总第5期

2021年8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

CVE-2021-26084:Confluence OGNL 注入漏洞
CVE-2021-36958: Windows Print Spooler打印机漏洞
CVE-2021-20090:数百万个路由器中的严重漏洞
APT29—觊觎全球情报的国家级黑客组织
Liquid货币交易所遭受黑客攻击，损失超过 9000 万美元
IT咨询巨头埃森哲遭遇Lockbit勒索软件攻击
3800 万条记录因 Microsoft 配置错误而暴露
黑客出售超过 130 万俄罗斯人的护照

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8月，360CERT共收录55个漏洞，其中严重22个，高危18个，中危13个,低危2个。主要漏洞类型包含代码执行、内存越界漏洞、访问控制不当、命令注入、服务器端请求伪造等。涉及的厂商主要是Windows、VMware、Atlassian、Apple、Apache、IBM、Google等。

二、安全事件

本月收录安全事件213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、Cisco、华为、FBI、WordPress、Apple、Twitter等。涉及的行业主要包含IT服务业、制造业、金融业、政府机关及社会组织、批发零售业、医疗行业、交通运输业等。

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8月，全球新增的活跃勒索病毒家族有:LockFile、MBC、Karma、Malki、GetYourFilesBack、Salma、AllDataStolen、GoodMorning等勒索软件。其中LockFile严格意义上来说是2021年7月新增，但在7月仅发现一个受害者，从8月20日开始已出现10多个受害者；

Karma是本月新增的双重勒索软件；MBC在本月成功攻击伊朗伊斯兰共和国铁路系统，并拥有自己的数据泄露网站，但尚未泄露受害者数据。

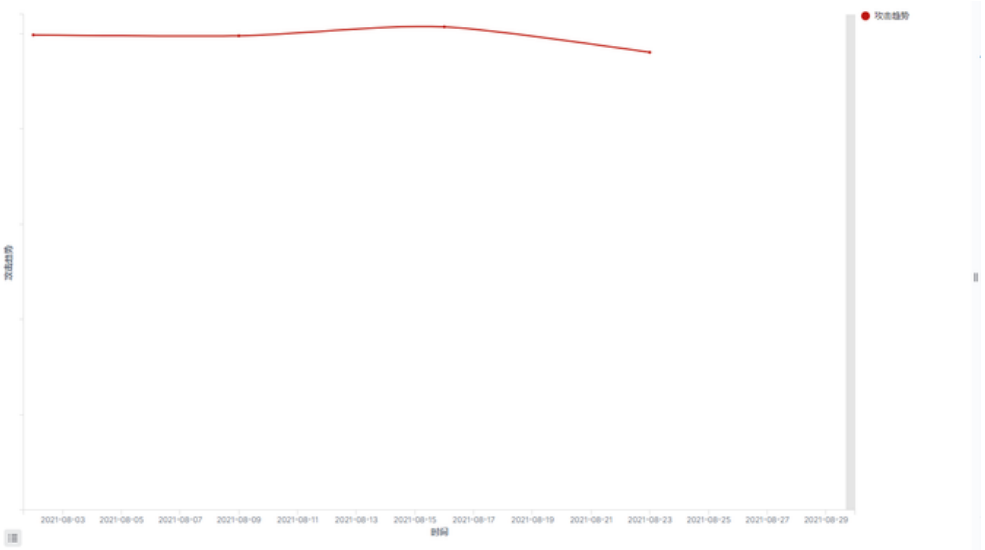
通过隐私窃取拦截量TOP10来看，广东、上海、福建这三个省份移动端隐私窃取数量占据前列，基本上可以体现人口越集中、经济越发达、移动设备使用数量越多的省份，软件恶意行为更加猖獗、恶意软件存活比例越大。

本月攻击态势

Attack situation analysis

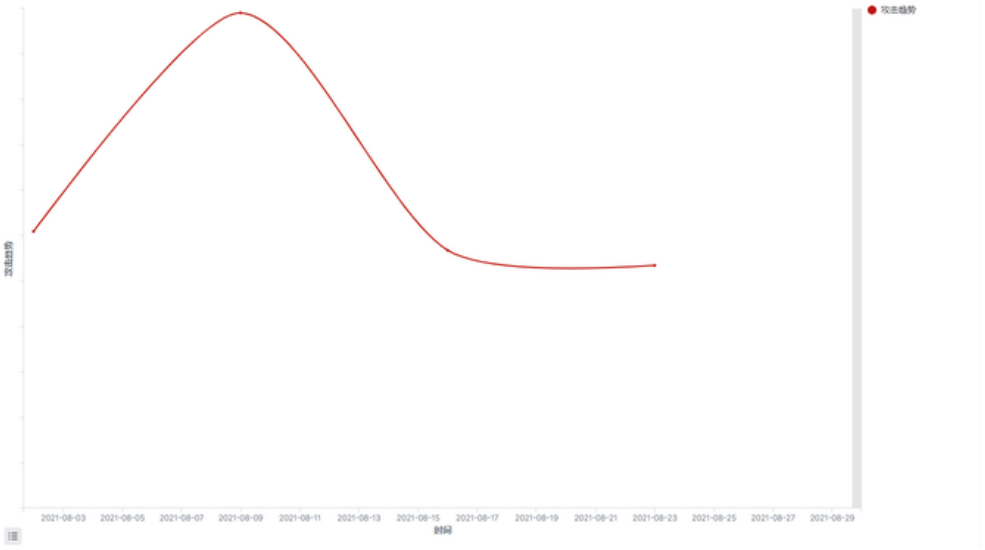
一、僵尸网络攻击

8月份僵尸网络总体攻击趋势非常平稳，几乎未见浮动。



8月份僵尸网络攻击趋势

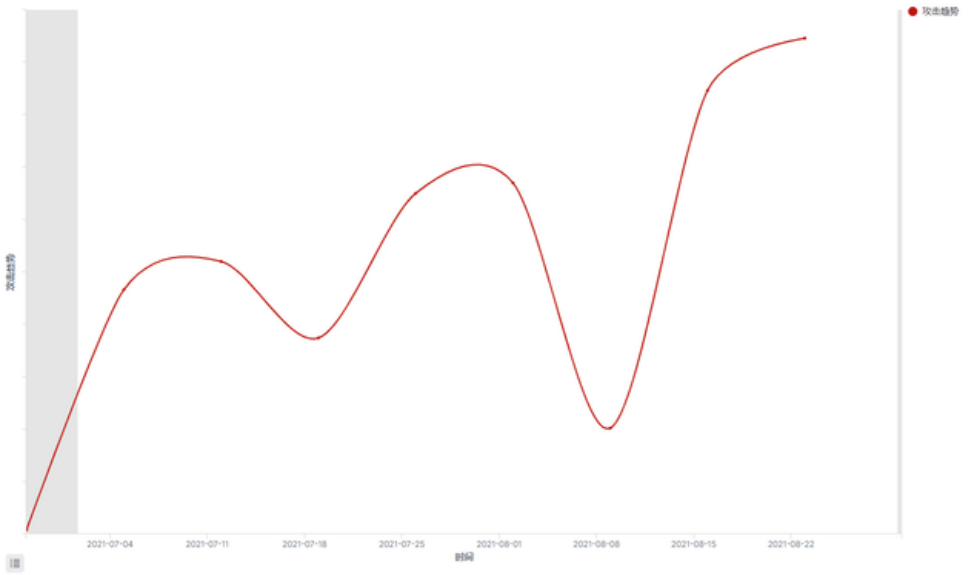
目前Windows平台活跃的大型僵尸网络在8月份均未进行较大更新。唯一在8月有一定波动的成规模僵尸网络是来自“8220”团伙的挖矿僵尸网络，该僵尸网络在8月上旬对互联网中的Weblogic应用发起一波攻击，在受害机器中植入挖矿木马和僵尸程序，之后其攻击趋势就恢复平稳。



8月份“8220”团伙控制的僵尸网络攻击趋势

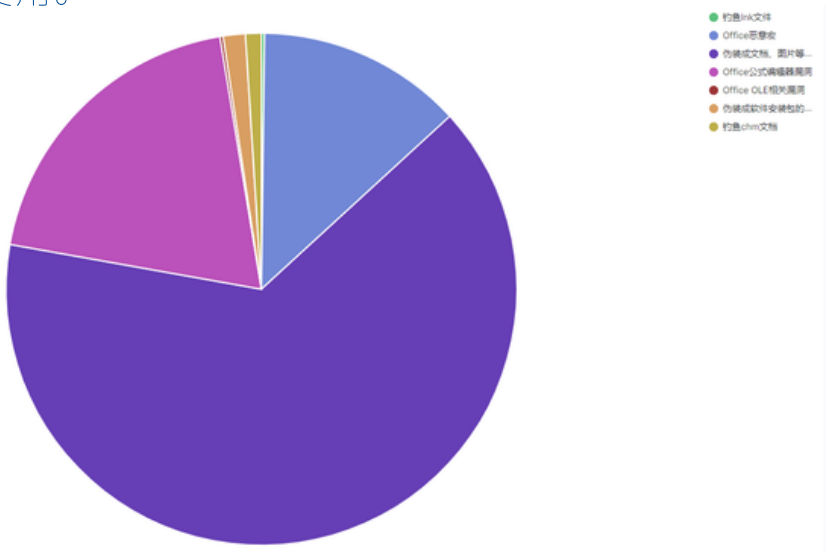
二、钓鱼邮件攻击

本月钓鱼邮件攻击趋势相比较7月份有所增长，原因在于本月银行木马攻击相比7月份要活跃得多。自6月份起，银行木马越发活跃，连续两个月呈现上升趋势。



7、8月份钓鱼邮件攻击趋势

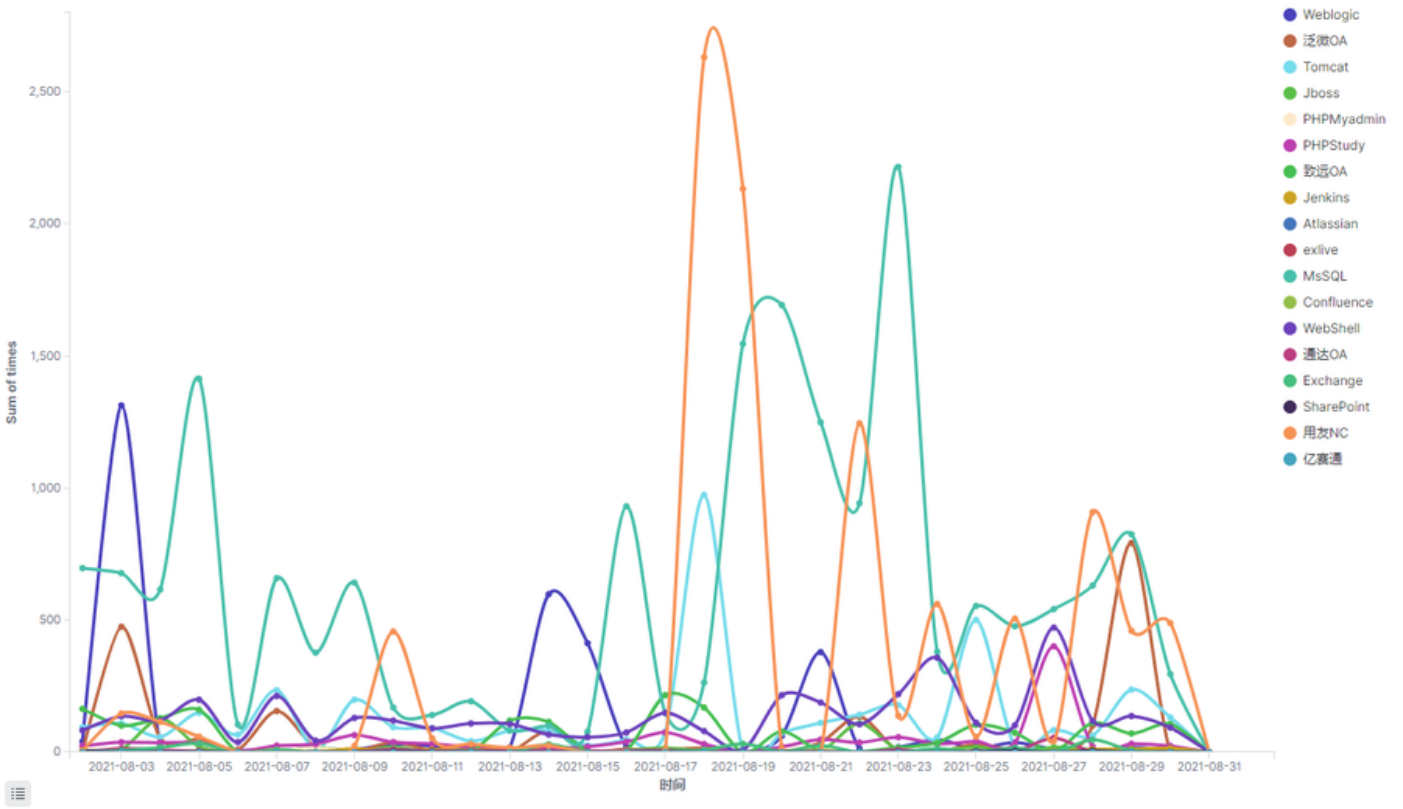
在钓鱼方式分布上，伪装成文档、图片的可执行文件依然是攻击者最青睐的攻击方式，在银行木马攻击以及针对性钓鱼攻击中使用颇多，此外Office公式编辑器漏洞以及Office恶意宏也在以投递银行木马为目的的钓鱼攻击中被广泛使用。



8月份钓鱼攻击方式分布

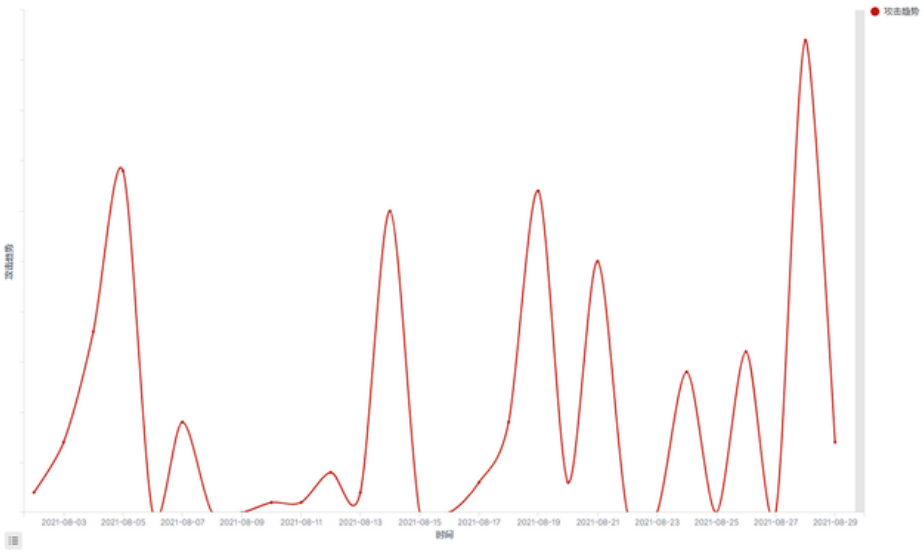
三、针对Web应用和数据库的攻击

8月针对Web应用和数据库的攻击中，针对用友OA平台的攻击最为普遍，有多个不同黑客团伙在不同时间段对互联网中的用友OA平台进行漏洞扫描，并对存在漏洞的用友OA平台发起攻击，攻击成功后在受害机器中植入挖矿木马或远控木马。此外还有一个黑客团伙在攻击用友OA的同时，对亿赛通文档加密系统和泛微OA发起攻击。



8月份针对Web应用和数据库的各类攻击趋势

本月，Exchange远程代码执行漏洞ProxyShell的POC代码在互联网上被公开，在POC被公开之后，我们监测到针对Exchange服务的攻击出现一定程度的增加，怀疑该攻击可能与ProxyShell漏洞有关。下图是8月份每日针对Exchange服务的攻击趋势图。



8月份每日针对Exchange服务的攻击趋势图

安全漏洞

VULNERABILITIES

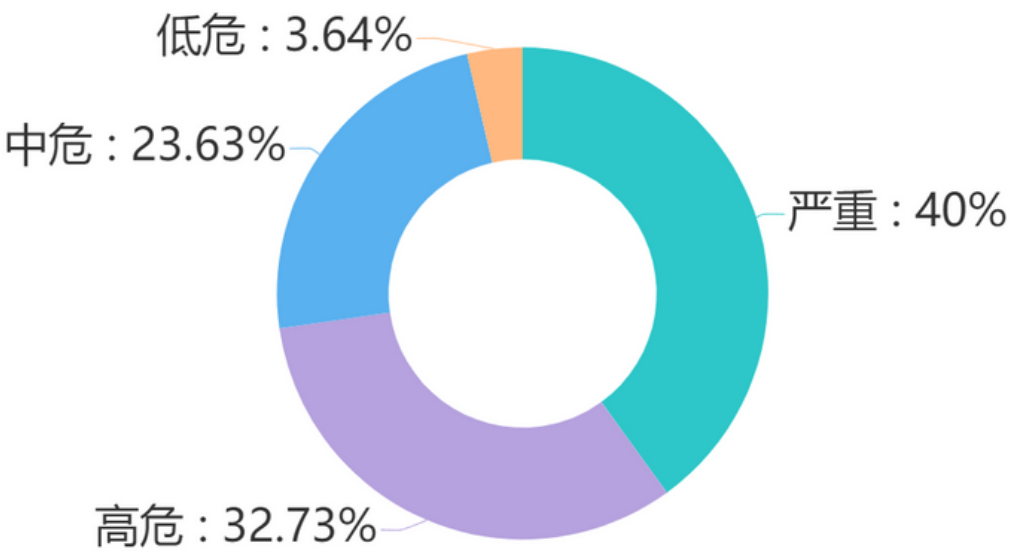
前言

2021年8月，360CERT共收录55个漏洞，其中严重22个，高危18个，中危13个,低危2个。主要漏洞类型包含代码执行、内存越界漏洞、访问控制不当、命令注入、服务器端请求伪造等。涉及的厂商主要是Windows、VMware、Atlassian、Apple、Apache 、IBM、Google等。

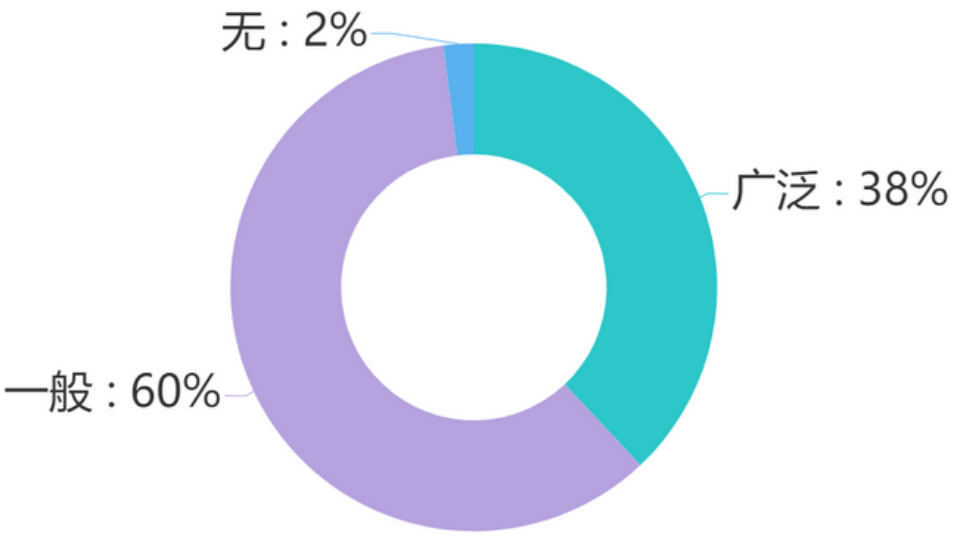
目录预览

漏洞图表

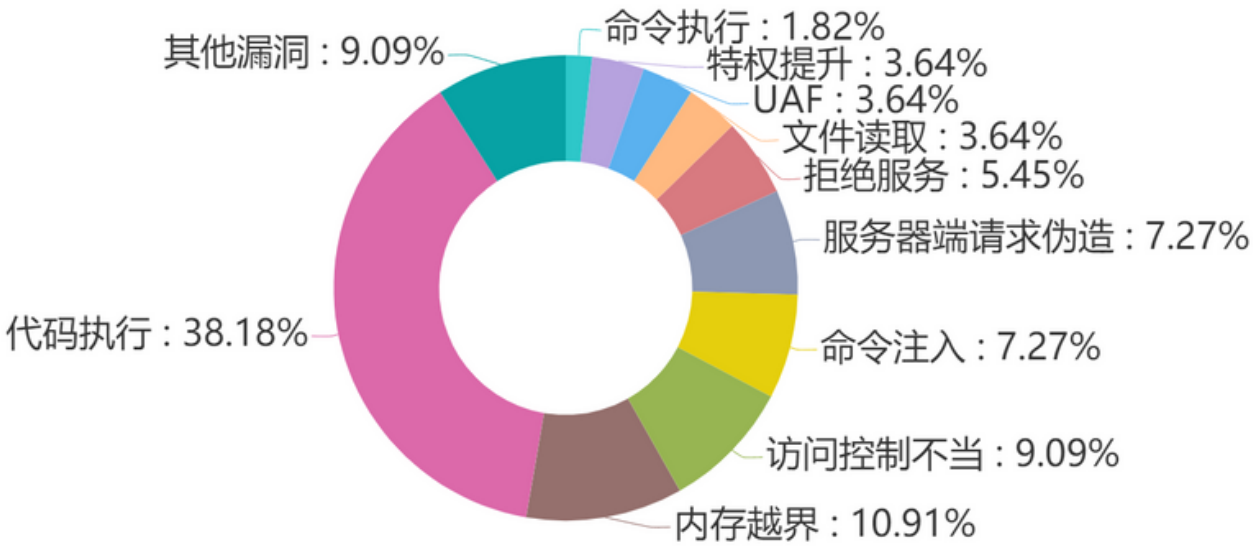
Charts Of Vulnerabilities



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
Exchange
vRealize Operations Manager
Confluence
iCloud
OFBiz
Xstream
WebSphere Application Server
TensorFlow
OpenSSL

热门组件列表

重点漏洞回顾

Review Of Vulnerabilities

CVE-2021-26084：Confluence OGNL 注入漏洞

评分：8.8　安全补丁已发布

2021年08月26日，360CERT监测发现Atlassian官方发布了Confluence OGNL 注入漏洞的风险通告，漏洞编号为CVE-2021-26084，漏洞等级：严重，漏洞评分：8.8。目前该漏洞安全补丁已更新，漏洞细节未公开，POC（概念验证代码）未公开，在野利用未发现。Confluence是Atlassian公司的一个专业的企业知识管理与协同软件，也可以用于构建企业wiki，因此，Confluence的使用面很广。在某些情况下，未授权的攻击者可以构造特殊的请求，造成远程代码执行。

2021-08: XStream 多个高危漏洞

评分：9.8　安全补丁已发布

2021年08月23日，360CERT监测发现XStream官方发布了XStream的风险通告，漏洞编号为CVE-2021-39139,CVE-2021-39140,CVE-2021-39141 等。漏洞等级：严重，漏洞评分：9.8。目前该漏洞安全补丁已更新，漏洞细节已公开，POC（概念验证代码）已公开，在野利用未发现。XStream是Java类库，用来将对象序列化成XML/JSON或反序列化为对象，不需要其它辅助类和映射文件，使得XML序列化不再繁琐。XStream在很多中间件中以第三方依赖的形式引入，使用广泛。攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上本地执行命令。

CVE-2021-20032：SonicWall Analytics 远程代码执行漏洞

评分：9.8　安全补丁已发布

2021年08月17日，360CERT监测发现 SonicWall 官方发布了 SonicWall Analytics 的风险通告，漏洞编号为 CVE-2021-20032，漏洞等级：严重，漏洞评分：9.8。SonicWall Analytics 是一种强大的情报驱动分析服务，可以解决安全以及网络性能问题，SonicWall Analytics 的使用场景多，适配于多种防火墙。SonicWall Analytics 默认将 JDWP 接口的调试端口 9000 暴露，攻击者能够访问该接口，构造特殊的请求造成远程代码执行。

CVE-2021-36958: Windows Print Spooler打印机漏洞

评分：9.9　安全补丁已发布

2021年08月12日，360CERT监测发现 微软 发布了 Print Spooler远程代码执行漏洞的风险通告，漏洞编号为 CVE-2021-36958 ，漏洞等级：严重，漏洞评分：9.9。Windows Print Spooler是用于管理打印机的后台服务，在办公场景下，该服务是一定会被频繁使用，且持续在电脑中运行。这就给予了攻击者相应的攻击场景。Windows系统中默认开启Pirnt Spooler打印机服务，攻击者可以通过构造特制的数据包，发送给该服务并造成远程代码执行。

2021-08 补丁日: 微软多个产品漏洞安全更新

评分：9.9　安全补丁已发布

2021年08月11日，360CERT监测发现 微软 发布了 8月份安全更新，事件等级：严重，事件评分：9.9。此次安全更新发布了44个漏洞的补丁，主要覆盖了以下组件：Windows操作系统、Microsoft Graphics Component、Remote Desktop Client、Windows NTLM、Windows TCP/IP、Windows Update Assistant等。其中包含7个严重漏洞，37个高危漏洞。本次安全更新漏洞编号为：CVE-2021-36948、CVE-2021-36936、CVE-2021-36942等。

漏洞时间线

Timeline Of Vulnerabilities

2021-08-02

CVE-2021-29781 严重
Partner Engagement Manager 代码执行

CVE-2021-29736 中危
WebSphere Application Server 特权提升

2021-08-03

CVE-2021-34556 中危
Kernel 敏感信息泄漏

CVE-2021-35477 中危
Kernel 敏感信息泄漏

2021-08-04

CVE-2021-22930 高危
Node.js UAF

CVE-2021-26104 高危
FortiPortal 命令注入

CVE-2021-24006 中危
FortiManager SD-WAN Orchestrator 访问控制不当

2021-08-06

CVE-2021-22002 高危
vRealize Suite Lifecycle Manager (vIDM) 访问控制不当

CVE-2021-22003 低危
vRealize Suite Lifecycle Manager (vIDM) 访问控制不当

2021-08-11

CVE-2021-36948 高危
Windows Update Medic Service 特权提升

CVE-2021-36936 高危
Windows Print Spooler 代码执行

CVE-2021-36942 严重
Windows LSA 欺骗攻击

CVE-2021-34535 严重
Windows Remote Desktop Client 代码执行

CVE-2021-34530 高危
Windows Graphics Component 代码执行

CVE-2021-26424 严重
Windows TCP/IP 代码执行

2021-08-12

CVE-2021-36958 严重
Windows Print Spooler 代码执行

2021-08-13

CVE-2021-3050 中危
PAN-OS 命令注入

CVE-2021-3045 低危
PAN-OS 命令注入

CVE-2021-37608 高危
OFBiz 文件上传

CVE-2021-37690 严重
TensorFlow UAF

2021-08-17

CVE-2021-20032 严重
sonicwall analytics on-prem 代码执行

2021-08-18

CVE-2021-30779 高危
iCloud 缓冲区溢出

CVE-2021-30785 高危
iCloud 缓冲区溢出

2021-08-19

CVE-2021-34730 严重
RV130W Wireless-N Multifunction VPN Routers 代码执行

CVE-2021-22156 严重
QNX OS Safety 整形溢出

2021-08-20

CVE-2021-22029 中危
Workspace ONE UEM console 拒绝服务

CVE-2021-22123 高危
FortiWeb 命令注入

2021-08-23

CVE-2021-28372 高危
Kalay P2P Development Kit 身份验证绕过

CVE-2021-39139 严重
xstream 代码执行

CVE-2021-39140 中危
xstream 拒绝服务

CVE-2021-39141 严重
xstream 代码执行

CVE-2021-39144 严重
xstream 代码执行

CVE-2021-39145 严重
xstream 代码执行

CVE-2021-39146 严重
xstream 代码执行

CVE-2021-39147 严重
xstream 代码执行

CVE-2021-39148 严重
xstream 代码执行

CVE-2021-39149 严重
xstream 代码执行

CVE-2021-39150 中危
xstream 服务器端请求伪造

CVE-2021-39151 严重
xstream 代码执行

CVE-2021-39152 中危
xstream 服务器端请求伪造

CVE-2021-39153 严重
xstream 代码执行

CVE-2021-39154 严重
xstream 代码执行

2021-08-25

CVE-2021-3711 高危
OpenSSL 缓冲区溢出

CVE-2021-3712 高危
OpenSSL 缓冲区溢出

CVE-2021-35940 中危
Portable Runtime 内存越界

2021-08-26

CVE-2021-26084 严重
confluence 代码执行

CVE-2021-22023 中危
VMware Cloud Foundation 不安全的直接对象引用

CVE-2021-22024 高危
vRealize Operations Manager 文件读取

CVE-2021-22022 中危
VMware Cloud Foundation 文件读取

CVE-2021-22027 高危
vRealize Operations Manager 服务器端请求伪造

CVE-2021-22025 高危
vRealize Suite Lifecycle Manager 失效的访问控制

CVE-2021-22026 高危
VMware Cloud Foundation 服务器端请求伪造

2021-08-30

CVE-2021-23032 中危
BIG-IP DNS 拒绝服务

CVE-2021-23025 高危
BIG-IP 命令执行

CVE-2021-32941 严重
NVR N48PBB 代码执行

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

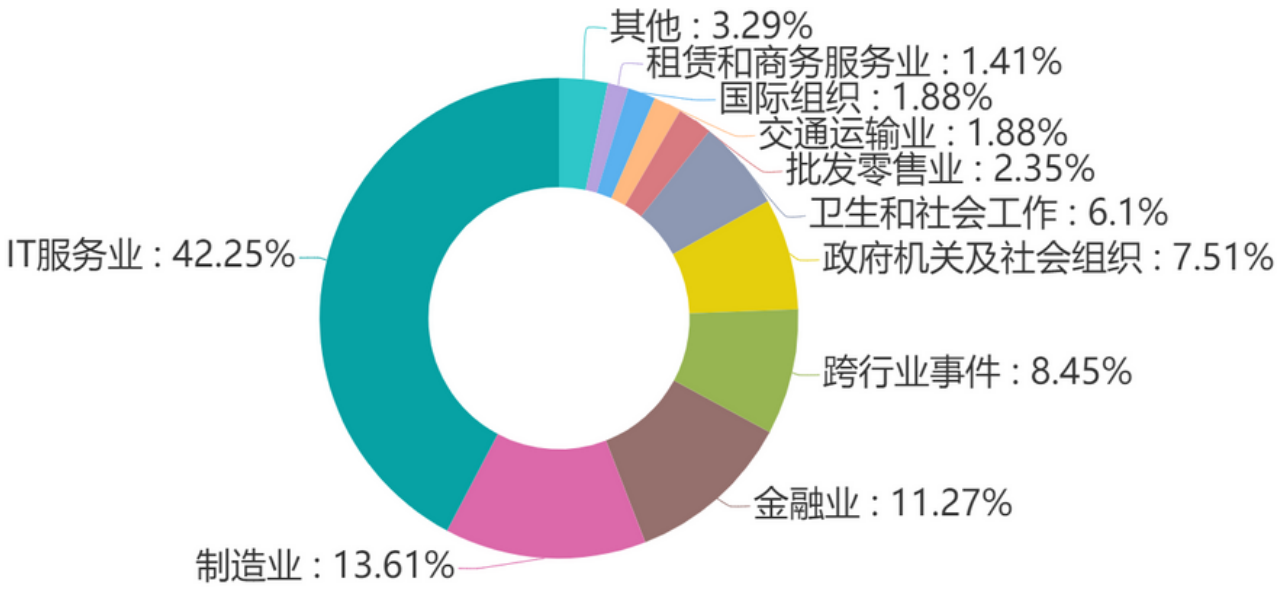
前言

本月收录安全事件213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、Cisco、华为、FBI、WordPress、Apple、Twitter等。涉及的行业主要包含IT服务业、制造业、金融业、政府机关及社会组织、批发零售业、医疗行业、交通运输业等。

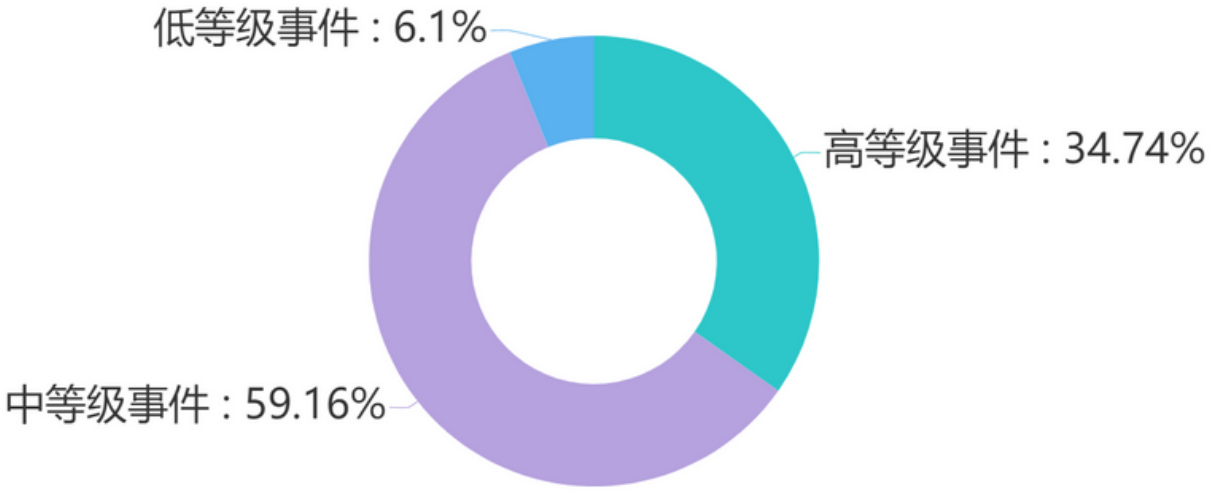
目录预览

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

来自美色的诱惑- APT-C-09（摩诃草）组织近期攻击活动披露

标签：APT-C-09, C2, APT
链接：https://mp.weixin.qq.com/s/_LHJYgf6l9uFYMN23fUQAA

APT-C-09（摩诃草）组织，又称HangOver、VICEROY TIGER、The Dropping Elephant、Patchwork，是一个来自于南亚地区的境外APT组织，该组织已持续活跃了7年。摩诃草组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。
近日360威胁情报中心捕获到几例借助美女图片作为诱饵的恶意样本程序，这些样本通过婚介主题来诱骗用户执行恶意程序or文档文件，运行后释放对应图片文件并打开以达到伪装的效果，自身主体则与服务器连接，接收指令数据，达到攻击者远程控制用户设备的效果。

APT-C-54(Gamaredon)近期技战术总结

标签：APT-C-54, C2, APT
链接：https://mp.weixin.qq.com/s/0zCpEQT4XHPOnB6h_9zg2Q

Gamaredon组织是具有俄罗斯背景的APT组织，长期以来针对乌克兰及周边地区进行着高频的网络攻击活动。该组织向来以活动强度大和活动频率高为主要特点，常常在短期内产生大量的威胁情报指标，且丝毫不在意暴露自身的俄罗斯相关背景。本篇报告将结合往期内容，针对该组织近期攻击活动中使用的不同载荷及暴露出的特征进行介绍。

南亚地区APT组织2020年度攻击活动回顾

标签：南亚地区, C2, APT
链接：https://mp.weixin.qq.com/s/IG8g8F6-YqTTcGX1BaSNaQ（上）
https://mp.weixin.qq.com/s/XcBuxlDh2DIjIMdFH6KCKQ（下）

回顾2020年间，来自于南亚地区的APT组织一直处于十分活跃的状态，其重点攻击目标依旧是东亚和南亚地区国家，360高级威胁研究院对2020年度所捕获的南亚地区APT组织的攻击进行了统计，并对具体行动、组织体系进行了分析。下篇重点介绍了2020年南亚地区的组织APT-C-08（蔓灵花）、APT-C-24（响尾蛇）、APT-C-35（肚脑虫）等的攻击活动，以及各组织针对移动端的攻击情况。
南亚地区的APT组织众多，且一直保持高度的活跃状态。通过长时间的跟踪分析360高级威胁研究院发现了南亚地区各个组织间存在较密切的关联，并给出了详细介绍。

猎天行动——CNC（APT-C-48）组织最新攻击活动披露

标签：APT-C-48, C2, APT
链接： https://mp.weixin.qq.com/s/dMFyLxsErYUZX7BQyBL9YQ

CNC（APT-C-48）组织是于2019年新出现的组织，由于其使用的远程控制木马的PDB包含了“cnc_client“的字样，所以将该组织命名为CNC，该组织主要攻击对象为我国军工和教育行业。去年年初我国疫情爆发初期，CNC组织通过伪造疫情相关的文档以及钓鱼网站对医疗行业发起攻击。
近日360高级威胁研究院监测到CNC组织在6月中旬我国航天相关时事热点前后，针对我国科研机构、高等院校以及航天相关领域进行多次情报窃取的定向攻击活动。因此将此次攻击活动命名为“猎天行动”。在本次攻击活动中，CNC组织采用了两种不同的攻击方式进行攻击。

“透明部落”近期利用印度国防部会议记录为诱饵的攻击活动分析

标签：APT-C-56, C2, APT
链接：https://mp.weixin.qq.com/s/3Je-DmyQrqNHxzRo70FTJw

Transparent Tribe（“透明部落”）组织为Proofpoint于2016年2月披露并命名的组织，也称为C-Major、PrijectM，是一个具有南亚背景的APT组织。该组织的主要攻击目标为印度政府、军队或相关组织，其利用社会工程学进行鱼叉攻击，向目标投递带有VBA的doc、xls文档，执行诱饵文档中的宏代码释放执行CrimsonRAT、PeppyRAT，窃取相关敏感资料信息。
近日，奇安信威胁情报中心红雨滴在日常的威胁狩猎发现，Transparent Tribe针对南亚地区的攻击活动近期主要以国防部会议、军事材料等为主题。根据红雨滴研究人员跟踪分析，此次的攻击活动有如下特点：

- 在此次攻击活动中，攻击者利用此前披露的透明部落组织类似攻击手法，即通过带恶意宏的文档最终释放CrimsonRAT执行。
- 未发现影响国内。

新的伊朗组织Siamesekitten发起的网络间谍活动

标签：Siamesekitten, C2, APT
链接：https://www.clearskysec.com/siamesekitten/

2020年5月初，clearskysec发现了Siamesekitten组织针对以色列IT公司的网络攻击。Siamesekitten (又名Lyceum/Hexane）是具有伊朗背景的APT组织，主要在中东和非洲地区发起供应链攻击。Siamesekitten建立了广泛的基础架构以至于能够模仿目标公司甚至公司内部的HR人员。而构建此基础架构是为了诱骗 IT 专家并入侵他们的计算机以访问公司客户。此次攻击与“Job seekers”攻击事件类似，使用了近年来广泛使用的攻击技术——模仿。许多组织都使用类似的技术，例如朝鲜Lazarus组织发起的”Dream Job“行动、伊朗OilRig组织于2021年一季度针对中东的攻击行动。
2021年7月，clearskysec再次发现了针对以色列其他公司的类似攻击。此次攻击中，Siamesekitten使用升级后的最新版“Shark”恶意软件取代了老版本“Milan”恶意软件。本篇报告总结了Siamesekitten的攻击行动，给出了该组织的攻击模式及使用的恶意软件。

朝鲜BLUELIGHT：InkySquid 部署 RokRAT

标签：InkySquid, C2, APT, APT37
链接：https://www.volexity.com/blog/2021/08/24/north-korean-bluelight-special-inkysquid-deploys-rokrat/

在最近的一篇博客文章中， Volexity 披露了朝鲜InkySquid组织的部分攻击细节。该组织入侵了一个新闻门户网站，以使用最近修补的浏览器漏洞分发自定义的BLUELIGHT恶意软件。
这篇文章描述了 Volexity 最近的调查结果，发现攻击者同时交付了BLUELIGHT与RokRAT（又名DOGCALL）后门（RokRAT之前归因于 ScarCruft/APT37/ InkySquid)。应该指出的是，Volexity 发现了本篇文章和[另一篇文章](https://medium.com/s2wlab/matryoshka-variant-of-rokrat-apt37-scarcruft-69774ea7bf48)存在部分重叠。

APT29—觊觎全球情报的国家级黑客组织

标签：APT29, C2, APT
链接：https://mp.weixin.qq.com/s/x0Y8psN_luaIH8dfQjwp3w（上）
https://mp.weixin.qq.com/s/Ln7iBm-Go17CQhIaRNHD0Q（中）
https://mp.weixin.qq.com/s/GBGJ1WOVsQCpVTY9audJPA（下）

依托国家情报机构发动的网络战日益频繁。在各国的网络战博弈中，俄美等国家凭借其长期的情报机构建设积累以及强大的武器库资源储备在公众眼中暂处第一梯队。国内情报分析人员接触到的有关这类高度复杂的 APT 组织相关情报信息大多数来源于国外安全机构。拥有俄罗斯联邦对外情报局（SVR）背景的APT29 组织即是如此，近半年时间内，随着 SolarWinds 供应链攻击的曝光以及后续多家安全机构的调查分析，疑似幕后黑手的 APT29 开始回归大众视野中。
当前针对 APT29 的公开披露情报信息因为国家政治公关、敏感信息“阉割”等因素显得繁琐混杂、可信度高低不一。微步情报局基于已积累的情报信息以及网络公开情报信息甄别研判结果，对 APT29 的重大攻击事件、组织关联归因、攻击技战法等进行了深度复盘分析，致力于客观、全面地向大众解读 APT29 的真实面貌。
本文主要输出以下内容：

- 梳理当前公开情报信息，APT29 组织结构分析及各分支机构经典攻击事件分析；
- 探究 The Dukes、WellMess、Nobelium（Solarwinds）归因点及可信度；

APT29 关键 TTPS 剖析；
微步视角下的 APT29 组织画像。

Bear Tracks：30多个活跃的 APT29 C2 服务器

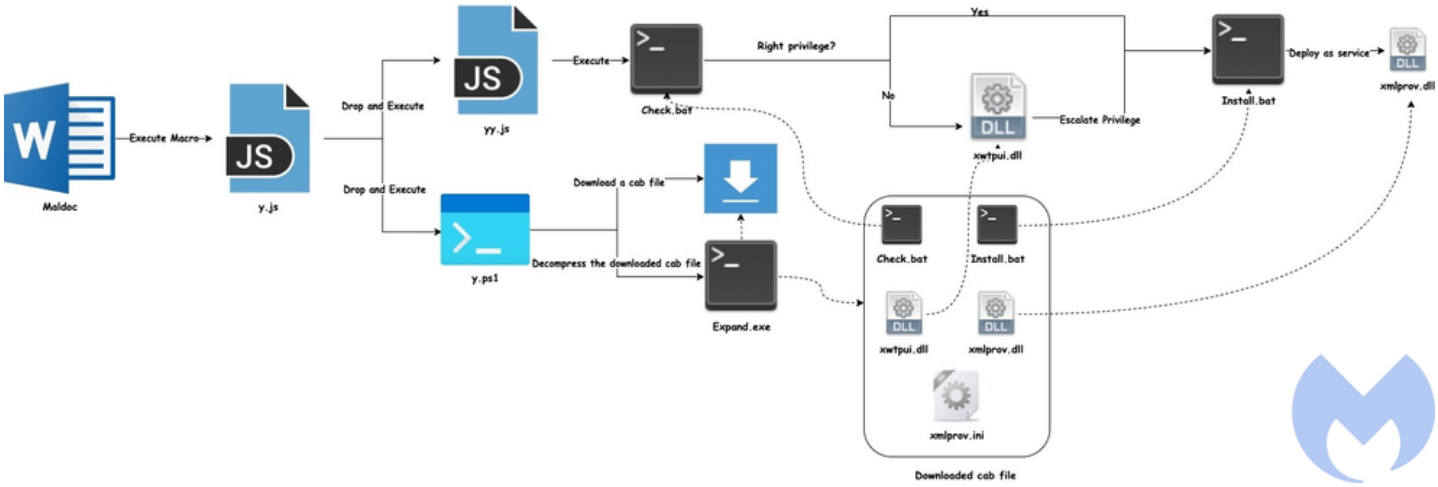
标签：APT29, C2, APT
链接：https://community.riskiq.com/article/541a465f

一年前，美国、英国、加拿大政府联合发表的[咨询报告]（https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf） 详细介绍了俄罗斯针对COVID-19 疫苗研究工作的网络间谍活动，并将此活动归因于APT29（又名YTTRIUM、THE DUKES、COZY BEAR），明确指出该组织与俄罗斯情报部门 (SVR) 有关联；同时首次公开将攻击活动中使用的恶意软件WellMess和WellMail归咎于APT29。2020年，RiskIQ的Team Atlas报告确定了另外十多个与该组织有关的C2（报告链接：https://community.riskiq.com/article/642d186e）。近期，RiskIQ的Team Atlas团队再次确定了30多个与WellMess/WellMail相关的基础设施。

Konni 使用恶意软件新变种攻击俄罗斯

标签：Konni, C2, APT, Russia
链接：https://blog.malwarebytes.com/threat-intelligence/2021/08/new-variant-of-konni-malware-used-in-campaign-targetting-russia/

2021年7月下旬，Malwarebytes发现Konni组织正在针对俄罗斯发起鱼叉式网络钓鱼活动。
攻击者使用了两个内嵌相同恶意宏的俄语文档，文档之一的主题是关于俄罗斯与朝鲜半岛之间的贸易和经济问题，另一个是关于俄罗斯与 蒙古政府间的会议；此外，攻击者开发了一种新的经过严重混淆的Konni RAT变体，该变体配置的加密方式不再使用base64编码，而且也不继续使用FTP协议。
攻击过程使用了以下两种技术来逃避安全检测：
(1)根据受害者的操作系统选择不同的UAC绕过技术：令牌模拟UAC绕过技术和针对Windows 10的UAC绕过技术；
(2)巧妙的混淆技巧：攻击者将执行攻击活动的恶意JS脚本隐藏在了文档内容的末尾，而不是直接嵌入到宏中。
Malwarebytes在博客中概述了此次攻击活动，下图展示了整个鱼叉式钓鱼攻击流程：



Confucius利用与 Pegasus 间谍软件相关的诱饵攻击巴基斯坦军方

标签：Confucius, C2, APT
链接： https://www.trendmicro.com/en_us/research/21/h/confucius-uses-pegasus-spyware-related-lures-to-target-pakistani.html

调查Confucius组织时，趋势科技发现了近期的一起鱼叉式网络钓鱼活动，该活动利用与 Pegasus 间谍软件相关主题的诱饵，诱使受害者打开可以下载文件窃取程序的恶意文档。
本篇博客中，趋势科技分析了攻击者使用的诱饵文档，并对下载的文件窃取程序进行了简短的分析。

ITG18：操作安全错误继续困扰着规模庞大的伊朗威胁组织

标签：ITG18, C2, APT
链接：https://securityintelligence.com/posts/itg18-operational-security-errors-plague-iranian-threat-group/

IBM Security X-Force 威胁情报研究人员持续跟踪疑似伊朗威胁组织ITG18的基础设施和攻击活动。该组织的战术、技术和过程(TTP)与被称为 Charming Kitten、Phosphorus和TA453 的组织有所重叠。
自IBM Security X-Force于2020年5月首次披露该组织以来，再次发现了该组织的其他操作性安全错误。X-Force进一步分析发现了一个之前未关联到该组织的恶意工具——自定义Android后门，并将其命名为“LittleLooter”。LittleLooter仅被观察到由ITG18使用，尚不清楚其他组织是否使用此后门。
此外，从2020年8月到2021年5月，X-Force 观察到ITG18成功地攻击了与伊朗改革主义运动相关的多名受害者。鉴于攻击的时间安排和重点，这可能是为了在2021年6月伊朗总统选举之前对目标进行监视。
尽管OPSEC错误不断，ITG18似乎仍完成了大规模且成功的攻击活动，重点是入侵私人网络邮箱和社交媒体帐户。

重点事件回顾

Review Of Incidents

恶意程序事件

IT咨询巨头埃森哲遭遇Lockbit勒索软件攻击

IT服务业

Lockbit2.0在其数据泄露网站发布关于埃森哲（网络保险提供商、全球IT咨询巨头）已遭受勒索攻击相关新闻，该团伙不仅加密了埃森哲2500台设备，还从内网中窃取了6TB数据。Lockbit团伙发出警告，若不在指定时间内支付5000万美元(约3.2亿人民币)赎金，将公开发布窃取到的全部数据。Lockbit2.0团队原本计划在2021年8月11日公开埃森哲的数据，但可能因为埃森哲或者其他对埃森哲数据感兴趣的人正在和该团伙进行数据购买沟通，该团伙已两次调整公开数据期限，当前公开时间为2021年8月13日。目前埃森哲已通过备份，将受影响机器恢复。

虽然Lockbit尚未在数据泄露网站公开埃森哲相关的任何数据，但是在与其沟通的记录中可看到部分埃森哲内部的口令凭证。

SideWalk恶意软件分析

批发零售业

ESET 研究人员最近发现了一个新的未公开的模块化后门 SideWalk，APT组织SparklingGoblin 最近针对一家美国计算机零售公司的攻击活动中使用了这个后门。这个后门与该组织使用的另一个后门CROSSWALK 有很多相似之处。

数据安全事件

T-Mobile 证实系统遭到破坏

IT服务业

美国 T-Mobile 公司2021年8月16日证实其电脑系统被非法侵入。一个在线论坛的卖家声称，从 T-Mobile 的系统中获取了 1 亿条个人记录，其中 3600 万条是唯一的。部分数据包括 3000 万个社会保障和驾驶执照号码，在在线论坛上以 6 个比特币出售，价值约 286,000 美元。其余个人数据据称包括姓名、地址、出生日期和技术电话数据，例如国际移动用户识别码（IMSI）和国际移动设备识别码（IMEI）号码。

地下黑客论坛出售7000万AT&T用户的私人信息

IT服务业

据报道，一个臭名昭著的黑客组织 Shinyhunters，正在出售一个包含 7000 万AT&T客户私人详细信息的数据库。 然而，美国电信供应商AT&T否认遭受数据泄露。

Shinyhunters 共享了被盗数据、姓名、联系电话、实际地址、社会安全号码 (ssn) 和出生日期的样本子集。一位匿名安全专家称样本中的四人中有两人是AT&T数据库中的用户。

3800 万条记录因 Microsoft 配置错误而暴露

卫生和社会工作

据专家称，使用微软 Power Apps 门户平台的 1000 多个 Web 应用程序中的大约 3800 万条数据可以在线访问。 数据来自 covid-19 接触者追踪操作、疫苗注册和员工数据库的数据，包括家庭住址、电话号码、社会安全号码和疫苗接种状态。

黑客出售超过 130 万俄罗斯人的护照

批发零售业

黑客在网络犯罪论坛 raidforums 上发布了一个 809 GB 的档案，其中包含超过 130 万份俄罗斯公民护照扫描件，这些文件是在入侵化妆品公司oriflame的服务器后被盗的。7月31日和8月1日，oriflame 遭受了一系列网络攻击，导致该公司的信息系统被未经授权访问。oriflame保证用户的银行帐号、电话号码、密码和商业交易不受攻击影响。

网络攻击事件

IT服务业

Liquid货币交易所遭受黑客攻击，损失超过 9000 万美元

Liquid 是全球最大的加密货币法币交易平台之一（基于每日现货交易量）。该交易所拥有来自 100 多个国家/地区的超过 800,000 名客户，并表示2021年其日交易量达到了 1.1亿美元。在攻击者破坏了其热钱包后，日本的加密货币交易所 Liquid 已暂停存款和取款，并且将其资产转移到冷钱包中。

Cosmos 数据库严重漏洞影响了数以千计的 Microsoft Azure 客户 IT服务业

云基础设施安全公司wiz披露了azure cosmos数据库漏洞的细节，目前该漏洞已修复。该漏洞允许任何azure用户在未授权的情况下对其他客户的数据库进行完全管理和访问。该漏洞授予读取、写入和删除权限，被称为“chaosdb”。

其他事件

工业控制设备中广泛使用的嵌入式TCP/IP协议栈存在严重漏洞 电热燃水及其供应业

网络安全研究人员在8月4日披露了 14 个影响常用 tcp/ip 堆栈的漏洞，该堆栈由不少于 200 家供应商制造并部署在制造工厂、发电、水处理和基础设施部门的数百万个操作技术 (ot) 设备中使用。漏洞存在于nichestack（又名 interniche 堆栈，是一种用于嵌入式系统的闭源 tcp/ip 堆栈），利用漏洞攻击者能够实现远程代码执行、拒绝服务、信息泄漏、tcp 欺骗，甚至 dns 缓存中毒。

CVE-2021-20090:数百万个路由器中的严重漏洞 制造业

严重的安全漏洞使全球数百万台路由器面临风险，该漏洞可绕过身份验证并影响使用 Arcadyan 固件的家庭设备。 这允许攻击者控制它们并使用 Mirai 僵尸网络进行攻击。此漏洞会影响许多电话型号和运营商，并且可以被远程利用。漏洞编号为 CVE-2021-20090，其严重性等级为 9.9（总分 10）。

事件时间线

Timeline Of Incidents

2021-08-02
FBI 发现了 100 多个活跃的勒索软件变种
PTS 系统中的 PwnedPiper 漏洞影响了 80% 的美国医院

2021-08-04
工业控制设备中广泛使用的嵌入式TCP/IP协议栈存在严重漏洞

2021-08-06
vpnMentor报告显示6300万美国用户的信息遭泄露

2021-08-07
硬件厂商技嘉遭勒索软件攻击

2021-08-08
破坏美国最大燃油管道的黑客团伙卷土重来

2021-08-09
Todler 木马扩大在欧洲的攻击范围
CVE-2021-20090:数百万个路由器中的严重漏洞

2021-08-10
Chaos 恶意软件介于勒索软件和 Wiper 之间

2021-08-11
黑客从 Poly Network 窃取了价值超过 6 亿美元的加密货币
勒索软件eCh0raix衍生出新变种：可感染QNAP和群晖NAS设备
WordPress 网站在 Aggah 鱼叉式网络钓鱼活动中被滥用
IT咨询巨头埃森哲遭遇Lockbit勒索软件攻击

2021-08-12
100万张被盗信用卡在暗网曝光
Heimdal发现新的DeepBlueMagic勒索软件菌株

Apple的 XProtect 防御可能无法抵御AdLoad 恶意软件新变种
Crytek 承认在遭受 Egregor 勒索软件攻击后数据被盗

2021-08-13
黑客使用莫尔斯电码来躲避检测
Vice Society 勒索软件加入了正在进行的 PrintNightmare 攻击

2021-08-15
福特漏洞暴露了内部系统的客户和员工记录

2021-08-16
新的 Trickbot 攻击伪造 One Password 安装程序以提取数据
发现了数十个STARTTLS相关漏洞，影响了流行的电子邮件客户端
一个数据交易论坛出售属于立陶宛外交部的电子邮件

2021-08-17
T-Mobile 证实系统遭到破坏
燃料管道运营商数据泄露影响数千人
俄亥俄州Memorial卫生系统最近遭到袭击
来自 FBI 的恐怖分子观察名单中190 多万条记录被泄漏
黑客诱骗英国人下载 Flubot 恶意软件
恶意广告使用Cinobi银行木马攻击加密货币用户
大通银行客户敏感数据意外泄露
Confucius利用与Pegasus间谍软件有关的诱饵攻击巴基斯坦军方

2021-08-18
数以百万计的物联网设备、婴儿监视器对音频、视频监听开放
HolesWarm 恶意软件利用未打补丁的 Windows、Linux 服务器
日本保险公司 Tokio Marine 承认遭受勒索软件攻击
BadAlloc 漏洞影响数百万汽车和医疗设备中使用的 BlackBerry QNX

2021-08-19
黑客攻击后，Liquid货币交易所损失超过 9000 万美元

COVID-19 接触者追踪数据暴露
Siamesekitten 发起针对以色列组织的新行动

2021-08-20
保险公司 Tokio Marine 遭到勒索软件攻击
Aggah APT 组织攻击台湾、韩国
LockFile 勒索软件使用 PetitPotam 攻击 Windows 域

2021-08-21
美国国务院最近遭受网络攻击
巴西最大的服装连锁店 Lojas Renner 遭受勒索软件攻击

2021-08-22
黑客利用ProxyShell 漏洞扫描，超过 1900 台服务器被黑

2021-08-23
Ursnif 银行木马
LockFile 勒索软件通过 ProxyShell 危害 Microsoft Exchange
Razer Synapse存在漏洞可让攻击者接管目标计算机
地下黑客论坛出售7000万AT&T用户的私人信息

2021-08-24
Mirai 僵尸网络攻击数十万台设备使用的Realtek SDK
3800 万条记录因 Microsoft 配置错误而暴露
诺基亚分公司SAC Wireless在Conti勒索软件事件后遭受数据泄露
Konni RAT 变体针对俄罗斯
cloudflare遭受DDoS攻击 - 每秒收到1720万次http请求
SideWalk恶意软件分析

2021-08-25
新的 SideWalk 后门瞄准了美国的计算机零售业务

2021-08-26

未打补丁的 Microsoft Exchange 服务器遭到 ProxyShell 攻击

21 岁的年轻人是 T-Mobile 黑客攻击的幕后黑手

黑客出售超过 130 万俄罗斯人的护照

2021-08-27

Cosmos 数据库严重漏洞影响了数以千计的 Microsoft Azure 客户

新加坡一家眼科诊所遭勒索软件攻击，73,500名患者数据被泄露

2021-08-29

Raven Hengelsport 数据泄露暴露了 18GB 的客户数据

2021-08-30

BazaLoader 恶意软件隐藏在虚假的 DMCA 和 DDoS 投诉中

对瑞士城市的勒索软件攻击暴露了公民的数据

曼谷航空高管为数据泄露道歉

富士通称暗网上出售的被盗数据与客户有关

2021-08-31

黑客从 Cream Finance 窃取了超过 2900 万美元的加密货币资产

黑客可利用Microsoft Exchange ProxyToken漏洞窃取用户电子邮件

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8月，全球新增的活跃勒索病毒家族有 :LockFile、 MBC、 Karma、 Malki、GetYourFilesBack 、 Salma 、AllDataStolen、GoodMorning等勒索软件。其中LockFile严格意义上来说是2021年7月新增，但在7月仅发现一个受害者，从8月20日开始已出现10多个受害者；Karma是本月新增的双重勒索软件；MBC在本月成功攻击伊朗伊斯兰共和国铁路系统，并拥有自己的数据泄露网站，但尚未泄露受害者数据。

目录预览

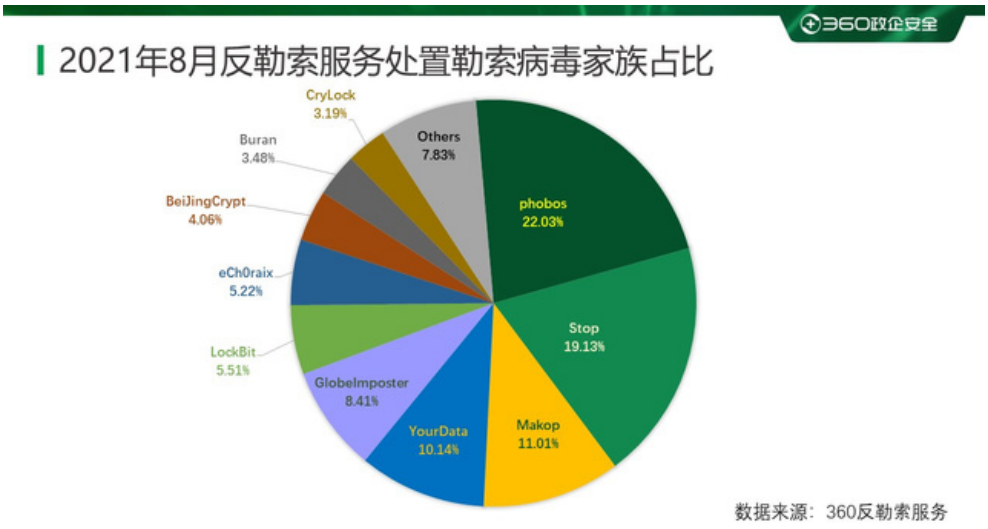
勒索病毒态势分析

Ransomware Situation Analysis

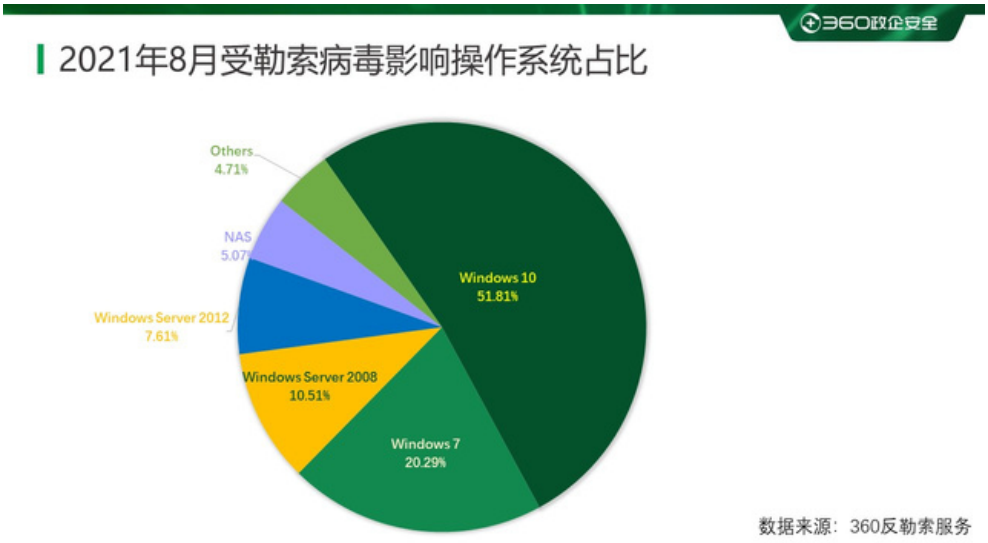
一、感染数据分析

针对本月勒索病毒受害者所中勒索病毒家族进行统计，phobos家族占比22.03%居首位，其次是占比19.13%的Stop，Makop家族以10.01%位居第三。

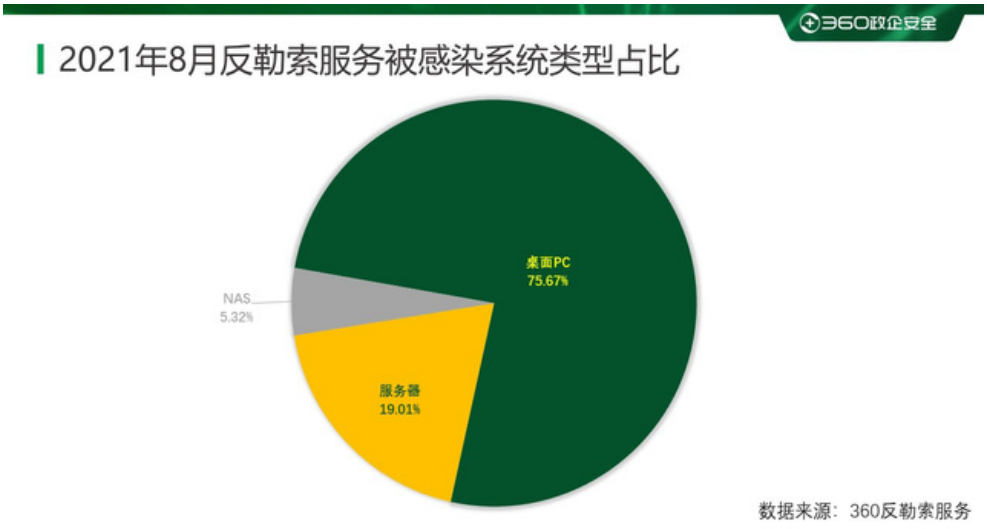
对比近三个月的感染数据，GlobeImposter家族有持续下降的态势；已消失几月的BeiJingCrypt勒索软件再次活跃；通过长时间的观察发现，在国内传播的LockBit勒索软件并非都涉及数据泄露，受灾面积小的企业/组织并未被该家族公开发布被窃取数据(但仍不排除有数据泄露风险)。



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8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。



二、黑客信息披露

以下是本月收集到的黑客邮箱信息：

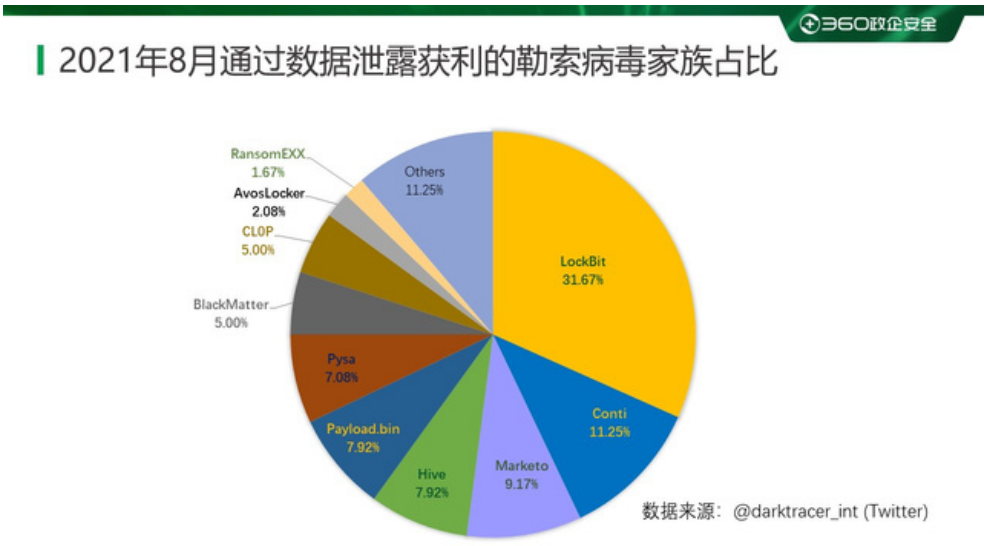
maz3@tuta.io	recovery.pc@aol.com	ransom1999@tutanota.com
in0x2@int.pl	kalitulz@yandex.com	ransom2000@tutanota.com
1bmx1@tuta.io	johnnylo@keemail.me	ransomwaree2020@cock.li
break@cock.li	globalbtc2@mein.gmx	ransomwaree2021@cock.li
jerjis@tuta.io	Decode@criptext.com	sdjhf4df@potronmail.com
fata52@cock.li	mangerman@firemail.d	unlockfile@criptext.com
fata54@cock.li	holylolly@airmail.cc	ezfilesdec@tutanota.com

dtramp@tuta.io	gluttony_001@aol.com	basani400@mailfence.com
decphob@tuta.io	moon4x4@tutanota.com	coderunlocker@gmail.com
getmydata@bk.ru	cyvedira@firemail.cc	howrecover@tutanota.com
supp0rt@cock.li	filedec@tutanota.com	sharm777@protonmail.com
rantime@tuta.io	chadmad@ctemplar.com	recoverman@tutanota.com
newera@tfwno.gf	filesdecrypt@aol.com	magicbox@outlookpro.net
mikolio@cock.li	wugenaxu@firemail.cc	kalitulz@protonmail.com
mikolio@xmpp.jp	databack@firemail.cc	highlvlservice@tfwno.gf
recofile@mail.ee	btcunlock@airmail.cc	chinadecrypt@msgsafe.io
pusheken91@bk.ru	ghosttm@zohomail.com	nullcipher@tutanota.com
pandabit@tuta.io	decrypt20@stealth.tg	xdatarecovery@msgsafe.io
decrypt20@vpn.tg	lepuscrysupp@mail.ee	Goodhack@privatemail.com
subik099@cock.li	lepuscrysupp@cock.li	mydataback@mailnesia.com
trizvani@aol.com	maykeljakson@cock.li	mymakopfile@tutanota.com
datashop@list.ru	unlocker@firemail.cc	kingstonbtc@tutanota.com
fastwind@mail.ee	958f895@tutanota.com	serioussam@thesecure.biz
johnsonz@cock.lu	johnlo@techmail.info	digistart@protonmail.com
pandora9@tuta.io	phobos@mailfence.com	tsec3x777@protonmail.com
files@restore.ws	zahary@techmail.info	savemyself1@tutanota.com
infoback@mail.ee	Help1999@tutanota.com	HELPUNKNOWN@Tutanota.com
help4dec@cock.li	assistant@firemail.de	itambuler@protonmail.com
recover1@cock.li	hublle@protonmail.com	dcrptfile@protonmail.com
sharm777@aol.com	paymantsystem@cock.li	encrypted60@tutanota.com
tutik337@tuta.io	Hubble77@tutanota.com	jonneydep@protonmail.com
tutik337@cock.li	crioso@protonmail.com	sdx-20200@protonmail.com
covidv19@cock.li	eleezcry@tutanota.com	fastwind2@protonmail.com
globalbtc@gmx.de	dozusopo@tutanota.com	keydecryption@airmail.cc
picklock@elude.in	subik099@tutanota.com	datastore@outlookpro.net
greed_001@aol.com	trizvani@tutanota.com	harpia2019@mailfence.com
pride_001@aol.com	btcunlock@firemail.cc	sacura889@protonmail.com
wiruxa@airmail.cc	anticrypt2020@aol.com	coderunlockerr@gmail.com
happy@gytmail.com	yongloun@tutanota.com	ransom19999@tutanota.com
falcon360@cock.li	alonesalem@keemail.me	emiliantor@mailfence.com
lexus@gytmail.com	sdx-2020@tutanota.com	paybackformistake@qq.com
getmydata@cock.li	dragon.save@yahoo.com	John.Muller@mailfence.com
basani400@aol.com	covidv19@tutanota.com	JohnMuller88@tutanota.com
databankasi@bk.ru	decrypt20@firemail.cc	harmagedon0707@airmail.cc
gracia154@tuta.io	infoback@criptext.com	pecunia0318@protonmail.ch
gracia154@cock.li	ghiedksjdh6hd@cock.li	hinduism0720@tutanota.com
boomblack@cock.li	anticrypt2021@aol.com	yourfriendz@techmail.info
safetynet@mail.ee	crashonlycash@gmx.com	helpmedecoding@airmail.cc
2magicbox@cock.li	help4rec@tutanota.com	reynoldmuren@tutanota.com
johnlo@keemail.me	unlocker@criptext.com	moonlight101@tutanota.com
decrypt20@xmpp.jp	gener888@tutanota.com	redsnow911@protonmail.com

indyan@airmail.cc	vnhack@protonmail.com	alonesalem@protonmail.com
riscattu@gmail.com	Howtodecrypt@elude.in	forumsystem@techmail.info
kabura@firemail.cc	johnnylo@techmail.info	ransomsophos@tutanota.com
raboly@firemail.cc	recofile@mailfence.com	dr.cryptor@protonmail.com
kubura@firemail.cc	getthekey@tutanota.com	maykeljakson@criptext.com
dacowe@firemail.cc	ithelp02@decorous.cyou	recovery.pc@mailfence.com
phobos2020@cock.li	rans0me@protonmail.com	ransom199999@tutanota.com
surpakings@mail.ee	payfast290@mailtor.com	ransom200000@tutanota.com
ransomtime@cock.li	serioussam@firemail.cc	strike8889@protonmail.com
in0x2@tutanota.com	decphob@protonmail.com	emilianazizi@tutanota.com
harpia2019@aol.com	eight20@protonmail.com	evilmosquito@onionmail.org
jennymombu@aol.com	divevecufa@firemail.cc	Leslydown1988@tutanota.com
helpme2021@aol.com	itambuler@tutanota.com	cryptonation92@outlook.com
james2020m@aol.com	surpaking@tutanota.com	decrypt_ad1@protonmail.com
james2020m@cock.li	cifrado60@tutanota.com	Black_Wayne@protonmail.com
jackkarter@gmx.com	opticodbestbad@aol.com	dataencrypted@tutanota.com
jackkarter@cock.li	opticodbestbad@mail.ee	xiaolinghelper@firemail.cc
safetynet@tfwno.gf	unlockdata@firemail.cc	jobiden1942@protonmail.com
rottencurd@mail.ee	encryption2020@aol.com	decryption24h@criptext.com
dr.help888@aol.com	grootp2@protonmail.com	mrs.help888@protonmail.com
sacura1716@cock.li	noobt56@protonmail.com	reopening1999@tutanota.com
help2021me@aol.com	decryption24h@elude.in	pablokariablo@mail2tor.com
nullcipher@goat.si	dr.cryptor@secmail.pro	venomous.files@tutanota.com
help@wedecrypt.net	unlockfile@firemail.cc	ithelp02@wholeness.business
pecunia0318@goat.si	jennymombu@firemail.cc	quickrecovery05@firemail.cc
Natonyx@firemail.cc	sacura889@tutanota.com	davidshelper@protonmail.com
greenreed007@qq.com	jonnylow@techmail.info	dowendowxxx@privatemail.com
clean@onionmail.org	boomblack@tutanota.com	decryption24h@mailfence.com
r4ns0m@tutanota.com	rottencurd@vivaldi.net	highlvlservice@ctemplar.com
contactjoke@cock.li	958f895@protonmail.com	bob_marley1991@tutanota.com
qirapoo@firemail.cc	borisrazor@nerdmail.co	crazydecrypt@horsefucker.org
rodrigos@keemail.me	strike999@tutanota.com	maksimbockovskij315@gmail.com
chadmad@nuke.africa	phobossp@protonmail.ch	jackiesmith176@protonmail.com
falcon360@cock.li	alonesalem@keemail.me	emiliantor@mailfence.com
lexus@gytmail.com	sdx-2020@tutanota.com	paybackformistake@qq.com
getmydata@cock.li	dragon.save@yahoo.com	John.Muller@mailfence.com
basani400@aol.com	covidv19@tutanota.com	JohnMuller88@tutanota.com
databankasi@bk.ru	decrypt20@firemail.cc	harmagedon0707@airmail.cc
gracia154@tuta.io	infoback@criptext.com	pecunia0318@protonmail.ch
gracia154@cock.li	ghiedksjdh6hd@cock.li	hinduism0720@tutanota.com
boomblack@cock.li	anticrypt2021@aol.com	yourfriendz@techmail.info
safetynet@mail.ee	crashonlycash@gmx.com	helpmedecoding@airmail.cc

databack@airmail.cc	operator@wedecrypt.net	DECRYPTUNKNOWN@Protonmail.com
moonlight10@mail.ee	riscattu@protonmail.com	erichhartmann_reserve@tuta.io
onlyway@secmail.pro	clean@privyinternet.com	backupransomware@tutanota.com
forumsystem@cock.li	payfast290@mail2tor.com	chinadecrypt@fasthelpassia.com
dragon.save@aol.com	contact@contipauper.com	bob_marley1991@libertymail.net
drgreen1@keemail.me	recoryfile@tutanota.com	JamesHoopkins1988@onionmail.org
newera@ctemplar.com	clearcom@protonmail.com	ollivergreen1977@protonmail.com
johnsonz@keemail.me	phobos2020@tutanota.com	Decryptdatafiles@protonmail.com
hellook@gytmail.com	anygrishevich@yandex.ru	jeffreyclinton1977@onionmail.org
5559912@firemail.cc	drgreen2@protonmail.com	GunsOFThePatriots@privatemail.com
firmaverileri@bk.ru	tebook12@protonmail.com	erichhartmann_main@protonmail.com
jonnylow@keemail.me	rody_218@protonmail.com	fourfingeredfrankie@onionmail.org

当前，通过双重勒索或多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）。

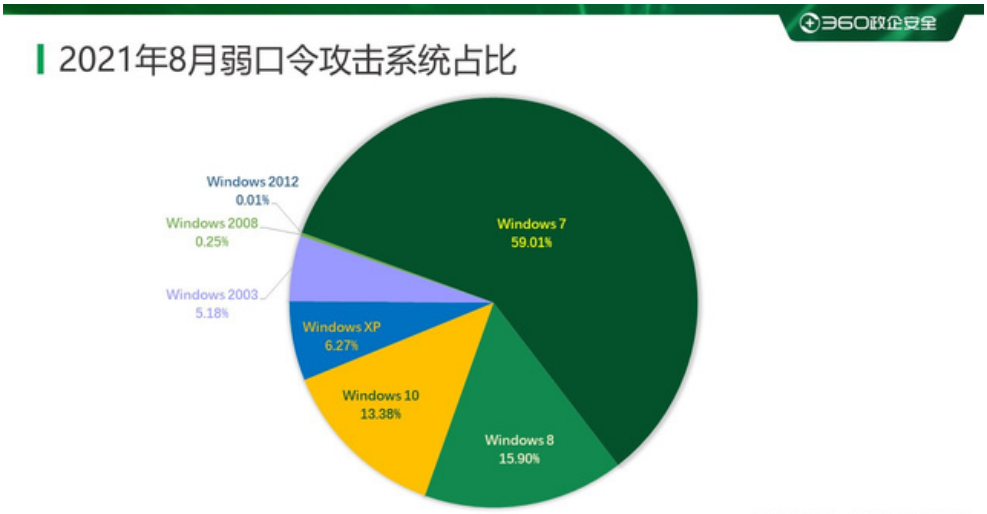


以下是本月被双重勒索病毒家族攻击的企业或个人。若未发现被数据存在泄露风险的企业或个人也请第一时间自查，做好数据已被泄露准备，采取补救措施。

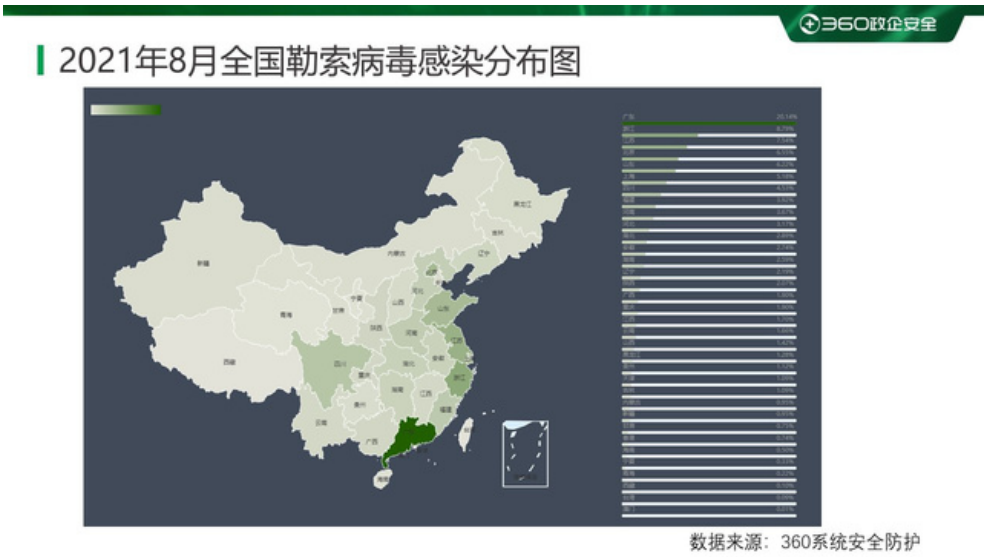
dimeo	Geneva, Ohio	Arabian Cargo Group
imasa	Stevens & Lee	Breydons Solicitors
cegos	Talbert House	Pesquera Exalmar SAA
KASEYA	Paxton Access	ensingerplastics.com
Walsin	Paxton Access	Dragon Capital Group
Alcedo	aris-services	cecengenharia.com.br
Bamford	cometgroup.be	Commune De Villepinte
ALBIOMA	kennen.com.ar	Heller Injury Lawyers
CHADDAD	betonlucko.hr	swiftlogistics.com.my
Beckley	anderscpa.com	Virginia Defense Force
habasit	Techni+Contact	Belperio Clark Lawyers
matchmg	siro-group.com	europeanaccounting.net
Gulf Oil	The Wild Rabbit	creditoycaucion.com.ar
Hx5, LLC	Mambrino S.A.C.	sahintoptangida.com.tr
DiaSorin	Gateway College	classicalmusicindy.org
keltbray	INSERM-TRANSFER	Sierra Air Conditioning
friedrich	grupodismar.com	kuk.de / KREBS + KIEFER
PCM Group	f**********	Florida Sugar Cane League
BHoldings	vincents.com.au	Walter's Automotive Group
Cinépolis	SAC Wireless Inc	Elm3 Financial Group, LLC
Actiontec	Sandhills Center	Nottingham City Transport
infovista	Home in Brussels	Haftpflichtkasse Darmstadt
Jhillburn	Grupo DINA S.A.	GATEWAY Property Management
HUF GROUP	Phoenix Services	Artas Holding / Artas Insaat
Daylesford	riostarfoods.com	South Carolina Legal Services
inocean.no	modernbakery.com	Century 21 Gold Key Realty, Inc
IBC24 News	Agrokasa Holdings	Walter's Mercedes-Benz of Riverside
apg-neuros	Aquazzura Firenze	Trifecta Networks & CloudFirst Labs
ccz.com.au	Revision Skincare	On logistics Services Algeciras, S.L
Mega Vision	spiralfoods.com.au	Corporación Nacional de Telecomunicación
supplyforce	cspmould-stampi.it	SALZBURGER EISENBAHN TRANSPORT LOGISTIK GmbH
Colligan Law	WT Microelectronics	Orange County Chrysler Jeep Dodge Ram Dealership

三、系统安全防护数据分析

通过将2021年7月与8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8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8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。MSQQL属于正常的波动范围。

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。
- hauhitec：属于CryptoJoker，由于被加密文件后缀会被修改为hauhitec而成为关键词。通过“匿隐” 僵尸网络进行传播。
- 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：Lockbit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。
- hoop：属于Stop勒索病毒家族，由于被加密文件后缀会被修改为hoop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。
- 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。
- reqg:同hoop。
- nooa：同hoop。
- orkf: 同hoop。
- encrypt：该后缀被很多家族均使用过，但在本月活跃的是ech0Raix勒索软件，由于被加密文件后缀会被修改为encrypt而成为关键词。该家族针对网络存储设备NAS进行攻击，主要通过弱口令攻击以及漏洞攻击进行传播。

数据来源：360勒索病毒搜索引擎

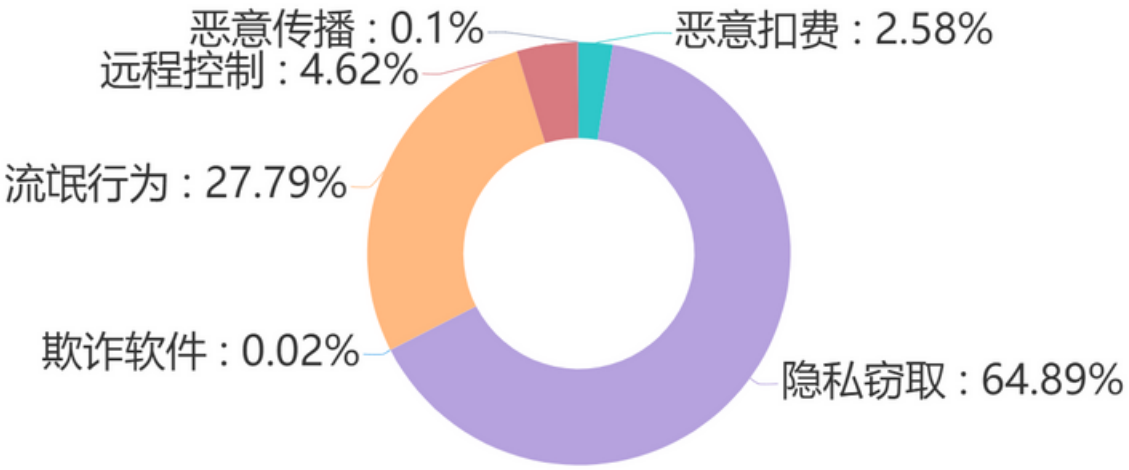
五、解密大师

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Stop家族加密的设备，其次是被Crysis家族加密的设备。

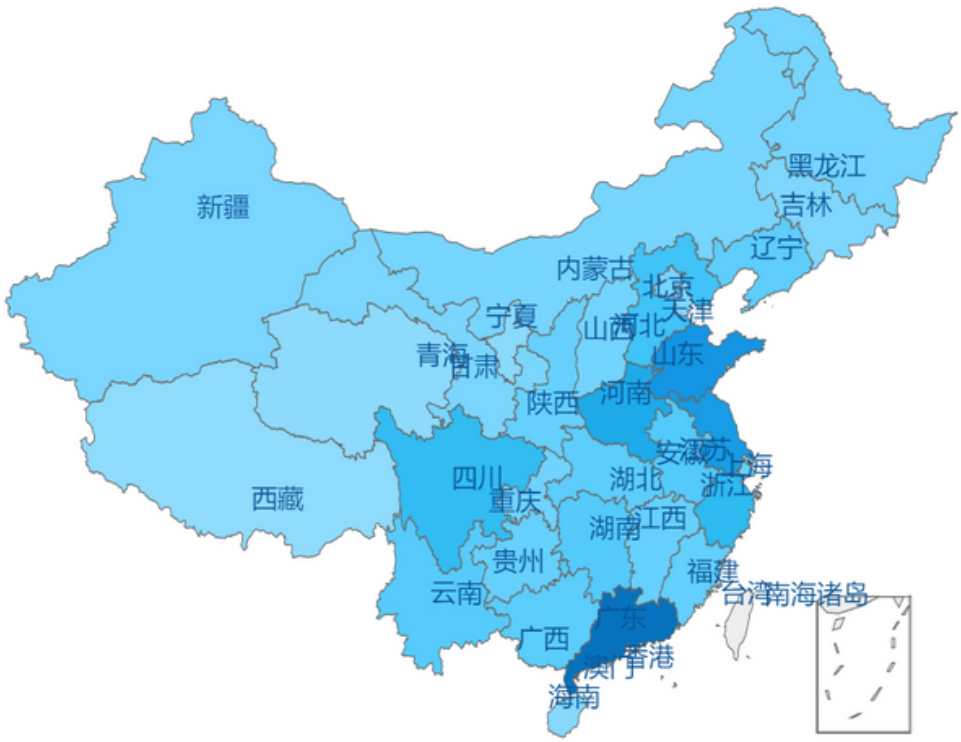
数据来源：反勒索服务统计数据

移动安全数据分析

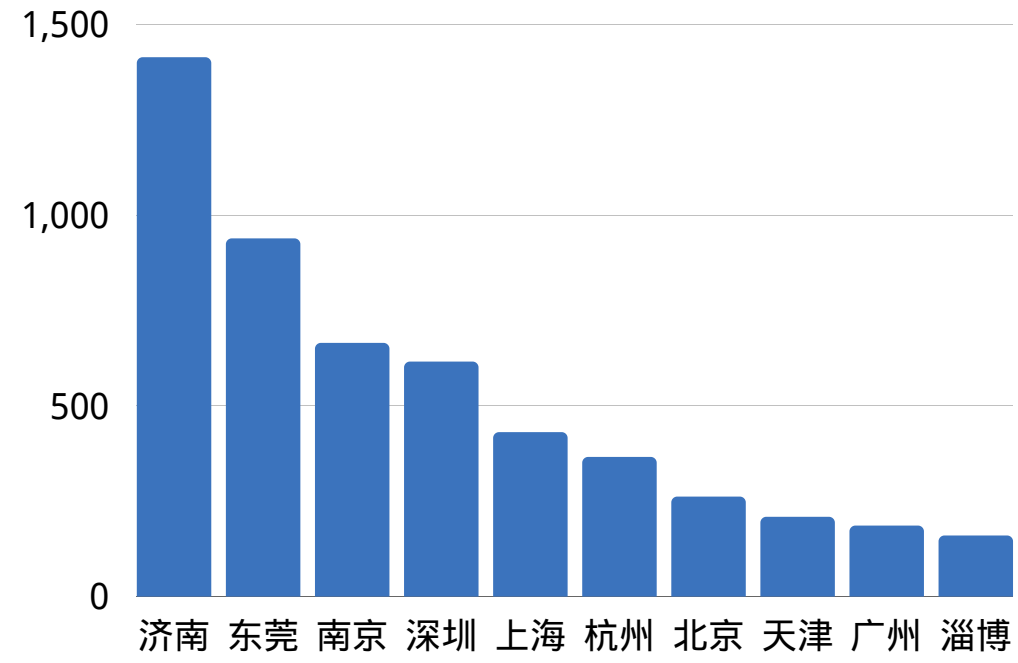
Mobile Security Data Analysis



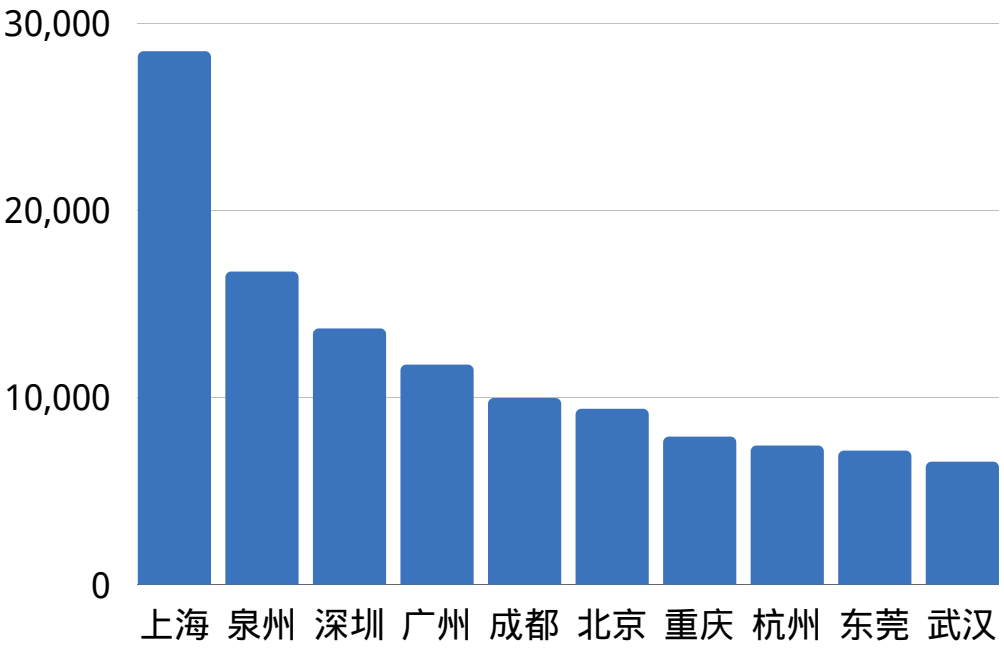
数据总览



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

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

2021.08

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