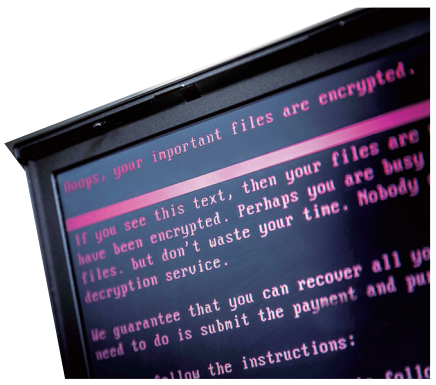
勒索病毒再度来袭

全球多国相继“中招”,罪魁祸首是美国国家安全局



俄罗斯部分机构和企业电脑遭勒索病毒攻击

新华社电 全球多个国家的网络27日遭新一轮勒索病毒攻击。乌克兰受害严重,其政府部门、国有企业相继“中招”。据西方媒体报道,有研究人员发现,与上月的“想哭”勒索病毒相似,新勒索软件使用了遭泄密的美国国家安全局网络“开锁工具”。

最先攻击乌克兰 随后蔓延至欧洲、北美

美联社报道,27日出现的勒索病毒看似最先攻击乌克兰,随后蔓延至欧洲、北美地区多个国家。

据西方媒体报道,受影响的全球大公司包括:俄罗斯石油公司、丹麦航运与石油集团马士基、英国传播服务集团WPP、荷兰TNT国际快递公司、美国制药公司默克、美国食品业集团亿滋国际、美国欧华律师事务所等。

俄罗斯网络安全公司Group-IB说,乌克兰和俄罗斯境内已有超过80家公司受影响。勒索软件侵入电脑后,将文件加密锁定,要求受害者支付价值300美元的比特币才能解锁文件。

另据俄网络安全公司卡巴斯基实验室初步调查显示,该勒索软件当天已实施约2000次攻击,90%以上在乌克兰和俄罗斯,波兰、意大利、德国、法国、英国、美国也受害。

俄罗斯石油公司证实,其网络服务器当天遭遇了一次“强力”攻击,但多亏其“备用系统”,公司的石油生产和开采并未中断。

美联社报道,该勒索软件的蔓延速度看似呈逐渐放缓趋势,部分原因可能是该软件需要通过电脑系统“直接接触”传播,在与乌克兰网络关联较少的地区,其传播受限。另据路透社,已有30多名受害者支付了比特币赎金。

乌克兰影响最为严重

据西方媒体报道,乌克兰高级别政府部门、中央银行、国家电力公司、首都基辅的机场、切尔诺贝利核事故隔离区监测系统、乌克兰地铁、乌克兰电信公司、飞机制造商安东诺夫公司及一些商业银行、能源公司、自动提款机、加油站、大型超市均受影响。

切尔诺贝利核事故隔离区辐射监测系统被迫“下线”。乌克兰中央银行在一份声明中说,受网络袭击影响,“一些乌克兰银行的业务、客户服务正遭遇困难”。

乌克兰总理弗拉基米尔·格罗伊斯曼在社交网站脸书上说,这样的网络袭击在乌克兰“史无前例”,但他称该国“重要系统未受影响”。

一款“从没见过的”新型勒索软件

上月12日,名为“想哭”的勒索病毒席卷全球约150个国家、实施超过20万次攻击,影响政府部门、公共交通、医疗、邮政、通信等领域。受害者被要求限期支付价值300美元的比特币以换取文件解锁,否则赎金上涨。“想哭”软件风波随后在较短时间内被平息。

目前,新一轮勒索病毒的来源、传播途径及其背后动机还不清楚。

微软公司说,这一病毒软件利用了微软系统的一个漏洞,尽管该漏洞在今年3月的一次安全升级中被打过补丁。

Group-IB公司和一些网络安全专家说,新勒索软件看似是去年出现的Petya勒索软件变体。但卡巴斯基实验室说,这是一款“从没见过的”新型勒索软件。

新勒索软件使用NSA研发的“开锁工具”

有专家发现,与“想哭”病毒相似,新勒索软件也使用了由美国国家安全局(NSA)研发的“开锁工具”。今年4月,美国国安局遭遇泄密事件,其研发的黑客攻击工具被名为“影子中间人”的神秘组织公布在网上。

美国韦拉科德公司首席技术官克里斯·威索帕尔说,两起事件针对的是同一个微软“视窗”系统代码漏洞。

美国企业安全公司Proofpoint安全专家瑞安·卡伦贝尔则说,即便是一些对已曝光漏洞打了补丁的电脑,也可能在此次袭击中“中招”。卡伦贝尔说,与常规网络勒索袭击不同的是,此次袭击不仅针对受害者的个人信息文件,还改写了电脑的主引导记录(MBR),因而更难对付。

多方跟踪 微软采取妥善措施保护用户

微软公司发言人说,正调查这起网络袭击,将采取妥善措施保护用户,并称微软公司的杀毒软件能够发现并删除该勒索软件。

美国白宫国家安全委员会在一份声明中说,美政府机构正调查这起事件,美国“决心对相关负责人追究责任”。美国国土安全部称,正监视这起网络袭击并与其他国家协调配合;建议受害者不要支付赎金,因为即使付了赎金,也不一定能保证文件恢复。国际刑警组织说,正密切监视网络袭击情况并与相关成员国保持联络。法国国家信息系统安全局也称正分析这起网络袭击。

美宣布找到失踪中国学者乘坐的涉事汽车

新华社电 美国联邦调查局27日宣布,已经找到中国访问学者章莹颖失踪前乘坐的汽车,呼吁公众继续提供有利于破案的线索。

联邦调查局在声明中说,在得到公众提供的大量有关涉事汽车的线索后,已经找到这辆黑色土星汽车,目前正在积极调查章莹颖的下落。联邦调查局表示不再需要公众提供关于车辆的信息,但继续向公众征集任何有利于找到章莹颖的线索,之前承诺的1万美元悬赏金仍然有效。由于案件仍在调查中,不能透露关于何时何地发现汽车的具体信息。

现年26岁的章莹颖今年4月前往伊利诺伊大学厄巴纳-尚佩恩分校进行访问学习,本月9日14时左右坐上一辆汽车后失踪。美国联邦调查局14日正式将这一事件定性为绑架案。监控录像显示,涉嫌绑架章莹颖的犯罪嫌疑人是一名白人男子,在她上车之前,这名嫌疑人驾驶一辆黑色轿车一直在周边区域兜圈。

委内瑞拉最高法院遭手榴弹恐袭?

新华社电 委内瑞拉一名警察27日下午驾驶一架直升机,向位于加拉加斯市区的委内瑞拉最高法院大楼开枪射击,并投下手榴弹,袭击未造成人员伤亡。

据报道,实施袭击的奥斯卡·佩雷斯是一名警察,他驾驶一架直升机飞往总统府,并在飞行中打出支持反对派街头运动的“自由”标语。随后他向委内瑞拉最高法院、内政和司法部大楼等建筑开枪射击,并朝最高法院大楼投下手榴弹。据最高法院大楼附近的居民称,听到了枪声和爆炸声。

委内瑞拉总统马杜罗在其后的电视讲话中谴责袭击事件,称该事件是反对派策划的“恐怖袭击”。按照马杜罗的说法,这一事件的幕后黑手与美国中央情报局有关联。马杜罗指认,美国政府暗中支持委内瑞拉反对派、觊觎委内瑞拉石油资源。他提醒美国总统特朗普,称一旦委内瑞拉出现“毁灭性”局势,大批难民将会涌向美国。

自今年4月以来,马杜罗政府和反对派的冲突愈演愈烈,委内瑞拉国内爆发持续大规模反政府游行,截至目前已有76人死于游行中的暴力事件。

被诉受贿 特梅尔斥“谎言”

新华社电 巴西总统米歇尔·特梅尔27日针对前一天遭受贿罪名起诉一事发表讲话,称这是“肥皂剧”,质疑巴西总检察长罗德里戈·雅诺特目的不纯,暗示后者可能“吃回扣”。他指责巴西总检察长雅诺特编造了一场“肥皂剧”,不仅抹黑总统名声,还可能让刚刚走出经济衰退的巴西再受打击。

“我不会让自己因没有犯下的罪行而面临指控,我想为巴西工作,我不会逃避眼下这场‘战争’。”

雅诺特26日以受贿罪向联邦最高法院正式起诉总统特梅尔,并指出“被指控者的非法行为非常恶劣”。除受贿罪名,雅诺特眼下还在调查特梅尔涉嫌妨碍司法、与犯罪团伙有关联等罪名。作为回应,雅诺特办公室在一份声明中强调,雅诺特在处理公众事务时清廉透明。

朝鲜宣布对所有参与暗杀朝鲜最高领导人者处以极刑

新华社电 朝鲜有关部门28日宣布,将对所有参与暗杀朝鲜最高领导人金正恩的人处以极刑,其中包括韩国前总统朴槿惠。

朝鲜国家保卫省、人民保安省和中央检察院当天发表声明说,有确凿证据表明,朴槿惠从2015年年底开始策划企图暗杀金正恩的阴谋,并由韩国国情院负责。

声明说,朝鲜近期破获一个由美国中央情报局和韩国国情院派入境内的恐怖主义小组。朝方根据这些人的供词及其他调查结果认为,朴槿惠曾亲自决定对朝鲜开展“政权更迭”的秘密行动,并在韩国国情院的有关执行方案上签了字。

这些暗杀计划包括制造车祸和火车出轨事故等。但由于朴槿惠本人被弹劾以及朝鲜安全部门的警觉,阴谋没能实现。