总第6期

2021年9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

微软官方发布MSHTML组件在野0day漏洞
美国农民合作社遭受blackmatter勒索攻击，被勒索590万美元
印度尼西亚政府的新冠病毒检测程序泄漏130万用户信息
微软Exchange Autodiscover漏洞泄漏10万个Windows凭据
38亿俱乐部和Facebook用户记录被在线出售
黑客集团利用ProxyLogon漏洞攻击全球酒店
SideWinder针对巴基斯坦的海军
APT组织使用加强型TTP瞄准印度国防官员
三边行动：针对南亚、中东多国长达数年的网络间谍活动

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9月，360CERT共收录13个漏洞，其中严重1个，高危9个，中危3个。主要漏洞类型包含身份验证绕过、栈溢出、服务器端请求伪造等。涉及的厂商主要是Apache、Cisco、QNAP、Windows、 VMware等。

二、安全事件

本月收录安全事件211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、Intel、Cisco、Apple、FBI、instagram、等。涉及的行业主要包含IT服务业、金融业、制造业、政府机关及社会组织、医疗行业、交通运输业等。

三、恶意程序

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9月，全球新增的活跃勒索病毒家族有:AtomSilo、BlackByte、Groove、Sodinokibi(REvil)等勒索软件。其中AtomSilo的数据泄露网站与BlackMatter高度相似，两者可能存在密切关系；Groove勒索软件由Babuk核心成员之一开发，并创建了一个名为RAMP的暗网论坛；消失近两月的Sodinokibi(REvil)在本月正式回归。

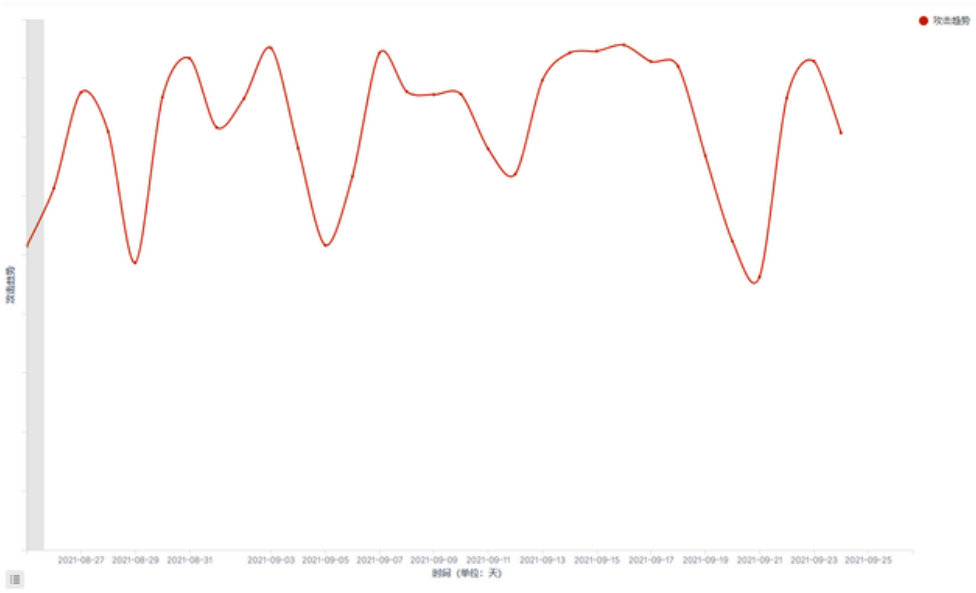
通过隐私窃取拦截量TOP10来看，上海、泉州、深圳这三个省份移动端隐私窃取数量占据前列，基本上可以体现人口越集中、经济越发达、移动设备使用数量越多的省份，软件恶意行为更加猖獗、恶意软件存活比例越大。

本月攻击态势

Attack situation analysis

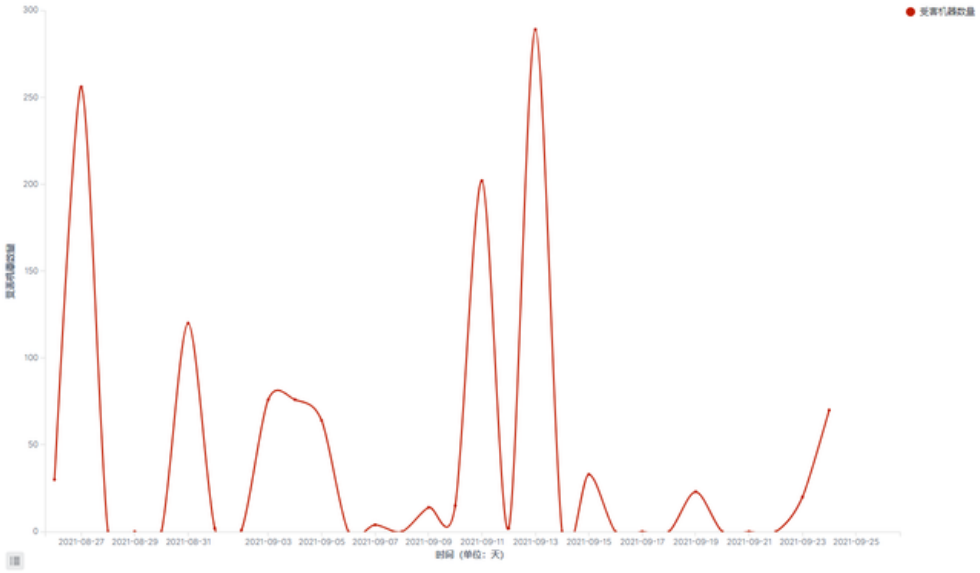
一、僵尸网络攻击

9月份僵尸网络总体攻击趋势相对较为平稳，相比较8月份有略微的上涨。



9月份僵尸网络攻击趋势

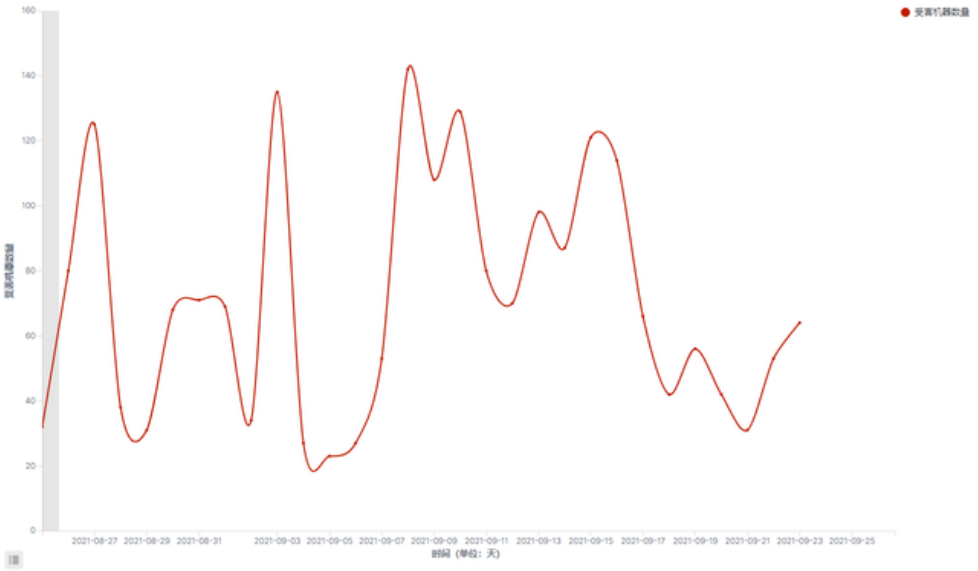
上涨的原因主要在于8月底披露的Atlassian Confluence远程代码执行漏洞CVE-2021-26084正在被多个僵尸网络所使用，包括“8220”团伙、JavaxMiner在内的多个挖矿僵尸网络利用该漏洞攻击部署Atlassian Confluence的服务器，攻击成功后在机器中植入挖矿木马获利。下图展示了自CVE-2021-26084漏洞披露以来，Windows平台遭到僵尸网络攻击的Atlassian Confluence的服务数量。



Windows平台遭到僵尸网络攻击的Atlassian Confluence的服务数量

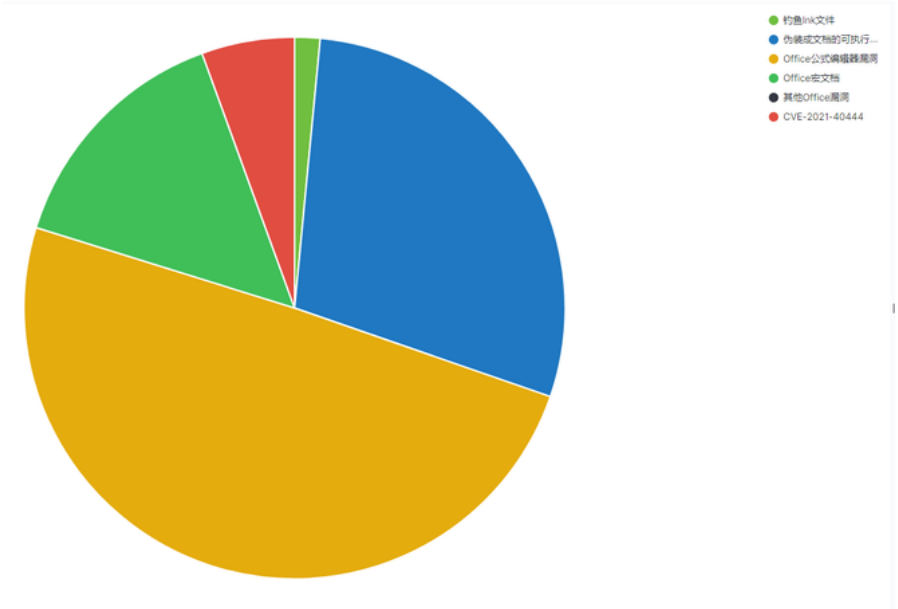
二、钓鱼邮件攻击

本月钓鱼邮件攻击较为活跃，攻击依然以投递银行木马的垃圾邮件攻击为主，攻击者通过大量投递垃圾邮件，在邮件中添加恶意附件，利用Office恶意宏、公式编辑器漏洞等在受害机器中植入Lokibot、AgentTesla等窃密木马，窃取机器中的浏览器登陆凭证、FTP登陆凭证、虚拟货币钱包信息等。



9月份钓鱼邮件攻击趋势

9月初，mshtml远程代码执行漏洞CVE-2021-40444被披露，仅仅几天后，该漏洞的概念验证以及漏洞利用代码生成程序就在社交网络上广泛传播。攻击者可以以Office文档为载体利用该漏洞在目标机器上执行任意代码，且利用难度简单，是钓鱼攻击的大杀器。在漏洞被披露后，360安全大脑监控到互联网上有不少CVE-2021-40444的漏洞利用测试，并且有少量攻击者利用该漏洞发起攻击。下图展示了9月份钓鱼邮件攻击的攻击方式分布，其中有11例攻击是通过CVE-2021-40444漏洞发起的。

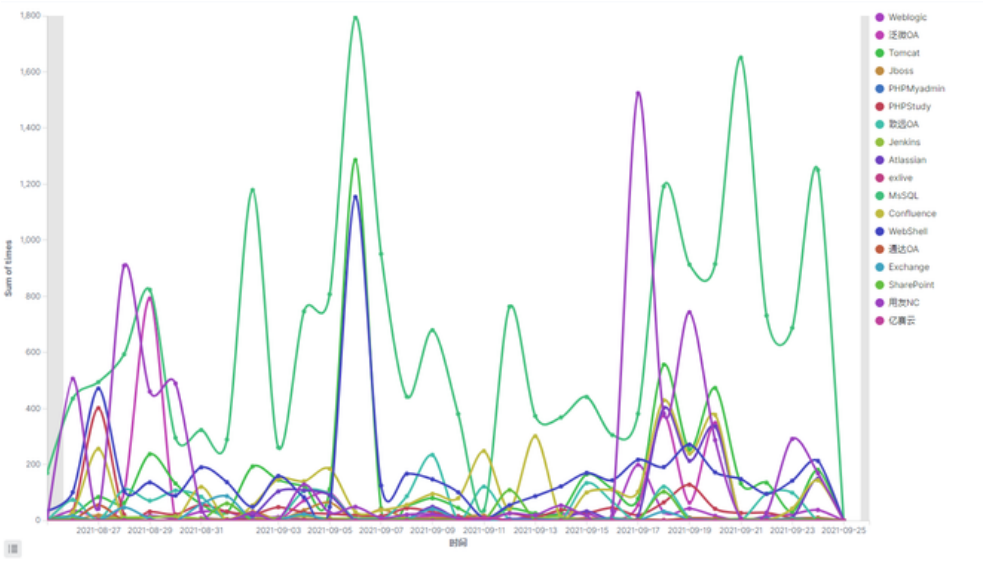


9月份钓鱼攻击方式分布

三、针对Web应用和数据库的攻击

9月针对Web应用和数据库的攻击中，针对Atlassian Confluence的攻击出现显著增长，主要原因为8月底Atlassian Confluence 远程代码执行漏洞CVE-2021-26084 的漏洞细节被披露后，大量黑产团伙利用该漏洞发起攻击，投递DDoS木马、挖矿木马、远控木马等。此外，针对MsSQL的攻击也非常活跃，这类攻击主要由紫狐和MyKings两个大型僵尸网络发起。而针对用友OA和亿赛云的攻击相比较8月份有所减少，主要原因为之前针

对这两个目标发起攻击的黑产团伙已经攻下一定数量存在漏洞的服务器，无法再寻找更多存在漏洞的服务器，因此该团伙将目光转向了新的目标——Atlassian Confluence，从而减少对用友OA和亿赛云的攻击。



9月份针对Web应用和数据库的各类攻击趋势

安全漏洞

VULNERABILITIES

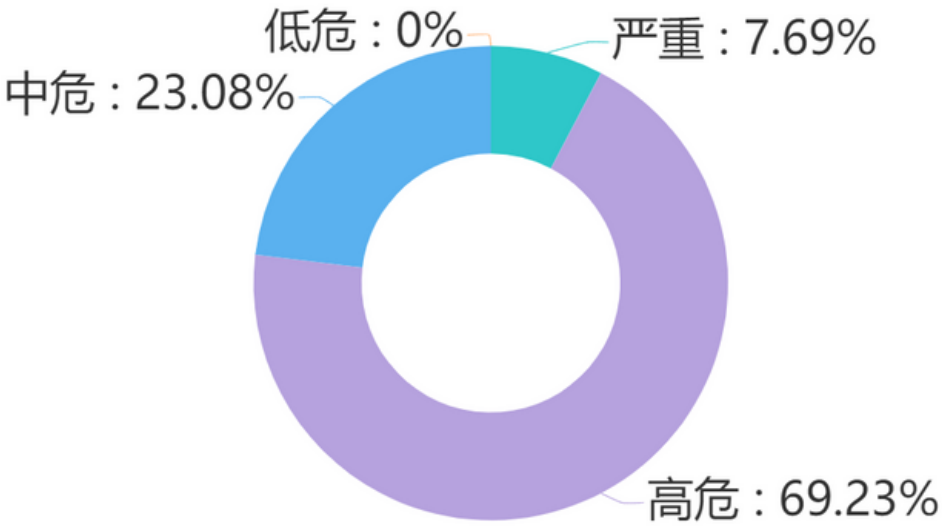
前言

2021年9月，360CERT共收录13个漏洞，其中严重1个，高危9个，中危3个。主要漏洞类型包含身份验证绕过、栈溢出、服务器端请求伪造等。涉及的厂商主要是Apache 、Cisco、QNAP、Windows、 VMware等。

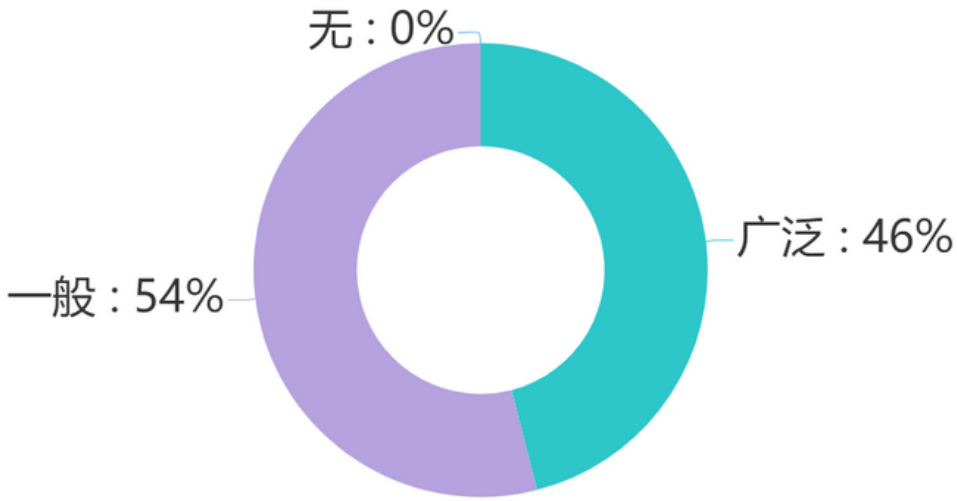
目录预览

漏洞图表

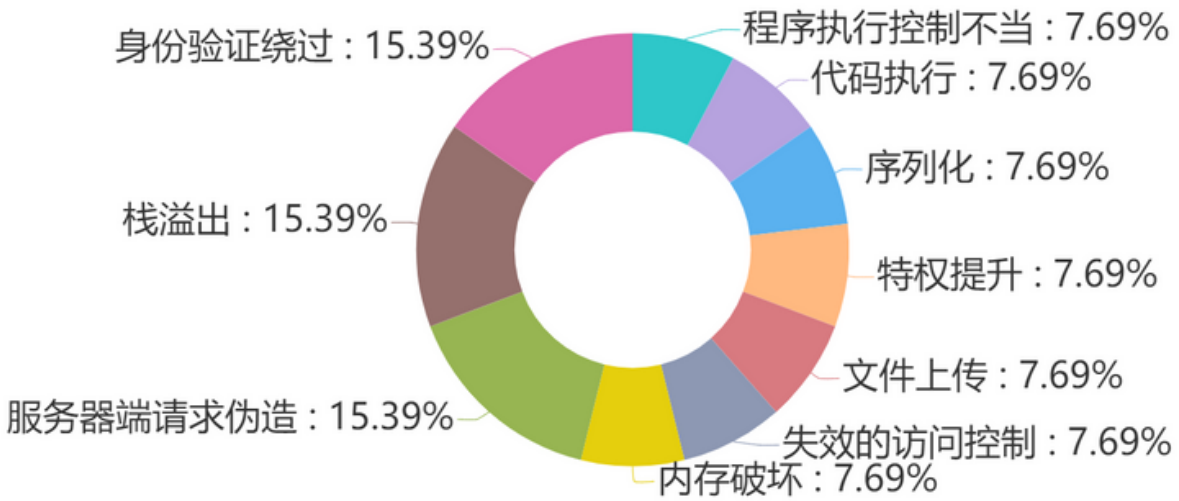
Charts Of Vulnerabilities



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

Dubbo
Nexus Repository 3
Enterprise NFVIS
QuTScloud
dxflib
QTS
SD-WAN vEdge
MSHTML
vcenter server
QuTS hero

热门组件列表

重点漏洞回顾

Review Of Vulnerabilities

VMware vCenter Server多个高危漏洞

评分：9.8　安全补丁已发布

2021年09月22日，360CERT监测发现VMware官方发布了VMware vCenter Server和VMware Cloud Foundation的风险通告，事件等级：严重，事件评分：9.8。相关漏洞编号：CVE-2021-22005、CVE-2021-21991、CVE-2021-22006、CVE-2021-22011等，目前这些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。VMware vCenter Server是VMware虚拟化管理平台，广泛的应用于企业私有云内网中。通过使用vCenter，管理员可以轻松的管理上百台虚拟化环境，同时也意味着当其被攻击者控制后会造成私有云大量虚拟化环境将被攻击者控制。

2021-09 补丁日: 微软多个漏洞安全更新

评分：9.8　安全补丁已发布

2021年09月15日，微软发布了9月份安全更新，事件等级：严重，事件评分：9.8。此次安全更新发布了66个漏洞的补丁，主要覆盖了以下组件：Windows操作系统、Azure、Edge、Office、BitLocker等。其中包含3个严重漏洞，62个高危漏洞。本次更新已经对近期公开的严重漏洞MSHTML漏洞CVE-2021-40444发布了修复补丁。

2021-09 补丁日: Chrome多个漏洞安全更新

评分：8.4　安全补丁已发布

2021年09月14日，Google发布了Chrome的9月份安全更新，事件等级：高危，事件评分：8.4。Chrome是热门的网络浏览器，同时底层的V8引擎也是最重要的浏览器内核之一。此次安全更新发布了9个高危漏洞，涉及页面布局功能、V8引擎、Indexed DB API、权限控制功能等。

微软官方发布MSHTML组件在野0day漏洞

评分：8.8　安全补丁已发布

2021年09月08日，微软官方发布了MSHTML组件的风险通告，漏洞编号为CVE-2021-40444，漏洞等级：高危，漏洞评分：8.8。微软表示已经监测到该漏洞存在野利用。微软AcitveX控件是微软公司的COM架构下的产物，在Windows的Office套件、IE浏览器中有广泛的应用。利用ActiveX控件即可与MSHTML组件进行交互。

Confluence OGNL 注入漏洞

评分：8.8　安全补丁已发布

2021年09月01日，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：高危，漏洞评分：8.8。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。该漏洞的 POC 与 漏洞细节 在网上已经公开。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。

漏洞时间线

Timeline Of Vulnerabilities

2021-09-03

CVE-2021-34746 高危
Enterprise NFVIS 身份验证绕过漏洞

CVE-2021-40143 中危
Nexus Repository 3 服务器端请求伪造漏洞

2021-09-08

CVE-2021-40444 高危
MSHTML 代码执行漏洞

2021-09-09

CVE-2021-36163 中危
Dubbo 序列化漏洞

CVE-2021-21897 中危
dxflib 内存破坏漏洞

2021-09-10

CVE-2021-20791 高危
Browser 程序执行控制不当漏洞

CVE-2021-20790 高危
Browser 失效的访问控制漏洞

CVE-2021-28816 高危
QuTScloud 栈溢出漏洞

CVE-2021-34343 高危
QuTScloud 栈溢出漏洞

2021-09-22

CVE-2021-22005 严重
vcenter server 文件上传漏洞

CVE-2021-21991 高危
vcenter server 特权提升漏洞

CVE-2021-22006 高危
vcenter server 服务器端请求伪造漏洞

CVE-2021-22011 高危
vcenter server 身份验证绕过漏洞

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

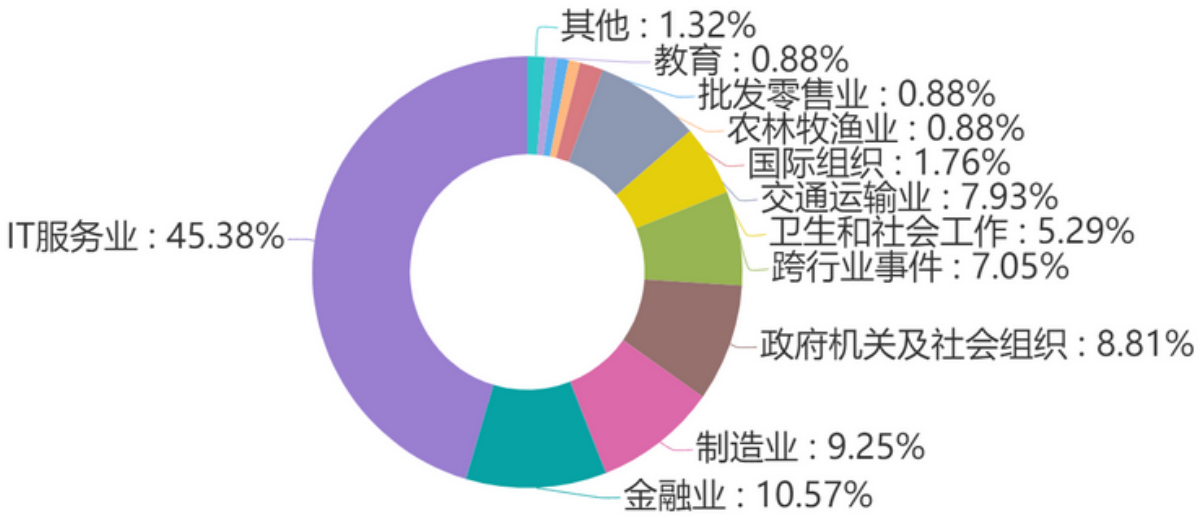
前言

本月收录安全事件211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、Intel、Cisco、Apple、FBI、instagram、等。涉及的行业主要包含IT服务业、金融业、制造业、政府机关及社会组织、医疗行业、交通运输业等。

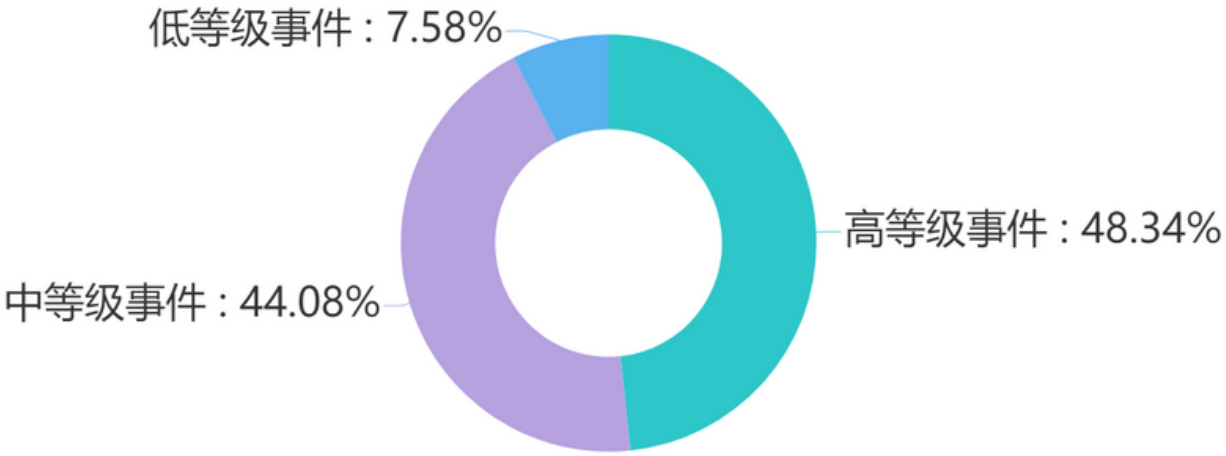
目录预览

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-56（透明部落）近期最新攻击分析与关联疑似Gorgon Group攻击事件分析预警

标签：APT-C-56, C2, APT
链接：https://mp.weixin.qq.com/s/xUM2x89GuB8uP6otN612Fg

透明部落（Transparent Tribe）别名APT36、ProjectM、C-Major，是一个具有南亚背景的APT组织，其长期针对周边国家和地区（特别是印度）的政治、军事进行定向攻击活动，其开发有自己的专属木马CrimsonRAT，还曾被发现广泛传播USB蠕虫。TransparentTribe也曾经对Donot的恶意文档宏代码进行模仿，两者高度相似。之前透明部落也曾经模仿响尾蛇组织进行攻击。其一直针对印度的政府、公共部门、各行各业包括但不限于医疗、电力、金融、制造业等进行攻击和信息窥探。近日360高级威胁研究分析中心在日常情报挖掘中发现并捕获到了透明部落攻击印度的文档，恶意文档最终释放CrimsonRAT。与此同时，360高级威胁研究分析中心还监控到了疑似Gorgon Group利用Netwire对印度的攻击行动，该组织由疑似巴基斯坦或与巴基斯坦有其他联系的成员组成。该组织一直有针对性的攻击英国、西班牙、俄罗斯和美国。Gorgon也曾经被怀疑与Transparent Tribe有关联，并可能负责Aggah活动。

疑似APT-C-36盲眼鹰攻击活动披露

标签：APT-C-36, C2, APT
链接：https://mp.weixin.qq.com/s/PEi2aaprbO3h3FMw_7Es_A

第四大洲，拥有丰富的自然环境资源，但是由于历史原因导致殖民经济一直存在，战乱不断，政治不稳定，各国经常出现暴乱，伴随着南美洲的动乱，以及政治意见的不同，针对性的情报窃取攻击广泛存在，这类APT攻击持续性强，针对性明确，即使被安全厂商披露，也不会停止行动潜伏，应该时刻保持关注。APT-C-36盲眼鹰组织是一个疑似来自南美洲的、主要针对哥伦比亚的APT组织，该组织自2018年持续发起针对哥伦比亚的攻击活动。近日，360高级威胁研究院在日常情报挖掘中发现并捕获到了疑似盲眼鹰的攻击行动。恶意文档最终释放RAT对中招机器进行远程控制，360高级威胁研究院已经监控到有国外哥伦比亚用户受到了影响。

TinyTurla - Turla 部署新的恶意软件以在受害机器上保留秘密后门

标签：Turla, C2, APT
链接:https://blog.talosintelligence.com/2021/09/tinyturla.html

Cisco Talos最近发现了俄罗斯Turla APT组织使用的一个新后门，以实现对受感染设备的持久化访问。该后门冒充了"Windows Time Service"被安装在受感染的机器上，代码非常简单但足够有效，可以上传、执行文件或从受感染系统中窃取文件，并且能够逃避安全检测。目前发现，美国、德国以及阿富汗均有中招。

疑似APT-C-56透明部落攻击预警

标签: APT-C-56, C2, APT
链接: https://mp.weixin.qq.com/s/hHBsy_B3jECr2FLk5g9gbA

APT-C-56（透明部落）别名APT36、ProjectM、C-Major，是一个具有南亚背景的APT组织，长期针对周边国家和地区（特别是印度）的政治、军事目标进行定向攻击活动，开发有自己的专属木马CrimsonRAT，还曾被发现广泛传播USB蠕虫。透明部落在2019年下半年一直非常关注阿富汗地区，在2020年开始再次转为关注印度用户。到了2021年，先是利用疫情相关信息对印度医疗、电力行业进行信息窃取，随后伪装印度国防部会议记录的诱饵文档尝试进行信息窃取。
近日，360高级威胁研究院在日常情报挖掘中发现并捕获到了多批疑似透明部落攻击印度的文档，恶意文档最终释放NetWireRAT。

NOBELIUM组织的新恶意软件FoggyWeb的深入分析

标签: NOBELIUM, C2, APT
链接: https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/

微软威胁情报中心对新检测到的NOBELIUM组织的FoggyWeb后门进行深入分析。NOBELIUM组织使用FoggyWeb远程窃取被入侵的AD FS服务器的配置数据库、解密的令牌签名证书和令牌解密证书，以及下载和执行其他组件。早在2021年4月，就在野观察到了FoggyWeb的使用。
FoggyWeb是一种被动的、具有高度针对性的后门，能够从被入侵的AD FS服务器远程窃取敏感信息。它还可以从C2服务器接收额外的恶意组件，并在被入侵的服务器上执行它们。

疑似Nobelium组织开发的新后门Tomiris

标签: Nobelium, C2, APT
链接: https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/

今年6月，卡巴斯基的内部系统发现了一个成功的DNS劫持的痕迹，影响了独联体国家的几个政府区域。这些事件发生在2020年12月和2021年1月，并允许攻击者将流量从政府邮件服务器重定向到他们控制的机器。Tomiris是一个用Go语言编写的后门，它的作用是不断地查询C2服务器以下载并在受害系统上执行可执行文件。在执行任何操作之前，它至少会休眠9分钟，可能是为了规避基于沙箱的分析系统。并通过创建计划任务建立持久性。

APT-C-23 使用 Android 间谍软件的新变种攻击中东用户

标签：APT-C-23, C2, APT
链接：https://blog.cyble.com/2021/09/15/apt-c-23-using-new-variant-of-android-spyware-to-target-users-in-the-middle-east/

在例行威胁狩猎过程中，Cyble研究实验室发现一条[推文](https://twitter.com/malwrhunterteam/status/1437498154501480451)，提到了APT-C-23使用的Android恶意软件新变种 Google_Play_Installer7080009821206716096，伪装成Google Play相关的应用程序。Cyble研究实验室下载了该样本，并确定 APT-C-23（又名“双尾蝎”）使用此版本的Android恶意软件攻击中东，从受感染的设备中窃取敏感信息，例如联系人数据、短信数据和文件等。

APT-C-36 使用更新版的商业RAT发起针对南美实体的垃圾邮件活动

标签：APT-C-36, C2, APT
链接：https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

2019年，Trend micro发表了一篇关于疑似哥伦比亚攻击组织（APT-C-36或盲眼鹰）的博客文章，该组织通过垃圾邮件攻击哥伦比亚和其他南美国家的目标实体。从那以后，Trend micro持续追踪该组织，并在这篇博客文章中分享了关于APT-C-36正在进行的垃圾邮件活动的新发现。

SideWinder针对巴基斯坦的海军

标签：SideWinder, C2, APT
链接：https://cluster25.io/wp-content/uploads/2021/09/a_rattlesnake_in_the_navy.pdf

SideWinder(又名RattleSnake)APT组织，据称主要代表印度政府的利益。攻击活动的动机是窃取信息，并且对南亚不同国家进行间谍活动。
此次攻击，Sidewinder使用了与之前行动略微不同的的技术，更新了DLL侧加载技术(T1574.002)，使用合法的control.exe可执行文件加载旨在解密和执行最终载荷的恶意DLL。
Cluster25对通过鱼叉式钓鱼发送给受害者的(T1566.001)的恶意附件进行了分析，发现攻击目标极有可能是巴基斯坦的海军部门，并以极高的可信度将此次攻击归因于SideWinder组织。

Operation Armor Piercer：使用商业RAT攻击印度次大陆

标签：Operation Armor Piercer, C2, APT
链接：https://blog.talosintelligence.com/2021/09/operation-armor-piercer.html

研究人员发现一起针对印度政府人员的攻击活动，使用的主题和战术类似于APT36（又名透明部落），比如利用被入侵的合法网站和假域名托管恶意有效载荷。此活动分发伪装成与印度政府基础设施和操作相关的指南的恶意文档和压缩文件，例如 Kavach 和 IT 相关指南，以部署Netwire和Warzone (AveMaria) RAT。

BladeHawk 组织：针对库尔德族群的 Android 间谍活动

标签：BladeHawk, C2, APT
链接：https://www.welivesecurity.com/2021/09/07/bladehawk-android-espionage-kurdish/

ESET研究人员调查了针对库尔德少数民族的移动端间谍活动。该活动至少从2020年3月开始活跃，利用Facebook分发伪装合法应用程序的888 RAT和SpyNote安卓后门。这些Facebook账户似乎提供库尔德及其支持者的相关新闻，其中部分账号故意将其他间谍应用程序传播到带有亲库尔德内容的Facebook团体中。下载数据显示，仅仅几篇帖子中就有至少1481次下载量。

EGoManiac | 肆无忌惮的土耳其威胁组织

标签：EGoManiac, C2, APT
链接：https://www.sentinelone.com/labs/egomaniac-an-unscrupulous-turkish-nexus-threat-actor/

- EGoManiac是之前报道的“Octopus Brain”行动的幕后攻击者，在该行动中，安全人员禁用了部署恶意软件的OdaTV记者的机器，为逮捕他们提供了有效的证据。
- 我们将“Octopus Brain”行动与一个名为Rad的工具包联系起来，该工具包早在2010年就在开发中，直到2015年才被使用。
- Rad样本使用硬编码的电子邮件地址逃避检测。其中一个电子邮件地址被指与起诉土耳其国家警察的流氓成员以及Datalink Analiz公司高管有关，并将Rad称为“HORTUM”。
- 根据“Datalink Analiz”的线索，我们怀疑EGoManiac的行动使用了Hacking Team的远程控制系统(RCS)，其早在2011年就开始了一系列违规行为。
- 2013年，发表了一份关于在美国境内针对土耳其受害者使用RCS的报告。受害者怀疑该RCS的使用代表了土耳其政府内部未经批准的危险分子的利益。

在这篇文章中，我们提供了对这个肆无忌惮的威胁组织攻击行动的部分调查结果。完整的报告提供了恶意软件样本的详细技术分析、完整的IoCs、狩猎规则以及更多的属性细节。

疑似双尾蝎APT组织近期针对巴勒斯坦地区的攻击活动分析

标签：双尾蝎，C2，APT
链接：https://mp.weixin.qq.com/s/nE_cvvooXvVjLhZd0EnXcQ

双尾蝎（奇安信内部跟踪编号：APT-Q-63）是一个长期针对中东地区的高级威胁组织，其最早于2017年被披露。至少自2016年5月起，持续针对巴勒斯坦教育机构、军事机构等重要领域进行网络间谍活动，以窃取敏感信息为主的网络攻击组织，开展了有组织，有计划，有针对性的攻击。
近日，奇安信威胁情报中心红雨滴团队在日常的威胁狩猎中捕获了该组织多起攻击样本，捕获的样本包括伪装成政治热点、教育相关的可执行文件诱饵，以及伪装成微软图像处理设备控制面板程序(ImagingDevices.exe)，此类样本运行后，将会释放展示正常的诱饵以迷惑受害者，同时后门将继续在后台运行以窃取受害者计算机敏感信息。

Lazarus APT组织近期针对区块链金融、能源行业的攻击活动分析

标签：Lazarus，C2，APT
链接：https://mp.weixin.qq.com/s/axdINLybUO3b7U-i8H-Bww

Lazarus APT组织是疑似具有东北亚背景的APT团伙，该组织攻击活动最早可追溯到2007年，其早期主要针对韩国、美国等政府机构，以窃取敏感情报为目的。自2014年后，该组织开始针对全球金融机构 、虚拟货币交易所等为目标，进行以敛财为目的的攻击活动。
据公开情报显示，2014年索尼影业遭黑客攻击事件，2016年孟加拉国银行数据泄露事件，2017年美国国防承包商、美国能源部门及英国、韩国等比特币交易所被攻击等事件都出自APT组织Lazarus之手。
近日，奇安信红雨滴团队使用内部高价值样本狩猎流程捕获多个Lazarus组织新的攻击样本，相关攻击活动具有以下特征：

- 本次鱼叉式网络攻击活动中，攻击目标包括区块链与石油天然气等行业，使用了zip打包Lnk后缀文件或和诱饵文件。
- Lnk文件使用了的伪装后缀包括txt、pdf、docx等，运行后打开谷歌云盘的诱饵文件或自释放诱饵文件，并同时加载具有后门功能的恶意js代码，将恶意Lnk文件写入到%startup%文件夹中。
- 近期捕获的诱饵样本标题包括Security Bugs in rigs.zip（钻机安全漏洞），SALT Lending Opportunities.zip （SALT Lenging工作机会），New Development Guidelines.zip （新发展指南），Blockchain Intelligence Group Opportunities.docx.lnk（区块链智囊团工作机会），JP Morgan Chase Job Opportunities.pdf.lnk（摩根大通工作机会）。涉及的企业包括J.P. 摩根大通、SALT Lenging等。

- 未发现影响国内。

APT组织使用加强型TTP瞄准印度国防官员

标签: Side Copy, C2, APT
链接: https://blog.cyble.com/2021/09/14/apt-group-targets-indian-defense-officials-through-enhanced-ttps/

在例行威胁狩猎过程中，Cyble研究实验室发现了某研究人员在[Twitter](https://twitter.com/s1ckb017/status/1435888576710029315)上发布的恶意软件样本，并将该恶意软件归属于Transparent Tribe APT组织。鉴于受害者的性质和攻击目标的方式，Cyble研究实验室发现其与Side Copy APT组织存在相似之处，并对恶意软件及攻击流程进行了分析。

三边行动：针对南亚、中东多国长达数年的网络间谍活动

标签: C2, APT
链接: http://report.threatbook.cn/%E4%B8%89%E8%BE%B9.pdf

近期微步在线捕获数起针对南亚、中东地域多个国家的 APT 攻击活动，主要涉及到签订"恰巴哈尔港协议"的三方成员国，包括伊朗、阿富汗和印度，具有明显的国家战略目的。背后攻击组织进行的历史间谍活动至少可以追溯到2013年，擅长使用钓鱼和水坑攻击，攻击平台涉及到 PC 端和移动端，使用的工具以开源木马为主，同时也具备一定的开发能力，拥有自己的窃密后门。
微步情报局分析有如下发现：

- 此次发现攻击活动背后的组织至少从2013年活跃至今，攻击地域覆盖伊朗、阿富汗、印度和巴基斯坦国家，涉及人权活动家、运输部门、军事、退役军人、极端信仰者和政府部门等；
- 投递的后门具备 PC 和安卓双平台攻击能力，PC 平台使用 PrisrolRAT 和 QuasarRAT 两种后门，安卓平台则使用 AndroRAT 后门；
- 在资产 Whois 信息、AndroRAT 木马配置、攻击目标和地域上，发现该组织和透明部落存在一定的重合，疑似也具备巴基斯坦背景；

Wintervivern组织针对欧洲政府机构的攻击活动

标签: Wintervivern, C2, APT
链接: https://lab52.io/blog/winter-vivern-all-summer/

2021年7月，Lab52发现一个活跃的感染活动,归因于一个名为Wintervivern的组织。Lab52尝试着寻找一些有趣的excel文件，直到发现了一组excel文件，这些文件揭示了一场反对欧洲政府的活动。

重点事件回顾

Review Of Incidents

恶意程序事件

新型安卓恶意软件从378个银行和钱包应用程序中窃取金融数据

金融业

blackrock移动恶意软件背后的运营商重新浮出水面，他们推出了一款名为ermac的新型安卓银行木马程序，该木马的目标是波兰的378个银行和钱包应用程序。

美国农民合作社遭受blackmatter勒索攻击，被要求支付赎金590万美元

政府机关及社会组织

美国农民新合作社遭到 blackmatter 勒索软件攻击，被要求支付赎金590万美元，以防止被盗数据泄露并获得解密器，如果5天内没有支付赎金，赎金将增加到1180万美元。新合作社是一个农民饲料和粮食合作社，在爱荷华州有60多个地方。

新型安卓木马从1000多万用户那里窃取了数百万美元

IT服务业

一项新发现的侵略性移动广告已经感染了来自70多个国家的1000多万用户，这些木马通过看似无害的android应用程序在用户不知情的情况下订阅每月36(约42美元)的高级服务。Zimperium zlabs将这种恶意木马称为“grifhorse”。据报道，澳大利亚、巴西、加拿大、中国、法国、德国、印度、俄罗斯、沙特阿拉伯、西班牙、英国和美国都有受害者。

数据安全事件

印度尼西亚政府的新冠病毒检测程序泄漏130万用户信息

医疗行业

印度尼西亚卫生部官员 Anas Ma’ruf 透露，该国的 COVID-19 测试和追踪应用程序存在固有的安全漏洞，大约 130 万人的个人信息和健康状况因此而暴露。有关人士表示:“这一漏洞是在早期版本中发现的，从2021年7月开始就没有更新过。”

黑客泄露了 500,000 个 Fortinet VPN 帐户的密码

IT服务业

一名黑客泄露了近 50万 个 fortinet vpn 登录名和密码的列表，据称这些名称和密码是去年夏天从可利用设备中获取的。虽然该黑客声称利用的 fortinet 漏洞已被修补，但许多 vpn 凭据仍然有效。此次泄漏是一起严重事件，因为 VPN 凭据可能允许攻击者访问网络以造成数据泄露、安装恶意软件和执行勒索软件攻击。

Microsoft Exchange Autodiscover漏洞泄漏10万个Windows凭据

IT服务业

Microsoft Exchange的Autodiscover功能中的漏洞已在全球范围内泄露了大约10万个windows域的登录名和密码。在guardicore的安全研究avp amit serper的一份新报告中，研究人员揭示了Autodiscover协议的不正确实现是如何导致Windows凭证被发送到第三方不可信网站的。

38亿俱乐部和Facebook用户记录被在线出售

IT服务业

一个黑客论坛的用户正在出售一个据称包含38亿clubhouse和facebook用户记录的数据库。据称，该数据库是将之前从clubhouse秘密数据库中收集的38亿个电话号码与用户的facebook个人资料结合起来编制的，似乎包括姓名、电话号码和其他数据。

网络攻击事件

美国政府呼吁修补被大规模利用的 Confluence 漏洞

IT服务业

美国网络司令部 (uscybercom) 2021年9月3日发布了一个罕见的警报，敦促美国组织立即修补一个被大规模利用的 Atlassian Confluence 严重漏洞，因为攻击者正在对 Atlassian Confluence cve-2021-26084 进行大规模利用。

黑客集团利用ProxyLogon漏洞攻击全球酒店

跨行业事件

至少自2019年以来，一个被新发现的网络间谍组织一直在针对世界各地的酒店、政府、国际组织、律师事务所和工程公司等。slovakian网络安全公司eset发现了这个黑客组织(被称为“famoussparrow”)。该组织利用暴露在互联网上的网络应用程序中的多种攻击载体来攻击目标的网络，包括微软sharepoint的远程代码执行漏洞，oracle opera酒店管理软件，以及微软exchange安全漏洞。

一个0day漏洞使100万台物联网设备暴露于风险之中

制造业

一个被广泛使用的物联网(iot)基础设施代码的漏洞，使1万家企业的1亿多台设备容易受到攻击。guardara的研究人员利用他们的技术在nanomq中发现了一个0day漏洞。nanomq是Emq的一个开源平台，它实时监控物联网设备，然后充当消息代理，在检测到非典型活动时发出警报。Emq的产品被用于监测出院患者的健康状况，检测火灾，监控汽车系统，智能手表，智能城市应用等等。

针对VMware vCenter CVE-2021-22005漏洞的有效POC已被公开

IT服务业

针对vmware vcenter中的cve-2021-22005远程代码执行漏洞的一个完全有效的POC已经被公开，并且存在在野攻击。和早期开始流行的版本不同，这种变体可用于在易受攻击的系统上反弹shell，允许远程攻击者启动他们喜欢的代码。该漏洞无需认证，允许入侵者上传文件到vcenter服务器分析服务。

其他事件

蓝牙 BrakTooth 漏洞可能影响数十亿台设备

制造业

统称为 braktooth 的漏洞正在影响来自十多个供应商的片上系统 (soc) 电路上实现的蓝牙堆栈。这一系列问题影响了从消费电子产品到工业设备的各种设备。漏洞类型包括拒绝服务攻击、设备死锁状态、任意代码执行。

这个每周下载数百万次的 NPM 包修补了 RCE 缺陷

IT服务业

流行的 npm 包 pac-resolver 中修复了一个严重的远程代码执行 (rce)漏洞。开发人员 tim perry 发现了该漏洞，只要尝试提交 http 请求，本地网络上的攻击者就可以利用该漏洞在 node.js 进程中启动恶意代码。 该软件包每周接收 300 万次下载，并在 github 上拥有 285,000 个公共依赖存储库。

事件时间线

Timeline Of Incidents

2021-09-01

包含 Guntrader 客户详细信息的数据文件被泄露并共享

DuPage 医疗集团患者的数据泄露

印度尼西亚政府的新冠病毒检测程序泄漏130万用户信息

2021-09-02

70 万法国人的 Covid 测试结果被泄露

Autodesk 透露它是俄罗斯 SolarWinds 黑客的目标

卡巴斯基实验室报告了能自动窃取资金的 Android 木马程序

蓝牙 BrakTooth 漏洞可能影响数十亿台设备

2021-09-03

美国政府呼吁修补被大规模利用的 Confluence 漏洞

2021-09-04

警惕“Windows 11 Alpha”附件

2021-09-05

加密货币交易所Bilaxy受到攻击，黑客窃取了ERC20钱包代币

新西兰的主要 IPS 遭受大规模 DDoS 攻击

2021-09-06

在俄罗斯销售的廉价按键式手机中发现预装恶意软件

FBI IC3 警告性勒索攻击激增

爱尔兰警方破坏了 HSE 攻击者的行动

2021-09-07

这个每周下载数百万次的 NPM 包修补了 RCE 缺陷

麦当劳将数据库的密码泄露给游戏获胜者

Confluence 漏洞导致Jenkins 项目的服务器被入侵

BladeHawk 组织：针对库尔德族群的 Android 间谍活动
研究人员发布了针对 Ghostscript 零日漏洞的 PoC
印尼COVID-19追踪应用报告了两起数据泄露

2021-09-08
霍华德大学在遭受勒索软件攻击后关闭网络
正在进行的 Office 365 0day攻击有一个临时修复
黑客泄露了 500,000 个 Fortinet VPN 帐户的密码
DDoS 攻击破坏新西兰银行和邮局
700万以色列人的个人信息可供出售

2021-09-09
Yandex 遭受 Runet 历史上最大的 DDoS 攻击
Zoho警告0day身份验证绕过漏洞正被广泛利用

2021-09-10
南非司法部网络系统遭到黑客攻击陷入瘫痪
联合国称入侵者破坏了其系统

2021-09-12
专家担心新的Android银行木马SOVA的出现

2021-09-13
BlackMatter 勒索软件团伙袭击了科技巨头奥林巴斯
Vermilion Strike：新的Cobalt Strike Beacon
HHS 就 BlackMatter 攻击警告卫生部门

2021-09-14
新的 Android 银行恶意软件窃取墨西哥用户金融凭证
新的 Zloader 攻击可以禁用Windows Defender
Mēris Bot 感染了 曾在2018 年遭到入侵的 MikroTik 路由器

2021-09-15
匿名黑客入侵Epik网络主机

2021-09-16
健身手环中 16.17 GB 的用户数据被泄露
假 TeamViewer 下载广告分发新的 ZLoader 变体
微软称Windows MSHTML 漏洞现在正被勒索软件团伙利用

2021-09-17
Numando银行木马分析
一种新的 Windows 恶意软件出现
新型Go恶意软件Capoae利用多个漏洞攻击WordPress、Linux
Mirai僵尸网络大肆利用网络漏洞
Ryuk勒索软件团伙利用Microsoft MSHTML漏洞

2021-09-18
南非司法部遭受勒索软件袭击

2021-09-19
在黑客勒索1000万美元后，扬克斯市拒绝支付赎金

2021-09-20
针对南美组织的新一波恶意软件攻击
共和党州长协会电子邮件服务器被黑客攻破
DDoS勒索攻击中断VoIP.Ms电话服务
美国农民合作社遭受blackmatter勒索攻击，被勒索590万美元

2021-09-21
泰国1.06亿游客的数据在网上泄露
图拉黑客组织发起针对美国和阿富汗的新的后门攻击
BlackMatter袭击爱荷华州农民合作社
俄罗斯黑客使用TinyTurla恶意软件作为二级后门

2021-09-22
VMware修复了vCenter Server中的一个严重漏洞
新的Nagios软件漏洞可能让黑客接管IT基础设施

美国财政部将俄罗斯加密交易所列入黑名单
微软警告说将有大规模的PHaaS出现
pNetwork遭受了价值1200万美元的比特币损失
海康威视摄像头存在严重漏洞，可能被远程黑客攻击
微软Exchange Autodiscover漏洞泄漏10万个Windows凭据

2021-09-23
哥伦比亚房地产中介公司的10万买家数据泄漏
Microsoft Windows中的一个新漏洞可能让黑客轻松安装Rootkit
新的Mac恶意软件冒充合法的macOS工具欺骗用户
新型安卓恶意软件用新冠病毒信息作为诱饵,攻击美国与加拿大用户
黑客利用MSHTML漏洞攻击俄罗斯国防部火箭中心
黑客集团利用ProxyLogon漏洞攻击全球酒店
黑客入侵了俄罗斯和其他十多个邻国政府机构雇员的账户
一个0day漏洞使100万台物联网设备暴露于风险之中

2021-09-24
38亿俱乐部和Facebook用户记录被在线出售
新型恶意软件攻击印度国防人员

2021-09-25
黑客利用“双倍现金”在Bitcoin.org中窃取17000美元
休斯顿港遭到Zoho 0day漏洞攻击
欧洲呼叫中心遭受勒索软件攻击
FBI决定扣留Kaseya勒索软件解密密钥引发争议

2021-09-26
Drinik恶意软件欺骗用户提供他们的手机银行详细信息
JSC GREC Makeyev和其他俄罗斯实体受到攻击

2021-09-27
来自WhatsApp的虚假备份消息向西班牙用户发送恶意软件
新型恶意软件BluStealer出现

新发现的ZE Loader针对网上银行用户进行攻击
Jupyter infostealer通过MSI安装程序进行传播
新安卓恶意软件从378个银行和钱包应用程序中窃取金融数据
假安装者丢弃恶意软件并为机会主义攻击者打开大门
新型恶意软件窃取Steam、Epic游戏商店和EA源帐户

2021-09-28
SolarWinds黑客利用FoggyWeb后门攻击ActiveDirectory服务器
Squirrelwaffle：新型Cobalt Strike加载器

2021-09-29
新型安卓木马从1000多万用户那里窃取了数百万美元
儿童童话应用Farfaria暴露了290万用户的数据
复杂网络攻击袭击GiantPay
黑客以巴西PIX支付系统为目标，盗取用户的银行账户
针对VMware vCenter CVE-2021-22005漏洞的有效POC已被发现
专家首次观察到FinFisher感染涉及使用UEFI引导套件

2021-09-30
Forward Air Corporation最近披露了一起勒索软件攻击后的数据盗窃事件

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9月，全球新增的活跃勒索病毒家族有 :AtomSilo 、 BlackByte 、 Groove 、 Sodinokibi(REvil) 等 勒 索 软 件 。 其 中 AtomSilo的数据泄露网站与BlackMatter高度相似，两者可能存在密切关系；Groove勒索软件由Babuk核心成员之一开发，并创建了一个名为RAMP的暗网论坛；消失近两月的Sodinokibi(REvil)在本月正式回归。

目录预览

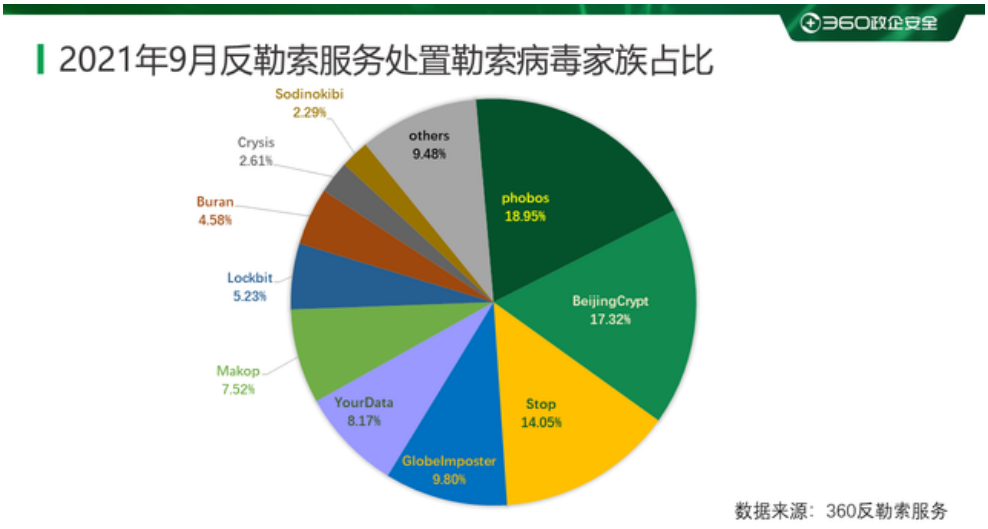
勒索病毒态势分析

Ransomware Situation Analysis

一、感染数据分析

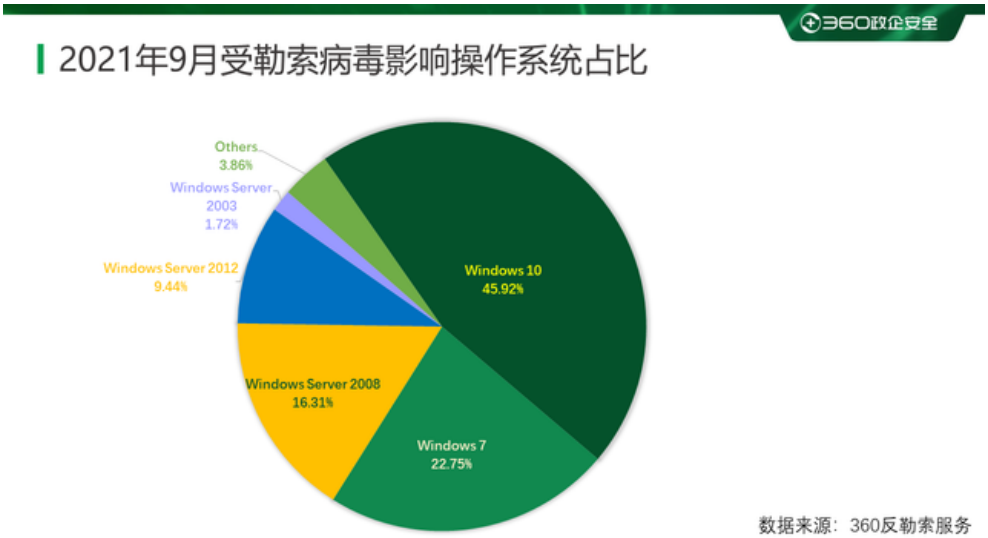
针对本月勒索病毒受害者所中勒索病毒家族进行统计，phobos家族占比18.95%居首位，其次是占比17.32%的BeijingCrypt，Stop家族以14.05%位居第三。

本月BeijingCrypt勒索感染量有大幅度的上升，从8月份的4.06%上升至本月的17.32%。在本月底，该家族出现新的变种，将被加密文件后缀修改为“.520”。



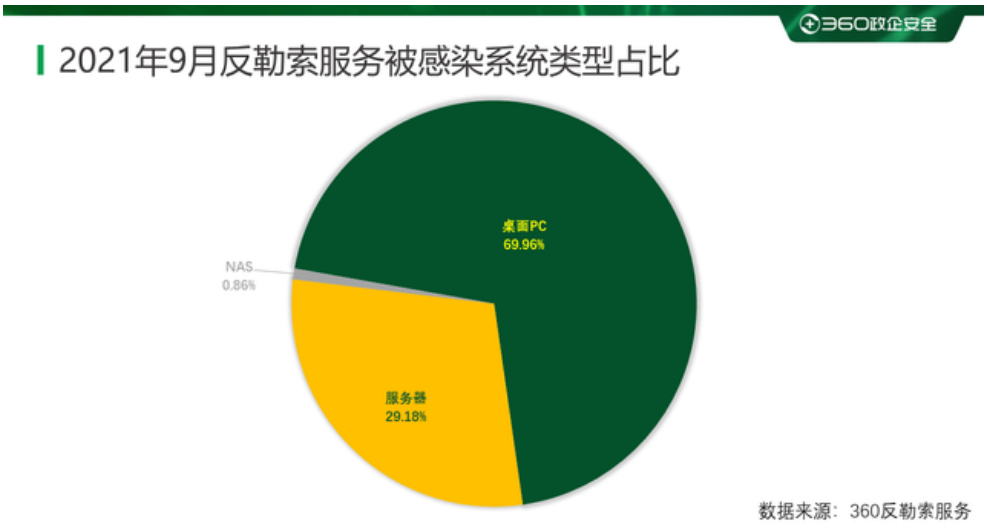
数据来源：360反勒索服务

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 10、Windows 7、以及Windows Server 2008。



数据来源：360反勒索服务

2021年9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。

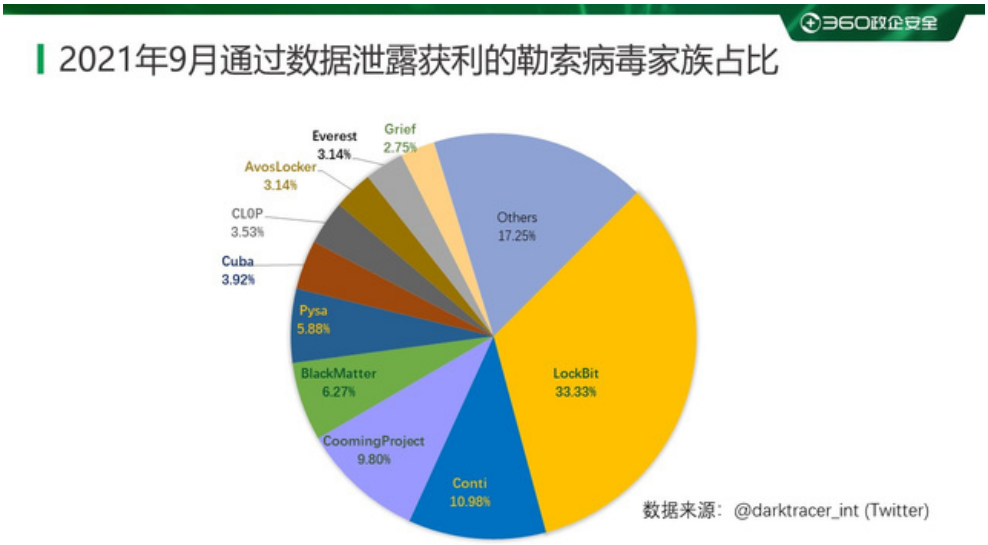


二、黑客信息披露

以下是本月收集到的黑客邮箱信息：

predator3@gmx.us	Arenono@protonmail.com
1527436515@qq.com	iosif.lancmann@mail.ru
monster666@tuta.io	decryptionwhy@india.com
pecunia0318@goat.si	predatorthre@bigmir.net
pagar40br@gmail.com	lialumpolis@tutanota.com
clean@onionmail.org	paybackformistake@qq.com
recofile@firemail.cc	FilesRecoverEN@Gmail.com
drac1on@tutanota.com	d4tab3ckup@onionmail.org
BrusLi@aolonline.top	xdatarecovery@msgsafe.io
RansHelp@tutanota.com	JimThompson@ctemplar.com
hoti2020@tutanota.com	Resp0nse1999@tutanota.com
guan_yu@mailfence.com	FerdinandCohn1828@gmx.com
louisvega@tutanota.com	harmagedon0707@airmail.cc
ithelp02@decorous.cyou	pecunia0318@protonmail.ch
HydaHelp1@tutanota.com	melling@confidential.tips
tspans@privatemail.com	retrievedata300@gmail.com
ormecha19@tutanota.com	cyberlock06@protonmail.com
decryptdelta@gmail.com	biggylockerteam@yandex.com
Leslydown1988@tutanota.com	AstraRansomware@protonmail.com
adolfgizbreht234@gmail.com	recoveryscmyfiles@mail2tor.com
CHRISTIAN1986@TUTANOTA.COM	JamesHoopkins1988@onionmail.org
janelle2021@protonmail.com	ollivergreen1977@protonmail.com
ithelp02@wholeness.business	anonymoushacks33@protonmail.com
clay_whoami_1@protonmail.ch	CCSMEDIA.COMPLIANCE@protonmail.com
baltassarebruno1999@tuta.io	BM-2cUm1HG5NFf9fYMhPzLhjoBdXqde26iBm2@bitmessage.ch
decryptioner@uncryptfile.com	BM-2cUaG3dRVoUVQEf9rJNhPxdyfYfDuxPeQy@bitmessage.ch
unibovwood1984@protonmail.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。

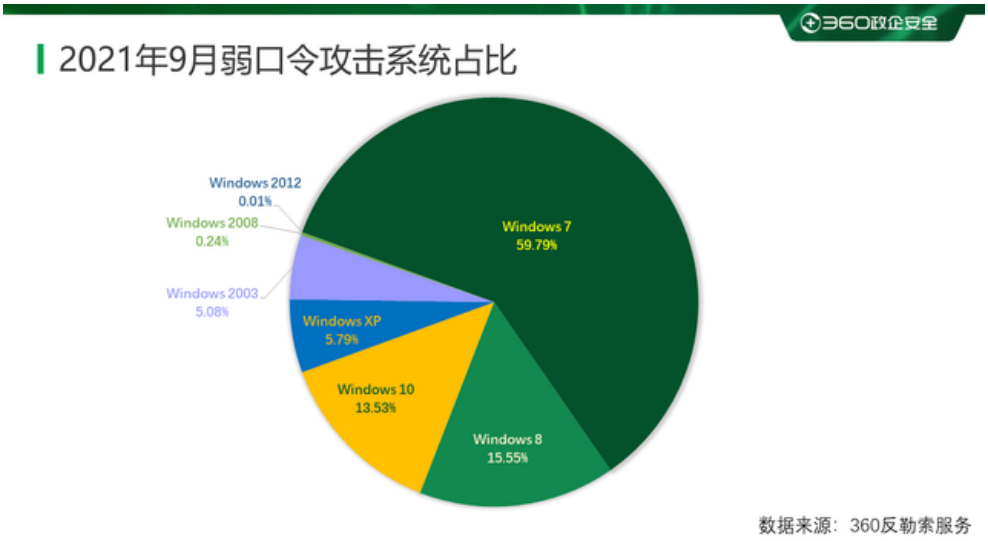
AZA	hbfinanse.pl	CROMOLOGY SERVICES
HBE	atstrack.com	WEST TREE SERVICE
HABI	ebarc.adv.br	Bellissima Fashions
AMAX	grupowec.com	MangaDex - MangaDex
VIVEA	ibes-gmbh.de	odeffinancierasa.hn
Dohuk	noone.com.au	Irish Pioneer works
Andel	drsdoors.com	shop.jerryleigh.com
UUOOI	novotech.com	hotelservicepro.com
Axley	C & C FRANCE	scisairsecurity.com
Bulley	Aria Systems	transrendufense.com
Saurer	IJmond Werkt	pulmuonewildwood.com
Nwdusa	dataspeed.it	ATIVY CYBER SECURITY
Butali	RTI Surgical	royalporcelain.co.th
Irz.de	GEO-Alpinbau	Jesse Engineering Co
Phminc	newhotel.com	One Community Health
Ohagin	Famous Supply	mitchellsternlaw.com
Linkmfg	benner.com.br	Unified Technologies
iibg.ca	SUNSETHCS.COM	Office Star Products
calsoft	ROC Mondriaan	Unione Reno Galliera

Fountain	jaylon.com.au	rabbalshedekraft.com
Wibernet	alderking.com	Chamco Industries Ltd
nrpa.org	crystalvalley	Trust Capital Funding
AUTO.RIA	cheadlelaw.com	soenen-golfkarton.com
myyp.com	GENESISNET.COM	Haverhill High School
parcoinc	cansmart.co.za	EQUITY TRANSPORTATION
Meriplex	Steel Projects	Pramer Baustoffe GmbH
SI Group	BRPRINTERS.COM	United Health Centers
Meditopia	BCP Securities	Macdonald Devin, P.C.
ASSU 2000	Actief-Jobmade	papierswhitebirch.com
comebi.mx	Citrocasa GmbH	buffingtonlawfirm.com
pi-hf.com	hoffsuemmer.de	peabodyproperties.com
Grupo SAN	daylewis.co.uk	FEINBERGLAWOFFICES.COM
Southland	Memory Express	Global Crypto Exchange
Elementia	hoistcrane.com	novohamburgo.rs.gov.br
ds.net.au	Schultheis-ins	EMPIRICAL-RESEARCH.COM
Real Time	Potter Concrete	johncockerillindia.com
PeakLogix	remedios.lawyer	Huali Industrial Group
KESSEL AG	hpe-konstanz.de	Cedar Grove Composting
PRECREDIT	Dassault Falcon	River City Construction
Grupo GSS	STORAFILE.CO.UK	BLUEBONNETNUTRITION.COM
amista.cz	ohiograting.com	Modern Testing Services
advint.com	Xmedicalpicture	Plastipak Holdings, Inc.
advint.com	miller-rose.com	Hörmanseder Stahlbau GmbH
Journality	TPI Corporation	coldwellbankerhubbell.com
Ellerboeck	SCREEN Holdings	Marans Weisz & Newman, LLC
Miningbase	CasagrandeGroup	Bumper to Bumper Autoparts
Technicote	j-addington.com	Barlow Respiratory Hospital
BPATPA.COM	northstarak.com	Spartanburg & Pelham OB-GYN
tesa46.com	Amphenol Canada	Charles Crown Financial Ltd
ofplaw.com	robsonstreet.ca	The Plastic Forming Company
gahesa.com	IN2 Engineering	DEBTIN CONSULTANTS (PTY) LTD
cimico.net	advantecmfs.com	PrÃ©-Sal PetrÃ³leo S.A. PPSA
aathonrton	Vera Wang Group	Whitefish River First Nation
esopro.com	Karavan Trailers	Annonces et Vous Particuliers
dykman.com	LJ Hooker Aspley	VIVA Formwork and Scaffolding
51talk.com	Align Technology	Eisvogel Hubert Bernegger GmbH
sete.co.uk	Iraqi Government	Afohs Club â Enjoy The Pride
anasia.com	autohausdaehn.de	Beat The System With Beatchain
denark.com	callabsolute.com	northwoods & spectrumfurniture
DataXsport	Woodlake Unified	South Carolina State University
fugybat.fr	callabsolute.com	Запатченные fortinet точки входа
Bob Poynter	NASCO Industries	Spiezle Architectural Group Inc.
ludofact.de	LA-Martiniquaise	Gaulhofer Industrie-Holding GmbH

barolit.com	geda-produkte.de	C-PatEx - Cryptocurrency Exchange
prototal.se	texasacehvac.com	Primary Residential Mortgage inc.
cimaser.com	nitropiso.com.mx	Greensville County Public Schools
rlsblaw.com	Pacific City Bank	Cristália - Indústria Farmacêutica
BÖWE SYSTEC	denverhousing.org	Société de transport de l'Outaouais
drhrlaw.com	Creditriskmonitor	Marquez Brothers International, Inc.
iiservz.com	russellwbho.co.uk	United Carton Industries Company Ltd
glenroy.com	wijnendeclerck.be	Hamilton Duncan Armstrong | Law firm
abcp.org.br	BONTEMPI VIBO SPA	Ward Arcuri Foley & Dwyer | Law Firm
riscossa.it	Clay County Clerk	Lancaster Independent School District
tes-amm.com	Jakes Finer Foods	EAP Films and Theatres Private Limited
Aluflexpack	franklinempire.com	Fimmick CRM Hong Kong (www.fimmick.com)
BOSCA S.p.A	TaxLeaf Corporate	Instituto Nacional de Medicina GenÃ³mica
Minjar Gold	YASH Technologies	Catalogue des cours de TÃ©lÃ©com SudParis
vlastuin.nl	calautomotive.com	the NET - Northeast Tennessee Media Group
wortmann.de	Gershman Mortgage	South African National Space Agency: SANSA
ch13bham.com	Bar-Ilan University	The Virginia Federation of Republican Women
WPSD Local 6	Betson Enterprises	Municipal Government of Calamba, Philippines
Sarmad Steel	robinwoodortho.com	Canadian Warmblood Horse Breeders Association - Home
Berding-weil	Pulmuone Co., Ltd.	Synthetic Roofing Products and Information - InterWrap
suenco.co.th	Pines Ford Lincoln	Politeknik Elektronika Negeri Surabaya | Emerging Technology
tovogomma.it	PowerGrid Services	Freewallet | Multi-currency Online Crypto Wallet for BTC, ETH

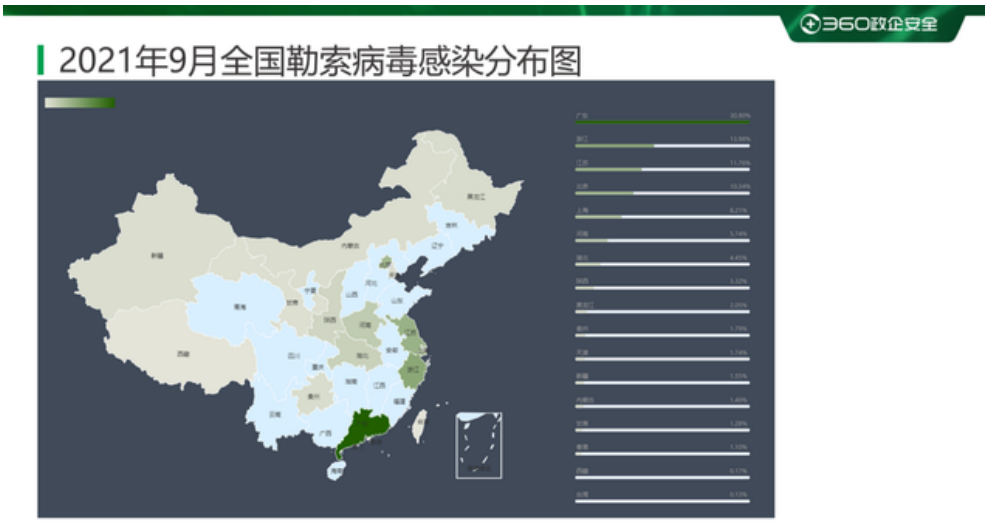
三、系统安全防护数据分析

通过将2021年8月与9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。



数据来源：360反勒索服务

以下是对2021年9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。



数据来源：360系统安全防护

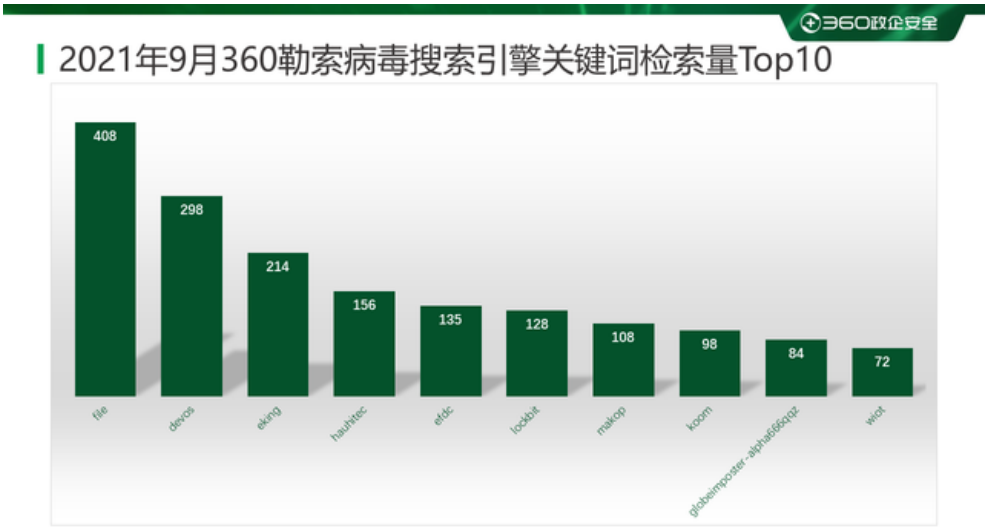
通过观察2021年9月弱口令攻击态势发现，RDP和MYSQL弱口令攻击整体无较大波动。MSQQL属于正常的波动范围。

数据来源：360系统安全防护

四、勒索病毒关键词

- file：属于BeijngCrypt勒索病毒家族，由于被加密文件后缀会被修改为file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。
- 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。
- 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。
- 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。
- efdc：属于Stop勒索病毒家族，由于被加密文件后缀会被修改为efdc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。
- 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。
- 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。
- koom:同efdc。

- GlobeImposter-Alpha666qqz: 属于GlobeImposter勒索病毒家族，由于被加密文件后缀会被修改为GlobeImposter-Alpha666qqz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以及获取数据库口令后远程执行恶意代码加密系统文件。
- nwiot：同efdc。



数据来源：360勒索病毒搜索引擎

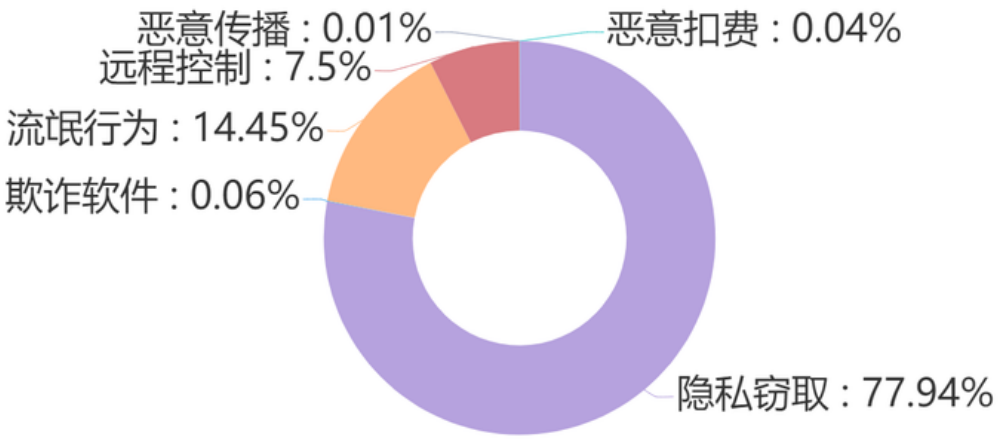
五、解密大师

从解密大师本月解密数据看，解密量最大的是Sodinokibi（REvil），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。

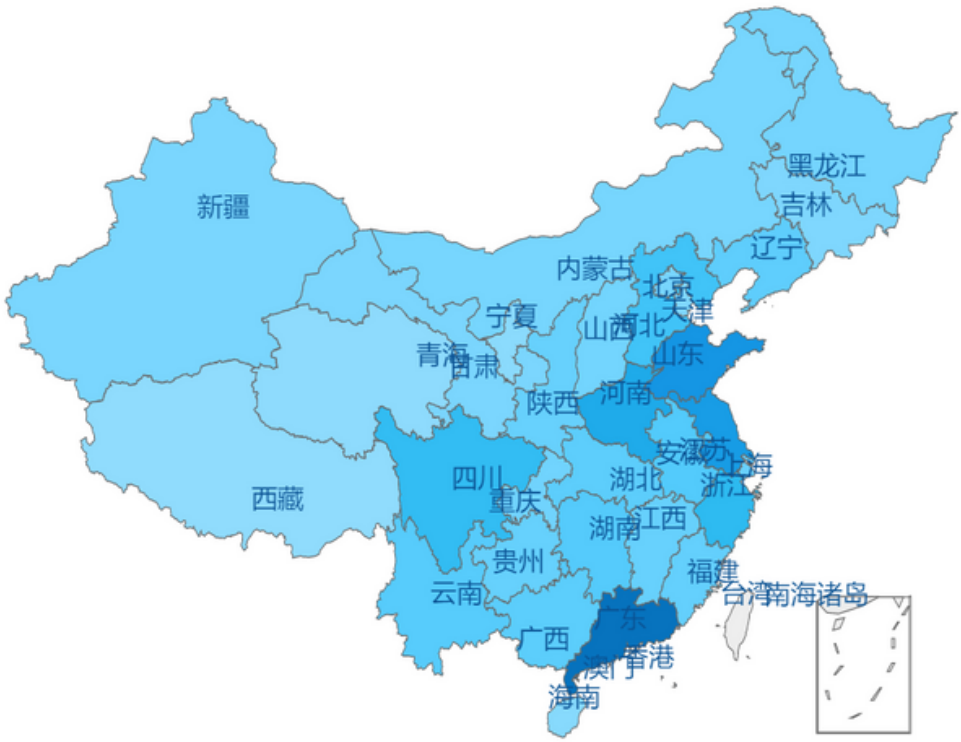
数据来源：反勒索服务统计数据

移动安全数据分析

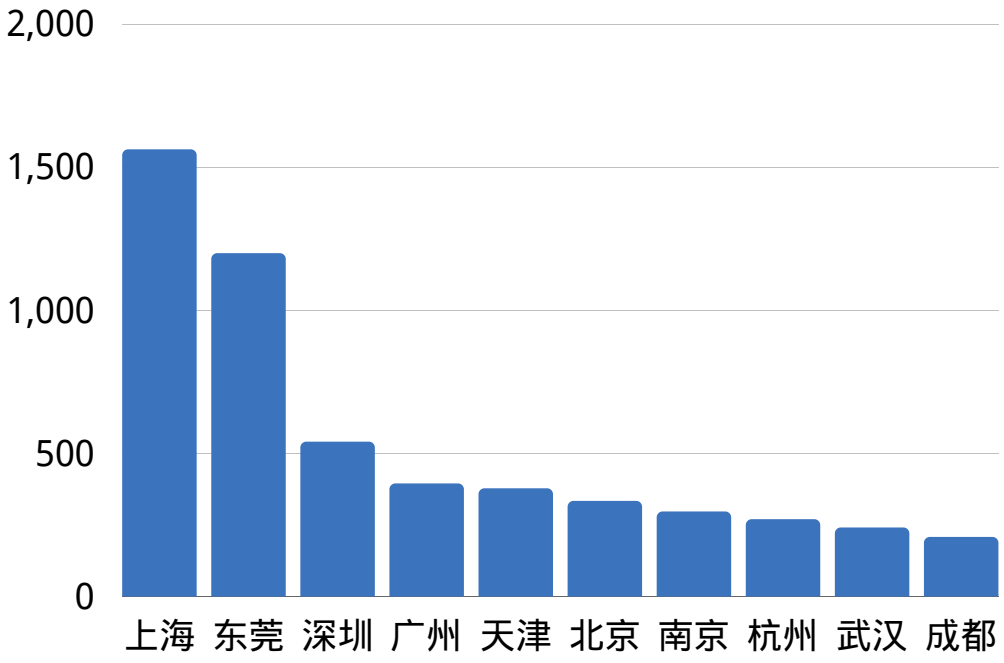
Mobile Security Data Analysis



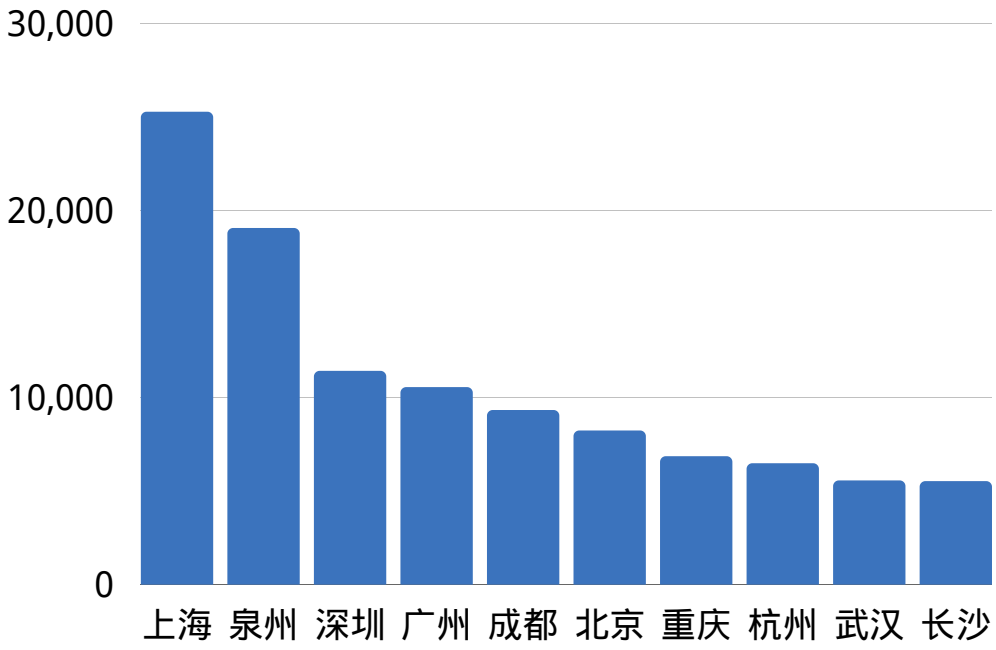
数据总览



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

2021.09

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