安天发布《Farseer 木马家族样本分析报告》

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发现一个名为 Farseer 的恶意软件家族。该恶意软件专门针对 Windows 操作系统构建，并且与 HenBox, PlugX, Zupdax, 9002, Poison Ivy 等恶意软件家族都有关联。

Farseer 家族的木马已发现三十多种，集中出现在 2017 到 2018 年。早期的 Farseer 木马通过 PDF 诱饵文档来触发执行，后期的则使用 DLL 侧载技术。这种技术会利用合法的、受信任的可执行文件来加载恶意代码。在一个近期样本中，攻击者利用 bscmake.exe，一个较老的微软可执行文件，是 Visual Studio 软件的一部分，当 bscmake.exe 运行时，它需要导入依赖文件 mspdb80.dll，而 mspdb80.dll 的运行需要导入 sys.dll。根据 Windows 系统在导入依赖文件时的搜索顺序，系统首先会在可执行文件的当前目录下查找文件，如果找到，直接将该文件载入内存。利用这一特性，攻击者将 Farseer 木马伪装成 sys.dll 放在 bscmake.exe 的当前目录下，从而触发木马执行。而 bscmake.exe 和 mspdb80.dll 都是合法的文件，并未被篡改。sys.dll 运行后会加载“stub.bin”文件到内存中，stub.bin 是一个经过压缩加密的 payload，在内存中解密后便开始恶意代码的执行。stub.bin 会从“sys.dat”文件中读取配置信息，该文件保存了 C2 服务器地址和一些其他信息。

安天 CERT 提醒广大政企客户，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

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程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、文件来源信息鉴定器、数据证书鉴定器、文件元数据鉴定器鉴定器、聚类分析鉴定器、防病毒引擎鉴定器、动态（WinXP）鉴定器、动态（Win7 x86）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 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	271e29fe8e23901184377ab5d0d12b40d485f8c404aef0bdcc4a4148ccbb1a1a
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	299 KB
MD5	DA4E06996A1F242539E74CA06263192C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Dropper]/Win32.Agent
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=DA4E06996A1F242539E74CA06263192C

◆ 运行环境

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

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
延时	★★★	删除自身	★★★★

◆ 常见行为

行为描述	危险等级	行为描述	危险等级
获取驱动器类型	★	Run 自启动	★
打开自身进程文件	★	对照发现设置自启动	★
访问文件尾部	★	获取当前光标位置	★
读取自身	★★	DNS 请求	★
释放 PE 文件	★	连接网络	★
创建挂起进程	★★	获取计算机名	★
创建特定窗体	★	获取主机内存信息	★★
获取驱动加载权限	★	疑似桌面控制	★
壳行为填充导入表	★★	疑似查找浏览器进程	★★

◆ 进程监控

PID	创建	命令行
1356	target.exe	"c:\eb3bc605825b4234b3749bb0b71d62bb\share\target.exe"
1440	explorer.exe	C:\WINDOWS\Explorer.EXE
.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 04 月 29 日 (总第 181 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天态势感知平台再获认可 | 两项目入选工信部《网络安全技术应用试点示范项目名单》

近日，工业和信息化部网络安全管理局发布了《网络安全技术应用试点示范项目公示名单》，对经过专家评审的 101 个网络安全技术应用试点示范项目予以公示，安天申报的黑龙江省网信办态势感知与监测预警平台即《网络安全态势感知和应急处置平台》项目（第 53 项）、与中国民航大学共同申报的《民航网络与信息安全管理平台》项目（第 73 项）成功入选。

安天网络安全态势感知可视化平台

态势感知在信息系统安全积极防御体系中对提供响应决策、支持保障业务弹性和风险控制至关重要。安天态势感知平台分为面向网信主管部门和职能部门的“监测型态势感知平台解决方案”，以及面向重要信息系统及关键信息基础设施的“战术型态势感知平台解决方案”。本次安天入选的两个态势感知平台项目，是安天监测型态势感知平台的重要案例。安天以帮助客户促进信息共享、融合，有效监测网站安全为宗旨，全面动态的掌握网络威胁情况，准确感知网络安全态势，实现网络安全威胁的有效预警、响应，做到“抵近部署，集中感知，有效防护，快速响应”。

截至目前，安天监测型态势感知平台已先后获得中国信息安全产业年度“优秀创新型产业解决方案”、中国网络安全产业联盟“2018 年网络安全解决方案优秀奖”、“金帽子”年度优秀安全产品奖等多个奖项，本次两个项目的入选再度体现了行业和主管部门对安天监测型态势感知平台产品的认可。

安天是引领威胁检测与防御能力发展的网络安全国家队，依托自主先进核心技术与安全理念，致力为战略客户和关键基础设施提供整体安全解决方案。安天产品和服务为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置等基础能力。安天为客户建设实战化的态势感知体系，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，赋能客户筑起可对抗高级威胁的网络安全防线。

俄罗斯黑客利用 TeamViewer 攻击部分驻欧大使馆

近日，Check Point 研究人员发现了以欧洲政府财政部官员和部分国家驻欧大使馆代表为目标的网络攻击行为。攻击始于伪装成美国绝密文件的恶意 XLSM 附件，启用恶意宏后将提取合法 AHK 脚本，通过向 C2 服务器发送 POST 请求，来通过 URL 下载并执行另外三个 AHK 脚本，它们可分别实现拍摄受害者 PC 的屏幕截图、受害者的用户名和计算机信息和下载恶意版本 TeamViewer 并执行，将以上数据及 TeamViewer 登陆凭据发送到 C2。恶意 TeamViewer DLL 通过 DLL 侧加载技术加载，通过连接程序调用的 Windows API 来添加更多恶意功能。研究人员目前发现受攻击的国家和地区有尼泊尔、圭亚那、肯尼亚、意大利、利比里亚、百慕大、黎巴嫩，归因分析发现诱饵文档中包含西里尔语元素，例如工作簿名称，还追踪到似乎是该活动中使用工具的创建者，他是名为“EvaPiks”的暗网在线俄语黑客，因此研究人员表示幕后攻击者可能是出于经济动机的黑客团体。

（原文链接：https://research.checkpoint.com/finteam-trojanized-teamviewer-against-government-targets/）

尊敬的读者：
2019 年五一假期即将来临，《安天周观察》将于五一期间休刊一期，恢复出版时间为 2019 年 5 月 13 日。感谢所有读者对《安天周观察》一直以来的支持与关注！

2019 年 4 月 29 日

每周安全事件

类 型	内 容
中文标题	暗网出现新型勒索软件定制服务 INPIVX
英文标题	New INPIVX Service May Change the Ransomware Game
作者及单位	Ionut Ilascu
内容概述	研究人员发现了正在 Tor 网站上推广的一项名为 Inpivx 的新恶意服务，该服务为缺乏开发恶意软件并构建管理面板的技术能力的恶意攻击者提供了便利。该服务用 C++ 编写的，可以通过 Windows 10 在 Windows XP 上运行，仪表板采用 PHP 编码。与勒索软件即服务（RaaS）方法不同，它可以直接提供恶意服务，根据价格提供使用对称或“AES 加密 +RSA 公钥”加密文件的恶意软件源代码，以及管理仪表板，还允许对代码进行自定义修改。勒索软件加密受害者文件后，仪表板将显示感染状态概述，快速查看包括加密文件总数、勒索软件安装、受感染操作系统及其地理位置的详细信息，客户端部分显示受害者 id、操作系统、个人赎金价格、解密密钥和当前支付状态。仪表板还提供简单聊天功能。
链接地址	https://www.bleepingcomputer.com/news/security/new-inpivx-service-may-change-the-ransomware-game/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码值得关注

关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.hdfour.a[exp,rog] 2019-04-20	该应用程序伪装成其他应用，程序运行会私自联网下载 js 脚本并加载执行，私自发送短信，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.9rpn.a[prv,exp] 2019-04-21	该应用程序安装无图标，后台获取用户短信箱内容、联系人、通话记录、网络参数、手机号、是否 root、地理位置、手机固件信息等隐私信息并联网上传，会造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级高）
		Trojan/Android.InfectionAds.a[exp,rog] 2019-04-25	该应用程序运行后加载恶意子包，联网获取感染应用列表，向感染应用和广告 sdk 中植入恶意代码，推送广告，私自下载并利用系统漏洞静默安装，造成用户资费损耗，建议卸载。（威胁等级中）
	较为活跃的样本	RiskWare/Android.Zlbocai.a[rog]	该应用程序是一款线上赌博游戏，可以通过微信等方式进行充值，可能给用户的财产带来较大风险，且难以保障财产权益，建议谨慎使用。（威胁等级低）
		Trojan/Android.daohao.a[prv]	该应用程序为盗号测试应用，会通过短信和联网上传用户输入的账号密码，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.FakeIns.b[prv,rog]	该应用程序伪装正常应用，运行访问钓鱼页面，诱骗用户填写社交账号密码并后台上传，导致用户隐私泄露，请立即卸载。（威胁等级中）
		Trojan/Android.FakeFB.ab[prv]	该应用程序伪装成 facebook 相关应用，诱导用户输入账号密码并发送到指定号码，造成用户隐私泄露，建议卸载。（威胁等级低）
		RiskWare/Android.WZHQ.a[rog,exp]	该应用程序是色情网站网址获取工具，运行联网获取色情网址，其内容可能影响用户身心健康，请注意提示信息，使用绿色健康软件。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft XML 远程代码执行漏洞（CVE-2019-0790）	当 Microsoft XML Core Services 分析器处理用户输入时，存在远程代码执行漏洞。攻击者需要诱使用户点击电子邮件或即时消息中的链接诱使用户访问存在恶意代码的网站。当 Internet Explorer 分析 XML 内容时，攻击者可以远程运行恶意代码控制用户的系统。（威胁等级高）
	较为活跃样本	Trojan[Ransom]/HTML.Agent	此威胁是一种利用浏览器漏洞的木马家族。该类型的家族样本在执行后可以启动勒索软件来对系统中的文件进行加密，从而要求用户支付赎金来解密文件。（威胁等级高）
		Trojan/Win32.Gofot	此威胁是一种具有窃密行为的木马家族。该家族的样本在执行后会连接远程服务器以发送其在用户设备上收集到的数据。（威胁等级中）
		Trojan[Packed]/Win32.Mentiger	此威胁是一种具有窃密行为的木马家族。该家族的样本通常以加壳的形式存在。该家族的样本在执行后会收集用户的数据，并通过网络回传给特定的服务器。（威胁等级中）
		GrayWare[AdWare]/JS.Agent	此威胁是一种具有广告件行为的灰色软件家族。该家族的样本利用了 iframe 的漏洞，在 iframe 中嵌入 JS 脚本并通过此方式弹出广告。（威胁等级低）
		Trojan[Ransom]/Win32.Bitman	此威胁是一种勒索软件家族。该家族具有别名 Tescrypt。该家族的样本执行后会加密计算机中的文件，并打开浏览器转向勒索信网页，要求用户支付赎金解密自己的文件。（威胁等级高）

今年第一季度，定制的针对性勒索软件攻击成为热门趋势。

Coveware 公司的一份新研究报告显示，虽然勒索软件攻击的数量出现下降，但与该威胁相关的其他指标都呈上升趋势，例如：更高的赎金、更大的停机损失、更长的恢复时间等。

该报告分析了 2019 年第一季度勒索软件的攻击情况。总体而言，受害者支付了更高的赎金，经历了更长的停机时间和恢复时间。

Coveware 公司表示，这些趋势大多是因 Ryuk、Bitpayment 和 Iencrypted 等勒索软件的出现所致，这些勒索软件通常针对大型企业执行定制攻击。

现在，大多数勒索软件攻击都是针对性的。要想有效地防御它们，需要部署多层安全方案、实施访问控制并进行数据备份。

以下是今年第一季度勒索软件攻击的六大特点。

赎金金额越来越高

与机会主义攻击的受害者相比，针对性定制攻击的受害者被要求支付更高的赎金以恢复数据。在 Coveware 事件响应小组处理和解决的案件中，受害者支付的平均赎金金额飙升 89%，从 2018 年第四季度的 6733 美元增加至 2019 年第一季度的 12762 美元。

手动攻击增加

Securonix 公司威胁研究主管表示，相比于自动攻击，攻击者更多地利用获取的登录凭证对目标企业执行手动攻击。他们专门攻击高价值系统，如电子邮件服务器、数据库服务器、文档管理服务器和面向公众的服务器。

“在某些情况下，勒索软件攻击是以半自动化、人工辅助的方式进行的。这在传统的勒索软件攻击中并不常见，”他说，“这会对受害企业造成更大的损失和破坏。”

研究人员认为，在针对铝生产商挪威海德鲁（Norsk Hydro）的破坏性攻击中，攻击者手动将 LockerGoga 勒索软件在该厂商的计算机网络中传播。

停机时间增加

与之前相比，在今年第一季度，企业遭受勒索软件攻击后的平均恢复时间急剧增加。

在 2018 年第四季度，平均恢复时间为 6.2 天；而在 2019 年第一季度，这一时间增加至 7.3 天。Coveware 发现，这与 Ryuk 和 Hermes 等难以解密的勒索软件的活动增加有关。与其他种类的勒索软件相比，Hermes 等勒索软件也造成了更高的数据丢失率。

Coveware 指出，导致恢复时间延长的另一个因素是：针对备份数据的攻击增加了，它们要么被彻底删除掉、要么也被加密。

停机成本增加

幸运的是，绝大多数勒索软件受害者并未像挪威铝业巨头那样遭受巨额损失——在攻击发生后的一周内损失高达 4000 万美元。

但是，各公司在一次攻击中的平均停机成本大致相同，约为 65645 美元。根据企业所在的行业和地理位置，成本会有较大的差异。Coveware 表示，未投保网络或业务中断险的公司受创最为严重。

“停机通常是最严重的损失，而处于高速运转供应链中的公司，或者具有高可用性服务级协议要求的公司受到的影响最为严重。”西格尔说。他指出，如果托管公司违反了正常运行、可用性和保障承诺，他们就会面临损失客户的风险。

制造行业成为勒索软件的攻击目标

没有任何企业 / 行业可以完全避免勒索软件攻击。但 Malwarebytes Labs 一主管表示，与其他行业的公司相比，制造行业的公司遭受的攻击更为严重。

“很难说这是攻击者有意为之，还是这类制造业公司自身的安全措施所致。”他指出，不管怎样，对于攻击者来说，制造行业的公司都是极具吸引力的目标。那些正常的生产和运营遭勒索软件攻击后，导致生产效率降级或破坏的制造商更有可能支付赎金。

受害者支付赎金主要是为了恢复数据

安全和执法官员强烈建议勒索软件受害者不要支付赎金来恢复数据。他们认为，满足攻击者的赎金要求只会激励更多的勒索软件攻击。

即便如此，Coveware 的数据显示，在第一季度，支付赎金的公司能够获得解密密钥并恢复 96% 的数据。这比 2018 年第四季度增加了 3%。平均而言，支付赎金的受害者能够恢复 93% 的数据。

但是，勒索软件的种类不同，数据的恢复率会有很大的差异。例如，Ryuk 勒索软件的受害者通常只能使用解密密钥恢复约 80% 的数据；而在 GandCrab 攻击中，受害者几乎能够 100% 地恢复数据。Coveware 在报告中指出，造成这种差异的原因包括：不同勒索软件使用的加密方法不同、有瑕疵的解密工具、加密文件被修改等。

并非所有支付赎金的公司都拿到了解密密钥。一些攻击者，如 Dharma 勒索软件家族背后的组织，即使收到赎金，也往往不给受害者提供解密工具。“而使用 Ryuk 等勒索软件的攻击者几乎总能提供解密工具，但该工具的功效相对较低。”西格尔说。

原文名称	6 Takeaways from Ransomware Attacks in Q1
作者简介	Jai Vijayan。Jai Vijayan 是一位经验丰富的技术记者。
原文信息	2019 年 4 月 18 日发布于 Dark Reading 原文地址 https://www.darkreading.com/attacks-breaches/6-takeaways-from-ransomware-attacks-in-q1/d/d-id/1334472
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。