勒索软件“BitCrypt”瞄准比特币！电子钱包、信息均成目标

趋势科技提醒警惕陌生邮件　保护好你的比特币

[趋势科技中国]– [2014 年 4 月 18 日]全球服务器安全、虚拟化安全及云安全领导厂商趋势科技公布，近期发现勒索软件(Ransomware)新手法，自称为 BitCrypt。该勒索软件除了加密感染电脑中的文件进行勒索之外，还专门从当前流行的各类电子钱包内窃取资金、并窃取用户电脑内重要信息。由于这个新变种加入了中文语言版本，有可能将针对中国地区攻击。趋势科技提醒广大网友，打开陌生邮件时千万要小心，建议比特币用户使用离线电子钱包、并备份电脑内的重要资料，避免遭到勒索。目前，趋势科技最新中国区病毒码 10.714.60 已可以检测并处理此勒索软件，用户可升级到最新病毒码以进行防护。

趋势科技（中国区）技术总监蔡昇钦表示：“CryptoLocker 或是其它类似勒索软件的严重威胁在国外已经持续很久了，近两年开始在中国流行。 最近我们又确认了此类威胁的两个不同变种 ‘TROJ_CRIBIT.A’，TROJ_CRIBIT.B。除了会对加密文件加上后缀 ‘.bitcrypt*’ 之外。其中一个变种更是使用了含中文在内的 10 种语言发送勒索邮件。攻击者还 ‘体贴’ 的加入了 Tor2Web 链接使受害者无需安装 tor 软件即可连接存在于 DeepWeb 的 web 页面进行支付、解密 ”

蔡昇钦指出，此勒索程序会从各种渠道入侵用户电脑，尤其是垃圾邮件。趋势科技主动式云端截毒服务(Smart Protection Network)的资料显示，有 40%的 CRIBIT 受害者来自美国，另外有 11%来自日本。

勒索信内容如下：

注意！

你的 BitCrypt ID：{ 交易编号 }

你电脑上所有的必要文件（照片、文件、资料库和其他）都通过唯一的 RSA-1024 密钥加密。

只有通过一个特殊程序才能解密你的文件，而且每个 BitCrypt ID 都对应一个程序。

来自电脑维修服务和防毒实验室的专家无法帮助你。

为了收到解密程序，你需要遵照此链接 { 恶意网站＃1 } 和跟随指示。

如果现有链接无法作用，你需要按照以下步骤恢复文件：

1.尝试打开连结｛恶意网站＃2｝。如果失败，继续执行步骤 2。

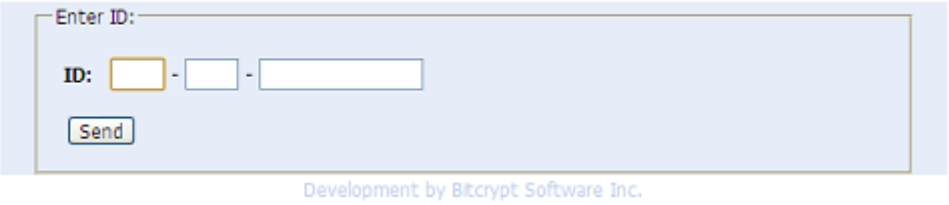
2.下载并安装 Tor 浏览器｛Tor 专案网站｝

3.安装完成后，启动 Tor 浏览器，连接下列网址｛恶意网站＃3｝

记住，你越快采取行动，越有机会去恢复你的文件。

除了上述情况外，TROJ_CRIBIT.B 还会将桌面变成黑色背景加上白色文字，来通知用户目前状况。为了让分析更加困难，勒索软件 Ransomware 不会在系统内留下副本，所以很难取得样本来研究行为并确定其感染媒介。经过进一步的调查，趋势科技发现一个 FAREIT 信息窃取恶意软件变种“TSPY_FAREIT.BB”，它会下载“TROJ_CRIBIT.B”。这种变种还具备“从多种比特币钱包窃取信息”的能力，它会搜寻并尝试盗取文件信息。

和 CryptoLocker 一样，用户会被引导进入一个看来专业的网站来解密他们的文件。该网站实际上是深层网络的一部份，只能够通过 Tor 来连上，但攻击者已经周到的提供到 Tor2Web 的链接，这是一个可以让用户无须使用 Tor 就能连上深层网络网站的服务。他们被要求输入在勒索信中所提供的 BitCrypt ID 登录。（如下图）



【网站中所提供的 BitCrypt ID 登录窗口】

登录之后，用户被引导进入 BitCrypt 网页（它将自己描述为 Bitcrypt 软件公司），提供了用户如何回复信息的说明。然而，这需要支付 0.4 比特币（现在价值约等于 1500 元人民币）。网络犯罪分子甚至还在其网站上提供常见问答页面，如下图所示：

【网站上的常见问答页面】

BitCrypt 只是我们最近所看到许多 Bitcoin 相关威胁中的最新一个。虽然比特币的价值已经从去年年底的巅峰下降了，但它的价值还是足够大到值得作为窃取的目标——无论是利用 Bitcoin 窃取恶意软件的形式（像 BitCrypt），或是更大的攻击形式，例如将目标放在交易所（像是 Mt. Gox 和 Vircurex）。

趋势科技建议比特币用户可采用“离线电子钱包”管理比特币，将电子钱包储存在一个没有网络连接且安全的地方，并经常离线备份重要信息，避免被窃取并遭到勒索。此外，用户还需要养成良好的网络安全习惯，不要随意点开未知发送者的邮件附件，也不要随意访问未知的国外站点（特别是黄色站点或是视频下载站点）。

除了以上这些措施之外，建议用户最好安装趋势科技 PC-cillin 2014 云安全版等信息安全软件，以进行更周密的安全防护。PC-cillin 2014 云安全版软件采用了全球独家“主动式云端拦截技术”，能够主动防御并阻挡病毒入侵电脑，并在全球用户联动的环境中，实现全球威胁实时检测，甄别出隐藏的安全威胁，帮助用户安享数字生活。

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn 。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。

趋势科技 PC-cillin 零售门店信息

区域	门店名称（席位号）	门店地址
安徽区	蚌埠万达普通仓	安徽省蚌埠市东海大道 4399 号万达广场内街 2 楼 2012 铺
安徽区	合肥包河万达普通仓	安徽省合肥市合肥市马鞍山路 130 号万达广场内街 2-69 铺
安徽区	合肥天鹅湖万达普通仓	安徽省合肥市蜀山区南二环路 3818 号天鹅湖万达广场 2-38 铺
华南区	福州万达普通仓	福建省福州市仓山区浦上大道仓山万达广场 2-39+商铺
华南区	晋江万达店普通仓	福建省晋江市世纪大道 888 号万达广场 2-66 铺
华南区	莆田万达店普通仓	福建莆田市城厢区荔华东大道 8 号万达广场 1 号门 2 楼 2059 铺美承数码
华南区	泉州万达店普通仓	福建省泉州市丰泽区宝洲路 689 号 2-53 铺
华南区	温州万达店普通仓	温州市龙湾区永中街道永定路 1188 万达广场 2007B、2008 铺
华南区	厦门万达普通仓	福建省厦门市湖里区仙岳路 4666 号厦门湖里万达广场 230，231 铺位
华中区	成都金牛万达店普通仓	四川省成都市金牛区一环路北三段 1 号万达广场三楼 3036A，3036B
华中区	汉街店普通仓	湖北省武汉市中央文化区商业步行街汉街 J2-2-8 号商铺
华中区	汉口凯德广场普通仓	武汉市硚口区中山大道 238 号 凯德广场武胜路 01 层 16-17 号
华中区	经开万达店普通仓	湖北省武汉经济技术开发区东风大道 111 号经开万达广场室内步行街 2-63，2-65 号
华中区	菱角湖万达普通仓	湖北省武汉市江汉区菱角湖万达广场室内步行街 2-37-38-39 号
华中区	绵阳万达店普通仓	四川省绵阳市涪城区花园路 9 号万达广场二楼 2018
华中区	武汉大洋店普通仓	湖北省武汉市江汉区中山大道 890 号大洋百货 B1F
华中区	武汉三星专卖店普通仓	武汉市洪山区珞瑜路 100 号广埠屯资讯广场 B 座一楼三星专卖店
华中区	襄阳民发店普通仓	湖北省襄樊襄阳市樊城区长虹路 16 号，长虹路与人民路交叉口处民发-城市印象一层 108 号
华中区	襄阳万达普通仓	湖北省襄樊襄阳市高新区长虹北路襄阳万达广场室内步行街 132 号
华中区	宜昌万达普通仓	湖北省宜昌市伍家区夷陵大道 188 号宜昌万达广场室内步行街 103 号商铺
华中区	郑州万达普通仓	河南省郑州市二七区大学南路 8 号万达广场二楼 2001 铺
江苏区	常州丰臣店普通仓	常州新北区三井街道通江中路 108 号（丰臣国际广场）主题区 3 号楼 101,201 号
江苏区	常州万达店普通仓	江苏省常州新北去通江中路 88 号新北万达广场 3010、3011、3012
江苏区	江阴虹桥店普通仓	江苏省江阴市澄江镇虹桥北路 11 号
江苏区	苏州观前店普通仓	苏州市干将东路 886-900 号 204 室

江苏区	无锡惠山万达店普通仓	无锡市惠山区吴韵路 321 号万达广场 2005、2006A 号铺美承数码馆
江苏区	宜兴店普通仓	江苏省宜兴市宜城镇通贞观西路 1 号（人民中路交叉口)
江苏区	宜兴万达数码馆普通仓	无锡市宜兴市东虹路 550 号万达广场 2003B/2003A 号铺
江苏区	张家港国购店普通仓	江苏省张家港市沙洲中路步行街 2 号 （国购负一层屈臣世对面）
南京区	淮安万达店普通仓	江苏省淮安市清河区翔宇中路 169 号万达广场 1 层 106A、107、108 号商铺
南京区	南京新街口店普通仓	江苏省南京市白下区汉中路 1 号 南京国际金融中心负一层 A2-A4
南京区	南京珠江路 291 号三星店普通仓	南京市玄武区珠江路 291 号
南京区	泰州万达店普通仓	江苏省泰州市海陵区济川东路 232 号万达室内步行街二层 2036 号
南京区	徐州万达店普通仓	江苏省徐州市云龙区和平大道 58 号二楼 2083 室
南京区	盐城店普通仓	江苏省盐城市人民中路 9 号宝莱百货一楼
上海区	宝山万达普通仓	上海市宝山区一二八纪念路 878 弄,万达广场 3 楼 327 铺
上海区	杭州百脑汇 1C07 佳能普通仓	浙江省杭州市教工路 23 号百脑汇 1 楼 1C07
上海区	杭州中心店普通仓	浙江省杭州市西湖区文三路 345 号 1-2 楼 C 铺位
上海区	嘉定罗宾森普通仓	上海市嘉定区城中路 138 号罗宾森广场 1 楼美承
上海区	江桥万达普通仓	上海市嘉定区金沙江西路 1051 号 万达广场 1 号门 2 楼 2093，2094
上海区	昆山百盛店	昆山市前进西路 300 号昆山中茵世茂百盛一楼 L1-1 号美承数码
上海区	南汇万达普通仓	上海市南汇周浦镇沪南公路 3449 号二楼 218 室（万达广场）
上海区	太仓店普通仓	江苏省太仓市南洋广场 A 区 1 楼 22 室人民南路上海路口二楼
上海区	太仓南洋店普通仓	江苏省太仓市人民南路 96 号南洋广场 A-1-10~11-A-2-10~12 商铺
上海区	太仓万达数码馆普通仓	江苏省太仓市上海路 288 号万达广场 2037 铺美承数码