360CERT
COMPUTER EMERGENCY READINESS TEAM

总第1期

2021年4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

Chrome 远程代码执行漏洞影响微信
Facebook5.33亿用户数据被发布
针对安全研究人员的最新网络攻击
伊朗核电站遭遇网络攻击
新增的QLocker勒索病毒，短短五天获得260000美元

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

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 是政企安全创新中心的尖兵团队，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4月，360CERT共收录30个漏洞，其中严重15个，高危10个，中危5个。主要包含代码执行漏洞、命令执行漏洞、特权提升漏洞、文件读取漏洞、XML外部实体注入漏洞等。涉及的组件主要是Exchange、Pulse Connect、Chrome、Win32K、GitLab、Homebrew cask等。

二、安全事件

2021年4月，360CERT收录安全事件227项，话题集中在数据泄露、恶意程序、网络攻击方面，涉及的组织有：Microsoft、Google、Facebook、LinkedIn、Twitter、华为等。涉及的行业主要包含IT服务业、政府机关及社会组织、制造业、教育业、金融业、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4月，全球新增活跃勒索病毒:QLocker、WhiteBlackGroup、Jormungand、Cring、Wintenzz、GEHENNALocker、RIP_lmao、Runsomware、Nocry、CryBaby等。其中QLocker是本月新增针对QNAS进行攻击的勒索病毒，短短五天获得260000美元。

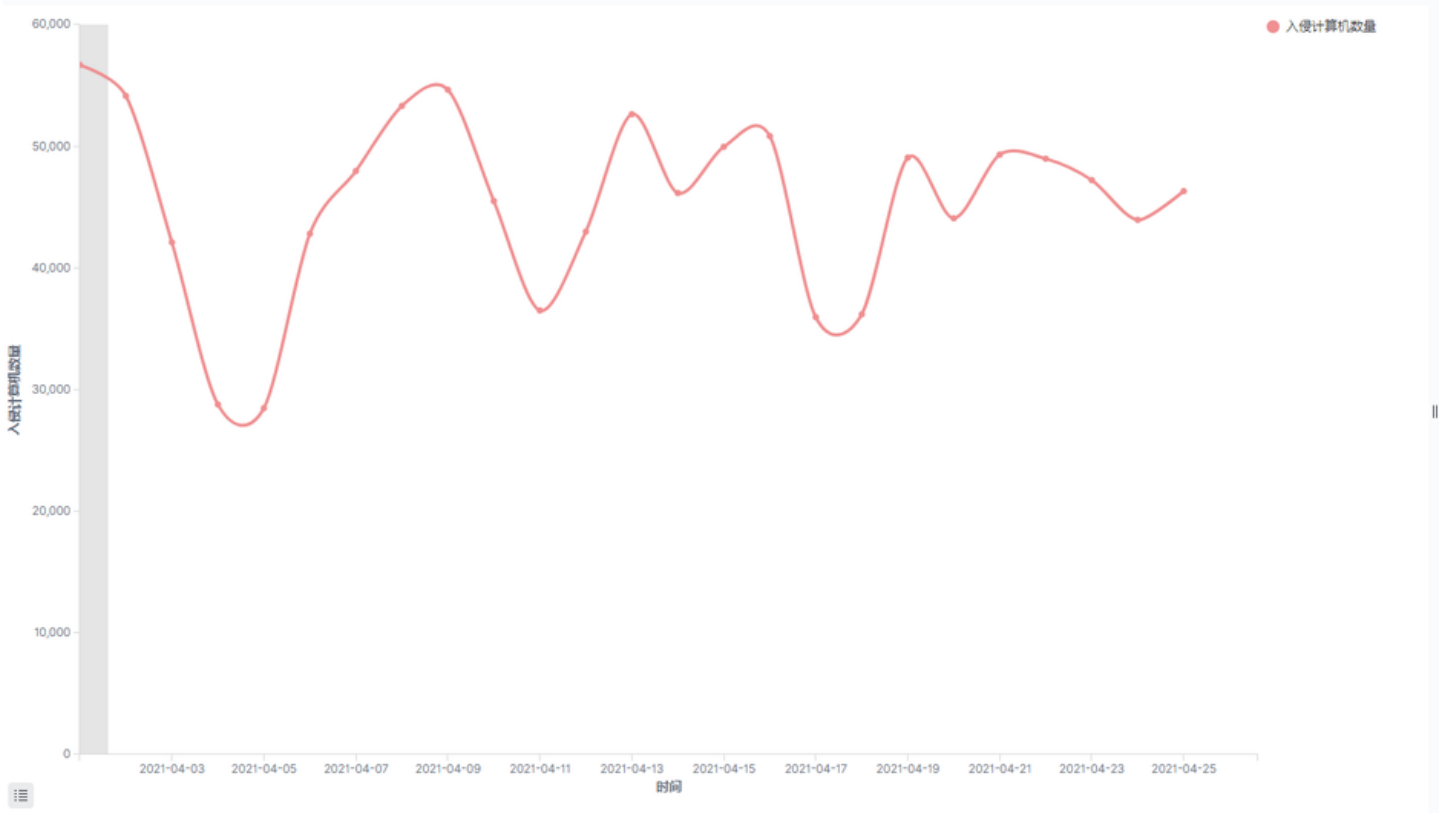
通过移动恶意软件传播TOP10来看，广东、山东、江苏这三个省份恶意软件传播数量依旧占据前列，基本上可以体现人口越集中、经济越发达、移动设备使用数量越多的省份，恶意攻击和软件存活比例越大。

本月攻击态势

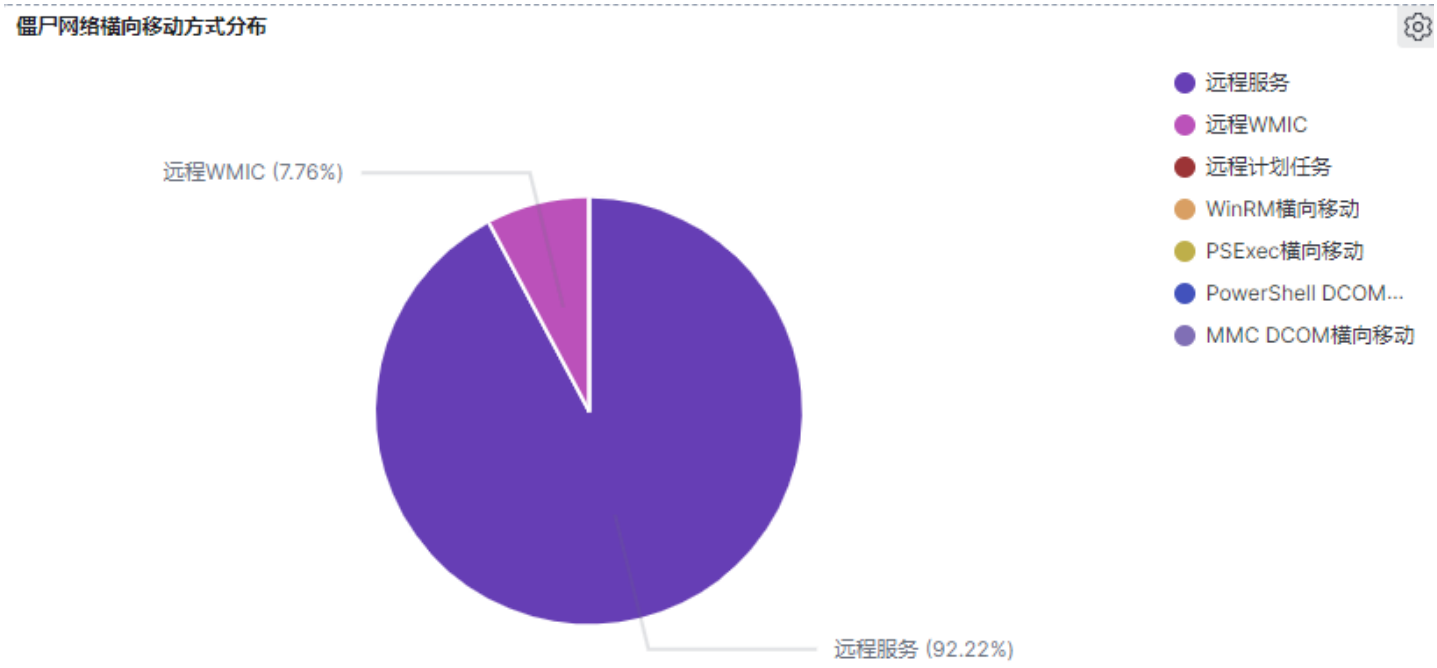
Attack situation analysis

一、僵尸网络攻击

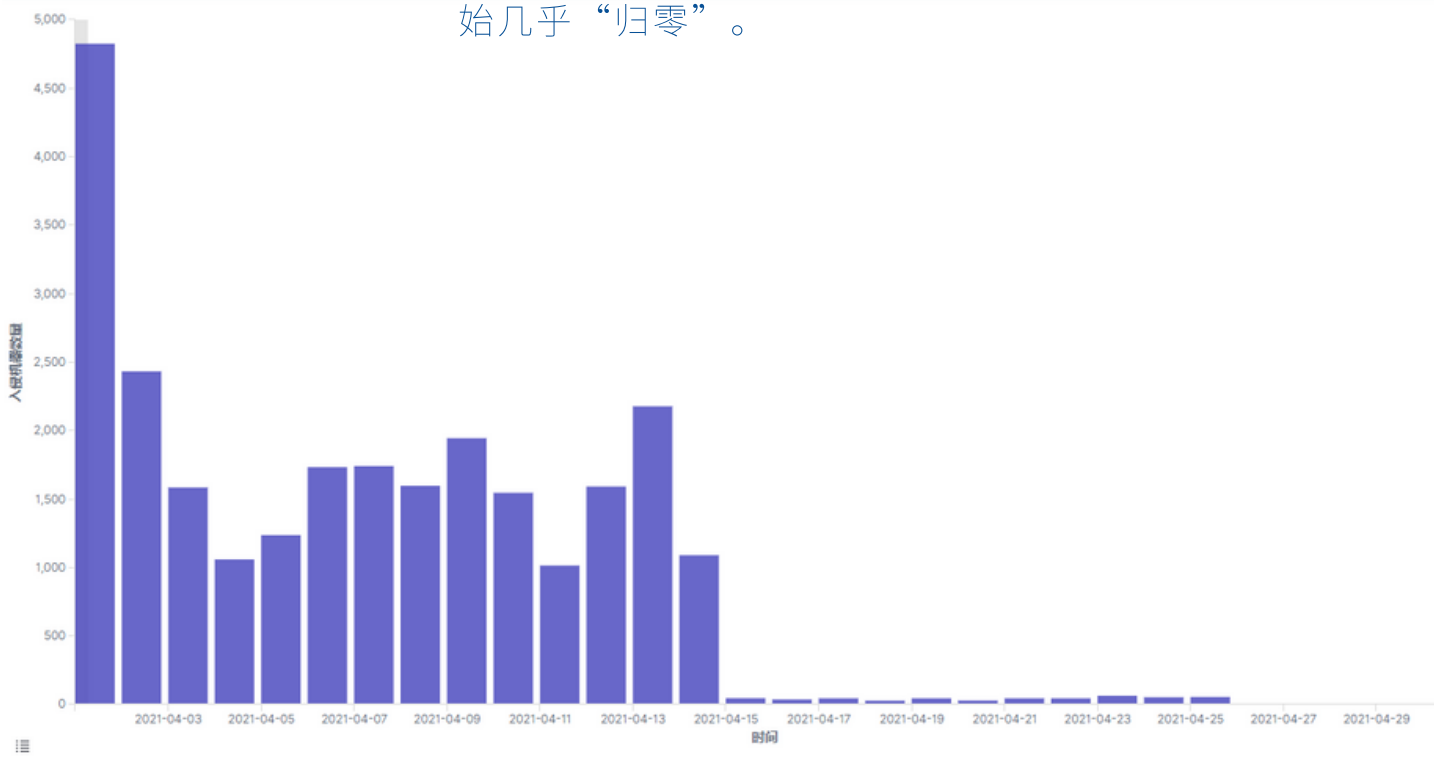
本月Windows系统下僵尸网络活动呈现放缓趋势，原因在于大型挖矿僵尸网络“紫狐”的攻击趋势在进入4月后骤然下降，并在4月15日左右停止攻击。除了“紫狐”外，其他僵尸网络基本呈现稳定状态。4月Windows系统下僵尸网络攻击趋势如下图所示。



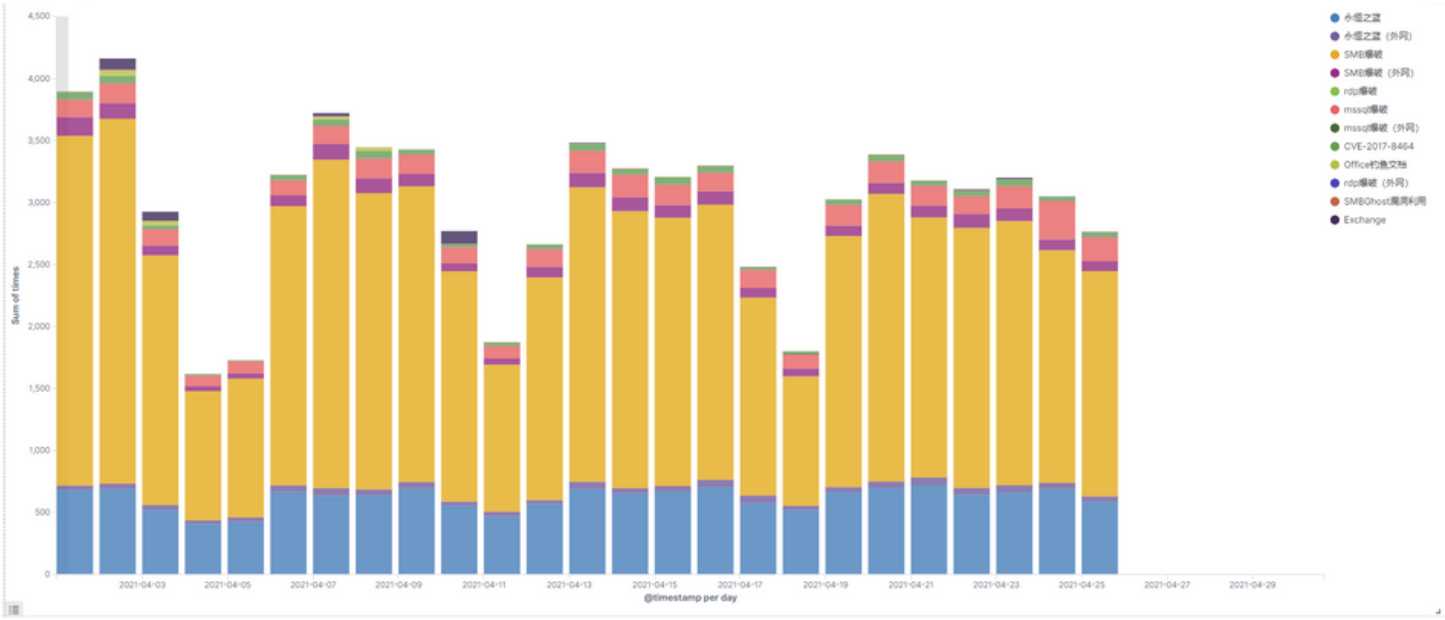
内网横向移动是僵尸网络扩张自身的重要途经。在僵尸网络内网横向移动方式上，远程服务和远程WMI命令执行依然是僵尸网络优先选择的攻击方式，其中92%左右的内网横向移动通过远程服务实现。除了这类攻击手法，“永恒之蓝”漏洞攻击武器也是僵尸网络针对局域网、互联网上暴露资产进行攻击的重要武器。



本月，国内规模最庞大、攻击最活跃的挖矿僵尸网络之一——“紫狐”僵尸网络攻击趋势自4月起骤然下降，并在4月15日左右停止攻击。根据360安全大脑的监测数据，4月15日之后，“紫狐”僵尸网络的内网横向移动、僵尸程序下载等行为几乎停止，被攻击计算机数量从3月份的8000台左右降到不到50台。目前暂时无法确定“紫狐”僵尸网络是为何停止攻击。下图是“紫狐”僵尸网络的攻击趋势图，可以清晰看到，“紫狐”的攻击自4月15日开始几乎“归零”。

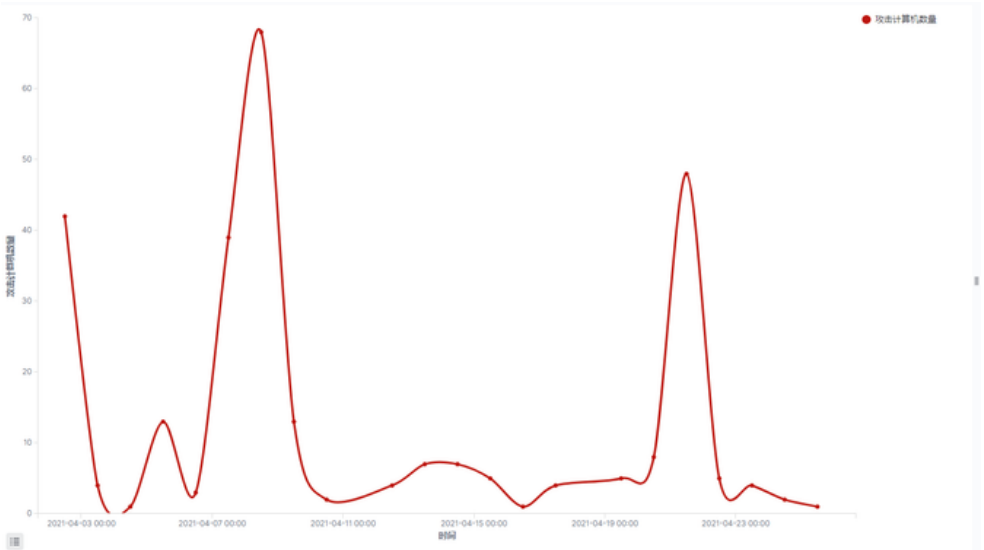


除了“紫狐”僵尸网络外，另一大型挖矿僵尸网络”驱动人生“在本月也有大动作。自3月份Exchange远程代码执行漏洞被曝光以来，“驱动人生”僵尸网络背后控制者持续测试和小范围地利用该漏洞发起攻击，进入四月后，“驱动人生”挖矿僵尸网络开始将Exchange漏洞利用代码集成到攻击模块中，攻击Exchange服务器后在目标服务器中植入WebShell和挖矿木马。下图是“驱动人生”僵尸网络攻击方式分布，其中黑色部分为利用Exchange漏洞发起的攻击，不难看出，“驱动人生”僵尸网络在4月初利用Exchange漏洞发起过一波攻势。

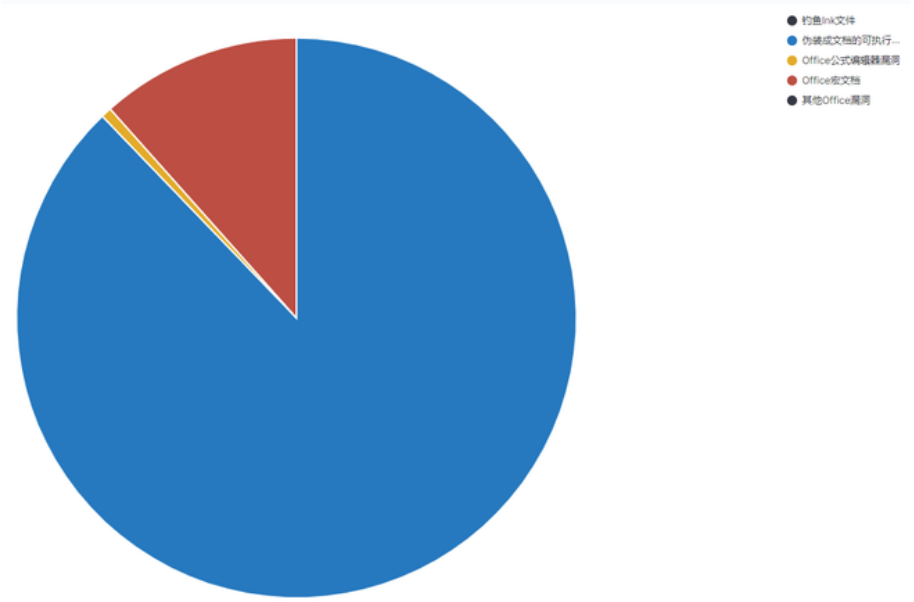


二、钓鱼邮件攻击

本月钓鱼邮件攻击趋势相比较上月有所下降，主要原因在于银行木马活跃度有所下降。本月钓鱼邮件攻击趋势如下图所示。

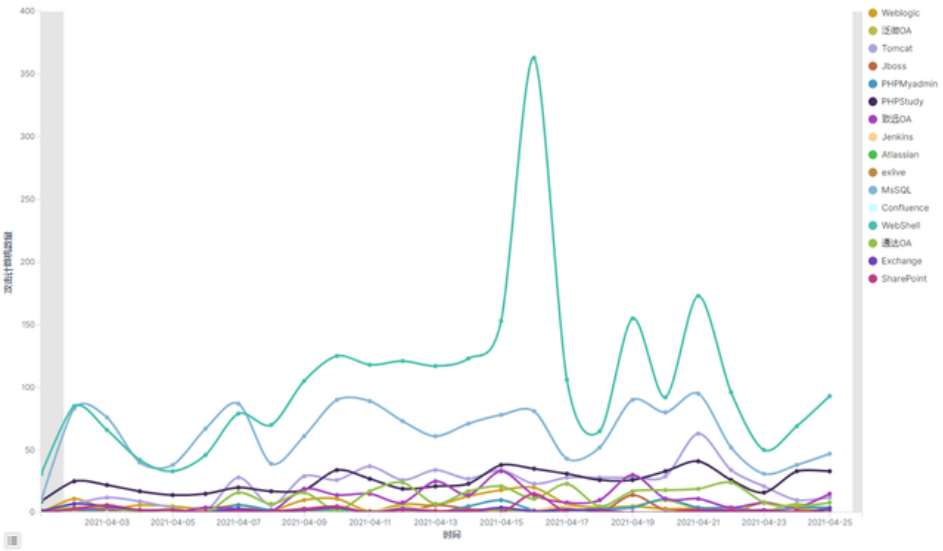


在攻击方式上，伪装成文档的可执行文件是攻击者的首选。攻击者一般以“xxx订单.exe”、“xxx文件.exe”等命名方式命名钓鱼文件。



三、针对Web服务器的攻击

本月针对Web应用和数据库的攻击数量相比3月有显著上升，主要原因在于攻防演练期间攻击队使用大量Web应用和数据库漏洞对防守队的服务器发起攻击。在针对Web应用和数据库的攻击中，通过向网页中植入WebShell发起的攻击数量最多，此外攻防演练期间，针对Tomcat服务、致远OA、通达OA等Web应用或OA系统的攻击也十分频繁。下图展示了4月针对不同Web应用和数据的攻击趋势。



安全漏洞

VULNERABILITIES

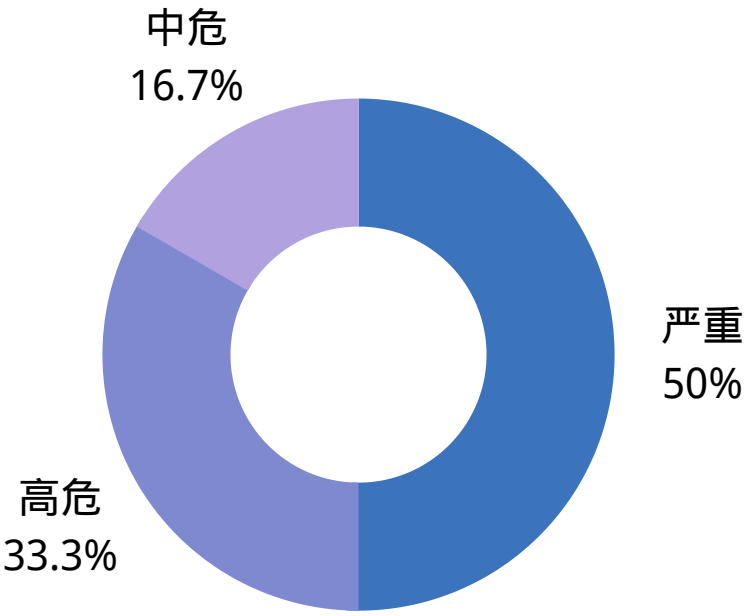
前言

2021年4月，360CERT共收录30个漏洞，其中严重15个，高危10个，中危5个。主要包含代码执行漏洞、命令执行漏洞、特权提升漏洞、文件读取漏洞、XML外部实体注入漏洞等。涉及的组件主要是Exchange、Pulse Connect、Chrome、Win32K、GitLab、Homebrew cask等。

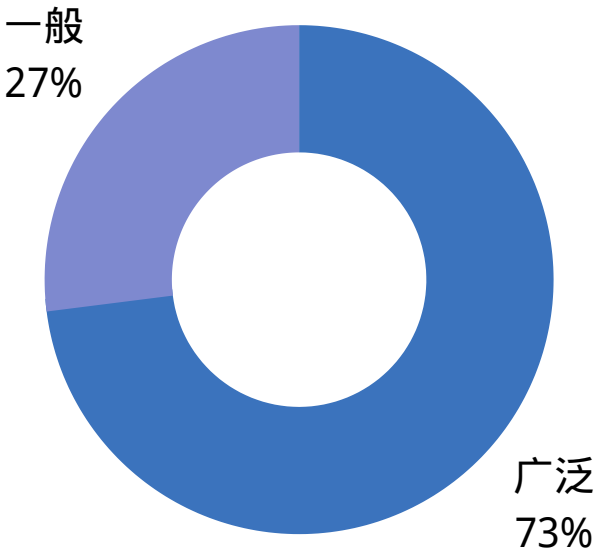
目录预览

漏洞图表

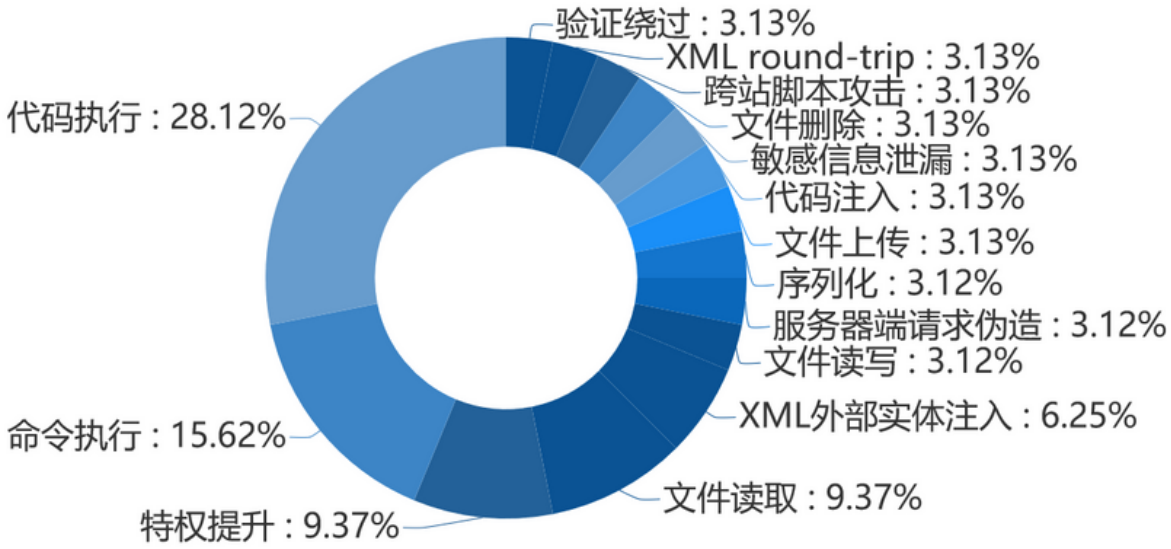
Charts Of Vulnerabilities



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

- Exchange Server
- Pulse Connect
- Chrome
- Win32k
- GitLab
- Homebrew cask
- VMWare Carbon Black Cloud Workload
- Oracle Weblogic Server
- Apache OFBiz
- Cisco Unified
- Cisco SD-WAN vManage
- IBM WebSphere Application Server

热门组件列表

重点漏洞回顾

Review Of Vulnerabilities

Exchange Server多个蠕虫级远程命令执行漏洞 评分：9.8

360CERT监测到Exchange Server中有4个严重漏洞，这些漏洞编号为CVE-2021-28480、CVE-2021-28481、CVE-2021-28482、CVE-2021-28483。攻击者利用这些漏洞，可绕过Exchange身份验证，并且不需要用户交互，即可达到命令执行的效果。同时，这些漏洞是蠕虫级的，所以可在内网的Exchange服务器间横向扩散，请广大用户务必尽快更新。

CVE-2021-22893：Pluse Connect远程代码执行漏洞 评分：10

Pulse Connect远程代码执行漏洞的CVE编号为CVE-2021-22893。Pulse Connect是企业级高性能的VPN系统，在企业中被广泛的使用。Pulse Connect中存在的严重漏洞，允许未通过身份验证的攻击者直接在系统中执行任意代码。建议升级Pulse Connect到9.1R.11.4。

多个Chrome远程代码执行漏洞（影响微信） 评分：9.8

360CERT监测到Chrome中有2个严重漏洞。攻击者利用此漏洞，可以构造一个恶意的web页面，当用户访问该页面时，会造成远程代码执行。同时，这些漏洞威胁到了Windows版微信，攻击者可以通过微信发送一个特制的web链接，用户一旦点击链接，Windows版微信便会加载执行攻击者构造的恶意代码，最终使攻击者控制用户PC。

CVE-2021-28310：Win32k特权提升漏洞 评分：10

2021年04月14日，360CERT监测发现Microsoft官方发布了4月安全更新，其中包括Win32k特权提升漏洞，其cve编号为CVE-2021-28310。成功利用该漏洞的攻击者可以在目标系统上提升权限，根据微软官方的描述，该漏洞很可能已经出现了在野利用。

CVE-2021-22205：GitLab远程代码执行漏洞 评分：9.9

2021年04月16日，360CERT监测发现GitLab官方发布了GitLab安全更新，漏洞等级：严重，漏洞评分：9.9。Gitlab是一个用于管理代码仓库的开源项目，使用Git作为代码管理工具，可通过Web界面访问公开或私人项目。攻击者可以上传特制的图像文件触发远程代码执行。建议尽快将所有运行上述受影响版本的安装升级到最新版本。

Homebrew cask恶意软件包投毒漏洞 评分：10

Homebrew是一款自由及开放源代码的软件包管理系统，用以简化macOS系统上的软件安装过程。Homebrew组织使用review-cask-prGithub Action程序自动审核用户提交的软件包，并将其合并到homebrew-cask或homebrew-cask-*仓库的主分支中。在review-cask-pr中使用了git_diff依赖，当其解析用户提交的合并请求时会对合并进行diff检查，由于其diff检查逻辑存在缺陷，将忽略存在问题的代码，从而使存在恶意代码的合并请求通过验证完成自动合并。

CVE-2021-21982: VMware Carbon Black身份验证绕过漏洞 评分：9.1

2021年04月02日，360CERT监测发现VMware发布了VMSA-2021-0005的风险通告，漏洞编号为CVE-2021-21982，漏洞等级：高危，漏洞评分：9.1。VMware Carbon Black Cloud Workload是一种软件即服务(SaaS)解决方案，提供下一代反病毒(NGAV)、终端检测和响应(EDR)、高级威胁狩猎和漏洞管理，使用单个传感器在单个控制台中实现。攻击者通过访问设备管理界面可获得有效的身份验证令牌，从而可以利用该身份验证令牌查看和更改任意管理配置。

Oracle Weblogic Server多个远程代码执行漏洞 评分：9.8

2021年04月21日，360CERT监测发现Weblogic发布了2021年4月份的安全更新，本次更新了多个严重漏洞，这些漏洞允许未经身份验证的攻击者通过IIOP或T3协议发送构造好的恶意请求，从而在Oracle WebLogic Server执行代码或窃取关键数据。严重漏洞详情如下：

- CVE-2021-2136：未经身份验证的攻击者通过IIOP协议发送恶意请求，最终接管服务器，评分9.8
- CVE-2021-2135：未经身份验证的攻击者通过T3或IIOP协议发送恶意请求，最终接管服务器，评分9.8
- CVE-2021-2157：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终对关键数据进行未授权访问，评分7.5

多个Apache OFBiz远程代码执行漏洞 评分：9.8

2021年04月28日，360CERT监测发现Apache OFBiz发布了漏洞风险通告，共包含2个漏洞，漏洞编号分别为CVE-2021-29200、CVE-2021-30128，漏洞等级：严重，漏洞评分：9.8。OFBiz是一个非常著名的电子商务平台，其提供了创建基于最新J2EE/XML规范和技术标准，构建大中型企业级、跨平台、跨数据库、跨应用服务器的多层、分布式电子商务类WEB应用系统的框架。由于Apache OFBiz存在不安全的反序列化，可能会导致代码执行，服务器被接管。

Cisco SD-WAN vManage多个严重漏洞 评分：9.8

2021年04月08日，360CERT监测发现Cisco官方发布了SD-WAN vManage多个漏洞风险通告，此次通告的漏洞编号分别为CVE-2021-1479（严重）,CVE-2021-1137（高危）,CVE-2021-1480（高危）。这些漏洞是由于易受攻击的组件对输入验证不正确导致的。攻击者可以通过构造特殊的请求来利用漏洞，该请求在被处理时会造成缓冲区溢出的结果。成功利用该漏洞的攻击者可以接管服务器。

漏洞时间线

Timeline Of Vulnerabilities

2021-04-01

暂无编号 严重
GitLab 文件读取漏洞

暂无编号 高危
GitLab 文件读取漏洞

暂无编号 中危
GitLab 跨站脚本攻击漏洞

暂无编号 中危
GitLab 文件读取漏洞

暂无编号 中危
GitLab 文件删除漏洞

2021-04-02

CVE-2021-21982 严重
Carbon Black Cloud Workload appliance 验证绕过漏洞

2021-04-08

CVE-2021-1362 高危
Cisco Unified套件 代码执行漏洞

CVE-2021-1472 中危
RV Routers 文件上传漏洞

CVE-2021-1473 高危
RV Routers 命令注入漏洞

CVE-2021-1479 严重
SD-WAN vManage 代码执行漏洞

CVE-2021-1137 高危
SD-WAN vManage 特权提升漏洞

CVE-2021-1480 高危
SD-WAN vManage 特权提升漏洞

2021-04-13

CVE-2021-27905 高危
Solr 服务器端请求伪造漏洞

CVE-2021-29262 中危
Solr 敏感信息泄露漏洞

CVE-2021-29943 严重
Solr 文件读写漏洞

暂无编号 严重
Chrome 命令执行漏洞

2021-04-14

CVE-2021-28480 严重
Exchange Server 代码执行漏洞

CVE-2021-28481 严重
Exchange Server 代码执行漏洞

CVE-2021-28482 严重
Exchange Server 代码执行漏洞

CVE-2021-28483 严重
Exchange Server 代码执行漏洞

CVE-2021-28310 严重
win32k 特权提升漏洞

2021-04-15

暂无编号 严重
Chrome 代码执行漏洞

2021-04-16

CVE-2021-22205 严重
GitLab 代码执行漏洞

CVE-2021-28965 高危
GitLab 远程代码执行漏洞

2021-04-17

暂无编号 严重

Wechat 代码执行漏洞

2021-04-21

CVE-2021-22893 严重

Pulse Connect 代码执行漏洞

2021-04-22

CVE-2021-20453 高危

WebSphere Application Server XML外部实体注入漏洞

CVE-2021-20454 高危

WebSphere Application Server XML外部实体注入漏洞

2021-04-28

CVE-2021-29200 严重

OFBiz 代码执行漏洞

CVE-2021-30128 严重

OFBiz 序列化漏洞

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

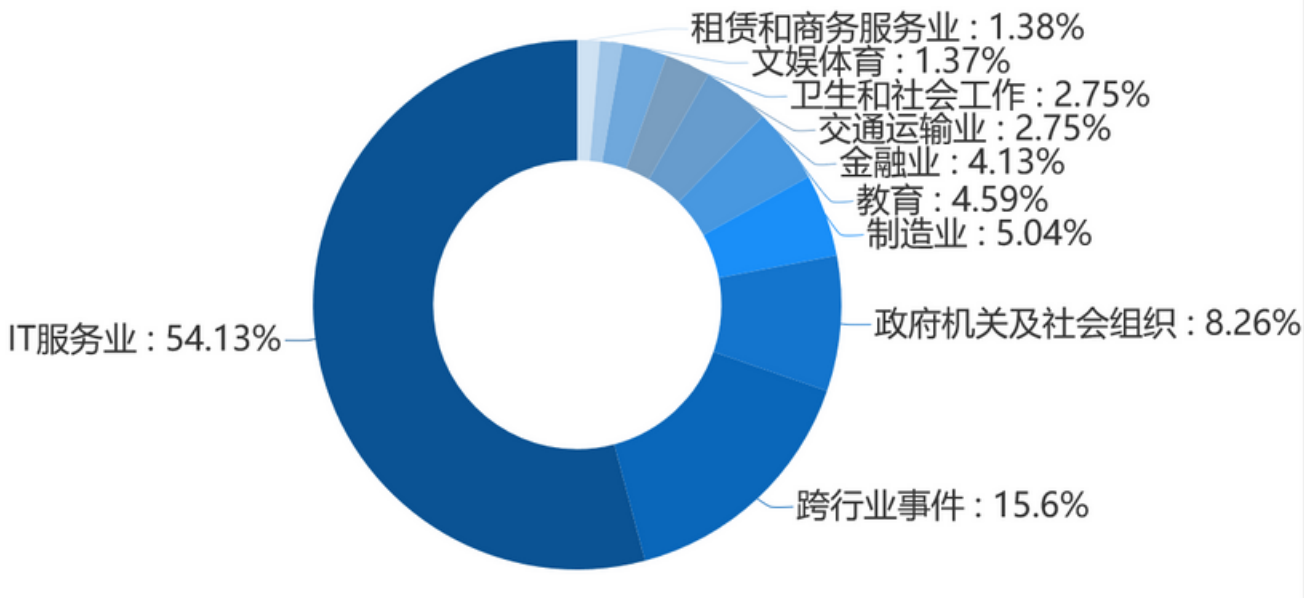
前言

本月收录安全事件227项，话题集中在数据泄露、恶意程序、网络攻击方面，涉及的组织有：Microsoft、Google、Facebook、LinkedIn、Twitter、华为等。涉及的行业主要包含IT服务业、政府机关及社会组织、制造业、教育业、金融业、交通运输业等。

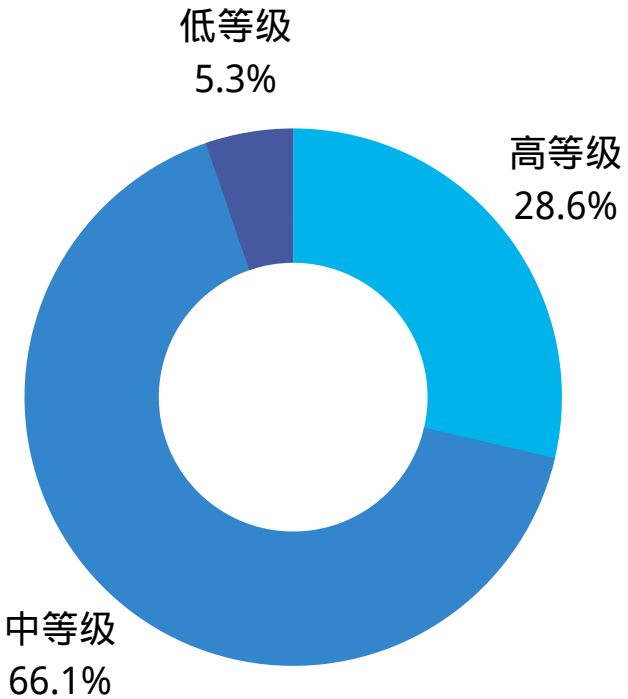
目录预览

事件图表

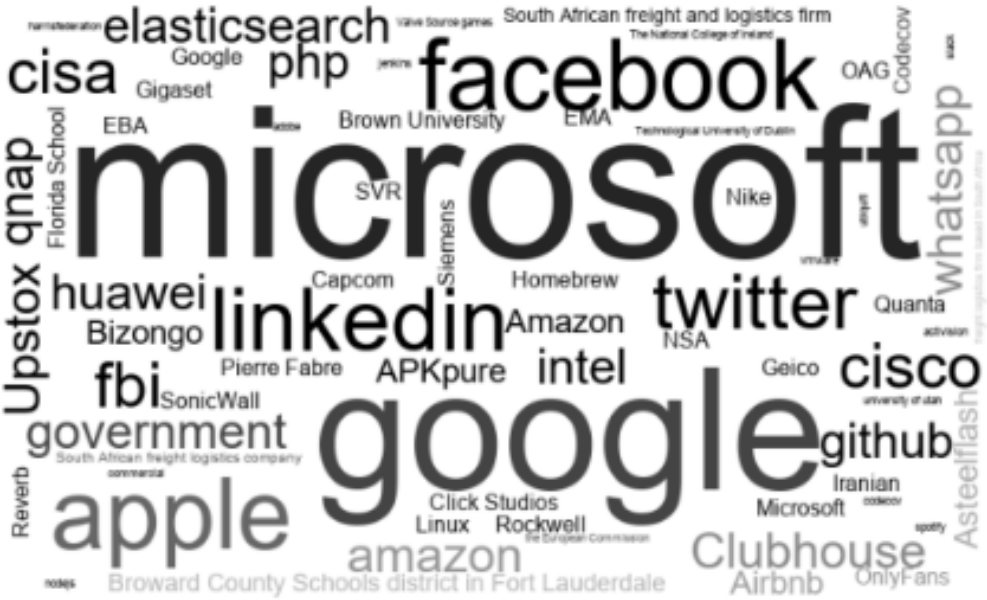
Charts Of Incidents



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

针对性伪装攻击，终端信息安全的间谍--海莲花 APT

标签：海莲花，C2，APT
链接：https://mp.weixin.qq.com/s/WnKc0JbjA5_IsjPFSzFoYA

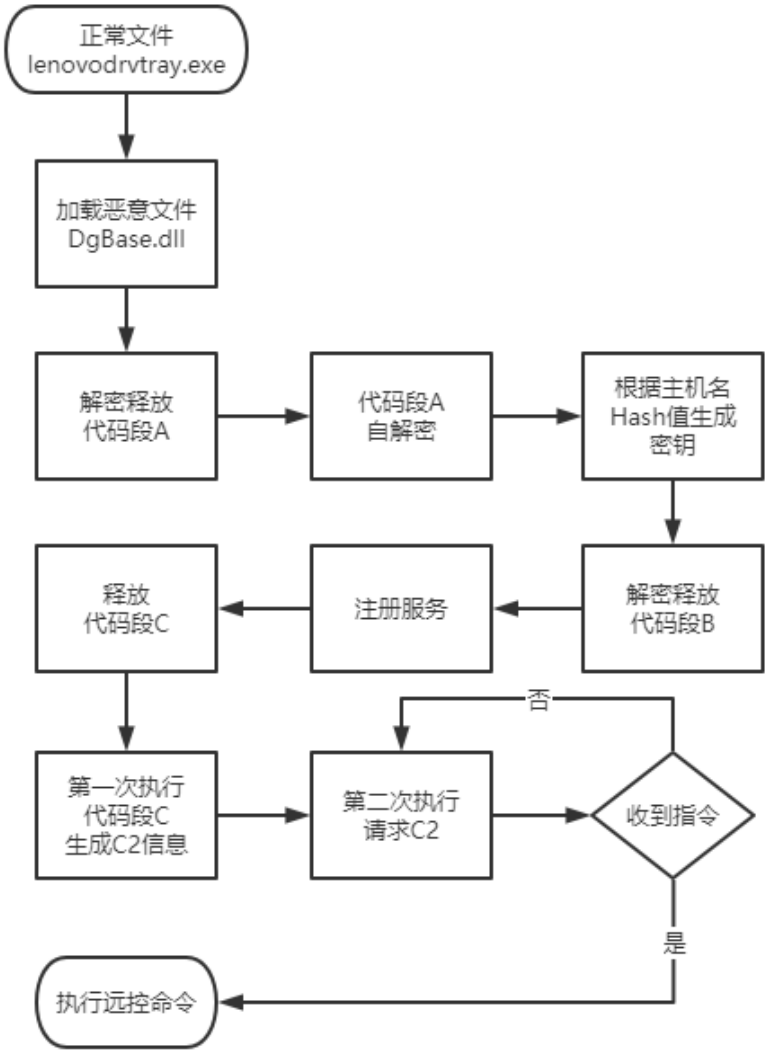
近期，深信服终端安全团队捕获并分析了一个APT样本，经过分析人员确认来自近年来频繁活跃的“海莲花”组织。

“海莲花”组织自首次发现以来，已被发现先后使用了4种不同形态的木马程序。初期的木马程序并不复杂，比较容易被发现和查杀。但近年来捕获的“海莲花”攻击样本均增加了一系列复杂的攻击技术，防护查杀的难度也呈正比增加。

此次深信服终端安全团队捕获的样本就具备了以下特征：

- 白加黑投递，利用正常软件加载恶意攻击载荷
- 精确攻击，只有特定主机才能解密执行远控木马
- 多重加密，在生成最终载荷前，执行了四次解密操作

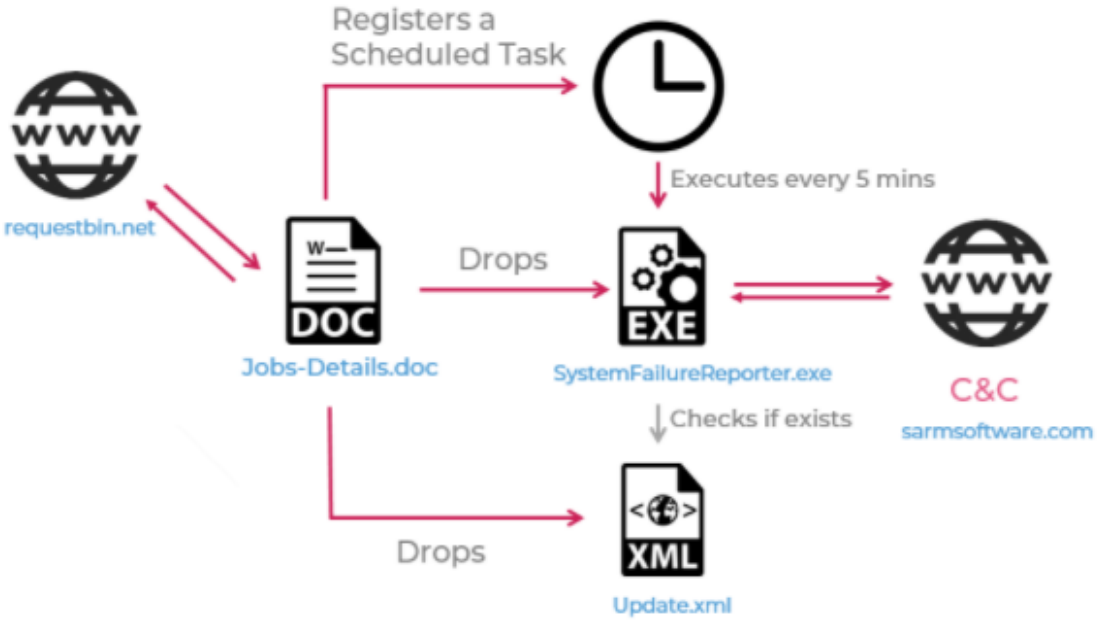
执行流程图如下：



伊朗组织 APT34 使用更新后的武器库发起攻击活动

标签：APT34, C2, APT
链接：https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/

Check Point Research于2021年1月发现了针对黎巴嫩的最新攻击活动，根据攻击时使用的恶意代码、后门、技战术、攻击目标等，将本次活动归因于伊朗背景的组织：APT34。同时，在报告中对 APT34 的攻击行为及其使用的最新后门变种——SideTwist 进行了分析。
攻击者使用了惯用的攻击手法，即向目标投递伪造成招聘信息的恶意文档，一旦受害者启用文档中嵌入的恶意宏，就会触发后续的攻击操作。
攻击流程如下所示：



(你)怕黑吗？小心Vyveva，Lazarus的新后门

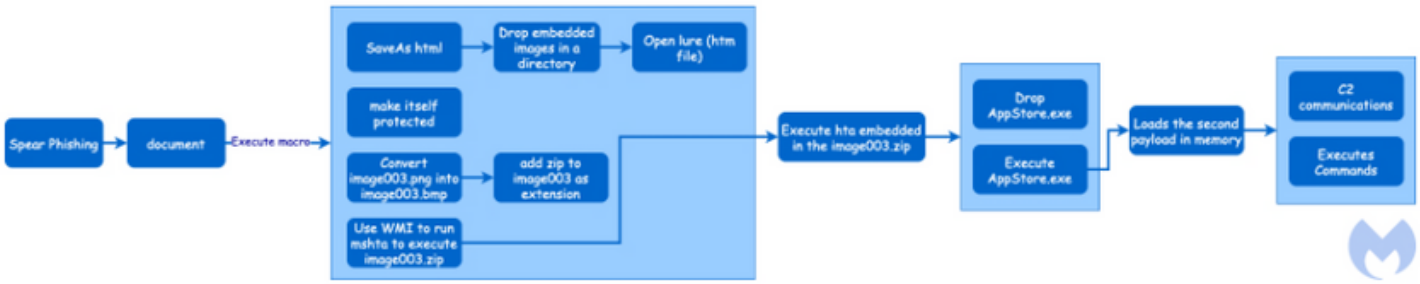
标签：Lazarus, C2, APT
链接：https://www.welivesecurity.com/2021/04/08/are-you-afreight-dark-watch-out-vyveva-new-lazarus-backdoor/

ESET 在2021年4月8日发布报告首次公开分析了之前未知的 Lazarus 后门——Vyveva，该后门包含多个恶意组件，并且通过Tor 网络与攻击者的C&C通信。Vyveva后门具有搜集文件、机器信息的功能，同时具有其他后门的常见功能，如执行攻击者指定的恶意代码。
攻击活动于2020年6月发现，根据已知的两台中招服务器推测，此次攻击主要针对南非地区的物流货运公司，目的可能是窃取信息、收集情报。
ESET通过对Vyveva后门的代码相似度、执行与通信方式等进行分析，将本次攻击活动归因于Lazarus。

Lazarus 使用BMP image文件隐藏恶意代码以释放远控木马

标签：Lazarus, BMP image, C2, APT
链接：https://blog.malwarebytes.com/malwarebytes-news/2021/04/lazarus-apt-conceals-malicious-code-within-bmp-file-to-drop-its-rat/

2021年4月13日，malwarebytes发现了Lazarus针对韩国的攻击，疑似通过分发附带恶意文档的钓鱼邮件作为初始攻击媒介，有趣的是，攻击者将恶意HTA对象嵌入到BMP文件中以释放 RAT Loader，完成后续攻击。
malwarebytes在报告中对本次攻击的样本及过程进行了分析。攻击流如下所示：



深入分析Zebrocy组织的恶意文档

标签：Zebrocy, C2, APT
链接：https://labs.sentinelone.com/a-deep-dive-into-zebrocys-dropper-docs/

Sofacy（又名FancyBear、APT28）至少从2008年开始活跃，主要攻击政府、军事及私营组织，因参与hack-and-leak operations而倍受关注。过去几年，为逃避安全检测与追踪，Sofacy彻底改变了其使用的工具集。而Zebrocy则是与Sofacy高度一致的组织之一，二者的攻击对象都由最初的前苏联国家转向了亚洲地区。
2021年3月，sentinelone观察到针对哈萨克斯坦的攻击活动，攻击中使用了与Zebrocy有联系的恶意软件Delphocy。4月19日发表报告对与Delphocy有关的6个恶意文档进行了分析，并给出了分析人员是如何绕过加密的宏、如何使用IDR (Interactive Delphi Reconstructor)反编译Delphi、以及如何将保存的IDC文件导入到Ghidra中。

Primitive Bear (Gamaredon) 利用时政主题攻击乌克兰政府

标签：Gamaredon, Russia, APT
链接：https://www.anomali.com/blog/primitive-bear-gamaredon-targets-ukraine-with-timely-themes

Anomali Threat Research观察到Primitive Bear于2021年1月至3月下旬，针对乌克兰政府官员的攻击活动。攻击者分发了以政治时事为主题的.docx诱饵文件，试图通过远程模板下载.dot文件。因远程模板通信C&C在发现时已停用，因此尚不清楚本次攻击的最终目的。

透明部落利用新冠疫苗热点对印度医疗行业的定向攻击活动分析

标签：Transparent Tribe, C2, APT
链接：https://mp.weixin.qq.com/s/ELYDvdMiiy4FZ3KpmAddZQ

近日360高级威胁研究院监测到透明部落组织利用疫情相关信息对印度医疗行业进行情报窃取的定向攻击活动。
此次攻击活动涉及的诱饵文档是ZIP包形式，包含一个伪装成PDF的快捷方式，攻击者诱使目标点击lnk快捷方式文件后，lnk文件会调用mshta.exe加载隐藏在远程网页中的hta脚本。

Facebook采取行动阻止巴勒斯坦背景黑客的攻击行动

标签：Preventive Security Service (PSS), AridViper, C2, APT
链接：https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/

2021年4月21日，Facebook发表报告称其已对两个与巴勒斯坦有联系的黑客组织采取行动，包括禁用其社交帐号、阻止对钓鱼域名的访问、公布恶意软件Hash。这两个组织分别为：Preventive Security Service (PSS)（首次公开报道）及 AridViper组织。
Preventive Security Service (PSS)据调查与巴勒斯坦情报部门有关，攻击主要集中在巴勒斯坦和叙利亚境内，土耳其、伊拉克、黎巴嫩和利比亚也有所波及。攻击手法为：定制化Android恶意软件、公开可用的Windows恶意软件、伪造社交账号等。
AridViper攻击活动的受害者为巴勒斯坦的政府官员、Fatah政党成员、学生团体和国家安全部队。攻击时使用了一百多个网站，目的为托管iOS、Android恶意软件以窃取合法登录凭证或者作为攻击通信的C&C，同时Facebook也给出了关于AridViper攻击活动的详细报告（https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf）。

Donot 组织使用已知的攻击模式攻击Android设备

标签：Donot, C2, APT
链接：https://cybleinc.com/2021/04/21/donot-team-apt-group-is-back-to-using-old-malicious-patterns/

Donot(APT-C-35)除了通过发送带有漏洞或恶意宏附件的钓鱼邮件传播恶意软件外，还擅长利用恶意的Android APK对其目标进行攻击。一旦受害者安装了伪造的Android APP，攻击者就可以实现Trojan功能，远程控制受害者的系统并窃取机密信息。
近日，某安全研究员分享了关于Donot伪造APP进行攻击的Twitter消息，Cyble研究人员根据这条推文分析发现：所有伪造的app都包含包“com.update.gooqle”，其伪装成了合法的Google更新程序，并在报告中给出了详细的分析。

Ghostwriter Update：疑似网络间谍组织UNC1151发起了“Ghostwriter”行动

标签：UNC1151, C2, APT
链接：https://www.fireeye.com/blog/threat-research/2021/04/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity.html

2020年7月，Mandiant Threat Intelligence发布报告披露了名为“Ghostwriter”的网络攻击事件，主要针对立陶宛、拉脱维亚、波兰的公民，并在东欧地区宣扬不利于北约组织(NATO)的言论。该事件发生之后，Fireeye对其进行了追踪监控，并确定攻击时间要早于[2020年7月报告](https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html)中给出的开始时间。
2020年7月以来，Fireeye观察到“Ghostwriter”背后的攻击者扩大了其攻击手法、攻击对象范围及TTPs。根据现有证据，Fireeye将部分攻击归因于黑客组织：UNC1151，但是由于情报有限，因此不能将整个“Ghostwriter”事件全都归因于UNC1151。
UNC1151 组织疑似具有政府背景，攻击主要为窃取凭证、部署恶意软件，2021年初，UNC1151 针对德国政客发起了攻击，德国Tagesschau新闻媒体曾进行过报道。

Lazarus 利用工作招聘话题针对大型医药公司发起攻击

标签：Lazarus, C2, APT
链接：https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazarus-recruitment/

2020年9月底，Positive Technologies Expert Security Center（PT Expert Security Center、PT ESC）参与了针对大型医药公司攻击事件的调查，根据此次攻击者使用的TTPs，发现了其与之前的《Operation: Dream Job》和《Operation (노스 스타) North Star：A Job Offer That's Too Good to be True?》存在相似之处，并将此次攻击归因于朝鲜组织 Lazarus。
本篇文章揭示了之前未知的APT行动以及Lazarus的攻击技战术，主要说明Lazarus是如何在短短四天之内获得该公司的部分网络控制权，以及其他的诸如：初始攻击媒介、网络侦察、持久化驻留等方式。
调查之后，PT ESC还发现了其他无关但相似的攻击活动，据称针对的是俄罗斯某公司，并且由安全人员Anonymous Security Agency @AnonySecAgency发[推文](https://twitter.com/AnonySecAgency/status/1329635511393140743?s=19)进行了披露。

重点事件回顾

Review Of Incidents

恶意程序事件

REvil窃取苹果产品蓝图并向其勒索

制造业

Quanta是一家总部位于台湾的原始设计制造商（ODM），并且是Apple Watch、Apple Macbook Air和Apple Macbook Pro的制造商。REvil勒索软件团伙声称他们通过该公司窃取了苹果的产品蓝图，并要求苹果公司在5月1日之前支付赎金，以防止其窃取的数据被泄露。根据Tor付款页面，Quanta或苹果必须在4月27日之前支付5,000万美元，或者在倒计时结束后支付1亿美元，否则相关敏感数据将会被泄露。

Emotet恶意软件被警方强行删除

跨行业

Emotet是近段时间最危险的僵尸网络之一，2021年4月25日，在执法部门1月份发布的恶意软件卸载模块的帮助下，所有受感染的设备中的恶意软件都将被卸载。该模块会更改Emotet恶意软件的配置，将其C2目标指向由警方部署的服务器。之后，执法部门将32位EmotetLoader.dll形式的新Emotet模块分发给所有受感染的系统，这些系统随后将自动卸载该恶意软件。

RotaJakiro:Linux上一个至少隐藏三年的秘密后门

IT服务业

360NETLAB 的 BotMon 系统标记了具有 0VT 检测的可疑 ELF 文件（MD5=64f6cfe44ba08b0babdd3904233c4857），该文件和TCP 443（HTTPS）上的4个域通信，但流量不是TLS / SSL。仔细查看该样本，发现它是针对Linux X64系统的后门程序，该家族已经存在至少3年了，根据它的行为将其命名为RotaJakiro。RotaJakiro使用多种加密算法，并且隐藏踪迹做得非常好，包括使用AES算法对样本中的资源信息进行加密，C2通信组合使用了AES、XOR、ROTATE encryption和ZLIB compression加密算法。

数据安全事件

Facebook 5.33亿用户数据泄漏

IT服务业

5.33亿Facebook用户的数据，包括电话号码、Facebook id、全名、出生日期和其他信息都被发布在网上。安全公司哈德逊洛克（hudsonrock）的首席技术官阿隆·加尔在推特上公布了受影响用户的国家名单，根据他的名单，美国有3230万受影响用户，英国有1150万。

5亿LinkedIn用户数据在暗网销售

IT服务业

在Facebook大规模数据泄露成为头条新闻几天后，一份据称是从5亿LinkedIn个人资料中获取的数据档案已在一个热门黑客论坛上出售，卖家泄露了200万条记录作为证据。这些被泄露的文件中包含了据称被窃取数据的用户的信息，包括他们的全名、电子邮件地址、电话号码、工作场所信息等。

网络攻击事件

针对安全研究人员的最新网络攻击

IT服务业

2021年1月，威胁分析小组记录了一次黑客攻击活动，并将其归因于朝鲜政府支持的一个针对安全研究人员的实体。3月17日，这些黑客为一家名为“ SecuriElite”的假公司建立了一个具有相关社交媒体资料的新网站。该网站谎称自己是一家位于土耳其的红队安全公司，可提供渗透测试、软件安全评估和漏洞利用。与这些黑客以前创建的网站一样，该网站在页面底部也有指向其PGP公钥的链接。

伊朗核电站遭遇网络攻击

能源业

以色列公共媒体称，以色列政府发动的网络攻击导致伊朗一座核电站关闭，伊朗称这是“蓄意破坏”的行为，此次攻击拖延了伊朗浓缩提炼铀进度。

Passwordstate密码管理器被用于供应链攻击

跨行业

Passwordstate是一种本地密码管理解决方案，已被全球29,000家公司的370,000多名安全和IT专业人员使用。它的客户名单中涵盖了政府、国防、金融、航空、零售、汽车、医疗保健、法律和媒体等领域。Passwordstate密码管理器背后的公司Click Studios通知客户，攻击者破坏了该应用程序的更新机制，在破坏其网络后以供应链攻击的形式传播恶意软件。在4月20日至4月22日期间下载了升级程序的客户可能已经中招。

黑客利用0day漏洞攻击MacOS操作系统

IT服务业

苹果发布了macOS操作系统的更新，以解决一个被积极利用的零日漏洞，该漏洞可能绕过所有安全保护，从而允许未经批准的软件在Macos上运行。macOS的漏洞被识别为CVE-2021-30657。

其他事件

VMWare数据中心安全产品中发现严重漏洞

IT服务业

攻击者可以利用VMware Carbon Black Cloud Workload appliance中的一个严重漏洞，绕过身份验证并控制易受攻击的系统，该漏洞编号为CVE-2021-21982，在CVSS评分9.1，影响1.0.1之前的所有产品版本。

PHP Composer漏洞可导致广泛的供应链攻击

IT服务业

PHP的软件包管理器Composer的维护者已发布了一个更新程序，以解决一个严重漏洞，该漏洞可能允许攻击者执行任意命令并给每个PHP软件包安装上后门，从而导致供应链攻击。该漏洞源于处理程序包源时会通过URL下载程序包，当程序包存在后门时，就可能触发远程命令执行。

事件时间线

Timeline Of Incidents

2021-04-01
针对安全研究人员的最新网络攻击

2021-04-02
Asteelflash电子制造商遭遇勒索软件攻击
《使命召唤：战区》恶意软件

2021-04-03
针对加密货币的自动攻击行为
Facebook5.33亿用户数据泄漏

2021-04-05
医疗网络钓鱼事件导致重大数据泄露
黑客通过Linkedin进行钓鱼攻击

2021-04-06
Rockwell FactoryTalk AssetCenter存在严重漏洞
EtterSilent为黑客提供廉价工具

2021-04-07
欧盟委员会和其他机构遭到重大网络攻击
在VMWare数据中心安全产品中发现严重的身份验证绕过错误
Facebook将5.33亿用户的数据泄露归咎于爬虫而非黑客攻击
疑似PHP用户数据库泄漏

2021-04-08
勒索软件瞄准易受攻击的VPN设备
5亿LinkedIn用户数据在暗网销售
0day漏洞仍在影响思科SOHO路由器

2021-04-09
Gigaset Android更新服务器遭黑客攻击，在用户设备上安装恶意软件

2021-04-10
Joker恶意软件感染超过50万台华为Android设备

2021-04-11
新的蠕虫Android恶意软件通过WhatsApp消息传播

2021-04-12
伊朗核电站遭遇网络攻击
Valve游戏引擎漏洞影响多个旗下游戏
勒索软件的发展影响了取证分析
BRATA恶意软件冒充Android安全扫描程序

2021-04-13
NAME:WRECK DNS漏洞影响超过1亿台设备
新的Linux、macOS恶意软件隐藏在假冒的Browserify NPM包中
Capcom勒索事件攻击报告
美国国家安全局发现了影响Microsoft Exchange服务器的新漏洞
研究人员发布Chrome、Edge、Brave、Opera的0day POC

2021-04-14
黑客通过网站联系表格来传递IcedID恶意软件
twitter修复第二个Chrome 0day漏洞
SAP修复了Business Client、Commerce和NetWeaver中的漏洞

2021-04-15
美国国家安全局发布俄罗斯黑客利用的5大漏洞
美国因SolarWinds网络攻击制裁俄罗斯并驱逐10名外交官
未修补的MS Exchange服务器受到加密劫持恶意软件攻击

2021-04-16
工业系统以太网/IP堆栈中报告严重错误
休斯顿火箭队调查勒索软件攻击

2021-04-18
Monero加密货币活动利用ProxyLogon缺陷

2021-04-19
Codecov受到供应链攻击
通过Xcode项目传播的恶意软件开始针对苹果的Mac
Lazarus APT黑客使用BMP图像隐藏RAT恶意软件

2021-04-20
朝鲜黑客利用网络浏览器盗取比特币
黑客假冒微软商店、Spotify网站来传播窃取信息的恶意软件
REvil窃取苹果产品蓝图并向其勒索

2021-04-21
黑客们正积极瞄准VPN设备漏洞
Qlocker勒索软件攻击使用7zip加密QNAP设备
Homebrew远程代码执行漏洞披露
黑客利用虚假的Facebook广告进行网络钓鱼

2021-04-22
“ToxicEye”恶意软件在Telegram平台中泛滥
Joker恶意软件的目标是更多的Android设备

2021-04-23
Passwordstate密码管理器被用于供应链攻击

2021-04-24
黑客入侵安卓手机来模仿联网电视产品

2021-04-26
黑客曝光2.5亿美国户口记录
Reverb泄露音乐家个人信息
32亿个被泄露的密码中包含150万条与政府有关的电子邮件记录

2021-04-27
黑客利用0day漏洞攻击MacOS操作系统

2021-04-28
Apple修补了macOS Gatekeeper被绕过的漏洞
FluBot间谍软件遍布欧洲
F5 BIG-IP易受Kerberos KDC欺骗漏洞攻击

2021-04-29
RotaJakiro: Linux上一个隐藏三年的秘密后门

2021-04-30
PHP Composer漏洞可能导致广泛的供应链攻击
黑客利用SonicWall 0Day漏洞部署FiveHands勒索软件
First Horizon银行被黑客窃取客户资金
卡巴斯基发现了具有后门功能的中情局恶意软件

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

随着新型勒索病毒的不断涌现，企业数据泄漏事件不断上升，过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将越来越广，危害性也越来越大。2021年4月，全球新增活跃勒索病毒：QLocker、WhiteBlackGroup、Jormungand、Cring、Wintenzz、GEHENNALocker、RIP_lmao、Runsomware、Nocry、CryBaby等。其中QLocker是本月新增针对QNAS进行攻击的勒索病毒，短短五天获得260000美元。

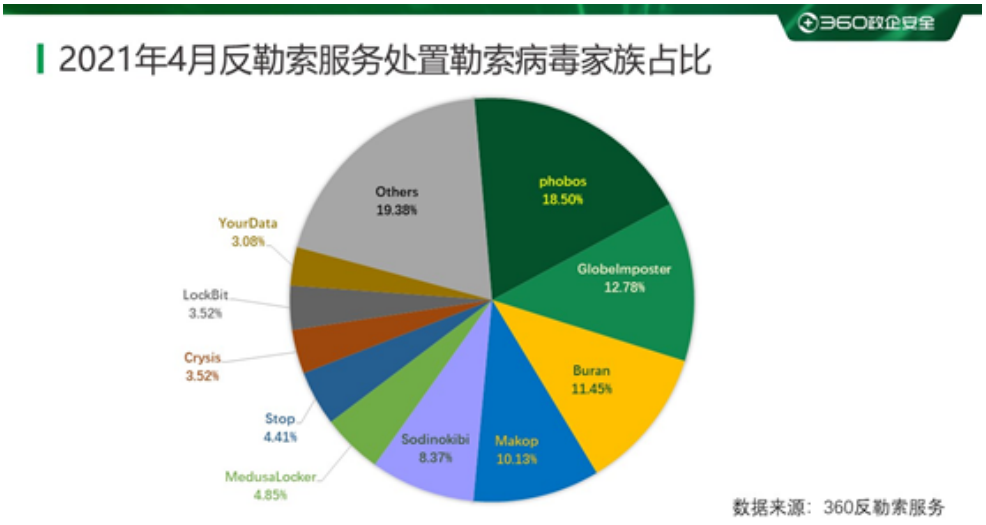
目录预览

勒索病毒态势分析

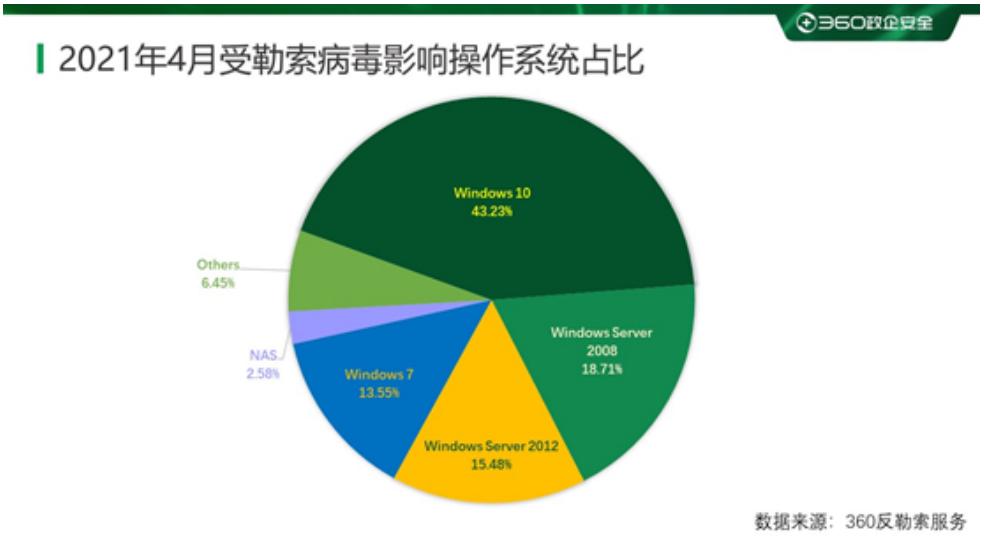
Ransomware Situation Analysis

一、感染数据分析

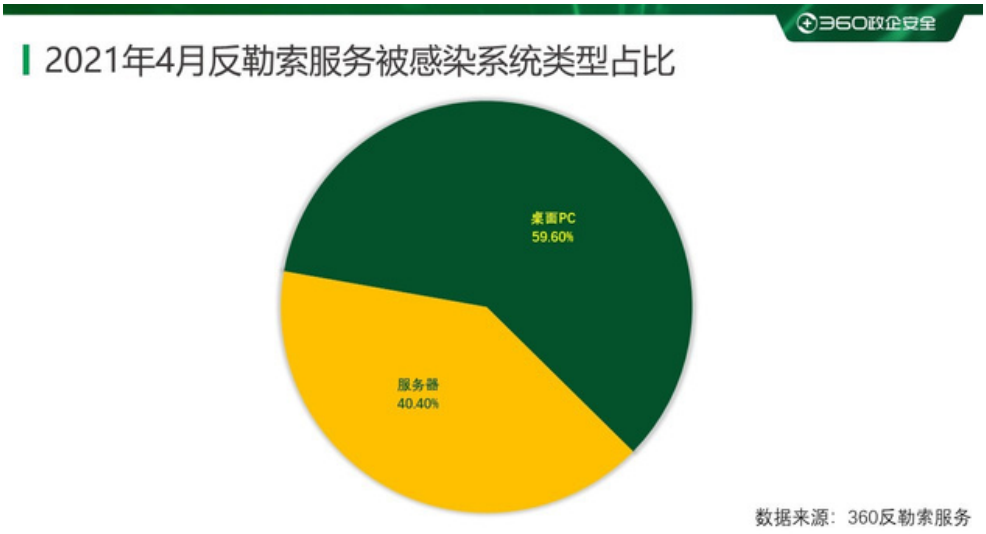
针对本月勒索病毒受害者所中勒索病毒家族进行统计，phobos家族占比18.50%居首位，其次是占比15.03%的GlobeImposter，Buran家族以11.45%位居第三。QLocker虽未进入本月勒索病毒家族TOP10,但该勒索病毒家族针对QNAS利用7zip加密网络存储设备中的文件带来了不小的影响。



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 Server 2008以及Windows Server 2012。



2021年4月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统仍主要是桌面系统，比重与上月相比变化不大。



二、勒索病毒疫情分析

YourData疑似针对国内用户进行攻击

360安全大脑监控到一款名为YourData的勒索病毒正瞄准国内企业以及个人，从目前的监控来看该家族仍主要使用暴力破解远程桌面口令的方法，然后手动投毒。而该病毒在本月又出现了一个新的变种，在加密文件后会将后缀修改为.kingdee。

该家族又被称作Hakbit、Thanos家族，最早出现于2019年11月。但在2021年1月中旬之前，该家族在国内实际发生的勒索案例并不多。此次在国内传播的变种主要特征为其联系邮箱为yourdata@RecoveryGroup.at，后缀更新过多次，但其接受谈判信息的邮箱一直未曾更改，且这几个变种只在国内出现过。怀疑该变种仅针对中国地区进行攻击。

What Happen to my computer?

Your important files are encrypted. Many of your documents, photos, passwords, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for way to recover your files , but do not waste your time. Nobody can recover your files without our decryption KEY (if somebody will tell that they can do it, they will also contact me and I will make the price so much expensive than if you contact directly).

DON USE GMAIL.COM TO CONTACT US

!!!THE DATARECOVERY COMPANIES JUST WANT YOUR MONEY!!!
!!DATA RECOVERY COMPANIES WILL ONLY INCREASE THE DECRYPTION TIME!!

Can i Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily But You have not so enough time . So If you want to decrypt all your data, you need to pay .As fast you pay as fast all of your data will be back as before encryption.

Send e-mail to this address: yourdata@RecoveryGroup.at

You have to pay for decryption in Bitcoins.

ATTENTION
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

If you want to try datarecovery company just ask for testfile.They have to give it for you if they can do something.

They will not.

Key Identifier:

华盛顿警方遭勒索病毒攻击，警方线人信息存在泄漏风险

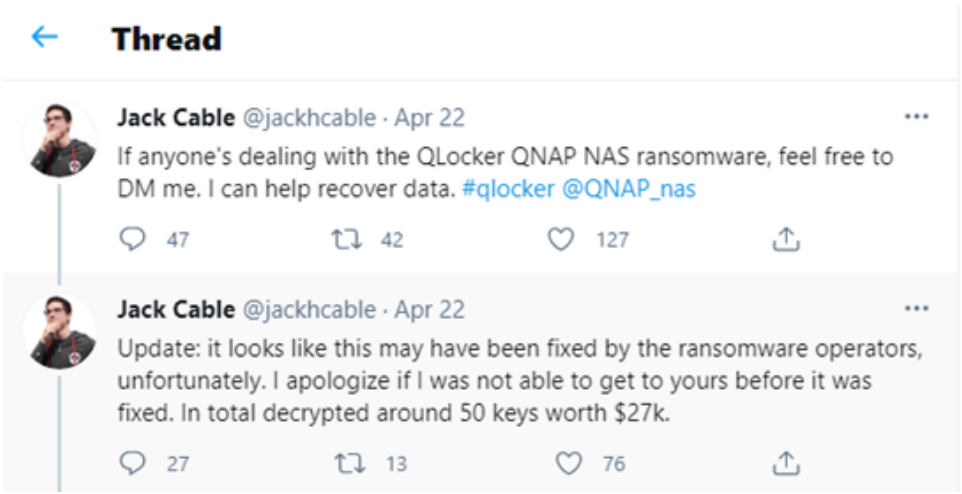
华盛顿警方遭遇Babuk勒索病毒攻击，被窃取250GB数据。从目前公开的截图看，被窃取数据包括调查报告、警官纪律文件以及其他行政文件。该勒索病毒家族要求华盛顿警方在3天内和他们取得联系，超过时间将公布警方线人信息。同时该团伙还称他们还将继续攻击美国的州机构，并自称比FBI的CSA（网络盾牌联盟）更早发现0day，他们后续还将采取更大规模的攻击。

QLocker大规模传播，短短五天时间盈利26万美元

近日QNAP（威联通）的网络存储设备再次成为勒索病毒攻击对象，受害者设备上的文件均被使用7zip加密。QLocker勒索病毒首次发现于4月19日，而最近该家族开始大量传播，每天约有数百个QNAP设备被其感染。短短五天时间， QLokcer家族收到的赎金便高达26万美元。其单个设备赎金为500美元左右，粗略计算已有525个受害者中招。

此次事件黑客利用了最新修复的CVE-2020-36195（多媒体控制台和媒体流加载项SQL注入漏洞）。使用QNAP设备的用户应立即更新多媒体控制台、媒体流加载项和混合备份同步应用程序到最新版本，避免遭遇该勒索病毒攻击。

该勒索早期解密程序存在的BUG曾被国外安全研究员发现，并协助过50名受害者成功恢复文件，但目前黑客已修补该BUG。



因广达电脑遭遇勒索病毒攻击，导致其合作商苹果被勒索

全球第二大笔记本电脑研发设计制造公司广达电脑遭遇Sodinokibi(REvil)勒索病毒攻击，被索要5000万美元作为赎金。攻击者还表示若支付日期超过4月27日，将需支付1亿美元赎金。

此次攻击事件中，大量客户数据被窃取，目前尚不明确到底有多少客户数据被窃取，但其客户包括了苹果、戴尔、惠普 、亚马逊、思科、富士通、联想、LG等大型公司，目前苹果的部分设计图纸已被该团伙公布到暗网中。

在和广达电脑谈判时，广达电脑表示他们不关心客户和员工数据，允许黑客公布和出售所有数据。目前Sodinokibi(REvil)正尝试与苹果谈判，想尝试通过威胁苹果——称若其不购回被窃取数据，便将在春季发布会之前将苹果最新产品设计数据在暗网公布。

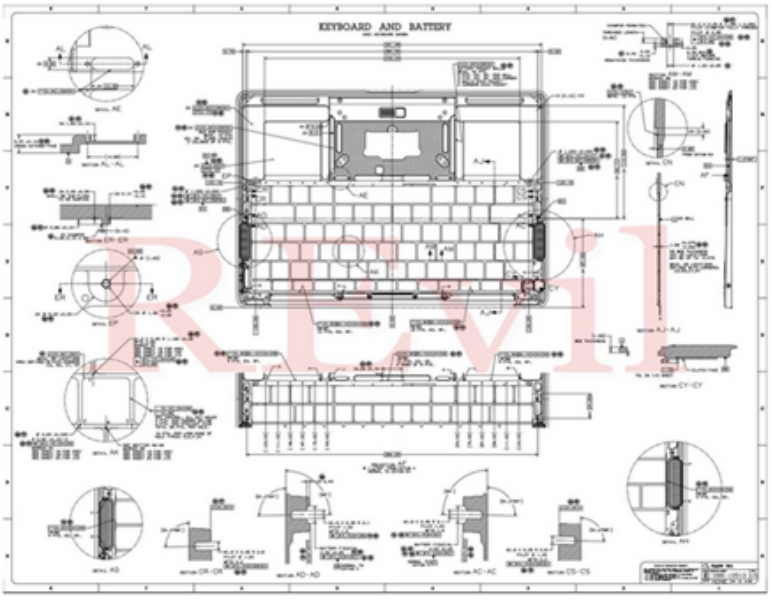
Products:
Apple Watch
Apple Macbook Air
Apple Macbook Pro
ThinkPad Z60m

In order not to wait for the upcoming Apple presentations, today we, the REvil group, will provide data on the upcoming releases of the company so beloved by many.Tim Cook can say thank you Quanta.From our side, a lot of time has been devoted to solving this problem. Quanta has made it clear to us that it does not care about the data of its customers and employees, thereby allowing the publication and sale of all data we have.

P.S.
Our team is negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands.
We recommend that Apple buy back the available data by May 1.

More and more files will be added every day.
The same is in pdf format

Proofs:

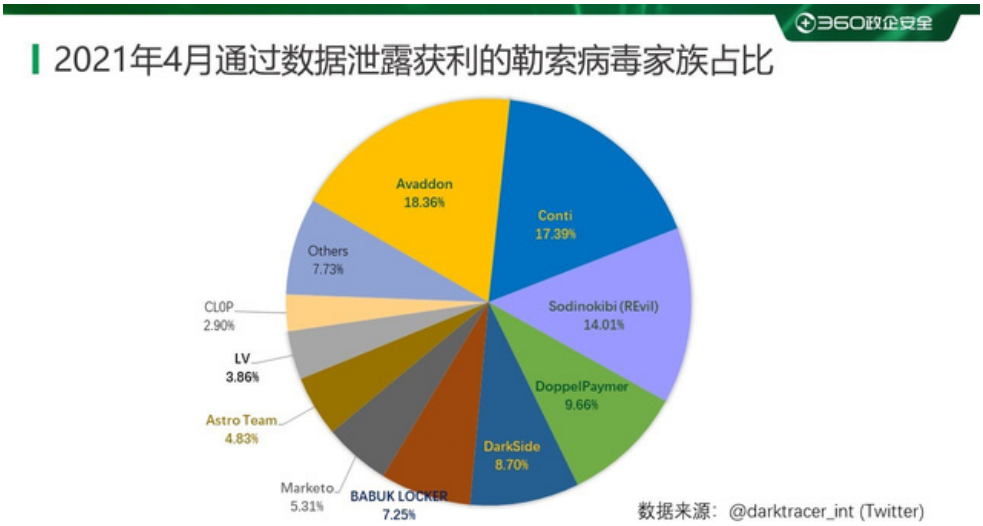


三、黑客信息披露

以下是本月搜集到的黑客邮箱信息：

oral@tuta.io	Ux3oe7ae@secmail.pro	magicbox@outlookpro.net
zphc@cock.li	Rekoh4th@secmail.pro	pyyring23@protonmail.com
vip05@cock.li	Uroo7ohM@secmail.pro	FilesRecoverEN@Gmail.com
ghjujy@tuta.io	mishacat@secmail.pro	soft.russian@secmail.pro
fastway@tuta.io	bichkova@secmail.pro	Rahidproject@secmail.pro
Vankosa@rape.lo	rahidproject@cock.li	rahidproject@secmail.pro
mikolio@xmpp.jp	rrrkkktttaaa@cock.li	decoding_service@aol.com
bad_dev@tuta.io	ppprrrkkkttt@tuta.io	kavariusing@tutanota.com
Mishacat@cock.li	2Hamlampampom@cock.l	DYAQrvHmy@protonmail.com
mishacat@cock.li	black_privat@tuta.io	decryptionservice@mail.ru
Bichkova@cock.li	jamesdecicio@aol.com	ransomware.attack@list.ru
sharm777@aol.com	decoder44@rambler.ru	BTCBREWERY@protonmail.com
goldmind@tuta.io	Wbgroup022@gmail.com	Helpforfiles@criptext.com
hpjar@keemail.me	oplatabtc3@gmail.com	Rusoftfond@protonmail.com
hanta@420blaze.it	ramilo2122@yandex.com	G.kulahmet@protonmail.com
miadowson@tuta.io	cryptservice@inbox.ru	padredelicato@secmail.pro
kobs@tutanota.com	tikitakbum@rambler.ru	m0absupport@protonmail.cn
xmmh@tutanota.com	2Hamlampampom@cock.li	servewintenzz@secmail.pro
Cybell@firemail.cc	akzhq725@tutanota.com	prometheusdec@hotmail.com
onioncrypt@aol.com	back_data@foxmail.com	decryptionservice@inbox.ru
decrypt@europe.com	yoursite@yoursite.com	Ivanmalahov@protonmail.com
wyooy@tutanota.com	prometheushelp@mail.ch	Galgalgalgalk@tutanota.com
2021@onionmail.org	herbivorous@keemail.me	olaggoune235@protonmail.ch
drakoshka@yahoo.com	sacura889@tutanota.com	alpinbovuar@protonmail.com
sparem@kolabnow.com	decryptservice@mail.ru	postal.surgut@danwin1210.me
vankosa@secmail.pro	catapultacrypt@tuta.io	Ooosferaplus@protonmail.com
Sportdieago@cock.li	eed8Aeta@danwin1210.me	Soft.russian@protonmail.com
sevenoneone@cock.li	dizelmon@danwin1210.me	personaliddecryptor@aol.com
bufalo@boximail.com	g.kulahmet@secmail.pro	thefancybears@protonmail.com
backdata@qbmail.biz	decrypt1nfo@airmail.cc	Whiteblackgroup002@gmail.com
deus69@criptext.com	decryptinfo@msgsafe.io	yourdataback1@protonmail.com
supportdata@cock.li	FileEnc@protonmail.com	niggapoopoo123@protonmail.com
Recovery.PC@aol.com	ouardia11@tutanota.com	FilesRecoverEN@Protonmail.com
Daijie@tutanota.com	decryptservice@inbox.ru	backupransomware@tutanota.com
sparem@kolabnow.com	decryptservice@mail.ru	postal.surgut@danwin1210.me
vankosa@secmail.pro	catapultacrypt@tuta.io	Ooosferaplus@protonmail.com
Sportdieago@cock.li	eed8Aeta@danwin1210.me	Soft.russian@protonmail.com
sevenoneone@cock.li	dizelmon@danwin1210.me	personaliddecryptor@aol.com
bufalo@boximail.com	g.kulahmet@secmail.pro	thefancybears@protonmail.com
backdata@qbmail.biz	decrypt1nfo@airmail.cc	Whiteblackgroup002@gmail.com
deus69@criptext.com	decryptinfo@msgsafe.io	yourdataback1@protonmail.com
supportdata@cock.li	FileEnc@protonmail.com	niggapoopoo123@protonmail.com
Recovery.PC@aol.com	ouardia11@tutanota.com	FilesRecoverEN@Protonmail.com
Daijie@tutanota.com	decryptservice@inbox.ru	backupransomware@tutanota.com
Cusapool@firemail.cc	godecrypt@onionmail.org	thorntitini1979@danwin1210.me
vgrieffers@gmail.com	sportdieago@secmail.pro	Andrey.taranov@protonmail.com
wbgroup022@gmail.com	anobtanium@tutanota.com	Jeremyspineberg11@tutanota.com
decryptdata@inbox.ru	recovery.helper@aol.com	6281fjds93hdfj5396dfgk@gmail.com
btcbrewery@india.com	lunasplank@tutanota.com	Jeremyspineberg11@protonmail.com
honestandhope@qq.com	prometheusdec@yahoo.com	payfor_hackedsecret@protomail.com
Xieth8ie@secmail.pro	prometheusdec@gmail.com	GeromeSkinggagard1999@tutanota.com
Iyieg9eB@secmail.pro		

当前，通过双重勒索模式获利的勒索病毒家族越来越多，勒索病毒所带来的数据泄漏的风险也越来越大。以下是本月通过数据泄漏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。若企业或个人发现有数据泄漏风险，请第一时间自查，做好数据已被泄露的准备，采取补救措施。

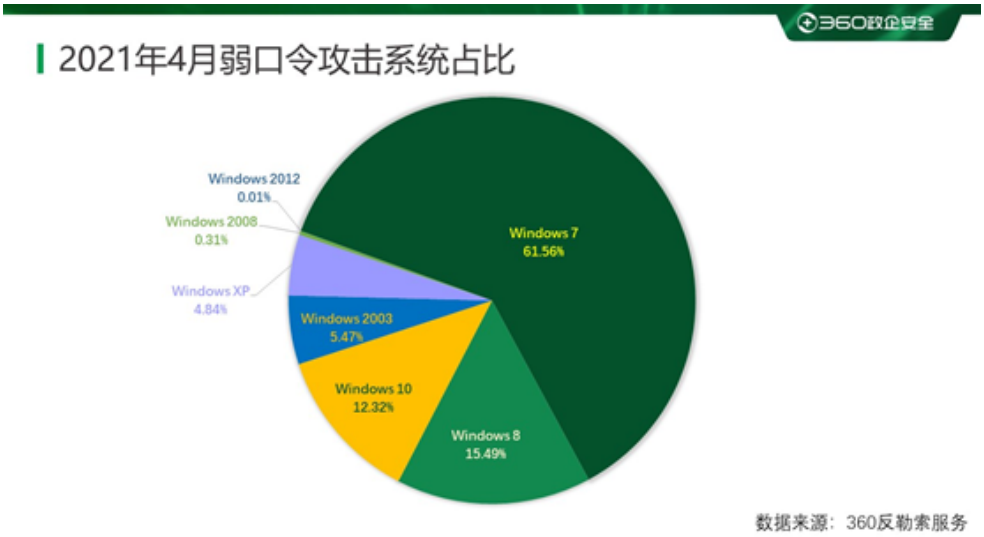
CNE	PSU Technology	Cosmetica Laboratories
Aldes	FOODLAND.COM	Matratzen Concord GmbH
IPSEN	PLDevelopments	BEE LINE LOGISTICS, INC
ALIZON	PB Swiss Tools	Quality Packaging, Inc.
Vincle	Ford Meter Box	National Public Seating
NewsRx	DT Engineering	MITCHAM INDUSTRIES INC
ISOLVED	PROSOLARTEC.de	Município de Constância
bdhouse	Kens Foods Inc.	BTU International, Inc.
FNBNWFL	Gijima Holdings	Animal Behavior College
DirickX	Comfort Keepers	Premi Beauty Industries
OLOMOUC	TRAVELSTORE.COM	Marietton Développement
AlohaABA	moba-automation	StoneGate Senior Living
MSPharma	Hames Homes LLC	Plimpton and Hills Corp
Capmatic	Houston Rockets	Readie Construction Ltd
Apperton	apmmguntown.com	Hensley Beverage Company
Bertucci	Call Assist Ltd	Bauder Roofing Solutions
SpecPage	Absolute Dental	OAK VALLEY COMMUNITY BANK
jpscu.com	Tata Steel GROUP	DeVincenzi Metal Products
Gamma Spa	Vivida Assistans	JST Global, Acme-Hardesty
DURHAM.CA	HOYA Corporation	CERINNOV, UNIPESSOAL, LDA

EMO Trans	Zambon Group SpA	Cambridge Weight Plan Ltd
Gorzynski	Lozano Smith LLP	Heartland Automotive, LLC
CAVENDERS	The Village Vets	Città di Caselle Torinese
Saddlemen	SOUTHERN ASPHALT	Illinois Attorney General
Flaghouse	Braman Motorcars	Department of Agriculture
Filtertek	Zambon Group SpA	OpTech Staffing Solutions
HW Fisher	Cuddy & Feder LLP	Newcomb Secondary College
HumanWare	B.W. Wilson Paper	Mairie de Marolles-en-Brie
Nobiskrug	Pavages Maska Inc	Mevion Medical Systems Inc
vgcargo.de	Harris Federation	MUNICIPIO DE QUATRO BARRAS
paslin.com	Federal land inc.	Hardy Buoys Smoked Fish Inc
Seven Seas	BOUTINEXPRESS.COM	American Signal Corporation
SIUMED.EDU	kirwanspellacy.com	Protectim Security Services
boulos.com	Nachi America Inc.	Kaleidoscope Charter School
PNGC Power	Tristate Midstream	Edifice General Contractors
aspire inc	Briggs Corporation	Iron Orbit Inc. and Clients
mipharm.it	NEO DERM GROUP LTD	Active Business & Technology
dwmrlaw.com	Pierre Fabre Group	Honeywell International Inc.
Infolog Spa	RHA Health Service	Centro Hospitalar de Setúbal
ginospa.com	Phone House España	Colorado River Indian Tribes
PVR Cinemas	MURPHYBATTISTA.COM	Precision Terminal Logistics
Lime Energy	Union High School	COMUNE DI VILLAFRANCA D'ASTI
Matco-Norca	Harold Marcus Ltd.	Broward County Public Schools
Habia Cable	Varner & Brandt LLP	VAUGHN CONCRETE PRODUCTS , INC
ReklamStore	Rosco Manufactoring	NorthWest , Insuranse Services
Komatsu Ltd	Greatwide Truckload	Presque Isle Police Department
Kajima corp	C. Watkins Plumbing	ADUANAS Y SERVICIOS FORNESA SL
Dade City FL	DIGroupArchitecture	McCurley Integrity Dealerships
Curbell Inc.	Brown Strauss Steel	Campbell Sales and Service, Inc
Khalili Center	Complete Automation	Innovative Office Solutions LLC
Grupo Prilux	All Star Automotive	Bertucci's Oven Pizza and Pasta
Cathar Games	Elite Software , Inc	Valley Transportation Authority
Oré Peinture	Abu Issa Holding LLC	UPL (United Phosphorus Limited)
Fonds Finanz	spiritlakecasino.com	Siemens Gamesa Renewable Energy
Mankato Ford	Klenda Austerman LLC	Loma Systems - A Division of ITW
Pocket Money	Fultz Maddox Dickens	Diversified Plastics Corporation
omnidecor.net	Universal Group Inc.	Newbridge Securities Corporation
Southwest KIA	Partit Nazzjonalista	[NASDAQ: DXYN] thedixiegroup.com

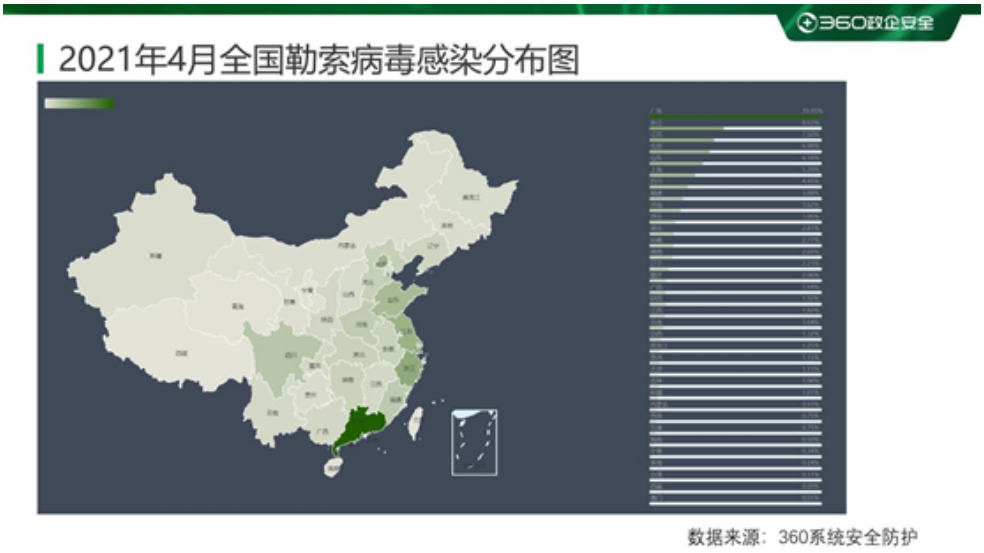
Comune di Rho	Quanta Computer INC.	HealthCare Global Enterprises Ltd
Comune di Rho	CREST Hotel & Suites	Metropolitan Police Department DC
Carpenter Co.	Citizens Of Humanity	C.E.E. Schisler Packaging Solutions
Pezutto Group	www.schnepsmedia.com	Intensive Care On-Line Network , Inc.
Cairn Capital	Eduro Healthcare, LLC	Maestri Murrell Commercial Real Estate
Interfel Corp	Thomas Concrete Group	Indonesia Infrastructure Guarantee Fund
govnet of fiji	Options Greathire Ltd	Rogers Engineering & Manufacturing Co., Inc.
Condor Ferries	Titanium Industries Inc	EMC, Electric Motor and Contracting Co., Inc
CJ Selecta S/A	von Drehle Corporation	CONSORZIO INNOVAZIONE ENERGETICA RINNOVABILE
supabets.co.za	ASBIS CZ, spol. s r.o.	Maharashtra Industrial Development Corporation
Baker & Taylor	Ajuntament de Castelló	UNIONE DEI COLLI DIVINI NEL CUORE DEL MONFERRATO

四、系统安全防护数据分析

通过将2021年3月与4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。

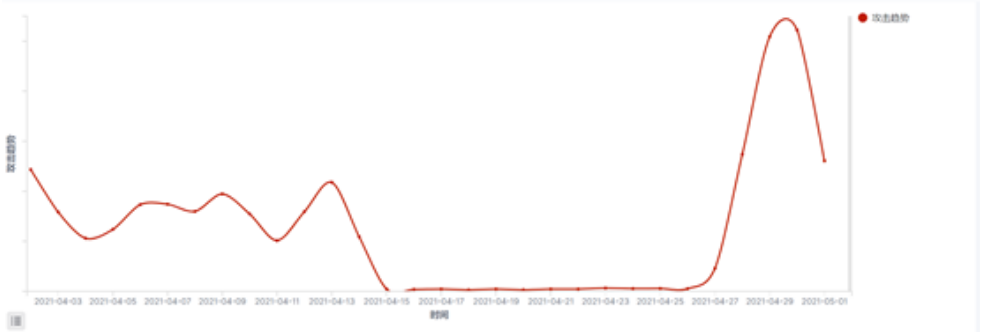


以下是对2021年4月被攻击系统所属地域采样制作的分布图，与之前几个月采集到的数据进行对比，地区排名和占比变化均不大。数字经济发达地区仍是攻击的主要对象。



通过观察2021年4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在本月大幅度下降。这可能和紫狐病毒存在一定关联。紫狐是一款通过MSSQL弱口令爆破攻击进行传播的病毒，该家族的拟在通过感染更多机器来推广用户安装不需要的软件，从而盈利。 在本月中旬该家族利用MSSQL传播的量大幅度下降。

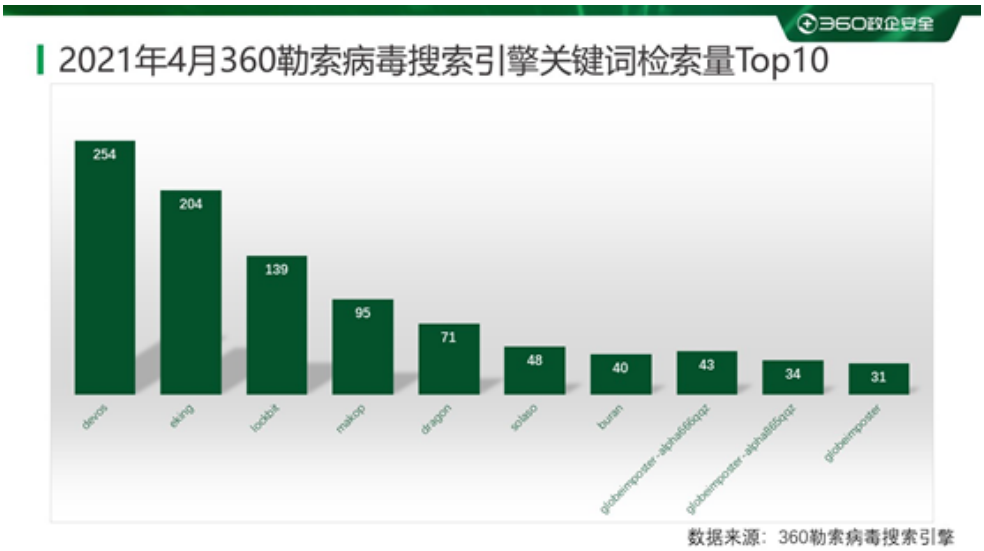
以下是本月监控的紫狐病毒的活动趋势图，和MSSQL的攻击趋势大体符合。



五、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。本月活跃的是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。
- Lockbit: 属于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。
- Dragon:属于Dragon勒索病毒家族，由于被加密文件后缀会被修改为dragon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。
- solaso: 属于Cryptojoker勒索病毒家族，由于被加密文件后缀会被修改为solaso而成为关键词，该家族的传播方式为: 通过“匿隐” 僵尸网络进行传播。
- Buran: 属于Buran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。
- globeimposter-alpha666qqz：属于GlobeImposter勒索病毒家族，由于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。
- globeimposter-alpha865qqz: 同 globeimposter-alpha666qqz。
- globeimposter: 同globeimposter-alpha666qqz。



数据来源：360勒索病毒搜索引擎

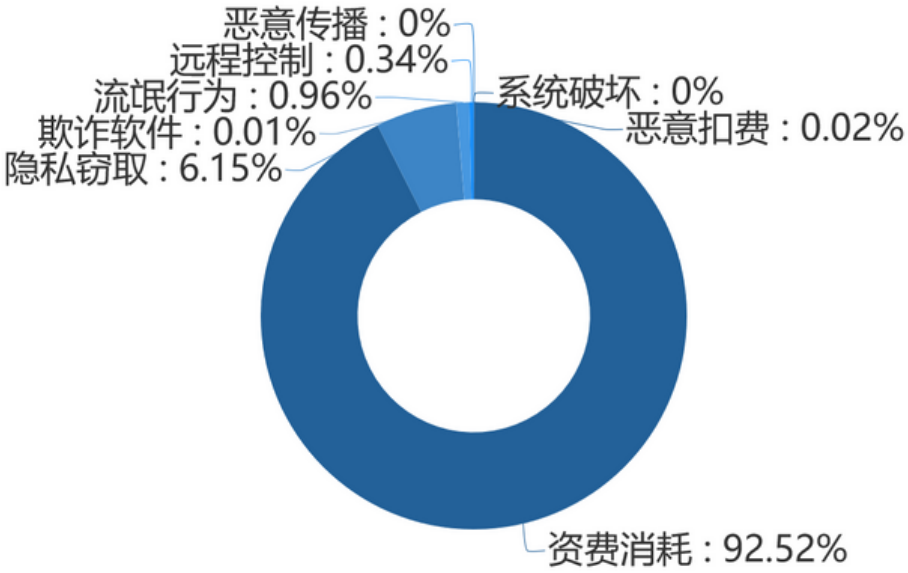
六、解密大师

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

数据来源：反勒索服务统计数据

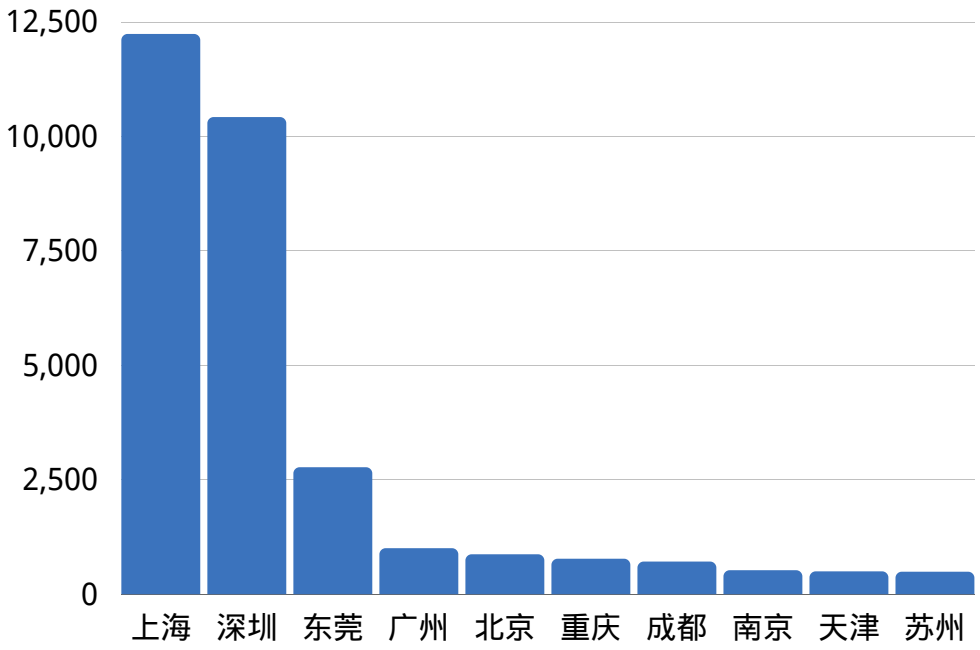
移动安全数据分析

Mobile Security Data Analysis

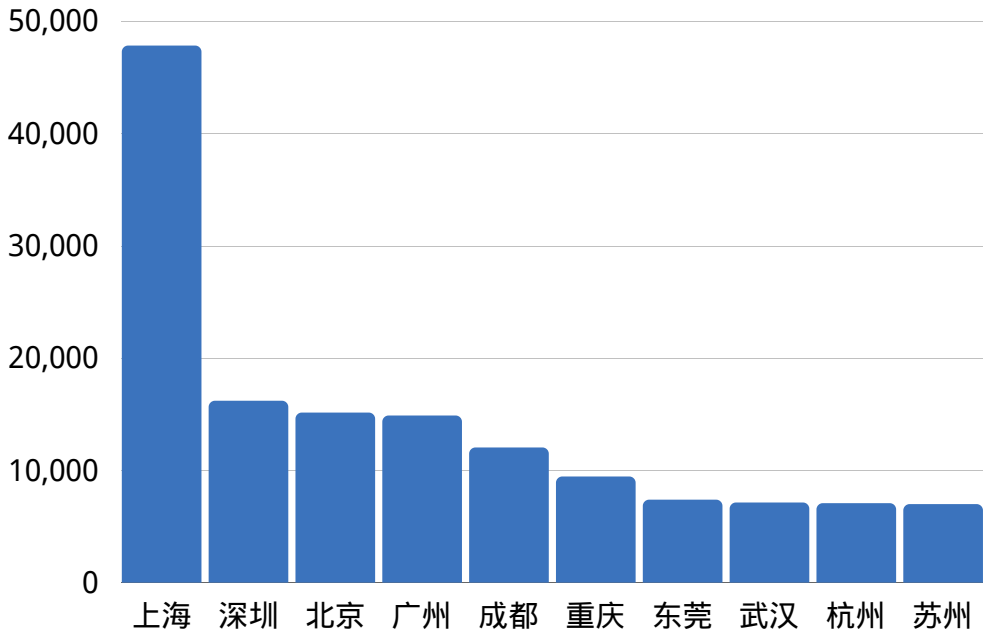


数据总览

拦截量整体情况



流氓行为拦截量前10城市



隐私窃取拦截量前10城市

样本分析检测

White List Analysis

一、4月份签名冒用

签名冒用是指黑客冒用知名公司的身份资料，在境外签名机构申请知名公司的数字签名用于签发恶意程序，此类攻击通常因为签名信任机制而导致安全软件对木马放行。360白名单分析组对此类攻击进行长期监控，已累计发现数百个此类冒用的证书，以下为4月份监控到的新增冒用证书，均为“Sectigo RSA Code Signing CA”机构签发，包含3家知名公司的数字签名，均用于仿冒聊天软件传播木马。

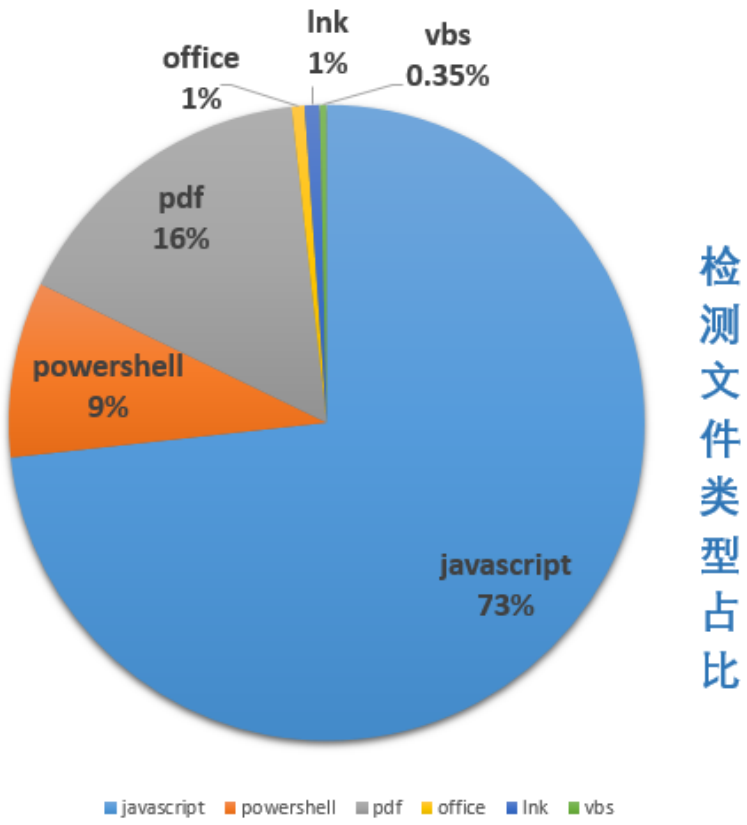
数字签名	证书sha1	颁发机构	发现日期	描述
Ascora GmbH	76F132E7E8D486206035A78F17E80266D3D2BF1E	Sectigo RSA Code Signing CA	2021/4/19	仿冒potato聊天软件嵌入木马相关团伙
Ventis Media, Inc.	1C058F9DE2ADA9EE6B0680AF4B65DFCD87E9FAC2	Sectigo RSA Code Signing CA	2021/4/14	仿冒potato聊天软件嵌入木马相关团伙
Acoustica, Inc	A05AF5D7D629B7559A590EED67B84E7373576C3A	Sectigo RSA Code Signing CA	2021/4/7	仿冒potato聊天软件嵌入木马相关团伙

二、4月份非PE样本VT检出TOP比例

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

检出名	文件类型	占比	检出说明
ex_virus.js.fakejquery.*	javascript	17.73%	仿冒jquery恶意链接
ex_virus.pdf.phisher.*	pdf	16.05%	pdf钓鱼
ex_virus.js.brocoiner.a	javascript	11.77%	CoinHive挖矿
ex_virus.js.miner.a	javascript	10.11%	js挖矿
ex_virus.powershell.bypassamsi.a	powershell	8.93%	bypass amsi防护
ex_virus.js.kryptik.*	javascript	5.73%	kryptik家族
ex_virus.js.evalobfs.a	javascript	4.70%	js执行混淆重定向代码
ex_virus.js.gnaeus.a	javascript	4.48%	gnaeus家族浏览器劫持
ex_virus.js.hidelink.a	javascript	3.93%	恶意隐藏链接
trojan.js.likejack.a	javascript	3.72%	刷赞木马
js.iframe.packed.b	javascript	2.82%	恶意框架插入
ex_virus.js.agent.*	javascript	2.65%	js恶意跳转代理
ex_virus.js.faceliker.a	javascript	1.47%	facebook刷赞木马

ex_virus.js.mousefollower.b	javascript	1.45%	facebook刷赞木马
ex_virus.js.redirector.a	javascript	1.19%	js重定向代码
macro.office.excel.gen.5001	office	0.66%	office宏病毒
js.bitcoinminer.1.2	javascript	0.57%	js挖矿
ex_virus.js.decode.a	javascript	0.54%	js恶意混淆木马
virus.lnk.vbsworm.b	lnk	0.39%	lnk蠕虫链接
ex_virus.js.iframeDownloader.a	javascript	0.39%	js框架下载者
ex_virus.lnk.joke.a	lnk	0.37%	lnk恶作剧
ex_worm.vbs.agent.b	vbs	0.35%	vbs蠕虫病毒



检测文件类型占比

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

2021.04

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