安天发布《SLUB 后门木马样本分析报告》

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种被称为 SLUB 的新型后门木马。该木马从 GitHub 获取要执行的命令，并通过 Slack 消息协作系统进行通信，主要窃取受害者的个人信息及通讯信息。

SLUB 后门通过水坑攻击的方式传播，当用户访问一个已被入侵的网站时，会被重定向到一段恶意代码，该代码会下载一个 DLL 文件，并通过 PowerShell 执行它。文件执行后，首先检查计算机上是否有杀毒软件，如果有则退出执行，否则下载并运行 SLUB 后门，最后，它还会利用 CVE-2015-1701 漏洞提升本地权限。SLUB 后门运行后，首先将自身复制到 \ProgramData\update\ 目录下，并添加为注册表自启动项，然后从 GitHub 上下载特定的“gist”段，提取行内的 cmd 命令并执行，执行结果会用嵌入的 tokens 发布到特定工作区的 Slack 私有信道上。SLUB 后门除了窃取计算机环境、运行的进程、屏幕截图、硬盘列表、用户列表等系统信息外，还会搜寻 Twitter, Skype, KakaoTalk, BBS 等通讯类软件的目录，窃取大量和受害者相关的个人信息。

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、数字证书鉴定器、文件元数据鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、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	43221eb160733ea694b4fdda70e7eab4a86d59c5f9749fd2f9b71783e5da6dd7
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	837 KB
MD5	F3004DDAEF5B8C18883E716DDA966141
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.RunDll
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=F3004DDAEF5B8C18883E716DDA966141

◆ 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

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
0.0.0.0	68	255.255.255.255	67
192.168.122.111	138	192.168.122.255	138
192.168.122.1	67	192.168.122.111	68
192.168.122.111	137	192.168.122.255	137
192.168.122.111	123	13.65.88.161	123

◆ 静态启发式检测

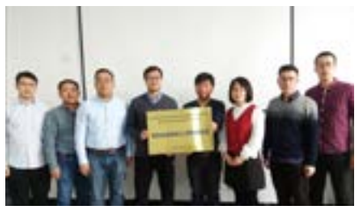
检测类型	检测点	详细说明
PE 结构	含有 tls 表	恶意代码作者常用的反调试技术。PE 结构中的 TLS 结构早于程序运行。
编译指令	未知壳	未被公开的壳，经常被恶意代码使用，用来保护恶意程序被查杀。
PE 结构	无版本信息并且不是 GCC 编译器	除 GCC 编译器外，常规编译器均默认包含版本信息。如果不是 GCC 编译器，并且不包含版本信息，显然是作者故意抹掉版本信息，逃避追查。

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 01 日 (总第 177 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天研究院携手吉林大学符号计算与知识工程教育部重点实验室共建网络安全威胁知识工程联合实验室

3 月 20 日，安天研究院与吉林大学符号计算与知识工程教育部重点实验室（以下简称吉大符号实验室）共同建立的“网络安全威胁知识工程联合实验室”在吉林大学计算机科学与技术学院大楼举行揭牌仪式，并召开了首次联合实验室学术交流会。

吉大符号实验室副主任张永刚主持揭牌，吉大符号实验室主任、网络威胁知识工程联合实验室联席主任杨博教授与安天研究院基础引擎研发部技术负责人童志明为揭牌仪式致词。吉大符号实验室吴春国副教授、赖永副教授，安天研究院院长助理、高级安全研究员赵超，安天驻长春技术负责人刘锦兰等联合实验室团队成员等共同参加了揭牌仪式。



联合实验室揭牌合影

吉大符号实验室主任杨博在致辞中表示，吉大符号实验室定位于应用基础研究，由王湘浩院士创建的吉林大学数学与计算机两个一级学科支撑，计算机与数学交叉融合，在符号计算与知识工程领域居国内领先地位。安天是知名网络安全企业，持续多年坚持自主先进网络安全技术研发，工程技术能力强，有海量威胁分析研究数据和样本资源。希望通过与安天研究院共建联合实验室，促进强强联合，将科研教学与工程技术实践更加紧密结合，共同推动产学研协同创新发展。

安天反病毒引擎技术负责人在致辞中表示，各种威胁行为体的长期持续活动，各种攻击行为复杂交织，威胁载荷数量持续膨胀，仅仅依靠传统的恶意代码检测对抗方式来应对是不够的。需要针对威胁行为体及其工程体系、装备体系、以及海量恶意代码载荷等建立起知识图谱。安天当前正在研发实战化运行的战术型态势感知平台，需要全面加速威胁知识图谱、心智模型等方面的探索。

吉大在知识工程和人工智能结合领域的研究上有较强理论优势，通过建立联合实验室，可以将吉大的科研教学人才优势和安天的工程能力优势相结合，推动知识工程在网络安全领域的实战化应用。

在揭牌仪式后的首次联合实验室学术会议上，吉林大学与安天研究人员分别分享了《吉林大学符号计算与知识工程教育部重点实验室在知识工程方向的研究》和《安天的威胁研究资源及在网络安全威胁知识工程上的思考》的技术报告，并在会上进行了热烈的交流讨论。

为实现对网络的有效防护，态势感知与积极防御能力不可或缺。通过实现网空态势感知，能够对不断演化的网空威胁做出识别、理解和预见，发现潜伏的安全威胁，并提供相应决策信息支撑从而及时做出应对。知识图谱能够让程序“理解”真实世界中存在的各种实体或概念及其关系，同时借助人工智能、数据挖掘等技术，能够对大量网空观察结果和数据进行推理，并推断出有助于分析师和决策者形成态势感知的重要情境特征，是实现网空态势感知的重要支撑。因此，安天研究院与吉大符号实验室共建联合实验室，双方将共同推进知识工程、人工智能、数据挖掘等技术在威胁分析、态势感知等领域的前沿探索，在科研合作、资源共享、学术交流、联合课题申报等方面扎实深入合作，积极推动自主先进技术成果的网络安全实战化应用，形成校企共建、培养复合人才、输出有效工程成果和先进学术成果的合作模式。

首次联合实验室学术研讨会

高校和企业受到自身角色和模式影响，过去在形成高水平成果方面有一定的局限条件。高校的网络安全研究多数缺少成熟工程能力支持，部分研究成果难以有效落地；而网络安全企业，工程师多数投入到产品和支撑能力开发，工作往往缺少前瞻性，缺少跟进和转化先进理论的动力。

在校企合作科研工作中，安天坚持优势互补、窄带聚焦、实战导向、追求领先的原则。安天针对合作高校的特点，选择自身有工程能力和数据基础、高校有学术积累的窄带专业方向进行合作，以形成具有实际防护价值的工程成果为目标，与重点高校开展专业方向的深度聚焦合作。在合作中，充分发挥高校科研理论优势，发挥安天的基础工程能力和数据优势，直接由企业技术带头人对接高校学术带头人，安天提供平台资源、工程资源和安全大数据资源支撑，助力高校形成具有前瞻性和实用前景的高水平学术成果，推动科研成果向有效的安全价值转化。

每周安全事件

类 型	内 容
中文标题	医疗器械制造商 ZOLL 泄露超 27 万名患者数据
英文标题	ZOLL notifies over two hundred thousand patients of data exposure
作者及单位	Ryan Stewart
内容概述	医疗器械制造商 ZOLL 去年发生数据泄露，时间发生在 2018 年 11 月 8 日至 2018 年 12 月 28 日之间。根据公司发布的官方声明，ZOLL 用于归档和其他目的的第三方服务导致了 ZOLL 客户数据的曝光。今年 1 月，ZOLL 现由第三方存档的电子邮件在供应商的服务器迁移过程中暴露，该公司已发布了一份详细说明数据曝光的新闻稿。暴露的信息包括患者姓名、地址、出生日期和部分医疗信息，一些患者的身份证信息也被暴露。发现泄露事件后，ZOLL 立即启动了内部审查，277,319 名患者受此事件影响。
链接地址	https://cyware.com/news/zoll-notifies-over-two-hundred-thousand-patients-of-data-exposure-2e67a78a

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

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	Trojan/Android.FakeBankia.a[prv,exp] 2019-03-25	该应用程序伪装金融相关软件，运行后隐藏图标，诱导用户填写银行账号和密码，监听用户短信，私自发送短信，造成用户隐私泄露和经济损失，建议卸载。（威胁等级高）
		Trojan/Android.RomanSpy.a[prv,rmt,spy] 2019-03-26	该应用程序运行后隐藏图标，激活设备管理器，通过短信接收远程指令，上传用户短信、联系人等隐私信息，还能执行解锁屏幕、设置锁屏密码等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.jeini.b[exp] 2019-03-27	该应用程序运行后诱导激活设备管理器，隐藏图标，后台监听拦截短信，私自回复，还会向联系人群发指定短信，造成用户资费损耗，请卸载。（威胁等级中）
	较为活跃的样本	G-Ware/Android.xeapk.a[exp,rog]	该应用程序伪装其他应用，无实际功能，安装无图标，程序运行会加载恶意子包，警惕其 root 用户设备私自下载安装应用，造成用户资费消耗，建议不要使用。（威胁等级中）
		Trojan/Android.hardshipspy.a[prv]	该应用程序运行后会隐藏图标，窃取用户短信、通讯录、通话记录、照片、视频、文件、浏览器记录和定位等隐私信息，并在后台将数据上传至服务器，造成用户隐私泄露，请立即卸载。（威胁等级中）
		RiskWare/Android.repackBilumin.a[rog]	该应用程序经过重打包处理，已植入了广告插件，而非官方版本，运行后会加载广告，可能泄露用户 imei 号，请用户下载和使用官方版本。（威胁等级低）
		RiskWare/Android.qhb.a[pay,rog]	该应用程序是一款微信抢红包工具，包含多个支付件，运行后诱导用户付费以便获取更多功能，同时包含风险代码，触发后红包群中抢到红包最少的用户发红包，具有一定的赌博行为，可能造成用户的经济损失，建议谨慎使用。（威胁等级中）
		Tool/Android.wxautojiaren.a[exp]	该应用程序是一款微信自动加粉工具，设置手机号码前 7 位后，自动开始发送申请，会造成用户资费消耗，可能干扰其他用户，请谨慎使用。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows Office 访问连接引擎远程代码执行漏洞（CVE-2019-0671）	当 Windows Office 访问连接引擎处理内存中的对象时存在远程代码执行漏洞。攻击者可以通过向目标发送经特殊设计的文件，诱使其打开该文件来利用此漏洞，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。（威胁等级高）
	较为活跃样本	RiskWare[Downloader]/NSIS.Spigot	此威胁是一种使用 NSIS 制作的风险软件类程序。NSIS 打包工具将该家族与正常程序打包在一起。该家族会自动下载并运行未经用户允许或用户不知情的安装软件，同时它能够不断地检查更新文件安装本身。（威胁等级中）
		Trojan[Downloader]/JS.DarDuk	此威胁是一种使用 JS 脚本编写的木马家族。该家族并没有统一的行为、统一的功能，而是像一个木马集合一样，将大量的恶意代码像基因片段一样进行定性归类。一般该家族样本通过网页挂马，当用户访问网页时，恶意 JS 脚本即会触发，可能会下载恶意代码并运行，窃取用户信息并回传。（威胁等级中）
		RiskWare[Downloader]/Win32.Dartsmound	此威胁是一种可以下载安装推广应用的风险软件类程序。该家族样本运行后连接网络，下载并安装推广应用，可能弹出广告，占用系统资源，影响用户使用。（威胁等级低）
		RiskWare[Monitor]/Win32.WebWatcher	此威胁是一种具有监听功能的风险类程序。该家族样本通过频繁快照对用户进行监控和记录，并将其回传到指定的电子邮件。（威胁等级低）
		RiskWare[RiskTool]/Win32.SProtector	此威胁是一种风险软件类程序。该家族样本运行后可以连接网络下载风险工具，该工具漏洞可能会被攻击者利用，造成用户信息泄露。（威胁等级中）

攻击者 AI vs 企业 AI

Satish Abburi/ 文 安天技术公益翻译组 / 译

企业正在使用人工智能和机器学习技术，而攻击者也开始使用同样的逻辑和功能来对抗企业。

攻击者以恶意方式使用人工智能（AI）和机器学习（ML）技术的情况可能还处于萌芽阶段，但是正在逐渐变成现实。这是一个渐进的过程：AI 和 ML 技术脱胎于实验室，之后被应用于安全防御；而现在，攻击者也开始使用同样的逻辑和功能来对抗这些防御措施了。

攻击者和首席信息安全官（CISO）都可以获得这些强大的功能，其中一些已经是现成的、“即插即用的”产品，使攻击者能够快速发动攻击。鉴于企业在防御策略中使用了 AI 技术，攻击者利用 AI 的灵活性来发现企业的漏洞只是时间问题。

从意图上看，基于情报的攻击与“常规”攻击是相同的。攻击者可能出于政治动机（国家攻击）、窃取知识产权（企业攻击）、窃取资金（金融机构攻击）等目的。AI 和 ML 技术通常被认为是一种“好的”力量。但是，在攻击者手中，它们则会造成严重的伤害。想象一下，在不久的将来，网络空间中会不会是机器人在相互对抗呢?

当“好”软件变“坏”

利用 ML 技术的自动渗透测试已经出现好几年了。现在，攻击者可以使用 Deep Exploit 等工具对目标企业进行渗透测试，并在 20 到 30 秒内找到防御系统中的漏洞——而在过去，这一过程需要数小时。ML 模型快速获取数据、分析数据并生成结果，为下一阶段的攻击做好准备，从而大大加快了这一过程。

攻击者对云计算和功能强大的中央处理器 / 图形处理器（CPU/GPU）技术的掌握，进一步增加了他们利用这些 AI/ML 工具的风险——而这些工具原本是为企业设计的。

当与 AI 结合使用时，ML 可以自动搜索漏洞利用工具包，从而攻破使用 AI 和 ML 技术构建的网络防御系统。

在这些漏洞利用工具包中，许多都达到了前所未有的自动化水平，能够使攻击者更加智能和高效。许多 DevOps 和 IT 团队正在使用 AI 和 ML 技术来深入了解他们的运营情况，而攻击者也在效仿这一点。

注入损坏的数据

正如研究人员所述，攻击者将了解企业如何使用 ML 技术进行防御，然后在企业使用的独特算法和统计模型中注入损坏的数据，使其防御模型失效。获取企业的 ML 数据是关键，有助于攻击者破解企业 AI。

网络安全解决方案中的许多 ML 模型，特别是深度学习模型，被认为是安全界的黑匣子。它们使用超过 10 万个功能输入来检测和识别异常情况，例如检测企业网络中的异常行为。

从安全团队的角度来看，这需要信任黑匣子中的模型或算法，但是他们可能并不理解这些模型或算法。这就导致他们产生了疑问：依靠这些算法真得可以防御攻击吗?

数据“投毒”

与其要求安全运营中心（SOC）团队完全信任 ML 算法，不如让他们理解 ML 模型是如何得出结论的——这一项改进正在进行中。即，当 ML 模型认为存在异常的风险行为时，软件可以解释推理过程。

如果企业难以检测攻击者是否已经向安全工具注入了“被损坏的”数据（或向其“投毒”），上述问题就非常重要了。通过向 ML 模型数据投毒，攻击者可以创建基准行为范式。这样一来，他们的攻击行为就会被认为是低风险的，并被允许继续进行。

未来会走向何方

攻击者可能出于其他目的，例如影响选民投票。在此类攻击中，攻击者利用 ML 技术来统计推特消息，以识别政治家用来影响特定选民群体的模式。一旦 ML 算法确定了竞选活动和模式，攻击者就可以创建反竞选活动，以操纵民意或对抗政治团体。

此外，还存在僵尸网络威胁。Mirai 是第一个造成广泛破坏的僵尸网络。现在，它的一些变种使用新的攻击向量来创建物联网（IoT）僵尸网络，甚至出现了更复杂的、旨在破坏核设施甚至整个智慧城市的工业物联网（IIoT）攻击。研究人员发现，潜在的高级僵尸网络会导致供水系统和电网崩溃。

AI 和 ML 技术已经投入使用——中级工程师也可使用它们，而不再只有数据科学家才能使用。这些技术会被企业使用，还是被攻击者使用，关键在于如何操作以减少误报和漏报。

这就是新的“认知”技术（不仅仅是 AI 和 ML 技术的总和）的目标，该技术不仅可以准确地检测出大数据中的不良行为模式，还可以提供处理建议，帮助企业做出决策。

原文名称	Hacker AI vs. Enterprise AI: A New Threat
作者简介	Satish Abburi。Satish Abburi 是 Elysium Analytics 公司的创始人。
原文信息	2019 年 3 月 21 日发布于 Dark Reading 原文地址 https://www.darkreading.com/vulnerabilities---threats/advanced-threats/hacker-ai-vs-enterprise-ai-a-new-threat-/a/d-id/1334201
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。