[安全热点周报]

第一百六十四期（2020/10/16）

全球网络安全大事件，你都没有错过

本期资讯导视：

黑客利用 VPN 漏洞入侵美国政府选举支持系统
国家安全机关破获数百起台湾间谍情报机关窃密案件
欧盟起草“打击名单” 大型科技公司将面临更严格的监管
全国首个比特币勒索病毒制作者落网
美国国防部宣布投入 6 亿美元用于 5G 军事实验
防止黑客攻击特斯拉推出双重验证功能
“五眼联盟”要求科技公司应用程序为其设置“后门”

奇安信 CERT

本期安全大事件

安全文章 | 黑客利用 VPN 漏洞入侵美国政府选举支持系统

黑客通过结合 VPN 漏洞与最近的 Windows CVE-2020-1472 安全漏洞，入侵了美国选举支持系统，并获得了访问权限。美国网络安全与基础设施安全局（CISA）表示，APT 攻击者使用此漏洞链接策略，攻击联邦和 SLTT（州，地方，部落和领土）政府网络以及选举组织，基础设施。为了获得对这些系统的访问权限，攻击者利用了 Fortinet FortiOS 安全套接字层（SSL）VPN 中的 CVE-2018-13379 漏洞或 MobileIron 统一端点管理（UEM）中的 CVE-2020-15505 漏洞，使移动设备获得初始访问权限。然后，再利用 Windows Netlogon 身份验证协议中的严重安全漏洞 CVE-2020-1472（又名 Zerologon）。攻击者可以在成功利用此漏洞后将特权提升给域管理员，从而控制整个域并更改用户的密码。CISA 警告说，他们还可能在攻击中使用其他漏洞来针对未修补和面向 Internet 的网络边缘设备，进而影响 2020 年的美国大选。

点击阅读原文：黑客利用 VPN 漏洞入侵美国政府选举支持系统

权威发布&安全趋势

点击图片阅读原文

近期，国家安全机关组织实施“迅雷-2020”专项行动，依法打击台湾间谍情报机关渗透破坏活动，破获数百起间谍窃密案件，抓获一批台湾间谍及运用人员，打掉台湾间谍情报机关针对祖国大陆布建的间谍情报网络，有效维护了国家安全和利益。更多详细内容请查看原文。

点击图片阅读原文

《金融时报》消息称，欧盟正在起草一份涉及多达20家大型科技公司的 "打击名单"，这些公司将面临比小型竞争对手更严厉的监管，比如强制数据共享和提高透明度的要求。该名单的制定基于市场份额、用户数以及他人对其平台的依赖性等标准。更多详细内容请查看原文。

点击图片阅读原文

在“净网2020”专项行动中，南通、启东两级公安机关联手，日前成功侦破一起由公安部督办的特大制作、使用勒索病毒破坏计算机信息系统，从而实施网络敲诈勒索的案件，抓获巨某、谢某、谭某等3名犯罪嫌疑人，其中巨某系多个比特币勒索病毒的制作者。截至案发，巨某已成功作案百余起，非法获利的比特币折合人民币500余万元。更多详细内容请查看原文。

安全快讯

点击图片阅读原文

据外媒CNET报道，美国国防部宣布将为圣地亚哥海军基地等、犹他州希尔空军基地、华盛顿州刘易斯-麦克乔德联合基地五个军事基地的5G实验提供6亿美元资金。这些测试将集中在虚拟现实训练、机器人和无人机等方面，国防部前几日称5G对美国国家和经济安全至关重要。

点击图片阅读原文

随着车辆联网程度越来越高，不少车辆容易受到黑客的袭击，为了尽可能避免这种情况，提升用车安全性，特斯拉推出了基于令牌功能的两重验证，用户可以使用 Tesla 账户使用第三方身份验证来激活该功能，该功能降低了车辆被黑客攻击的可能性，在一定程度上可以提升车辆的安全性。

点击图片阅读原文

由美国、英国、澳大利亚、加拿大和新西兰组成的“五眼”情报联盟，要求科技公司在加密的应用程序中设置“后门”，以允许“五眼”国家执法机构获得他们声称的监控网络犯罪的权限。当地时间10月11日，“五眼”国家最高司法官员在发布的一份声明中表示，Signal、Telegram、Facebook Messenger和WhatsApp等端到端加密应用的增长，使执法部门无法监管，这对公共安全构成了重大挑战。