360-CERT
COMPUTER EMERGENCY READINESS TEAM

安全事件分析报告

2020下半年

https://cert.360.cn

负责人

蔡玉光

王宇恒

李依林

主编

王泽辰

编辑

黄小鹏

赵萱

设计

罗智华

杜艳如

赵萱

扫码关注

前言

本次报告主要对 2020 年下半年的所有**《安全事件周报》**所写的国际安全事件数据进行一个简单的回顾，同时从大家感兴趣的方向出发，做一个简单的阐述。

事件行业的划分参考，以中华人民共和国国家质量监督检验检疫总局和中国国家标准化管理委员会联合发布的《国民经济行业分类》为基础。

团队介绍

360-CERT 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 DIRECTORY

新冠疫情下的网络安全

CYBER SECURITY IN THE CONTEXT OF COVID-19

前言

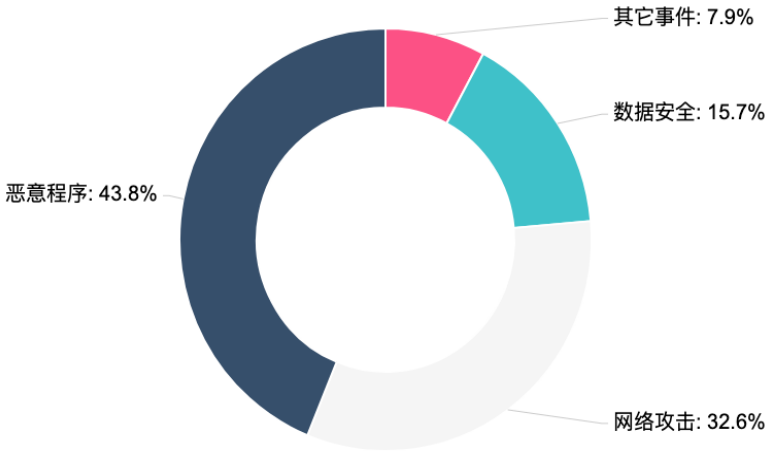
2020 年是特殊的一年，新冠疫情下，各行各业都发生了巨大的变动，安全行业也不列外。疫情发展和推动了一些新的安全趋势，从攻击战法、社工方案到防护重点、安全策略，都有所改变。而这些攻防趋势的持续时间可能比疫情的持续时间更长。

1. 社工利用
2. 远程办公面临的威胁
3. 卫生行业
4. 个人追踪程序

社工利用
Social Engineering

疫情下社工大肆利用新冠主题分发恶意软件，应谨慎打开疫情相关邮件和链接，只相信官方渠道的消息。

疫情爆发后，恶意软件在社工阶段，使用新冠相关主题大肆传播，**新冠疫苗、疫情进展、疫情最新治疗缓解措施**等等都是常用的诈骗主题。为了增强传播影响力，黑客甚至对自己的恶意软件服务（Raas）开展了折扣活动。早在今年1月，安全厂商就报告了Emotet使用带有冠状病毒相关内容的诈骗邮件，对日本用户进行诈骗活动，在当时就有数千个与冠状病毒相关的注册域名被用于各种诈骗活动。



新冠事件类型占比

相关安全事件

巴西网络钓鱼攻击通过新冠肺炎假新闻扩散

根据卡巴斯基的网络钓鱼研究报告显示，巴西成为受网络钓鱼攻击影响最严重的国家之一。钓鱼攻击者通过传播政府应对 COVID-19 的假新闻快速扩散了钓鱼攻击的影响面。卡巴斯基在报告中指出，在 2020 年 4 月至 6 月期间，巴西约八分之一 (12.9%) 的互联网用户都访问过一个恶意链接，该链接导致用户浏览的正常网站出现恶意内容。报告中还提到一个通过钓鱼邮件进行诈骗的案例，钓鱼邮件中叙述了巴西政府在新冠疫情期间已经暂停了能源账单支付的虚假信息，诱导用户点击钓鱼链接完成诈骗。

AgentTesla 木马通过 COVID-19 援助活动传播

Area 1 Security 的研究人员表示，恶意攻击者在疫情期间策划了一场提供口罩及其他个人防护设备的援助活动，通过该活动散布 AgentTesla 木马。该援助活动始于 2020 年 5 月，它利用人们在疫情期间对口罩和温度计短缺的担忧，使用钓鱼邮件对化学品制造商及进出口企业实行诈骗。据悉，恶意攻击者每 10 天就会改变其钓鱼策略和程序，并对钓鱼邮件和恶意域名进行调整，以防被发现。

远程办公面临的威胁
Threats to telecommuting

随着疫情的发展，许多企业开始远程工作，从而使大量的工作流程面临攻击威胁。

疫情下，许多企业开始远程办公。因此，**企业 VPN、视频会话软件、内部通信平台**都成为了恶意攻击者所关注的重要目标。攻击者通过注册假域名冒充 Zoom，Microsoft Teams 等远程办公软件的官网传播恶意软件。随着 RDP 和 VPN 等远程访问技术使用频率的增加，RDP 爆破攻击的数量也急剧上升。

Fortinet VPN 漏洞使 20 万个企业面临安全风险

根据网络安全平台提供商 SAM Seamless network 的数据显示，超过 20 万家企业使用了 Fortinet VPN 用于解决远程办公需求。该 VPN 存在漏洞，恶意攻击者可以通过提供有效的 SSL 证书对 VPN 连接者实现中间人 (MitM) 攻击。

SonicWall VPN 高危漏洞可造成远程代码执行

2020 年 10 月 16 日，SonicWall 官方发布安全通告，SonicOS 中存在缓冲区溢出漏洞，远程攻击者可以在未授权的情况下构造特定的 HTTP 请求触发该漏洞，造成拒绝服务（DoS）攻击。该漏洞还可以通过堆栈破坏更改程序执行流，所以还可能造成远程代码执行。该漏洞存在于产品管理服务及 SSL VPN 远程准入服务中。

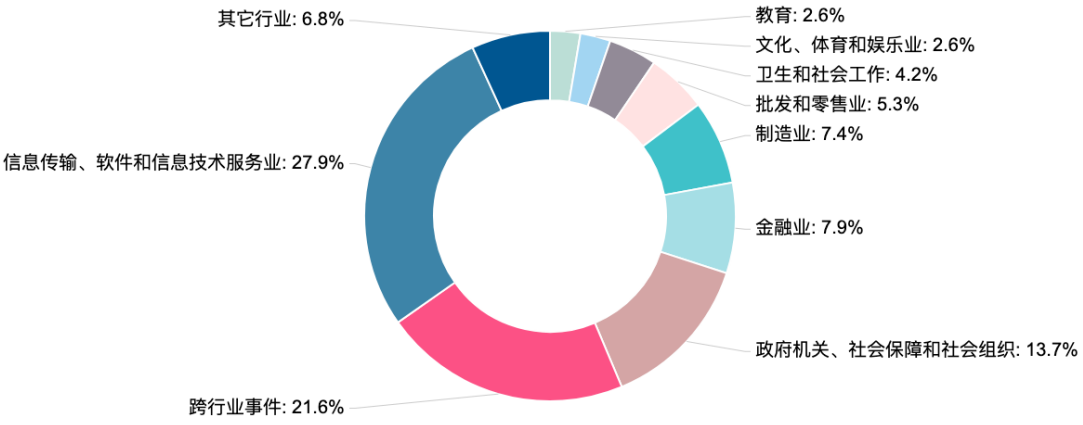
27.9%

IT 相关占比

360-CERT 对《安全事件周报》中网络攻击事件的数据进行了整理，形成了一张**网络攻击事件行业分布图**，可以看到，**信息传输、软件和信息技术服务业**占比颇高，这是由于远程办公的激增，攻击者瞄准了 IT 相关的各个部分。同时，由于各种扫描器进行地毯式无差别扫描，跨行业网络攻击事件也占到了 21.6% 的比重。

21.6%

跨行业网络攻击事件占比

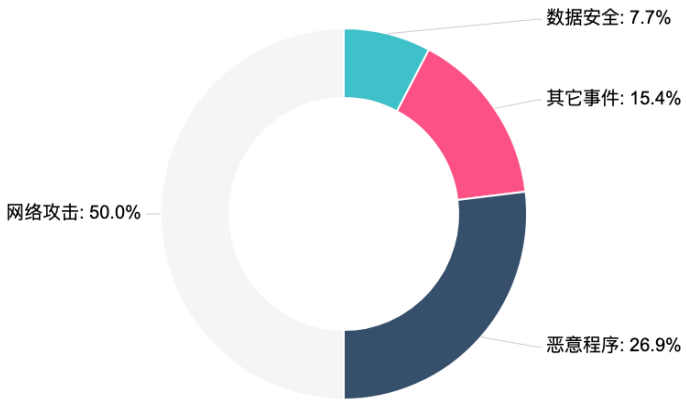


网络攻击事件行业占比

50%

政府机关攻击事件中网络攻击占比

同时，我们可以看到，比起其它传统行业，**政府机关**是网络攻击的重中之重。包括 APT 组织的各种恶意攻击团体，都将国家政务机关作为了他们的首要目标。



政府机关事件类型占比

在对政府机关的安全事件类型进行数据整理后，发现网络攻击占比 50%，所以各大政府机构一定要对自身的网络防护施以足够的重视。

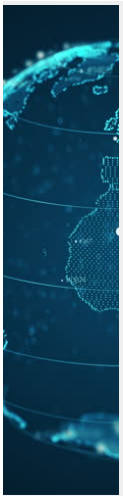
相关安全事件

数千个加拿大政府帐户遭到黑客攻击

加拿大财政部发布公告，数千个在线政府服务账户遭到恶意攻击者攻击。恶意攻击者通过凭据填充攻击 GCKey 服务，该服务被大约 30 个联邦部门使用。攻击者盗取了 9041 名 GCKey 账户的登录凭证，并使用这些账户尝试访问政府服务。

乌克兰国家警察网站因黑客入侵而关闭

2020 年 9 月 23 日，乌克兰国家警察局确认其官网被黑客入侵而暂时关闭。这并非是乌克兰国家机关网站第一次因遭受网络攻击而关闭。几年前，乌克兰能源部网站遭到比特币勒索软件攻击，其邮政服务、能源部门、核电站及机场都遭受过恶意软件攻击。



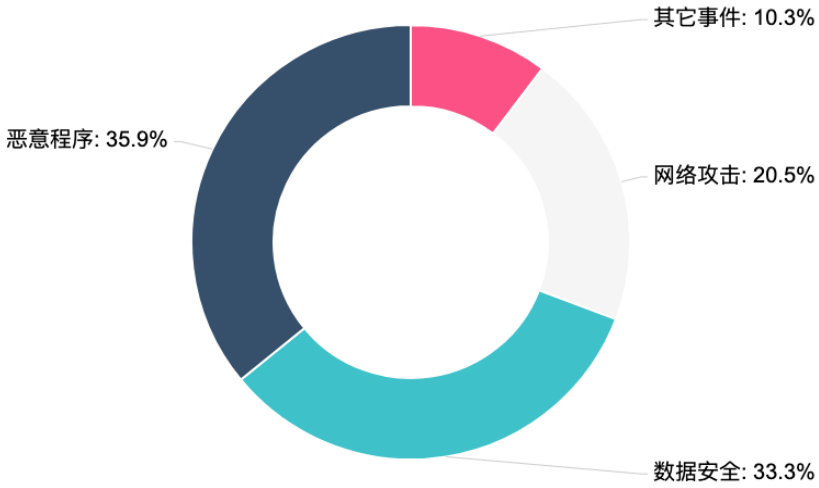
安全建议

1. 内部计算机、网络服务、个人账号等认证服务都使用复杂密码
2. 登陆入口采用双重验证方案
3. 及时对系统及各个服务组件进行版本升级和补丁更新
4. 浏览器、邮件客户端、vpn、远程桌面等个人应用程序，应及时更新到最新版本

卫生行业
Health care industry

在疫情期间，卫生行业应该比其它传统行业更注重自己的数据保护和勒索防范。

在 360-CERT 采集到的**新冠相关事件**中，大量的事件来源于**卫生和社会工作行业**。在疫情期间，卫生部门、卫生国际组织、疫苗研究机构、病毒分析机构、医院等都是网络攻击的重点目标。



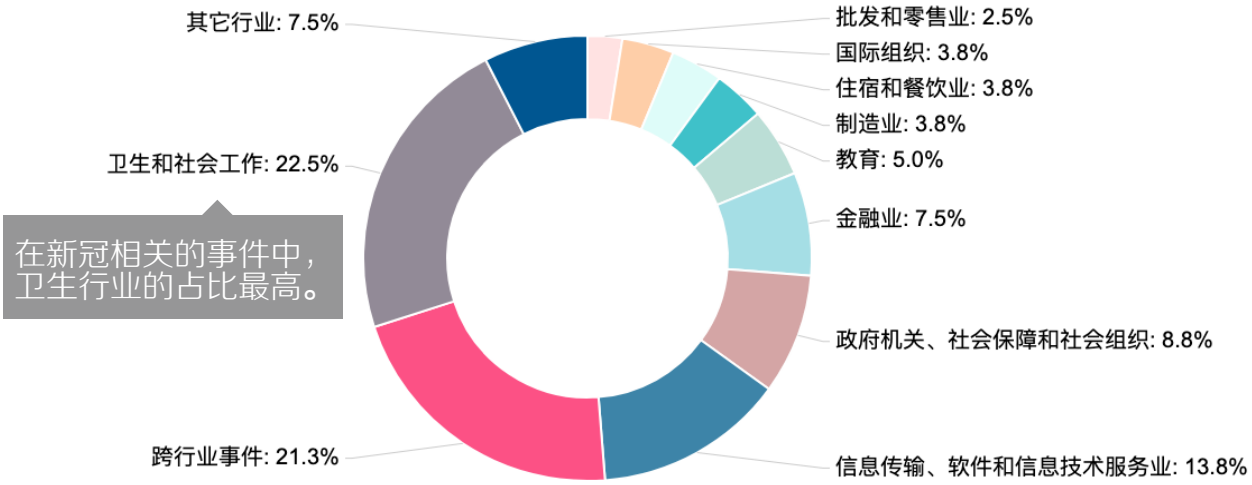
卫生业事件类型占比

在卫生行业相关事件中，**恶意程序和数据泄露**的事件类型占比颇高。医院、病毒疫苗组织、卫生机构的内部数据（尤其是新冠相关数据）在攻击者眼中具有很高的价值。因此，虽然有不少勒索软件都声称不以医院为目标，但仍有许多卫生相关的机构和组织受到各大勒索团伙的攻击。

69.2%

恶意程序和数据泄露占比

卫生部门承受着巨大的压力，在治疗大量患者的同时，还要努力研究疫苗及其它抑制这种病毒的药物。在新冠相关的事件中，卫生行业的占比最高，像 Maze 这样的勒索软件运营商在 2020 年持续攻击着卫生行业。



新冠事件行业占比

相关安全事件

REvil 勒索软件运营商攻击医疗保健组织

根据《 Cisco / Cybersecurity Ventures 网络安全年鉴》，医疗机构遭受的网络攻击比其他行业的次数更多。医疗机构管理的敏感数据是黑客的重点目标。由于新冠疫情的肆虐，这些机构面临更大的压力，也更容易遭受网络攻击的威胁。Cyble 研究团队发现 REvil 勒索软件运营商发布消息，声称已经入侵了一家医疗机构——山谷医疗系统 (Valley Health Systems)，导致医患敏感信息泄露（包括患者的处方及详细信息，患者的医学扫描报告，数字成像和通讯医疗文件等）。

勒索软件攻击扰乱了 COVID-19 医学试验

总部位于费城的医疗科技公司 eResearchTechnology（ERT）是医疗机构的软件供应商，该机构遭遇勒索软件攻击，所幸没有患者受到影响。由于受到勒索攻击，ERT 研究人员无法以电子方式访问数据。他们不得不通过传统的笔和纸方法来追踪患者。

安全建议

1. 定期备份数据，隔离存放数据备份
2. 独立主机存放敏感数据
3. 设置数据访问白名单
4. 各主机安装 EDR 产品
5. 及时更新系统、安装补丁升级

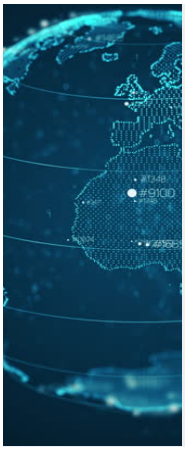
个人追踪程序
Personal tracking program

疫情的爆发推动了个人追踪系统的发展，也产生了相关的安全问题。

疫情的爆发促使许多国家颁布了紧急法规，启动了个人追踪系统以抗击疫情，例如我国的健康码。而在印度，**Aarogya Setu** 联系人跟踪应用程序下载量已超过1亿，这引发了新的隐私和安全问题。安全标准实施不力可能会使用户的数据面临风险。

印度新冠监视工具暴露了数以百万计的用户数据

一份来自 VPNnentor 的研究报告显示，Uttar Pradesh 地方政府的 COVID-19 监视工具在 8 月 1 日遭到攻击，导致大量数据泄露。该工具是一个大型测绘项目的一部分，其主要目的是追踪印度各地的冠状病毒患者。由于缺乏数据安全协议，不慎使平台的访问权限对外完全开放，导致印度数百万人的个人数据暴露。



安全建议

1. 做好个人追踪程序的内部安全测试
2. 尽量减少外网不相干的业务和接口
3. 由于个人追踪程序会和政务内网连接，因此要做好数据传输的安全策略

供应链攻击
SUPPLY CHAIN ATTCK

前言

供应链攻击历史悠久，是一种面向软件开发人员和供应商的高级威胁。一旦上游供应链遭受攻击，其所有下游用户都会遭到威胁。供应链攻击难以检测、隐蔽性强、攻击面广。基于这些特点，供应链攻击将会在未来的攻防对抗中愈演愈烈。

1. 影响深远性
2. 入侵路径多样性
3. 攻击持久性

在网络安全解决方案日益完善的今天，专业的APT组织能利用供应链攻击造成更为深远的影响。

影响深远性
Affect profoundly

身处数字化时代，软件已经成为日常生活不可或缺的必需品，依赖成熟的软件供应链，用户可以快速地获取并使用自己想要的软件。在提供便利的同时，软件供应链也为用户带来了巨大的安全风险，这种风险称为**供应链攻击**。

供应链攻击本质上是软件供应链各环节中由于“相对信任”所产生的“信任误差”导致的。攻击者可以从软件供应链任一环节侵入，伪装成受信任的程序来分发恶意代码。对于安全防护水平较高的系统，供应链攻击是一种非常有效的攻击方式。

供应链攻击的严重程度主要取决于软件的使用行业、使用量。对于国家机构而言，供应链攻击的风险尤为严重，无论是关键设施还是政府机构都大量采购并使用外部的软硬件设备，一旦攻击者从供应链上游进行攻击，便可以绕过严密的安全防护，直接攻陷国家关键系统，威胁国家安全。

在网络安全解决方案日益完善的今天，供应链攻击成为专业 APT 组织惯用的手法，最具代表性的案例为 2020 年 FireEye 和微软披露的 **SolarWinds** 供应链攻击。

SolarWinds 是著名的 IT 管理软件和远程监控工具，具有广泛的用户群体，客户覆盖了超过 9 成的世界 500 强企业及大量重要的政府机构，包括美国十大电信公司、美国军方的五大军种（海陆空军、美国海军陆战队、太空军）、美国国务院、美国国家安全局及总统办公室等。

美国时间 2020 年 12 月 13 日，美国网络安全公司 FireEye 和微软公司相继发布技术分析报告，披露了国家级 APT 组织针对 **SolarWinds** 产品的供应链攻击，并对相关软件植入的后门进行了技术分析。同时 **SolarWinds** 官方发布安全公告，确认了该公司的 **SolarWinds Orion** 平台软件收到供应链攻击，并提醒用户检查升级到最新版本。此次供应链攻击使美国的核心企业、军事机构和政府机构遭受了史上最严重的 APT 攻击，众多重要机构被国家级 APT 组织入侵。

历史安全事件

XshellGhost 事件

软件厂商 NetSarang 是全球领先的跨平台集成解决方案的供应商，其产品覆盖了世界 90 多个国家，拥有极其庞大的用户量。2017 年 8 月 7 日 NetSarang 与卡巴斯基发布联合声明，确认于 2017 年 7 月 18 日发布的 Xmanager Enterprise、Xmanager、Xshell、Xftp、Xlpd 五款软件更新中被植入了恶意代码，用户机器一旦启动软件，黑客便可以直接控制用户机器执行任意命令。该系列软件被程序员及运维开发人员广泛用于管理企事业单位的重要服务器资产，所以恶意攻击者能够以此窃取用户所管理的服务器身份验证信息，秘密入侵相关的服务器，造成不可挽回的后果。

入侵路径多样性
Diversity of attack paths

供应链攻击的入侵路径涵盖了软硬件生产、交付、使用的方方面面。

2020 年 12 月公开的 SolarWinds 供应链事件中，攻击组织通过入侵 SolarWinds 的软件开发、打包、签名服务器，将恶意的代码植入 **SolarWinds Orion Core Service** 组件中。该核心服务组件被打包进 **SolarWinds** 离线安装程序，同时被上传至官方更新服务器，通过在线服务分发给所有的客户端进行升级。因此，拥有完整官方数字签名的后门组件，通过 **SolarWinds** 官网传播到每个用户的服务器上。

此次攻击意味着攻击者完整地接管了 **SolarWinds** 生产交付系统，并利用交付系统的便利性，对所有的 **SolarWinds** 用户无差别投递后门应用程序。再通过后门应用程序，进行后续的攻击目标筛选和命令控制。供应链入侵路径多种多样，就算是如此精心设计的入侵流程，也仅涵盖寥寥几种。

在最近 10 年内，除开这次 **SolarWinds** 攻击，供应链攻击所使用的入侵路径主要有：

- 包管理器
- 代码编辑器
- 应用商店
- 实用软件

包管理器供应链攻击

RubyGems 包管理器

2020 年，Ruby 包管理器 RubyGems 上被上传了两个恶意的软件包，这些软件包伪装成了比特币库和一个显示字体颜色的库（开发者常用类型库），并在被导入的时候自动执行。包管理器因为其开放性难以进行严格的代码审核，软件开发人员在使用之前应当做好代码审查验证工作。

代码编辑器供应链攻击

XcodeGhost

2015 年，国内大量的 iOS 应用中被发现植入恶意代码。原因是，有攻击者在国内网盘分发 Xcode 代码编辑器安装程序，而这些安装程序中含有恶意代码，使得通过该版本的 Xcode 编译打包的应用程序都带有恶意代码。影响：微信、网易云音乐、滴滴、高德地图等。

应用商店供应链攻击

Chrome User-Agent Switcher

2017 年，Chrome 应用商店中的热门 User-Agent 切换工具中存在恶意代码，收集用户隐私信息。该开源插件通将恶意代码隐藏在图片文件中，避开了 Chrome 市场的安全审查。该插件潜伏一定时间之后，通过收集用户敏感信息和向用户恶意推送广告获取收益。

实用软件供应链攻击

驱动人生

2018 年，驱动人生旗下产品的自动升级组件下发恶意木马执行程序。该自动升级组件拥有驱动人生的完整数字签名，借此绕过系统防护软件之后，开始通过感染的计算机向同一网段的计算进行端口扫描和漏洞攻击。

攻击持久性
Attack permanently

供应链攻击具有更强的生命力和持久性。

在 **SolarWinds** 供应链攻击事件中有一点值得注意：根据供应商发布的安全公告，**SolarWinds Orion** 平台软件在 2020 年 3 月至 6 月之间发布的 2019.4 – 2020.2.1 版本都受到了供应链攻击的影响。而直到 2020 年 12 月中旬，才被初次曝光。也就是说，这次攻击下放的恶意程序，即使在目标范围如此之广、目标组织体积如此之大的情况下，依然可以持续活动 9 个月之久。由此我们可以看出，当恶意程序或后门等威胁通过供应链侵入系统时，往往比通过其它攻击手段更加容易存活。主要原因为以下几点：

1. 供应链攻击目标更多更广，其威胁面积几乎覆盖供应商的所有下游用户。
2. 供应链攻击过程更加合法化，往往通过软件更新、硬件购买等正常渠道入侵。
3. 供应链攻击执行程序通常拥有其软硬件供应商的合法签名，故难以被 EDR 等设备检测。
4. 伴随合法主程序的运行，供应链攻击入侵的程序往往作为副属行为或子进程启动，更加难以被监测。

正是由于这种良好的隐蔽性，通过供应链成功攻陷系统后，侵入的威胁往往具有极强的生命力和持久性。

通常，可以通过如下方式对供应链攻击进行检测：

1. 增强代码安全检测能力，如引入代码检测复盘机制。
2. 通过入侵过后的行为活动检测，如引入动态沙箱。

相关安全事件

NPM nukes NodeJS 恶意软件存在多个月后才被删除

NPM 删除了其存储库上的 4 个恶意软件包，这些软件包在服务器上植入了后门应用程序，并窃取了用户数据。这 4 个软件包已被下载超过 1000 次，直到 2020 年 10 月 15 日才被 NPM 发现并删除。

安全建议

由于供应链攻击有区别于一般的攻击手段，各企业和组织往往处于供应商的下游，并且由于供应链攻击一般拥有官方数字签名，所以难以检测，一些常规的安全建议已经不再具有通用性，这就需要企业做到：

1. 建立可信的的软件开发环境
2. 关注所使用组件的安全通告
3. 企业安全建设中积极监测威胁情
4. 定期进行安全检查

云计算
CLOUD COMPUTING

前言

云计算是发展的趋势，越来越多的企业把自己的服务器、数据存储托管在云计算平台上。由此，云计算相关的安全管理和安全技术也迅速发展，受到各行各业的重视。2020 年，云计算相关的安全事件频发，越来越多的数据泄露、网络攻击都与“云”联系起来，云计算的防护、安全策略、漏洞等逐渐成为了大家研究的重心。

1. 云相关的漏洞
2. 数据泄漏
3. 知识匮乏的运维人员
4. 利用云的社工

在云计算领域，Web 应用安全、虚拟化技术、密码安全将持续成为安全的核心问题。

云相关的漏洞
Cloud computing vulnerabilities

云计算作为未来互联网的发展方向，一直都是各大安全研究人员高度关注的领域。

我们将云计算的安全分为三大领域：

- web 应用服务安全
- 虚拟化安全
- 密码安全

web 应用服务安全 主要威胁来自于热门的组件、框架所产生的通用漏洞，也就是通常所理解的网络攻击所导致的安全问题。该领域的安全问题将直接对所有的云上应用产生影响，一处应用出现问题，将影响该容器中的所有应用。

虚拟化安全 主要是系统底层架构实现云上服务的核心保障。虚拟化技术的安全问题主要存在以下特征：虚拟环境、容器将直接影响甚至控制宿主。目前应用于云计算的主要技术是 QEMU 和 Docker。该领域的安全问题将直接对物理服务主机产生影响，底层虚拟化的漏洞，将直接影响该主机上的所有容器以及容器中的所有服务。

密码安全 几乎是所有安全体系的基石，目前大规模采用的密码信任体系为 RSA（非对称加密）、ECC（椭圆曲线加密）。目前 RSA 应至少采用 1024 位密钥，ECC 应采用严格实施算法规范的认证库。该领域的安全问题将直接干扰所有安全机制的实施和运行。

相关安全漏洞

CVE-2020-14364：QEMU 虚拟机逃逸漏洞

2020 年 08 月 24 日，QEMU 发布安全补丁更新，修复了一处虚拟机逃逸漏洞。该漏洞编号为 CVE-2020-14364，漏洞等级：高危，漏洞评分：8.2。攻击者通过在云上虚拟环境（申请虚拟机即可）执行特制的二进制程序，可造成虚拟环境逃逸，并在宿主系统上执行任意命令。该漏洞由 360VulcanTeam 团队发现并在 ISC2020 上公开。

CVE-2020-14298: Docker Runc 环境逃逸漏洞

2020 年 07 月 13 日，RedHat 发布 Docker Runc 安全更新，修复了一处 runc 容器环境逃逸漏洞。该漏洞编号为：CVE-2020-14298，漏洞等级：高危，漏洞评分：8.8。攻击者通过在 docker 虚拟环境中执行特制的二进制程序，覆盖宿主 runc 可执行程序，从而造成虚拟环境逃逸，并在宿主系统上执行任意命令。

CVE-2020-8558: Kubernetes 本地主机边界绕过漏洞

2020 年 07 月 10 日，Kubernetes 官方发布边界绕过漏洞风险通告，该漏洞编号为：CVE-2020-8558，漏洞等级：中危。本地攻击者通过同一网络环境下的容器或在集群中访问特定的地址，可直接访问 kube-proxy 提供的所有接口功能（在特定情况可造成严重影响，包括但不限于：创建 / 销毁容器，在任意容器中执行命令）。

CVE-2020-0601: Windows ECC 签名算法漏洞

2020 年 01 月 15 日，微软官方发布了 2020 年 1 月份安全更新，其中修复了 Windows CryptoAPI 验证绕过漏洞。因 CryptoAPI 中验证椭圆曲线加密算法证书的方式存在漏洞。本地攻击者通过伪造特制的证书进行中间人攻击，可绕过加密校验并解密用户使用软件的机密信息。

安全建议

针对云服务商

1. 及时更新应用底层依赖及安装漏洞补丁
2. 容器间实施强隔离策略，同网段，但不同用户的容器主机都应默认隔离
3. 镜像防篡改，认证每一次镜像修改行为
4. 物理主机采用最低端口开放原则，并使用 EDR 等安全应用或设备保证底层安全
5. 用户行为严格校验，并及时告警反常的用户行为
6. 针对安全事件及时响应、排查、修复
7. 针对突发事件，优先保证数据的可恢复性

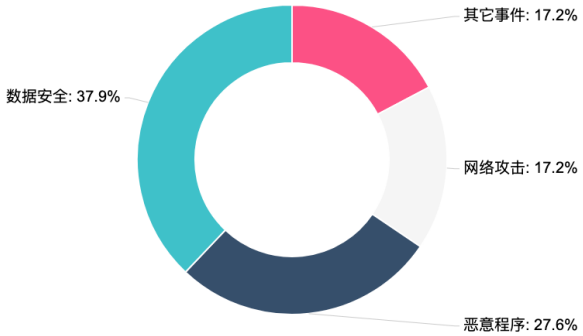
针对用户 / 企业

1. 应用间使用加密通信（例如：https）
2. 应用应只暴露服务端口（例如：80，443）
3. 应用与应用之间尽量分散部署，避免多服务在同一容器内
4. 应用部署应禁止使用同一套密钥，避免因泄漏而导致失陷
5. 应用做好接口鉴权，保证单一 Session 存活时间为有限时间
6. 应用数据隔离，避免水平服务间数据互通
7. 应用最低权限原则，应用内部任何程序都应使用单独的用户组及用户
8. 针对关键数据，保持冷热备份

云上托管发生了多起数据泄露事件，企业应该重视对托管数据的安全保护和安全策略配置。

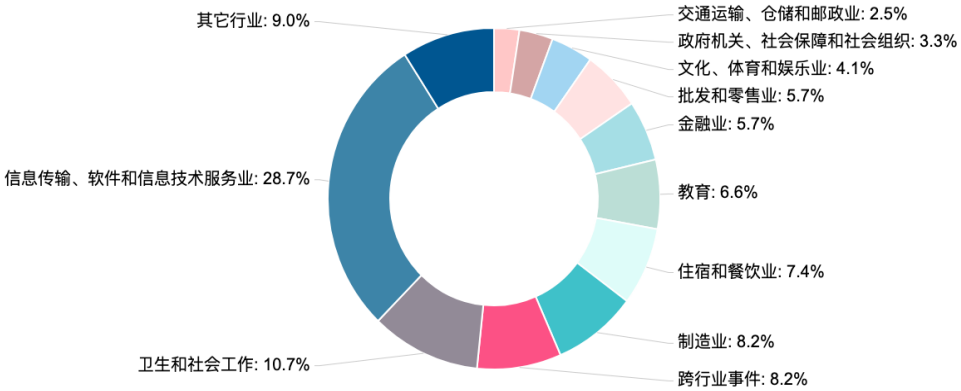
数据泄漏
Data Breach

360-CERT 监测发现，在云计算的相关事件中，数据泄漏事件占了 37.9% 的比重，各种暴露在公网的数据库，无疑是数据窃取贩卖者的天堂。



云计算事件类型占比

同时，由于大量数据泄露事件产生于云托管的服务器和数据库，导致**信息传输、软件和信息技术服务**行业的事件在所有数据安全事件中占比颇高，脆弱的 Amazon S3 Bucket、Elasticsearch、Mssql、Mysql 等暴露在公网的云数据库泄漏了大量的信息。同时，由于疫情原因，**卫生和社会工作**行业的数据泄露事件占比也名列前茅，新泽西大学医院、DNA 分析服务机构 GEDmatch、英国牙医工会、英国慈善机构等卫生组织都遭受过数据泄漏。



数据安全事件行业占比

数据泄露主要来源

1. 未加密数据库

高校招生数据库泄露近百万学生数据

CyberNews 发现了一个不安全的 Amazon S3(简单存储服务) 数据库，其中包含近 100 万条高中生学术信息记录 (包括 GPA 分数，ACT, SAT 和 PSAT 分数，非官方的成绩单，学生证，学生和家长的姓名，电子邮件地址，家庭住址，电话号码等)。不安全的数据库属于 CaptainU，该数据库还包含学生的运动成绩的图片和视频、教练的信息以及其他招聘材料。

2.Github 等代码托管平台

巴西 1600 万 COVID-19 患者的详细信息在网上曝光

由于巴西医院工作人员的失误，超过 1600 万巴西 COVID-19 患者的个人和健康详细信息在网上意外暴露。圣保罗阿尔伯特爱因斯坦医院的一名员工在 GitHub 上上传了一份包含用户名、密码和敏感政府系统访问密钥的电子表格。该电子表格包含用于多个系统的登录凭据，包括用于管理 COVID-19 患者数据的 E-SUS-VE 和 Sivep-Gripe 应用程序。

安全建议

1. 敏感数据库尽量不放在互联网，也尽量不要托管在云平台
2. 若数据库服务器必须放在公网，务必做好防火墙策略以及身份认证等相关设置
3. 加强开发人员安全培训
4. 上传到 Github 等托管平台的代码一定要经过严格监控
5. 及时检查并删除外泄敏感数据

安全管理的不规范、安全策略的不成熟是大部分安全事件产生的原因。

知识匮乏的运维人员

Site reliability engineer lacking of knowledge

360-CERT 监测发现，大部分安全事件都是安全管理的问题，而并非安全技术的问题。因此，安全运维人员尤其需要注重**加强内部的安全建设、提高安全响应速度、完善公司的安全策略**，避免弱口令等低级安全错误产生。

安全管理的主要问题

1. 弱口令，配置错误

谷歌云存储服务因错误配置导致数据泄露

Comparitech 对 2,064 个谷歌云存储服务进行调查后，发现其中 131 个谷歌云存储服务可被非法访问，恶意攻击者可因此列举，下载，上传文件。 该公司发现的暴露数据中，有 6,000 份扫描文件，包括护照，出生证和印度儿童的个人资料。

法国制药分销平台泄漏 1.7 TB 以上的数据

Apodis Pharma 是一家为药房、医疗机构、制药实验室和健康保险公司提供数字化供应链管理平台和其他软件解决方案的公司。CyberNews 调查小组发现了一个属于该公司的 ElasticSearch 数据库，由于配置错误，可被攻击者非法访问。该数据库包含超过 1.7 TB 与业务相关的机密数据（包括药品销售数据，Apodis Pharma 合作伙伴和员工的全名，客户仓库库存统计信息，药品装运位置和地址等）。

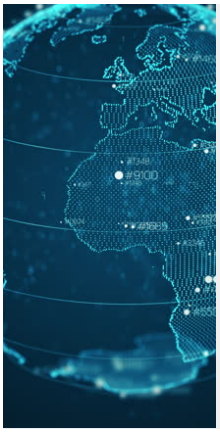
2. 不及时更新补丁

超过 61% 的 Exchange 服务器易受 RCE 攻击

超过 247000 台 Microsoft Exchange 服务器仍然容易受到 CVE-2020-0688RCE 漏洞的攻击。CVE-2020-0688 漏洞存在于 Exchange 控制面板（ECP）组件中，漏洞产生的原因是 Exchange 服务器无法在安装时正确创建唯一密钥。截至 2020 年 9 月 21 日，61% 的 Exchange 服务器（Exchange 2010、2013、2016 和 2019）仍易受到攻击。

近 5 万个存在漏洞的 Fortinet VPN 密码遭泄露

2020 年 11 月 21 日，一名黑客泄露了近 5 万个易受攻击的 Fortinet vpn 服务器的密码。该黑客利用 FortiOS 漏洞（CVE-2018-13379），从 Fortinet VPN 中访问敏感的“ sslvpn_websession”文件。这些文件会显示 Fortinet VPN 用户的纯文本用户名和密码。



安全建议

1. 优化安全管理流程
2. 细化安全管理措施
3. 制定安全管理规范
4. 提升安全管理意识

恶意攻击者常利用云平台进行社工攻击，不盲目信任云端文件和链接是防止遭受攻击的有效方案。

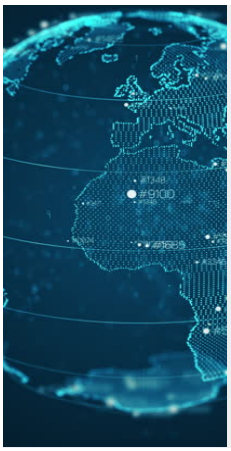
利用云的社工

Social Enginering with cloud plantform

360-CERT 监测发现，有多起安全事件使用云平台（Google Drive、OneDrive、SharePoint 等）来进行社工攻击。攻击者利用目标用户对知名云服务商的信任，诱使目标下载运行恶意文件或点击恶意链接从而完成攻击。

钓鱼攻击者利用云协作服务进行攻击

攻击者正在利用基于云的协作服务（如微软的 SharePoint Online 和 OneDrive），诱骗用户点击恶意链接，进行网络欺诈或供应链欺诈。网络安全公司 Proofpoint 在 2020 年上半年收集了大约 590 万封带有恶意 SharePoint Online 和 OneDrive 链接的电子邮件。据统计，该类型的钓鱼邮件数量占包含恶意网址的电子邮件总数的 1%，但其用户点击量却占总数的 13% 以上。



安全建议

1. 谨慎点击来源不明的链接
2. 谨慎下载来源不明的文件（尤其是可执行程序）
3. 隔离打开运行来源不明的网络文件
4. 电脑安装反病毒程序

勒索
RANSOM

前言

勒索是网络攻击的主力军之一。勒索软件在巨大的利益驱使下，不断的更新迭代，威胁着网络安全的方方面面。与勒索软件的对抗，实际上是与漏洞的对抗、与攻击技术的对抗、与社工策略的对抗，也是对自身安全防护策略的一大考验。

当前勒索软件都采取双重方案，企业在防范勒索软件的同时，更要做好数据保护和备份。

双重勒索
Double Extortion Ransomware

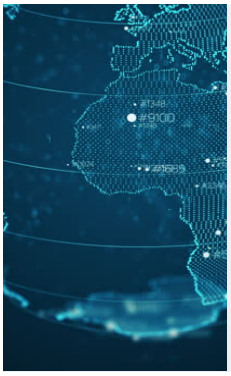
现在的勒索软件都采取双重方案，先窃取数据，再加密文件。一份勒索赎金为解密文件，一份勒索赎金为删除窃取的数据。

受害者遭受 LockBit 勒索软件双重勒索

2020 年 9 月，勒索软件集团 LockBit 推出了一个新的数据泄露网站，作为他们双重勒索策略的一部分，以恐吓受害者支付赎金。 自 2019 年底以来，勒索软件团伙采取了双重勒索策略，即在加密电脑数据之前，先窃取未加密的文件。然后勒索软件团伙利用窃取的文件，以在数据泄露网站上公开为由，迫使受害者支付赎金。

Clop 勒索软件攻击了 Software AG

德国软件集团公司 (Software AG) 遭受 Clop 恶意软件攻击。Clop 在加密文件的同时，窃取了 Software AG 的敏感数据，并索要了 2300 万美元的巨额赎金。



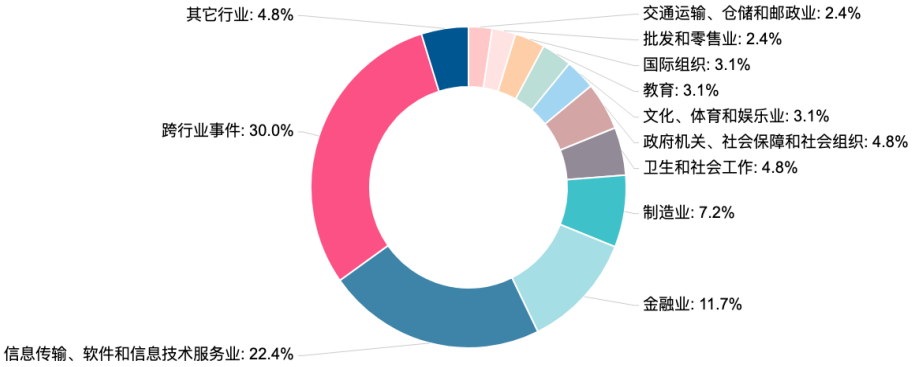
安全建议

1. 设置严格的访问策略 (如访问白名单)
2. 定期对重要数据进行备份，并将备份文件隔离保存
3. 定期进行密码更改操作，并使用复杂密码策略

恶意程序部署大量跨行业无差别扫描器。在点对点攻击方面，银行等金融业是勒索软件的最爱

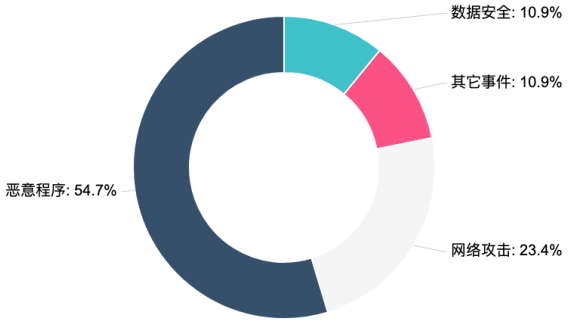
行业分布
Industry distribution

360-CERT 认为，在恶意程序的攻击策略中，更多的是跨行业、无差别攻击，扫描全球网络来寻找目标，随后加密文件，窃取数据，并索取赎金。在传统行业方面，金融业明显更加受到恶意程序的青睐，银行、证券交易所、虚拟货币交易市场等，都是恶意程序进行勒索的重点目标。



恶意程序事件行业占比

有意思的是，由于新冠疫情，医院的运转关系着每个人的安危，所以许多勒索软件都对医院手下留情，比如 NetWalker 背后的团队就公开表示，不会将医院作为攻击目标。所以在上图中，卫生行业并未达到很高的占比（卫生行业事件占比 4.8%）。



金融业事件类型占比

金融业一直是勒索软件的重要目标，塞舌尔开发银行、智利银行、Experian 信贷机构等都遭受过勒索攻击。如 Emotet、Cerberus、Mekotio 等都是臭名昭著的银行木马。

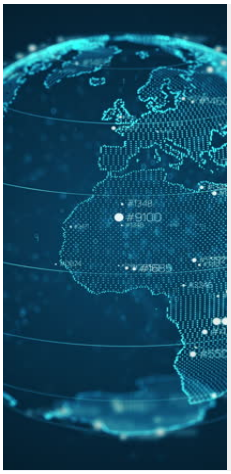
相关安全事件

勒索软件迫使保险公司关闭了 200 个管理员帐户

Ardonagh Group 保险公司被迫暂停 200 个具有管理员特权的内部帐户。英国《金融时报》称，Ardonagh Group 是英国第二大私有保险经纪公司，该公司最近公布了财务报告，显示在攻击事件之后损失 9400 万英镑。Ardonagh 的发言人 KellyAnnKnight 并不确定公司遭受的此次攻击是由勒索软件引起的。

智利银行 BancoEstado 遭 REVil 勒索软件袭击

智利最大的银行之一智利银行（BancoEstado）受 REvil 勒索软件攻击，迫使其分支机构自 2020 年 9 月 7 日起关闭。勒索软件对该公司的大多数服务器和工作站进行了加密。



安全建议

1. 每个主机安装反病毒程序
2. 内部使用的系统、服务应用、中间件等，及时进行版本升级和补丁更新
3. 在内部开展员工安全培训，提升员工安全防范意识
4. 做好内部监控，出现勒索事件立刻隔离受害主机，并及时联系安全部门或安全公司处理

中招常见原因
Common reasons

360-CERT 对勒索事件进行分析后总结出了勒索中招常见的 3 个原因：漏洞利用、社工手段、弱口令（未加密）的数据库和服务器，这也是各企业应该重视的角度。

一、漏洞利用

利用软件或服务的漏洞入侵到服务器中，最终窃取服务器数据，是恶意攻击者的惯用手段。
与往年相同，应用服务或设备自身的漏洞仍然是恶意攻击者入侵企业内部最常用的入口之一。

> **专家入侵了 28000 台不安全的打印机**
> CyberNews 安全团队的安全专家入侵了 27944 台存在漏洞且暴露在公网上的打印机，并使用被劫持的设备打印出打印机防护指南。该团队的入侵成功率为 56%，从而推测在全球 800000 台连接互联网的打印机中，至少有 447000 台是不安全的，以此来反映全球普遍缺少网络设备保护的现象。

360-CERT 对因漏洞利用而导致勒索的事件进行整理复盘时，还发现了与往年不同的现象：**因安全产品的漏洞而导致的勒索事件数量上升。**
安全产品通常用于保护相关服务器或主机免遭攻击者攻击，因其功能的特殊性，通常具备以下特点：

1. 在部署安全产品的服务器上，安全产品通常具备较高的系统权限
2. 在企业内网中，安全产品通常处于关键性位置，且在内网中权限较高

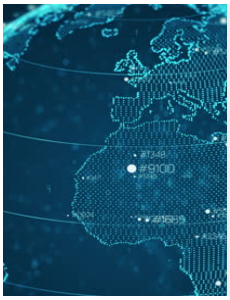
正是因为这两个特点，当恶意攻击者利用安全产品漏洞入侵到服务器或企业内网中，将更加容易的窃取数据，进行勒索攻击。同时因为缺少对安全产品的行为进行审计，在进行后续溯源时将非常困难。

美国视频传输提供商遭受勒索软件攻击

总部位于美国的视频交付软件解决方案供应商 SeaChange International 证实，在 2020 年第一季度，该公司因受到勒索软件攻击而中断了正常运营。攻击者通过利用 CVE-2019-11510 Pulse Secure VPN（用于远程访问内部网络的安全产品）远程文件读取漏洞获得了用户名及密码，从而导致攻击者可以直接访问其公司内网资源，窃取敏感数据。

全球最大眼镜公司 Luxottica 遭遇勒索袭击

全球最大眼镜公司 Luxottica 遭遇勒索袭击，攻击者利用了 CVE-2019-19781 Citrix 网关（用于远程请求准入的安全产品）远程命令执行漏洞入侵了该公司的服务器，窃取并加密了该公司的数据，最终影响了其全球各地公司的正常业务。即使在勒索发生后的三天，其办公网仍然无法正常使用。



安全建议

1. 及时关注相关应用或设备的威胁情报
2. 及时联系厂商安装漏洞修补程序

二、社工手段

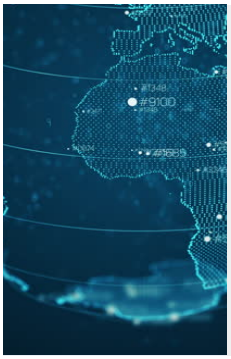
安全的本质是人与人之间的对抗，而通过社工钓鱼正是这一观点的最好体现。通过社工钓鱼的方式，攻击者可以简单高效的进入到企业内网中，从而窃取敏感数据。这也是恶意攻击者最常用的方式之一。

使用社会工程学的攻击者通过充分的数据收集，分析并利用目标对象的心理弱点，诱使目标对象提供相关敏感信息，或完成攻击者所指定的操作。在多种恶意的社会工程行为中，网络钓鱼是最常见的攻击方式。

网络钓鱼电子邮件通常模仿来自合法公司或个人的邮件，利用受害者的心理弱点，诱使受害者点击恶意链接或运行恶意程序。攻击成功的攻击者可以因此获取受害者的敏感信息甚至远程控制受害者的主机。当受害者的主机位于办公网时，攻击者可以以受害者主机为跳板，直接入侵企业内网。

澳大利亚网络安全中心：社工仍是勒索主要攻击手段

2020 年 09 月澳大利亚网络安全中心发布年度网络威胁报告，报告中称电子邮件仍然是恶意攻击者最常用的攻击载体之一，邮件中经常携带勒索软件、信息窃取工具和其他恶意代码。通过利用邮件钓鱼的方式，攻击者可以轻松进入企业内网，从而窃取数据。



安全建议

1. 对员工进行内部安全培训，提高员工安全意识
2. 不轻信网络消息，不随意打开邮件附件，不随意访问未知链接，不随意运行可执行程序

三、弱口令

随着应用上云的趋势，将服务和数据托管到公有云服务器上的方案被越来越多的企业所采纳，但同时因使用弱密码的配置而导致数据被窃取的勒索事件也越来越多，这也是恶意攻击者窃取数据进行勒索的主要方式之一。

黑客勒索 26,000 个脆弱的 MongoDB 数据库

据安全研究员的研究发现，三个黑客组织针对公开在外网的 MongoDB 数据库进行了攻击，共劫持了 26000 台数据服务器，并索要赎金以还原数据。

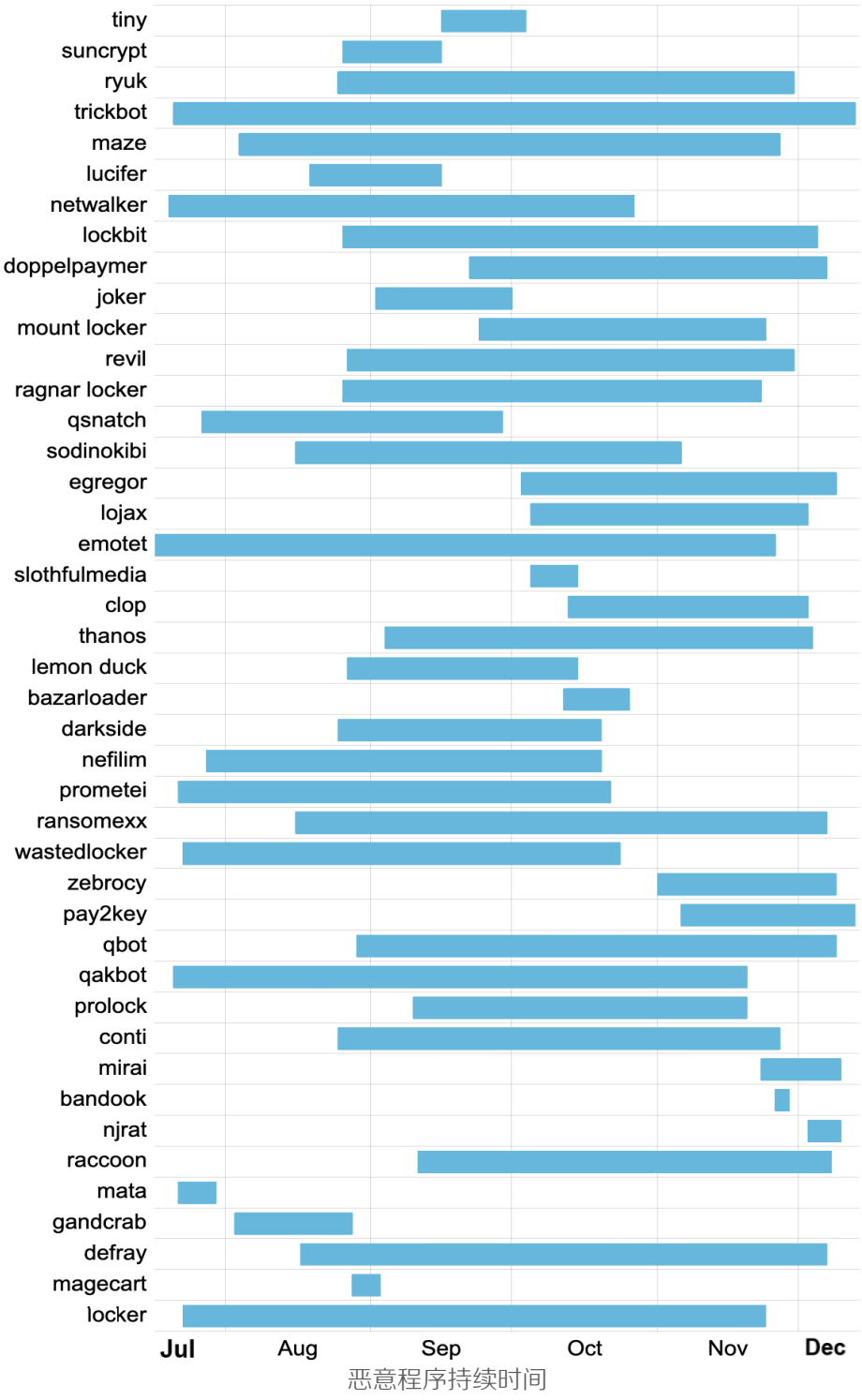
安全建议

1. 敏感数据库尽量不放在互联网上，也不要托管在云平台上。
2. 若数据库必须放在公网上，应做好防火墙访问策略以及身份认证策略，以防止攻击者恶意爆破数据库密码
3. 对员工进行内部安全培训，禁止将应用的敏感配置文件上传到 Github 等公开代码托管平台。

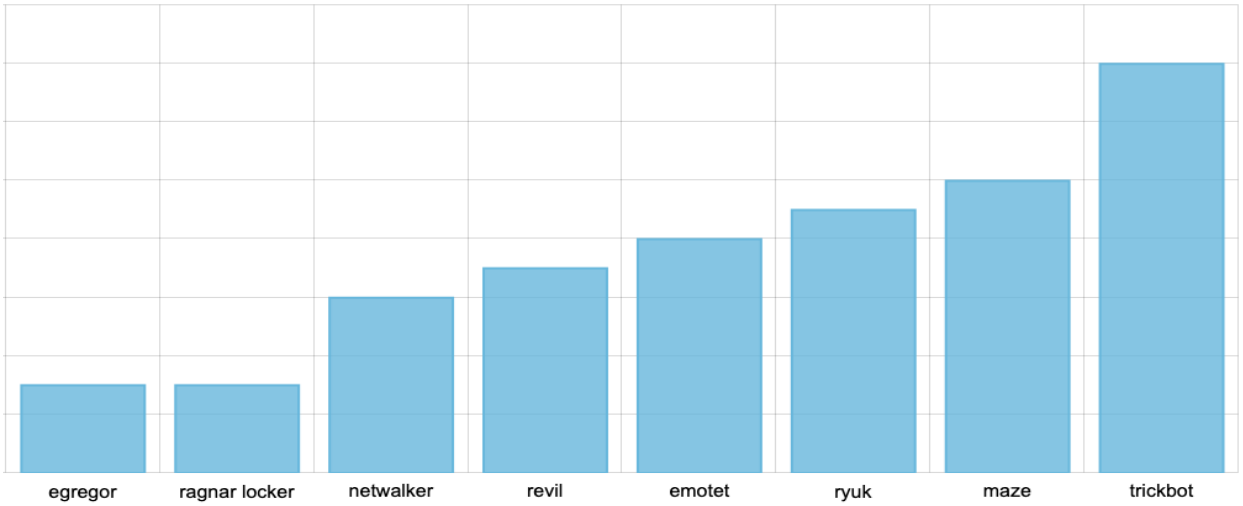
勒索大家族一直都是威胁大型企业和社会组织的主力军，了解勒索大家族有助于各行各业做出有针对性的防御措施。

勒索大家族
Ransomware families

2020 下半年，全球范围内的勒索事件激增。我们对勒索程序的持续活跃时间做了对比，形成下图



恶意程序持续时间



恶意程序活跃程度

Trickbot 当属 2020 年最活跃的勒索软件，是最流行的银行恶意软件家族之一，于 2016 年底首次被检测到，是目前规模最大，寿命最长的僵尸网络之一。2020 年 10 月，TrickBot 大部分服务器被攻陷，这迫使 TrickBot 关闭了其大部分的主要基础设施，不过其作者已将其部分代码移至 Linux 上了，以扩大成为目标的受害者的范围。

Maze 是活跃程度第二高的勒索大家族，Maze 勒索软件于 2019 年 5 月首次被发现，在过去的一年里，Maze 勒索软件已经成为威胁企业和大型组织的最臭名昭著的恶意软件家族之一，Maze 勒索软件是第一批如果受害者拒绝合作就泄露机密数据的勒索软件家族之一。直到 2020 年 11 月 2 日，Maze 勒索软件团伙宣布他们正式关闭勒索软件业务，不再在他们的网站上泄露新公司的数据。

Ryuk 勒索软件同样活跃在恶意程序中，平均每周攻击 20 家公司。Ryuk 勒索软件最早于 2018 年 8 月首次被发现，是最早的勒索软件系列之一，它可以禁用 Windows 系统的恢复功能，使得在没有外部备份或回滚技术的情况下无法从攻击中恢复。Ryuk 勒索的目标往往是一些知名度较高的组织，以此获得高额的赎金。Ryuk 通过垃圾邮件进行传播，当用户打开垃圾邮件中带有恶意宏的文档时，恶意宏便会执行 PowerShell 命令，从而下载勒索软件。

Emotet 银行木马于 2014 年被发现，是 2019 年最活跃的网络犯罪活动和恶意软件僵尸网络，不过，Emotet 在 2020 年 2 月 7 日停止了所有活动，休息了 5 个多月后，于 2020 年 7 月卷土重来。并开始在全球范围内发送大量恶意垃圾邮件，通过垃圾邮件附件来传播恶意软件。迄今为止，Emotet 攻击了大量美国和欧洲的个人，公司和政府实体，并窃取了目标的财务数据甚至比特币钱包。

REvil （也被称为 Sodinokibi) 勒索软件于 2019 年 4 月 17 日首次被发现，REvil 勒索软件组织通过批量扫描攻击技术、RDP 服务器爆破和后门软件，利用漏洞分发勒索软件。REvil 可能与 GandCrab 勒索软件有关，原因是两者代码相似，并且随着 GandCrab 勒索软件活动的减少，REvil 勒索软件开始活跃。

NetWalker 也是活跃度较高的勒索软件，最初被称为 Mailto，于 2019 年 8 月首次被发现。自 2019 年以来，NetWalker 勒索软件的目标主要是在西欧国家和美国。在侵入后，Netwalker 勒索软件会终止所有在 Windows 上运行的进程和服务，对磁盘上的文件进行加密，并删除存储在同一网络中的备份。因此，受害者网络中存储在设备上的所有东西都无法访问。由于新冠疫情，医疗服务提供商是 NetWalker 最大的目标之一，除此之外，教育机构、地方政府和私人公司也是 NetWalker 攻击的目标。

Ragnar Locker 勒索软件会影响运行微软 Windows 操作系统的设备，最初是在 2019 年 12 月底发现的。在启动 Ragnar Locker 勒索软件之前，攻击者注入一个后门，可以从受感染的机器收集敏感数据，并将其上传到自己的服务器上。接下来，恶意软件背后的威胁者会通知受害者，如果赎金没有支付，这些文件将被公开。

Egregor 是一种新发现的勒索软件的变种，于 2020 年 9 月 25 日首次被发现，并针对全球范围内的大型组织（包括游戏行业巨头 Crytek 和 Ubisoft）发起攻击。截至 2020 年 11 月 17 日，Egregor 勒索软件团伙已经列出了 71 名受害者，横跨 19 个不同的垂直行业。Egregor 勒索软件的受害者需要下载暗网浏览器 TOR，并在三天内联系勒索软件开发人员。如果受害者不遵循指示并支付赎金，那么这些受害者的公司数据将在“Egregor News”数据泄漏站点（DLS）被公开。

常用的 ATT&CK 攻击方式
Common attack pattern of ATT&CK

攻击者将系统设置配置为在主机启动或登录期间自动执行程序，以保持持久性或在受到感染的系统上获得更高级别的特权。

Boot or Logon Autostart Execution（自启动）

编号：T1547

目的：持久化，权限提升

平台：Linux, Windows, MacOS

权限要求：Administrator, User, Root

安全建议：
1. 监视可用于触发自动启动执行的机制的增删添改（例如注册表）。
2. 查找与已知更新、补丁程序或其他计划中的管理活动不相关的更改。
3. 当与历史数据进行比较时，可疑程序的自启行为会出现异常的过程。
4. 监视进程的 DLL 加载，特别是无法识别或不正常加载到进程中的 DLL。查找可能由进程加载恶意 DLL 引起的异常进程行为。
5. 监视内核修改或驱动程序安装中涉及的实用程序和命令行参数的异常使用。

攻击者可尝试获取有关系统上正在运行的进程的信息。获得的信息可用于了解网络内系统上运行的通用软件 / 应用程序。

Process Discovery（进程信息收集）

编号：T1057

目的：信息收集

平台：Linux, Windows, MacOS

权限要求：Administrator, SYSTEM, User

攻击者可能会尝试获取有关操作系统和硬件的详细信息，包括版本，补丁，热修复 (hotfixes)，服务包和体系结构等。

System Information Discovery（系统信息收集）

编号：T1082

目的：信息收集

平台：AWS, Azure, GCP, Linux, Windows, MacOS

权限要求 : User

安全建议：
1. 使用白名单工具（如 AppLocker、 或软件限制策略）审计和拦截恶意程序。
2. 监视可以收集系统和网络信息的进程和命令行参数的操作
3. 多维度监测，某些远程控制工具会与 Windows API 交互以收集信息，所以监测网络行为也是不错的选择

攻击者枚举文件和目录，或在主机或网络共享的特定位置搜索文件系统内的某些信息。

File and Directory Discovery（文件目录信息收集）

编号：T1083

目的：信息收集

平台：Linux, Windows, MacOS

权限要求：Administrator, SYSTEM, User

安全建议：
1. 监视可以收集系统和网络信息的进程和命令行参数的操作

攻击者通过使用通用的标准化应用层协议（如 HTTP，HTTPS，SMTP 或 DNS）与已控制机器进行通信，并尝试通过与现有通信流混合来避免检测。

Application Layer Protocol(应用层协议)

编号：T1071

目的：命令控制 (C&C)

平台：Linux, Windows, MacOS

权限要求：Administrator, SYSTEM, User, Root

安全建议：
1. 使用网络签名来区别恶意软件的网络流量。
2. 分析不常见数据流的网络数据（例如，客户端发送的数据远多于从服务器接收的数据）。
3. 未遵循内部网络协议规范的进程是可疑的

攻击者可能滥用命令和脚本解释器来执行命令、脚本、二进制文件。这些界面和语言提供了与计算机系统交互的方式，并且是许多不同平台之间的共同功能。大多数系统都具有一些内置的命令行界面和脚本功能，例如，MacOS 和 Linux 发行版包含某种形式的 Unix Shell，而 Windows 则包括 Windows Command Shell 和 PowerShell。

Command and Scripting Interpreter(命令和脚本解释器)

编号：T1059

目的：命令 / 代码执行

平台：Linux, Network, Windows, MacOS

权限要求： User

安全建议：

1. 防病毒 / 反恶意软件：防病毒可用于自动隔离可疑文件。
2. 代码签名：在可能的情况下，仅允许执行签名的脚本。
3. 禁用不恰当的程序：禁用或删除任何不必要的或未使用的 shell 或解释器。
4. 可执行程序白名单：严格限制活动范围。
5. 特权账户管理：当需要 PowerShell 时，请将 PowerShell 执行策略限制为管理员。请注意，根据环境配置，有一些绕过 PowerShell 执行策略的方法。
6. 限制基于 Web 的内容：对于通过广告等 web 方式投放的恶意代码，adblocker 等程序可以帮助阻止代码的执行。

初始访问
面向公众应用的利用

执行
命令行界面
通过API接口执行
定时任务
用户执行

持久化
端口试探
定时任务

权限升级
访问令牌操纵
进程注入
定时任务

横向移动
远程服务

防御逃逸
访问令牌操纵
连接代理
文件或信息解混淆和解码
删除主机上指示信息
伪装
混淆文件或信息
端口试探
进程注入

凭据访问
凭据转储
输入捕捉

发现
进程发现
查询注册表
远程系统发现
软件发现
系统信息发现
系统所有者/用户发现

采集
本地系统数据
数据暂存
邮件收集
输入捕捉
屏幕截图

命令与控制
连接代理
失败回退通道
端口试探
远程访问工具
标准应用层协议
标准非应用层协议

数据渗漏
自动化数据渗漏
C&C通道的数据渗漏
定时传输

勒索软件常用攻击方式矩阵图

事件相关数据统计
DATA PRESENTATION

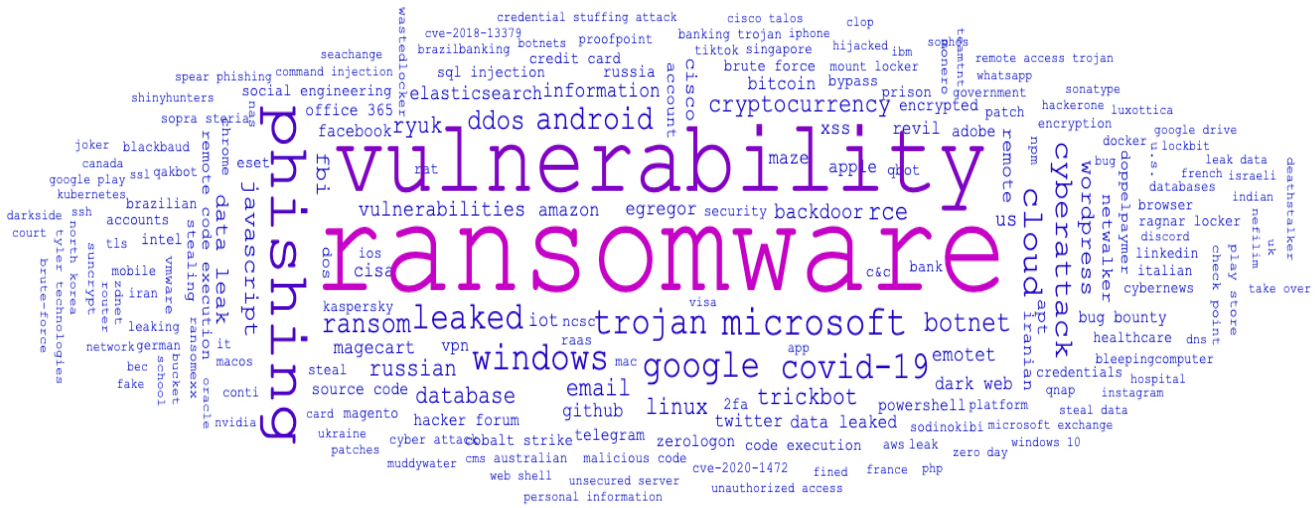
前言

通过对 2020 下半年所有《安全事件周报》的国际安全事件进行统计，我们从热词、常用漏洞、常见组件、热门组织四个方面，得出了一份数据统计信息，这些信息反映了企业最应该重视的攻击方式、漏洞、组件、产品和安全防护方向。

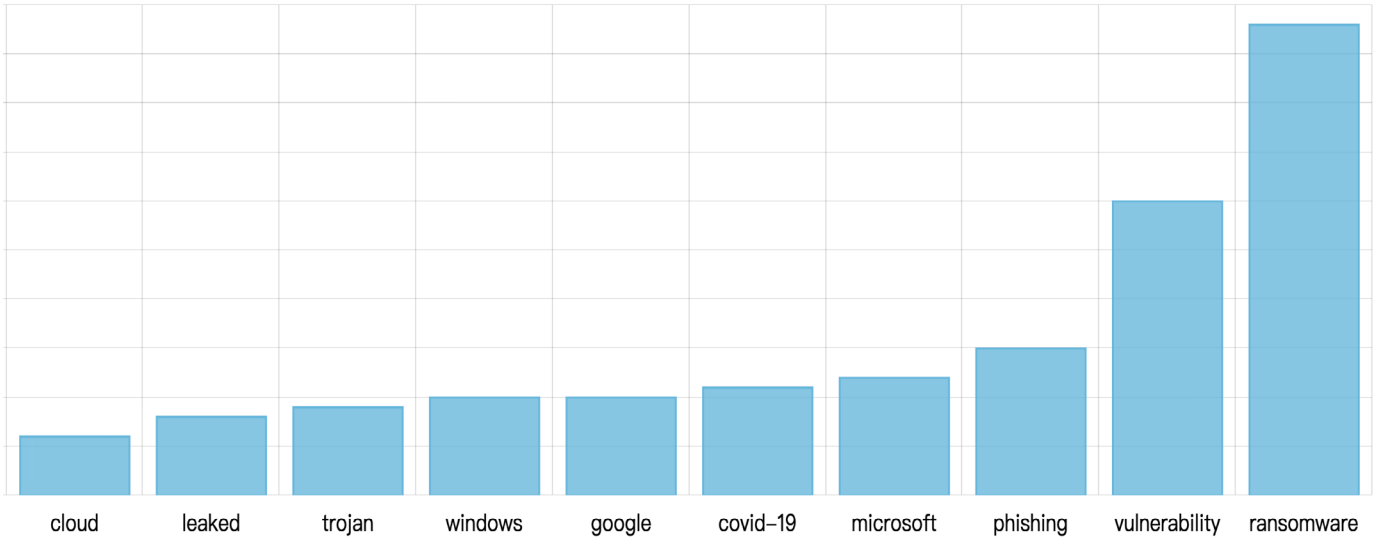
1. 热词 TOP
2. 漏洞 TOP
3. 涉及组织 TOP
4. 组件 TOP

热词
TOP

热词词云图



热词 TOP10 柱状统计图



漏洞 TOP10

01

CVE-2020-1472

NetLogon 特权提升漏洞

攻击者通过 NetLogon（MS-NRPC），建立与域控间易受攻击的安全通道时，可利用此漏洞获取域管访问权限。成功利用此漏洞的攻击者可以在该网络中的设备上运行特殊设计的应用程序。

02

CVE-2020-0688

Microsoft Exchange 远程代码执行漏洞

经过身份验证的攻击者可以从身份验证的 session 中收集 ViewStateUserKey，并在登录请求的原始响应中获得 __VIEWSTATEGENERATOR。通过这两个值可以利用 YSoSerial.net 工具生成恶意的 ViewState，从而在 ECP 中执行任意的 .NET 代码。

03

CVE-2019-11510

Pulse Secure SSL VPN 非授权任意文件读取漏洞

Vpn 用户和密码 hash 存储 mtmp/system 中，dataa/data.mdb 存储这用户登陆后缓存的明文密码，randomVal/data.mdb 存储着用户 Session。攻击者可以利用该漏洞获取账号密码，并登录后台。

04

CVE-2019-19781

Citrix 路径遍历漏洞

该漏洞的目录遍历被限制在 vpns 文件夹下，任意用户可通过 HTTP 请求直接访问该目录下的文件。

05

CVE-2020-5902

F5 BIG-IP 远程代码执行漏洞

未授权的远程攻击者通过向漏洞页面发送特制的请求包，可以造成任意 Java 代码执行。进而控制 F5 BIG-IP 的全部功能，包括但不限于：执行任意系统命令、开启 / 禁用服务、创建 / 删除服务器端文件等。该漏洞影响控制面板，不影响数据面板。

06

CVE-2018-13379

Fortigate SSL VPN 任意文件读取漏洞

攻击者利用此漏洞可以读取目标系统任意文件、获取相关账号密码，并结合其它漏洞获得服务器权限

07

CVE-2020-14882

Weblogic Console HTTP 协议代码执行漏洞

远程攻击者可以构造特殊的 HTTP 请求，在未经身份验证的情况下接管 WebLogic Server Console ，并在 WebLogic Server Console 执行任意代码。

08

CVE-2020-15999

Chrome Freetype 字体库堆溢出漏洞

由于 FreeType 字体库存在堆溢出漏洞，未授权的攻击者通过此漏洞可造成代码执行。

09

CVE-2020-17087

Microsoft cng.sys 权限提升漏洞

CVE-2020-17087 是 Windows 内核密码驱动程序（cng.sys）中的缓冲区溢出漏洞。该漏洞来自输入 / 输出控制器（IOCTL），并且可能允许本地攻击者提升特权，以及沙盒逃逸。

10

CVE-2020-15505

MobileIron 远程代码执行漏洞

MobileIron Core 10.6 及之前版本、Connector 10.6 及之前版本和 Sentry 9.8 及之前版本中存在安全漏洞。远程攻击者可利用该漏洞执行任意代码。

涉及组织
TOP10

Microsoft
微软是美国一家跨国电脑科技公司，以研发、制造、授权和提供广泛的电脑软件服务为主。

Google
Google 是总部位于美国加州门洛帕克的跨国科技公司，业务范围涵盖互联网广告、互联网搜索、云计算等领域，开发并提供大量基于互联网的产品与服务。

Facebook
Facebook 是源于美国的社交网络服务及社会化媒体网站，总部位于美国加州圣马特奥县门洛帕克市。

Twitter
Twitter，是美国一个微博客和社交网络服务平台。

Amazon
亚马逊公司是一家总部位于美国西雅图的跨国电子商务企业，业务起始于线上书店，不久之后商品走向多元化。

Github

GitHub 是通过 Git 进行版本控制的软件源代码托管服务平台，由 GitHub 公司的开发者 Chris Wanstrath、PJ Hyett 和 Tom Preston-Werner 使用 Ruby on Rails 编写而成。

Cisco

思科系统是一间跨国际综合技术企业，总部设于加州硅谷。思科开发、制作和售卖网络硬件、软件、通信设备等高科技产品及服务，并透过子公司打入其他科技市场，比如物联网、域名安全、能源管理。

Apple

苹果公司，原称苹果电脑公司，是总部位于美国加州库比蒂诺的跨国科技公司。

Intel

英特尔公司是世界上最大的半导体公司，也是首家推出 x86 架构处理器的公司，总部位于美国加利福尼亚州圣克拉拉。

Adobe

Adobe 公司，是美国一家跨国电脑软件公司，总部位于加州的圣何塞。

涉及组件
TOP10

Exchange
Microsoft Exchange Server 是微软公司的一套电子邮件服务组件。

Cisco
思科的路由器和交换机在业界具有统治的地位。其路由器一直为各大园区、数据中心和分支机构网络提供高度安全可靠的服务。而交换机则具备出色的性能和安全性，兼具扩展能力和成本效益，能够满足各种规模企业的需求。

WordPress
WordPress 是一个以 PHP 和 MySQL 为平台的自由开源的博客软件和内容管理系统

Elasticsearch
Elasticsearch 是一个基于 Lucene 库的搜索引擎。它提供了一个分布式、支持多租户的全文搜索引擎，具有 HTTP Web 接口和无模式 JSON 文档。

Weblogic
WebLogic 是美商 Oracle 的主要产品之一。是商业市场上主要的 Java 应用服务器软件之一，是世界上第一个成功商业化的 J2EE 应用服务器。

QNAP

威联通科技，品牌名称 QNAP，为台湾一家网络附加储存设备制造商，2004 年自威强电工业电脑分割成立，总部位于新北市。

Mysql

MySQL 原本是一个开放源码的关系数据库管理系统，原开发者为瑞典的 MySQL AB 公司，该公司于 2008 年被昇阳微系统收购。

Jenkins

Jenkins 是一款由 Java 编写的开源的持续集成工具。

Redis

Redis 是一个使用 ANSI C 编写的开源、支持网络、基于内存、可选持久性的键值对存储数据库。

Drupal

Drupal 是由德赖斯·布伊泰尔特创立的自由开源内容管理系统，用 PHP 语言写成。

大事件回顾
INCIDENTS REVIEW

2020-07-13

黑客窃取了安全公司数据

一名黑客攻击了一家美国网络安全公司的后端服务器，并从该公司的“数据泄漏检测”服务中窃取了数据。其称，被盗的数据包括 8200 多个数据库，其中包含过去其他公司泄漏的数十亿用户的信息。这些数据库已收集在 DataViper 内部，DataViper 是一种数据泄漏监视服务，由美国网络安全公司 Night Lion Security 背后的安全研究人员 Vinny Troia 管理。

2020-07-14

黑客在暗网上出售 1.42 亿米高梅酒店客人的详细信息

米高梅度假村 2019 年的数据泄露事件的规模远比最初报道的要大得多，已影响超过 1.42 亿酒店客人，而不仅是 ZDNet 最初于 2020 年 2 月报告的 1060 万。黑客在一个暗网网络犯罪市场上以略高于 2900 美元的价格出售了 142,479,937 名米高梅酒店客人的详细信息。

2020-07-15

埃隆马斯克等人 twitter 账号被盗，并发布欺诈信息

2020 年 7 月 15 日，包括比尔 · 盖茨，埃隆 • 马斯克和苹果在内的许多高知名度的 Twitter 帐户遭到攻击。 盖茨，马斯克和苹果的账户发布了恶意推文，并且留下区块链钱包地址，要求关注者将钱寄到该地址以换取更大的回报。 美国总统候选人乔 · 拜登、美国总统奥巴马的推特账号也遭到攻击。

2020-07-20

勒索程序团伙要求阿根廷 ISP 提供 750 万美元赎金

7 月 18 日，一个勒索程序团伙感染了阿根廷电信（该国最大的互联网服务提供商之一）的内部网络，要求提供 750 万美元的赎金以解锁加密文件。该攻击被认为是阿根廷最大的黑客事件之一。ISP 内部人员称，黑客在设法获得内部 Domain Admin 的控制权后，对该公司的网络造成了严重破坏，传播安装了勒索软件 payload 到 18,000 多个终端。

2020-07-28

黑客免费泄漏了 18 家公司的 3.86 亿条用户记录

有攻击者正在黑客论坛泄露大量数据，披露超过 3.86 亿用户记录，他们声称从 18 家公司窃取了数据。 自 7 月 21 日起，一个名为 ShinyHunters 的数据泄露商，开始在一个黑客论坛上免费公开泄露数据库。 在过去的一年中，ShinyHunters 参与了一系列数据泄露事件，泄露的数据包括 Wattpad、Dave、Chatbooks、Promo.com、Mathway、HomeChef，以及微软私有 GitHub 存储库。

2020-08-06

英特尔泄露 20GB 的源代码和内部文档

2020 年 8 月 6 日，美国芯片制造商英特尔的机密文件被上传到了一个公共文件共享服务上，据称这些文件是由黑客入侵获得的。数据容量为 20GB，来源不明。这是英特尔一系列泄密事件的一部分。 被泄露的文件包括技术规范和相关的内部芯片组设计，包括 Kaby Lake 平台和英特尔管理引擎 (ME)。

2020-08-10

Chrome 浏览器漏洞导致数十亿用户数据被盗

Google 的基于 Chromium 的浏览器中的漏洞可能使攻击者绕过网站上的内容安全政策（CSP），窃取数据并执行恶意代码。 据 PerimeterX 网络安全研究员 Gal Weizman 称，该漏洞影响（CVE-2020-6519）可在 Windows，Mac 和 Android 的 Chrome，Opera 和 Edge，可能影响数十亿网络用户。 Chrome 版本 73（2019 年 3 月）到 83 版本（84 已在 7 月发布并修复了该问题）受到影响。

2020-08-17

数千个加拿大政府帐户遭到黑客攻击

加拿大财政部发布公告，数千个在线政府服务账户遭到恶意攻击者攻击。恶意攻击者通过凭据填充攻击 GCKey 服务，该服务被大约 30 个联邦部门使用。攻击者盗取了 9041 名 GCKey 账户的登录凭证，并使用这些账户尝试访问政府服务。

2020-08-19

新的 FritzFrog P2P 僵尸网络已经侵入了至少 500 家企业和政府服务器

在 2020 年之前，研究人员新发现的 P2P 僵尸网络攻击了至少 500 台政府和企业 SSH 服务器。 2020 年 8 月 19 日，网络安全公司 Guardicore 公布了对 FritzFrog 的研究，这是一种 P2P 僵尸网络。根据研究人员 Ophir Harpaz 的说法，在过去的八个月中，FritzFrog 试图暴力破解全球的政府，教育，金融，医疗和电信的 SSH 服务器。

2020-08-19

数据搜集公司泄露了 2.35 亿 Instagram、TikTok 和 YouTube 的用户记录

2020 年 8 月 1 日，Comparitech 的 Bob Diachenko 发现该公司的一个数据库被曝光。其中包含来自不同社交网络的 2.35 亿用户的个人资料，包括以下内容：Instagram：192,392,954 条记录，TikTok：42,129,799 条记录，YouTube：3,955,892 条记录，曝光的数据包括用户名、真实姓名、联系方式、图片、粉丝统计数据、年龄、性别，以及一些其他的细节。

2020-08-26

美国政府警告称，朝鲜黑客攻击全球银行

2020 年 8 月 26 日多家美国政府机构发布的联合咨询报告称，朝鲜黑客组织 BeagleBoyz 一直在使用恶意远程访问工具，以从国际银行窃取数百万美元。自 2020 年 2 月以来，朝鲜的 BeagleBoyz 黑客组织通过互联网远程抢劫银行，以资助朝鲜政权。美国网络司令部在推特上称，BeagleBoyz 目前正在对 30 多个国家的银行实施抢劫计划，企图盗窃 20 亿美元。

2020-08-27

3.5 亿个解密后的电子邮件地址暴露在不安全的服务器上

CyberNews 发现了一个不安全的数据存储库，其中包含 7 千兆字节的未加密文件，包括 3.5 亿串独特的电子邮件地址。大量的数据保存在了一个可公开访问的 AWS 服务器上，任何人都可以下载和访问这些数据。

2020-08-28

变化多端恶意软件 Gozi

自 Gozi 2007 年首次公开亮相以来，它就是一个简单的恶意程序，以单个代码库的形式一直在网络攻击者群体中传播。2010 年，第一版 Gozi 的源码遭到泄漏。攻击者获取并更新了代码，创建了两个新版本：Gozi Prinimalka（后来与 Pony 合并成为 Neverquest）和 Gozi ISFB。当第二波 Gozi 出现了足够长的时间后，一些攻击者感到市场上已经有了成熟的时机，从而导致了 Goziv3（RM3 加载程序），ISFB3 和 Gozi2RM3（IAP 2.0）的诞生。

2020-08-29

Emotet 恶意软件采用 Red Dawn 附件进行攻击

Emotet 僵尸网络已经开始使用一个新的模板来处理他们的恶意附件。在经历了 5 个月的“休假”后，Emotet 恶意软件于 2020 年 7 月卷土重来，并开始在全球范围内传播大量恶意垃圾邮件。这些垃圾邮件活动假装是发票、发货信息、COVID-19 信息、简历、财务文档或扫描文档。这些垃圾邮件的附件都是恶意的 Word（.doc）附件或下载链接。打开后，这些附件将提示用户“启用内容”，以便恶意宏运行。之后便在受害者的计算机上安装 Emotet 恶意软件。

2020-08-28

联邦调查局称：网络恋情诈骗案金额超 4.75 亿美元

网络恋情诈骗是种持续存在的网络犯罪事件，会导致巨大的经济损失，以及情感创伤。这类骗子利用伪造的网络身份，在社交媒体和交友网站上获得受害者的信任。一旦目标被引诱进来，骗子就利用恋爱为媒介，操纵受害者给他们寄钱。网络恋情诈骗经济损失额每年都在急剧增加，2017 年损失超过 2.11 亿美元，2018 年超过 3.62 亿美元，2019 年的损失则超过 4.75 亿美元。

2020-08-31

AgentTesla 木马通过 COVID-19 援助活动传播

Area 1 Security 的研究人员表示，恶意攻击者在疫情期间策划了一场提供口罩及其他个人防护设备的援助活动，通过该活动散布 AgentTesla 木马。该援助活动始于 2020 年 5 月，它利用人们在疫情期间对口罩和温度计短缺的担忧，使用钓鱼邮件对化学品制造商及进出口企业实行诈骗。据悉，恶意攻击者每 10 天就会改变其钓鱼策略和程序，并对钓鱼邮件和恶意域名进行调整，以防被发现。

2020-09-01

美国百万选民的详细资料被泄露

据俄罗斯报纸报道，一名网名为 Gorka9 的用户在一个不具名的论坛上发布消息称，密歇根州 760 万选民的个人信息可以公开获取。安全人员 Kommersant 还发现了包含康涅狄格州、阿肯色州、佛罗里达州和北卡罗来纳州 200 万至 600 万选民详细信息的数据。泄露的记录包括姓名、出生日期、性别、选民登记日期、地址、邮政编码、电子邮件、选民登记号码和投票站号码。

2020-09-03

在线营销公司曝光 3800 多万美国公民记录

CyberNews 发现了一个不安全的数据仓库，它属于在线营销公司 View Media。这个数据仓库有近 3900 万份美国公民记录，包括他们的全名、电子邮件地址、街道地址、电话号码和邮政编码。任何人都可以访问和下载数据。

2020-09-06

勒索软件袭击使阿根廷边境过境暂停 4 小时

阿根廷官方移民局 Dirección Nacional de Migraciones 遭遇 Netwalker 勒索软件攻击，暂停止了出入境业务。虽然针对城市和地方机构的勒索软件攻击已经非常普遍，但这可能是已知的第一次针对联邦机构的攻击，它已经中断了一个国家的运作。为了防止勒索软件感染其他设备，移民局和控制站使用的计算机网络已被关闭。

2020-09-07

新南威尔士州 738GB 的客户数据在电子邮件泄露期间被盗

新南威尔士州服务局透露，由于 2020 年 47 名员工的电子邮件账户遭到网络攻击，18.6 万名客户的个人信息被盗。新南威尔士州服务机构表示，他们发现有 738GB 的数据从电子邮件账户中被盗，其中 380 万份文件被盗。

2020-09-08

微软发布的补丁修复了严重漏洞

微软已经在其 9 月补丁日更新中发布了 129 个安全漏洞的补丁。 其中包括 23 个严重漏洞，105 个高危漏洞和一个中危漏洞。据研究人员说，这当中最严重的漏洞是 CVE-2020-16875。这是 Microsoft Exchange 中的一个内存破坏漏洞，它仅需向目标发送电子邮件，就能造成远程代码执行 (RCE)。运行任意代码可以为攻击者授予他们创建新帐户、访问、修改或删除数据以及安装程序所需的访问权限。

2020-09-09

第三方代码中的严重漏洞可以导致接管工控系统

Wibu 是一个软件管理组件，许多顶级工业控制系统（ICS）软件供应商都授权使用该组件，包括罗克韦尔自动化（Rockwell Automation）和西门子（Siemens）。8 月 11 日，Wibu 的 CodeMeter 组件中发现了六个严重漏洞。未经验证的远程攻击者可以利用这些漏洞发动各种恶意攻击，包括部署勒索软件、关闭并接管关键系统。

2020-09-08

严重的 Adobe 漏洞允许攻击者在浏览器中运行 JavaScript

2020 年 9 月 Adobe 在 其 Experience Manager 中修补了 11 个漏洞，其中有五个严重级别的 XSS 漏洞：CVE-2020-9732，CVE-2020-9742，CVE-2020-9741，CVE-2020-9740 和 CVE-2020-9734。Adobe 称：“对这些漏洞的成功利用会导致攻击者在目标浏览器中任意执行 JavaScript。

2020-09-09

美国视频传输提供商证实勒索软件攻击

总部位于美国的视频交付软件解决方案供应商 SeaChange International 证实，在 2020 年第一季度，该公司因受到勒索软件攻击而中断了正常运营。攻击者通过利用 CVE-2019-11510 Pulse Secure VPN（用于远程访问内部网络的安全产品）远程文件读取漏洞获得了用户名及密码，从而导致攻击者可以直接访问其公司内网资源，窃取敏感数据。

2020-09-10

黑客从加密货币交易平台 ETERBASE 窃取了 540 万美元

2020 年 9 月 10 日斯洛伐克加密货币交换机构 ETERBASE 披露了一个安全漏洞。黑客通过该漏洞窃取了比特币、Ether、ALGO、Ripple、Tezos 和 TRON 价值 540 万美元的资产。ETERBAS 因此暂停了所有交易。

2020-09-14

Zerologon 攻击能让 Windows 域完全沦陷

Zerologon 攻击允许攻击者通过利用 CVE-2020-1472 来接管企业网络。CVE-2020-1472 漏洞是 Netlogon 特权提升漏洞。Netlogon 服务是 Windows 客户端身份验证体系结构中使用的一种身份验证机制，用于验证登录请求，并对域控制器进行注册、身份验证和定位。企业 Windows 服务器的管理员必须尽快安装 2020 年 8 月的补丁，以保护他们的系统免受 CVE-2020-1472 的 Zerologon 攻击。

2020-09-16

多个热门购物网站数据泄露

有报道称，一个配置错误的 Elasticsearch 数据库暴露了 70 个约会和电子商务网站的 882GB 数据。IT 安全研究人员发现了其中含有一个属于德国在线购物网站 Windeln.de 的数据库。该商店的生产服务器数据库暴露了 6.4 TB 数据，其中包含 60 亿条记录，泄露了超过 70 万名客户的个人信息。

2020-09-22

全球最大眼镜公司 Luxottica 遭遇勒索袭击

攻击者利用了 CVE-2019-19781 Citrix 网关（用于远程请求准入的安全产品）远程命令执行漏洞入侵了该公司的服务器，窃取并加密了该公司的数据，最终影响了其全球各地公司的正常业务。即使在勒索发生后的三天，其办公网仍然无法正常使用。

2020-09-23

印度的新冠监视工具暴露了数以百万计的用户数据

一份来自 VPNnentor 的研究报告显示，Uttar Pradesh 地方政府的 COVID-19 监视工具在 8 月 1 日遭到攻击，导致大量数据泄露。该工具是一个大型测绘项目的一部分，其主要目的是追踪印度各地的冠状病毒患者。由于缺乏数据安全协议，不慎使平台的访问权限对外完全开放，导致印度数百万人的个人数据暴露。

2020-09-25

Windows XP 的源代码已被泄漏

据称，WindowsXP SP1 和其他版本操作系统的源代码 2020 年 9 月 25 日在网上被泄露。一位黑客声称花了两个月时间来编译泄露的 Windows 源代码。该代码由一个 43GB 的 torrent 进行传播，在这个 torrent 中包含了所谓的 Windows XP 和 Windows Server 2003 以及一系列更旧版本的操作系统的源代码。

2020-09-26

黑客从 KuCoin 加密货币交易所偷走了 1.5 亿美元

位于新加坡的加密货币交易所 KuCoin 披露了一起重大安全事件，黑客攻破了它们的热钱包，盗走了所有资金，约 1.5 亿美元。热钱包用作当前正在交换的资金的临时存储系统，冷钱包是指任何未连接到互联网的加密货币钱包。在 KuCoin 公司调查这起安全事件期间，存款和取款被暂时停止。

2020-09-26

匈牙利遭遇大规模的 DDoS 攻击

据电信公司 Magyar Telekom 称，9 月 24 日匈牙利金融机构和电信基础设施遭到来自俄罗斯、越南服务器的大规模 DDoS 攻击。这次 DDoS 攻击袭击了匈牙利的一些银行和电信服务，使它们短暂中断服务。这次攻击非常强大，这是匈牙利有史以来遭受的最大的网络攻击之一。

2020-10-06

美国公司 1500 万美元网络抢劫案剖析

经验丰富的网络攻击者通过邮件诈骗从一家美国公司窃取了 1500 万美元，这起诈骗案件耗时 2 个月。这名网络罪犯在获取了商业交易的电子邮件对话后，他们在交易中插足，转移了资金，并得以将偷窃行为隐瞒了足够长的时间，最终拿到了钱。尽管研究人员只调查了一个受害者的事件，但他们发现的线索表明，建筑、零售、金融和法律行业的数十家企业都在他们的目标名单上。

2020-10-01

BEC 诈骗活动造成巨额损失

据事件应对公司 Migrate 称，最近破获的一个针对高管微软 Office365 账户的商业电子邮件泄露诈骗案 (Business Email Compromis， 简称 BEC) 迄今已在全球范围内攻击了 150 多家机构，诈骗者已经赚取约 1500 万美元。在过去的几年里，BEC 诈骗案对欺诈者来说越来越有利可图。美国联邦调查局（FBI）互联网犯罪投诉中心 2020 年 2 月发布的年度网络犯罪报告发现，BEC 计划在 2019 年造成了约 17 亿美元的损失。

2020-10-06

勒索软件迫使保险公司关闭了 200 个管理员帐户

Ardonagh Group 保险公司被迫暂停 200 个具有管理员特权的内部帐户。英国《金融时报》称，Ardonagh Group 是英国第二大私有保险经纪公司，该公司最近公布了财务报告，显示在攻击事件之后损失 9400 万英镑。Ardonagh 的发言人 KellyAnnKnight 并不确定公司遭受的此次攻击是由勒索软件引起的。

2020-10-13

迈阿密的科技公司泄露了 1TB 的客户和业务数据

位于迈阿密的增值解决方案和技术产品公司 Intcomex 遭遇重大数据泄露，数据为近 1TB 的用户数据。其中包括信用卡、护照和执照扫描、个人数据、工资单、财务文档、客户数据库、员工信息等。部分数据是在俄罗斯一个流行的黑客论坛上免费公开的，该泄露数据的第一部分于 2020 年 9 月 14 日公开，第二部分于 2020 年 9 月 20 日公开。

2020-10-14

SonicWall VPN 高危漏洞导致 DoS、RCE

2020 年 10 月 16 日，SonicWall 官方发布安全通告，SonicOS 中存在缓冲区溢出漏洞，远程攻击者可以在未授权的情况下构造特定的 HTTP 请求触发该漏洞，造成拒绝服务（DoS）攻击。该漏洞还可以通过堆栈破坏更改程序执行流，所以还可能造成远程代码执行。该漏洞存在于产品管理服务及 SSL VPN 远程准入服务中。

2020-10-19

网络电话服务提供商泄漏了 3.5 亿客户记录

互联网语音协议公司 Broadvoice 的一个超过 3.5 亿客户记录的数据库，存储在了不安全的 Elasticsearch 集群中。10 月 1 日，安全研究员 Bob Diachenko 发现了这个不安全的数据库。他观察到，未受保护的 Elasticsearch 集群包含了 3.5 亿客户记录的敏感信息。包括呼叫者姓名、电话号码和地点。其中一个数据库被发现包含数十万封语音邮件以及其它信息，如医疗处方和金融贷款。

2020-10-21

Google 补丁修复了 Chrome 浏览器的 0day 漏洞

Google 发布了其 Chrome 浏览器的更新程序，该更新程序修补了 Chrome 浏览器的 FreeType 字体渲染库中的一个 0day 漏洞，该漏洞已被广泛使用。 该漏洞为堆缓冲区溢出漏洞。Glazunov 在 2020 年 10 月 19 日向谷歌提交了这个漏洞。

2020-10-20

美国国安局：黑客常用的 25 大漏洞

在 2020 年 10 月 20 日发布的一份报告中，美国国家安全局表示，它知道有黑客发起了针对国家安全系统 (NSS)、美国国防工业基地 (DIB) 和国防部 (DoD) 信息网络的攻击。在这些攻击的中，美国国家安全局已经发现了使用了 25 个公开的漏洞，这些漏洞被用来访问网络，部署恶意移动应用，并通过横向传播，窃取敏感数据。美国国家安全局建议所有机构立即给易受攻击的设备打补丁，以防止数据盗窃、银行欺诈和勒索软件攻击。

2020-10-21

WordPress 对流行插件进行了强制的安全更新

2020 年 10 月，WordPress 安全团队强行为一个流行插件推送安全更新。运行 Loginizer 插件的 WordPress 站点 2020 年 10 月 20 日被强制更新到 1.6.4。这个版本修复了一个 SQL 注入漏洞。该漏洞可让黑客接管 WordPress 站点。Loginizer 是当今最流行的 WordPress 插件之一，该插件为 WordPress 登录页面提供了安全性增强。

2020-10-27

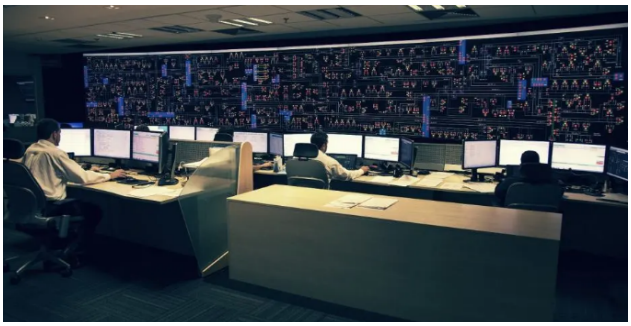
黑客在窃取 Harvest Finance 2400 万美元

黑客已经从分布式金融服务 Harvest Finance 窃取了价值约 2400 万美元的加密货币资产。攻击者最初在 Harvest Finance 公司的服务中投资了大量加密货币资产，然后利用加密技术窃取平台的资金，并将其转移到 Harvest Finance 公司控制的钱包中。专家们注意到攻击发生后不久，黑客返还了大约 250 万美元给 Harvest Finance，但并没有说出原因。

2020-10-27

Enel 集团今年遭受了第二次勒索软件攻击

跨国能源公司埃奈尔集团 (Enel Group) 的系统被网络勒索软件感染，这是该集团在 2020 年遭受的第二次勒索软件攻击。网络勒索软件运营商要求支付 1400 万美元的赎金来换取解密密钥。黑客声称已经从该公司窃取了数 TB 的数据，并威胁说如果不支付赎金，就会公开这些数据。埃奈尔集团 (Enel Group) 是意大利的一家跨国能源公司，活跃于发电、配电以及天然气分销领域。该公司在 40 个国家拥有 6100 多万客户，在《财富》全球 500 强中排名第 87 位，2019 年的收入为 900 亿美元。



2020-10-29

严重的 Oracle WebLogic 漏洞被在野利用

攻击者已经开始寻找运行 Oracle WebLogic 实例的服务器，这些服务器容易受到一个严重漏洞的攻击，这个漏洞允许攻击者跳过认证就能控制系统。攻击中利用的漏洞是 CVE-2020-14882，其严重性评级为 9.8(满分 10 分)，攻击者能够通过一个简单的 HTTP GET 请求控制系统。Oracle 在 2020 年 10 月发布的高危补丁更新中修复了该漏洞。

2020-11-27

1600 万巴西 COVID-19 患者的详细信息在网上曝光

由于巴西医院工作人员的失误，超过 1600 万巴西 COVID-19 患者的个人和健康详细信息在网上意外暴露。圣保罗阿尔伯特爱因斯坦医院的一名员工在 GitHub 上上传了一份包含用户名、密码和敏感政府系统访问密钥的电子表格。该电子表格包含用于多个系统的登录凭据，包括用于管理 COVID-19 患者数据的 E-SUS-VE 和 Sivep-Gripe 应用程序。

2020-12-01

黑客利用黑盒攻击从意大利的 atm 机中窃取了 80 万欧元

一个犯罪组织利用一种新的黑匣子攻击技术，从意大利的至少 35 台自动取款机中盗取钱财。意大利执法机构证实，该网络犯罪组织利用 ATM 黑盒攻击，在短短 7 个月内窃取了约 80 万欧元。在这种攻击中，黑盒设备（如移动设备或覆盆子）与 ATM 物理连接，攻击者利用它向机器发送命令，然后从自动取款机中提取所有现金。

2020-11-27

物联网芯片制造商 Advantech 受勒索软件攻击，要求 1250 万美元的赎金

Conti 勒索软件团伙袭击了工业自动化和工业物联网（IIoT）芯片制造商 Advantech 的系统，目前要求 1400 万美元赎金，以解密受影响的系统，并停止泄露被盗的公司数据。Advantech 是全球领先的医疗保健设备和解决方案制造商，拥有超过 8000 人的嵌入式计算机和服务器。2018 年，该公司以 34% 的 WW 市场份额成为世界工业计算领域的领导者，2019 年公司的年销售收入超过 17 亿美元。

2020-12-01

Talos 报告了 WebKit 的远程代码执行漏洞

思科的 Talos 团队发现了 WebKit 浏览器引擎中的安全漏洞，这些漏洞的严重性很高，其中包括可以由远程攻击者利用的安全漏洞，通过诱使用户访问恶意网站来实现代码执行。WebKit 是由 Apple 开发的浏览器引擎，主要用于其 Safari Web 浏览器以及所有 iOS Web 浏览器。BlackBerry Browser、PlayStation 控制台、Tizen 移动操作系统以及 Amazon Kindle 电子书阅读器随附的浏览器都使用的 WebKit。

2020-11-02

万豪因客户数据泄露被英国监管机构罚款 1840 万英镑

信息专员办公室 (ICO) 已经就 2014 年的数据泄露对万豪开出了 1840 万美元的罚单。万豪酒店集团 (Marriot hotel group) 曾在 2014 年遭遇数据泄露事件，影响到万豪于 2015 年收购的喜达屋 (Starwood) 度假连锁酒店。攻击者渗透进喜达屋的系统，并通过一个 web shell 执行恶意软件（包括远程访问工具和凭证收集软件）。攻击者随后得到了用于存储客人预订数据的数据库访问权限，这些数据包括姓名、电子邮件地址、电话号码、护照号码、旅行细节和信用卡信息。这一事件一直持续到 2018 年，在四年的时间里，大约 3.39 亿宾客的信息被盗。总共有 700 万条与英国客人有关的记录被曝光。

2020-11-03

Oracle 发布远程代码执行漏洞的紧急补丁

Oracle 在 2020 年 11 月 1 日发布了一个安全更新，主要修复了 Oracle WebLogic 服务器上的一个远程代码执行漏洞：CVE-2020-14750。该漏洞是 CVE-2020-14882 漏洞补丁的绕过。攻击者无需任何认证即可远程利用，Oracle 强烈建议用户尽早应用这些更新。Oracle WebLogic Server 是一个 Java EE 应用服务器。

2020-11-04

日本电子游戏公司 Capcom 遭遇勒索袭击

游戏开发商 Capcom 承认遭遇勒索攻击，该公司拥有多个知名游戏 IP，包括街头霸王，生化危机，鬼泣，丧尸围城等。该公司发布的关于网络问题的公告称，在 2020 年 11 月 2 日上午遭受了网络攻击，针对该事件，游戏开发商关闭了部分公司网络，以防止恶意软件传播。勒索软件团伙声称在运行了 Ragnar Locker 样本之后窃取了 1 TB 的文件，包括会计文件、银行报表、机密预算和收入文件、税务文件、知识产权、专有商业信息、客户和员工信息等敏感数据。

2020-11-09

漏洞赏金猎人发现美国国防部的严重漏洞

美国国防部已经修复了一个严重影响其内部网络的漏洞，该漏洞允许攻击者通过修改发送到国防部服务器的 web 请求中的一些参数来劫持国防部账户。该漏洞是由美国安全公司 Silent Breach 的安全研究员 Jeff Steinburg 发现的。这个漏洞的严重程度被评为“严重”。

2020-11-09

全球数百万酒店客人遭遇大规模数据泄露

一个被广泛使用的酒店预订平台已经曝光了世界各地不同酒店的 1000 万份与客人相关的文件，这是由一个错误配置的 AWS S3 bucket 引起的。这些记录包括敏感数据（信用卡细节）。酒店使用 Prestige Software 的 Cloud Hospitality 将其预订系统与在线预订网站（如 Expedia 和 Booking.com）集成。Planet 安全团队称，该事件泄露了总计 24.4 GB 的数据。研究人员说，此次数据泄露影响的人数很可能超过 1000 万。

2020-11-07

暗网上泄露了 2000 万 Bigbasket 用户数据

杂货电子商务网站 Bigbasket 遭遇了数据泄露，暗网上有超过 2000 万人的详细信息可供购买。该数据有 15GB 大小，包含 2000 万用户记录，它以超过 40000 美元的价格出售。Bigbasket 由阿里巴巴集团，Mirae Asset-Naver 亚洲成长基金和 CDC 集团共同创立，其上市产品有 1000 多个品牌的 18000 多种产品。在新冠肺炎疫情继续在全球蔓延的同时，网络购物对用户来说变得越来越重要，此类事件使数百万用户面临黑客攻击的风险。

2020-11-10

新的“Ghimob”恶意软件可以监视 153 个 Android 移动应用程序

安全研究人员发现了一种新的 Android 银行木马，它可以从 153 个 Android 应用程序中窃取数据。据安全公司卡巴斯基(Kaspersky)2020 年 11 月 9 日发布的一份报告称，这款名为 Ghimob 的木马被认为是由 Windows 恶意软件 Astaroth (Guildma) 背后的同一个组织开发的。卡巴斯基说，新的 Android 木马已经被打包在恶意的 Android 应用程序中提供下载。

2020-11-11

微软发布了 112 个安全漏洞修复程序

2020 年 11 月 10 日，微软发布了 112 个安全漏洞修复程序，其中 17 个被评为严重漏洞。受影响的 Microsoft 产品有 15 种，包括：Microsoft Windows, Office, Internet Explorer, Edge (EdgeHTML and Chromium), ChakraCore, Exchange Server, Dynamics, Windows Codecs Library, Azure Sphere, Windows Defender, Teams, Azure SDK, Azure DevOps, 和 Visual Studio。其中一个已修复的漏洞正在被积极利用，即 Windows 内核加密驱动程序漏洞 (CVE-2020-17087)，由谷歌的 Project Zero 在 10 月底披露。

2020-11-10

微软前工程师因盗窃 1000 万美元被判 9 年监禁

一名前微软软件工程师因从公司盗窃超过 1000 万美元被判有期徒刑 9 年。陪审团做出的判决发现，被指控的 Volodymyr Kvashuk 犯有 18 项重罪。其中包括 5 项电信欺诈指控，6 项洗钱指控，2 项严重身份盗窃指控，2 项虚假纳税申报单指控，以及 1 项邮件欺诈、访问设备欺诈和访问受保护的计算机以欺诈的指控。Kvashuk 在 2016 年 8 月成为一名员工之前曾担任微软承包商的工作。在微软发现他的盗窃行为后，他于 2018 年 6 月被解雇。

2020-11-11

Animal Jam 儿童虚拟世界遭遇数据泄露，影响 4600 万用户

Animal Jam 是 WildWorks 创建的虚拟世界，孩子们可以在这里和其他成员一起玩在线游戏。Animal Jam 面向 7 至 11 岁的儿童用户，由儿童创造的动物角色超过 3 亿，每 1.4 秒就会有新玩家注册。2020 年 11 月 10 日，一个攻击者在一个黑客论坛上免费共享了两个属于 Animal Jam 的数据库，他们说这些数据库是由知名黑客 ShinyHunters 窃取的。这两个被盗的数据库名为 game_accounts 和 users，包含约 4600 万被盗用户的数据。

2020-11-12

ModPipe 后门攻击了酒店行业使用的 POS 软件

ESET 的研究人员发现了一个模块化后门 ModPipe，可以让攻击者访问 MICROS RES 3700 POS 餐饮系统中的敏感信息。该系统是一个管理软件，被全球数十万家酒吧、餐厅、酒店使用。该后门的独特之处在于它的可下载模块及其功能。其中一个名为 GetMicInfo 的算法，通过从 Windows 注册表值中解密来收集数据库密码。

2020-11-13

Vertafore 数据泄露案曝光 2770 万德州司机信息

保险软件提供商 Vertafore2020 年 11 月 13 日披露了一起数据泄露事件，承认黑客窃取了 2770 万德克萨斯州司机的详细信息。这起事件发生在 3 月 11 日，由于人为错误，三个数据文件意外暴露在一个不安全的外部存储服务中。Vertafore 表示，这些文件于 8 月 1 日从外部存储系统中删除，但经过调查，他们发现这些文件仍在未经授权的情况下被访问。

2020-11-19

警告：GO SMS Pro 应用程序的漏洞会暴露数百万条媒体消息

流行短信应用程序 GO SMS Pro 中存在一个未修补的安全漏洞，该漏洞会暴露用户之间的媒体传输，包括私人语音信息、照片和视频。Trustwave 高级安全顾问 Richard Tan 说：“这意味着该应用程序的用户之间共享的敏感消息都有被攻击者破坏的危险”。该漏洞存在于该应用程序的 7.91 版本中，该版本于 2020 年 2 月 18 日在 Google Play 商店中发布。

2020-11-23

巴西政府从有史以来最严重的网络攻击中恢复过来

在 11 月 3 日发生勒索软件攻击后，最高法院 STJ 的系统有 26 个小时完全不可用。调查机构还包括联邦数据处理服务公司 Serpro 和美国陆军网络防御单位。在 11 月 20 日系统全面恢复之前，最高法院 STJ 在处理紧急案件时能力受限。最高法院 STJ 的总统部长 Henrique Martins 表示，就规模和复杂性而言，这是巴西政府机构遭遇的“有史以来最严重的”网络攻击。

2020-11-20

三菱电机公司受到网络攻击

三菱电机受到大规模网络攻击，可能导致其业务合作伙伴的相关信息泄露。公司管理人员 11 月 20 日表示，他们正在检查与之有业务往来的 8653 个账户，以确定是否有信息泄露。入侵发生在 2019 年 6 月 28 日，该公司于 2019 年 9 月展开了调查。在两家当地报纸《朝日新闻》(Asahi Shimbun) 和《日本经济新闻》(Nikkei) 报道了安全漏洞之后，三菱电机才披露了这一安全事件。有关国防部门、铁路和电力供应组织的高度机密信息被盗。

2020-11-23

假冒的 Minecraft mods 用广告淹没了超过百万台 Android 设备

攻击者绕过 Google 对 Play 官方商店的保护，为流行游戏 Minecraft 发布了 20 多个假 modpack。这些应用程序只是空壳，旨在吸引想要修改其游戏玩法的儿童和青少年。一旦安装，几乎无法正常使用手机。 该 modpacks 将每两分钟打开一个带有广告的浏览器窗口。卡巴斯基的安全研究人员在 7 月检测到了此操作，发现最假 modpack 被安装超过一百万次。

2020-11-24

Peatix 的用户数据被泄露

2020 年 11 月，一名黑客泄露了在活动组织平台 Peatix 上注册的 420 多万用户的数据。Peatix 目前是 Alexa 网站中最受欢迎的 3500 个网站之一。该网站的用户数据可通过 Instagram stories、Telegram 频道以及几个不同的黑客论坛获得。根据友商侦测到的 Peatix 数据样本，泄露的信息包括全名、用户名、电子邮件以及加密的密码。

2020-11-25

5 万个存在漏洞的 Fortinet VPN 密码被泄露

2020 年 11 月 21 日，一名黑客通过 CVE-2018-13379 漏洞，泄露了 5 万个 Fortinet vpn 的密码。利用严重的 FortiOS 漏洞 CVE-2018-13379，攻击者可以从 Fortinet VPN 中访问敏感的“ sslvpn_websession”文件。这些文件包含与会话有关的信息，但最重要的是，这些文件可能会显示 Fortinet VPN 用户的纯文本用户名和密码。

2020-11-25

NCSC 敦促修复 MobileIron RCE

英国国家网络安全中心（NCSC）发出警报，敦促各大公司修复 MobileIron 移动设备管理（MDM）系统中的 CVE-2020-15505 漏洞。该漏洞是 MobileIron 移动设备管理（MDM）软件中的远程代码执行问题，该漏洞使远程攻击者可以执行任意代码，并接管远程公司服务器。

2020-11-26

勒索软件攻击将使法国 IT 服务部门损失 6000 万美元

2020 年 10 月 21 日，Sopra Steria 声称遭受 Ryuk 勒索软件攻击。当时，该公司表示，没有客户或公司数据泄漏，该公司管理的客户系统也没有任何重大损失。但到了 2020 年 11 月，该公司表示，由于自攻击发生以来的修复成本和公司各种系统的相继沦陷，该攻击预计将对其运营利润造成 4700 万至 5900 万美元的负面影响。

2020-12-01

法国制药分销平台泄漏 1.7 TB 以上的数据

CyberNews 调查小组发现了一个可公开访问的 ElasticSearch 数据库。该数据库包含法国软件公司 Apodis Pharma 的机密数据。Apodis Pharma 是一家为药房，医疗机构，制药实验室和健康保险公司提供数字化供应链管理平台和其他软件解决方案的公司。CyberNews 发现的数据库中有超过 1.7 TB 的与业务相关的机密数据，包括药品销售数据，Apodis Pharma 合作伙伴和员工的全名，客户仓库库存统计信息，药品装运位置和地址等。

2020-12-01

尽管修复了漏洞，但 Android 应用程序仍泄露了 1 亿用户的信息

GO SMS Pro 是一个 Android 即时消息应用程序，安装量超过 1 亿，尽管开发人员已经为修复漏洞付出了将近两个星期的努力，但该程序仍在公开数百万用户的私人共享消息。该漏洞由 Trustwave 的研究人员三个月前发现并于 11 月 19 日公开披露，未经身份验证的攻击者可以利用该漏洞，不受限制地访问 GO SMS Pro 用户私下共享的语音消息，视频和照片。

2020-12-01

印度就业网站 IIMJobs 的数据库被泄露

根据 Alexa 流量分析，IIMJobs 是印度访问量最大的 700 家网站之一。印度就业委员会 IIMJobs 的数据库在一个著名的黑客论坛上被泄露。根据 Hackread.com 网站分析，该数据库于 2020 年 11 月 23 日被泄露，其中包含多达 46GB 的数据，这些数据来源于在 IIMJobs 注册的求职者和招聘人员的信息。IIMJobs 网站约 140 万注册用户受到数据泄露的影响。

2020-12-02

俄罗斯黑客论坛上泄露了 850 多万条图片网站的用户记录

一个免版税的图片网站的数据在一个俄罗斯黑客论坛上被泄露。123RF.com 公司是一家位于马来西亚的数字股票内容代理公司，销售免版税的图片、录像和音频。它是 Inmagine 集团的一部分，每月有超过 1200 万活跃用户（包括苹果、谷歌、亚马逊和微软等）。数据库中 8500246 条用户记录泄露了用户的全名、电子邮件地址、IP 地址、位置、使用 MD5 哈希算法进行哈希处理的密码等。

2020-12-03

勒索软件团伙声称从 E-Land 窃取了 200 万张信用卡

Clop 勒索软件声称在过去的一年时间里从 E-Land Retail 盗窃了 200 万张信用卡。E-Land Retail 是 E-Land Global 的子公司，经营着许多零售服装店，包括 New Core 和 NC 百货商店。2020 年 10 月，E-Land Retail 在遭受 Clop 勒索软件攻击后不得不关闭 23 个 NC 百货商店和 New Core 商店。在被攻击之后，E-Land Retail 表示敏感的客户数据是安全的，因为这些数据被加密存储在另一台服务器上。

2020-12-03

扫描 400 万个 Docker images 后发现：51%存在严重漏洞

容器安全公司 Prevasio 分析了 Docker Hub 上托管的 400 万个公共 Docker 容器镜像，发现其中大多数具有严重漏洞。有 51%的镜像包含至少一个严重漏洞的程序包或应用程序依赖项，而 13%的镜像具有严重的漏洞。动态分析还揭示了 6,432 个恶意或潜在有害的镜像，占 Docker Hub 所有公开可用镜像的 0.16%。

2020-12-03

新的 TrickBot 版本可以篡改 UEFI/BIOS 固件

TrickBot 恶意软件的运营商添加了一项新功能，可以使他们与受感染计算机的 BIOS 或 UEFI 固件进行交互。安全公司 Advanced Intelligence 和 Eclypsium 在 2020 年 12 月 3 日发表的联合报告中称，他们发现了 TrickBot 新的功能模块，该模块在 10 月底首次出现。新模块使安全研究人员感到担忧，因为其功能将使 TrickBot 恶意软件在受感染的系统上建立更持久的立足点，从而使恶意软件能够在操作系统重新安装后存活下来。

2020-12-04

温哥华地铁的交通系统被 Egregor 勒索软件攻击

Egregor 勒索软件的行动已经破坏了温哥华地铁运输机构 TransLink，此次网络攻击导致服务和支付系统中断。在恢复了支付系统后，TransLink 发表了一份声明称：“我们的一些 IT 基础设施遭到勒索软件攻击，包括安检系统与通信系统”。Global BC 记者乔丹·阿姆斯特朗（Jordan Armstrong）在推特上发布了一张勒索单的图片，并称 TransLink 打印机正在反复打印赎金单。

2020-12-05

勒索软件袭击直升机制造商 Kopter

直升机制造商 Kopter 已经成为勒索软件攻击的受害者，黑客入侵了它的内部网络并加密了公司的文件。在 Kopter 拒绝与黑客接触后，勒索软件团伙在暗网上公布了该公司的一些文件，共享的文件包括商业文件，内部项目，以及各种航空航天和国防工业标准。

2020-12-07

富士康遭勒索软件袭击，赎金高达 3400 万美元

2020 年 11 月 29 日左右，富士康在墨西哥的一家工厂遭遇勒索软件攻击，攻击者窃取了未加密的文件，然后对设备进行加密。富士康是全球最大的电子制造公司，2019 年的营业收入达到 1,720 亿美元，在全球拥有超过 80 万名员工。 2020 年 12 月 7 日，DoppelPaymer 勒索软件在其勒索软件数据泄漏站点上发布了属于富士康 NA 的文件。泄漏的数据包括常规业务文档和报告，但不包含任何财务信息或员工的个人详细信息。

2020-12-07

数以百万计的物联网设备面临 TCP/IP 堆栈漏洞的风险

数以百万计的消费者和企业 IoT 设备在其 TCP/IP 堆栈软件中存在漏洞，该漏洞会导致远程代码执行、拒绝服务。Forescout 将该漏洞称为 Amnesia:33。多达 150 个供应商的设备可能会受到攻击。这些漏洞影响最大的是物联网设备，以及各种各样的嵌入式系统，包括医疗设备、工业控制系统、路由器和交换机。

2020-12-10

25 万个被盗的 MySQL 数据库在暗网出售

黑客在暗网上建立了一个拍卖网站，出售数万个 MySQL 服务器中的 25 万个数据库，整个数据库的大小为 7TB。数据库勒索业务自 2020 年 10 月以来急剧增加。早在 2020 年 5 月份，BleepingComputer 就报告说，一个攻击者正在从网上商店窃取 SQL 数据库，并威胁受害者，如果他们不支付比特币，就将他们的数据公开。

2020-12-14

SolarWinds 供应链攻击

根据 SolarWinds 官方发布的安全公告，SolarWinds Orion 平台软件在 2020 年 3 月至 6 月之间的更新程序受到了供应链攻击的影响，这些版本的安装包内存在恶意的后门应用程序。这些安装程序通过 SolarWinds 的数字证书绕过了检查。安装更新后会释放一个 SolarWinds.Orion.Core.BusinessLayer.dll 文件。同时该恶意程序的所有网络通信都会伪装成 Orion Improvement Program（OIP）协议的网络流量，并将通信返回结果存储在合法的插件配置文件中，从而使其能够无缝的与 SolarWinds 自身活动融合，进而达到隐蔽的目的。

2020-12-10

牙科诊所供应商遭黑客攻击，泄露了 100 多万名患者的信息

佛罗里达州的一家牙科诊所服务公司表示遭到了黑客攻击，泄露了 100 多万名患者的信息，包括支付卡号。该公司在其网站上称自己是美国规模最大、历史最悠久的牙科支持机构之一。若联邦监管机构确认细节，该事件将是 2020 年迄今为止报道的最大的健康数据泄露事件之一。2020 年 10 月 11 日，总部位于佛罗里达州萨拉索塔的 Dental Alliance Care 11 发现了这起黑客事件。

2020-12-14

美国临时人力资源机构 440GB 的数据被泄露

美国临时人力资源机构(Automation Personnel Services)的 440GB 档案在一个黑客论坛上被泄露。Automation Personnel Services 公司表示，目前正在进行调查，受影响数据的范围和性质尚未得到确认。被泄漏的文件包含公司的机密数据、用户信息、合作伙伴和员工有关的敏感文件，例如薪资数据以及各种法律文件。该归档文件于 11 月 24 日被泄露，被泄漏的原因是 Automation Personnel Services 拒绝支付赎金。

2020-12-15

微软和科技公司合作攻击了 SolarWinds 黑客的核心服务器

2020 年 12 月 15 日，微软和科技公司联盟，攻破了 SolarWinds 黑客事件中起着核心作用的服务器。该服务器的域名是 avsvmcloud.com。它作为命令和控制（C&C）服务器，通过公司 Orion 应用程序的木马更新向大约 18,000 个 SolarWinds 客户发送了恶意软件。SolarWinds Orion 在 2020 年 3 月至 2020 年 6 月之间发布了从 2019.4 到 2020.2.1 的更新版本，其中包含一种名为 SUNBURST（也称为 Solorigate）的恶意软件。

2020-12-15

世界各地医院的 4500 万医疗扫描记录被泄漏

有 2000 台医疗服务器在无身份验证的状态下暴露在互联网中，这些服务器上的 4500 万张 X 射线图像和其他医学扫描图像被泄漏。泄漏的数据包括患者的姓名、出生日期、地址、身高、体重、个人健康信息等。研究人员称，不仅敏感的个人信息被泄漏，而且恶意攻击者还在服务器上安装了恶意软件。

2020-12-15

Medtronic MyCareLink 的漏洞可让黑客接管植入心脏的设备

美敦力公司（Medtronic）的 MyCareLink Smart 25000 Patient Reader Reader 产品存在漏洞，攻击者可以利用该漏洞控制配对心脏的设备。MyCareLink Smart 25000 Patient Reader 是 Medtronic 设计的平台，可从患者植入的心脏设备中收集数据并将其传输到 Medtronic CareLink 网络。研究人员发现了三个漏洞，可以利用这些漏洞来修改或伪造从植入的心脏设备接收到的数据。这些漏洞还可能使远程攻击者能够控制配对的心脏设备，并在 MCL 智能患者读取器上执行任意代码。

2020-12-17

SignSight 行动：针对东南亚认证机构的供应链攻击

在 Able Desktop 软件的供应链攻击发生几周之后，越南政府认证局（VGCA）的网站上就发生了另一起类似的攻击，攻击者修改了两个可以从该网站下载的软件安装程序，并添加了后门程序。ESET 的研究人员于 2020 年 12 月上旬发现了这种新的供应链攻击，并通知了受感染的组织和 VNCERT。VGCA 表示，他们已经意识到了这次攻击，并通知了下载该木马软件的用户。

2020-12-17

黑客使用移动模拟器窃取数百万美元

IBM Trusteer 报告说，一个黑客组织正在使用移动模拟器来欺骗银行客户的移动设备，并从美国和欧洲的银行中窃取了数百万美元。IBM Security 的执行安全顾问 Limor Kessem 说，尽管已经通知了受到黑客攻击的银行，但第二波攻击可能已经开始。开发人员通常使用移动模拟器来测试各种设备类型上的应用程序和功能。攻击者使用了 20 个移动模拟器，模拟了 1.6 万部设备，并从中账户中窃取资金。

2020-12-17

安装了 500 万次的 WordPress 插件存在严重漏洞

WordPress 插件团队披露了一个严重的文件上传漏洞，并发布了一个补丁。易受攻击的插件 Contact Form 7 被安装了超过 500 万次，建议使用该插件的 WordPress 用户立即更新。Contact Form 7 插件中存在一处任意文件上传漏洞，攻击者可以利用该漏洞在上传文件时绕过 Contact Form 7 的文件名保护措施。

2020-12-20

Symrise 在 Clop 勒索软件攻击后停止了生产

2020 年 12 月，Symrise 遭受了一次 Clop 勒索软件攻击，据称攻击者窃取了 500GB 的未加密文件，并加密了近 1000 台设备。Symrise 是全球 30000 多个产品中使用的香料和香料的主要供应商，包括雀巢、可口可乐和联合利华的产品。2019 年，Symrise 实现了 34 亿欧元的收入，员工超过 10000 人。

360-CERT
COMPUTER EMERGENCY READINESS TEAM

安全事件分析报告

2020下半年

联系我们

电话：010-52448119
邮箱：g-cert-report@360.cn
官网：https://cert.360.cn