总第8期

2021年11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-2021-42321:微软Exchange Server远程代码执行漏洞
Windows Installer 权限提升漏洞
APT组织利用CVE-2021-40539漏洞瞄准关键部门
印APT组织蔓灵花针对巴基斯坦政府机构展开定向攻击
黑客在Gmail和Instagram钓鱼欺诈中利用Microsoft MSHTML漏洞
50%的GitLab安装仍然受到RCE漏洞的影响
Cloudflare缓解了迄今为止最大的DDoS攻击
Sea Mar医疗数据被盗影响68万患者
Magniber勒索软件升级，瞄准国内用户
Conti勒索病毒团伙策划让Emotet僵尸网络卷土重来
“阎罗王”勒索软件正驶入攻击美国金融部门

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11月，360CERT共收录28个漏洞，其中严重8个，高危15个，中危5个。主要漏洞类型包含特权提升、代码执行、UAF、拒绝服务等。涉及的厂商主要是Apache、Linux、VMware、Windows、Google等。

二、安全事件

本月收录安全事件278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、Twitter、Facebook、Apple、FBI、YouTube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、医疗行业、交通运输业等。

三、恶意程序

2021年11月，全球新增的活跃勒索病毒家族有：Doyuk2、HarpoonLocker、Rozbeh、BlackCocaine、Cryt0y、Flowey、54BB47H (Sabbath)、Entropy、ROOK、RobinHood、AvGhost等勒索病毒家族，其中54BB47H (Sabbath)、Entropy、ROOK、RobinHood四个家族为本月新增的双重勒索病毒家族；本月最值得关注的勒索病毒Magniber，该勒索病毒家族通过网页挂马疯狂传播；老牌勒索家族Snatch也开始采用双重勒索模式运营;AvGhost勒索软件针对服务器进行攻击，虽然受害者联系到黑客后，黑客表示此次攻击只是测试并承诺替用户免费解密文件，但实际结果是受害者仍有大量数据无法恢复。

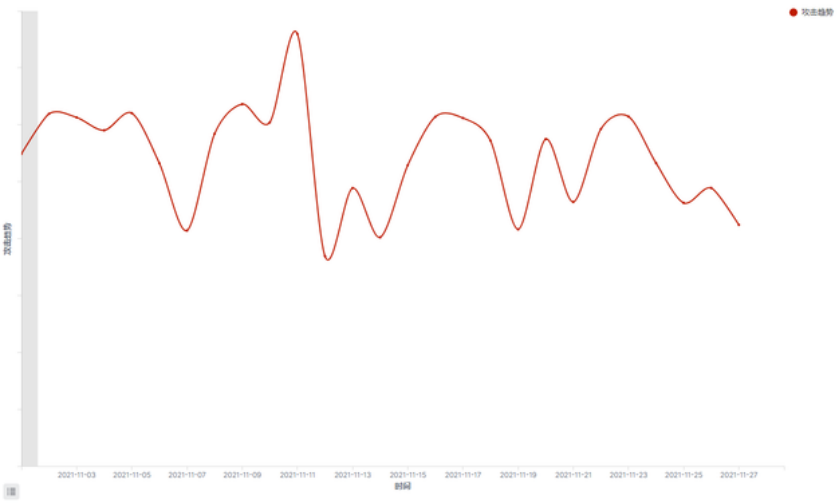
通过隐私窃取拦截量TOP10来看，广州、上海、成都这三个省份移动端隐私窃取数量占据前列，基本上可以体现人口越集中、经济越发达、移动设备使用数量越多的省份，软件恶意行为更加猖獗、恶意软件存活比例越大。

本月攻击态势

Attack situation analysis

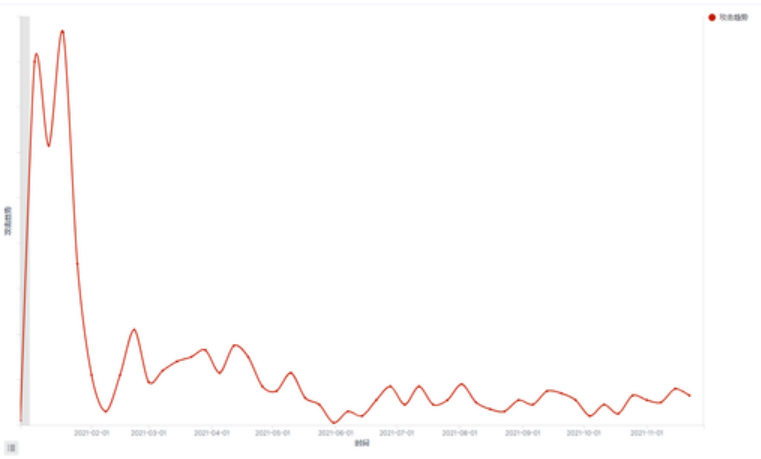
一、僵尸网络攻击

11月份Windows平台僵尸网络总体攻击趋势相对较为平稳，未见较大幅度的增长或减少。



11月份僵尸网络攻击趋势

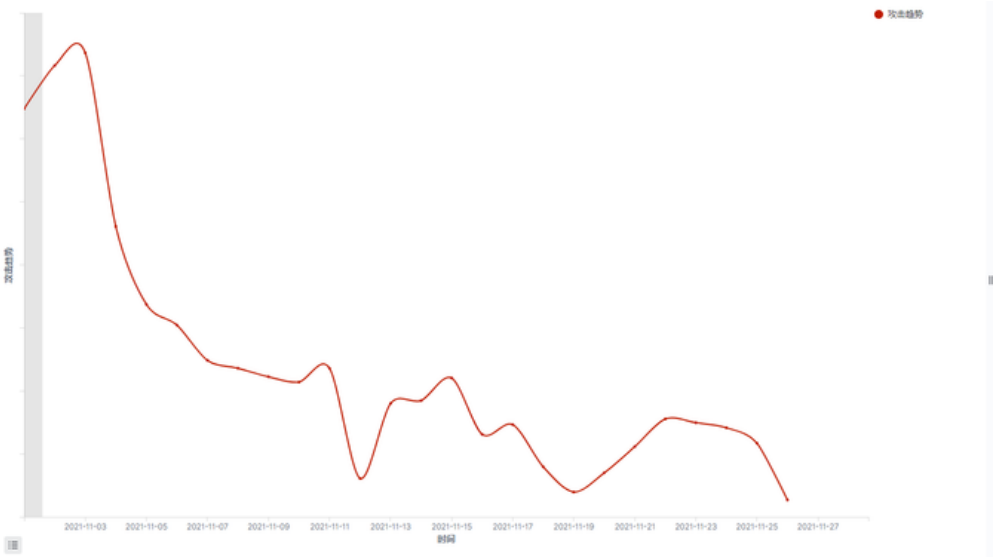
本月需要关注的是，Emotet僵尸网络在停摆了多月之后，于本月再次出现传播，疑似其部分运营者重启了该僵尸网络的运作。今年年初，欧洲刑警组织宣布关闭了Emotet僵尸网络的关键基础设施，这也使得Emotet僵尸网络攻击趋势出现断崖式下降。虽然本月Emotet僵尸网络重启，但根据360安全大脑的监测数据显示， Emotet重启后传播规模并不大。下图展示了今年Emotet僵尸网络的攻击趋势。



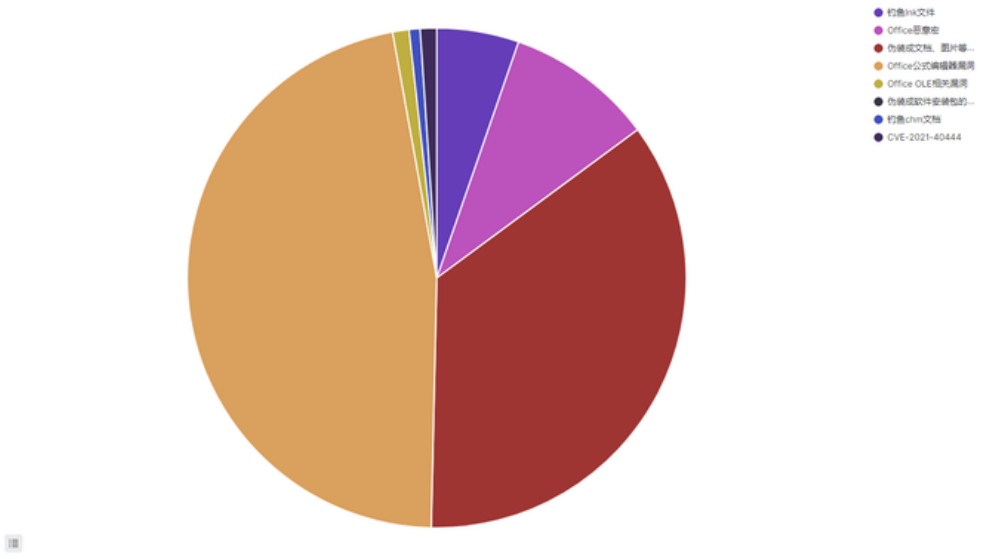
2021年Emotet僵尸网络攻击趋势

二、钓鱼邮件攻击

在经历了10月底至11月初“看门狗”黑产团伙猛烈的钓鱼攻击后，11月的钓鱼攻击趋势开始逐步下降。“看门狗”黑产团伙也在本月逐步停止了针对特定人群的钓鱼攻击。



11月份钓鱼邮件攻击趋势

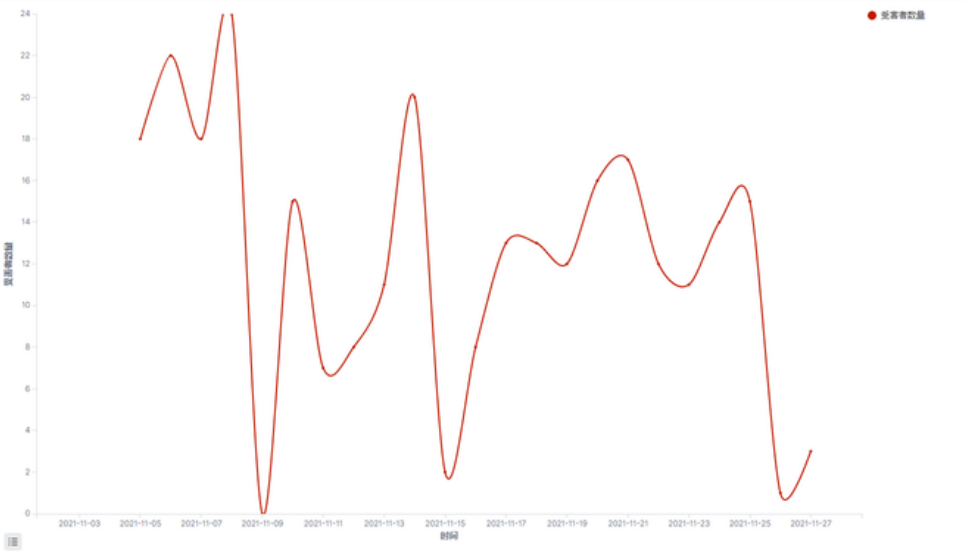


11月份钓鱼攻击方式分布

在攻击方式分布上，本月主要以Office公式编辑器漏洞利用为主，黑产团伙利用该漏洞传播Lokibot、Agenttesla等窃密木马。此外，伪装成文档、图片等的可执行文件和Office恶意宏也是攻击者在本月使用较多的攻击方式。

三、网页挂马攻击

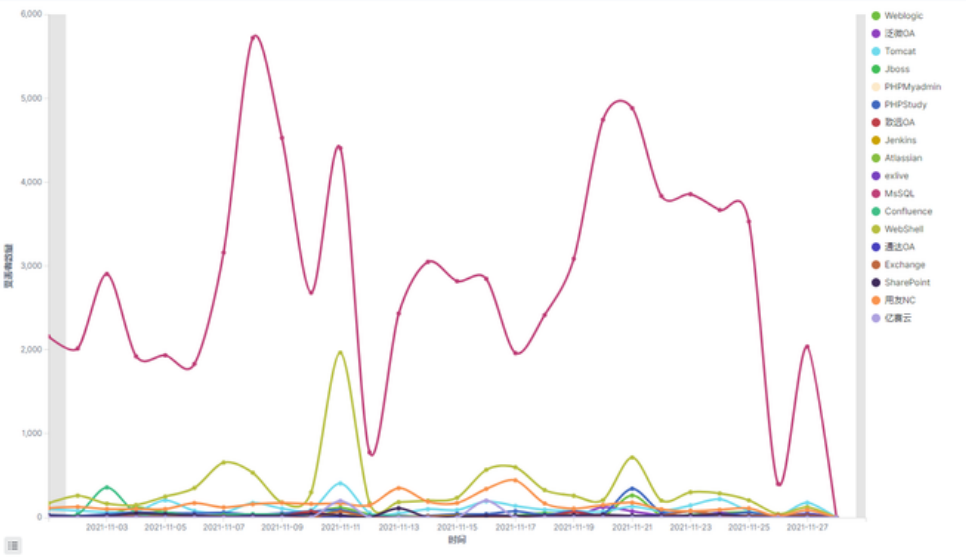
本月初，有黑客团伙使用Magnitube EK 漏洞利用套件在网页广告中植入CVE-2021-40444漏洞利用代码，传播Magniber勒索病毒。由于部分广告页面在访问量较大的色情网站中被展示，此次攻击对不少用户造成了影响。下图展示了本月遭到CVE-2021-40444挂马攻击的受害者数量变化趋势。



11月遭到CVE-2021-40444挂马攻击的受害者数量变化趋势

四、针对Web应用和数据库的攻击

本月针对Web应用和数据库的攻击趋势与上个月相比未有较大变化。其中最为活跃的还是SQLGlobelimposter，该团伙通过爆破MSSQL数据库入侵服务器，并根据情况在服务器中植入挖矿木马、远控木马或勒索病毒。该团伙在本月平均每天入侵超过1000台服务器。



11月份针对Web应用和数据库的各类攻击趋势

安全漏洞

VULNERABILITIES

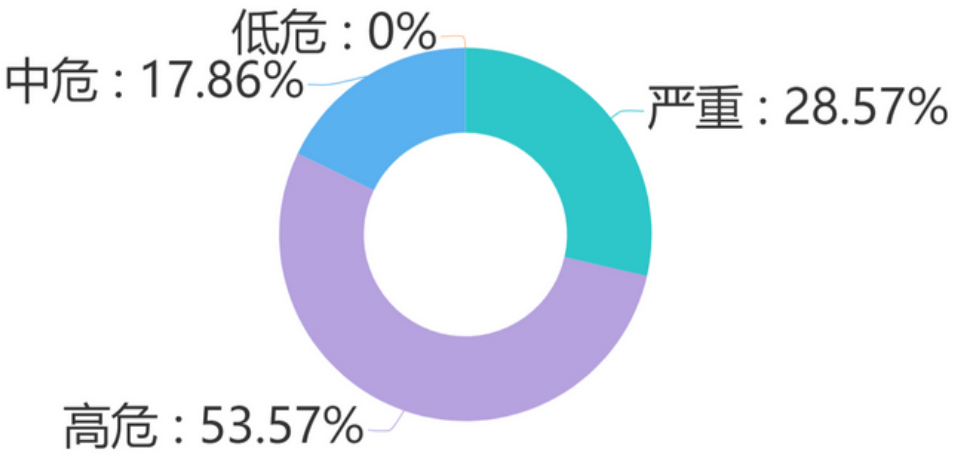
前言

2021年11月，360CERT共收录28个漏洞，其中严重8个，高危15个，中危5个。主要漏洞类型包含特权提升、代码执行、UAF、拒绝服务等。涉及的厂商主要是Apache 、Linux、VMware、Windows、Google等。

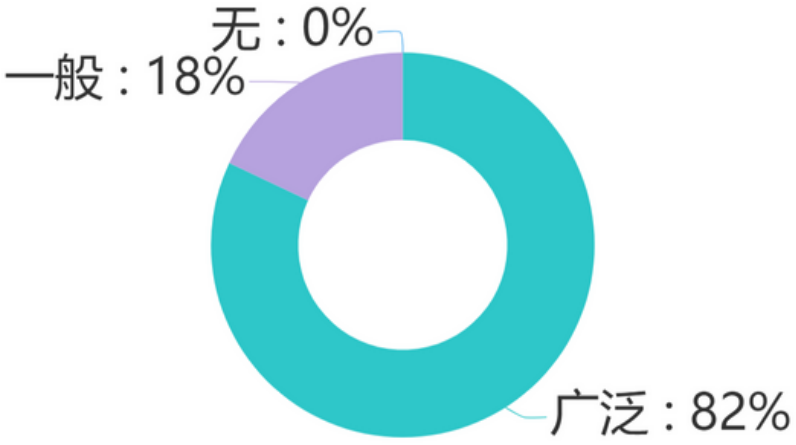
目录预览

漏洞图表

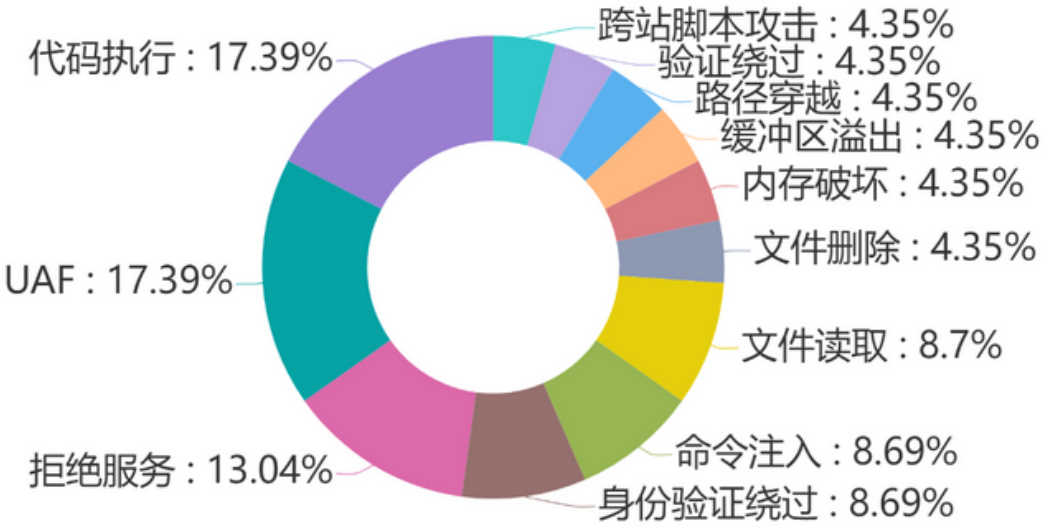
Charts Of Vulnerabilities



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

Intel
Apache Storm
Chrome
metabase
Windows Desktop
Linux
Exchange Server
SonarQube
PAN-OS
VMware vCenter Server
Windows Installer

热门组件

重点漏洞回顾

Review Of Vulnerabilities

CVE-2021-42321:微软Exchange Server远程代码执行漏洞

评分：8.8安全补丁暂未发布

2021年11月22日，360CERT监测发现微软Exchange Server的poc已在互联网公开，漏洞编号为CVE-2021-42321，漏洞等级：严重，漏洞评分：8.8。Exchange Server是一个设计完备的邮件服务器产品， 提供了通常所需要的全部邮件服务功能。经过身份验证的攻击者，可以在Exchange Server上执行代码。目前该漏洞相关poc已公开。

Windows Installer 权限提升漏洞

评分：7.8 安全补丁暂未发布

2021年11月24日，360CERT监测发现Windows Installer权限提升漏洞的POC已公开，该漏洞为CVE-2021-41379补丁的绕过，目前暂无漏洞编号，漏洞等级：高危，漏洞评分：7.8。微软在 2021 年 11 月的补丁星期二发布了CVE-2021-41379的补丁，本次漏洞可造成对该补丁的绕过，是一个本地特权提升漏洞，攻击者利用该漏洞，能够提升到高权限用户组。

CVE-2021-43267:Linux Kernel TIPC远程代码执行漏洞

评分：9.8 安全补丁已发布

2021年11月29日，360CERT监测发现Linux Kernel TIPC 远程代码执行的POC已公开，漏洞编号为CVE-2021-43267，漏洞等级：严重，漏洞评分：9.8。在 5.14.16 之前的 Linux 内核中的 net/tipc/crypto.c 中发现了一个漏洞。透明进程间通信 (TIPC) 功能允许远程攻击者利用用户提供的 MSG_CRYPTO 消息类型大小验证不足的问题。该漏洞是一个堆溢出漏洞，攻击者可以远程或本地利用此漏洞以执行任意代码，获取内核权限，从而攻击整个系统。

CVE-2021-3064：PAN-OS 远程代码执行漏洞

评分：9.8 安全补丁已发布

2021年11月11日，360CERT监测发现Palo Alto 官方发布了PAN-OS: GlobalProtect接口和网关接口内存破坏漏洞的风险通告，漏洞编号为CVE-2021-3064，漏洞等级：严重，漏洞评分：9.8。该漏洞仅影响启用了GlobalProtect的PAN-OS防火墙配置。PAN-OS 的 GlobalProtect 接口和网关接口存在内存破坏漏洞，使未经身份验证的基于网络的攻击者能够扰乱系统进程，并可能使用root权限执行任意代码，攻击者必须通过网络访问GlobalProtect接口才能利用这个漏洞。

CVE-2021-21980：VMware vCenter Server任意文件读取漏洞

评分：9.9 安全补丁已发布

2021年11月25日，360CERT监测发现VMware发布了vCenter Server的安全更新，漏洞编号为CVE-2021-21980，漏洞等级：高危，漏洞评分：7.5。VMware vCenter Server可集中管理 VMware vSphere 环境，与其他管理平台相比，极大地提高了 IT 管理员对虚拟环境的控制。vSphere Web Client (FLEX/Flash) 包含一个未经授权的任意文件读取漏洞。对 vCenter Server 上的 443 端口具有网络访问权限的黑客可利用此漏洞来获取敏感信息。

CVE-2021-41277: Metabase 任意文件读取漏洞

评分：9.9 安全补丁已发布

2021年11月22日，360CERT监测发现Metabase 任意文件读取漏洞的poc已在互联网公开，漏洞编号为CVE-2021-41277，漏洞等级：严重，漏洞评分：9.9。Metabase是一个开源的数据分析平台，通过给公司成员提问，从得到的数据中进行分析、学习。在受影响的版本中，自定义GeoJSON地图(' admin->settings->maps->custom maps->add a map ')存在本地文件包含(包括环境变量)漏洞，url在加载之前没有经过验证，攻击者利用该漏洞能够读取任意文件。

Hadoop Yarn RPC未授权访问漏洞

评分：7.8 安全补丁已发布

2021年11月23日，360CERT监测发现Hadoop Yarn RPC未授权访问漏洞的poc与漏洞细节均已在互联网公开，并且该漏洞存在在野利用，漏洞等级：高危，漏洞评分：7.8。Hadoop Yarn默认对外开放RPC服务且不需要身份认证，攻击者在未授权的情况下可以编写Yarn Client并且向Apache Hadoop Yarn RPC Serve提交Application，利用RPC服务执行任意命令，进而控制服务器。同时由于Hadoop Yarn RPC服务访问控制机制开启方式与REST API不一样，因此即使在 REST API有授权认证的情况下，RPC服务所在端口仍然可以未授权访问。

漏洞时间线

Timeline Of Vulnerabilities

2021-11-02

CVE-2021-37997 高危
Chromium UAF漏洞

CVE-2021-41973 中危
MINA 拒绝服务漏洞

2021-11-04

CVE-2021-38504 高危
Thunderbird UAF漏洞

CVE-2021-41174 中危
Grafana 跨站脚本攻击漏洞

CVE-2021-1924 严重
qualcomm 身份验证绕过漏洞

2021-11-05

CVE-2021-40113 严重
PON Switch 命令注入漏洞

2021-11-08

CVE-2021-43267 严重
Linux 代码执行漏洞

2021-11-09

CVE-2021-25219 中危
BIND 拒绝服务漏洞

2021-11-10

CVE-2021-38666 严重
Windows Desktop 代码执行漏洞

CVE-2021-26443 严重
Virtual Machine Bus 代码执行漏洞

CVE-2021-42321 高危
Exchange Server 代码执行漏洞

CVE-2021-42292 高危
Excel 验证绕过漏洞

2021-11-11

CVE-2021-3064 严重
PAN-OS 内存破坏漏洞

CVE-2021-38294 严重
Apache Storm 命令注入漏洞

CVE-2021-42385 中危
BusyBox UAF漏洞

CVE-2021-22048 高危
Cloud Foundation 特权提升漏洞

2021-11-15

CVE-2020-27986 高危
SonarQube 身份验证绕过漏洞

2021-11-16

CVE-2021-0157 高危
Intel 特权提升漏洞

2021-11-18

CVE-2021-38008 高危
chrome UAF漏洞

CVE-2021-22101 中危
VMware Tanzu Application Service 拒绝服务漏洞

CVE-2021-42705 高危
PLC Editor 缓冲区溢出漏洞

CVE-2021-42021 高危
Siemens Siveillance Video DLNA Server 路径穿越漏洞

2021-11-22

CVE-2021-41277 严重
metabase 文件读取漏洞

2021-11-24

CVE-2021-41379 高危
Windows Installer 特权提升漏洞

CVE-2021-44140 高危
JSPWiki 文件删除漏洞

2021-11-25

CVE-2021-21980 高危
VMware vCenter Server 文件读取漏洞

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

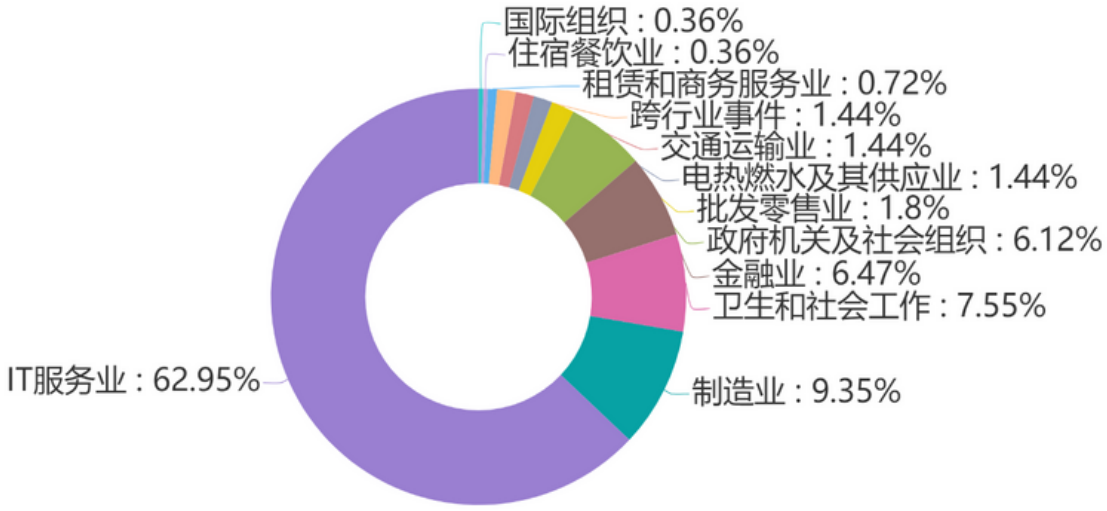
前言

本月收录安全事件278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、Twitter、Facebook、Apple、FBI、YouTube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、医疗行业、交通运输业等。

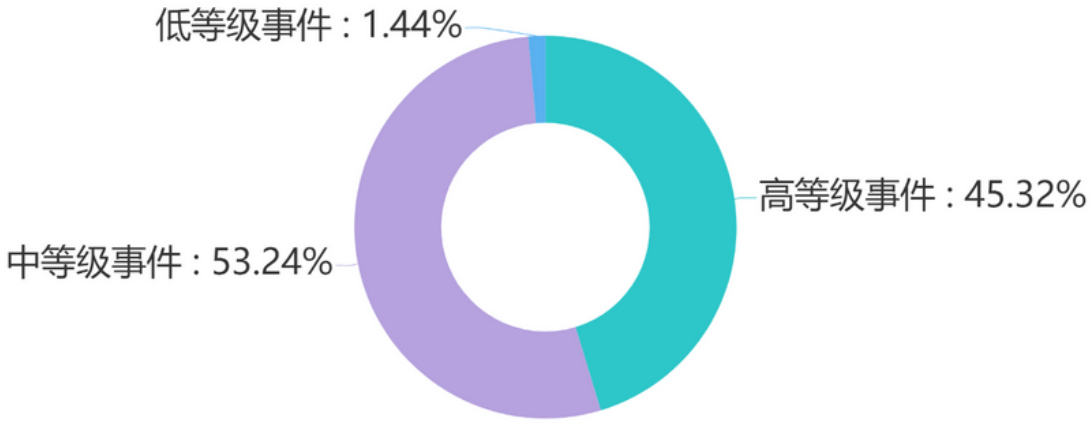
目录预览

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

APT-C-59（芜琼洞）组织2021年攻击行动揭秘

标签：APT-C-59, C2, APT
链接：https://mp.weixin.qq.com/s/WBpML3BTxFPHmBgyunmEEA

2021年上半年，360高级威胁研究院发现了来自同一个新APT组织的多起攻击活动，根据该组织的攻击特征分析显示，我们发现其相关攻击行动未与目前已知APT组织关联，同时我们观察到该组织的两次攻击行动中都使用了0day漏洞攻击手段，所以将其背后的攻击者命名编号为APT-C-59（芜琼洞）。APT-C-59（芜琼洞）组织的最早的攻击活动可以追溯到2020年8月，早期该组织就利用了部分浏览器的伪协议0day漏洞攻击我国相关单位，同时还攻击了越南地区的部分受害者。通过攻击数据综合分析，我们可以看到该组织的攻击目标地区是以东亚和东南亚为主，涉及政府、智库、媒体、医疗多个行业。

疑似APT-C-55（Kimsuky）组织利用商业软件Web Browser Password Viewer进行攻击

标签：APT-C-55, C2, APT
链接：https://mp.weixin.qq.com/s/QDI912ogVKyyKFYdKvBGdQ

近日，360高级威胁研究院在日常高价值样本狩猎过程中，捕获疑似Kimsuky组织利用利用商业软件Web Browser Password Viewer进行测试的样本，疑似测试功能是收集用户浏览器密码信息，可见该APT组织再次活跃并“蠢蠢欲动”。根据研究人员跟踪分析，此次活动有如下特点： 此次捕获样本疑似在测试阶段，功能尚不完善。初始载荷与近期Kimsuky组织投递的hancom载荷样本有所差异。 样本利用RC4+ZLIB解密出后续载荷, 载荷后续注入到svchost.exe进程中。 第二阶段载荷利用开源商业软件Web Browser Password Viewer进行更改，疑似测试功能为收集用户浏览器密码信息。 本次捕获样本并没有进行持久化的的注册表写入操作，收集的信息，也没有相关上传操作。

针对我国和南亚次大陆等国家的钓鱼攻击活动分析

标签： C2, APT
链接：https://mp.weixin.qq.com/s/CGHDuJAb4dav_th25yYpWA

2021年3月份以来，安天捕获了多起针对我国和部分南亚次大陆国家等的钓鱼攻击活动，该活动涉及网络节点数目众多，主要攻击目标为中国、尼泊尔、巴基斯坦、斯里兰卡、孟加拉国、阿富汗以及马尔代夫等国家的政府、国防军事以及国企单位。攻击者会将自身伪装成目标国家的政府或军队人员，向对方邮箱投递挂有钓鱼附件或嵌有钓鱼链接的攻击邮件，并诱导目标通过链接访问攻击者通过各种方式搭建的钓鱼网站，收集受害者输入的账号密码以供情报收集或横向攻击所用。

分析KIMSUKY组织的新后门APPLESEED

标签：KIMSUKY, C2, APT
链接：https://www.telsy.com/dissecting-new-appleseed-backdoor-of-kimsuky-threat-actor/

Telsy威胁情报小组追踪各种威胁组织，其中包括名为Kimsuky的网络间谍组织，该组织至少从2012年就开始活跃，据信是代表朝鲜政府运作的。 该组织因在世界各地发动网络攻击而臭名昭著，其中包括针对韩国智库的攻击行动，但在过去几年里，他们已将目标扩大到美国、俄罗斯和欧洲等多个国家。Kimsuky使用各种钓鱼和社会工程方法来获得进入受害者网络的初始权限。在电子邮件中嵌入恶意附件是Kimsuky最常用的战术。

相煎何急，印APT组织蔓灵花针对巴基斯坦政府机构展开定向攻击

标签：CETARAT, C2, APT
链接：https://blogs.quickheal.com/cetarat-apt-group-targeting-the-government-agencies/

CetaRAT首次出现在SideCopy APT攻击行动中，现在它正在不断扩大其活动。Quick Heal已经跟踪这个RAT很长时间了，发现其增加了针对印度政府机构的攻击。CetaRAT攻击链始于带有恶意附件的鱼叉式网络钓鱼邮件。附件是一个zip文件，可以从远程的、被攻陷的URL下载一个HTA文件。一旦这个HTA文件通过mshta.exe启动，就会下载并执行CetaRAT有效载荷，与C2进行通信。

朝鲜TA406组织攻击活动分析

标签： TA406,C2, APT
链接：https://www.proofpoint.com/us/blog/threat-insight/triple-threat-north-korea-aligned-ta406-scams-spies-and-steals

Proofpoint的研究人员将Kimsuky组织分成三个小组来跟踪，分别是：TA406、TA408和TA427。TA406从事间谍活动和网络犯罪，经常针对研究、教育、政府、媒体和其他组织开展证书盗窃活动。TA406通常不会在攻击活动中使用恶意软件。然而2021年，该组织在两个值得注意的活动中试图分发可用于收集信息的恶意软件。

Kimsuky利用恶意博客向韩国智库人员分发恶意软件

标签： Kimsuky, C2, APT
链接: https://blog.talosintelligence.com/2021/11/kimsuky-abuses-blogs-delivers-malware.html

思科Talos最近发现了朝鲜Kimsuky APT组织的一起攻击活动，该组织向韩国的高价值目标——地缘政治和航空航天研究机构，发送恶意软件。攻击活动至少从2021年6月开始，使用了Gold Dragon/Brave Prince家族的植入物。攻击者在这次活动中使用博客来托管他们的恶意软件。

ScarCruft组织监视朝鲜叛逃者和人权活动人士

标签： ScarCruft, C2, APT
链接: https://securelist.com/scarcruft-surveilling-north-korean-defectors-and-human-rights-activists/105074/

ScarCruft组织(也被称为APT37或Temp.Reaper)是卡巴斯基在2016年首次披露的一个具有国家背景的APT组织。最近，一家新闻机构请求卡巴斯基在其网络安全调查期间提供技术援助。因此，卡巴斯基有机会对被ScarCruft破坏的主机进行更深入的调查。受害者被PowerShell恶意软件攻击，有证据表明，该组织已经从受害者那里窃取了数据，并监视了受害者几个月。

重点事件回顾

Review Of Incidents

恶意程序事件

APT组织利用CVE-2021-40539漏洞瞄准关键部门

跨行业事件

2021 年 9 月 16 日，美国网络安全和基础设施安全局 (CISA) 发布警报警告，高级持续威胁 (APT) 组织正在大肆利用自助密码管理和单点登录解决方案中新发现的漏洞，称为ManageEngine ADSelfService Plus。早在9月17日，攻击者就利用在美国租用的基础设施扫描互联网上数百个易受攻击的组织。随后，利用尝试于 9 月 22 日开始，并可能持续到 10 月初。在那期间，攻击者成功地攻陷了技术、国防、医疗保健、能源和教育行业的至少九个全球实体。

Lazarus黑客团伙用木马程序IDA Pro攻击研究人员

IT服务业

一个被称为“Lazarus”的北朝鲜政府支持的黑客团伙再次试图攻击安全研究人员，这次他们使用的是广受欢迎的IDA pro逆向工程应用程序的木马盗版版本。IDA pro是一个将可执行文件转换成汇编语言的应用程序，允许安全研究人员和程序员分析程序的工作方式并发现潜在的错误。然而，由于IDA pro是一个昂贵的应用程序，一些研究人员下载盗版破解版本而不是购买它。

APT C-23黑客使用新安卓间谍软件变种瞄准中东用户

国际组织

以攻击中东目标而闻名的黑客组织 APT-C-23 再次改进了其 Android 间谍软件，增强了隐蔽性和持久性，能够伪装成看似无害的应用程序，在用户Android终端上长期地潜伏。新变种在其恶意应用程序中加入了新的功能，使其更能抵御用户的行动，用户可能会试图手动删除它们，安全公司和网络托管公司试图阻止访问或关闭它们的命令和控制服务器域。至少自2017年以来，该手机间谍软件一直是APT C-23黑客的首选工具。

黑客在Gmail和Instagram钓鱼欺诈中利用Microsoft MSHTML漏洞

IT服务业

这些攻击始于2021年7月，攻击者利用Microsoft MSHTML漏洞攻击海外伊朗人。SafeBreach实验室的研究人员发现了一个新的伊朗攻击者，试图窃取全球波斯语使用者的Instagram和Gmail登录凭证。攻击者正在使用一种新的基于powershell的窃取工具，被SafeBreach实验室称为PowerShortShell。

超过30万安卓用户下载了这些银行特洛伊木马恶意软件应用

IT服务业

超过30万安卓智能手机用户在成为绕过谷歌Play应用商店检测的恶意软件的受害者后，下载了被证明是银行特洛伊木马的软件。四种不同形式的恶意软件通过通常下载的应用程序的恶意版本，包括文档扫描仪、二维码阅读器、健身监视器和加密货币应用程序，向受害者交付。这四个恶意软件分别是：Anatsa、Alien、Hydra和Ermac。这些应用程序通常附带一些功能，这些功能都是为了避免用户产生怀疑而发布的。在每种情况下，应用程序的恶意意图都是隐藏的，只有在安装应用程序后，才会开始交付恶意软件，从而使他们能够绕过Play Store检测。

数据安全事件

Sea Mar医疗数据被盗影响68万患者

医疗行业

根据提供商网站上发布的违规通知，在2020年12月开始的长达数月的系统黑客攻击之后，688,000 名Sea Mar 社区健康中心患者的个人和健康数据被访问、泄露和在线泄露。Sea Mar 是一个非营利实体，为华盛顿服务不足的患者提供服务。一项取证分析发现，在 2020 年 12 月至 2021 年 3 月之间，也就是发现数据之前的几个月，从受影响的系统中删除了其他数据。被盗数据因人而异，包括姓名、联系人、社会安全号码、出生日期、客户身份号码、治疗信息、保险详情、索赔数据和牙齿图像。

GoDaddy遭遇黑客攻击导致数据泄露影响120万客户

IT服务业

在2021年11月22日发布的一份数据泄露通知中，GoDaddy表示，在黑客进入该公司托管的wordpress主机环境后，多达120万用户的数据被泄露。GoDaddy公司于11月17日发现这起攻击，但攻击者至少从2021年9月6日起就进入了该公司的网络，并获取了被入侵系统中的数据。多达120万活跃和不活跃的wordpress管理客户的电子邮件地址和客户号码被公开。此次事件影响了几家受管理的WordPress服务经销商，包括tsoHost、Media Temple、123Reg、Domain Factory、Heart Internet和Host Europe。

网络攻击事件

50%的GitLab安装仍然受到RCE漏洞的影响

IT服务业

网络安全研究人员警告称，在gitlab的web界面中，有一个已被修复的严重远程代码执行(rce)漏洞，漏洞编号为cve-2021-22205，该漏洞在野外被积极利用。
在 60,000 个面向互联网的 GitLab 安装中：
21% 的安装已针对此问题进行了全面修补。
50% 的安装未针对此问题进行修补。
29% 的安装可能存在漏洞，也可能不存在漏洞。

乌克兰将Gamaredon黑客组织成员与俄罗斯联邦安全局联系起来

政府机关及社会组织

苏和乌克兰特勤局表示，他们已经确认了 Gamaredon 黑客组织的五名成员，该组织是俄罗斯政府支持的组织，自2014年以来一直以乌克兰为目标。自行动开始以来，被认为对乌克兰境内的5000多起攻击负责。乌克兰表示，在过去7年里，恐怖分子袭击了该国1500多个政府、公共和私人实体，目的是收集情报、扰乱行动，并控制关键的基础设施。

Cloudflare缓解了迄今为止最大的DDoS攻击

IT服务业

Cloudflare是一家美国网络基础设施和网站安全公司，提供内容分发网络和ddos缓解服务。该公司宣布已经缓解了分布式拒绝服务(ddos)攻击，该攻击峰值低于每秒2tb (tbps)，这是cloudflare迄今为止遇到的最大的攻击。这是一个结合了DNS放大攻击和udp flood的多矢量攻击。整个袭击只持续了一分钟。这次攻击是由大约15000个在物联网设备和未打补丁的gitlab实例上运行原始mirai僵尸网络发起的。

新的Chinotto间谍软件以朝鲜叛逃者、人权活动家为目标

政府机关

朝鲜叛逃者、报道朝鲜相关新闻的记者和在韩国的实体正被国家支持的apt组织攻击。卡巴斯基将此次入侵归因于一个被追踪到的朝鲜黑客组织，该组织名为scarcruft，也被称为apt37，reaper group，inkysquid和ricochet chollima。该组织使用了三种具有类似功能的恶意软件:powershell版本，Windows可执行程序和android应用程序。

其他事件

600万Sky路由器在17个月内面临接管攻击

IT服务业

英国约有600万台Sky宽带用户路由器受到一个严重漏洞的影响，其官方17个月的时间才向用户推出修复方案。这个公开的漏洞是一个DNS重绑定漏洞，如果用户没有更改默认的管理密码，或者攻击者可以强制使用凭据，那么攻击者可以很容易地利用这个漏洞。这种利用的结果将是危及客户的家庭网络，改变路由器的配置，并可能转移到其他内部设备。

事件时间线

Timeline Of Incidents

2021-11-01

研究人员发现感染了160多万台设备的“Pink”僵尸网络恶意软件
Balikbayan Foxes group欺骗菲律宾政府传播RATs
Snake Infostealer恶意软件窃取凭据，在50多个应用程序截图
FBI：HelloKitty勒索软件将DDoS攻击添加到勒索战术中
BlackShadow黑客入侵以色列主机公司勒索客户
卡巴斯基被盗的亚马逊SES令牌用于Office 365网络钓鱼
鱿鱼游戏加密货币退出骗局!运营商赚了210万美元

2021-11-02

50%面向internet的GitLab安装仍然受到RCE漏洞的影响
多伦多地铁遭到勒索软件袭击
加州诊所网络网络事件影响656000人
谷歌警告在主动目标攻击下新的Android 0-Day漏洞
新恶意软件引诱伪造Chrome更新攻击Windows PC

2021-11-03

TeamTNT升级了武器库，改进了Kubernetes和GPU环境
英国工党披露勒索软件攻击后数据泄露
Free Discord Nitro网络钓鱼主要针对Steam玩家

2021-11-04

Lockean多个勒索软件分支机构与袭击法国组织有关
乌克兰将Gamaredon黑客组织成员与俄罗斯联邦安全局联系起来
CISA通过指令，强制联邦民事机构修复306个漏洞
利用Microsoft Exchange ProxyShell漏洞部署Babuk勒索软件
流行的“coa”NPM库被劫持以窃取用户密码

2021-11-05

勒索失败后，伊朗黑客泄露以色列LGBTQ约会应用程序数据
Mekotio Banker凭借改进的隐形和古老的加密技术回归
针对医疗技术供应商QRS的网络攻击导致32万名患者的数据被盗

2021-11-06
攻击者从bZx DeFi平台窃取了价值5500万美元的加密货币
DanaBot恶意软件活动激增

2021-11-07
部落社区的赌场在勒索软件攻击中损失了数百万

2021-11-08
BlackBerry发现与3个不同黑客集团有联系的初始访问代理
APT组织利用CVE-2021-40539缺陷瞄准关键部门
专家们发现了一个仿冒安全公司Proofpoint的网络钓鱼活动
黑客利用谷歌广告进行凭证窃取和消费账户余额
REvil勒索软件疑犯在全球警方打击行动中被捕
WooCommerce Skimmer伪造结账页面
Black Shadow 泄露以色列患者记录和数据
Sitecore XP RCE漏洞现已被大肆利用

2021-11-09
Hive 勒索软件团伙攻击 MediaMarkt
Robinhood遭到数据泄露和敲诈勒索
Clop团伙利用勒索软件攻击中的SolarWinds Serv-U漏洞
泄露的Docker Hub帐户被滥用，被TeamTNT用于挖矿
伊朗黑客 Lyceum 瞄准电信，ISPS

2021-11-10
墨西哥出现Dridex银行恶意软件
研究人员发现PhoneSpy恶意软件在监视韩国公民
新型安卓恶意软件的目标是Netflix、Instagram和Twitter用户
Medatixx遭到勒索软件攻击，客户需要尽快更改密码
TrickBot与Shatak网络钓鱼者合作进行Conti勒索软件攻击
Lazarus黑客团伙用木马程序IDA Pro攻击研究人员
HPE称黑客使用被盗的访问密钥入侵了Aruba Central
Telnyx遭受DDoS攻击
Void Balaur黑客出售被盗邮箱和私人数据

2021-11-11

谷歌Play上的“Smart TV remote”Android应用程序是恶意软件
黑客在昆士兰水供应商的服务器上隐藏九个月未被发现
Magniber 勒索软件团伙正利用IE漏洞进行攻击
BotenaGo僵尸网络利用33个漏洞攻击数百万物联网设备
Abcbot：一种针对Linux的新型蠕虫僵尸网络恶意软件

2021-11-12

macOS 0Day在香港被利用在水坑攻击用户
理解 .htaccess 恶意软件
Costco 在发现信用卡欺诈后披露数据泄露
Windows 10应用程序安装程序被BazarLoader恶意软件滥用
俄亥俄州医院因遭受网络攻击转移救护车，取消预约

2021-11-13

伪造的端到端加密聊天应用程序分发Android Spyware
美国联邦调查局(FBI)系统被黑客入侵，发送“紧急”邮件警告虚假网络攻击

2021-11-15

Qakbot银行特洛伊木马的感染人数激增
黑客窃取索尼ps5的root密钥
Mac 0day警报：野外水坑攻击
Moses Staff黑客对以色列组织造成严重破坏
阿里云服务器实例被加密挖掘恶意软件主动劫持
Cloudflare缓解了迄今为止最大的DDoS攻击

2021-11-16

NPM修复了私有包名称泄漏、严重授权漏洞
电子欺诈活动呈现出稳步增长的趋势
Emotet恶意软件再次袭来
新银行特洛伊木马SharkBot在欧美掀起波澜
针对中东知名网站的战略网络入侵攻击
成人cam网站StripChat遭遇数据泄漏

2021-11-17
针对中东的ProxyShell相关攻击事件激增
FBI:一个APT在FatPipe VPNs中滥用0day长达6个月
以缅甸为目标的黑客利用域名前置来隐藏恶意活动
美国、英国和澳大利亚警告伊朗黑客利用微软fortinet漏洞

2021-11-18
Tiktok网红成为网络钓鱼活动的目标
RedCurl公司间谍黑客使用更新的工具继续攻击

2021-11-19
11个恶意PyPI Python库被抓到窃取Discord令牌和安装shell
新Memento勒索团伙利用WinRAR加密恶意文件
加州Pizza Kitchen遭遇数据泄露
Sea Mar医疗数据被盗影响68万患者
CKEditor漏洞对Drupal和其他下游应用程序构成XSS威胁
600万Sky路由器在17个月内面临接管攻击
假的TSA预检网站用假的续签合同欺骗美国旅客

2021-11-21
研究人员入侵了Conti gang的支付网站

2021-11-22
伊朗顶级航空公司马汉航空遭受网络攻击
包含敏感数据数千个火狐cookie出现在github存储库中
GoDaddy hack导致数据泄露影响120万客户
犹他州成像协会数据泄露影响583643名患者
风力涡轮机巨头维斯塔斯的数据在网络攻击中受损
Squirrelwaffle利用ProxyShell和ProxyLogon劫持电子邮件链
英国政府警告数千家中小企业他们的在线商店遭到黑客攻击
黑客滥用Glitch平台窃取凭证

2021-11-23
Tardigrade黑客用秘密恶意软件瞄准大型制药疫苗制造商
Wi-Fi管理软件公司泄露数百万巴西人的数据

BazarLoader将受损安装程序、ISO添加到攻击向量中
恶意软件正试图利用新的Windows Installer zero day进行攻击

2021-11-24
当心BrazKing Android恶意软件升级和攻击银行
数据窃取恶意软件影响超过900万台运行华为appgallery的Android设备
APT C-23黑客使用新安卓间谍软件变种瞄准中东用户
新的JavaScript恶意软件悄悄地用RATs感染Windows PC

2021-11-25
新的Linux恶意软件隐藏在日期无效的cron作业中
Linux恶意软件代理攻击电子商务网站并窃取支付数据
GoDaddy数据泄露更新：六家WordPress托管服务经销商受到影响

2021-11-26
海上服务提供商Swire Pacific Offshore被Clop勒索软件袭击
宜家电子邮件系统遭受持续的网络攻击
TrickBot网络钓鱼检查屏幕分辨率以逃避研究人员
在Gmail和Instagram钓鱼欺诈中利用Microsoft MSHTML漏洞
新墨西哥True Health公司的医疗数据被泄露
加密黑客使用Babadeda Crypter使其恶意软件无法检测

2021-11-28
与朝鲜有联系的Zinc集团冒充三星招聘人员，瞄准安全公司

2021-11-29
巴基斯坦国家数据库生物特征数据泄露
新的Chinotto间谍软件以朝鲜叛逃者、人权活动家为目标
黑客使用受损的谷歌云帐户挖掘加密货币
隐秘的WiRTE黑客瞄准中东政府
松下披露网络黑客攻击后数据泄露
活动滥用合法的远程管理工具使用假冒的加密货币网站

2021-11-30

超过30万安卓用户下载了这些银行特洛伊木马恶意软件应用

昆士兰政府能源发电机遭勒索软件袭击

EwDoor僵尸网络瞄准美国公司的AT&T网络边缘设备

Quest的Reposource因影响35万名患者数据泄露而面临患者诉讼

Flubot在芬兰通过短信传播

Yanluowang勒索软件与Thieflock的联系

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11月，全球新增的活跃勒索病毒家族有:Doyuk2、HarpoonLocker、Rozbeh、BlackCocaine、Cryt0y、Flowey、54BB47H (Sabbath)、Entropy、ROOK、RobinHood、AvGhost等勒索病毒家族，其中54BB47H (Sabbath)、Entropy、ROOK、RobinHood四个家族为本月新增的双重勒索病毒家族；本月最值得关注的勒索病毒Magniber，该勒索病毒家族通过网页挂马疯狂传播；老牌勒索家族Snatch也开始采用双重勒索模式运营;AvGhost勒索软件针对服务器进行攻击，虽然受害者联系到黑客后，黑客表示此次攻击只是测试并承诺替用户免费解密文件，但实际结果是受害者仍有大量数据无法恢复。

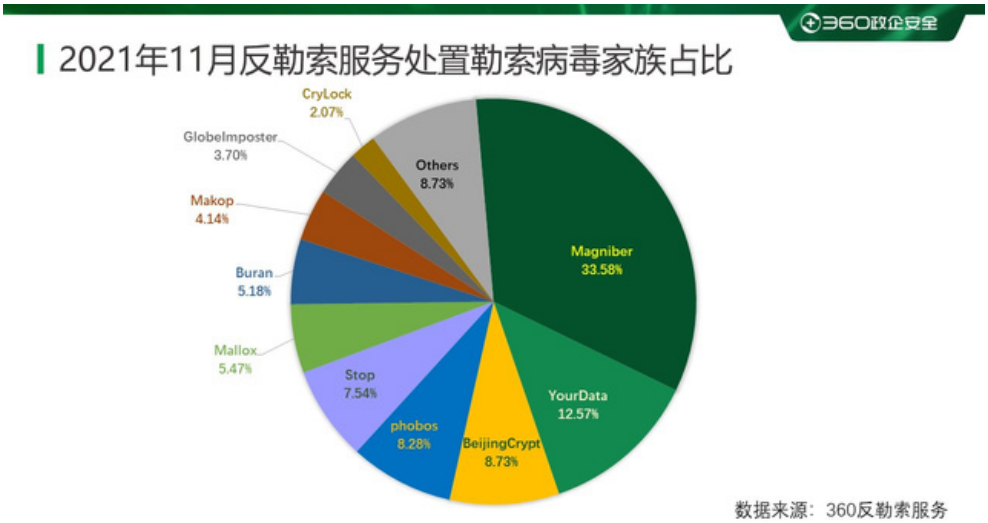
目录预览

勒索病毒态势分析

Ransomware Situation Analysis

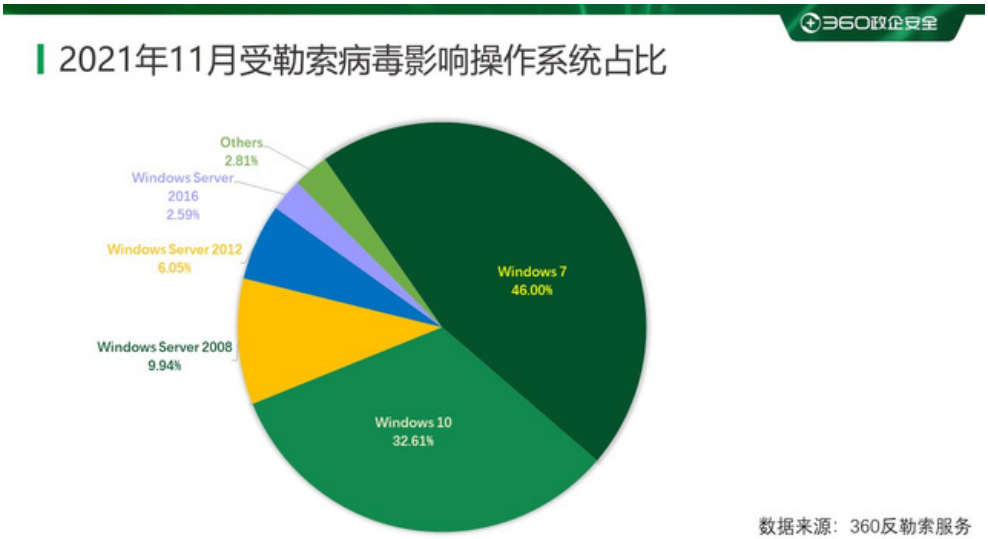
一、感染数据分析

针对本月勒索病毒受害者所中勒索病毒家族进行统计，Magniber家族占比33.58%居首位，其次是占比12.57%的YourData，BeijingCrypt家族以8.73%位居第三。刚做到国内第一的YourData勒索病毒仅仅一个月就被Magniber取代，究其原因并非是YourData传播减弱，而是从11月初开始，Magniber的传播者利用CVE-2021-40444漏洞，在网页广告中插入相关利用代码进行传播，在国内的感染量快速提升。



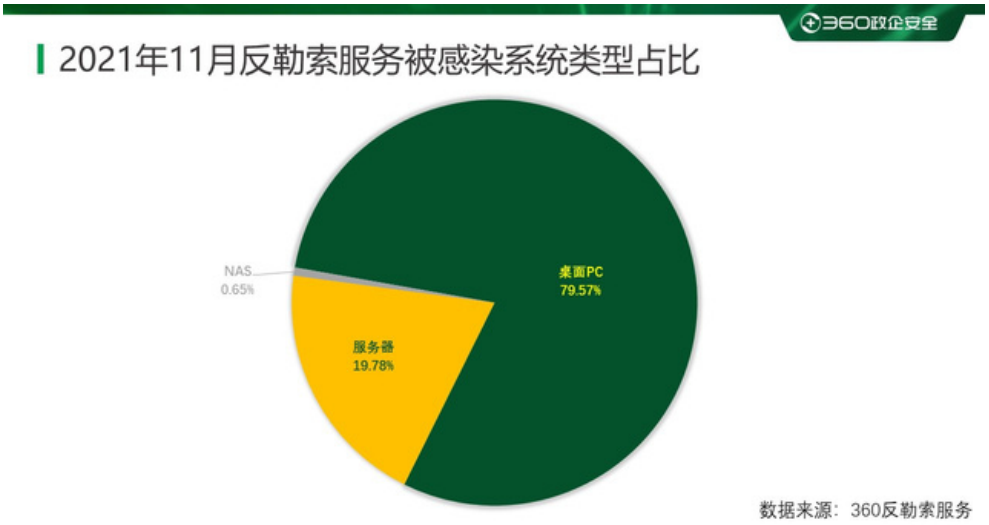
数据来源：360反勒索服务

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 7、Windows 10、以及Windows Server 2008。



数据来源：360反勒索服务

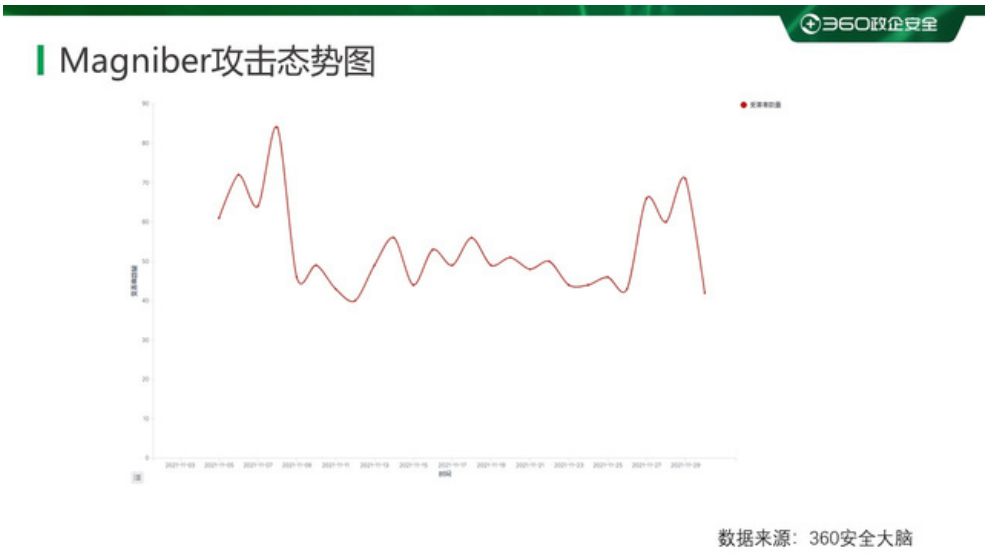
2021年11月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型仍以桌面系统为主。本月被感染的桌面PC与10月相比占比上涨超过18个百分点。这主要因为被Magniber勒索病毒攻击的受害者大部分使用的是桌面PC。



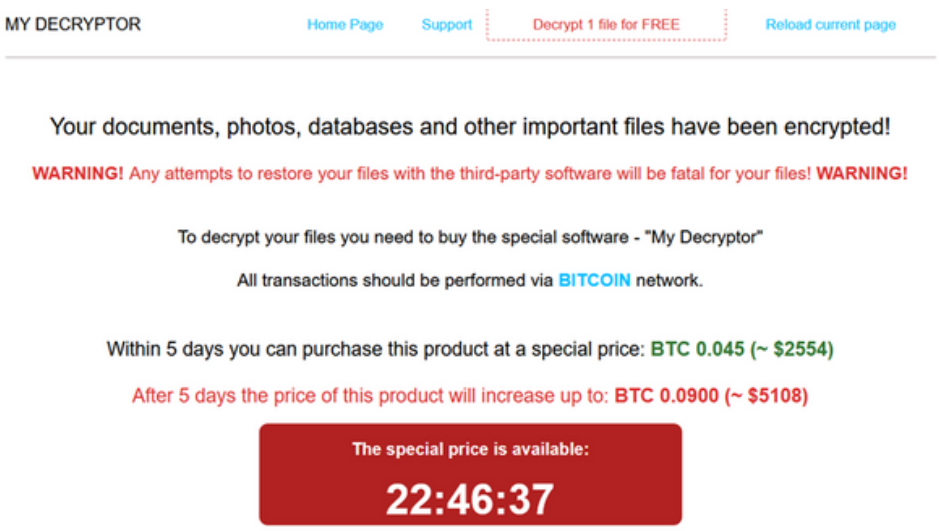
二、勒索病毒疫情分析

Magniber勒索软件升级，瞄准国内用户

11月5日开始，360安全大脑检测到CVE-2021-40444漏洞攻击拦截量有较明显上涨。经过360政企集团高级威胁研究分析中心分析追踪发现，这是一起挂马攻击团伙，利用CVE-2021-40444大肆传播勒索病毒的攻击事件，同时病毒在攻击过程中，还使用了PrintNightmare漏洞进行提权。该黑客团伙主要通过在色情网站、游戏网站（也存在少部分其它网站）的广告位上，投放植入带有攻击代码的广告，当用户访问到该广告页面时，就有可能中招，感染勒索病毒。截止当前360安全卫士仍能拦截到约500次每小时的挂马广告页面访问。而漏洞拦截量，最高单日也已超过1000次。



Magniber勒索软件是基于Magnitude exploit kit（Magnitude EK）开发套件进行开发，早期还曾传播过Locky、Cerber勒索病毒家族。被该勒索加密后，文件后缀将被修改为随机字符串，受害者需向攻击者支付0.044~0.048个比特(价格一直在波动,5天内若未支付，赎金将会翻倍)。



Conti勒索病毒团伙策划让Emotet僵尸网络卷土重来

根据情报公司Advanced Intelligence的消息，知名僵尸网络程序Emotet将被“复活”。而说服此次复活行动的正式Conti勒索病毒团伙的成员。

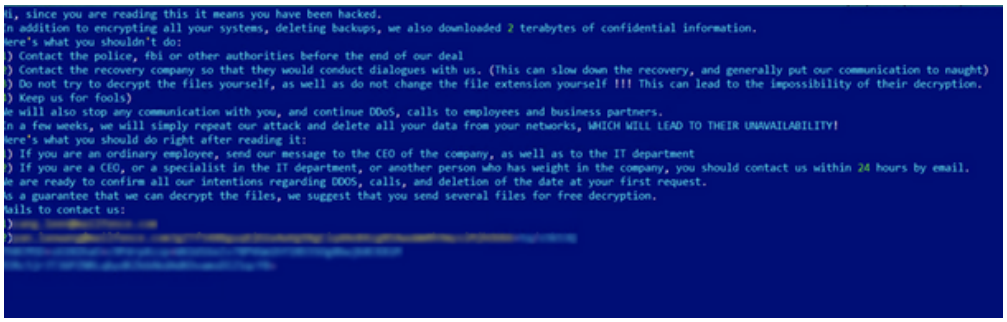
Emotet僵尸网络曾于约10个月前被关闭，而此次“复活”则会重新对分布官方的受控端开启控制。使其充当恶意软件加载程序，为其他恶意软件提供有价值的受感染系统访问权限。而Qbot和TrickBot则是Emotet僵尸网络的主要客户，这两款软件又会利用获取到的访问权限部署包括Conti在内的诸多勒索软件。

在被曝出Conti策划重启Emotet僵尸网络前，该勒索团伙的支付站点和对应域名则均因被劫持导致关闭，但其数据泄露站点页面及域名仍可以正常工作。

“阎罗王”勒索软件正驶入攻击美国金融部门

近日“阎罗王”勒索病毒的下属机构正在尝试使用BazarLoader恶意软件攻击美国金融部门。自从8月份以来，“阎罗王”勒索病毒不仅对金融机构发起攻击，还对制造业、IT服务、咨询及工程领域的公司进行攻击。

该攻击团伙在入侵阶段不仅部署了恶意软件，还尝试从受控设备上收集浏览器保存的登录凭证，例如：Firefox、Chrome、Internet Explorer，以及窃取KeePass密码管理器的主密钥等。受害者若不能在规定时间内联系黑客并支付赎金，黑客将对受害者采取DDOS攻击以及致电其员工和业务合作伙伴，若几周内仍未支付，黑客将删除其数据。

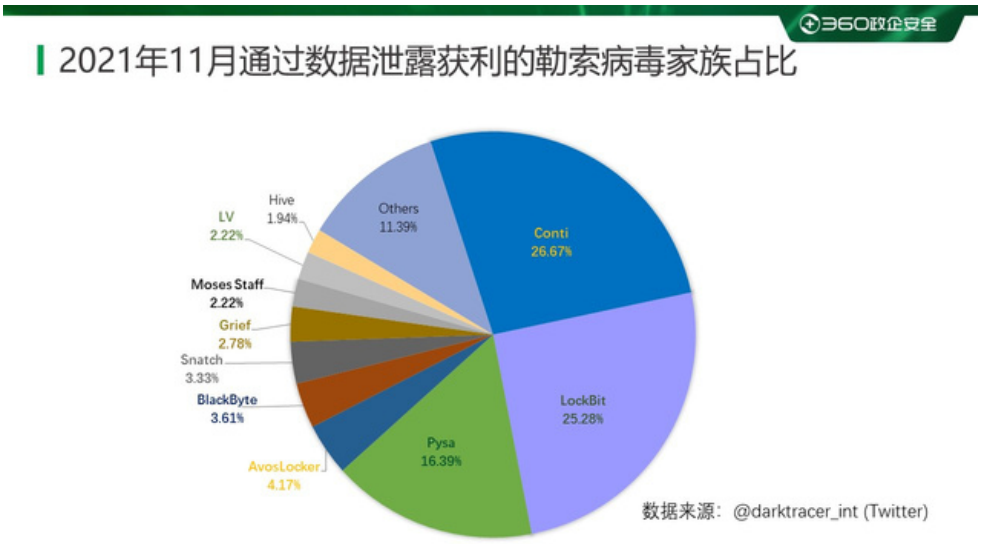


三、黑客信息披露

以下是本月收集到的黑客邮箱信息：

Merlen@Dr.Com	ransomware10@yahoo.com	dwaynehogan33@onionmail.org
sazepa@tuta.io	zeppelin_helper@tuta.io	AllenPool1987@onionmail.org
jericoni@pm.me	dr.helper@onionmail.org	Vasco_Alonso@protonmail.com
g.uan_yu@aol.com	mr.helper@onionmail.org	AndryCooper1988@tutanota.com
mak_supp@aol.com	alabacoman@tutanota.com	Mikedillov1986@onionmail.org
Merlen@Keemail.Me	ideapad@privatemail.com	helpdecryptmyfiles@yandex.com
psworm@keemail.me	uSuppor@privatemail.com	jackiesmith176@protonmail.com
zsebas@arimail.cc	zeppelin_decrypt@xmpp.jp	JerseySmith1986@onionmail.org
obamausa7@aol.com	datarecover@ctemplar.com	leonardred1989@protonmail.com
nexyum@zohomail.eu	pecunia0318@tutanota.com	JeremySaylor1987@tutanota.com
kameric@airmail.cc	EndryuRidus@tutanota.com	Rick_Astley_Helper@outlook.com
baseus0906@goat.si	admin@crypteyourdata.com	fionahammers1995@onionmail.org
ransomnow@yandex.ru	chickenwing@onionmail.org	MarkHuntigton1977@tutanota.com
pecunia0318@goat.si	yourfriendz@techmail.info	CharlesSLewis1987@onionmail.org
friend.dec@yandex.ru	Pringls_us@protonmail.com	DavidSchmidt1977@protonmail.com
cnlock@danwin1210.me	cheet0s_de@protonmail.com	JamesHoopkins1988@onionmail.org
pol.aris@tutanota.com	datarecovery@ctemplar.com	ollivergreen1977@protonmail.com
520hard@mailfence.com	jasonchow30@onionmail.org	jeffreyclinton1977@onionmail.org
seawolf@onionmail.org	Kirklord1967@tutanota.com	alberttconner2021@protonmail.com
coronaviryz@gmail.com	VinceGilbert@tutanota.com	DorothyFBrennan1992@tutanota.com
friend.dec@keemail.me	Vasco_Alonso@tutanota.com	noreywaterson1988@protonmail.com
koreadec@tutanota.com	korona@bestkoronavirus.com	rickysmithson1975@protonmail.com
helpservisee@elude.in	parpsrecovery@criptext.com	DerekWillson19878@protonmail.com
RansHelp@tutanota.com	yourrealdecrypt@airmail.cc	steven1973parker@libertymail.net
pol.aris@opentrash.com	Leslydown1988@tutanota.com	richardbrunson1892@protonmail.com
Merlens@Protonmail.com	vilidariobtc12@tutanota.com	ElizabethAntone1961@protonmail.com
coronavirus@exploit.im	zeppelindecrypt@420blaze.it	leticiaparkinson1983@onionmail.org
decryptdelta@gmail.com	harpoonlocker@onionmail.com	

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（已经支付赎金的企业或个人，可能不会出现在这个清单中）。



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。本月总共有360个组织/企业遭遇勒索攻击，其中中国有10个组织/企业在本月遭遇了双重勒索/多重勒索。

EHS	reigroup.com	Antal International
SWL	Glamox Group	Garner Dental Group
iPS	tornel.com.mx	Kent County Council
TTC	totalfire.biz	Symonds And Sampson
ION	cilentospa.it	breslowstarling.com
Ikma	eberlesrl.com	betsaisonparagot.fr
V-ON	Vision Source	Bruss North America
Hutt	Lucton School	consortiumlegal.com
Otip	Nordic Pharma	Team Computers Ltd.
DAMM	Eileen Fisher	comune.gonzaga.mn.it
AISD	Renault India	morganskenderian.com

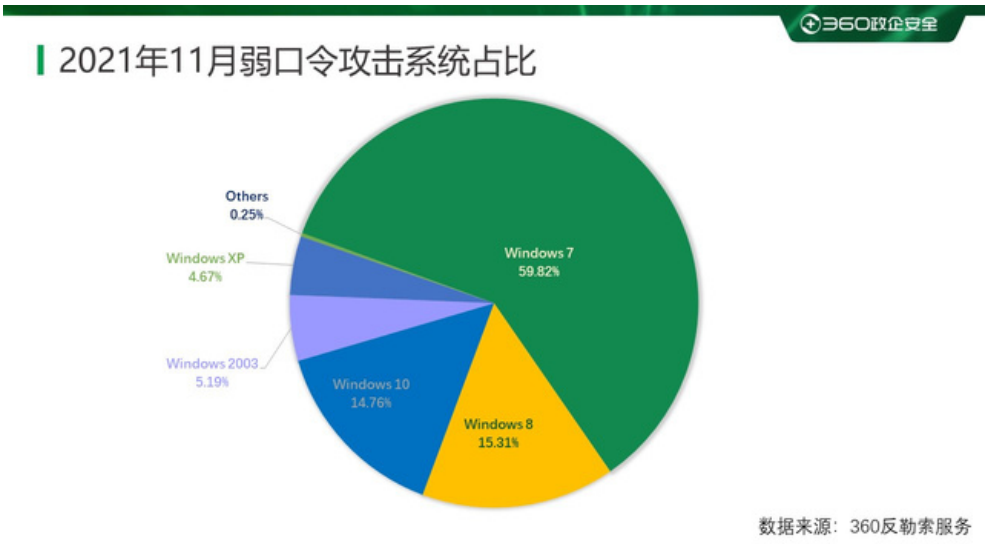
AECOM	INTOO Habitat	arrowheadadvance.com
UEMOA	Alco Plastics	waveridernursery.com
Varney	Police Brazil	ARGOS CONNECT ENERGY
socage	cloudpros.com	Family Dental Health
VERBIO	btc-alpha.com	Pitts Baptist Church
CHRYSO	reiss-beck.de	TestOil Oil Analysis
VISTRA	adhhealth.com	Greymouse VA PTY Ltd
INOXPA	apower.com.sg	Gibbs Wire And Steel
Grupo5	Charlie Hebdo	3D imagery of israel
Ishida	Argentina GOV	duncandisability.com
dlb.it	effectual.com	centerspacehomes.com
NOLATO	callay.com.tr	lawrencegroup.net.au
M3 Inc.	Bochane Groep	ardebolassessors.cat
Lantech	Power Plumbing	Burda Sanitärtechnik
PORTALP	benefitexpress	Align Technology, Inc
XacBank	Landmark Builders	The Harrison Law Firm
Ferrara	groweeisen.com	THE METRO GROUP, INC.
Emi Jay	mcmanislaw.com	Diputación de Segovia
Bayonet	nurihiko.co.jp	Capitol Beauty School
Epstein	Stratford Land	Architectural Systems
DUNMORE	Premier Energy	Purifoy Chevrolet Co.
SIRCHIE	The Xssentials	SNR Shopping PUREGOLD
KISTERS	Jonas Software	Volvo Car Corporation
wpdn.net	home.hktdc.com	VIENNA INSURANCE GROUP
Laurenty	daviscrump.com	autolaundrysystems.com
fandi.fr	City of Witten	W A RASIC CONSTRUCTION
eban.com	Visage Imaging	City of Bridgeport, WV
DALLOYAU	mtradeasia.com	Family Dentist Newbury
Burkhart	telepro.com.mx	Woodchurch High School
Jalasoft	Aspen Avionics	Tangent Communications
MPRL E&P	Besson Seguros	peschl-ultraviolet.com
abiom.nl	dtstechnical.ca	Area Energy & Electric
GC Micro	waclighting.com	lenzcontractorsinc.com
EDAN.COM	plumascounty.us	DUNA AUTO az Autovaros
Match MG	David Engineers	Westvale Primary School

Arbitech	ProActive Works	Las Vegas Cancer Center
gaben.cz	Astera Software	Johnson Memorial Health
DEWEtech	Westmont Helena	Cabinet Remy Le Bonnois
Starline	Connect Housing	The Della Toffola Group
Flagship	barfieldinc.com	The Grupo Daniel Alonso
ARM CHIN	The Glass House	Delta Group Electronics
rttax.com	NLB Corporation	Lakeway Publishers, Inc.
EZ Loader	REV Engineering	Enduro Pipeline Services
La Bodega	vicksburgha.org	Florida Heart Associates
itimCloud	Salinen Austria	Schmincke Künstlerfarben
Skatetown	RocTechnologies	evolvedevelopment.com.au
Unit 8200	promo.parker.com	fluidsealingproducts.com
FTI Group	Regence Footwear	DKS Deutsch Kerrigan LLP
a1ssi.com	besttaxfiler.com	WELLS FARM DAIRY LIMITED
iveqi.com	Agricorp Company	Supernus Pharmaceuticals
inlad.com	Community Brand	Creative Solutions Group
mpusd.net	Emkay Food Sales	ATA National Title Group
San Carlo	ONTEC Automatic	QRS Healthcare Solutions
UABL S.A.	thinkcaspian.com	pacificstarnetwork.com.au
gvalue.com	Moneyfacts Group	trueblueenvironmental.com
bdtaid.com	redsrugby.com.au	Rusty Hardin & Associates
ENESCO.C	Canada West Land	The Skinners Kent Academy
mym.com.	Aisha Steel-ASML	Emery Jensen Distribution
rintal.com	scotttesting.com	HELSA Group International
era.org.uk	hanshin-dp.co.jp	hsvgroup.talentnetwork.vn
GPV FRAN	The Cochran Firm	STAR REFRIGERATION LIMITED
pkf.com.au	telemovil.com.sv	Ehud Leviathan Engineering
royole.com	planters-oil.net	Bryant Industrial Services
ochsnerEF	nextech-asia.com	Rockbridge and Bath County
siix.co.jp	MCP Services LLC	Dealers Auto Auction Group
wnrllc.com	The Npd Group In	Karges-Faulconbridge, Inc.
APR Supply	owenscarolina.com	Comstock Johnson Architects
ALPSRX.CO	optimumdesign.co	Property Damage Restoration
jurelus.de	H.G.M Engineering	Hickory Veterinary Hospital
APG Neuro	Niemi Bil i Luleå	Holy Family RC & CE College

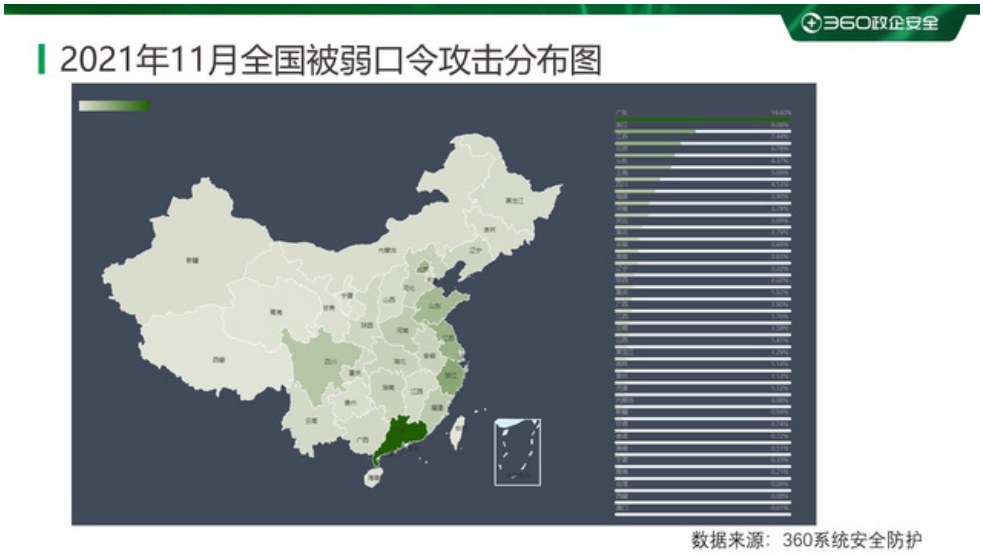
Koltepatil	CarpenterProjects	ASPECT STUDIOS ASIA PTY LTD
kenwal.cor	R.E. Pedrotti Co.	MATITIAHU BRUCHIM Law office
JEAN FLO(	comfacundi.com.c	Marshall Investigative Group
TRINA SOL	ideaitaliausa.com	Virginia Department of Health
Metaenerg	John Sisk and Son	Thunderbird Adventist Academy
Gulfport M	Lineage Logistics	Eason Horticultural Resources
MVS Maile	National Material	Williams & Rowe Company, Inc.
abvalve.co	General RV Center	Beaverhead County High School
EQUITY Ba	kankakeetitle.com	Marten Transport (MRTN NASDAQ)
bsg-llp.cor	Cadence Aerospac	FLUID COMPONENTS INTERNATIONAL
LOGROS S	Отбасы банк	Law Society of South Australia
VR Souliere	Epple Druckfarben	Eberspächer Group of Companies
evans.co.id	Wolverine freight	Goodwill of Central and Coastal Virginia, Inc.
mecfond.c	Stoningtonschools	HARTMANN FINANCIAL ADVISORS LLC
MENZ&GA	Finite Recruitment	Herman & Kittle Properties Inc.
FUND-X S	Southland Holding	City of Fulton police department
Websites.c	Blue Harbor Resor	The Center for Rural Development
Lootah BC	Valley Machine Co	Charley's Greenhouse Supply, LLC
interfor.co	cepimanagement.c	West Virginia Parkways Authority
logistia.cor	Pronghorn Contro	Midwest Packaging Solutions, Inc.
INDIAN CR	AHEC Tax Solution	Outdoor Venture Corporation (OVC)
chatrium.c	Raj Transport Inc.	Universitat Autònoma de Barcelona
Royale.co.u	Alternatives, Inc.	Wisconsin Homes Inc Home Builders
cool-pak.c	The Leschaco Grou	Cogan Wire and Metal Products Ltd
Dr Schneid	gunninglafazia.cor	Unione dei Comuni Terre di Pianura
Fly Arik Air	Star Island Resort	Bock, Hatch, Lewis & Oppenheim, LLC
Electra Lin	Tri Tech Surveying	HUDSON BROTHERS Construction Company
cardigos.co	JAFTEX Corporatio	MINISTRY OF ECONOMY AND FINANCE Peru
Axicorp GM	systematicatec.cor	Hospitality Furnishings & Design Inc.
Orgill, Inc.	Daylesford Organi	Società Italiana degli Autori ed Editori
mfitexas.co	Amtech Corporatio	Pueblo Bonito Pacifica Golf & Spa Resort
transaher.e	SWIRESPO.COM	Società Italiana degli Autori ed Editori
essextec.co	MGA RESEARCH	MOTOR VEHICLE ACCIDENT FUND PENSION FUND
docol.com.	MCH-GROUP.CO	COMMUNAUTÉ DE COMMUNES PAYS D'APT LUBERON
EL Pruitt C	PALMER LOGISTIC	The British Columbia Institute Of Technology
immodelae	MUTUAL MATERIA	ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
atlas.ind.br	FRONTIER SOFTW	Department of Justice and Constitutional Development
Acne Studi	MUSCHERT-GIERS	Jet Industries Full Service Design And Construction Services
Alixa Rx LL	MEYER CORPORA	Transco Süd Internationale Transporte Gesellschaft mit beschränkter Haftung

三、系统安全防护数据分析

通过将2021年10月与11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11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。



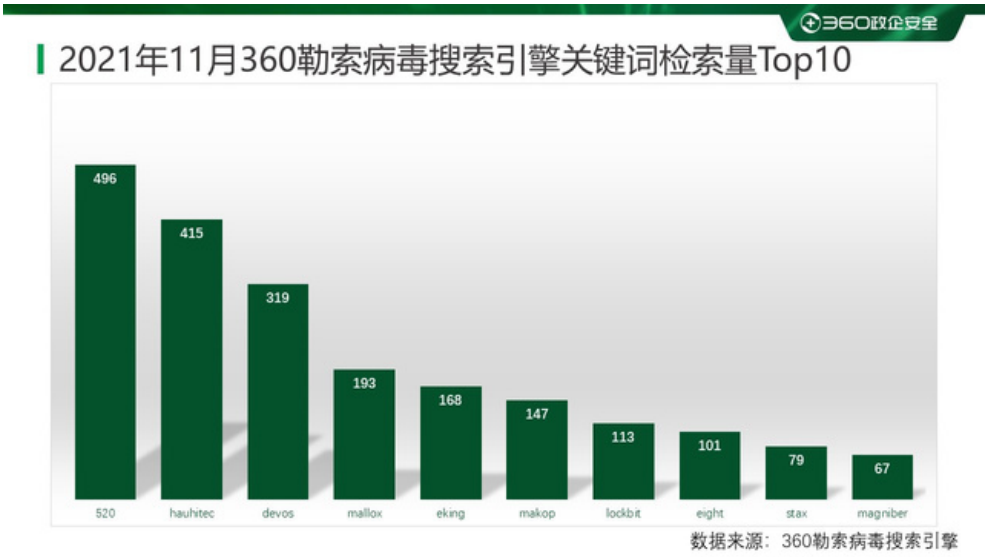
通过观察2021年11月弱口令攻击态势发现，RDP和MYSQL弱口令攻击整体无较大波动,MSSQL的攻击量整体呈下降态势。

四、勒索病毒关键词

- 520：属于BeijngCrypt勒索病毒家族，由于被加密文件后缀会被修改为520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。
- hauhitec：属于YourData，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。
- 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。
- Mallox:属于Mallox勒索病毒家族，由于被加密文件后缀会被修改为mallox而成为关键词。通过SQLGlobeImposter渠道进行传播。
- eking：同devos。
- 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。

- 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。
- eight:同devos。
- stax：属于Stop勒索病毒家族，由于被加密文件后缀会被修改为stax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。
- Magniber: 被该家族加密的文件，后缀均被修改为随机字符串，其主要传播方式为：通过挂马网站进行传播。



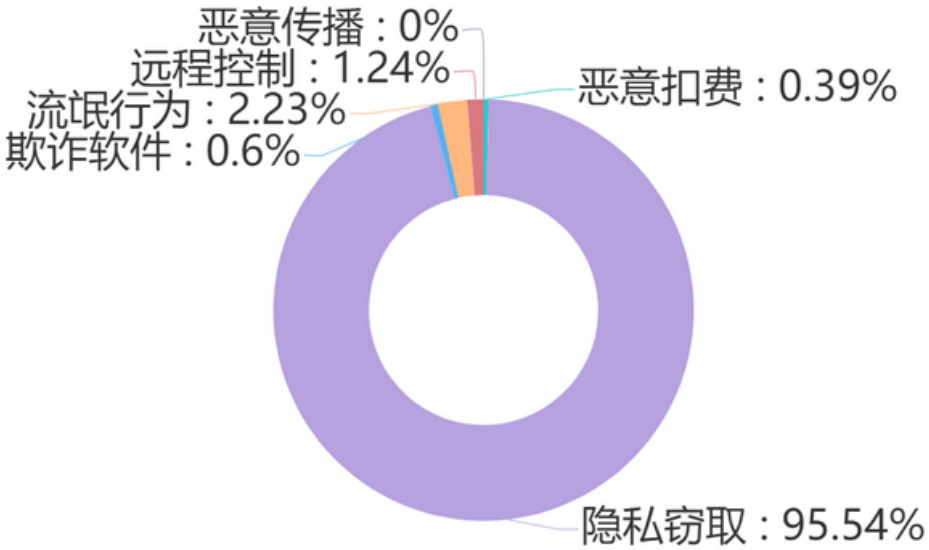
五、解密大师

从解密大师本月解密数据看，解密量最大的是GandCrab，其次是Crysis。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。

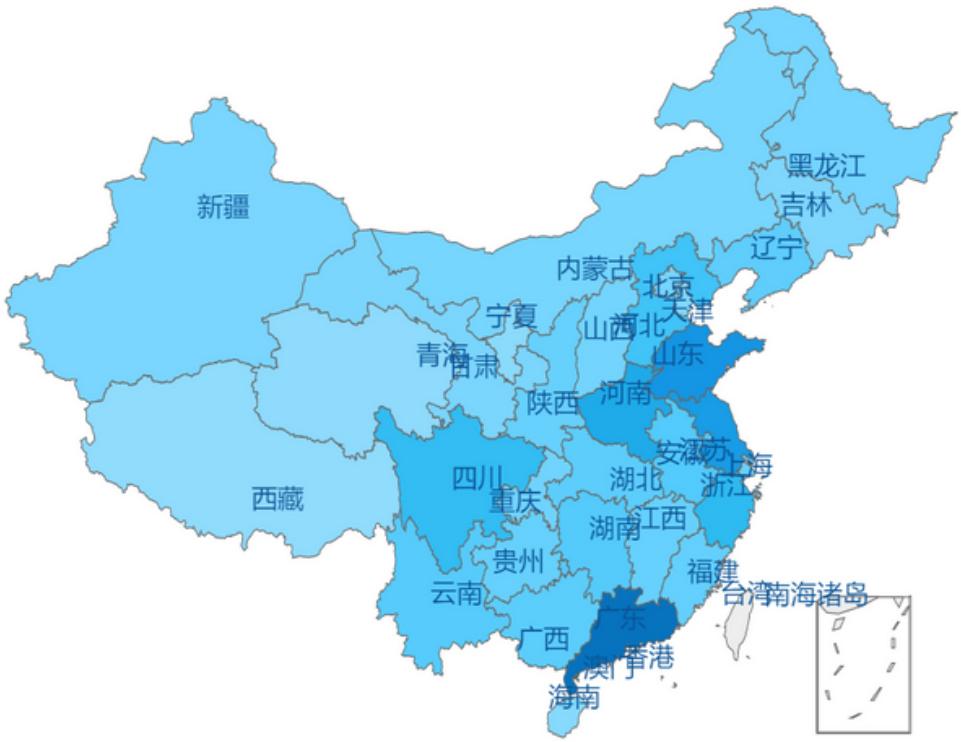
数据来源：反勒索服务统计数据

移动安全数据分析

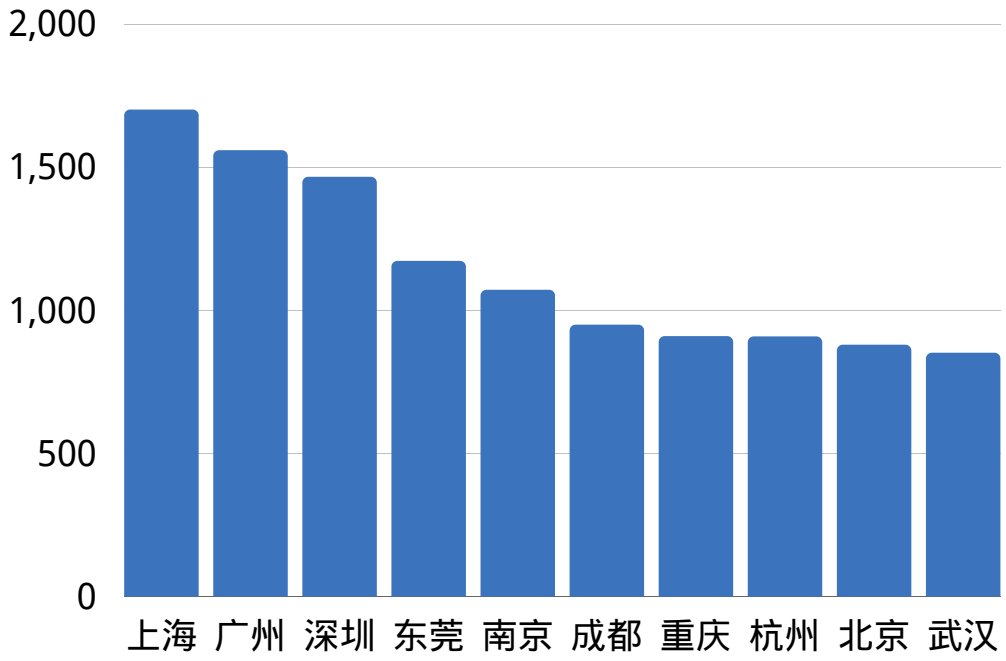
Mobile Security Data Analysis



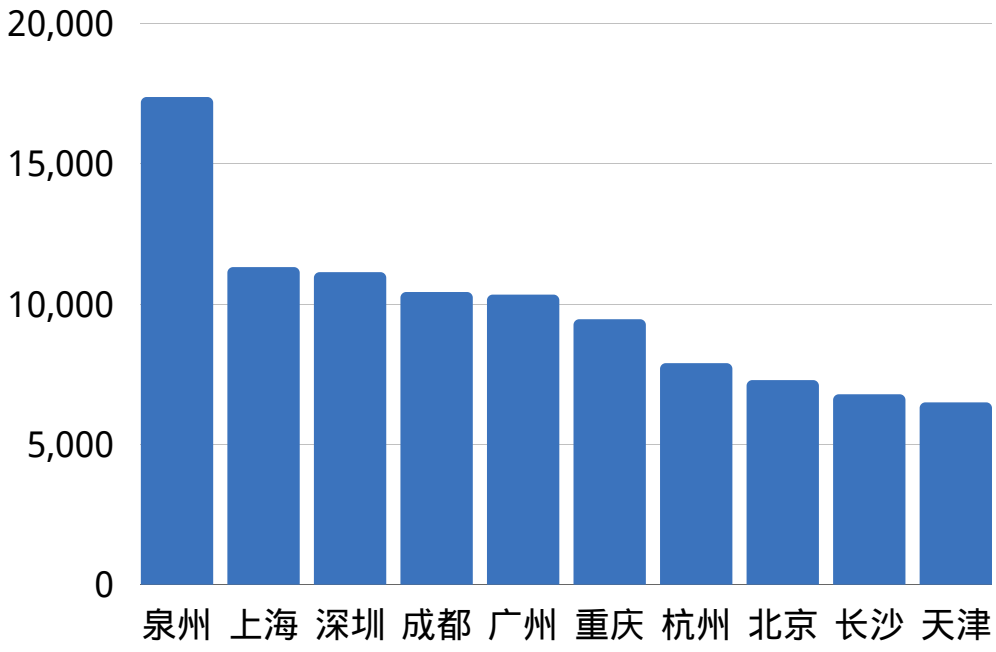
数据总览



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

2021.11

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