国内外云计算+安全动态报告

2019 年第 2 期

启明星辰云计算安全事业部

目录

本期云安全动态内容摘要

云厂商方面，AWS 增加多项功能支持，包括 AWS Batch 现在支持 Amazon EC2 A1 实例、Amazon ECS 现在对 GPU 激活的 EC2 实例提供增强的支持、AWS Site-to-Site VPN 现在支持 IKEv2、AWS Well-Architected Tool 支持对本地和混合云工作负载的架构审核、AWS Elemental MediaConvert 增加对视频旋转和广告标记插入的支持以及 Amazon GuardDuty 新增三种威胁检测，同时 AWS IoT Device Defender 现在提供统计异常检测和数据可视化功能；VMware 达成协议收购技术合作伙伴 AetherPal；Google 宣布收购云计算公司 Alooma-智东西，谷歌云市场新增加密货币 Ontology(ONT)的开发平台；阿里云年营收首次突破 200 亿元，成亚洲最大云服务公司；腾讯云游戏平台“腾讯即玩”公布 适用于 PC、手机，腾讯云三大项目落户江北；华为云宣布新加坡大区正式开服。

开源云方面，EasyStack 与 Kyligence 联合发布企业云数据仓库解决方案。

云安全厂商方面，全国政协委员、启明星辰集团首席执行官严望佳受邀参加 2019 年春节团拜会、启明星辰漏扫产品火速支持 Adobe ColdFusion 反序列化漏洞扫描、 启明星辰泰合产品为用户信息安全提供全方位保障、启明星辰顺利完成四川甘孜州道孚县学生体检助学项目；深信服 EDR 获 IT168 年度产品创新奖；山石网科获得《信息安全产品指南》颁发的安全产品及解决方案“2019 年全球卓越奖”金奖；田溯宁等全球 40 位商业领袖支持《数字宣言》；绿盟科技 Cloud-in-a-box 获得“2019 年全球卓越奖”；安恒信息入选“大数据网络安全态势感知及职能防控技术国家地方联合工程研究中心”依托单位；360 企业安全发布《政企终端安全态势分析月度报告（2019.1）》；阿曼数据园选择了 Fortinet

的 SD-WAN 服务来增强其托管安全服务组合。

容器动态方面，RunC 曝出容器逃逸漏洞，允许恶意人士对主机系统进行 root 访问，影响范围甚广；Docker 宣布企业版支持 Windows Server 2019；Linkerd 2.2 发布，引入自动请求重试，以及支持自动注入 linksd 到 pod。

安全新技术方面， 政府发力网络安全，越南网络安全新法生效责令互联网公司删除“有毒”内容，《网络空间安全工程技术人才培养体系指南（1.0 版）》现可下载，四部委联合开展“App 违法违规收集使用个人信息专项治理”；多家厂商推出新安全防御能力，微软推出全新的 Microsoft 365 安全性和合规性软件包，Adobe 修复了 Experience Manager 中可能导致信息泄露的漏洞；同时，NSA 宣布开源 GHIDRA 逆向工程工具，USB-C 接口将可加入认证协定，对抗恶意 USB 设备。

网络安全投融资方面，分别发生 1 起收购和 3 起融资事件。全球领导安全厂商赛门铁克公司收购云安全接入公司 Luminate，收购价未公开。融资方面，自适应安全服务平台厂商 Illumio 以 6500 万美元的 E 轮融资拔得头筹，边界安全服务公司 vArmour 以 4400 万美元的 E 轮融资位列第二，安全威胁防护公司 Perimeterx 则以 4300 万美元的 C 轮融资排名第三。

2019 年 2 月 27 日

云计算安全事业部

国内外云+安全动态报告

一、 云厂商动态

1. AWS 云动态

1.1 AWS Batch 现在支持 Amazon EC2 A1 实例

2 月 4 日消息，用户现在可以将 AWS Batch 与 Amazon EC2 A1 和 G3s 实例上运行的工作负载一起使用。AWS Batch 让开发人员、科学家和工程师能够轻松高效地在 AWS 上运行成千上万个批处理计算作业。根据提交的批处理作业量和特定资源需求，AWS Batch 可动态预置计算资源（如 CPU 或内存优化实例）数量和类型。

AWS Batch 现在支持 Amazon EC2 A1 实例，这可以显著节省成本，非常适合广泛的 Arm 生态系统支持的横向扩展和基于 Arm 的工作负载，此外，AWS Batch 还借助完全托管服务的便利，允许客户低成本运行批处理作业。A1 实例可为客户工作负载节约成本，这些工作负载可运行 Arm 指令并适应可用的 A1 内存占用。

AWS Batch 现在还支持 G3s 实例，通过 Batch 的托管扩展和调度服务运行渲染工作负载时，为客户提供了额外的灵活性。G3s 实例非常适合渲染视觉效果 (VFX) 和虚拟工作站的工作负载，用于设计与工程应用程序。

1.2 Amazon ECS 现在对 GPU 激活的 EC2 实例提供增强的支持

2 月 4 日，Amazon Elastic Container Service (ECS) 宣布对 EC2 GPU 实例上运行的机器学习和高性能计算应用提供增强的支持。ECS 任务定义现可允许用户指定多个 GPU 分配至具体的容器，ECS 将相应地标定实现工作量隔离和最优性能。

在 ECS 上运用 GPU 之前，用户必须先自定义配置 AMI，使用自定义 vCPU 布局逻辑作为代理，以尝试将物理 GPU 分配至特定容器。此外，用户不能执行任何标定或隔离。现在，用户可以使用具有 p2 和 p3 实例的经 ECS GPU 优化的 AMI，通过预先配置的 Nvidia 内核驱动程序、适当的 Docker GPU 运行时间以及 CUDA 默认版本而准备就绪。任务定义现允许用户指定多个 GPU 分配至特定容器，ECS 将其用作调度机制。由于用户的容器位于这些实例上，因此 ECS 将物理 GPU 标定至所需容器，以实现工作负载隔离和最佳性能。

1.3 AWS Site-to-Site VPN 现在支持 IKEv2

2 月 6 日，AWS Site-to-Site VPN 开始支持用于通道设置的 Internet Key Exchange 版本 2 (IKEv2)。新的 VPN 连接将能够使用 IKEv2 或 IKEv1 来协商 VPN 会话。这使得客户能够使用更新更强的协议来建立他们的 VPN。

为了能够立即使用此功能，用户需要创建一个新的 VPN 连接。通过更新客户网关设备的配置，用户可以控制要使用的 IKE 版本，并且 AWS 侧终端节点将使用相同的协议协商会话。此功能不可用于 AWS Classic VPN。

1.4 Amazon GuardDuty 新增三种威胁检测

2 月 8 日，Amazon GuardDuty 新增了三种威胁检测。其中两种是新的渗透测试检测，第三种是策略违规检测。 这三种新检测代表了不断增长的完全托管威胁检测库中的最新版本，可供在其 AWS 账户中启用 Amazon GuardDuty 的客户使用。

如果任何运行 Parrot Linux 或 Pentoo Linux 的计算机使用用户的 AWS 凭证进行 API 调用，与渗透测试相关的两种新检测会提醒您。这些新检测扩展了现有的 Kali Linux 检测，现在也涵盖了 Parrot Linux 和 Pentoo Linux。虽然这些工具有合法用途，但获取被盗帐户凭证的人也可能用其来实施恶意行为。这些新发现类型是：PenTest:IAMUser/ParrotLinux 和 PenTest:IAMUser/PentooLinux。

Amazon GuardDuty 还添加了一个新策略违规检测，它会提醒用户使用 AWS 账户根凭证的所有请求。当 AWS 根账户凭证被用于向 AWS 服务发出编程请求或登录 AWS 管理控制台时，这个新的策略违规检测会通知您。避免使用根凭证访问 AWS 服务是强烈建议的最佳安全实践。这个新发现类型是：Policy:IAMUser/RootCredentialUsage。

一旦启用后，Amazon GuardDuty 可持续监控恶意或未经授权的行为，帮助保护用户的 AWS 资源，包括您的 AWS 账户和访问密钥。GuardDuty 可识别异常或未经授权的活动，例如在从未使用过的地区进行加密货币挖矿或基础设施部署。当检测到威胁时，用户会收到 GuardDuty 安全发现的警报，它提供了观察到的情况和所涉及资源的详细信息。在威胁情报分析和机器学习的支持下，GuardDuty 不断改进，以帮助保护用户的 AWS 环境安全。

1.5 AWS Well-Architected Tool 支持对本地和混合云工作负载的架构审核

2 月 19 日消息，现在可以使用 AWS Well-Architected Tool 对混合云工作负载以及完全在本地部署的工作负载执行架构审核。

在定义工作负载时，可以选择部署工作负载的 AWS 和非 AWS 区域。这使用户能够记录工作负载是完全在 AWS 上部署、部分在 AWS 上部署还是完全在本地运行。然后，用户可以像之前一样继续使用 Well-Architected 审核。

1.6 AWS IoT Device Defender 现在提供统计异常检测和数据可视化功能

2 月 19 日消息，AWS IoT Device Defender 是一项完全托管的服务，可帮助用户保护互联设备的安全。使用 AWS IoT Device Defender，用户可以持续监控各个设备和 AWS IoT Core 的安全指标，验证它们的行为是否偏离了用户为每台设备所定义的相应行为。每当设备违反自定义的行为时用户都会收到警报，以便采取措施来解决问题。

自今日起，可以使用统计异常检测，并在设备不在基于百分位的阈值内时收到警报。例如，当设备不在队列行为的第 90 个百分位内时，用户会收到警报。用户还可以配置应触发警报的每台设备的连续违规次数。

此外，AWS IoT Device Defender 现在提供了一种简单方法，即使在设备没有违反自定义的行为时也能在 AWS 管理控制台中可视化所有设备的安全指标。提高安全指标和相关统计信息（如百分位级别）的可见性意味着，可以更快速地调查行为违规并查看历史设备行为和警报。

1.7 AWS Elemental MediaConvert 增加对视频旋转和广告标记插入的支持

2 月 21 日，AWS Elemental MediaConvert 开始支持视频旋转和广告标记插入。使用 MediaConvert，用户可以基于输入的元数据自动旋转视频，也可以通过指定旋转值手动旋转视频。通过将视频旋转到所需的方向，可以对移动电话等设备上创建的视频进行编码。

此外，即使输入视频不包含 SCTE-35 标记，也可以在输出中指定广告插入点。为此，用户可以向 MediaConvert 作业设置中添加事件信号和管理 (ESAM) XML 文档。这使用户能够在不中断的情况下通过插入广告或强制执行内容限制来更好地将 VOD 资产货币化。

AWS Elemental MediaConvert 让具有任何规模内容库的视频提供商能够轻松可靠地对点播内容进行转码，用于广播和多屏播放。该服务可独立运行，也可作为 AWS Elemental Media Services 的一部分运行，AWS Elemental Media Services 是一系列服务，构成了基于云的工作流的基础，提供传输、创建、打包和交付视频所需的各种功能。

2. VMWare 云动态

2.1 VMware 达成协议收购技术合作伙伴 AetherPal

2 月 18 日消息，VMware 通过收购合作伙伴 AetherPal 扩大其产品组合，AetherPal 开发的软件可帮助企业支持员工端点和“物联网”设备。

VMware 最终用户计算副总裁 Shankar Iyer 表示，这次未披露条款的收购将为 VMware 的 Workspace One 平台提供支持。Workspace One 提供了一系列用于管理组织员工在其工作中使用应用和设备的工具。

位于美国新泽西州的 AetherPal 带来的服务可以让管理员远程维护这些设备。这款名为 Remote Support 的产品可以帮助用户快速利用配置文件和其他所需的来解决故障端点问题。如果无法简单地解决用户端的问题，那么管理员可以远程登录设备进行自行修复。

AetherPal 的软件在全球超过 4500 万个端点上运行。企业在各种类型的设备上使用 Remote Support，包括员工电话、仓库用的手持扫描仪、POS 机甚至某些类型的医疗设备。

3. GOOGLE 云动态

3.1 Google 宣布收购云计算公司 Alooma - 智东西

2 月 20 日消息，美国时间 2 月 19 日，Google 官方声明收购云计算公司 Alooma 。据了解，Alooma 成立于 2013 年，是硅谷一家做实时数据管道的公司，可以集成任何数据源，如数据库、应用程序和任何 API。高管团队有 4 人，员工不到 50 人。据 Google 称，此次收购将帮助其为云客户提供更加简化的自动化迁移体验，提供一系列数据库服务；还将使 Google 能够更好地向其用户群推广其分析、安全、人工智能和机器学习工具。

3.2 谷歌云市场新增加密货币 Ontology(ONT)的开发平台

2 月 25 日消息，谷歌云平台市场已经新增了面向企业加密货币 Ontology (ONT)的 开发软件—— ont_dev_Platform。据悉，该软件是一套在 Ontology 区块链开发智能合同的工具。这使得该项目成为第一个在谷歌云市场上拥有开发平台的公链。据称，截至 2018 年 12 月，在亚马逊网络服务和微软 Azure 的市场上也能使用 Ontology 开发平台。

4. 微软 Azure 云动态

暂无消息。

5. 阿里云动态

5.1 阿里云年营收首次突破 200 亿元，成亚洲最大云服务公司

1 月 30 日，阿里巴巴发布 2019 财年 Q3 财报。财报显示，2018 自然年阿里云营收规模达到 213.6 亿元，首次突破 200 亿大关，上一年这一数字为 111.7 亿元。阿里云 4 年间增长了约 20 倍，目前已成为亚洲最大的云服务公司。

财报显示，阿里云营收的强劲增长得益于大型企业的收入提升。据统计，40%的中国 500 强企业、近一半中国上市公司、80%中国科技类公司在使用阿里云，数字经济正在阿里云上得到快速发展。

同时，阿里云正在快速增强自己在企业数字化转型市场的技术优势。仅过去一个季度，阿里云就推出了 678 种产品和功能，主要集中在数据智能、AI 应用和企业解决方案相关方面。

就在财报发布的 5 天前，据彭博社报道，阿里巴巴集团副主席蔡崇信在一场香港会议上宣布：阿里巴巴云业务已在中国占据 50%的市场份额。此外，蔡崇信还表示，阿里巴巴将继续投资感兴趣的领域。

云计算一直是阿里对于未来的投资。过去 10 年间，阿里巴巴对阿里云累计投入超过 430 亿人民币。

阿里巴巴还在继续加码对云业务的战略投入。2 个月前，阿里巴巴宣布将阿里云升级为阿里云智能事业群，整合全集团技术团队，将集团中台和达摩院的技术力量与阿里云全面结合，目标是构建数字经济时代面向全社会基于云计算的智能化基础设施。

6. 腾讯云动态

6.1 腾讯云游戏平台“腾讯即玩”公布 适用于 PC、手机

MWC 大会上腾讯与英特尔联手，推出云游戏平台“腾讯即玩”。“腾讯即玩”借助云服务能力，在云端完成最耗费硬件资源和功能，从而让玩家摆脱硬件和平台的束缚，省去漫长的下载和等待时间，在不同联网的终端上都可以获得高品质的游戏大作体验。“腾讯即玩”

将适用于 PC 和智能手机，将在下个月的 GDC 上公布更多细节。

“腾讯即玩”云游戏平台在基于英特尔 酷睿 i7-8709G 处理器平台的 PC Farm 高密度解决方案上，构建整个云游戏的音视频采集/处理/编解码，控制采集/重现以及网络传输控制等能力。作为英特尔面向游戏、AR/VR、高清视频处理所打造的全新处理器平台，英特尔酷睿 i7-8709G 具备出色的运算性能，它与英特尔 MediaSDK 卓越的硬件编码性能相配合，为云游戏平台带去高效的游戏编解码和推流能力。以怪物猎人为例，在 1080p /50~60 FPS 画面品质时，操作延时已被大大压缩，显著改善了玩家的体验。

6.2 腾讯云三大项目落户江北

2 月 26 日，在宁波市江北区经济工作会议暨数字经济大会上，江北与腾讯云签署合作协议，双方牵手乘“云”而上，将在数字经济领域展开深度合作。

未来，腾讯云将在江北建设腾讯云启（宁波）基地、腾讯云万物互联工业物联网实验示范区、腾讯新工科实验室三大项目，分别在大数据、工业云平台、人才教育培训等方面用数字赋能，打造本地化智慧应用与解决方案。同时，根据合作协议，腾讯云将首批引进腾讯 30—50 名高新科技人才与专家，孵化 100 家以上物联网、大数据、人工智能领域的创新企业，培养 1000 名以上本地高新科技人才，助力数字经济在江北生根发芽开枝散叶。

腾讯云作为腾讯倾力打造的云计算品牌，在物联网、云计算、大数据、人工智能等领域具有较强技术优势和资源优势。

这次合作，腾讯方面提供人才和专家，还提供孵化创新企业的服务，把三大项目落户在江北，这是为何？江北在数字经济方面有扎实的产业基础，正快速发力智能终端制造、卫星导航、光学薄膜和产业互联网领域，双方合作互相依托一拍即合。

作为腾讯云全国首个落地运营项目，腾讯云启（宁波）基地以数字经济产业为运营方向，加大数据与产业的深入融合开发。而腾讯云万物互联工业物联网实验示范区将以落地江北的项目为依托，为数字经济发展提供最新的物联网、大数据、人工智能等技术和产品，促进物联网与宁波智能制造的深度融合。同时，在颇受关注的数字经济人才培养方面，双方将依托腾讯新工科实验室等产学研平台，根据企业需要，输出人工智能、云计算、大数据等课程，大力培养应用型人才。

7. 华为云动态

7.1 华为云宣布新加坡大区正式开服

2 月 20 日消息，华为云宣布新加坡大区正式开服，将立足新加坡面向亚太区提供全栈云平台及 AI 能力，新加坡大区是华为云资源规模最大的海外大区之一。

二、 开源云动态

1. Openstack 动态

暂无消息。

2. Easystack 动态

2.1 EasyStack 与 Kyligence 联合发布企业云数据仓库解决方案

2 月 24 日消息，易捷行云 EasyStack 与 Kyligence 共同为企业客户提供统一的云上大数据分析平台，支持自助式建模，无需编程，并与主流 BI 工具实现无缝集成，在企业客户关注的实施效率、安全控制、性能优化、自助式敏捷 BI、系统监控和管理等方面进行了全面创新和增强。

3. 99CLOUD（九州云）动态

暂无消息。

三、 云安全厂商动态

1. 启明星辰

1.1 全国政协委员、启明星辰集团首席执行官严望佳受邀参加 2019 年春节团拜会

中共中央、国务院 2 月 3 日上午在人民大会堂举行 2019 年春节团拜会。中共中央总书记、国家主席、中央军委主席习近平发表讲话，并代表党中央、国务院，向全国各族人民，向香港特别行政区同胞、澳门特别行政区同胞、台湾同胞和海外侨胞拜年。

党和国家领导人李克强、栗战书、汪洋、王沪宁、赵乐际、韩正、王岐山等出席团拜会，李克强主持。中共中央、全国人大常委会、国务院、最高人民法院、最高人民检察院、全国政协、中央军委领导同志和老同志出席了团拜会。参加团拜会的还有中央党政军群各部门及北京市主要负责同志，各民主党派中央、全国工商联负责人和无党派人士代表，离退休老同志代表，著名专家学者及首都各界人士代表，2000 多人欢聚一堂，全国政协委员、启明星辰信息技术集团股份有限公司首席执行官严望佳作为党外知名人士受邀参会，与会人员共迎新春。

1.2 启明星辰漏扫产品火速支持 Adobe ColdFusion 反序列化漏洞扫描

2019 年 2 月 12 日，Adobe 官方发布了 Adobe ColdFusion 的一个补丁更新，编号为 APSB19-10，修复了一处启明星辰 ADLab 发现并提交的反序列化漏洞。该漏洞危害程度非

常高，利用该漏洞攻击者可远程执行任意代码，漏洞编号为 CVE-2019-7091。启明星辰漏洞扫描产品团队在第一时间对这个漏洞进行了紧急响应。

漏洞影响范围：

ColdFusion 11 Update 15 及之前版本

ColdFusion 2016 Update 7 及之前版本

ColdFusion 2018 Update 1 及之前版本

漏洞检测：

启明星辰天镜脆弱性扫描与管理系统 V6.0 于 2019 年 2 月 15 日紧急发布针对该漏洞的升级包，支持对该漏洞进行检测，用户升级天镜漏扫产品漏洞库后即可对该漏洞进行扫描。6070 版本升级包为 607000204，升级包下载地址：

https://www.venustech.com.cn/article/type/1/146.html

漏洞修复建议：

方案一：

修改 gateway-config.xml 文件的配置，禁止 JavaBeanAdapter 的使用。

方案二：

升级最新补丁 APSB19-10：

https://helpx.adobe.com/security/products/coldfusion/apsb19-10.html。

Adobe ColdFusion 反序列化 RCE 漏洞分析相关链接：

https://mp.weixin.qq.com/s/8_D8xwXwgETItMmJRgp6XQ

1.3 启明星辰泰合品牌“绝不能让用户的信息安全流浪”

最近在火热上映一部华语科幻大片《流浪地球》，影片中有一个情节讲到，地球遭遇了全球发动机停摆的事件。这个事件刺痛了每一位安全从业人员的神经。 在用户的网络世界里，任何一个偶然事件，都可能上升为安全事件，影响业务连续性、安全生产，甚至威胁到生命。

启明星辰深知，在用户的安全观里，信息安全是一项体系化工程，更是一项保障性工程。所以，启明星辰泰合产品担负的使命是“绝不能让用户的信息安全流浪”。 从以下几个方面提供保障措施：

从产品化交付的角度

启明星辰泰合产品可以为用户提供成熟商用的安全工具和安全产品，让用户的系统安全

有保障，包括：CSA 态势感知平台、SOC 安全管理平台、SA 日志审计系统、AEM 资产管理系统、CVS 配置核查系统、NBA 流量异常分析系统、BSM 业务支撑安全、LAS 安全审计日志分析系统、云安全管理平台、流量异常检测 Detector 等。另外，还可以根据用户需求量身定制各类安全工具、高级分析工具、设备运维管理工具等，便于满足用户在追踪溯源、安全管理便利性上的需求。

从平台化管理的角度

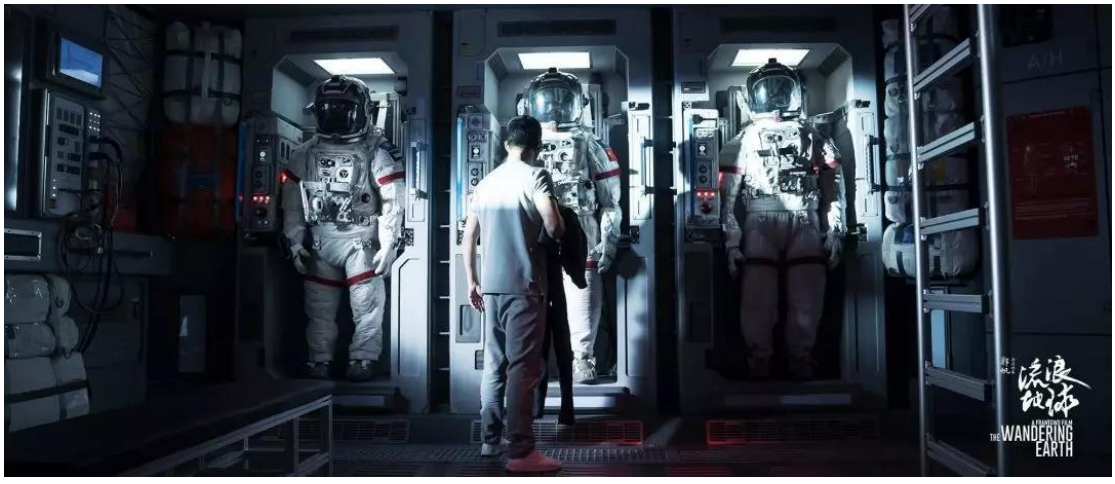
可为用户提供成套平台级解决方案，为用户赋能，为用户的体系化安全建设形成支撑，同时，提供安全信息与事件管理（SIEM）、安全管理（SOC）平台、大数据安全分析（BDSA）、专业安全运营（PSP）、未知威胁溯源（UTT）等体系化建设方面的解决方案级支撑。

从技术输出角度

可为用户提供各类最佳的新技术落地，如：自动范式化（AN）、机器学习（ML）、用户实体行为分析（UEBA）、深度关联分析（AA）、可视化展现（Visualization）、跨矩阵运算（Tran-Matrix Opt.）、知识图谱（KG）、快速交付（QD）、威胁狩猎（TH）等形成成果输出，帮助用户提升安全能力带来帮助。

从安全服务角度

可为用户提供一支专业的安全分析队伍的保障，它具备五大核心能力，即：安全分析能力 PAC、安全运营能力 PBC、态势监测能力 PCC、专家服务能力 PSC、应急响应能力 SRC。安全事件的深度分析服务、态势的集中监测服务、事件的应急响应服务、产品的专家服务等专业服务，同时，帮助用户进行日志采集与分析，安全威胁场景建模与有效性验证、攻击行为溯源取证、重点项目效果保障及安全事件应急响应等。



帮助用户梳理安全事件，进行精准分析，发现业务系统安全策略中存在的不足，为安全策略的完善提供依据，保障业务系统的安全与连续，制定应急通报和分级预警机制，闭环安

全态势，满足用户各个阶段的自适应安全的建设需求。

地球在流浪，安全不能忘。启明星辰泰合品牌的产品、平台、能力、服务，可让用户将日常安全管理工作无序变有序、复杂化简单，从单点防御提升为协同防御，从模糊管理提升为量化管理，从单一分析提升为多维分析，通过全面提升用户网络安全管理能力，不再让广大用户的信息安全“流浪”。启明星辰将持续努力，力争成为用户信息安全“一站式服务”的最佳选择。

1.4 启明星辰资助道孚县学生体检助学项目顺利完成

2019 年春节前，四川甘孜州道孚县学生体检助学项目顺利完成。此项公益活动是经中国西藏文化保护与发展协会指导，道孚县教育体育局和专业体质健康检测机构负责具体实施，由北京启明星辰慈善公益基金会全额捐助。本项公益活动的受助学生共有 5406 人，其中小学生 3363 人、初中生 2043 人。

党中央、国务院高度重视青少年体质健康工作。目前少数民族地区青少年体检工作可提升的空间较大，本次公益活动的顺利完成，是一次有益的探索，通过科学化、信息化的学生体质检测，有利于带动其他少数民族地区青少年体检工作的纵深发展。

北京启明星辰慈善公益基金会成立于 2012 年，是启明星辰集团独立捐资成立的慈善组织，宗旨是以信息网络技术为基础打造公益平台，募善款，救贫困，助教育，促和谐。

2. 深信服

2.1 深信服 EDR 获 IT168 年度产品创新奖

近日，深信服终端检测响应平台 EDR 荣获国内知名 IT 业务资讯网站——IT168 评选的“2018 年度产品创新奖”。

传统终端安全已无法适应当下的安全攻击形势。

1）基于规则的杀毒工具无法有效抵御新型病毒

从 2017 年 5 月大规模爆发勒索病毒开始，2018 年勒索病毒同样层出不穷，且病毒变种多，扩散方式上不仅集成了永恒之蓝系列的利用工具而且增加了多种漏洞利用工具。此外，各式各样的挖矿病毒在 2018 年也屡见不鲜，很多主机感染之后病毒不断复制，普通工具无法隔离、删除，严重影响正常业务。

然而传统杀毒软件因单点工作模式、规则库更新的延时性等限制，在应对勒索和挖矿等新型恶意软件的时候呈现被动、后知后觉等特点，对于频发的未知风险的感知和捕获都力不从心。

2）终端主机的安全需求不局限于病毒查杀

首先，企业中往往终端资产的数量庞大，且用户的终端不止一种类型，不同的操作系统、不同的设备类型、不同的 Web 应用等，如果这些都需要分别管理将会是一项很耗时的工作，而且面对安全事件很难快速、全面的响应。统一管控成为热点需求。

此外，《网络安全法》明确提出，国家实行网络安全等级保护制度。终端安全产品帮助主机满足等保 2.0 合规要求成为用户的关键需求之一。

深信服 EDR 帮助用户构建轻量级、智能化、响应快的下一代终端安全系统。

深信服终端检测响应平台 EDR，围绕终端资产安全生命周期，通过预防、防御、检测、响应赋予终端更为细致的隔离策略、更为精准的查杀能力、更为持续的检测能力、更为快速的处置能力。在应对高级威胁的同时，通过云网端联动协同、威胁情报共享、多层级响应机制，帮助用户快速处置终端安全问题，构建轻量级、智能化、响应快的下一代终端安全系统

1）智能检测，洞察威胁本质

深信服 EDR 通过人工智能持续学习、自我进化能力实现无特征检测，真正洞察威胁本质，能够更有效的鉴定未知病毒。利用深度学习训练数千维度的算法模型，多维度的检测技术，应用高检出率和低误报率的算法模型，并使用线上海量大数据的运营分析，用特征训练不断完善算法。与此同时，辅以信誉库加上行为分析、基因特征等技术，构建完善的防御体

系，全面预防、有效检测。

2）迅捷灵动处置，及时响应威胁

一方面，深信服 EDR 可根据检测命中的威胁内容，进行迅捷处置。区别于传统终端安全的文件隔离方式，深信服 EDR 提供基于文件、机器、群组等全面处置手段。隔离响应手段包括：终端主机隔离、业务组隔离、文件信任、文件隔离、文件删除、文件恢复等。另一方面，深信服 EDR 通过与深信服下一代防火墙、安全感知平台等安全设备智慧协同、自动处置，形成立体防护能力，帮助用户快速封堵威胁，缩短威胁在用户环境的发现和处置时间。

3）一体化管理，终端资产全面防护

深信服EDR采用一体化统一管理方式，全面兼容不同终端/服务器形态、操作系统类型，全类型资产策略一体化，并辅以多层次威胁检测、Web 后门检测、僵尸网络检测、入侵攻击检测、基线合规检测、热点事件 IOC 检测等手段，确保终端具备更为全面的防护能力，全面满足在等保 2.0 标准中针对主机防病毒\补丁、漏洞管理\集中管控等安全控制点的合规要求。助力用户进行等保二级、三级建设，也使得每一台终端上的资产信息更加清晰，便于管理。

深信服全新推出的终端检测响应平台 EDR 融合了传统的 EPP 和新兴的 EDR 功能，形成基于终端资产为主的预防、防御、检测、响应的自适应、可视化、持续闭环的体系。 目前，深信服 EDR 已经赢得各级政府单位、医院、教育行业用户、能源行业用户和大型企业等众多用户的认可，部署端点超过 20W+。

3. 山石网科

3.1 山石网科获《信息安全产品指南》颁发的“2019 年全球卓越奖”金奖

山石网科近日宣布，其数据中心安全防护平台 X10800 获得《信息安全产品指南》颁发的安全产品及解决方案“2019 年全球卓越奖”金奖，同时山石网科更被评为“年度最佳综合网络安全厂商。

山石网科数据中心安全防护平台 X10800，是应用在数据中心边界，应对大流量、高可靠场景的数据中心级安全防护产品，具备电信级高可靠性的保障、强大的网络适应性、创新的分布式架构、虚拟化防护技术以及面向未来的平台化设计。X10800 整机吞吐性能目前最大 1Tbps，新建连接速率 1000 万，并发连接数 4.8 亿，支持高达 400Gbps 的 IPS 防护性能，

同时全面支持 IPv6。

X10800 可广泛部署于运营商、大型企业和政府机构的高速互联网出口及数据中心等场景，帮助用户应对最新安全挑战。

4. 亚信

4.1 田溯宁等全球 40 位商业领袖支持《数字宣言》

近日，GSMA（全球移动通信系统协会）在达沃斯世界经济论坛发表了《数字宣言》，其阐述了数字时代道德行为主要原则，旨在帮企业向数字环境下的公民、行业和政府提供最重要的信息。该宣言获得了来自亚信集团、中国移动、中国电信、德国电信、巴帝电信、爱立信、三星、西班牙电信、沃达丰、小米、Verizon 等 40 余家企业相关领导人的支持。

当下，数字浪潮汹涌而至，企业和消费者都经历着前所未有的变化，预计到 2022 年，全球 60%的 GDP 将经由数字化活动产生，而 5G 将大大加剧这一趋势。与此同时，消费者对数字服务的需求和期望不断提高，被服务者（消费者）与服务者（一般指企业）之间的信任关系也在经受着考验。

《数字宣言》呼吁企业：尊重公民隐私，安全、透明地处理个人数据；致力减少网络威胁；助力打击网络骚扰；营造人人都能参与的数字经济环境，让互联网成为开放平台，不断贡献创新推动力。

亚信集团董事长田溯宁：“从实现数字化转型到建立更安全的网络空间，从初创企业的投资到全球化合作，我们分享了这一愿景并期待数字化的未来，这将是一个漫长而又美好的旅程。”

据悉，全球移动用户数超 50 亿，预计到 2025 年将增至近 60 亿。GSMA 称，随着智能互联时代的到来，5G 和物联网将实现无限连接，结合大数据和人工智能的强大支持，行业转型也将不断加剧。通过《数字宣言》，商业领袖们展现了紧跟技术变革步伐、勇于担当的企业家精神。

5. 绿盟

5.1 绿盟科技 Cloud-in-a-box 获得“2019 年全球卓越奖”

近日，绿盟科技 Cloud-in-a-box 获得硅谷通信《信息安全产品指南》颁发的“2019 年全球卓越奖”。硅谷通信作为国际知名信息安全研究和咨询指导机构，其发布的《信息安全产

品指南》在帮助终端用户了解可选解决方案、保护其数字资源安全方面具有权威的指导作用。

6. 安恒

6.1 安恒信息入列国家级科研载体创新平台

近日，国家发改委正式发布“2018 年度国家地方联合工程研究中心”确定名单。浙江省共入选三家单位，安恒信息位列其中，成为“大数据网络安全态势感知及职能防控技术国家地方联合工程研究中心”的依托单位。

大数据网络安全态势感知及智能防控技术国家地方联合工程研究中心的战略定位是以“科技成果产业化、运作机制企业化、发展方向市场化”为指导思想，依托国家战略为核心，针对网络信息安全与智能防控等国际性难题，在公共互联网、视频监控专网、工业控制系统等相关领域中开展技术突破及示范应用，解决关系国计民生的信息安全领域的重点问题。依托企业技术力量与国家支持，围绕互联网、物联网、工控系统三大领域中的重要安全问题展开技术攻坚，特别是将人工智能方法引入信息安全领域，重点突破基于智能算法的未知威胁检测和脆弱性发现的关键技术，在相关领域中开展示范应用，形成引领浙江经济发展新兴龙头产业和可持续健康发展的增长点。

工程研究中心建设期 3 年，将搭建具有一定国际影响力的大数据网络安全态势感知及智能防控技术创新及成果转化服务平台，组建培养领域最具规模、实力的创新和服务团队，建立一批信息安全智能防控领域的新技术试点工程或示范工程，从而进一步提高国家在大数据态势感知、智能防控技术领域的国际地位。

7. 360

7.1 360 企业安全发布《政企终端安全态势分析月度报告（2019.1）》

《2019 年 1 月政企终端安全态势分析报告》是 360 终端安全实验室每月发布的针对政企网络终端的安全态势分析报告。报告数据来自 360 企业安全公有云安全监测数据，报告分为全病毒篇、勒索病毒篇、漏洞利用篇、蠕虫病毒篇四个主要部分，以每日感染病毒的终端为基本研究单位。通过对政企终端感染病毒情况的分析，希望可以帮助客户更清晰地看见风险态势，为安全决策提供更有力的参考依据。

病毒攻击政企整体分析摘要

360 终端安全实验室监测数据显示，2019 年 1 月，政企单位被病毒攻击的事件数量比

2018 年 12 月减少了 4.3%，被病毒攻击的政企终端的累计数量比 12 月减少了 4.3%，被病毒攻击的政企单位的绝对数量比 12 月减少了 11.3%。

勒索病毒攻击政企分析摘要

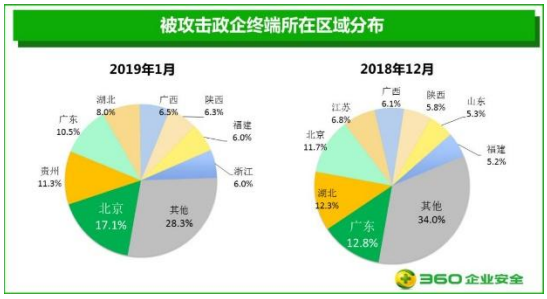
2019 年 1 月，政企单位被勒索病毒攻击的事件数量比 2018 年 12 月增加了 11.5%，被勒索病毒攻击的政企终端的累计数量比 12 月减少了 54.2%，被勒索病毒攻击的政企单位的绝对数量比 12 月减少了 4.8%。

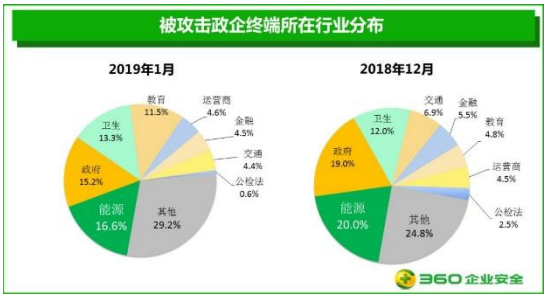
漏洞利用攻击政企分析摘要

2019 年 1 月，政企单位被漏洞利用攻击的事件数量比 2018 年 12 月减少了 8.3%，被漏洞利用攻击的政企终端的累计数量比 12 月减少了 36.4%，被漏洞利用攻击的政企单位的绝对数量比 12 月减少了 15.8%。

蠕虫病毒攻击政企分析摘要

2019 年 1 月，政企单位被蠕虫病毒攻击的事件数量比 2018 年 12 月减少了 4.6%，被蠕虫病毒攻击的政企终端的累计数量比 12 月增加了 5.8 %，被蠕虫病毒攻击的政企单位的绝对数量比 12 月减少了 9.7%。





8. 安天

暂无消息。

9. Fortinet

9.1 阿曼云选择 Fortinet 的 SD-WAN 服务来增强其托管安全服务组合

近日，阿曼云和托管服务提供商阿曼数据园选择了 Fortinet 的 SD-WAN 服务来增强其托管安全服务组合，这也是阿曼数据园作为托管企业服务组合所托管的第一个 SD-WAN。

此举也进一步增进了阿曼数据园和 Fortinet 7 年的合作伙伴关系，其中阿曼已将 Fortinet 的云和本地安全性出售给其企业客户，该服务提供商也将利用 Fortinet 的下一代防

火墙（NGFW）功能，包括入侵防御系统（IPS）、网络过滤、反恶意软件。

根据 Fortinet 网络安全产品高级主管 Nirav Shah 的说法，阿曼数据园选择 Fortinet 作为其第一个 SD-WAN，这主要归功于安全和 SD-WAN 功能相结合的服务。“它是现有 Fortinet 基础设施的简单附件，使得阿曼数据园可以轻松地为使用 Fortinet 的 NGFW CPE 的许多现有客户启用 SD-WAN 功能。”

Fortinet 于 2018 年 7 月推出了 SD-WAN。该技术将分支机构的多个产品整合到一个设备中，包括路由，WAN 优化，SD-WAN 和安全组件，组合设备可以在其防火墙硬件或虚拟机（VM）上运行。通过将 Fortinet SD-WAN 作为托管服务提供，阿曼数据园的客户可以利用单一服务提供自动 WAN 路径控制，安全性和多宽带支持。

10. Checkpoint

暂无消息。

四、 容器技术及安全动态

1. RunC 曝出容器逃逸漏洞

近期 RunC 曝出容器逃逸漏洞，允许恶意人士对主机系统进行 root 访问，影响范围甚广。

RunC 是一套位于 Docker、CRI-O、containerd 以及 Kubernetes 等基础设施与引擎之下的底层容器运行时。广泛用于生成及运行容器的 CLI 工具，当中曝出严重安全漏洞，其可能被用于破坏高权限 runC 容器内的 runC 主机二进制文件，这意味着攻击者将能够立足底层主机系统获取 root 访问权限。

此安全漏洞编号：CVE-2019-5736，由研究人员 Adam Iwaniuk 与 Borys Poplawski 向 runC 项目的维护者们上报。该安全漏洞允许恶意容器（在最低用户交互等级下）覆盖主机 runC 二进制文件，这意味着攻击者将借此获得在主机上以 root 层级执行代码的权限。具体来讲，攻击者能够利用一套其可以控制的镜像创建新的容器，或者是向其能够访问的现有容器之内添加 docker exec 文件。在这类情况下的任意容器当中，该攻击者都将能够通过当前用户交互等级以 root 权限运行任意命令（无论命令本身是否由攻击者所控制）。

目前面向 runC 以及 LXC 的修复补丁都已经正式发布。

红帽公司警告称，用户需要更新“docker”与“runc”软件包。另外，Debian 与 Ubuntu

也在着手发布修复补丁。

Docker v18.06.2 和 v18.09.2 版本已经顺利修复了这一漏洞。

2. Docker 宣布企业版支持 Windows Server 2019

Docker 宣布在其企业版平台（Docker Enterprise）中支持 Windows Server 2019 长期支持频道（Long Term Servicing Channel，LTSC）和 Server 1809 半年频道（Semi-Annual Channel，SAC）。Windows Server 2019 从之前的 SAC 频道发布到 LTSC 频道后，带来了一系列提升。包括入口路由、虚拟 IP 服务发现和命名管道挂载。

3. Linkerd 2.2 发布，引入自动请求重试，支持自动注入

2 月 12 日，Linkerd 2.2 版本正式发布。这个版本主要引入了自动请求重试和超时，以及完全支持（非实验）的自动注入功能。它添加了一些新的 CLI 命令（包括 logs 和 endpoints），为 Linkerd 的控制平面提供诊断可见性。最后，它带来了两个令人兴奋的实验性功能：加密安全的客户端标识头和 CNI 插件，该插件可以避免在部署时需要的 NET_ADMIN 内核功能。

其中，自动重试失败的请求，在应用程序出现部分故障时提高整体成功率。基于 2.1 版本中引入的服务配置文件模型，Linkerd 允许你为每个路由的基础配置此行为。当然，控制何时可以进行重试是安全使用重试的关键组成部分。Linkerd 2.2 允许你标记哪些路由是幂等（isRetryable），限制重试单个请求所花费的最长时间（timeout），以及配置可以重试的总体请求的百分比（retryBudget）。这些参数可以确保重试发生的安全性，并且不会在已经发生故障的系统中加重问题。

自动注入是一个完全支持（非实验）的功能。自动注入功能允许 Kubernetes 集群在部署时自动添加（“注入”）Linkerd 的数据平面代理到应用程序 pods。将代理注入从客户端移植到集群上有助于确保所有 pods 统一地运行代理，无论它们如何部署。

五、 安全新产品及技术

1. CNNVD 关于微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，包括 Microsoft Office 安全功能绕过漏洞（CNNVD-201902-356、CVE-2019-0540）、Windows 脚本引擎内存损坏漏洞（CNNVD-201902-405、CVE-2019-0590）、Microsoft SharePoint 远程执行代码漏洞（CNNVD-201902-349、CVE-2019-0594）等多个漏洞。

成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，采取修补措施。

2. 小米 M365 电动滑板车面临黑客攻击和远程控制风险

来自 Zimperium 的研究人员日前透露，小米 M365 电动滑板车存在严重设计缺陷，黑客能够在 100 米的距离内接管其刹车和加速功能。

该漏洞源于 M365 电动滑板车与其相应 APP 之间的不安全蓝牙通信链路，这也是物联网（IoT）设备经常面临的问题。

小米 M365 电动滑板车的配套 APP 可以让用户通过蓝牙使用多种功能，例如防盗、巡航控制、Eco 模式切换和车载固件更新。按照设计，使用 APP 执行功能受密码保护，用户更改该密码。但实际上 Zimperium 的研究人员发现：密码只在应用程序端进行验证，但小米电动滑板车本身不会跟踪身份验证状态，也就是说在认证过程中可以绕过密码保护，无需密码即可执行所有命令。

如果别有用心的人掌握了这个漏洞，车主的人身安全就会面临很大的风险。研究人员制作了一个 Android 应用程序，能够扫描附近的小米 M365 电动滑板车并发起攻击，可实现：

- 拒绝服务攻击 – 锁定任意小米 M365 电动滑板车；
- 部署恶意软件 – 安装能够完全控制电动滑板车的恶意固件；
- 发起针对性攻击 – 控制电动滑板车突然制动或加速，伤害用户的人身安全。

Zimperium 研究人员已经掌握用于安装能够加速电动滑板车的恶意固件的 PoC，但考虑到用户的人身安全不会放出。不过， Zimperium 开源了该电动车的锁定应用，以引起小米

的重视。

3. 京东金融就侵犯隐私致歉：安卓版有问题，属错误开发

近日有用户在微博上发布视频称京东金融 App 会保存用户的截屏图片在自己的文件夹内，因此质疑京东金融 App 侵犯用户隐私。京东金融方面昨日称，图片缓存为方便客户投诉或建议使用，不会上传京东金融后台，不会未经允许收集用户隐私。

今日，京东金融客服官方微博再发声明致歉，称排查后，发现安卓系统上的 App5.0.5 以后的版本存在该问题，并已定位问题且下线修复。京东金融在致歉信中称，2018 年 12 月，京东金融 App5.0.5 版本上线了客服截屏反馈功能，此功能的目的是，用户对京东金融 App 进行截屏时，本人可将京东金融 App 截屏发送给在线客服人员，以提高与在线客服的沟通效率。

京东金融 App 在该项功能上存在技术问题，具体为用户将京东金融 App 切换到后台后，该功能继续运行，继续接收新增图片通知（包括截屏和照片等）并在手机本地缓存，而原功能设计需求是切换后自动停止该功能，属于需求错误开发。

声明中也补充道，此次技术问题涉及的新增缓存图片仅存在用户手机本地，京东金融 App 坚决没有对用户照片和截屏进行私自上传，也对该功能进行了全面排查，并未发现任何一张未经授权的图片被收集。

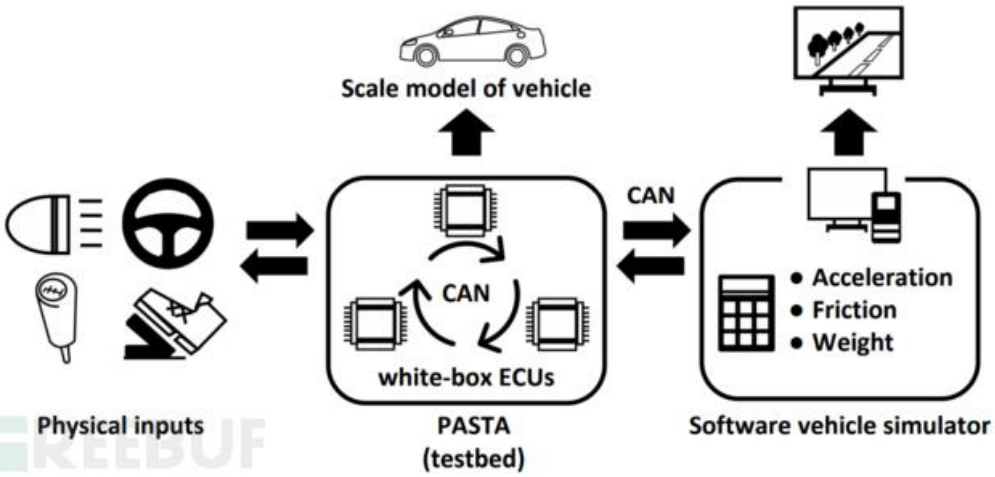
4. 国家计算机病毒应急处理中心公布十款违法移动应用

国家计算机病毒应急处理中心近期通过互联网监测发现，十款违法有害移动应用存在于移动应用发布平台中，其主要危害涉及隐私窃取、诱骗欺诈、流氓行为和赌博四类。其中，《财急送移动版》（版本 1.1.1.22）、《Fotoplace 足记分享》（版本 6.4.2）、《Flurv》（版本 5.3.4）、《电视之家》（版本 6.2.5）、《CybrFM 创意库》/《私密记事》（版本 7.7.9）等被点名。

5. 丰田便携式汽车安全测试台即将上线 GitHub

丰田 PASTA 首次进入大众视野是在去年 BLACK HAT EUROPE 2018 大会上，近日丰田宣布最早在下个月通过 GitHub 提供 PASTA 工具。

丰田 PASTA，即丰田官方便携式汽车安全测试台，由丰田信息技术中心的 Takuya Yoshida 和 Tsuyoshi Toyama 开发，是专为汽车黑客设计的开源测试平台，旨在帮助专家测试现代汽车的网络安全功能。



即将提供的开源套件包含用于汽车测试的 CAN（控制区域网络）ID 图、ECU（引擎控制单元）程序代码和 ECU 电路图，此外与 PASTA 配套的驾驶模拟器也在开源计划中。

6. 万事达联合 GCA 推出小型企业网络安全工具包

中小型企业与大型企业的网络安全问题大多相同，只是小型企业往往没有用于处理这些问题的足够资源。万事达联合 GCA 推出小型企业网络安全工具包，帮助小型企业弥合这一鸿沟，使小公司能够在越来越危险的网络环境中保证自己的安全。

该工具包由全球网络联盟（GCA）和万事达卡联合倡议，旨在为小企业主提供基本可用的安全控制能力和指导。万事达高级副总裁 Alexander Niejelow 表示：”小型企业同样拥有大量信息，美国和英国的政府机构为企业提供了大量有关网络安全的信息。

7. 首个完整利用 WinRAR 漏洞传播的恶意样本出现

2019 年 2 月 20 日，安全厂商 checkpoint 披露了一个存在于 WinRAR 中用于 ace 文件解析的 DLL 模块中的绝对路径穿越漏洞，可导致远程代码执行。2019 年 2 月 22 日，在该漏洞被披露后短短一天多时间后，360 威胁情报中心便截获了首个利用 WinRAR 漏洞（CVE-2018-20250）传播木马程序的恶意 ACE 文件。该恶意压缩文件被命名为 ModifiedVersion3.rar，并通过邮件发送，当受害者在本地计算机上通过 WinRAR 解压该文件

后便会触发漏洞，漏洞利用成功后会将内置的木马程序写入到用户计算机的全局启动项目录中，任意用户重启系统都会执行该木马程序从而导致电脑被控制。

六、 网络安全投融资、收购事件

1. 收购

1.1 Symantec 完成对 Luminate Security 的收购

2 月 12 日，Symantec 完成对 Luminate Security 的收购，收购价未公开。赛门铁克公司是互联网安全技术的全球领导厂商，为企业、个人用户和服务供应商提供广泛的内容和网络安全软件及硬件的解决方案。Luminate 提供安全访问云™，能够快速设置并易于对混合云资源访问管理。

2. 投融资

2.1 vArmour 获 4400 万美元 E 轮融资

2 月 6 日，vArmour 从 AllegisCyber 和 NightDragon Security 处获得 4400 万美元的 E 轮融资。vArmour 是一家提供边界网络安全服务的技术公司，主要关注移动、虚拟化和云计算等方面。

2.2 Illumio 获 6500 万美元 E 轮融资

2 月 7 日， Illumio 从 J.P. Morgan Asset Management 处获得 6500 万美元的 E 轮融资。Illumio 是一个自适应安全服务平台，致力于提供安全资产管理和安全策略配置。 公司主要为企业提供数据中心和云服务的安全保护，而且业务开展也需要一定的基量，除了具象的网络安全保护外，Illumio 还可以为整个网络的运营情况作扫描。

2.3 PerimeterX 获 4300 万美元 C 轮融资

2 月 11 日， PerimeterX 从 PerimeterX 和其他 4 位投资者处获得 4300 万美元的 D 轮融资。Perimeterx 为互联网、云计算和移动互联网提供可扩展的、基于行为的安全威胁防护技术。公司的 Perimeterx BOT 安全卫士利用行为指纹识别技术，能准确地检测并保护网站遭受所有类型的自动攻击。旗下产品 PX Bot Defender 旨在检测并抵御“肉鸡”或非人为攻击，

包括倒票、欺诈、账户接管等。