其中涉及5个严重漏洞。漏洞编号包含CVE-2021-28554、CVE-2021-28551、CVE-2021-28552、CVE-2021-28631、CVE-2021-28632。Adobe Reader用于处于企业内网的员工办公主机上，攻击者通常会使用社会工程学的方式将身份伪装成求职者等其他身份向企业员工发送包含恶意代码的PDF文件，当企业员工运行该文件时，攻击者便可在员工主机上直接执行任意代码，从而突破企业边界防御策略，直接入侵到企业办公网段。

Andriod越界写漏洞 评分：8.8

2021年06月09日，360CERT监测发现Google发布了Andriod越界写漏洞的通告，漏洞编号为CVE-2021-0507。Andriod系统被广泛的使用在手机、终端设备中，在Android系统中存在一个越界写漏洞，攻击者可以利用该漏洞造成远程代码执行。该漏洞存在于Android原生系统中，无需用户交互即可完成攻击，漏洞影响面极大，危害高，漏洞利用程序编写难度大。

Chrome BFCache UAF漏洞 评分：8.8

2021年06月09日，360CERT监测发现Google发布了Chrome BFCache 释放后重用漏洞的通告，漏洞编号为CVE-2021-30544。BFCache是Chrome的基础库，受益于Chrome在全世界的广泛使用量，一旦攻击者掌握该漏洞并利用该漏洞制造恶意站点进行钓鱼攻击，便可以在访问了该恶意站点的用户主机上执行任意代码。利用价值极高。

VMware Carbon Black App Control身份验证绕过漏洞 评分：9.4

2021年06月23日，360CERT监测发现VMware发布Carbon Black App Control身份验证绕过的风险通告，漏洞编号为CVE-2021-21998。VMware Carbon Black Cloud Workload（简称AppC）是一种软件即服务(SaaS)解决方案，提供下一代反病毒(NGAV)、端点检测和响应(EDR)、高级威胁搜索和漏洞管理等服务，被广泛的应用于云上主机中。攻击者利用该漏洞无需身份验证即可获得对该产品的管理访问权限。

Cortex XSOAR未认证REST API使用漏洞 评分：9.8

2021年06月23日，360CERT监测发现Palo Alto发布了Cortex XSOAR未认证REST API使用的风险通告，漏洞编号为CVE-2021-3044。Cortex XSOAR是Palo Alto公司的SOAR产品，其主要作用是跨源提取报警信息并执行自动化的工作流以加快事件响应速度，在世界范围内有大量客户。未认证的攻击者可以通过该漏洞访问Cortex XSOAR提供的API，并创建或执行剧本启动对应的自动化流程以进行敏感数据访问、执行命令等相关操作。

漏洞时间线

Timeline Of Vulnerabilities

2021-06-01

CVE-2021-27219 高危
glib2 整形溢出漏洞

CVE-2021-30465 高危
runc 虚拟化逃逸漏洞

CVE-2021-23017 高危
nginx 缓冲区溢出漏洞

2021-06-02

CVE-2021-28091 高危
lasso 验证绕过漏洞

2021-06-03

CNVD-2021-30167 严重
NC 代码执行漏洞

CVE-2021-24370 严重
Fancy Product Designer 代码执行漏洞

2021-06-04

CVE-2021-31181 高危
SharePoint 代码执行漏洞

CVE-2021-3560 中危
polikit 特权提升漏洞

2021-06-07

CVE-2021-33898 中危
invoiceninja 代码执行漏洞

2021-06-08

CVE-2021-33203 中危
Django 目录遍历漏洞

CVE-2021-33571 中危
Django 服务器端请求伪造漏洞

2021-06-09

CVE-2021-33742 严重
Windows Trident 代码执行漏洞

CVE-2021-31201 中危
Enhanced Cryptographic Provider 特权提升漏洞

CVE-2021-31199 中危
Enhanced Cryptographic Provider 特权提升漏洞

CVE-2021-31956 高危
NTFS 特权提升漏洞

CVE-2021-33739 高危
DWM Core Library 特权提升漏洞

CVE-2021-31968 高危
Remote Desktop Services 拒绝服务漏洞

CVE-2021-31985 严重
Defender 代码执行漏洞

CVE-2021-31963 严重
SharePoint 代码执行漏洞

CVE-2021-31955 高危
Windows 信息泄露漏洞

CVE-2021-28554 严重
Acrobat Reader DC 内存越界读漏洞

CVE-2021-28551 严重
Acrobat DC 内存越界读漏洞

CVE-2021-28552 严重
Acrobat DC UAF漏洞

CVE-2021-28631 严重
Acrobat Reader DC UAF漏洞

CVE-2021-28632 严重
Acrobat Reader DC UAF漏洞

CVE-2021-0507 严重
Android AOSP 内存越界写漏洞

CVE-2021-0516 严重
Android AOSP 特权提升漏洞

2021-06-10

CVE-2021-30544 严重
Chrome UAF漏洞

CVE-2021-30551 高危
Chrome 类型混淆漏洞

2021-06-14

CVE-2021-27033 高危
Design Review 内存多重释放漏洞

CVE-2021-27034 高危
Design Review 缓冲区溢出漏洞

CVE-2021-27035 高危
Design Review 内存越界漏洞

CVE-2021-27036 高危
Design Review 内存越界写漏洞

CVE-2021-27037 高危
Design Review UAF漏洞

CVE-2021-27038 高危
Design Review 类型混淆漏洞

CVE-2021-27039 高危
Design Review 内存越界漏洞

2021-06-15

CVE-2021-20027 高危
SonicOS 拒绝服务漏洞

CVE-2021-31812 中危
PDFBox 内存越界漏洞

2021-06-16

CVE-2021-31521 中危
IWSVA 跨站脚本攻击漏洞

CVE-2021-29702 高危
Db2 拒绝服务漏洞

2021-06-17

CVE-2021-1567 高危
AnyConnect DLL劫持漏洞

CVE-2021-34551 严重
PHPMailer 代码执行漏洞

CVE-2021-3603 严重
PHPMailer 代码执行漏洞

2021-06-18

CVE-2021-34553 中危
Nexus 目录遍历漏洞

CVE-2020-9493 高危
Chainsaw 序列化漏洞

2021-06-21

CVE-2021-30554 高危
Edge UAF漏洞

CVE-2021-30555 高危
Chrome UAF漏洞

CVE-2021-30556 高危
Edge UAF漏洞

CVE-2021-30557 高危
Chrome UAF漏洞

2021-06-22

CVE-2021-21999 中危
VMRC 特权提升漏洞

2021-06-23

CVE-2021-21998 严重
Carbon Black App Control 身份验证绕过漏洞

CVE-2021-3044 严重
Cortex XSOAR 未授权REST API使用漏洞

2021-06-24

CVE-2021-25641 高危
Dubbo 序列化漏洞

CVE-2021-30179 高危
Dubbo 验证绕过漏洞

CVE-2021-32824 高危
Dubbo 验证绕过漏洞

CVE-2021-30180 中危
Dubbo 序列化漏洞

2021-06-28

CVE-2021-27850 高危
Tapestry 序列化漏洞

CVE-2021-3476 高危
OpenEXR 未定义移位操作漏洞

CVE-2021-34824 高危
Istio 敏感信息泄漏漏洞

2021-06-29

CVE-2021-32461 高危
Password Manager 特权提升漏洞

CVE-2021-32462 高危
Password Manager 代码执行漏洞

CVE-2021-26691 中危
WebSphere Application Server 拒绝服务漏洞

CVE-2021-1675 严重
Windows Server 2012 代码执行漏洞

CVE-2021-21871 高危
PowerISO 内存越界写漏洞

2021-06-30

CVE-2020-3580 中危
ASA Software 跨站脚本攻击漏洞

CVE-2021-35464 严重
OpenAM 代码执行漏洞

安全建议

Security Advice

- 各行业主管部门应积极关注相关应用或设备的威胁情报，建立完善的漏洞管理流程及应急响应流程，及时推动严重漏洞的修复流程。
- 企业内部应做好资产管理，及时进行内部资产统计，完善内部资产管理体系，以便在漏洞出现时及时做好自查工作。
- 安装了安全产品企业应及时联系相关安全厂商定期更新安全产品检测规则，并定期进行内部漏洞扫描工作。
- 周期性的进行内部的安全测试或安全演习，及时发现并修复相关威胁。
- 定期进行企业安全培训，形成企业安全用网规范，提高员工安全意识。

安全事件

SECURITY INCIDENTS

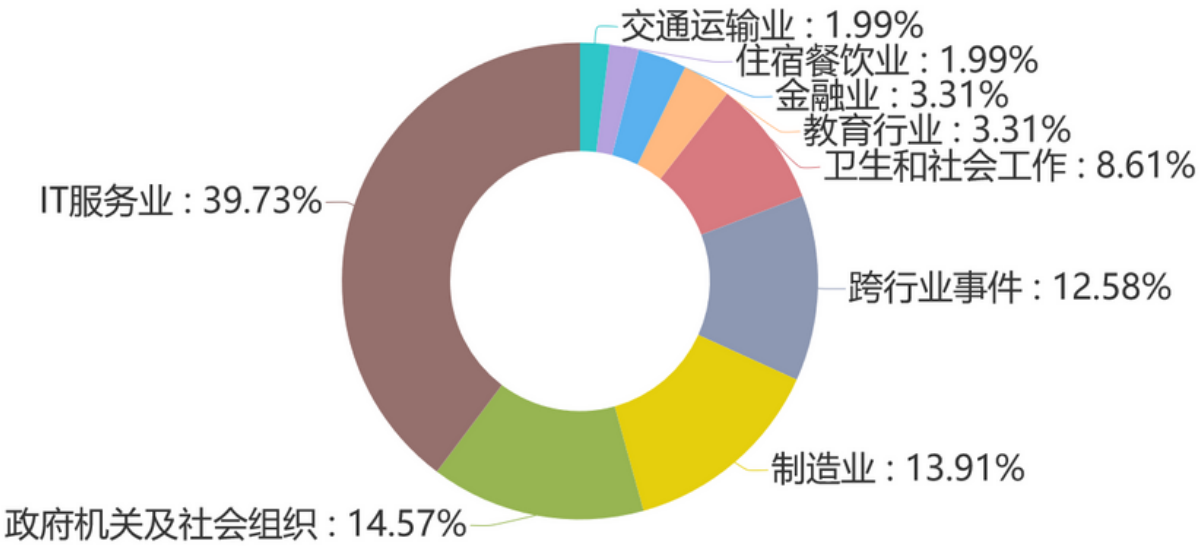
前言

本月收录安全事件161项，话题集中在数据泄露、恶意程序、网络攻击方面，涉及的组织有：Microsoft、Google、Facebook、Youtube、Adobe、JBS、三星、华为等。涉及的行业主要包含IT服务业、政府机关及社会组织、制造业、卫生和社会工作、教育行业、金融业等。

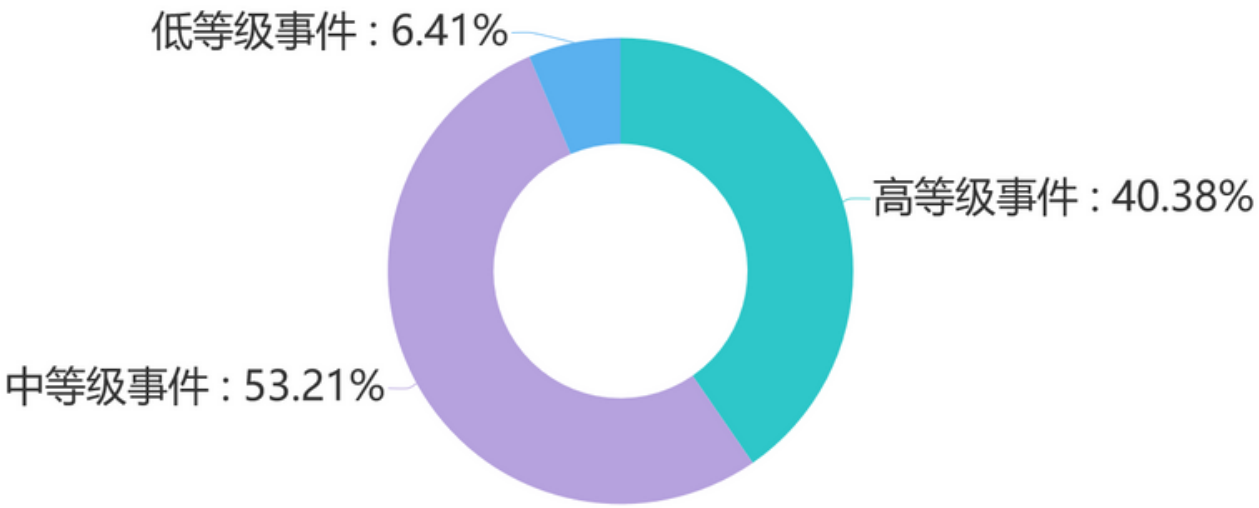
目录预览

事件图表

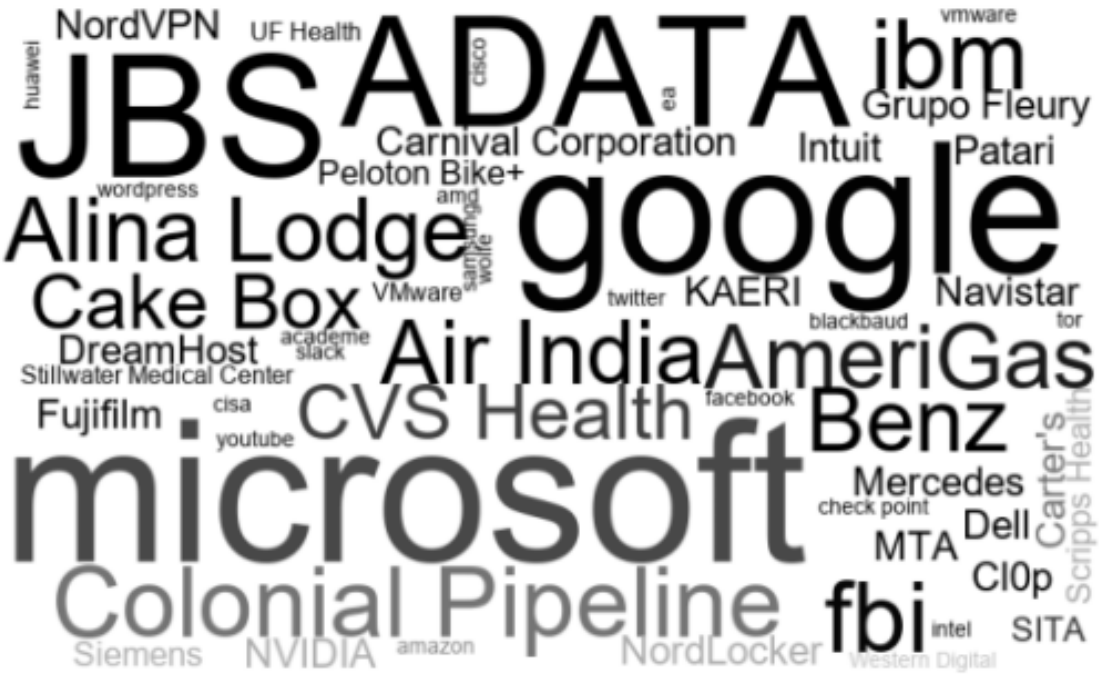
Charts Of Incidents



行业占比情况



事件等级占比情况



涉及厂商词云

攻击组织词云

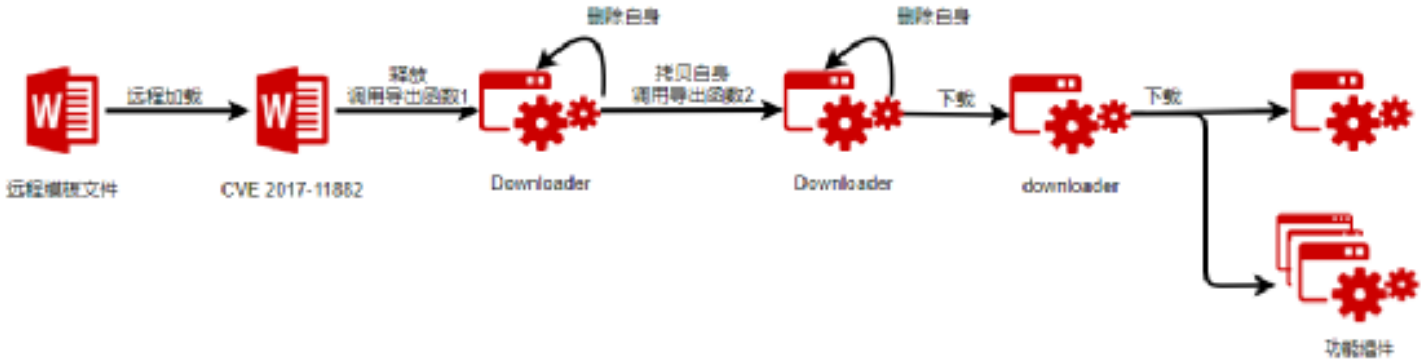
APT事件

Incidents Of Advanced Persistent Threat

肚脑虫（APT-C-35）组织最新攻击框架披露

标签：APT-C-35, C2, APT
链接:https://mp.weixin.qq.com/s/rMgQWQ8uW9foOy60LKtRJw

肚脑虫组织（APT-C-35），又称Donot，是一个针对巴基斯坦、斯里兰卡等印度周边国家政府机构等领域进行网络间谍活动，以窃取敏感信息为主的攻击组织。在对该组织追踪溯源的过程中，360高级威胁研究院发现Donot使用了一系列新型的后门框架，并多次对其程序进行更新。根据这些后门框架使用的组件名，将其命名为“Jaca“框架。
根据360高级威胁研究院的研究发现，近两年Donot在攻击流程上大体保持一致。通过鱼叉邮件的方式向目标用户投递远程模板注入文档或者是恶意宏文档来完成攻击活动的第一步。



PJobRAT：针对印度军事人员的间谍软件

标签：Android, C2, APT
链接：https://mp.weixin.qq.com/s/VTHvmRTeu3dw8HFyusKLqQ

近期，360烽火实验室发现一起主要针对印度军事相关目标的攻击活动，本次攻击活动使用了一种新的Android恶意软件，根据恶意软件包结构将其命名为PJobRAT。
PJobRAT主要伪装成印度婚恋交友和即时通讯软件。通过对同源样本进行分析，360烽火实验室推测本次攻击时间从2021年1月开始，该RAT家族或最早出现于2019年12底，本次攻击活动主要针对具有军事相关背景的印度人员。

启明星辰ADLab | APT34组织最新攻击活动深度分析报告

标签：APT34, C2, APT
链接：https://mp.weixin.qq.com/s/o_EVjBVN2sQ1q7cl4rUXoQ

2021年以来，启明星辰ADLab追踪到多起以军队事务和移动运营商业务为话题的定向攻击活动。攻击者伪装成为军事部门以军队内部事务如海军战舰就绪清单、某军官解雇令为诱饵对目标发起定向攻击并植入木马，同时也常常伪装成为一些国家的重要企业以招聘人员为由攻击目标。启明星辰ADLab通过对攻击目标、入侵技术特点、代码同源性等因素进行比对分析后，确认此批攻击来源于APT34组织。APT34组织2019年的武器库泄露事件中曾暴露出其控制的Exchange服务器的webshell列表，这些列表中包含了十多家被黑客成功渗透过的中国企业和机构。
本文将对APT34的本次攻击活动进行深入的分析和探讨，首先简要介绍该组织的历史活动，然后对其攻击手法，所使用的新的基础设施，以及本次攻击所采用的新技术进行分析，最后对攻击过程中所使用的后门以及相关的技术细节进行深入分析。

瑞星预警：APT组织Lazarus Group对中国发起攻击

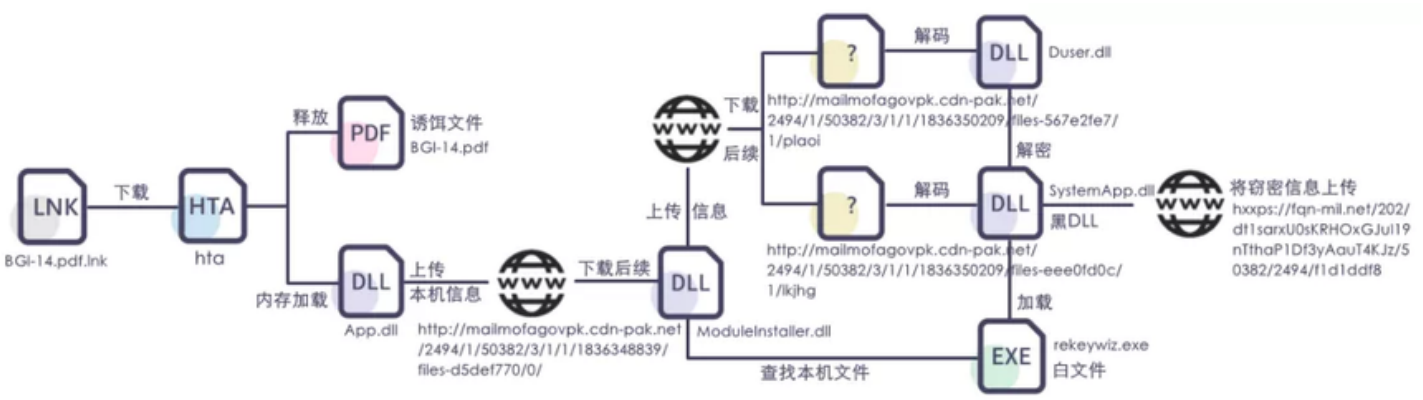
标签: Lazarus, C2, APT
链接: https://mp.weixin.qq.com/s/J1iWJSj3x0NinVrzo_5eNw

近日，瑞星威胁情报中心捕获到一起针对中国政府和企业发起的APT攻击事件，通过分析发现，攻击者利用钓鱼邮件等方式投递名为“安全状态检查.zip”的压缩包文件，其主题为《信息安全技术信息系统安全等级保护实施指南》，以此来诱使中国大量政府部门或企业上钩，一旦中招，电脑将被攻击者远程控制，执行任意代码并盗取重要数据信息。

SideWinder武器库更新：利用外交政策针对巴基斯坦的攻击活动分析

标签: SideWinder, C2, APT
链接: https://mp.weixin.qq.com/s/GrhuLcA_DopQ1V3F1a-N0A

响尾蛇（又称SideWinder）APT组织是疑似具有南亚背景的APT组织，其攻击活动最早可追溯到2012年。主要针对其周边国家政府、军事、能源等领域开展攻击活动，以窃取敏感信息为攻击目的。
今年3月，奇安信威胁情报中心捕获到几例利用相关国家外交政策为诱饵的恶意样本。此类样本伪装成大使馆向巴基斯坦委员会的投资回信、建立港口防疫能力等热点信息开展攻击。一旦受害者执行此类恶意样本，初始LNK文件将从远程服务器下载恶意脚本执行，恶意脚本将释放展示正常的诱饵文档以迷惑受害者，并继续从远程服务器获取第二阶段恶意脚本执行。第二阶段恶意脚本中更新了在受害者计算机上部署相关恶意软件的流程，最后通过白加黑的方式加载最终的远程木马，控制受害者机器，从而窃取敏感信息。
本文将披露响尾蛇APT组织在2021年上半年攻击活动中更新的攻击手法及代码细节如下：
- 二阶段荷载不再使用HTA脚本直接将内存数据解码释放在本地，而是由发送本机信息后的回传数据进行后续下载
- 函数调用不再使用系统API，而是由自定义繁杂的函数名封装所需调用的API
样本执行流程如下图所示：



Kimsuky组织继续使用AppleSeed后门攻击韩国政府

标签：Kimsuky, C2, APT
链接：https://blog.malwarebytes.com/

Kimsuky（又名 Thallium、Black Banshee、Velvet Chollima）是朝鲜背景的APT组织，2012 年以来一直活跃，主要针对韩国的政府实体展开网络间谍活动。
Malwarebytes威胁情报团队持续监控该组织的攻击活动，在本篇报告中给出了Kimsuky组织的受害者、网络钓鱼基础设施和通信基础设施，同时分析了近期Kimsuky用于攻击韩国外交部的AppleSeed后门。

Lazarus近期针对军工等行业的定向攻击活动分析

标签：Lazarus, C2, APT
链接：https://mp.weixin.qq.com/s/MBH8ACSTfC6UGzf2h1BuhA

Lazarus组织为境外大型APT组织，是当前活跃度最高的APT组织之一。该组织实力强劲，其攻击目标涵盖政府、国防、研究中心、金融、能源、航空航天、运输、加密货币等诸多具有高经济价值的行业领域，并且擅长针对不同行业实施精准的社会工程学攻击。
微步情报局近期通过威胁狩猎系统监测到Lazarus组织针对国防军工行业的攻击活动，结合以往该组织针对军工行业的攻击活动，一并分析有如下发现：
- 攻击者在此次攻击活动中冒充德国军工企业“莱茵金属”公司，以“工作要求”为主题向目标投递带有恶意宏的诱饵文档，Lazarus组织经常以目标所在行业头部企业的招聘信息为诱饵进行攻击活动；
- 此外还以韩国军工企业“大宇造船”相关话题为诱饵进行攻击；
- 诱饵文档中的恶意宏利用多阶段组件来执行恶意行为，最终加载执行远控模块，实现对目标主机的远程控制；
- 攻击者将事先入侵的站点作为C2通信服务器，这在Lazarus以往的攻击活动中经常看到；
- 结合该组织以往攻击活动样本分析，从执行流程上看具有高度相似性，但细节有一定程度变化，表明攻击者在持续开发并优化其攻击组件；

Kimsuky APT 组织分发虚假伪造的 KISA 安全程序

标签：Kimsuky, C2, APT
链接：https://cybleinc.com/2021/06/03/kimsuky-apt-group-distributes-fake-security-app-disguised-as-kisa-security-program/?_thumbnail_id=5079

朝鲜APT组织Kimsuky被发现通过恶意电子邮件分发虚假的韩国互联网和安全局 (KISA) 应用程序。移动端恶意软件研究人员在近期的一条[推文](https://twitter.com/m0br3v/status/1399637361697378306)中分享了有关假冒KISA疫苗或伪装成KISA安全程序的虚假Android APP的信息。
当受害者从电子邮件中下载APK安装包并安装程序时，恶意代码就会在受害者不知情的情况下隐蔽执行，并从其设备收集敏感信息。

Operation（अग्नि）Angi：游荡在喜马拉雅山脉的幽灵战象

标签：魔罗杪, C2, APT
链接：https://mp.weixin.qq.com/s/LJjXXHZEFxtbalU8XSXqVw

奇安信威胁情报中心红雨滴安全研究团队多年来持续对南亚次大陆方向的攻击活动进行追踪。对魔罗杪组织均做过大量的分析和总结。上述组织长期针对东亚和南亚地区进行了长达数年的网络间谍攻击活动，主要攻击领域为政府机构、军工企业、核能行业、商贸会议、通信运营商、智库期刊、广播电台、新闻媒体等。
本文内容是对魔罗杪组织在2020年的攻击活动做一个总结，并对南亚地区有争议的组织进行梳理，正本清源。在此过程中奇安信发现了魔罗杪组织使用的新型攻击手法和恶意软件。所涉及的恶意域名和IP均已无法访问。

TUNNELSNAKE攻击活动—通过部署被动后门隐藏C2

标签：C2, APT
链接：http://blog.nsfocus.net/tunnelsnake-apt/

近日，卡巴斯基发布了其监测到的名为TunnelSnake的攻击活动，攻击者的目标主要是东南亚和非洲的外交组织，针对这些目标可以在外部访问到的主机进行攻击，成功部署了Moriya rootkit。由于微软引入了驱动强制签名以及补丁检测机制，rootkit在攻击中很少被使用到，目前大多用在APT攻击活动中。
本篇报告对TunnelSnake活动攻击时部署的Moriya后门进行了分析。

Kimsuky APT组织对韩国国防安全相关部门的定向攻击活动分析

标签：Kimsuky, C2, APT
链接：https://mp.weixin.qq.com/s/SLocYak45PoOwLtMCn0PFg

Kimsuky组织为境外APT组织，该组织长期针对韩国政府、新闻、医疗、金融等机构进行攻击活动，经常以政府相关热点事件为诱饵进行定向攻击，窃取高价值情报是其主要攻击目的之一。
微步情报局近期通过威胁狩猎系统监测到Kimsuky APT组织针对韩国国防安全相关部门的定向攻击活动，分析有如下发现：
- 攻击者以“韩美峰会参考资料”、“韩国国防部招标文件”、“韩国互联网安全局APP”相关主题为诱饵进行定向攻击，其中所投递的诱饵文档为HWP格式，具有明显的针对性；
- 所使用木马包括Windows版本和Android版本；
- 使用的间谍类型RAT组件在旧版本的基础上丰富了间谍功能，包括键盘监控、屏幕监控、文件监控、USB监控等；
- 针对特定类型文档、文件进行窃取，具有明显的间谍属性；
- 攻击者在近半年时间持续对韩国国防安全相关部门进行定向攻击活动；
- 据韩国媒体《朝鲜日报》报道，韩国原子能研究院近期遭到Kimsuky攻击，攻击者利用原子能研究院VPN设备漏洞成功入侵其内网；
- 微步情报局近期监测到具有相同背景的Lazarus APT组织同样在针对军工企业进行定向攻击活动，与Kimsuky的攻击目标产生了一定的重叠，二者疑似是被统一策划进行定向攻击活动；

Ferocious Kitten: 在伊朗进行了 6 年的秘密监视

标签: Ferocious Kitten, C2, APT
链接: https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/

Ferocious Kitten是一个至少自2015年开始活跃的APT组织，似乎主要针对居住在伊朗境内的讲波斯语的人。尽管该组织已经活跃了很长时间，但从未被发现与披露。直到Twitter上的研究人员将诱饵文件上传到了 VirusTotal 才引起安全分析人员的注意。2021年3月13日，奇安信[发布报告](https://ti.qianxin.com/blog/articles/MKLG-Operation:%20Analysis-of-attacks-against-the-%20Middle-East-for-several-years/)对其中一个植入物进行了分析。
卡巴斯基分享了更多有关该组织的攻击发现，并提供了对其使用的其他恶意软件变种的分析。诱饵文档中释放的恶意软件被命名为“MarkiRAT”，具有记录键盘、获取剪贴板内容、文件下载和上传以及在受害机器上执行任意命令的功能。该恶意软件至少可以追溯到2015年，同时也存在其他变种，旨在劫持Telegram和Chrome应用程序从而实现持久化驻留。
该组织使用的一些TTP技术可以使分析人员联想到其他针对类似目标的组织，例如Domestic Kitten和Rampant Kitten。

重点事件回顾

Review Of Incidents

恶意程序事件

医疗保健巨头Grupo Fleury遭到REvil勒索软件攻击

医疗行业

Grupo Fleury是巴西最大的医疗诊断公司，拥有 200 多个服务中心和 10,000 多名员工。该公司每年进行大约 7500 万次临床检查。近期Grupo Fleury遭遇勒索软件攻击，公司将其系统下线后，造成业务运营中断。

Crackonosh病毒开采200万美元门罗币

多个行业

至少自2018年6月以来，一个之前没有记录的Windows恶意软件已经感染了超过22.2万个系统，给其开发者带来了不少于9000个门罗币(200万美元)的非法利润。这种恶意软件被称为“Crackonosh”，它通过非法破解流行软件进行拷贝传播，使得安装在机器上的反病毒程序失效，并安装一个名为xmrig的软件，用于偷偷地利用受感染主机的资源来挖掘门罗币。

数据安全事件

属于CVS Health的数十亿条记录遭遇泄露

卫生行业

安全研究人员发现了一个属于CVS Health的在线数据库，该数据库没有密码保护，也没有防止未经授权进入的身份验证形式。通过对数据库的检查，研究人员发现了超过10亿条与美国医疗和制药巨头有关的记录。该数据库大小为 204GB，包含事件记录和配置数据，以及访客 ID、会话 ID、设备访问信息的生产记录（例如访问公司域的访客使用的是 iPhone 还是 Android 手机），以及COVID-19疫苗和各种CVS产品的相关信息。

奥迪、大众330万客户遭遇数据泄露

制造业

奥迪和大众汽车遭遇数据泄露，影响了330万客户。泄露的数据包括姓名、个人或公司邮寄地址、电子邮件地址或电话号码。在某些情况下，数据还包括有关购买、租赁或查询的车辆的信息，如车辆识别号（VIN）、品牌、型号、年份、颜色和装饰。还有极少数客户的出生日期、社会保障或社会保险号码、账户或贷款号码以及税务识别号码。

Ragnar Locker勒索团队公开ADATA 700G 敏感数据

制造业

由于ADATA没有支付赎金并自行恢复了受影响的系统，Ragnar Locker 勒索软件团伙发布了从台湾内存和存储芯片制造商 ADATA 窃取的超过 700GB 存档数据的下载链接。从档案名称来看，Ragnar Locker 可能从 ADATA 窃取了包含财务信息、保密协议以及其他类型细节的文件。

网络攻击事件

研究人员发现了针对韩国政府的黑客行动

政府机关

一名自2012年以来活跃的朝鲜攻击者一直在幕后策划一场新的间谍活动，目标是与韩国相关的高级政府官员，通过安装Android和Windows后门以收集敏感信息。网络安全公司Malwarebytes追踪这一活动并定位到一名叫Kimsuky的攻击者，其攻击目标包括韩国互联网与安全局（KISA）、外交部、斯里兰卡驻斯里兰卡大使馆大使、国际原子能机构（IAEA）核安全官员、韩国驻香港总领事馆副总干事、国立首尔大学和大信证券。

西部数据NAS设备遭到网络攻击，硬盘遭遇格式化

制造业

西部数据已经确定，该公司的 My Book Live 设备遭到了攻击者的入侵，这种入侵会导致设备被恢复出厂设置，数据也被全部擦除。My Book Live 设备在 2015 年进行了最后的固件更新。

西部数据建议用户断开 My Book Live 设备与互联网的连接，以保护设备上的数据。

其他事件

一次大规模的CDN故障使大部分互联网服务离线

多个行业

2021年6月8日，互联网上的大部分网站都无法访问。包括《卫报》、《金融时报》、《纽约时报》和ZDNet在内的媒体出版物，以及Reddit、Twitch、亚马逊、PayPal和英国政府网站gov.UK在内的网站因设备故障而瘫痪。访问这些网站的访问者会收到一条错误消息：“错误503服务不可用”。这个问题可能与云平台和内容交付网络（CDN）的故障有关。

谷歌Android应用程序中检测到安全漏洞

IT服务业

迄今为止，和 Google 同名的一款 Android 应用程序中存在一个漏洞，该应用程序下载量超过 50 亿次，可能使攻击者能够秘密窃取受害者设备的个人信息。 该漏洞允许恶意应用程序继承谷歌应用程序的权限，这使它几乎完全访问用户的数据，此访问权限包括访问 Google 用户帐户、搜索历史记录、电子邮件、短信、联系人和通话记录，以及麦克风、摄像头和用户位置。 一旦攻击开始，恶意应用程序将被激活，但它是在用户不知情的情况下进行的。

事件时间线

Timeline Of Incidents

2021-06-01
Android恶意软件窃取银行信息
美国：JBS遭受勒索软件攻击背后可能是俄罗斯攻击者

2021-06-02
研究人员发现了针对韩国政府的黑客行动
华为USB LTE加密狗易受权限提升攻击

2021-06-03
FBI将JBS遭受的勒索软件攻击归咎于REvil
马萨诸塞州最大的渡轮服务遭遇勒索软件攻击
俄罗斯黑客利用新的SkinnyBoy恶意软件入侵敏感组织

2021-06-04
CODESYS工业自动化软件中发现10个严重漏洞
攻击者扫描未修补的VMware vCenter服务器，PoC可用
谷歌发现改变芯片内存的新漏洞

2021-06-07
勒索软件警告：针对学校和大学的攻击又一次激增
新的Kubernetes恶意程序通过Windows容器部署后门
美国卡车和军用车辆制造商Navistar数据泄露

2021-06-08
一次大规模的CDN故障使大部分互联网服务离线
深入调查Nefilim勒索软件集团
计算机内存制造商ADATA受到 Ragnar Locker 勒索软件的攻击
谷歌修补了Android RCE的关键漏洞

2021-06-09
西班牙劳动和社会经济部遭网络攻击
未知的恶意软件收集了数十亿的被盗数据

2021-06-10
JBS承认支付了1100万美元的赎金
新型勒索软件针对全球数十家企业
黑客入侵游戏巨头并窃取游戏源代码
餐饮服务供应商Edward Don遭遇勒索软件攻击

2021-06-11
Avaddon勒索软件停止运营并公开解密密钥
麦当劳客户及员工信息遭遇数据泄露

2021-06-12
奥迪、大众330万客户遭遇数据泄露

2021-06-14
REvil勒索软件攻击美国核武器承包商

2021-06-15
美国最大丙烷分销商遭遇数据泄露
天堂勒索软件源代码发布在黑客论坛

2021-06-16
乌克兰逮捕Cl0p勒索软件团伙成员
属于CVS Health的数十亿条记录遭遇泄露
俄克拉荷马州医疗系统被迫关闭

2021-06-17
匿名恶意软件从325万台计算机窃取2600万个登录凭据

2021-06-18
嘉年华电子邮件账户遭遇数据泄露

2021-06-21
据称朝鲜黑客组织是破坏韩国核研究所的幕后黑手
Ragnar Locker勒索团队公开ADATA 700G 敏感数据
Molerats黑客针对中东政府的最新活动
数以百万计的医学图像、患者数据仍通过 PACS 漏洞泄露
勒索软件攻击盗取了生育患者的记录
50% 的错误配置容器在一小时内就会被僵尸网络攻击

2021-06-22
恶意 PyPI 包劫持开发设备以挖掘加密货币
Tor浏览器发现新漏洞
乔治亚州的生育诊所遭到勒索软件攻击
谷歌Android应用程序中检测到安全漏洞
DirtyMoe Botnet在2021上半年中感染了100,000+ Windows系统

2021-06-23
医疗保健巨头Grupo Fleury遭到REvil勒索软件攻击
黑客泄露了巴基斯坦音乐流媒体网站Patari的26万个账户

2021-06-24
Dell SupportAssist漏洞使超过3000万台PC面临风险
VMware修复了严重的身份验证绕过漏洞
南亚和中亚的政府组织和电力公司遭受后门攻击

2021-06-25
Crackonosh病毒从22.2万台被黑客入侵的电脑中开采了200万美元的门罗币
西部数据NAS设备遭到网络攻击，硬盘遭遇格式化

2021-06-26
微软客户支持工具遭受SolarWinds黑客攻击

2021-06-27
Oscorp：新的银行木马出现在Android里

2021-06-28
Wolfe眼科诊所遭勒索软件攻击暴露了50万患者的数据

2021-06-29
微软再次遭遇依赖劫持攻击
LinkedIn 遭遇数据泄露
爱尔兰卫生部门遭勒索软件攻击损失的费用超过6亿美元
SolarWinds攻击造成的损失平均为1200万美元

2021-06-30
全球警方关闭黑客常用的VPN服务

安全建议

Security Advice

网络防护：

- 在网络边界部署安全设备，如防火墙、IDS、邮件网关等
- 做好资产收集整理工作，关闭不必要且有风险的外网端口和服务，及时发现外网问题
- 积极开展外网渗透测试工作，提前发现系统问题
- 模糊验证错误信息，仅返回“验证错误”即可
- 若系统设有初始口令，建议使用强口令，并且在登陆后要求修改
- 建议加大口令强度，对内部计算机、网络服务、个人账号都使用强口令
- 登陆入口增加验证码功能。
- 减少外网资源和不相关的业务，降低被攻击的风险
- 域名解析使用CDN
- 条件允许的情况下，设置主机访问白名单
- 严格做好http报文过滤
- 做好产品自动告警措施
- 做好文件（尤其是新修改的文件）检测
- 文件上传使用白名单限制
- 文件上传目录应避免http能够直接访问
- 文件上传做二次处理，比如重命名、二次渲染等

系统防护：

- 及时对系统及各个服务组件进行版本升级和补丁更新
- 各主机安装EDR产品，及时检测威胁
- 严格做好主机的权限控制
- 包括浏览器、邮件客户端、vpn、远程桌面等在内的个人应用程序，应及时更新到最新版本
- 移动端不安装未知应用程序、不下载未知文件

数据安全：

- 及时备份数据并确保数据安全
- 合理设置服务器端各种文件的访问权限
- 敏感数据建议存放到http无权限访问的目录
- 统一web页面报错信息，避免暴露敏感信息
- 明确每个服务功能的角色访问权限
- 安装网页防篡改软件
- 严格控制数据访问权限
- 及时检查并删除外泄敏感数据
- 发生数据泄漏事件后，及时进行密码更改等相关安全措施
- 数据库数据，尤其是密码等敏感信息需进行加密存储
- 使用Git等同步存储工具时，注意信息的过滤，避免上传敏感文件

安全管理：

- 网段之间进行隔离，避免造成大规模感染
- 主机集成化管理，出现威胁及时断网
- 注重内部员工安全培训
- 如果不慎勒索中招，务必及时隔离受害主机、封禁外链ip域名并及时联系应急人员处理
- 使用VPN等代理服务时，应当谨慎选择代理服务供应商，避免个人敏感信息泄漏
- 对于托管的云服务器(VPS)或者云数据库，务必做好防火墙策略以及身份认证等相关设置
- 强烈建议数据库等服务放置在外网无法访问的位置，若必须放在公网，务必实施严格的访问控制措施
- 不轻信网络消息，不浏览不良网站、不随意打开邮件附件，不随意运行可执行程序
- 受到网络攻击之后，积极进行攻击痕迹、遗留文件信息等证据收集
- 如果允许，暂时关闭攻击影响的相关业务，积极对相关系统进行安全维护和更新，将损失降到最小

- 勒索中招后，应及时断网，并第一时间联系安全部门或公司进行应急处理
- 积极监控内部数据泄漏事件，并及时做相关处理
- 不盲目信任云端文件及链接
- 不盲目安装官方代码仓库的第三方Package
- 不盲目安装未知的浏览器扩展
- 软硬件提供商要提升自我防护能力，保障供应链的安全

恶意程序

MALWARE

前言

2021年6月，全球新增的活跃勒索病毒家族有:Spyro、APISWiper、ChupaCabra、Vice Society、Findnotfile、Red Epsilon，Hive等。其中Red Epsilon家族利用Microsoft Exchange服务器漏洞对网络上的机器进行攻击，在攻击成功后还会在被攻陷设备中部署远程控制木马（Remote Utilities）；采用RaaS运营模式的HimalayA家族，仅需RaaS服务收费200美元便为其成员免费提供加密器，同时该团伙还宣称不会对医疗机构以及非盈利组织发动攻击；Hive家族采用双重勒索模式运营，目前为止该家族已在暗网发布了2个组织的数据。

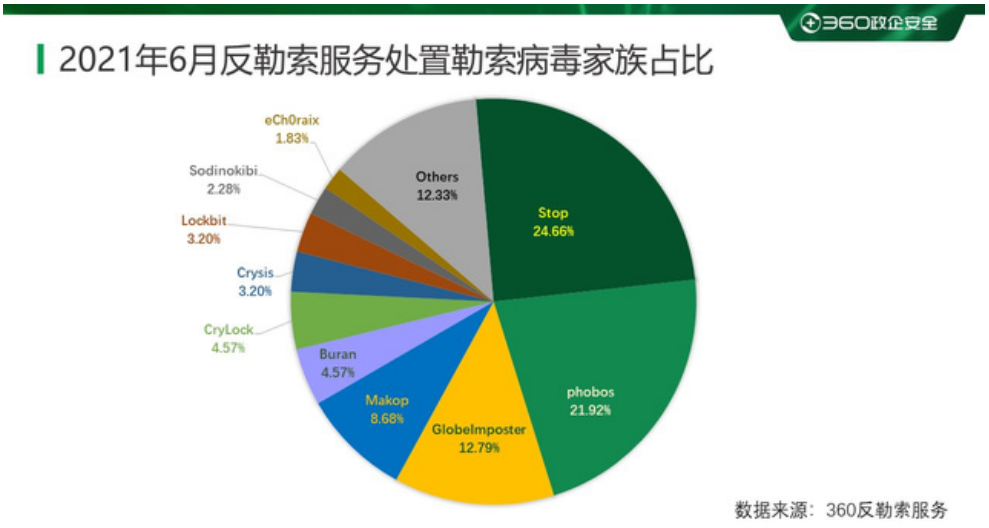
目录预览

勒索病毒态势分析

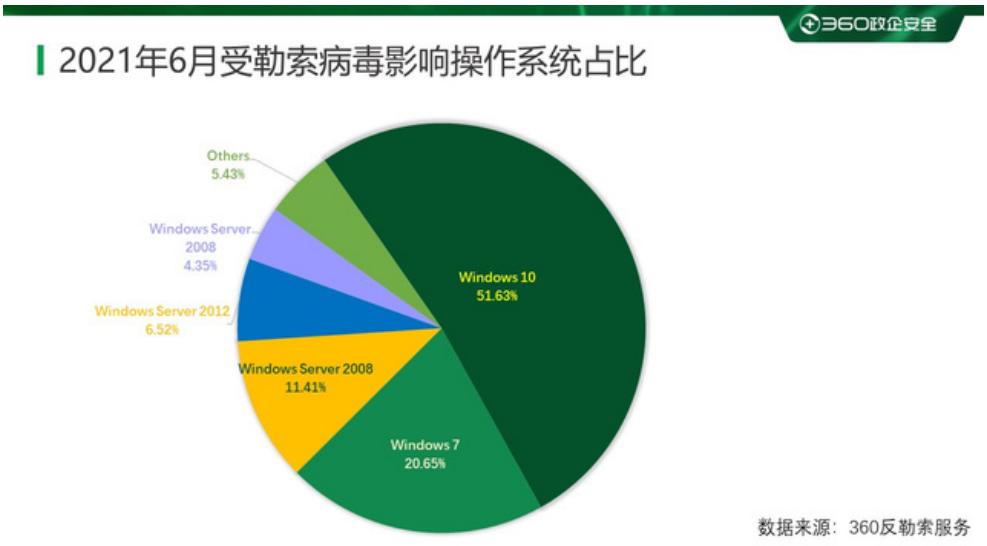
Ransomware Situation Analysis

一、感染数据分析

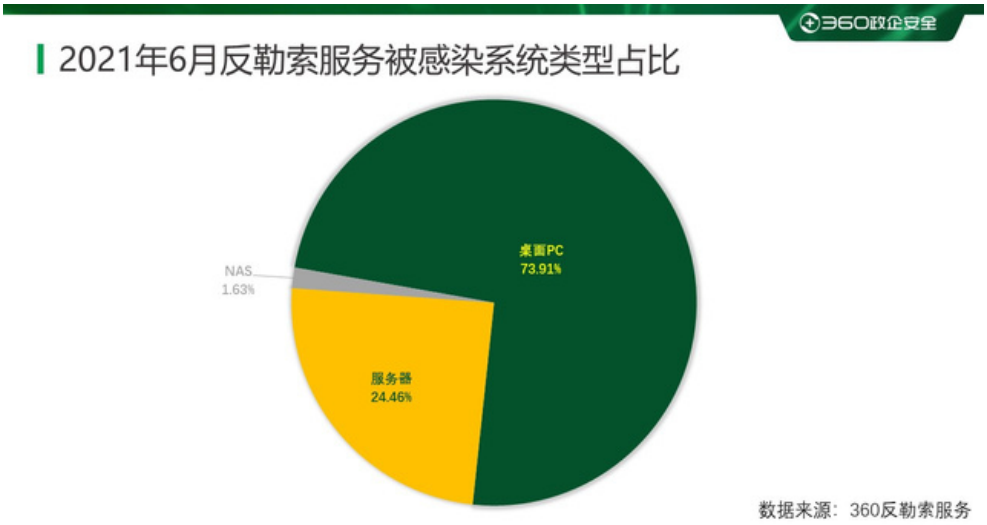
针对本月勒索病毒受害者所中勒索病毒家族进行统计，Stop家族占比24.66%居首位，其次是占比21.92%的phobos，GlobeImposter家族以12.79%位居第三。
本月因下载破解软件/激活工具导致中Stop勒索病毒的受害者仍有上升态势，应尽量避免下载破解软件或者激活工具。



对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows 7、以及Windows Server 2008。



2021年6月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面系统为主，与上月相比无较大波动。本月仍有用户因NAS设备被攻击导致文件被加密，受害者应立即将口令修改为高复杂度密码，若使用的NAS设备是威联通产品，还应及时对HBS多媒体软件进行升级。



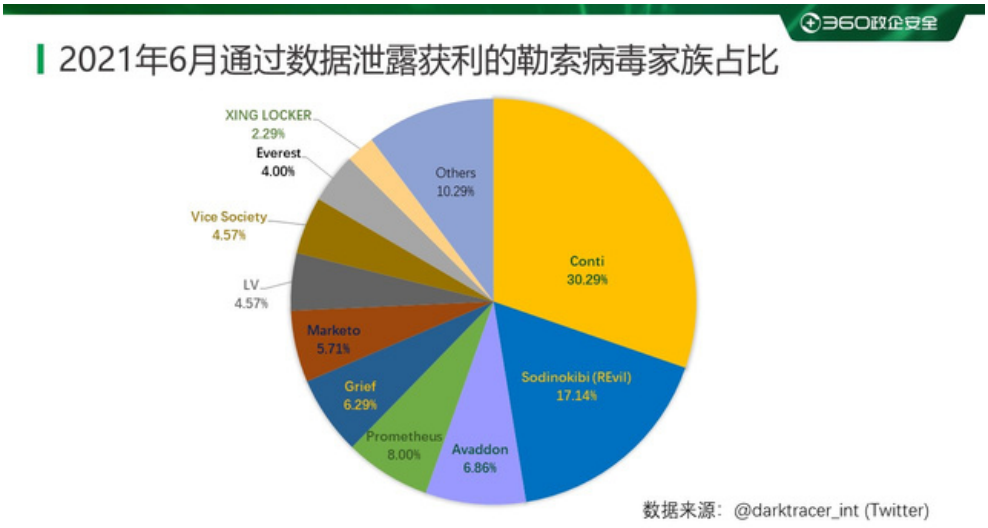
二、黑客信息披露

以下是6月收集到的黑客邮箱信息：

toobar@xmpp.jp	himalayaraas@dnmx.org	emilianazizi@tutanota.com
zucano@tuta.io	admin@yakuzacrypt.com	mammon0503@protonmail.com
mail@zimbabwe.su	MorganBel23@yahoo.com	samsung00700@tutanota.com
alien070@aol.com	schweeps@ctemplar.com	opensecurity@tutanota.com
itteam122@aol.com	MaryaLawra26@gmail.com	sceledruspolyb@olsapp.com
kingkong2@tuta.io	Feisaozhou@vegeta.cyou	daemonescaract@noffea.com
tiberiano@aol.com	prometheushelp@mail.ch	kermy.stapleton@vuzup.com
acuff@tutanota.com	dedisnotdead@gmx.com	equalitytrust@disroot.org
open@mailfence.com	alix1011@mailfence.com	Recovery7070@mailfence.com
Cybell@firemail.cc	iosif.lancmann@mail.ru	solvedproblem@tutanota.com
karusjok@gmail.com	itteam122@techmail.info	recovery_Potes@firemail.de
ForestMem33@aol.com	yourfriendz@secmail.pro	reopening1999@tutanota.com
Mennarl@firemail.cc	BlackSpyro@tutanota.com	helptounlock@protonmail.com
pecunia0318@goat.si	emiliantor@mailfence.com	highlvlservice@ctemplar.com
togerpo@zohomail.eu	CobraLocker@mail2tor.com	lilmoonhack7766@protonmail.ch
manager@mailtemp.ch	kabayaboo@protonmail.com	black.berserks@protonmail.com
RedDot@ctemplar.com	coleman.dec@tutanota.com	theonly_elchapo@protonmail.com
Recovery7070@aol.com	unknownteam@criptext.com	black.berserks@yakuzacrypt.com
zezoxo@libertymail.net	maedeh81@yakuzacrypt.com	perfection@bestkoronavirus.com

de-crypt@foxmail.com	alix1011@yakuzacrypt.com	Decryptor_Payment@scryptmail.com
maedeh81@firemail.cc	devos_devos@tutanota.com	kermy.stapleton@wantrepreneur.ca
gener888@tutanota.com	lockPerfection@gmail.com	Email_Decryptor_Payment@scryptmail.com
equalitytrust@tuta.io	BlackSpyro@mailfence.com	yourdata@RecoveryGroup.at
black_private@tuta.io		

当前，通过双重勒索模式获利的勒索病毒家族越来越多，勒索病毒所带来的数据泄露的风险也越来越大。以下是本月通过数据泄露获利的勒索病毒家族占比，该数据仅为未能第一时间缴纳赎金或拒缴纳赎金部分（因为第一时间联系并支付赎金的企业或个人不会在暗网中公布，因此无这部分数据）。



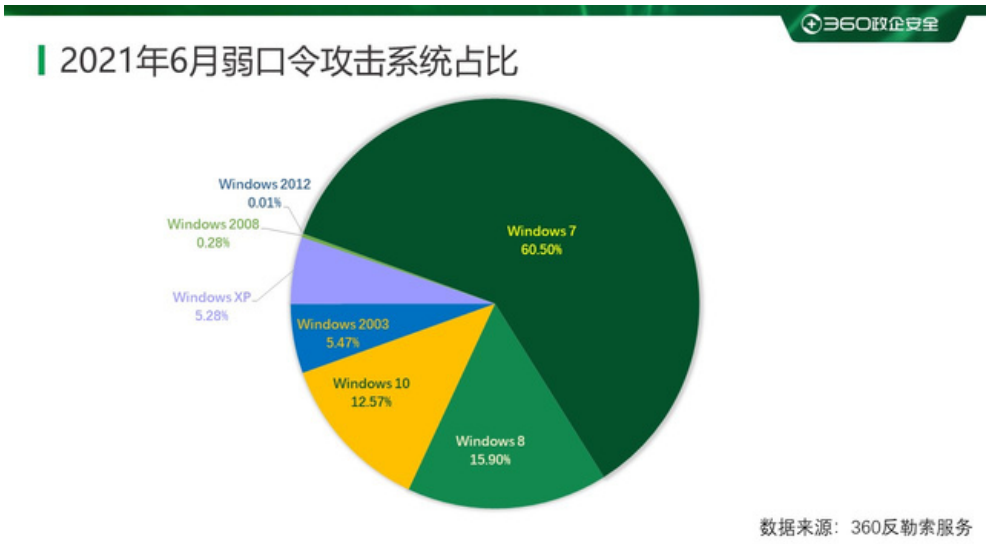
以下是本月被双重勒索病毒家族攻击的企业或个人。若未发现被数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄露准备，采取补救措施。

USI	beckshoes.com	Au Forum Du Batiment SAS
Sjk	ADG SARDA SRL	Windmill Health Products
SOL	A&A MECHANICAL	Performance Award Center
Xefi	Alltech France	Moore Stephens Cape Town
X-FAB	TOYO TANSO USA	Transform SR Brands, LLC
Labet	Thomas Westcott	National Louis University
ADATA	PLURIPHARMA SRL	Concept Building Services
Rolle	TPI Corporation	grupodiagnosticoaries.com
FILGO	The Brock Group	Universal Assistance S.A.
Ascenz	Sunsations Inc.	Macpherson Kelley Lawyers
Bhavna	BRANGEON Groupe	Feedback Technology Corp.

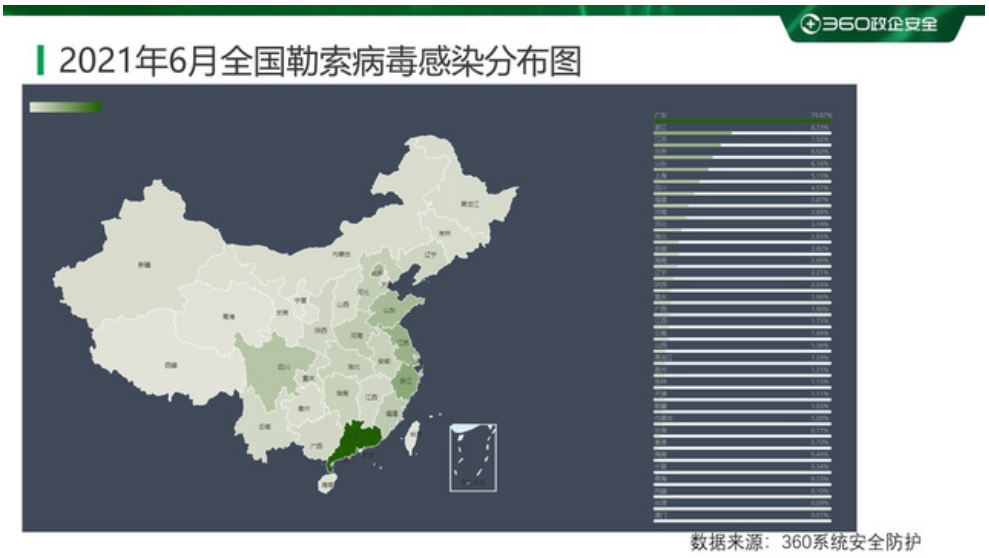
Hasgoe	Uniware Systems	Positive Promotions, Inc.
Elmich	Maître Prunille	CRYSTAL TRAVEL RETAIL S.L.
Aspire	Otto Instrument	TIMPANOGOS HARLEY-DAVIDSON
JEALSA	Homewood Health	Naz Financial Services Inc
Xoriant	Service Gel Srl	BERMAN SOBIN GROSS & DARBY
Willson	Sleep Outfitters	Buchanan Hauling & Rigging
Strongco	Birmingham Barons	ESD Dienstleistungs Gruppe
eCapital	Contrast Lighting	Malcolm C Foy & Co Limited
Voltalia	Cerfrance Côtes d	Southern Eagle Distributing
Navistar	demarnefreres.com	GROUPE CONFIANCE IMMOBILIER
AQUALUNG	Agency Matrix LLC	Clover Park School District
Tetra Law	PM Law Solicitors	Agencia de Aduana Juan León
Image one	French Connection	https://www.vedderprice.com/
Proponent	Blue Yonder Group	Aero-Space Computer Supplies
FNA GROUP	KSS ARCHITECTS LLP	Grúas & Equipos Cruz del Sur
Megaforce	Scott Felder Homes	Lareau Courtiers d'assurances
Lamaziere	JAMAC FROZEN FOODS	A-1 Machine Manufacturing Inc
segepo.fr	County of St Clair	Talma Servicios Aeroportuarios
Sincor-SP	Woodruff Institute	Grupo La Moderna, S.A. de C.V.
Tendriade	wbseedlings.com.au	BridgePoint Financial Services
I********	Factoring Baninter	The Waterloo Networking Company
HAAI GmbH	Alliance COAL, LLC	Langs Building Supplies Pty Ltd
Xpressdocs	Epsilon Hydraulique	Priority Building Services, LLC
Dynamic NC	LENAJA DISTRIBUTION	Greenwood Fabricating & Plating
KOMPAN A/S	Ingram Marine Group	Quad State Gauging & Measurement
DAVACO Inc	Whittlesey & Hadley	Southwest Recovery Services, LLC
Innovairre	atworksprofessional	ASSURANCES ET COURTAGES LYONNAIS
Istaff.com	ENE TECHNOLOGY, Inc	Warren Vicksburg School District
Stride Tool	INDUSTRIAS VIDECA SA	American Cotton Coop Association
Cambium Inc	Mechdyne Corporation	Sea Mar Community Health Centers
Altus Group	Dicky Smith & Co Inc	Communications Solutions Company
adartco.com	Solil Management, LLC	Nickerson Insurance Services, Inc
SMPDYNAMICS	Oritani - Valley Bank	McNamara & Thiel Insurance Agency
areteir.com	University of Corboda	Groupe Traon Industrie Development
Canad Inns.	Forefront Dermatology	Engineered Specialty Products, Inc
Primo Water	Oz Architecture, Inc.	WestCongress Insurance Services LLC
Always Group	crownlaboratories.com	Al Imtiaz Investment Company - K.S.C
Chilli Beans	M&J Evans Construction	Lancaster Independent School District
Grupo Fleury	VALLEY TRUCK & TRACTOR	Law Offices of Michael B. Brehne, P.A
Cormetech Inc	Temmel Logistik Center	Kawasaki Kisen Kaisha, Ltd. ("K" LINE)
Estendo S.p.A	King's Seafood Company	Whitehouse Independent School District
Sandlin Homes	Perfume Worldwide Inc.	Trasporti Internazionali Transmec s.p.a.
La Innovacion	Vogel Heating & Cooling	Nissin International Transport U.S.A., Inc.
Groupe ISERBA	Cerfrance Côtes d'Armor	Rehabilitation Support Services, Inc. (RSS)
City of Tulsa	Master Publicidade Ltda	The Smith & Wollensky Restaurant Group, Inc.
Goetze Dental	Arnoff Moving & Storage	University Medical Center of Southern Nevada
Fischer Homes	Asfaltproductienijmegen	Grupo Herdez, S.A.B. de C.V. Holding Companies
Refuah Health		

三、系统安全防护数据分析

通过将2021年5月与6月的数据进行对比，本月各个系统占比变化均不大，位居前三的系统仍是Windows 7、Windows 8和Windows 10。



以下是对2021年6月被攻击系统所属地域采样制作的分部图，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



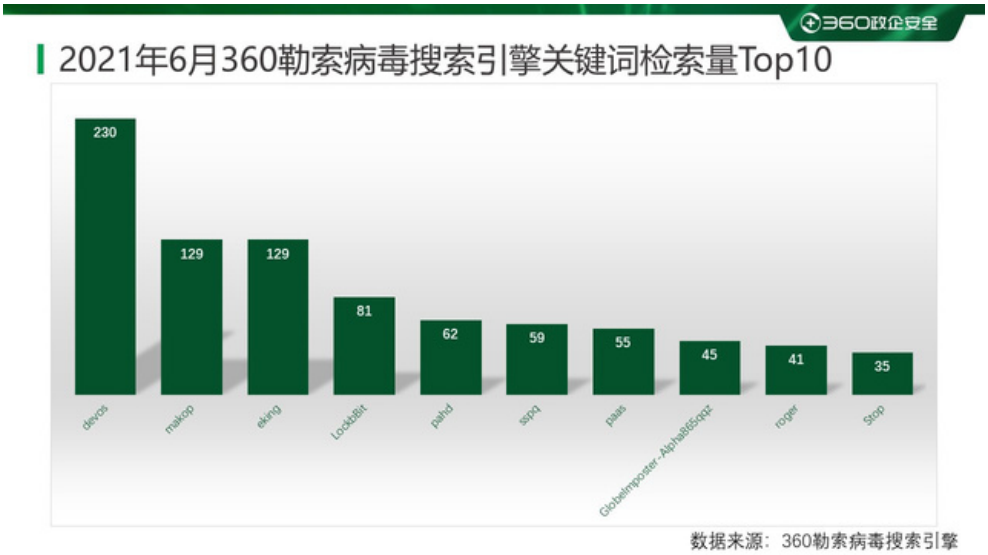
通过观察2021年6月弱口令攻击态势发现，RDP和MYSQL弱口令攻击整体无较大波动。MSSQL弱口令攻击虽然在6月一直呈现上升趋势，这和本月发现多个勒索病毒家族利用MSSQL弱口令远程投毒有一定关系,其中GlobeImposter家族已是多次发下利用该方式进行投毒，本月还发现phobos、CryLock勒索病毒家族也将该方式作为传播渠道之一。

数据来源：360系统安全防护

四、勒索病毒关键词

- devos：该后缀有三种情况，均因被加密文件后缀会被修改为devos而成为关键词。但月活跃的是phobos勒索病毒家族，该家族的主要传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
- Makop：该后缀有两种情况，均因被加密文件后缀会被修改为makop而成为关键词:
- 属于Makop勒索病毒家族，该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
- 属于Cryptojoker勒索病毒家族，通过“匿隐”进行传播。
- eking：属于phobos勒索病毒家族，由于被加密文件后缀会被修改为eking而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。

- Lockbit：Lckbit勒索病毒家族，由于被加密文件后缀会被修改为lockbit而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。
- pahd：属于Stop勒索病毒家族，由于被加密文件后缀会被修改为paha而成为关键词。该家族主要的传播方式为：伪装成破解软件或者激活工具进行传播。
- sspq：同pahd。
- paas：同pahd。
- GlobeImposter-Alpha865qqz：属于GlobeImposter勒索病毒家族，由于被加密文件后缀会被修改为GlobeImposter-Alpha865qqz而成为关键词。该家族的传播渠道主要有两个，第一个是通过暴力破解获取到远程桌面后手动投毒，第二个是获取到mssql数据库密码后，通过数据库向用户机器投毒。
- roger:同eking。
- Stop:属于Stop勒索病毒家族，该家族主要的传播方式为：伪装成破解软件或者激活工具进行传播。



数据来源：360勒索病毒搜索引擎

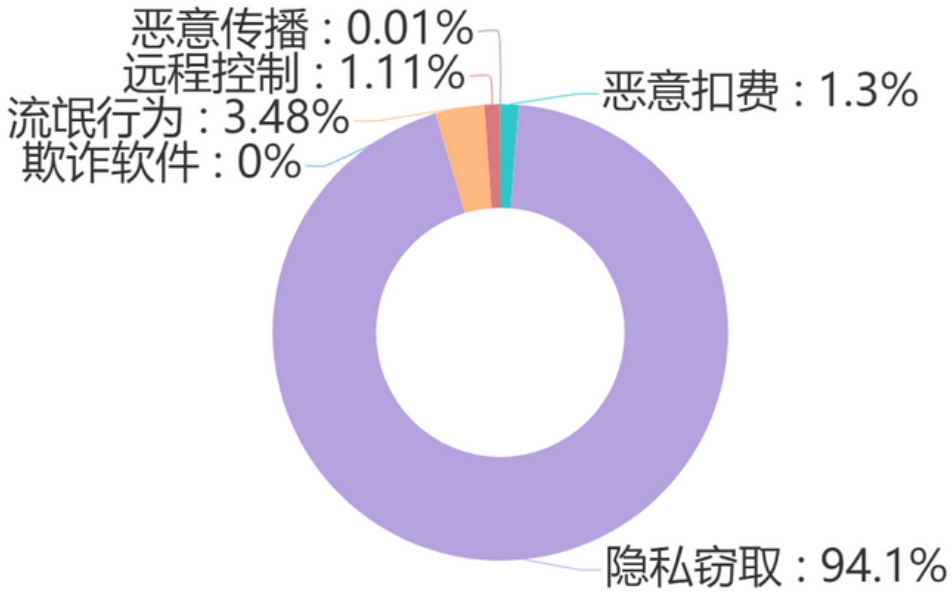
五、解密大师

从解密大师本月解密数据看，解密量最大的是GandCrab，其次是CryptoJoker。使用解密大师解密文件的用户数量最高的是被Crysis家族加密的设备，其次是被CryptoJoker家族加密的设备。

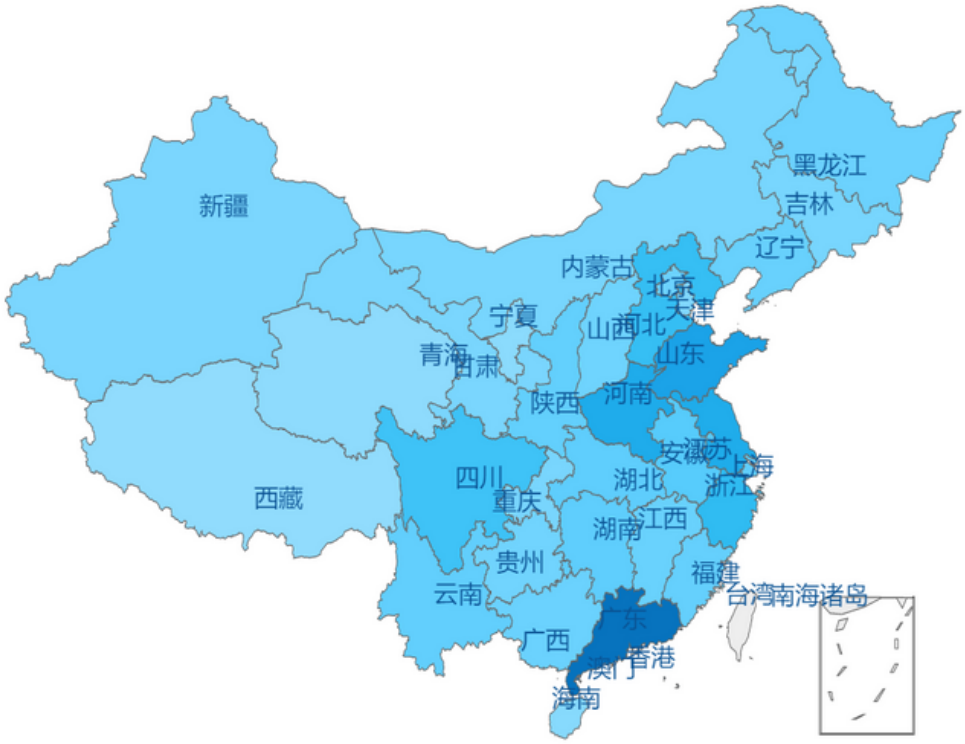
数据来源：反勒索服务统计数据

移动安全数据分析

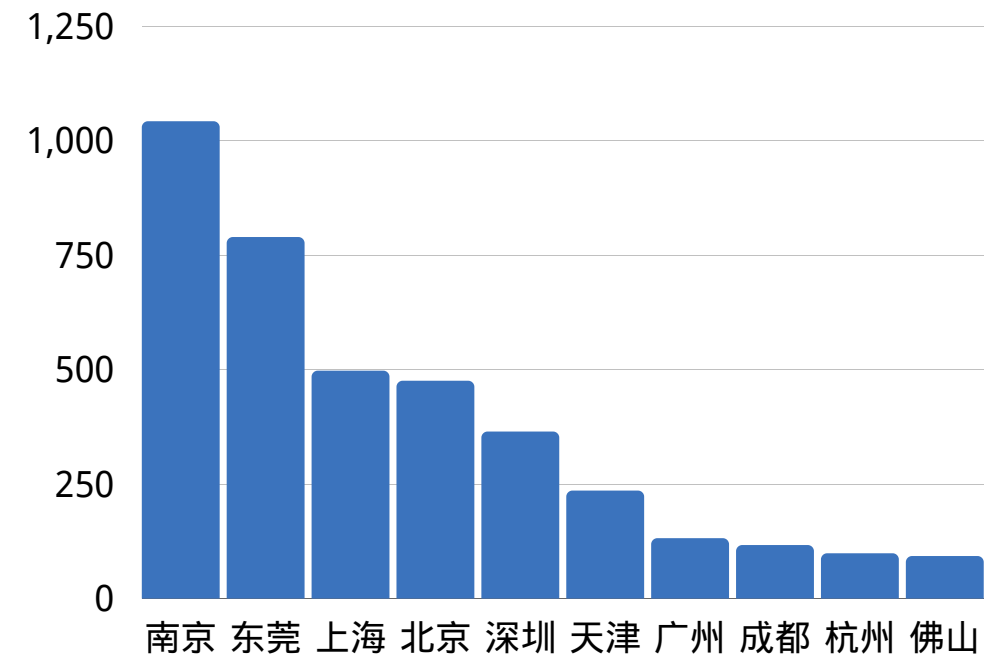
Mobile Security Data Analysis



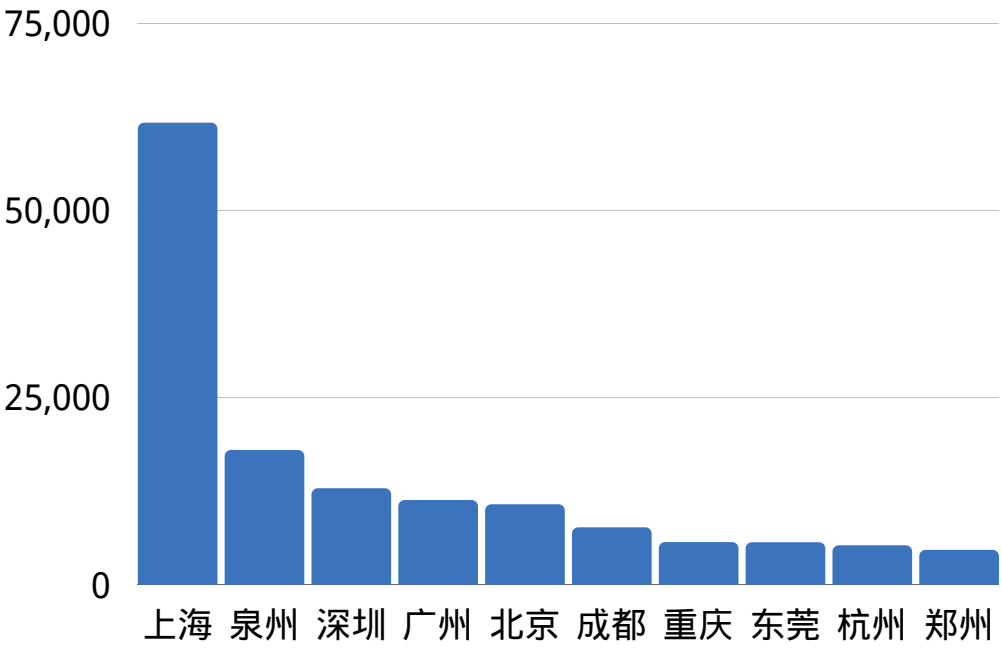
数据总览



拦截量整体情况



欺诈软件拦截量前10城市



隐私窃取拦截量前10城市

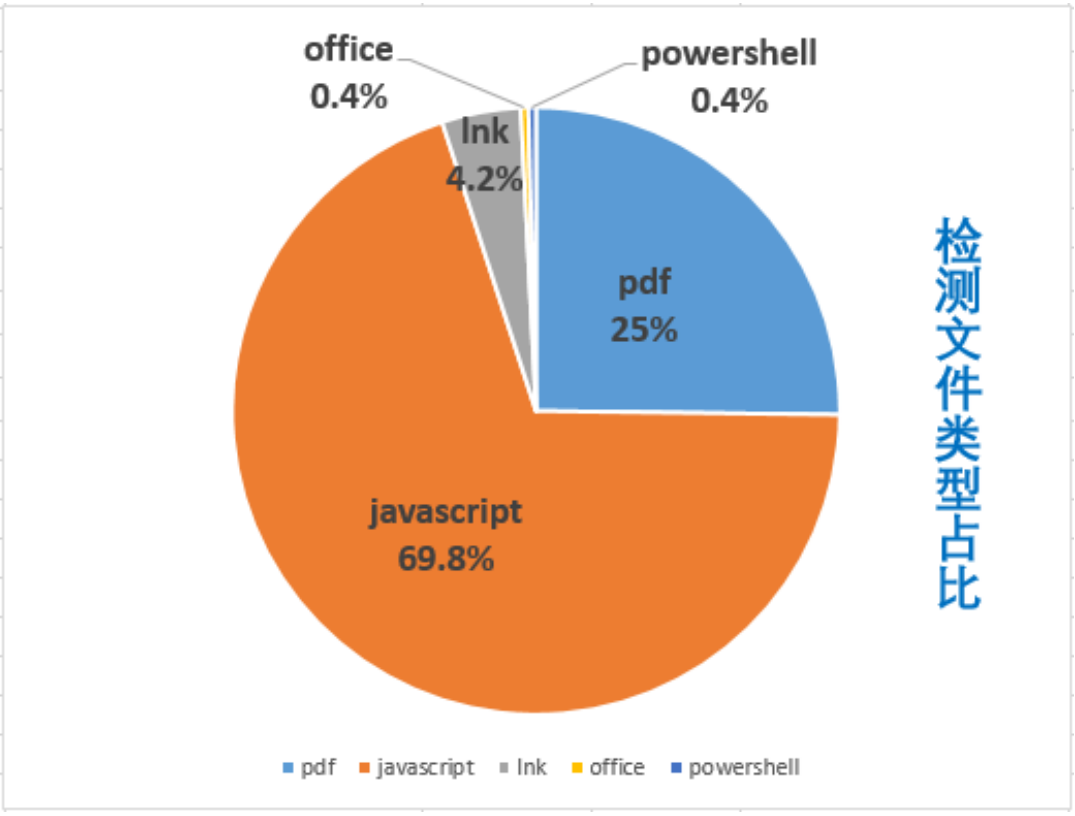
样本分析检测

White List Analysis

一、6月份非PE样本VT检出TOP比例

360QEX引擎专门用于查杀非PE恶意文件，能够精准识别并查杀多种文件类型的恶意文件。以下为VT（VirusTotal）样本监测的检出情况，主要选取流行的几种文件类型的恶意文件进行统计，用于观察恶意非PE文件的传播趋势。表格中按检出数从高到低列出每种恶意文件的检出占比和说明，饼图则显示了检出恶意文件的文件类型占比情况，从以下数据能够看出本月比较流行的恶意文件类型仍为JavaScript和PDF。

检出名	文件类型	占比	检出说明
ex_virus.pdf.phisher.*	pdf	25.20%	pdf钓鱼
ex_virus.js.iframeDownloader.a	javascript	13.80%	js框架下载者
ex_virus.js.faceliker.a	javascript	9.30%	facebook刷赞木马
ex_virus.js.gnaeus.a	javascript	9.10%	gnaeus家族浏览器劫持
ex_virus.js.brocoiner.a	javascript	6.40%	CoinHive挖矿
trojan.js.likejack.a	javascript	5.90%	刷赞木马
ex_virus.js.miner.a	javascript	5.20%	js挖矿
ex_virus.js.hidelink.a	javascript	5.00%	恶意隐藏链接
ex_virus.js.fakejquery.*	javascript	4.50%	仿冒jquery恶意链接
ex_virus.lnk.joke.a	lnk	3.20%	lnk恶作剧
js.iframe.packed.b	javascript	3.00%	js框架混淆
ex_virus.js.evalobfs.a	javascript	2.40%	js执行混淆重定向代码
ex_virus.js.iframe.*	javascript	2.30%	js框架劫持
ex_virus.js.kryptik.*	javascript	1.90%	kryptik家族
virus.lnk.vbsworm.b	lnk	1.00%	lnk蠕虫链接
ex_virus.js.redirector.a	javascript	0.50%	js重定向劫持
macro.ole.jork.ba	office	0.40%	office宏恶意代码
ex_virus.powershell.bypassamsi.a	powershell	0.40%	bypass amsi防护
ex_virus.js.mousefollower.b	javascript	0.40%	facebook刷赞木马
ex_virus.js.agent.e	javascript	0.30%	js恶意插入


office
0.4%
powershell
0.4%
lnk
4.2%
pdf
25%
javascript
69.8%
检测文件类型占比
pdf
javascript
lnk
office
powershell

安全建议

Security Advise

面对严峻的勒索病毒威胁态势，360安全大脑分别为个人用户和企业用户给出有针对性的安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索病毒感染。

一、对于个人用户：

（一）养成良好安全习惯

1. 电脑应当安装具有高级威胁防护能力和主动防御功能的安全软件，不随意退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。
2. 可使用安全软件的漏洞修复功能，第一时间为操作系统、浏览器和常用软件打好补丁，以免病毒利用漏洞入侵电脑。
3. 尽量使用安全浏览器，减少遭遇挂马攻击、钓鱼网站的风险。
4. 重要文档、数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。
5. 电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有8位，不使用弱口令，以防攻击者破解。

（二）减少危险的上网操作

1. 不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。
2. 不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接。也不要轻易打开扩展名为js 、vbs、wsf、bat、cmd、ps1等脚本文件和exe、scr、com等可执行程序，对于陌生人发来的压缩文件包，更应提高警惕，先使用安全软件进行检查后再打开。
3. 电脑连接移动存储设备（如U盘、移动硬盘等），应首先使用安全软件检测其安全性。
4. 对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏。

(三) 采取及时的补救措施

1. 安装360安全卫士并开启反勒索服务，一旦电脑被勒索软件感染，可以通过360反勒索服务寻求帮助，以尽可能的减小自身损失。

二、对于企业用户：

(一) 企业安全规划建议

对企业信息系统的保护，是一项系统化工程，在企业信息化建设初期就应该加以考虑，建设过程中严格落实，防御勒索病毒也并非难事。对企业网络的安全建设，我们给出下面几方面的建议。

1.安全规划

- 网络架构，业务、数据、服务分离，不同部门与区域之间通过VLAN和子网分离，减少因为单点沦陷造成大范围的网络受到攻击的几率。
- 内外网隔离，合理设置DMZ区域，对外提供服务的设备要做严格管控。减少企业被外部攻击的暴露面。
- 安全设备部署，在企业终端和网络关键节点部署安全设备，并日常排查设备告警情况。
- 权限控制，包括业务流程权限与人员账户权限都应该做好控制，如控制共享网络权限，原则上以最小权限提供服务。降低因为单个账户沦陷而造成更大范围影响的风险。
- 数据备份保护，对关键数据和业务系统做备份，如离线备份、异地备份、云备份等，避免因为数据丢失、被加密等造成业务停摆，甚至被迫向攻击者妥协。

2.安全管理

- 账户口令管理，严格执行账户口令安全管理，重点排查弱口令问题，口令长期不更新问题，账户口令共用问题，内置、默认账户问题。
- 补丁与漏洞扫描，了解企业数字资产情况，将补丁管理做为日常安全维护项目，关注补丁发布情况，及时更新系统、应用、硬件产品安全补丁。定期执行漏洞扫描，发现设备中存在的安全问题。
- 权限管控，定期检查账户情况，尤其是新增账户。排查账户权限，及时停用非必要权限，对新增账户应有足够警惕，做好登记管理。
- 内网强化，进行内网主机加固，定期排查未正确进行安全设置、未正确安装安全软件设备，关闭设备中的非必要服务，提升内网设备安全性。

3.人员管理

- 人员培训，对员工进行安全教育，培养员工安全意识，如识别钓鱼邮件、钓鱼页面等。
- 行为规范，制定工作行为规范，指导员工如何正常处理数据，发布信息，做好个人安全保障。如避免员工将公司网络部署、服务器设置发布到互联网之中。

(二) 发现遭受勒索病毒攻击后的处理流程

- 发现中毒机器应立即关闭其网络和该计算机。关闭网络能阻止勒索病毒在内网横向传播，关闭计算机能及时阻止勒索病毒继续加密文件。
- 联系安全厂商，对内部网络进行排查处理。
- 公司内部所有机器口令均应更换，因为无法确定黑客掌握了多少内部机器的口令。

(三) 遭受勒索病毒攻击后的防护措施

- 联系安全厂商，对内部网络进行排查处理。
- 登录口令要有足够的长度和复杂性，并定期更换登录口令。
- 重要资料的共享文件夹应设置访问权限控制，并进行定期备份。
- 定期检测系统和软件中的安全漏洞，及时打上补丁。
  - 是否有新增账户。
  - Guest是否被启用。
  - Windows系统日志是否存在异常。
  - 杀毒软件是否存在异常拦截情况。
- 登录口令要有足够的长度和复杂性，并定期更换登录口令。
- 重要资料的共享文件夹应设置访问权限控制，并进行定期备份。
- 定期检测系统和软件中的安全漏洞，及时打上补丁。

三、不建议支付赎金：

最后——无论是个人用户还是企业用户，都不建议支付赎金！

支付赎金不仅变相鼓励了勒索攻击行为，而且解密的过程还可能会带来新的安全风险。可以尝试通过备份、数据恢复、数据修复等手段挽回部分损失。比如：部分勒索病毒只加密文件头部数据，对于某些类型的文件（如数据库文件），可以尝试通过数据修复手段来修复被加密文件。如果不得不支付赎金的话，可以尝试和黑客协商来降低赎金价格，同时在协商过程中要避免暴露自己真实身份信息和紧急程度，以免黑客漫天要价。若对方窃取了重要数据并以此为要挟进行勒索，则应立即采取补救措施——修补安全漏洞并调整相关业务，尽可能将数据泄露造成的损失降到最低。

网络安全月报

2021.06

感谢阅读

360CERT
微信公众号：三六零cert
官网链接：https://cert.360.cn
联系我们：g-cert-report@360.cn

月报反馈

报告订阅

微信公众号