国内外最新网络安全发展动态

2022 年 8 月 29 日

PART 1.国内

工信部：我国网络安全产业总规模突破 2000 亿元，将出台促数据安全产业发展政策

8 月 19 日，工业和信息化部举行“新时代工业和信息化发展”系列新闻发布会第二场，主题是“打通经济社会信息大动脉”。在发布会上，工业和信息化部网络安全管理局一级巡视员周少清表示，2021 年，我国网络安全产业总体规模突破 2000 亿元，“十三五”时期年均增长率达 15%，产业综合实力快速提升。目前我国正在布局建设北京、长沙、成渝三大国家网络安全产业园区，打造一批产业公共服务平台、创新示范中心，网络安全产业集聚式、规模化发展态势初步形成。周少清表示，将推动出台促进数据安全产业发展等政策文件，培育具有国际竞争力的数据安全领军企业、专精特新“小巨人”企业，强化关键核心技术攻关和应用示范，为国家数据安全保障提供有力支撑。了解更多 》》

工信部：扎实推进信息通信行业电信网络诈骗防范治理工作

近日，工业和信息化部举行“新时代工业和信息化发展”系列新闻发布会第二场。会上，工信部网络安全管理局一级巡视员(正局长级）周少清表示：工业和信息化部高度重视防范治理电信网络诈骗工作，深入贯彻落实习近平总书记重要指示精神，坚持以人民为中心发展思想，扎实推进信息通信行业防范治理工作，为全国电信网络诈骗立案数连续 13 个月同比下降作出重要贡献。了解更多 》》

银保监会：理财公司要加强各项业务环节数据和个人信息安全管理

8 月 25 日，中国银保监会发布《理财公司内部控制管理办法》（以下简称《管理办法》），过渡期为六个月，不符合规定的，应当在过渡期内完成整改。《管理办法》要求，理财产品销售信息和数据交换原则上应当通过银保监会认可的技术平台进行。参与信息和数据交换的相关机构应当符合技术平台相关规范要求，采取切实措施保障信息数据传输和存储的保密性、完整性、准确性、及时性、安全性。了解更多 》》

工信部通报 47 款侵害用户权益 APP 和 SDK

8 月 26 日，依据《个人信息保护法》《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，工信部组织第三方检测机构对群众关注的酒店餐饮类、未成年人应用类等移动互联网应用程序（APP）及第三方软件开发工具包（SDK）进行检查，对发现存在侵害用户权益行为的共 227 款 APP（SDK）提出整改要求。截至目前，尚有 47 款 APP（SDK）未按要求完成整改，现予以通报。了解更多 》》

PART 2.国外

一、网络空间安全政策与管理动态

NIST 发布扩展的 AI 风险管理框架草案

8 月 19 日报道，美国国家标准与技术研究院（National Institute of Standards and Technology）发布了其人工智能风险管理框架（Artificial Intelligence Risk Management Framework）的扩展第二稿，其中包含有关开发可信赖和负责任的人工智能系统的更多细节，发言人周五表示。最新的迭代是在 3 月份的初稿之后进行的 ， 其中 NIST 首次认识到需要构建和部署 AI 系统的社会技术方法 - 供自愿使用，并计划在 2023 年 1 月正式发布 AI RMF 1.0。NIST 的第二稿简化了风

险部分，解释了机构和其他组织如何建立或重新配置其风险阈值，以及值得信赖的 AI 特征和类别。除了阐明 AI RMF 的好处外，最新的草案还邀请对其自身的有效性和用例的贡献进行评估，这将阐明如何在特定部门或应用中管理风险。随着第二稿的发布，NIST 发布了一本新的剧本，建议框架用户可以采取的行动，以确保人工智能系统的设计、开发、部署和使用中的可信度。

美墨网络谈判讨论网络安全最佳实践和双边分享威胁

8 月 22 日报道，上周，美墨网络问题工作组举行首次对话，重点是推进两国在网络空间和互联网安全问题上的合作。“两国政府承诺继续加强合作，以建立一个更安全，更有弹性的地区，并扩大合作以应对网络空间的共同威胁，”新闻公告中写道。“这些努力将增强两国社会和经济从新的数字和信息技术提供的机遇中受益的能力。两国的关键基础设施特别强调为恶意网络行为者的高风险目标。增加威胁情报通信，以改善两国公共和私营部门的网络安全意识状况。与墨西哥当局分享美国制定的来自国家标准与技术研究所和国家网络安全教育倡议等机构的框架也被列为两个代表团的承诺。“美国和墨西哥重申国际法在网络空间的适用性，并将继续促进遵守和实施联合国大会通过的负责任的国家行为框架，以促进网络空间的稳定和问责制，”公告指出。在最近发生临时关闭关键基础设施以及地缘政治紧张局势的高调事件之后，美国政府已将加强公共和私人数字网络以打击网络犯罪分子为重点。

墨西哥最近实施了自己的国家信息安全计划。2020 年 3 月，墨西哥总统办公室内的国家数字战略协调处启动了自己的框架，以在该国的数字基础设施内实施更强大的数据保护和网络安全实践。

美国网络安全与基础设施安全局的威胁信息共享工作进展缓慢

8 月 22 日报道，美国国土安全部（DHS）监察长办公室（OIG）审查了网络安全与基础设施安全局（CISA）“自动指标共享”（AIS）系统在 2019 年和 2020 年的表现，结果发现 AIS 系统提供的威胁信息质量不佳。

DHS OIG 承认 CISA 在满足《网络安全信息共享法》的基本信息共享要求上取得了一定成功，但也发现 AIS 系统提供的威胁指标缺乏对决策者有帮助的背

景信息。OIG 将这一缺陷归咎于 AIS 系统功能有限和人员不足等因素。鉴于 2017 年和 2018 年的审查报告也提到了相同的问题，可见 CISA 的威胁信息共享工作进展缓慢。针对这些不足，OIG 建议 CISA 完成系统升级，改进其员工培训和招聘工作，鼓励遵守信息共享协议并制定正式的报告流程。CISA 同意 OIG 的建议，并补充称在 2019 年和 2020 年，联邦机构的 AIS 系统用户增加了 15%，非联邦机构的用户则增加了 13%。

美国政府问责局呼吁国防部落实网络安全纪律实施计划

8 月 23 日报道，美国政府问责局（GAO）近期发布一份报告，其中呼吁美国国防部（DoD）制定计划完成日期，以落实国防部网络安全纪律实施计划中的四项任务。

GAO 报告的网络安全章节要求实施 9 项建议，以帮助国防部解决美国国家安全和经济安全面临的网络和电磁频谱威胁。首先，该报告要求国防部长确保国防部首席信息官（DoD CIO）采取适当措施，从而落实国防部的网络安全文化和合规倡议任务。此外，国防部长必须确保国防部各部门制定计划完成日期，以落实国防部网络安全纪律实施计划中的四项任务。该报告指出，国防部长必须确保国防部副部长指定一个下属部门来监督和报告网络安全学科实施计划中不在 DoD CIO 管辖范围内的 7 项任务的落实情况。此外该报告要求国防部制定一个下属部门来监控国防部网络防御措施的落实情况。该报告还表示，国防部长必须确保 DoD CIO 评估高级领导人掌握的信息足够做出基于风险的决策，并相应地修改报告或制定新报告。

英国政府发布建筑业信息安全指南

8 月 23 日报道，在英国行业专家的帮助下，英国国家网络安全中心（NCSC）、商业、能源和工业战略部（BEIS）以及国家基础设施保护中心（CPNI）于 23 日联合发布《建筑业合资企业：信息安全最佳做法》指南。

该指南就如何安全地处理合资项目中创建、存储和共享的数据提供了建议，帮助建筑企业保护敏感数据受到攻击。该指南吸收了一些合资公司的意见，包括关于 HS2 和 Crossrail 等重大基础设施合同（这些合同通常规模大、价值高且复

杂，因此信息安全风险较高）的意见。该指南阐述了为什么信息安全对合资企业很重要，并提供了管理风险的推荐方法，包括：

- 在合资企业内建立信息安全治理和问责制度，并确保董事会参与其中；
- 确定负责评估特定信息安全风险和制定共享信息安全策略的人员；
- 了解合资企业的具体风险和任何监管要求，并决定共同的风险偏好；
- 制定并商定共享信息安全战略，以全面管理和减轻包括物理、人员和网络在内的风险。

美国国家安全电信咨询委员会发布网络安全报告

8 月 23 日报道,美国国家安全电信咨询委员会(NSTAC)于 23 日决定向乔·拜登总统发送一份新的信息技术影响报告,并重申 NSTAC 对安全合规和强化关键基础设施的承诺。

该报告重点关注了用于多套数字系统的运营技术与信息技术在相互融合时带来的安全风险。NSTAC 成员兼信息技术与运行技术（ITOT）分委会主席杰克·胡法德（Jack Huffard）表示，该报告着眼于包括网络安全提供商和云提供商在内的公私机构以及联邦政策制定者，以评估 ITOT 互操作系统面临的威胁形势。该报告最终发现,关键行业内的许多组织对其运行技术环境及供应链网络缺乏了解。

该报告提出了 15 条建议来帮助各方加强 ITOT 数字网络，胡法德认为以下 3 条建议最为重要：

- 让网络安全与基础设施安全局（CISA）发布一项指令，以要求行政民事机构对其物联网或物联网设备进行盘点和互连，从而改善 IT 和网络安全需求；
- 要求 CISA 更新关于采购语言的指导，以使用于支持 ITOT 融合环境的签约产品具备网络风险洞察能力和网络安全能力；
- 要求 CISA 进一步与国家安全委员会（NSC）和国家网络安全总监办公室（ONCD）合作建立信息与数据共享机制，以更好地保护国家关键基础设施免受勒索软件攻击。

美国国防部将在2027年全面落实零信任架构

8月24日报道，美国国防部首席信息官约翰·谢尔曼（John Sherman）于24日证实，国防部计划到2027年在全面落实零信任架构。谢尔曼及其团队正在开展一些项目，以满足这一愿景。比如一名副首席信息安全官正在牵头制定一项全面的零信任战略，该战略将提供从主要控制措施到最高度敏感系统的一系列零信任方法。此外国防部官员正在制定一项新的“网络人才战略”，该战略预计将在未来2个月内出台。

美国陆军承诺将加快云技术应用

8月24日报道，美国陆军高级信息技术官员称，美国陆军将在未来12个月大力推动向云迁移和加大云计算使用量。

美国陆军G-6副参谋长约翰·莫里森（John Morrison）中将表示向云迁移的基础工作已经完成，明年将是“行动和加速”的时期，并承诺“更快地向云端移动”。陆军要求为从10月1日开始的2023财年提供166亿美元的网络与IT预算（占陆军1780亿美元预算申请的9%以上），同时莫里森和其他人正在与陆军首席信息官拉杰·艾耶（Raj Iyer）进行协调，以审查该如何加快陆军对云技术的运用。艾耶将明年描述为陆军“数字化转型之旅”的转折点，他表示基于2021财年和2022财年的情况，陆军的云计划将取得巨大进展。

美国网络安全与基础设施安全局关注量子计算威胁

8月24日报道，美国网络安全与基础设施安全局（CISA）于24日发布了《使关键基础设施为后量子密码学做好准备》的简报，就关键基础设施应如何应对量子计算带来的潜在安全风险提出了建议。

CISA敦促所有关键基础设施的所有者和运营商遵循国土安全部（DHS）和美国国家标准与技术研究所（NIST）发布的报告《为后量子密码学路线图做好准备》，该报告中的路线图指导了关键基础设施的利益相关者如何采取步骤，为组织过渡到后量子密码学做好准备，比如识别、排序和保护可能易受攻击的数据、算法、

协议和系统等。CISA 的指南遵循了 7 月份参议院提出的网络安全法案，而该法案则要求联邦机构改进和更新针对量子计算威胁的数据泄露防范措施。

美国能源部推动网络安全人才建设

8 月 24 日报道，美国能源部正将利益相关者召集在一起，试图提前在技术的设计和营销阶段整合网络安全功能和服务，从而使能源行业在遭受网络攻击时更具弹性。

能源部此前于 6 月份发布了网络信息工程战略，此战略适用于各个依赖工业控制系统的行业，比如水务、交通和先进制造等。按照这一战略，美国能源部正在制定教育和劳动力培训计划，这些计划完全符合国家网络总监办公室提出的网络劳动力发展优先方向。美国国家网络副总监乔伊斯·科雷尔（Joyce Corell）指出，劳工部长和其他内阁高级官员在最近举行的白宫峰会上讨论了这一问题。鉴于美国的网络安全人员缺口约为 70 万个，因此需要高度关注教育机构、培训机构和认证机构。

美国政府计划推动化工行业的网络安全工作

8 月 24 日报道，拜登政府上台 400 天后，计划在资源基础上推动化工行业的网络安全工作，以深入了解美国关键基础设施的网络安全态势，进而提高这些设施的网络弹性。

网络安全与基础设施安全局（CISA）局长珍·伊斯特利（Jen Easterly）表示，去年白宫要求 CISA 专注于保护工业控制系统，今年的重点则是化学行业。伊斯特利赞扬了化工行业在“解决工业控制系统管理下的信息技术和操作技术”方面建立的绩效标准，并表示 CISA 正准备为更广泛的企业群体发布基于绩效的网络安全标准。不过各行业的利益相关者已开始反对美国政府推广基于绩效的做法，而是要求按照国家标准与技术研究院（NIST）关键基础设施网络安全标准框架（CSF）来灵活处理，而 NIST CSF 允许运营商根据自身愿意接受的风险程度来选择各自的网络安全控制措施。

美国小企业管理局为小型企业提供网络安全补助

8 月 24 日报道，美国小企业管理局（SBA）已拨出近 300 万美元，以帮助小企业加强其网络安全基础设施。

SBA 向三个州的代表机构提供了网络安全补助金，其中阿肯色州的 Forge Institute 获得 999650 美元，马里兰州商务局获得 930155 美元，南达科他州的达科他州立大学获得 999933 美元。此项投资是小型企业网络安全试点计划（CSBPP）的一部分。SBA 称小型企业的网络安全基础设施相对薄弱，因此对黑客来说是有吸引力的目标。SBA 表示，CSBPP 将为小型企业提供创新、构建新工具和扩展网络安全解决方案所需的资源。

二、信息通信与网络安全技术发展

联邦政府利用人工智能打击网络犯罪

8 月 19 日报道，随着数百万人在大流行期间过渡到远程工作，犯罪分子利用了增加的在线活动量。据联邦调查局称，诈骗激增。据美国政府问责局报道，人口贩子和贩毒集团长期以来一直在寻求规避监管机构和执法部门的方法，通过在线市场和加密货币改进了他们的洗钱行为，这些市场和加密货币在连接买卖双方的同时提供了匿名性。为了适应这些威胁，监管机构和执法部门开始转向人工智能和机器学习来打击不良行为者。这些工具帮助官员发现趋势并制定规则，以帮助银行和其他机构识别和报告可疑交易。监管机构、执法部门和银行有类似的优先事项，尽管他们经常通过不同的视角来考虑它们。银行希望找到不良行为者并报告他们。政策制定者需要制定法律指南，帮助银行发现它们。执法调查人员认识到，创新技术为识别和关闭人口贩运者，毒品团伙和其他犯罪集团提供了最佳工具。

2020 年的《反洗钱法》制定了一个框架，以阻止利用促进网络犯罪的数据和技术。随着监管机构制定细节，该法律尚未完全生效。与此同时，美国证券交易委员会（Securities and Exchange Commission）提出了打击金融网络犯罪的规则，国会警告说，勒索软件受害者并不总是报告攻击。监管机构需要加快与 AMLA 相关的规则制定，SEC 也应该这样做。同样，国会应该采取行动，解决缺乏有关

勒索软件和涉及加密货币的犯罪的综合数据的问题，并利用有关拟议的 ENABLER 法案的讨论，该法案将修改 AMLA 以填补漏洞。这些努力虽然至关重要，但除非监管机构、执法部门和私营部门承认网络犯罪的主要漏洞是人，否则这些努力将落空。正如世界经济论坛所发现的那样，大约 95%的网络安全问题可以追溯到人为错误。缺乏网络安全专家使问题更加复杂。私营部门需要大约 40 万这样的专业人员来应对新的威胁。即使政府机构和金融机构明天可以雇用他们需要的每个人，他们仍然需要人工智能和机器学习来管理现在例行公事的大量网络犯罪。当今网络活动的大规模和网络威胁的范围对于任何规模的团队来说都太大了，即使在公共部门也是如此。人工智能和机器学习可以承担这项工作，为寻求在后大流行时代打击网络犯罪的监管机构和执法官员带来三个独特的好处。

1) 寻找“未知的未知数”

人工智能在发现过程中帮助官员，发现所谓的“未知未知因素”，或仍然对监管机构隐藏的问题，以及多个公司和系统的数据模式，这些模式指向新兴的威胁和新的行为模式。想想看，近年来东南亚所谓的浪漫骗局是如何升级的，这些骗局是由于个人在网上引诱受害者，并将他们的钱偷到庞大的犯罪组织中，这些组织负责监督整个地区的人口贩运，强迫劳动和暴力。执法部门可以收集并倾倒数据，以发现谁一次只犯下一起案件。多个司法管辖区和货币使他们的工作更加困难。相比之下，人工智能和机器学习增强了他们的领域专业知识，帮助他们连接众多数据流中的微妙线索，以揭示秘密的不法行为。

2) 减少误报

95% 的可疑活动报告是误报。银行正在用不相关的 SAR 淹没美国财政部的金融犯罪执法网络，浪费监管机构和金融机构在发现真实犯罪时可以更好地利用的资源。使用更广泛的数据集来捕获所有已知风险并减少警报，人工智能可以将误报减少 75%以上，更有效地发现犯罪，以便将资源重新集中在其他更真实的威胁上。随着发现新的犯罪，监管机构获得了更多的知识和机会来更新他们的方法来抓获新的犯罪分子，从而产生了良性循环。

3) 构建工具以追捕最严重的罪犯

人工智能和机器学习可以帮助执法部门挑选出最糟糕的不良行为者，并收集足够的证据来反对他们。

识别实体与人之间未知的关系和联系，发现实体之间行为的异常变化，活动的数字跟踪以及其他调查技术，有助于执法部门查明犯下最具破坏性的罪行的最神秘和最难以捉摸的不良行为者。例如，在堆积如山的数据中，人工智能可以识别真正可疑的模式和不一致之处，这些模式和不一致是毒品和人口贩运组织洗钱的明显迹象。

除了使用数据自动构建新案例之外，随着时间的推移，机器学习还允许 AI 从这些调查过程中获取知识并对其进行改进。因此，官员们有更好的机会捕捉到最大的鱼，因为他们的人工智能获得了“现场经验”。

新工具检查移动应用的浏览器是否存在隐私风险

8 月 19 日报道，一个名为“InAppBrowser”的新在线工具可让您分析嵌入在移动应用程序中的应用内浏览器的行为，并确定它们是否将威胁隐私的 JavaScript 注入您访问的网站。

该工具由开发人员 Felix Krause 创建，他在本月早些时候警告过这种潜在的风险行为，并解释了应用内浏览器通过在用户访问的每个网页上注入 JavaScript 跟踪器来跟踪用户在线看到和做的任何事情是多么容易。这些注入的潜力包括访问浏览历史记录，记录行为特征以派生兴趣，日志点击和按键，监控屏幕截图操作，甚至捕获您在登录表单中输入的密码。这些启示震撼了具有嵌入式浏览器的流行应用程序社区，因此为了帮助用户确定其应用程序活动的行为，Krause 发布了“InAppBrowser”在线工具并开源了其源代码。

- 如何使用 InAppBrowser

要了解应用是否表现出潜在的可疑行为，请通过应用的内置浏览器打开该工具的网站（inappbrowser.com）。对于社交媒体应用，请公开发布指向 https://InAppBrowser.com 的链接，并尝试使用应用内浏览器打开它。对于信使应用程序，请通过 DM 将链接发送给自己，然后通过应用程序的浏览器打开它。

这些简单的步骤足以生成有关应用程序浏览器添加到网站的 JavaScript 注入的报告。但是，必须澄清的是，没有检测的报告并不意味着可以肯定地排除代码注入。“这个工具无法检测所有执行的 JavaScript 命令，也不会显示应用程序可能使用本机代码（如自定义手势识别器）执行的任何跟踪，”Krause 在他的

文章中解释道。同样，代码注入的报告并不一定意味着应用正在执行跟踪活动，而只是意味着存在滥用的可能性。

“仅仅因为一个应用程序将 JavaScript 注入外部网站并不意味着该应用程序正在做任何恶意的事情，”该报告澄清道。“我们没有办法知道每个应用内浏览器收集的数据类型的完整细节，或者数据是如何或是否被传输或使用的。BleepingComputer 的进一步测试还表明，您可以使用该工具查找桌面浏览器中的扩展创建的风险代码注入。在测试安装了 Chrome 扩展程序（如 Phantom 或 Metamask 加密货币钱包）的工具时，InAppBrowser 网站检测到各种与隐私相关的代码注入。此外，浏览器扩展的工作原理是将 JavaScript 注入您访问的网站，因此对许多扩展的检测并不罕见。但是，我们的测试表明，许多扩展程序不会使用该工具生成任何警告。由于该工具不是为分析浏览器扩展而设计的，BleepingComputer 联系了 Krause 以了解这些结果是否可靠。

- 调查结果和争议

研究人员声称在 TikTok，Instagram，Facebook 和 Messenger 上发现了危险行为，而 Snapchat 和 Robinhood 在测试中表现干净。特别是对于 TikTok，Krause 找到了监视键盘输入和屏幕点击的脚本。虽然没有迹象表明 TikTok 滥用了这种能力，但研究人员警告说，它可能被滥用来收集密码和信用卡输入等敏感信息。TikTok 发言人与 Bleeping Computer 分享了以下声明，称他们不使用这些脚本来收集击键或文本输入。“该报告关于 TikTok 的结论是不正确的和误导性的。”

研究人员特别指出，JavaScript 代码并不意味着我们的应用程序正在做任何恶意的事情，并承认他们无法知道我们的应用程序内浏览器收集了什么样的数据。与报告的声明相反，我们不会通过此代码收集击键或文本输入，该代码仅用于调试，故障排除和性能监控。因此，TikTok 承认代码已经存在，但强调它仅用于改善用户体验，而不是跟踪或侵犯用户的隐私。此外，TikTok 告诉 Bleeping Computer，它不会跟踪用户在网络上的任何地方，但该公司可能会从广告商那里收到有关其用户在第三方应用程序和网站上为提供有效广告解决方案而执行的操作的有限数据。Bleeping Computer 也要求 Facebook / Meta 对报告的调查结果发表评论，但我们尚未收到回复。

美国空军将开发下一代指挥与控制所需的量子计算软件算法

8 月 22 日报道，美国空军要求工业界开发新的量子计算算法软件，以满足未来指挥、控制、通信和情报系统中的机器自动化和机器学习需求。

空军研究实验室信息局的官员周四发布了一份关于“量子信息服务”项目的泛机构公告（FA8750 AFRL RIK ROME NY 13441-4514 USA），希望工业界提交用于研究、设计、开发、概念测试、实验、集成、评估和技术交付的白皮书。“量子信息服务”项目有五个重点领域：量子算法和计算；量子信息处理；基于内存节点的量子网络；超导混合量子平台；量子信息科学。该项目将强调基于光子的量子比特，包括量子集成光子电路、基于光子的量子比特之间的相互作用以及其它量子比特技术。在未来两年，该项目的资金将约为 2000 万美元。

在“量子信息服务”项目的五个重点领域中，量子算法和计算旨在为当今的计算机开发量子软件算法，包括“嘈杂的中尺度量子”（NISQ）计算机、量子退火计算机和绝热量子计算机；量子信息处理涉及纠缠分布、量子信息处理以及局部和分布式量子计算；基于内存节点的量子网络包括量子网络、量子通信和量子信息处理，重点是捕获离子量子比特、超导量子比特、基于集成电路的量子比特和纠缠分布；超导混合量子平台专注于开发新的量子设备、新功能和探索基础量子网络物理，重点是混合超导系统；量子信息科学专注于量子通信、量子网络和量子计算，重点是量子比特技术、用于网络和计算的量子协议以及使能技术。

三、安全业界动态

LockBit 声称勒索软件攻击安全巨头 Trust，泄露数据

8 月 18 日报道，LockBit 勒索软件团伙声称对 6 月份对数字安全巨头 Trust 的网络攻击负责。上个月，BleepingComputer 爆料了 Entrust 于 2022 年 6 月 18 日遭受勒索软件攻击的故事。从 6 月初开始，Entrust 开始告诉客户，他们遭受了网络攻击，数据从内部系统被盗。“我们已经确定某些文件是从我们的内部系统中获取的，”Entrust 在给客户的安全通知中分享道。LockBit 被认为是目前最活跃的勒索软件操作之一，其面向公众的操作“LockBitSupp”积极与威胁参与者和网络安全研究人员合作。

苹果警告 Safari 中的关键安全风险 适用于 iPhone、iPad 和 Mac

8 月 19 日报道，苹果已经发布了更新，以修复 iPhone，iPad 和 Mac 设备上的安全漏洞，此前他们承认这些漏洞可能已被威胁行为者“积极利用”。据报道，该漏洞使黑客能够渗透到 WebKit 中，WebKit 是为 Apple 网络浏览器 Safari 提供支持的引擎。一旦获得最初的立足点，威胁行为者就可以控制设备的操作系统（OS）以“执行任意代码”，并可能通过“恶意制作的 Web 内容”渗透到设备中。在受影响的设备方面，苹果提到了可追溯到 6S 型号的 iPhone，iPad 第 5 代及更高版本，iPad Air 2 及更高版本，iPad mini 4 及更高版本，所有 iPad Pro 型号以及第 7 代 iPod touch。

关键基础设施的网络安全将获得 4500 万美元的资金

8 月 22 日报道，近年来，在对关键基础设施的几次攻击以及这些攻击的发生率不断提高之后，能源部正在为下一代技术提供 4500 万美元的资金，以保护电网免受网络攻击并帮助部署清洁能源。美国能源部网络安全，能源安全和应急响应办公室将资助多达 15 个研究，开发和示范项目，以创建新的网络安全工具和技术，以降低能源基础设施的网络风险。这些项目将与能源公用事业、供应商、大学、实验室和服务提供商建立或帮助现有的研究伙伴关系，致力于建立一个有弹性的能源系统。例如，美国能源部表示，这将允许研究人员“开发工具和技术，使能源系统能够自主识别网络攻击，试图阻止它，并自动隔离和根除它，而不会中断能源输送。

国防情报局在复杂的云迁移中面临数据访问挑战

8 月 23 日报道，国防部情报局（DIA）首席信息官表示，该机构在实现军事和情报界绝密 IT 网络——联合全球情报通信系统（JWICS）的现代化方面取得了进展，但目前需要一些时间来确定支撑它的设想的云基础设施的适当和最安全的数据接入点。作为 DIA 的首席信息官，Douglas Cossa 正在指导 JWICS 的显着改进，这是一个拥有三十多年历史的系统，将发展到集成所有美国情报一致的组件，

并实现绝密数据和信息在它们之间的安全传输。Cossa 表示，作为 JWICS 的企业提供商，其任务是查看需要云接入点的位置，并与世界各地的供应商合作确定优先事项。云接入点本质上是国防部连接到商业云的安全管道，使 DOD 组件能够监视通过它的通信量。至少在短期内，DIA 打算在混合云环境中运营，并托管自己的基础设施。虽然情报机构可以承担与这些业务功能现代化相关的一些风险，但首席信息官指出，与任务相关的流程在数据访问、身份管理、覆盖范围、容量和安全要求方面存在更多挑战。在这些情况下，DIA 官员需要能够看到供应商方面防火墙后面发生的事情的全部安全威胁。DIA 与美国最亲密的国际合作伙伴（包括五眼联盟国家）之间也有许多新的合作机会，这些国家也越来越多地转向基于云的服务。澳大利亚、加拿大、新西兰、英国和美国是该情报共享小组的成员，通过该小组，它们在信号情报方面进行联合合作。但是，从这个意义上说，围绕身份管理以及数据访问和集成策略的挑战仍然存在。

前推特高管揭发推特存在严重网络安全问题

8 月 23 日报道，在国社交媒体平台“推特”（Twitter）的前安全主管派特尔·扎科（Peiter Zatko）向美国有线电视新闻网（CNN）揭发推特存在重大安全问题，对推特用户的个人信息、公司股东、国家安全和民主构成威胁。扎科称，推特公司管理混乱，允许许多员工在没有充分监督的情况下访问平台的中央控制信息及其它最敏感的信息。推特的领导层试图隐瞒一些可能被外国间谍活动、黑客攻击和虚假信息活动所利用的严重系统漏洞，此外一名或多名现任员工可能正在为外国情报机构工作。比如印度政府就强迫推特公司将其代理人列入工资单，使他们能够访问敏感的用户数据对。

西方多国即将举行网络安全峰会

8 月 24 日报道，美国将于 9 月 7 日至 9 日期间在华盛顿特区举行第 13 届比灵顿网络安全峰会，届时来自以色列、德国、加拿大、英国和美国的网络领导人将讨论如何联合威慑网络恶意行为者。峰会议程包括由来自乌克兰的网络领导人讲述俄乌冲突中的网络经验，以及如何利用这些信息帮助西方更好地防御来自俄罗斯的网络攻击。此外来自美国和英国的顶级网络指挥官也将概述他们的战略网

络伙伴关系以及他们面临的重要技术挑战。包括美国网络总监在内的许多网络安全界重要人士还将在峰会期间发表演讲，演讲主题包括选举安全，确保基础设施运营商、联邦政府、州级政府和私营机构参与网络行动，国家网络事件响应计划，颠覆性技术，以及网络劳动力的发展等。

多米尼加政府机构遭到勒索软件攻击

8月24日报道，多米尼加共和国农业部下属的农业研究院（IAD）遭到Quantum勒索软件攻击，导致该机构的一些工作站被加密。当地媒体报道称，勒索软件攻击发生在 8 月 18 日，IAD 的几乎服务器（四台物理服务器和八台虚拟服务器）都受到影响，数据库、应用程序和电子邮件等都被泄露。协助 IAD 从攻击中恢复的国家网络安全中心（CNCS）表示，攻击者的 IP 地址来自美国和俄罗斯。攻击者声称已经窃取了超过 1TB 的数据，并威胁如果 IAD 不支付 65 万美元的赎金，就会公布这些数据。

新型恶意软件种类激增导致勒索软件攻击激增

8 月 25 日报道，根据网络安全公司 NCC Group 的数据，由于涉及新型恶意软件感染目标的攻击增加，勒索软件案件增加了 47% 。

据该公司称，通过跟踪发布受害者详细信息的网站发布有关勒索软件活动的半定期报告，报告的事件从 6 月的 135 起增加到 7 月的 198 起。就在本周，与 LockBit 相关的勒索软件攻击者一直在部署强大的新版本恶意软件，使法国一家医院陷入困境，导致一些患者不得不被转移到其他设施。

据 NCC Group 称，LockBit 与 7 月份的 62 起事件有关，比 6 月份的 52 起已知事件总数高出近 20%。该公司写道，LockBit 仍然是“最具威胁性的勒索软件组织，所有组织都应该意识到这一点”。

美国政府在网络安全上花费数十亿美元

8 月 25 日报道，近几个月来，众议院一直在努力起草 2023 财年的各种支出法案。虽然这些法案为大量的政府计划和机构提供了资金，但有一件事情确实很突出。总的来说，通过众议院的法案为网络安全支出分配了惊人的 156 亿美

元。这笔支出的最大份额（112 亿美元）分配给了国防部。然而，值得注意的是，近 30 亿美元将流向网络安全和基础设施安全局 (CISA)。尽管将这些网络安全预算分配视为政府过度支出的另一个例子可能很诱人，但值得考虑的是，156 亿美元的现金注入对 IT 安全行业意味着什么。同样重要的是要考虑为什么美国政府认为有必要将其网络安全支出提高到如此程度。

四、网络攻防动态

网络犯罪组 TA558 针对酒店和旅游组织进行攻击

8 月 19 日报道，一个出于财务动机的网络犯罪组织与针对拉丁美洲的酒店，酒店和旅游组织的持续攻击浪潮有关，其目的是在受感染的系统上安装恶意软件。该团体发起的网络钓鱼活动涉及发送带有预订主题诱饵的恶意垃圾邮件，例如包含武器化文档或 URL 的酒店预订，以诱使不知情的用户安装能够侦察，数据窃取和分发后续有效负载的特洛伊木马程序。这些攻击多年来一直在微妙地演变：在 2018 年至 2021 年期间发现的攻击利用包含 VBA 宏的 Word 文档的电子邮件或利用 CVE-2017-11882 和 CVE-2017-8570 等漏洞来下载和安装混合恶意软件，例如 AsyncRAT，Loda RAT，Revenge RAT 和 Vjw0rm。然而，最近几个月，TA558 已经观察到从宏负载的 Microsoft Office 附件转向 URL 和 ISO 文件以实现初始感染，此举可能是为了响应 Microsoft 决定阻止默认情况下从 Web 下载的文件中的宏。在该组织今年迄今为止开展的 51 个活动中，据说其中 27 个包含了指向 ISO 文件和 ZIP 档案的 URL，而从 2018 年到 2021 年总共只有五个活动。

攻击者利用假期袭击美国政府

8 月 19 日报道，美国政府行业主要在 2021 年第一季度处理了针对地方，联邦和州政府网络的严重违规行为。遥测数据显示，在 2021 年 3 月，通用后门检测（称为 Backdoor.Agent）中有一个小峰值，主要集中在田纳西州的孟菲斯。这一数据与加利福尼亚州 Azusa 警察局的袭击相吻合;但是，它揭示了有关下个月观察到的攻击的更多信息。在 2021 年 4 月，至少有三起针对政府服务的著名袭击事件成为新闻，其中包括纽约大都会交通管理局（MTA），伊利诺伊州总检

察长办公室和华盛顿特区警察局。在同一个月，我们还观察到了漏洞利用激增的开始，人工智能检测到的威胁在 2021 年剩余时间里占主导地位。

爱沙尼亚对抗大规模分布式拒绝服务（DDoS）攻击

据《信息安全杂志》8 月 22 日报道，8 月份针对爱沙尼亚公共当局和企业的大规模分布式拒绝服务（DDoS）攻击的数量和频率显着增加。到目前为止，这些攻击的高峰记录在 8 月 16 日和 17 日，爱沙尼亚信息系统管理局（RIA）事件响应（CERT-EE）部门负责人 Tõnu Tammer 告诉 Infosecurity。Tammer 表示，这些攻击来自 RIA 自 2022 年春季以来已知的网络犯罪分子，当时 4 月 9 日和 10 日，当锁定的盾牌国际网络防御演习在爱沙尼亚举行时，攻击有所增加。然而，他拒绝透露该组织的名字，因为“命名他们会给他们带来他们不值得的关注”。

超 80，000 台海康威视摄像机被注入易受攻击的漏洞

8 月 22 日报道，安全研究人员已经发现了超过 80，000 台海康威视摄像机容易受到关键命令注入漏洞的影响，该漏洞很容易通过发送到易受攻击的 Web 服务器的特制消息来利用。该漏洞被跟踪为 CVE-2021-36260，并由海康威视于 2021 年 9 月通过固件更新得到解决。但是，根据 CYFIRMA 发布的白皮书，100 个国家/地区的 2，300 个组织使用的数以万计的系统仍未应用该安全更新。

英国最大汽车经销商遭受了严重的勒索软件攻击

8 月 22 日报道，英国最大的家族汽车经销商之一承认上个月遭受了严重的勒索软件攻击，导致数据被盗和一些核心系统“无法修复”的损坏。总部位于特伦特河畔斯托克的 Holdcroft Motor Group 在黑客窃取了包括员工信息在内的两年数据后，遭到了赎金要求的打击。“2022 年 7 月 28 日星期四，该公司成为严重网络攻击的受害者，该攻击对公司的 IT 基础设施造成了重大损害，并导致我们内部存储区域的数据丢失，”StokeonTrentLive 看到的一封内部电子邮件中写道。

全球比特币 ATM 大型制造商遭受黑客零日漏洞攻击

8 月 22 日报道，一家比特币 ATM 公司的系统受到零日漏洞的攻击，该漏洞使黑客能够抽走未公开数量的数字货币。General Bytes 在周五的“最高”严重性警报中指出，其关键加密应用程序服务器（CAS）中的零日错误是攻击的罪魁祸首。

“攻击者能够通过 CAS 管理界面远程创建管理员用户，方法是在服务器上用于默认安装的页面上进行 URL 调用，并创建第一个管理用户，”警报显示。

该公司的攻击者没有设法访问主机操作系统，主机文件系统，数据库或任何密码，密码哈希，盐，私钥或 API 密钥。但是，目前尚不清楚在攻击被发现之前他们能够窃取多少客户资金。

谷歌研究人员揭露了伊朗黑客的工具

8 月 23 日报道，谷歌研究人员 8 月 23 日表示，与伊朗政府网络间谍部门有联系的黑客开发了一种软件工具，可以从 Gmail，雅虎和微软 Outlook 帐户中检索下载的电子邮件和其他数据。谷歌威胁分析小组（Threat Analysis Group）的研究人员称该工具为“HYPERSCRAPE”，他们在 2021 年 12 月检测到了该恶意程序。据谷歌安全工程师 Ajax Bash 称，伊朗黑客似乎已经将其部署在伊朗的不到二十多个帐户上。

之前对该小组工具的研究表明，持续的操作安全错误和相对基本的开发有助于归因，但仍然有效，就像 Hyperscrape 的情况一样。像他们的许多工具一样，Hyperscrape 并不以其技术复杂性而闻名，而是它在实现 Charm Kitten 目标方面的有效性。为了使该工具正常工作，受害者需要登录到他们的帐户，或者攻击者需要他们的凭据。进入内部后，该工具会将帐户的语言设置更改为英语，下载单个电子邮件，然后将其标记为未读。Bash 写道，该程序还删除了由该活动触发的 Google 的任何安全电子邮件。

微软发现了 Nobelium 黑客使用的新的入侵后恶意软件

8 月 25 日报道， SolarWinds 供应链攻击背后的威胁行为者与另一种“高度针对性”的利用后恶意软件有关，该恶意软件可用于维持对受损环境的持续访问。

该开发项目被微软的威胁情报团队称为 MagicWeb，重申了 Nobelium 对开发和维护专用功能的承诺。

Nobelium 是这家科技巨头的一系列活动的绰号，这些活动在 2020 年 12 月针对 SolarWinds 的复杂攻击中曝光，与广为人知的俄罗斯民族国家黑客组织 APT29、Cozy Bear 或 The Dukes 重叠。“Nobelium 仍然非常活跃，同时针对美国、欧洲和中亚的政府组织、非政府组织 (NGO)、政府间组织 (IGO) 和智库开展了多项活动，”微软表示。MagicWeb 与另一个名为 FoggyWeb 的工具有相似之处，据评估它已被部署以在修复工作期间保持访问和抢先驱逐，但只有在获得对环境的高度特权访问并横向移动到 AD FS 服务器之后。

虽然 FoggyWeb 具有提供额外负载和从 Active Directory 联合服务（AD FS）服务器窃取敏感信息的专门功能，但 MagicWeb 是一个流氓 DLL（“Microsoft.IdentityServer.Diagnostics.dll”的后门版本），有助于秘密访问 AD FS 系统通过身份验证绕过。微软表示：“Nobelium 部署 MagicWeb 的能力取决于能够访问对 AD FS 服务器具有管理访问权限的高特权凭据，从而使他们能够在他们有权访问的系统上执行任何他们想要的恶意活动。”

美联储警告针对医疗保健的新威胁攻击

8 月 25 日报道，美卫生与公众服务部卫生部门网络安全协调中心警告说，自 6 月以来，至少有四个医疗保健和公共卫生部门实体受到 Karakurt 的攻击，“一个相对较新的网络犯罪集团”。

警报称，最近的袭击受害者包括一家辅助生活设施、一家牙科公司、一家医疗保健提供者和一家医院。虽然 HHS HC3 没有按名称确定这些实体中的任何一个，但 Karakurt 在过去两周加大了针对其明显受害者之一卫理公会麦金尼医院的公开骚扰活动，威胁要公布据称从德克萨斯州窃取的超过 367 GB 的数据设施。

五、网络作战演训动向

CISA 在 2022 年中期选举前举办选举安全演习

8 月 22 日报道，网络安全和基础设施安全局以及选举社区的州和地方成员上周完成了为期三天的演习，为 2022 年中期选举前投票过程的一系列潜在网络和物理威胁做好准备。

CISA 在一份新闻稿中指出，这次演习“不是对任何特定或可信的威胁的回应”，而是一种让官员和选举管理人员“有机会分享有关网络和物理事件规划，准备，识别，响应和恢复的做法”的方式。来自司法部，联邦调查局，国土安全部，国家安全局和其他联邦机构的官员也参加了此次活动，还有州和地方选举官员以及十几家选举行业公司。

围绕这次演习的信息突显了各级政府官员正在进行的努力，在即将到来的中期选举之前，向人们对选举基础设施的安全性和弹性充满信心，特别是因为关于投票系统准确性的虚假信息继续对选举管理者构成严重挑战。众议院监督与改革委员会本月早些时候发布的一份民主党工作人员报告发现，错误信息的传播“几乎损害了选举管理的所有要素”，并“增加了选举颠覆的可能性”。

“本周的演习只是联邦政府，州和地方选举官员以及私营部门之间全年协调的众多例子之一，为 2022 年大选做准备，”组织该活动的选举官员机构和协会的领导人在一份联合声明中说。，并指出美国所有州，领土和地方管辖区已经共享并接收有关选举基础设施潜在威胁的信息。

虽然官员们在联合声明中表示，风险的“动态环境”——包括对选举基础设施的网络和物理威胁以及“削弱选民对这一过程的信任的虚假选举信息”——对选举官员构成了持续的挑战，但他们也强调了选民在选举过程中应该继续拥有的信心。

亚太地区举行 2022 年 APCERT 网络演习

8 月 22 日报道，亚太计算机应急响应小组（APCERT）组织的 2022 年度演练由，旨在促进信息安全、计算机病毒、恶意代码等主题的信息共享和技术交流，提高计算机应急响应能力。

今年的演习涉及一家制药公司的系统和数据被网络犯罪分子勒索，并威胁将敏感信息（包括客户的详细信息）发布到暗网上。澳大利亚网络安全中心 (ACSC)

负责人表示，勒索软件对澳大利亚组织构成了最重大的威胁之一，我们的年度网络威胁报告记录了 2020-21 财年勒索软件网络犯罪增加了 15%。拥有敏感个人信息的行业，例如医疗保健行业，是网络犯罪分子的主要目标。澳大利亚卫生部门报告的 2020/21 财年网络安全事件总体数量和与勒索软件相关的网络安全事件数量均位居第二。对于网络犯罪分子来说，地理位置无关紧要，只要有互联网连接，他们就会在全球范围内寻找目标。

像 APCERT 演习这样的活动是一个与国际合作伙伴合作的机会，通过合作、信任和真正的信息共享来帮助保护网络空间。APCERT 由来自印太地区的 33 个网络安全应急响应小组组成。ACSC 作为指导委员会和多个工作组的成员担任重要职务，加强了澳大利亚在促进该地区网络安全方面的领导作用。