安天周观察

安天官方微博　安天官方微信

主办：安天　2017 年 12 月 04 日 (总第 114 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布针对 VBA 宏勒索软件 BluFish 的检测分析与有效防护报告

传统勒索软件的重要功能模块多半为二进制可执行程序，而脚本仅作为加载器使用。安天在近期捕获的样本中发现了一种新型的完全使用 VBA 宏编写的文件加密勒索软件家族 BluFish。不同于其他勒索软件（如 Locky），其加密文件时不会改变文件名称，亦不会修改文件结构，而仅对 Microsoft Word 文档内容进行加密，其勒索信息将连同加密内容一起显示在 Word 文档内容中。

该勒索软件通过感染 Microsoft Word 的 Normal 模板进行传播，并在每个被感染的 Word 文档中增加名为“qkG”的恶意宏代码。当用户启用宏时，normal.dot 模板就会被感染，当用户关闭文档时，它就会将文件加密。

如果用户打开 Word 文件后，看到如图 1 中的字样，表明已经被感染。这与其他勒索软件感染后导致 Office 文件丢失，扩展名改变，或打开乱码的现象有明显差异。

安天对捕获的病毒样本的加密过程进行了深入分析，发现该病毒的执行流程如下：

1、修改 Word 安全属性设置，包括取消保护视图、降低宏安全级别等；

2、感染 Normal 模板，添加 Document_Close() 函数，将当前文档自身的恶意宏代码复制到新添加的 Document_Close() 函数中，通过 Normal 模板实现传播；

3、感染打开的活动文档，增加 Document_Open() 函数，将 Normal 模板中的恶意宏代码复制到新添加的 Document_Open() 函数中；

4、加密文档，通过简单的异或进行加密，将加密后的内容转化为 16 进制字符串保存至文档中，并在文档中添加勒索信息，包括赎金、支付地址、联系方式。

从目前的情况来看，该家族勒索软件处于编写者技术摸索进化阶段，并不完全成熟，但 VBA 宏编写勒索软件后续可能成为一种典型手法。技术成熟后，此类攻击可能大规模爆发，因此需提高警惕。

安天建议用户警惕第三方未知来源 Office 文件，切勿轻易打开或运行未知来源的文件；为防止勒索软件造成严重损失，应及时备份重要文档或资料；在终端安装可靠的安全防护产品，如内嵌安天自主先进的 AVL SDK 威胁检测引擎的安天智甲终端防御系统。

经验证，安天智甲在 BluFish 勒索软件家族出现前的版本即可有效拦截该病毒的攻击如图 2 中所示。

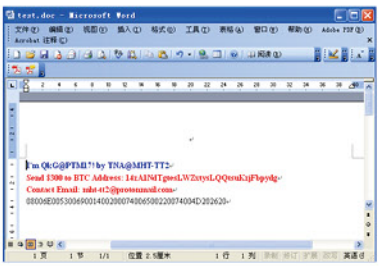

图 1：加密后的文件

图 2：安天智甲针对 BluFish 家族样本进行主动防御

报告详见

■ 牛津剑桥俱乐部电脑硬盘被盗，5000 名会员信息丢失

在 11 月 16 日，牛津剑桥俱乐部（Oxford and Cambridge Club）的一个备用电脑硬盘遭到了盗窃。硬盘中存储有 5000 多名会员以及 100 多名工作人员的个人信息，包括会员姓名、家庭住址和电子邮箱地址、电话号码、出生日期、照片和一些银行账户细节。这可能会导致一次大规模的数据泄露事件。

该俱乐部创立于 1830 年，总部位于伦敦市中心。如果不出意外，这应该是世界上拥有最多聪明人的私人俱乐部。因为，要成为该俱乐部的会员首先必须是牛津大学或剑桥大学的毕业生；然后，还需要其他会员的推荐，并经过严格的筛选。

此根据调查显示，菲利普亲王和查尔斯王子也都是该俱乐部的会员。所幸的是，他们似乎并没有受到此次盗窃事件的影响。

俱乐部的发言人 Alistair Telfer 表示，俱乐部目前已经联系了大都会警方，并聘请了私人侦探对此次事件进行调查。警方目前正在调取俱乐部的监控记录，用以查看在案发的这段时间都有什么人进出俱乐部。

所幸的是，根据 Telfer 的说法，在被盗窃的硬盘中并不包含任何借记卡和支付卡信息，并且硬盘也设置了多层安全措施保护，这使得盗窃者获取到敏感信息的几率很小。

俱乐部已经向所有会员发出了电子邮件，提醒他们留意自己的银行账户是否存在异常交易记录，并警惕可能的钓鱼欺诈式骗局。

每周安全事件

类 型	内 容
中文标题	航运巨人克拉克森遭遇安全漏洞
英文标题	The Shipping Giant Clarkson has suffered a security breach
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	全球最大的航运服务提供商之一 Clarkson 公开披露了一项安全漏洞。克拉克森证实黑客可能会释放一些被盗的数据，由于正在进行的执法调查，它没有提供进一步的细节。 该公司披露的信息表明，网络罪犯勒索公司要求支付赎金，以避免其数据泄露在网上。 根据克拉克森的说法，这些黑客入侵了一个用户账号，以此这个航运巨头的系统。 事件发生后公司已经关闭了帐户，并已开始通知受影响的客户和个人。 该公司曾期待网络犯罪分子星期二公布部分被盗数据，但目前还没有发生。该公司还表示，一直在对其架构的安全性进行审查，并宣布了新的 IT 安全措施。
链接地址	http://securityaffairs.co/wordpress/66172/cyber-crime/clarkson-security-breach.html

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 9 个移动平台恶意代码和 4 个 PC 平台的恶意代码值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	RiskWare/Android.uutf.a[exp,rog] 2017-11-27	该应用程序包含风险代码，运行后释放广告子包，加载广告，造成用户资费消耗，请谨慎使用。（威胁等级中）
		Trojan/Android.Facestealer.a[prv,exp,fra] 2017-11-27	该应用程序为虚假应用，诱导用户输入 Facebook 账号密码并短信转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.snowflake.a[prv,rmt,bkd] 2017-11-29	该应用程序包含恶意代码，存在后门，运行后会加载子包，接收远程控制命令，监听用户手机，窃取用户短信、联系人、通话记录、wifi 信息、地理位置信息等手机各项信息并上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.tpapay.a[exp,rog] 2017-11-29	该应用程序伪装正常应用，包含恶意代码，运行后联网加载脚本文件，私自发送注册短信和订阅扣费服务，造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.lakinerat.a[prv,rmt] 2017-11-29	该应用程序是一款服务器使用的远控客户端程序，运行后会与服务端进行远程通讯，请立即卸载。（威胁等级高）
		RiskWare/Android.fakeTelegram.a[exp] 2017-11-30	该应用程序重打包 Telegram，植入恶意代码下载子包并动态加载，存在一定安全隐患，请谨慎使用。（威胁等级中）
		Trojan/Android.CoreSystemSpy.a[prv,sys,spy] 2017-12-01	该应用程序伪装系统应用，运行隐藏图标，诱导用户开启通知读取权限，监控通知栏获取短信、聊天记录等隐私上传，同时监听来电和位置信息，上传通话录音和位置信息，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃样本	Trojan/Android.CPUMiner.c[exp,rog]	该应用程序运行诱导激活设备管理器，隐藏图标，上传设备 CPU 等参数信息，后台私自挖矿，会占用设备内存，同时造成损耗，建议卸载。（威胁等级高）
		Trojan/Android.spymessage.f[prv,exp]	该应用程序伪装成号码定位系统，私自拦截、上传短信，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft.NET SOAP WSDL 解析器代码注入漏洞（CVE-2017-8759）	该漏洞影响所有主流的 .NETFramework 版本。由于主流的 Windows 操作系统都默认内置了 .net 框架，黑客通过 Office 文档嵌入远程的恶意 .net 代码进行攻击，所有的 Windows 系统及安装了 Office 办公软件的用户都会受到影响。（威胁等级高）
	较为活跃样本	Trojan[Backdoor]/Win32.DDOS	此威胁是一种后门木马类程序，它可以连接远程服务器接受攻击者恶意操作，主要包括 DDoS 攻击和升级下载等功能。（威胁等级中）
		Trojan[Backdoor]/Win32.Danti	此威胁是一个后门家族。该家族的样本在执行后会联络控制端进行通信，将自身的信息传送给控制端，并接受控制端的控制命令。（威胁等级中）
		Trojan[Backdoor]/Linux.Mayday	此威胁是一种木马类后门程序，运行于 linux 平台上。它可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级中）

八个低成本或免费威胁情报来源

Steve Zurier / 文　安天技术公益翻译组 / 译

组织知道他们需要认真对待威胁情报，但是对于去哪里找可靠的信息并不是很清楚。虽然几乎所有的安全行业厂商网站都提供最新威胁的信息，但是有些网站的内容更好一些。在本文中，我们将推荐八个信息最丰富、最有用的网站。

我们邀请 Rosint Labs 总裁罗塞尔·萨夫兰（Roselle Safran）与我们一起总结网站清单。萨夫兰在网络安全方面拥有丰富的经验，曾在奥巴马政府的总统行政办公室和国土安全部任职多年。

萨夫兰提供了一些联邦政府网站，还提供了一些鲜为人知的、追踪勒索软件和恶意软件的网站。我们与萨夫兰联手制定了一份清单，旨在帮助新手获取他们需要的威胁情报，并为经验丰富的安全专家提供一些有用的情报。

国土安全部：自动信标共享网站

国土安全部（DHS）成立了免费的自动信标共享（AIS）网站，便于私营公司与联邦政府共享网络威胁信标。典型的威胁信标是诸如恶意 IP 地址或钓鱼邮件的发件人地址等信息。国土安全部旨在创建这样一个生态系统：一旦有公司或联邦机构发现攻击企图，就会立即与所有 AIS 参与者共享威胁信标。联邦政府官员说，虽然 AIS 不能清除复杂的网络威胁，但它能够清除复杂程度较低的攻击，使得联邦政府和私营公司能够专注于更具危害性的针对性攻击。

FBI：InfraGard 门户网站

联邦调查局（FBI）的 InfraGard 门户网站是一个信息交换中心，公共和私营部门可在此共享信息，以保护美国的关键基础设施。政府将关键基础设施分为从国防工业基地、制造业到水坝等 16 个行业。该网站提供有关 16 个行业相关事件的新闻，另外还附有网络犯罪和网

络逃犯的链接，其中包含最新的攻击和联邦调查局正在追踪的潜在威胁的信息。

信息共享和分析中心国家委员会

信息共享和分析中心（ISAC）国家委员会成立于 2003 年，ISAC 的概念是在 1998 年首次提出的。如今共有 24 个 ISAC，其中一些，如金融服务 ISAC（FS-ISAC），加盟费很高。但是很多 ISAC 提供低成本或免费的威胁情报。其基本思想是：每个关键基础设施部门都设有负责监视和发现该行业威胁信息的组织。大多数 ISAC 都提供全天候的威胁警报和事件报告，许多 ISAC 也为其部门设置威胁级别。请点击此链接查找适用于您所在行业的 ISAC。

Ransomware Tracker

Ransomware Tracker 是一个瑞士安全网站，由 @abuse.ch 管理，专注于追踪和监控与勒索软件相关的域名、IP 地址和 URL 的状态。它包括僵尸网络 C&C 服务器、传播站点和支付站点。通过使用由 Ransomware Tracker 网站提供的数据，托管服务提供商、ISP、国家 CERT、执法机构和安全研究人员可以获得勒索软件所利用的基础设施的信息，以及威胁源是否正在利用它们进行诈骗的信息。该网站还提供缓解勒索软件攻击的指导，以及需要在网络边界拦截的勒索软件列表。

Spamhaus 项目

Spamhaus 项目成立于 1998 年，是一家位于日内瓦和伦敦的国际非营利组织，负责追踪垃圾邮件和相关网络威胁，如网络钓鱼、恶意软件和僵尸网络。虽然 Spamhaus 以发布 DNS 拦截列表为人所知，但是它还能够生成用于互联网防火墙和路由设备的特殊数据，如 Spamhaus DROP 列表、僵尸网络 C & C 数据以及 Spamhaus 响应策略区数据（用于 DNS 解析器，这是一种有助于防止数百万互联网用户点击网络钓鱼和恶意邮件中的恶意链接的工具）。

互联网风暴中心

互联网风暴中心（Internet Storm Center，ISC）成立于 2001 年，是继 Li0n 蠕虫之后安全社区进行合作的结果。如今，ISC 每天从覆盖 50 多个国家的超过 50 万个 IP 地址的传感器中收集数以百万计的入侵检测日志条目。ISC 是由 SANS 研究所支持的免费服务，其资金源于参加 SANS 安全教育计划的学生支付的学费。该网站提供了许多工具、教育播客、论坛和安全专业人士工作板的链接。

免费的反恶意软件网站

威瑞信《2017 年数据泄露调查报告》发现，51% 的数据泄露涉及恶意软件。以下网站对感染网络的主要恶意软件进行分析，可免费访问：virustotal.com，malwr.com，VirusShare.com。

厂商博客

厂商的最终目的是销售产品，但这并不意味着他们不会发布信息丰富的博客，这些博客是很不错的信息来源，可由此了解厂商发现的最新攻击和保护网络的措施。我们向您推荐以下厂商博客：Alien Vault、思科威胁研究博客、CrowdStrike 研究和威胁情报博客、火眼威胁研究博客、Palo Alto Networks Unit 42、Recorded Future 和 Windows 安全博客。

原文名称	8 Low or No-Cost Sources of Threat Intelligence
作者简介	Steve Zurier 是一位自由撰稿人，拥有超过 30 年的新闻和出版经验。
原文信息	2017 年 11 月 6 日发布于 InformationWeek 原文地址 https://www.darkreading.com/threat-intelligence/8-low-or-no-cost-sources-of-threat-intelligence-------/d/d-id/1330447
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

安天发布《勒索软件“Locky 变种 Lukitus”分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时注意并拦截到了一个 Lukitus 勒索软件，其为 Locky 勒索软件的一个新变种。Lukitus 加密受害者的照片、视频以及文档，并将文件的名称更改为随机字符和数字，然后加上 Lukitus 作为文件的后缀名。这种变体目前正在通过垃圾邮件分发，这些邮件的主题是“No subject >”或“电子邮件”——csi – 034183_mb_s_7727518b6bab2，邮件包含有 JS 文件的 zip 或 rar 附件。当这些 JS 文件被执行时，他们将从一个远程站点下载 Lukitus 可执行文件。一旦该文件被下载并执行，它将扫描计算机文件并加密它们。

该软件运行后遍历系统文件并加密，修改文件后缀名为 Lukitus，并在每一个文件夹下面新建一个 htm 文件，使用 explore.exe，打开 Lukitus.htm，显示勒索信息链接，使用 rundll32.exe，打开 Lukitus.bmp 图片，显示勒索信息。之后连接到 http://46.183.165.45/imageload.cgi、http://146.120.110.46/imageload.cgi 使用 POST 方式传送系统信息。Lukitus 在对计算机进行加密时，它将删除下载的可执行文件，然后显示一张勒索信提供如何支付赎金的信息，最后勒索赎金可通过连接“暗网”Tor 匿名网络与远程服务器支付。恢复加密文件的唯一方法是通过备份，如果幸运的话可以通过阴影卷副本恢复加密文件。虽然 Lukitus 确实试图删除阴影卷副本，但很少有勒索软件可以做到。由于这一点，如果没有可用的备份，建议尝试从阴影卷副本中恢复加密的文件。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。目前，安天追影产品已经实现了对该类恶意代码的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马病毒进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 YARA 自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据静态分析鉴定器和之籍呢学习鉴定器将文件判定为木马程序。

文件名	download.zip
文件类型	Archive/Phil_Katz.ZIP
大小	605 KB
MD5	D101D3CB6BDA74B4297C8BDFC1ED7085
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.TSGeneric
判定依据	静态分析

◆ 运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 文件元数据分析

描述	值
File Size	605 kB
File Type	ZIP
MIME Type	application/zip
Zip Required Version	20
Zip Bit Flag	0
Zip Compression	None
Zip Modify Date	1980:00:00 00:00:00
Zip CRC	0x6a5c65ba
Zip Compressed Size	619520
Zip Uncompressed Size	619520
Zip File Name	994f764ab463003ce57186ae4a14fd5eaa28a79fad884581fe7d1634dee4fe6d