安天智甲有效防护 Bam 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 Bam 的勒索软件。该勒索软件最早于 2017 年 7 月出现，此变种被发现于 2021 年 6 月初，主要通过垃圾邮件进行传播。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 Bam 勒索软件的加密行为。

Bam 勒索软件运行后在注册表路径 HKEY_CURRENT_USER\Software\ 下添加 Rs 项，其键值包含随机生成的用户 ID。同时在桌面上创建“autorun.inf”和“Notify.jpg”两个属性为隐藏的文件，通过文件内容判断，“autorun.inf”文件的功能为实现勒索软件自动运行；“Notify.jpg”图片文件为勒索信息，并将其修改为用户桌面背景告知受害者已被勒索。根据图片文件对比发现，此前版本是通过邮箱（abc@xyz.com、acc@xyz.com）与攻击者联系获取具体要求，当前版本要求受害者支付价值 300 美元的比特币发到指定的比特币钱包地址，无其他联系方式。随后遍历磁盘对特定后缀名的文档、压缩包、图片、音视频等文件进行加密，采用的加密策略为使用随机 AES 密钥加密文件，并追加文件名后缀 ".bam!"；然后使用 RSA 非对称加密算法加密 AES 密钥。

▲Bam 勒索软件勒索信息

因其没有删除卷影，受害者可尝试通过卷影恢复数据。Bam 勒索软件采用“AES+RSA”组合的形式加密文件，目前被加密的文件暂时无法解密。

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、反病毒引擎鉴定器、动态行为鉴定器将文件判定为木马程序。

◆概要信息

文件名	84ffb87cc91d697db2f5685df68de7af
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	2.32 MB
MD5	84FFB87CC91D697DB2F5685DF68DE7AF
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Cryptor
判定依据	BD 静态分析

报告地址：https://1.119.163.6/vue/details?hash=84FFB87CC91D697DB2F5685DF68DE7AF

◆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、AdobeReader

◆危险行为

行为描述	危险等级
映射内存方式注入	★★★
修改文件后缀名	★★★★
搜索文件	★★★★

◆常见行为

行为描述	危险等级
文档篡改	★★
疑似桌面控制	★
加载运行时 DLL	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
打开现有服务	★

◆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 06 月 28 日 (总第 284 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

安天引领网安百强“竞争者”阵营

6 月 16 日，国内数字化产业第三方调研与咨询机构数世咨询正式发布《中国网络安全百强报告 (2021)》(以下简称“百强报告”)。安天凭借企业创新力、品牌影响力和引人注目的高速规模成长，获评独角兽企业，入围“综合实力百强”，引领“竞争者”阵营，携手网安创新力量挑战上市阵营。

引领“竞争者”矩阵 实力争当领军者

本次百强报告调研范围覆盖国内 700 余家网络安全企业，从上百项评价指标以及多角度、多维度的企业相关数据进行梳理与评价后得出结果。旨在突出网络安全能力方面表现优秀的企业，清晰客观地反映国内网络安全企业的真实状况，为国家、研究机构、行业用户、广大网络安全企业及网安从业者提供价值参考。

勇担独角兽重任，牢记“民企国家队”使命

作为“民企国家队”，安天始终致力于有效应对安全威胁，全面提升客户的网络安全防御能力。安天在关键核心技术领域长达二十年的坚持自主研发投入，建立了哈尔滨、北京、武汉、成都、深圳、上海六地研发中心、两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室，参与了一项国家重点实验室建设。安天的能力型产品和解决方案受到有关重要部门和政企机构的信赖，为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户提供防护，全方位助力客户构筑对抗高级威胁的网络安全防线。（原文链接：https://mp.weixin.qq.com/s/2SqmqF8_zY7Z76SikOhlQA）

扫描右侧二维码阅读全文

“2021 中国网安产业竞争力 50 强”安天位列 20

6 月 16 日，由中国网络安全产业联盟（CCIA）主办的“2021 CCIA 网络安全产业发展论坛暨网络安全优秀创新成果大赛启动仪式”在北京隆重举行。

此次活动揭晓“2021 年中国网安产业竞争力 50 强”，安天科技集团股份有限公司（以下简称“安天”）凭借自身在网络安全领域的的核心技术实力以及高效达成客户安全价值的能力成功入选，位列第 20 名。据悉，本次公布的“50 强”评价指标采用多维度综合评价法，对我国网络安全行业领军企业的发展状况进行综合研究，从产业视角和商业视角出发，对企业“竞争力”和“资源力”2 个维度进行画像判断与量化评估，得出 50 强排名。此次榜单旨在促进企业用户全面了解我国网络安全产业发展现状、分析网络安全技术和产业发展趋势，为相关政策制定、企业发展决策提供依据。（原文链接：https://mp.weixin.qq.com/s/5eBqF_zSfhvs8OO2rSZfWg）

扫描右侧二维码阅读全文

安天两款产品获“2021 网信优秀产品、解决方案评选”活动奖项

为了进一步促进网信成果尽快转化为生产力，解决核心技术和供应链受制于人的问题，由关键信息基础设施技术创新联盟、信息安全等级保护关键技术国家工程实验室、《网信自主创新调研报告》编委会联合主办了“2021 网信自主创新优秀产品、解决方案评选”活动。通过专家量化打分和评议，凭借自身优秀的设计理念、成熟的产品能力和技术创新能力，安天两款产品分获“盘古奖”（优秀产品技术创新奖）和“龙门奖”（优秀解决方案最具潜力奖）。6 月 20 日，颁奖仪式在第二届中国 I²S 峰会上举行。

优秀产品技术创新奖 - 盘古奖

安天追影威胁分析系统获奖

优秀解决方案最具潜力奖 - 龙门奖

威胁情报检测与分析解决方案获奖

（原文链接：https://mp.weixin.qq.com/s/_ShdKNOulHR1GhXEjjUK2A）

扫描上方二维码阅读全文

每周安全事件

类 型	内 容
中文标题	TA402 团伙使用新的恶意软件针对中东政府
英文标题	New TA402 Molerats Malware Targets Governments in the Middle East
作者	KONSTANTIN KLINGER, DENNIS SCHWARZ, AND SELENA LARSON
内容概述	Proofpoint 研究人员发现了一种由 TA402 威胁团伙分发的名为 LastConn 的恶意软件，TA402 也被称为 Molerats。该恶意软件的目标是中东的政府机构以及与该地区和地缘政治有关的全球政府组织。TA402 在最近观察到的活动中使用了包含恶意链接或附件的鱼叉式网络钓鱼电子邮件。在 6 月的活动中，TA402 利用带有一个或多个地理围栏 URL 的 PDF 附件，生成包含恶意软件的受密码保护的存档。邮件和 PDF 通常都是用阿拉伯语写的，诱饵通常是基于影响中东的地缘政治主题，尤其是加沙冲突。RAR 文件的密码可以在 PDF 的文本中找到。提取存档显示一个定制的 TA402 植入物。在最近的活动中，存档中删除了 LastConn 恶意软件。其他观察到的通过这种攻击路径分布的恶意软件包括 SharpStage、Loda 和 MiraiEye RAT。
链接地址	https://www.proofpoint.com/us/blog/threat-insight/new-ta402-molerats-malware-targets-governments-middle-east

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 DWM 核心库远程代码执行漏洞（CVE-2021-33739）	高	Microsoft DWM 核心库存在远程代码执行漏洞。由于 Microsoft DWM 核心库中的权限管理不当，使得攻击者可以诱使受害者运行特制的可执行文件或脚本并在系统上执行任意代码。
	Microsoft Paint 3D 远程代码执行漏洞（CVE-2021-31983）	高	Microsoft Paint 3D 存在远程代码执行漏洞。由于 Paint 3D 在中处理 PLY 文件时存在内存边界检查错误，使得攻击者可以创建一个特制的 PLY 文件，诱使受害者打开它，触发越界读取错误并在系统上执行任意代码。
	Microsoft Intune Management Extension 远程代码执行漏洞（CVE-2021-31980）	高	Microsoft Intune Management Extension 存在远程代码执行漏洞。由于 Microsoft Intune 管理扩展中的输入验证不正确。远程攻击者可以发送特制的请求并在目标系统上执行任意代码。
较为活跃样本家族	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/Win32.Cosmu	中	此威胁是一种下载类木马家族。该家族木马会从指定的服务器下载多种恶意软件和广告软件。该家族木马还会在系统后台定时访问指定的站点，以提高这些网站的访问量，为木马制作者获取利益。
	Trojan[Backdoor]/Win32.Padodor	中	此威胁是一种后门类木马家族。该家族样本会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。
	Trojan/Win32.Fsysna	中	此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。
	Trojan/Win32.Yakes	中	此威胁是一种恶意木马家族。该家族木马可以通过白名单机制绕过系统防火墙，获取系统的最高权限。该家族木马具有下载恶意程序、监控用户操作等行为。该家族木马会在执行完成后将自身删除。
	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。

XDR：零信任架构的中枢神经系统

大卫·比森 / 文 安天技术公益翻译组 / 译

如果零信任架构是关注数字身体健康的大脑，那么“扩展检测和响应”（XDR）就是为其提供信息的中枢神经。随着数字世界的迅速变化，XDR 可以迅速调整和适应。为何说将 XDR 与零信任相结合是正确的选择呢?

不断变化的世界中的零信任

企业的数字威胁形势不断变化，攻击的频率和复杂程度都在不断增长。在 2020 年上半年，FBI 网络部门每天都会收到多达 4000 起数字攻击投诉，比上一年增加了 400%。

与此同时，连接到企业网络的端点不断增加。许多美国企业发现，随着他们转向远程工作，连接到其公司网络的设备数量迅速增加。在 2021 年的一项调查中，普华永道发现，83% 的雇主认为向远程工作的转变是成功的；超过一半（55%）的员工表示，他们希望今后每周至少有 3 天能够进行远程工作。

是福也是祸

这些因素说明，随着威胁的不断增加和员工的日益分散，采用零信任架构对企业是有帮助的。但是，这也使得零信任架构的构建变得更加困难。那么，安全团队应该如何及时查看、验证和保护诸多不同类型的设备呢?

“及时”是非常重要的。安全团队不能将所有时间都花在手动验证 / 重新验证“连接尝试是否受信任”上——他们没有这么多时间。事实上，他们需要想办法来精简这一流程，以最大限度地提高工作效率。

转向 XDR

答案是转向 XDR。要想了解“XDR 是什么”，我们首先要知道 XDR 起源于什么——它可以追溯到“端点检测和响应”（EDR）。

EDR 的优势和局限性

EDR 的运作基于两个基本原则。第一个原则是持续监控网络。EDR 首先为端点设置安全基线，然后使用该基线来监控可疑用户、异常进程和其他潜在威胁的迹象。

第二个原则是自动响应。EDR 收集它在端点上观察到的所有信息，并将其聚合到一个中央数据库中。然后，它根据取证工具和 / 或人类分析师的输入来进行响应。

EDR 可以通过上述流程，帮助企业加强对潜在威胁的防御。但是，它只能从它所在的端点或端点组进行操作，难以实现可扩展性。随着连接到公司网络的设备越来越多，企业需要购买更多的许可证。

即便如此，EDR 也只能监控和检测某些类型的威胁。它仅限于端点，因此无法处理横向移动等事件。因此，对涉及多个资产、网络或云环境不同部分的攻击链，其可见性是有限的。

XDR 如何弥补差距并为零信任赋能

因此，企业需要 XDR。XDR 是 EDR、网络流量分析（NTA）工具、SIEM 解决方案和其他“反应式”工具的替代或演变。它使用威胁情报和多维流量算法，在损害造成之前发现潜在攻击。XDR 不仅可以跨各个端点实时执行此工作，还可以在云和整个网络中实时执行此工作。

通过这些功能，企业可以解决零信任架构的“不及时”问题。XDR 涉及人工智能、机器学习和其他高级分析，能够实时检测威胁。鉴于安全团队需要实时验证不同网络区域、越来越多的连接设备的信任，这一点非常重要。

从这个意义上说，XDR 是零信任架构的中枢神经系统。它能够提供对连网设备的实时可见性。然后，安全团队可以使用其告警和监控工具来发现数字威胁并尽快做出响应。

使用 XDR 扩展零信任架构

零信任架构并不是单一的技术。它依靠单点登录、多因子身份鉴别、网络分段等措施，来监控哪些用户是可以信任的。这些技术可以帮助企业实现零信任，但无法帮助其提升到企业范围的安全级别。

但是 XDR 可以。它通过在整个企业中的自动化可见性，来实现这一点。这样，企业就可以跟踪他们的设备连接并持续验证这些设备是否受信任，以更好地迎接新设备的涌入。

原文名称	XDR: The Central Nervous System of Zero Trust
作者简介	大卫·比森（David Bisson），是一名信息安全记者。
原文信息	2021 年 6 月 22 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/articles/xdr-nervous-system-zero-trust/
摘 要	XDR 是 EDR、网络流量分析（NTA）工具、SIEM 解决方案和其他“反应式”工具的替代或演变。它使用威胁情报和多维流量算法，在损害造成之前发现潜在攻击。XDR 不仅可以跨各个端点实时执行此工作，还可以在云和整个网络中实时执行此工作。从这个意义上说，XDR 是零信任架构的中枢神经系统。它能够提供对连网设备的实时可见性。然后，安全团队可以使用其告警和监控工具来发现数字威胁并尽快做出响应。
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。