安天智甲有效防护 AstraLocker 勒索软件

近日，安天CERT在梳理网络安全事件时发现了一个名为AstraLocker的勒索软件，该勒索软件最早于2021年8月被发现，主要通过垃圾邮件和僵尸网络进行传播。经验证，安天智甲终端防御系统（简称IEP）的勒索软件防护模块可有效阻止勒索软件的加密行为。

AstraLocker勒索软件运行后，复制自身程序到%Appdata%目录下，并重命名为“system.exe”。在短时间内完成对计算机上相关文件的加密，将被加密文件的文件名替换为以“.AstraLocker”命名的后缀。加密完成后，尝试在遍历到的文件夹中创建一个名为“read_it.txt”的勒索信，该勒索信具体内容包含了勒索说明、联系方式和受害者的个人ID等。并且特别说明购买他们的解密软件只能使用门罗币或比特币进行付款，需要支付0.2XMR（门罗币），该解密软件的价格约合50美元。AstraLocker勒索软件最后会创建一个随机字符串命名的图片，替换桌面背景，诱使受害者打开勒索信读取相关信息。

AstraLocker勒索软件采用“AES+RSA”加密算法组合的形式加密文件，目前被加密的文件暂时无法解密。

▲AstraLocker勒索软件勒索信息

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软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

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，下为其自动生成的分析报告：

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、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态(Win7sp1 x86)鉴定器、字符串分析鉴定器、文件相似分析鉴定器、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(WinXP)鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据BD静态分析鉴定器将文件判定为木马程序。

◆概要信息

文件名	7b2d5c54fa1dbf87d7de17bf0bf0aa61b81e178a41b04e14549fb9764604f54c
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	102 KB
MD5	36C5D6B54AE35EFED69419AC27585AD6
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Ransom
判定依据	BD静态分析

报告地址：https://1.119.163.6/vue/details?hash=36C5D6B54AE35EFED69419AC27585AD6

◆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、Office2003、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
通过标记进程可执行堆绕过DEP	★★★★★
搜索文件	★★★★
在系统目录创建文件	★★★
映射内存方式注入	★★★
创建互斥量	★★★
释放PE文件到临时文件夹	★★★

◆常见行为对比

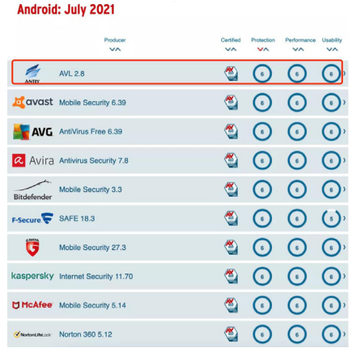
行为描述	危险等级
检测自身是否被调试	★★
镜像劫持	★★
使用windows COM库API	★★
.....	.....

◆扫描二维码查看完整报告

安天周观察
安天对外开放资料平台 安天官方微信
主办：安天 2021年08月30日(总第293期)试行 本期4版 扫描上方二维码查询安天所有对外开放资料

安天移动安全反病毒引擎在AV-TEST测试中再创双百佳绩

近日，国际权威评测机构AV-TEST公布了2021年7月全球各大反病毒引擎的测评结果，安天科技集团旗下的安天移动安全公司自主研发的AVL反病毒引擎凭借强劲的查杀能力连续获得AV-TEST 2021年5、7月检测率双百佳绩，继获得2018年、2019年全年零漏检率佳绩后，出色的病毒查杀能力再次得到国际权威机构的肯定。



在今年5月、7月份的AV-TEST测试中，安天移动安全AVL反病毒引擎凭借行业领先的针对移动恶意代码的动、静态检测能力，在常规测试和实时测试两项关键能力的测试中表现抢眼，以两项测试检出率皆为100%的成绩在全球近20家参测厂商中脱颖而出，继续领跑全球移动安全杀毒领域。

在7月份的测试中，AV-TEST对参测厂商在检测能力、可用性、用户体验三个方面的表现进行综合评定打分，不仅关注病毒查杀能力，也考量反病毒引擎的实用性以及终端用户的使用体验。经过综合测试评定，安天移动安全AVL反病毒引擎以强劲的查杀能力，零误报的实用性以及较低的CPU占用取得三项满分的佳绩。

基于十余年的反病毒技术的积累和沉淀，安天移动安全AVL移动反病毒引擎现已形成集样本捕获、分析判定、规则运维为一体的强大后端知识运营体系支撑，通过工程师智能化分析平台、人工智能技术形成了AVL专有知识库和判定模型，赋予移动反病毒引擎强大的威胁对象感知和精细化分析能力，形成针对移动恶意代码精准测量与识别的动、静态检测能力。

近年来，安天移动安全在国际权威评测机构AV-TEST的测试中屡获佳绩，一方面是对安天移动安全自主研发的AVL反病毒引擎检测、查杀能力的认可和肯定，另一方面也向全球展示了中国在移动杀毒领域的技术实力，充分体现了中国自主研发的移动反病毒引擎技术丝毫不逊色于海外众多知名厂商。

AV-TEST测试以海量病毒库检测、独立客观的检测过程和严格的标准著称，其在反病毒研究领域已拥有近20年历史。区别于其它国际测试，AV-TEST每年进行6次测试，其认为连续测试能更好的反映产品特性。因此AV-TEST成为全球最具权威的独立第三方反病毒能力专业测试机构之一，是业界公认的世界级杀软对决平台。

安天移动安全是安天科技集团旗下专注移动用户安全的科技公司。经过10年的技术积累，自主创新的安全引擎已成为国民级安全内核，为智能终端的用户生态实现全场景覆盖的移动应用安全治理，对导致用户权益受损的不良行为和黑灰产进行技术响应，并为开发者提供专业安全辅导和配套产品服务。（原文链接：https://mp.weixin.qq.com/s/LxS_Rcr8hXi6gknva4aWhA）

扫描右侧二维码阅读全文

研究人员披露ShinyHunters网络犯罪团伙的攻击方法

臭名昭著的地下网络犯罪组织Shiny-Hunters自去年以来一直在疯狂地进行数据泄露。一份对这些黑客行为的分析显示，他们一直在搜索公司GitHub存储库的源代码，用来发动更大规模攻击的漏洞。自2020年4月活跃以来，ShinyHunters声称对一系列数据泄露事件负责，包括Tokopedia、Wattpad、Pixlr、Bonobos、BigBasket、Mathway、Unacademy、MeetMindful和微软的GitHub账户等。（原文链接：https://thehackernews.com/2021/08/researchers-detail-modus-operandi-of.html）

恶意软件活动针对拉丁美洲旅游和酒店组织

思科安全研究团队（Cisco Talos）最近观察到一系列针对拉丁美洲国家的恶意软件活动，这些活动使用多种感染组件来传播两种广受欢迎的商品恶意软件和远程访问木马(RAT):njRAT和AsyncRAT。Cisco Talos还发现了一个基于.NET的感染链构建器/加密器二进制文件，用于生成最近活动中使用的恶意感染工件。此类构建器表明作者打算捆绑恶意软件生成功能，以便犯罪团伙轻松分发和使用。（原文链接：https://blog.talosintelligence.com/2021/08/rat-campaign-targets-latin-america.html）

安全研究人员发现了PRISM后门的新版本

AT&T Alien Labs的安全研究人员表示，他们发现了一组Linux ELF可执行文件，这些文件被确定为开源PRISM后门的修改版本，攻击者已经在多个活动中使用了三年多。PRISM是一个开源、简单和直接的后门，它的流量是清晰可辨的，它的二进制文件很容易被检测到。发现的PRISM变种之一是WaterDrop，它包括一个名为xencrypt的函数，该函数使用硬编码的单字节0x1F密钥执行XOR加密。（原文链接：https://www.govinfosecurity.com/updated-prism-backdoor-discovered-a-17367）

每周安全事件

类 型	内 容
中文标题	Flubot 恶意软件利用诈骗短信攻击澳大利亚用户
英文标题	Australians hit by ‘Flubot’ malware that arrives by text message
作者	Josh Taylor
内容概述	数千名澳大利亚人被一种名为 Flubot 的新型诈骗短信袭击，该短信旨在在他们的手机上安装恶意软件。Flubot 是一种针对 Android 用户的恶意软件，但 iPhone 用户也可以收到这些信息，它告诉接收者他们错过了一个电话或有了一个新的语音邮件，提供一个虚假的收听链接。这个链接将把人们带到一个看起来像官方品牌的网站，该页面告诉用户在电话上安装软件来接听消息。如果用户同意，它就会安装恶意软件，如果该应用程序获得许可，那么攻击者将获得信用卡信息、个人信息、拦截短信、打开浏览器页面和获取手机中的其他信息的能力。
链接地址	https://www.theguardian.com/technology/2021/aug/20/australians-hit-by-flubot-malware-that-arrives-by-text-message

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 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称	威胁等级	简要描述
活跃漏洞	Microsoft Edge 远程代码执行漏洞（CVE-2021-30598）	高	Microsoft Edge 存在远程代码执行漏洞。由于 V8 中的类型混淆错误，使得攻击者可以创建一个特制的网页，诱使受害者访问它，触发类型混淆错误并在目标系统上执行任意代码。
	Microsoft Edge 远程代码执行漏洞（CVE-2021-30602）	高	Microsoft Edge 存在远程代码执行漏洞。由于 WebRTC 中的释放后使用错误，使得攻击者可以诱使受害者访问特制网页，触发释放后使用错误并在系统上执行任意代码。
	Adobe Bridge 远程代码执行漏洞（CVE-2021-36072）	高	Adobe Bridge 存在远程代码执行漏洞。由于该应用程序在处理不受信任的输入时出现边界错误，使得攻击者可以创建一个特制的文件，诱使受害者使用受影响的软件打开它，触发越界写入并在目标系统上执行任意代码。
较为活跃样本家族	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan/Win32.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	Trojan[Proxy]/Win32.Qukart	中	此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。
	Trojan[Ransom]/Win32.Crypmodadv	中	此威胁是一种勒索软件家族。该家族的样本在运行后，会加密系统上多种文件格式的文 件，并将文件的扩展名更改为 .remind。在加密后，该样本会在全部的文件夹下各放置 一封 HTML 格式的勒索信说明情况。
	Trojan[Backdoor]/Win32.Finfish	中	该病毒家族是一种可以窃取用户信息的木马类程序。该家族样本运行后修改注册表使其自启动，窃取用户敏感信息，如帐号密码等。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan/Android.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。

自动化渗透测试无法弥补网络安全技能差距

王宁 / 文 安天技术公益翻译组 / 译

对现代企业来说，网络威胁是一个巨大的挑战。有些企业寄希望于从热门供应商那里购买最新安全产品，来应对网络威胁问题；但大多数企业都已经意识到，这样做不足以保护自己。

自动化渗透测试和安全人才缺口

网络安全工具和扫描程序确实很好用，但它们只能搜索已知的漏洞。然而，有很多漏洞是只有训练有素的安全专家才能发现的。不幸的是，企业缺乏此类安全专家，这加剧了其面临的网络安全挑战。

在安全人才缺口日益扩大的情况下，企业想出了各种办法来弥补技能差距。其中，最新的办法是自动化渗透测试，即，企业创建机器人来探测其防御系统，以发现漏洞。实际上，这种方法并非真正的渗透测试。真正的渗透测试不是自动扫描作业，而是利用经验丰富的网络安全专家进行创造性的漏洞识别。

渗透测试的意义在于其创造性，网络安全专家从攻击者的角度进行思考，并识别出机器和其他预内置逻辑无法识别的漏洞，从而领先网络犯罪分子一步。当我们教机器人去识别和解决某些漏洞时，黑客可以找到新的漏洞来绕过这些自动检测。

虽说我们应尽可能多地实现自动化，但是，仅仅依赖自动化的系统和网络安全测试是无法保护企业的。保护企业的唯一方法是与优秀的网络安全专家合作，以击败攻击者。

思维转变是关键

安全团队需要具备进攻性的思维——即，他们必须像攻击者一样思考。他们需要领先于网络犯罪分子一步，并就重要和及时的行动向企业的其他成员提供建议。

并非每个漏洞都是显而易见的。保护企业的最佳方法是让防御者像攻击者一样思考，并在每次遇到瓶颈时加倍努力，不轻易放过哪怕是看起来微不足道的安全隐患。要想成功防御企业的系统、网络和应用程序，他们不仅要了解攻击者的工具，还要了解他们如何以及何时使用这些工具。这需要进行大量的判断，问很多“为什么”，而这些事情是无法通过自动化测试来处理的。自动化渗透测试的好坏，取决于安全团队告知机器人要查找什么内容和执行什么操作。但是，攻击者经常改变攻击策略，因此自动化渗透测试无法保护企业。

攻击者不需要什么了不得的漏洞，就能够侵入企业——他们很有耐心，静待企业的某个员工犯错，然后通过网络钓鱼或社会工程手段进入企业网络。一旦进入企业网络，他们就会进行提权，以访问更多的敏感系统和数据。

严重的黑客攻击和数据泄露通常始于微小的事故。鉴于大多数系统和网络的设计没有考虑到必要的安全防御机制，因此攻击者将一些小漏洞关联起来产生破坏性影响的情况并不少见。

此外，攻击者不断开发新的恶意软件载荷，并测试新的威胁向量。要想防御攻击者，企业需要具备像攻击者一样富有创造力和毅力的防御者。此外，防御者还需要及时了解最新的漏洞、黑客技术、恶意软件等。

缩小网络安全技能差距

网络安全技能差距是“人”的问题，但这不仅是指找到足够的“人”来操作工具，因为只依靠工具也是不够的——攻击者找到应对这些工具的方法只是时间问题。

要想解决网络安全问题，企业需要加强对所有人的安全意识培训。我们需要对设计和构建系统和网络的人员进行培训，使其具备攻击者思维。企业的安全专家应该像攻击者一样思考，并及时了解最新的漏洞和安全问题。

毫无疑问，企业需要更多优秀的安全专家。但是，解决人才短缺问题没有什么灵丹妙药。安全专家需要具备敏锐的思维，能够创造性地思考问题，愿意付出精力，且不会轻言放弃。

安全专家的候选人可以来自多个部门，包括系统管理员、网络工程师、Web 开发人员、客户服务人员，甚至是应届毕业生。虽然他们无法立刻变身为“安全专家”，但他们具备在安全方面取得成功的基本特征。

归根结底，安全是“人”的问题。扫描程序、工具和自动化测试可以提供帮助，但要想真正解决安全问题，企业需要多层次的人类创造力。

原文名称	Why automated pentesting won’t fix the cybersecurity skills gap
作者简介	王宁（Ning Wang），是 Offensive Security 公司的首席执行官。
原文信息	2021 年 8 月 23 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/08/23/automated-pentesting/
摘 要	毫无疑问，企业需要更多优秀的安全专家。但是，解决人才短缺问题没有什么灵丹妙药。安全专家需要具备敏锐的思维，能够创造性地思考问题，愿意付出精力，且不会轻言放弃。归根结底，安全是“人”的问题。扫描程序、工具和自动化测试可以提供帮助，但要想真正解决安全问题，企业需要多层次的人类创造力。
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。