01

CODESYS WebVisu 产品出现严重漏洞

根据外媒 Securitweek 报道，Istury IOT发现 3S-Smart SoftwareSolutions 的 CODESYS WebVisu 产品所使用的 Web 服务器组件存在基于堆栈的缓冲区溢出漏洞，远程攻击者可以利用此漏洞触发拒绝服务（DoS），某些情况下还能在 Web 服务器上执行任意代码。

02

俄罗斯暗网出现新勒索软件GrandCrab

网络安全公司LMNTRIX的专家发现了一种名为GandCrab的新型勒索软件即服务（ransomware-as-a-service）。一旦感染病毒，如果受害者没有及时付款，他得要支付双倍的赎金。GandCrab RaaS支持使用加密货币Dash进行支付，并且该服务由托管在.bit域中的服务器提供。

06

中国对境外虚拟货币交易所采取措施

2月4日晚间央行旗下媒体《金融时报》报道，去年底以来，一些境内人士转向境外网站平台参与ICO和虚拟货币交易，相关行为又有了死灰复燃迹象。下一步将继续对虚拟货币相关行为保持严密关注，采取包括取缔相关商业存在，取缔、处置境内外虚拟货币交易平台网站等在内的一系列监管措施，以防范金融风险，维护金融稳定。

07

WannaMine：通过永恒之蓝传播的挖矿病毒

CrowdStrike的研究人员发现了一款名为WannaMine的新型Monero加密挖掘蠕虫，它会利用与NSA相关的EternalBlue漏洞进行传播。CrowdStrike的安全研究人员说，这个恶意代码非常复杂，它类似于国家支持的APT组织所使用的模型。

08

400万手机被僵尸网络DressCode感染

2016年，研究人员曝光了一个僵尸网络病毒“DressCode”，被它感染的安卓手机会变成一个中转监听站，从受保护的网络中提取敏感信息。当时，谷歌称将携带恶意僵尸代码的400个 Google Play App 下架，并且采取了“必要手段”保护已感染的用户。时隔16个月，一名黑客提供证据表明，这个所谓的DressCode僵尸网络仍在活跃，且可能已经感染400万台设备。