安天发布《Major 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为Major的勒索软件变种，Major 勒索软件又名 Bmps 勒索软件，最早于 2019 年 4 月在波兰被发现，主要通过垃圾邮件进行传播，邮件附件包含一个 .tar 的压缩文件，该附件诱使用户解压 Major 勒索软件程序并执行。

勒索软件 Major 执行后，首先会加密计算机上的文件并修改桌面背景，在原文件名后追加名为“.（感染主机 ID）.ex_parvis@aol.com.AIR”的后缀。加密结束后，在每个被加密文件目录中和桌面创建一个名为“TRY_TO_READ.html”格式的勒索信，勒索信中包含勒索说明、三个联系邮箱地址和 USER_ID，受害者可通过邮箱发送 USER_ID 和被加密文件与攻击者进行交互，得知需要支付的赎金金额。Major 勒索软件变种使用“RSA+AES”算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。目前被加密的文件在得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、关联分析鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、来源信息鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、关联分析鉴定器、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	cd8701c501bd6c60f15b004e92b67485e24c3d558759563f2d81baf6ef3cfcc5
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	172 KB
MD5	052C8C332A4CC159D54D7C8524FA9134
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.DelShad
判定依据	反病毒引擎

◆操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
在启动时禁用 Windows 错误恢复	★★★★
删除全盘所有卷影副本	★★★★
查询系统硬盘大小	★★★
查询系统硬盘大小	★★★
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
壳行为填充导入表	★★
获取系统信息（处理器版本、处理器类型等）	★
连接网络	★
创建挂起进程	★★
.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019年11月18日(总第208期)试行 本期4版 微信搜索：antiylab 内部资料 免费交流

第二届“纵横”网络空间安全创新论坛在合肥召开

近日，第二届“纵横”网络空间安全创新论坛在合肥胜利闭幕，安天作为主要承办单位参与了一系列相关活动及交流研讨。在大会主论坛环节，方滨兴院士、何积丰院士等五位知名专家和奇安信董事长齐向东、安天集团董事长肖新光两位企业负责人发表主旨演讲，安天的主旨演讲分享了网空威胁猎杀的思考。

第二届“纵横”网络空间安全创新论坛 10 月 28 日在安徽省合肥市举办。来自中央网信办、国家机关、军委机关、各战区、各军兵种及院校等单位的 500 余名专家和代表，围绕贯彻落实习主席关于建设网络强国的重要指示，就深化网络空间安全领域“需求牵引、技术推动”，开拓科技兴军新局面，促进网络空间安全创新驱动，进行了深入研讨。

此次论坛由军事科学院、国防科技大学牵头，联合国家计算机网络应急技术处理协调中心、中国信息安全测评中心、安徽省委网信办、合肥市人民政府等单位共同主办，旨在催生一批网络空间安全理论和技术装备创新点，引领网络空间产学研力量更好地服务于网络空间安全。

与会院士和专家，围绕网络空间安全人才培养、网络空间自主创新与安全生态等，进行了 30 余次主题报告和研讨，深入交流思想、碰撞智慧，并探索出一批理论研究成果和有关发展对策与建议。

——转自中国军网

微信扫描二维码阅读原文

主要的 ASP.NET 托管提供商遭勒索软件 Snatch 攻击

主要的 ASP.NET 托管提供商 SmarterASP 在 11 月 9 日遭勒索软件 Snatch 攻击，其客户数包括 Web 服务器和后端数据库被加密。SmarterASP.NET 是一个拥有超过 44 万个客户的 ASP.NET 托管提供商。SmarterASP.NET 公司网站也在周六遭到攻击导致关闭，在周日重新恢复上线。该公司在声明中表示正在积极与安全专家合作，尝试解密用户数据。但目前服务器恢复工作进展缓慢，许多客户仍然无法访问其帐户和数据。目前尚不清楚该公司是否支付了赎金要求，还是正在从备份中恢复。

（原文链接：https://www.zdnet.com/article/major-asp-net-hosting-provider-infected-by-ransomware/）

Adobe 修复影响体验平台移动软件开发套件的缺陷

在发现不安全的默认设置后，Adobe 更新了其体验平台移动软件开发工具包 (SDK) 附带的示例配置文件。Adobe 所提供 SDK 作为模板，可供开发人员将其应用程序与各种平台上的 Adobe 云服务集成。研究人员在 2019 年 3 月注意到主应用程序配置文件 ADBMobileConfig.json 包含几个连接到 SSL/HTTPS 数据传输的不安全设置，这可能允许攻击者可以查看或修改由应用程序传输回 Adobe 的云服务的信息。Adobe 于最近发布了其移动 SDK 的更新版本，修复了该问题。

（原文链接：https://nakedsecurity.sophos.com/2019/11/11/adobe-fixes-sdk-weakness-affecting-mobile-apps/）

CISA 发布针对假日购物和网络钓鱼诈骗的安全警报

美国国土安全部的网络安全和基础设施安全局（CISA）已警告美国公民警惕恶意的假日活动和欺诈行为。随着各种假日的到来，网络诈骗活动也将开始活跃。大多数假日骗局都是通过网络钓鱼电子邮件进行，让受害者产生了恐惧或紧迫感。这种策略使得攻击者很容易获取个人信息或盗取钱财。攻击者会在信用卡读取器上安装窃取器设备或冒充慈善组织或执法机构，要求快速付款。除了窃取个人和财务信息外，攻击者还利用假日骗局来分发恶意软件。

（原文链接：https://cyware.com/news/cisa-issues-a-security-alert-for-holiday-shopping-and-phishing-scams-a87ec459）

Nautilus ATM 漏洞允许攻击者窃取现金和数据

安全研究人员发现了在美国广泛使用的 Nautilus ATM 机中的两个漏洞，这些漏洞允许攻击者窃取现金和客户数据。Nautilus Hyosung America 是美国最大的 ATM 提供商。通过获得与目标 ATM 相同的网络，研究人员能够完全控制该机器并绕过其安全措施。目前没有证据表明有人曾经利用过这些漏洞，该公司在美国已安装了超过 150,000 台 ATM 机。该公司已发布固件安全更新，以减轻可能的威胁。

（原文链接：https://finance.yahoo.com/news/security-researchers-discover-flaws-u-110000512.html）

每周安全事件

类 型	内 容
中文标题	黑客利用 vBulletin 0day 漏洞入侵 ZoneAlarm 论坛
英文标题	Hackers Breach ZoneAlarm's Forum Site — Outdated vBulletin to Blame
作者及单位	Swati Khandelwal
内容概述	网络安全软件公司 ZoneAlarm 的论坛遭到黑客入侵，泄露了论坛用户的数据。ZoneAlarm 为以色列网络安全公司 Check Point 的子公司，为用户提供了防病毒软件、防火墙和其它病毒防护解决方案。该公司发言人称，黑客利用了 vBulletin 论坛程序套件中一个严重的 RCE 0day 漏洞（CVE-2019-16759），来破坏 ZoneAlarm 的网站并获得未经授权的访问。此漏洞影响了 vBulletin 5.0.0 版本至最新的 5.5.4，项目维护人员在 9 月下旬了解该漏洞后，已针对该版本发布了补丁更新，但仅适用于最新版本 5.5.2、5.5.3 和 5.5.4。目前该公司已向受影响用户发送了邮件通知，邮件中建议论坛用户立即更改其论坛帐户密码，并告知黑客未经授权获得对其名称、电子邮件地址、哈希密码和生日的访问权。
链接地址	https://thehackernews.com/2019/11/zonealarm-forum-data-breach.html

每周值得关注的恶意代码和漏洞信息

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 平台的恶意代码和漏洞值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.FakeCJ.a[prv,fra] 2019-11-10	高	该应用程序伪装为刺激战场相关应用，窃取用户 QQ 账号密码，诱导用户付费购买会员，会造成用户隐私泄露和财产损失，请卸载。
		Trojan/Android.FakeSystem.bg[prv,exp] 2019-11-11	中	该应用程序伪装为系统应用，安装无图标，后台上传用户手机设备固件信息，加载推广广告，会造成用户隐私泄漏和资费消耗，建议卸载。
		G-Ware/Android.FakeTimer.a[prv,rog] 2019-11-12	低	该应用程序运行会私自获取用户设备 id、手机号码、精确地理位置信息等隐私并联网上传到指定网址，会造成用户隐私泄露，建议不要使用。
	较为活跃样本	Trojan/Android.SocketSpy.b[prv,rmt,spy]	中	该应用程序运行隐藏图标，与局域网服务端建立连接，通过远程指令执行窃取用户短信、发送短信、私自截屏上传、窃取用户定位、窃取联系人和通话记录等危险行为，造成用户隐私泄露，建议卸载。
		Trojan/Android.MobTracker.a[prv,spy]	中	该应用程序是间谍件，运行窃取用户联系人、短信、通话记录、通话录音、照片、PDF 文件、聊天记录等隐私，会造成用户隐私泄露，请卸载。
		Trojan/Android.FakeBank.y[prv]	中	该应用程序伪装为银行应用，运行访问钓鱼界面，诱导用户输入账户相关信息，会造成用户隐私泄露和财产损失，建议卸载。
		Trojan/Android.LockScreen.cs[rog,lck]	中	该应用程序运行隐藏图标，监听用户短信，锁定用户页面，影响用户手机的正常使用，建议卸载。
		RiskWare/Android.Joke.c[rog]	低	该应用程序伪装为正常应用，实际为整蛊程序，监听收件箱短信内容、播放色情音频，会影响用户正常使用，请卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Jet 数据库引擎远程代码执行漏洞（CVE-2019-1359）	高	当 Windows Jet 数据库引擎不正确地处理内存中的对象时，存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码，攻击者可以通过诱使受害者打开经特殊设计的文件来利用此漏洞。
	较为活跃样本	Trojan/Win32.Jorik	中	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获取用户的信息，并且与远程的控制端通讯并接受后续的控制，控制端具有对用户机器的完全控制权。
		Trojan[Ransom]/Win32.Locky	中	此威胁是一种可以加密用户文件的木马类程序。该家族样本一般通过 JS 脚本下载，运行后遍历磁盘，加密特定格式的文件并勒索比特币。
		Trojan[Downloader]/Win32.Gootkit	中	此威胁是一种可以下载恶意代码的木马类程序。该家族样本运行后连接远程服务器下载恶意代码并执行，可能会窃取用户信息并回传。
		GrayWare[Dialer]/Win32.PlayGames	低	此威胁是一种可以强制用户计算机浏览网站导致用户付费的灰色软件家族。该家族样本运行后下载并安装推广应用，在用户浏览网页时可以弹出广告、占用系统资源、收集用户信息，影响用户使用。
		GrayWare[AdWare]/MSIL.BrowseFox	低	此威胁是一种可以安装浏览器扩展的风险软件家族。该家族样本基于 32 位系统，运行后连接网络下载浏览器扩展并安装，占用系统资源，影响用户使用。

机器学习：随强大的能力引入了新漏洞

Ankit Tripathi/ 文 安天技术公益翻译组 / 译

机器学习（ML）为我们带来了自动驾驶汽车、机器视觉、语音识别、生物特征鉴别以及解锁人类基因组的能力。但是，它也为攻击者提供了许多新的攻击面和攻击方法。

ML 应用程序与之前的应用程序不同，因此了解其风险非常重要。攻击控制自动驾驶汽车网络或协调医院工作人员访问控制的模型，会造成什么后果？在这些情况下，模型被攻击可能会造成灾难性的影响。此外，企业还需要考虑更普通的威胁，例如“欺骗生物特征安全控制措施，向未经授权的用户授予访问权限”。

ML 仍处于早期发展阶段，其攻击向量尚不清楚。同样地，这方面的网络防御策略也处于起步阶段。虽然我们无法阻止所有形式的攻击，但是了解这些攻击发生的原因，有助于我们缩小响应策略的范围。

ML 安全的结构化方法

威胁建模是一种采用结构化方法来识别和应对威胁的安全优化流程。对于 ML 模型来说，ML 安全威胁建模有相同的作用。在构建和部署 ML 模型的早期阶段，企业可以用它识别所有可能的威胁和攻击向量。

在威胁建模时，企业需要考虑以下四个基本问题。

1. 攻击者是谁？

攻击者包括从民族国家攻击者，到黑客主义者再到流氓员工的各种类别。每类潜在攻击者都有不同的特征，需要采取不同的防御 / 响应策略。他们发动攻击的原因也各不相同，这就是为什么下述两个问题（为何发动攻击，动机是什么）如此重要的原因。

2. 为何发动攻击，3. 动机是什么？

攻击者攻击 ML 系统的原因各不相同，如破坏系统的机密性、完整性和可用性等。因此，防御策略应从“CIA 数据安全三要素”开始(CIA 是一个包含机密性、完整性和可用性的信息安全管理模型）。

• 机密性是指确保只有具有适当权限的人员才能访问信息。这类保护措施可以防止意图通过破坏训练数据来窃取敏感数据的攻击者。

• 完整性攻击可能会试图影响模型的行为，例如在人脸识别系统中返回误报。经常备份、数字签名和审计等保护措施可以确保信息不被篡改。

• 可用性攻击旨在降低 ML 模型的一致性、性能，或限制对 ML 模型的访问。良好的可用性实践（例如维护冗余服务器和应用数据丢失防护工具）能够确保：用户需要信息时信息是可用的。

4. 如何执行攻击？

ML 系统为传统程序中不存在的攻击开辟了新的途径。其中一种攻击是规避或对抗攻击。在这类攻击中，攻击者试图向 ML 模型中注入输入数据，以触发错误。在“人”看来，这些数据可能是没有问题的，但是细微的差异会导致 ML 算法出现偏离。

通过以下两种方法（白盒攻击和黑盒攻击）之一利用模型的内部信息，可以执行规避攻击。在白盒攻击中，攻击者可以获得有关模型的信息，这些信息可以直接获得，也可以从数据处理过程中不受信的参与者获得。在黑盒攻击中，攻击者对系统的内部运作一无所知，但可以通过反复探测并在背离学习模型的结果中发现模式，来识别漏洞。

新威胁向量

我们可以使用两个维度对 ML 攻击“方式”进行分类：推断和训练。在推断阶段的攻击中，攻击者能够获得有关模型和 / 或用于训练模型的数据的信息。攻击者无需直接访问系统，即可获得此类信息。诸如侧信道攻击和远程攻击之类的探索性技术，可以通过对输入的响应来推断 ML 系统的逻辑，从而使攻击者能够渗透已部署的 ML 系统；或者，通过数据投毒直接攻击硬件。

训练阶段的攻击试图学习并破坏模型。根据数据的可用性，攻击者可能会使用替代模型来测试潜在输入，然后再将其发送给受害者。

还有两种方法可以篡改模型。一种是注入法，即通过插入不受信组件来篡改现有数据，导致模型的结果不可信。另一种特别危险的方法是逻辑破坏，在这种方法中，攻击者会篡改学习算法本身。这种方法极为危险，攻击者可以有效地控制系统并指挥系统产生所需的任何输出。

ML 攻击

综合上述所有因素，我们可以确定针对 ML 生命周期不同阶段的三种攻击：

1. 规避攻击。这类攻击是最常见的，通常发生在推断阶段，旨在引入导致模型产生错误结果的输入。

2. 投毒攻击。这类攻击发生在推断阶段，旨在威胁数据的完整性和可用性。攻击者通过插入、删除或编辑决策点来更改目标模型的边界，从而篡改训练数据集。

3. 隐私攻击。这类攻击通常发生在训练阶段，其目的不是破坏训练模型，而是检索敏感信息。

除上述三种攻击外，在训练阶段、推断阶段或者这两个阶段，可能会发生其他多种攻击。例如锚点、模仿、模型提取、路径查找、最小成本、约束和梯度下降攻击等。

不幸的是，我们预计，随着 ML 成为主流，还会出现新的攻击类型。但是，了解基本漏洞和预防策略是对抗这些攻击的第一步。

原文名称	Machine Learning: With Great Power Come New Security Vulnerabilities
作者简介	Ankit Tripathi。Ankit Tripathi 是 IBM 安全和数据隐私顾问。
原文信息	2019 年 11 月 5 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/machine-learning-with-great-power-come-new-security-vulnerabilities/
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。