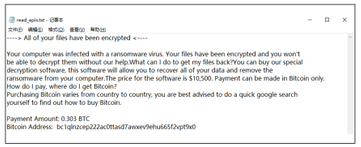
安天智甲有效防护 Chaos 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Chaos 的勒索软件。该勒索软件被发现于 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 Chaos 勒索软件的加密行为。

Chaos 勒索软件目前处于升级开发状态，其设计者在黑客论坛中公开构建器，并广泛征集修改建议，不断完善软件功能。因部分功能与 Ryuk 勒索软件较为相似，设计者想将其命名为 Ryuk。该勒索软件使用 .NET 框架开发，具备反调试功能，运行后创建名为 " 7z459ajrk722yn8c5j4fg" 的互斥体保证单实例运行。复制自身至 %Appdata%\Roaming 路径下并修改文件名为“svchost.exe”，添加注册表项 HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Store、在启动目录中创建“svchost.url”文件从而实现持久化驻留和自启动。该勒索软件不采用加密算法对文件进行加密，而是使用随机字节数据覆写原始文件数据，在原文件名后追加“.apis”后缀。在含有被覆写文件的位置创建“read_apis.txt”勒索信，内容为勒索提醒、赎金金额和比特币钱包地址。随后删除系统卷影，删除备份和禁用修复功能，以防止恢复被覆写文件。

Chaos 勒索软件采用随机字节数据覆盖的方式覆盖文件原始数据，会造成文件数据的丢失。无论受害者是否缴纳赎金，攻击者都无法为受害者解密文件。

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。



▲Chaos 勒索软件勒索信

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、静态特征检测鉴定器将文件判定为木马程序。

◆概要信息

文件名	8458ca4c230169e4ef4d3fca9a709690
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	18 KB
MD5	8458CA4C230169E4EF4D3FCA9A709690
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Ransom
判定依据	静态特征检测

报告地址：https://1.119.163.6/vue/details?hash=8458CA4C230169E4EF4D3FCA9A709690

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

◆常见行为

行为描述	危险等级
镜像劫持	★★
.....	.....

◆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07月05日(总第285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

100 年峥嵘岁月，100 年沧桑巨变。在举国上下喜迎中国共产党建党 100 周年之际，安天全面强化网络安全值守，保障战略客户安全；并组织系列活动，纪念建党百年。

“你们也是国家队，虽然你们是民营企业。”习近平总书记 2016 年视察安天时的话语，时刻激荡在安天人的心中。安天是沐浴着党的改革开放春风创业成长起来的，没有党的领导，就没有企业的成长发展。捍卫国家网络安全，担当网络强国使命，安天人通过加强党的建设，不断完善组织覆盖和工作覆盖，并由此带动了企业的全面发展。

安天从 2015 年起，先后在哈尔滨、北京、武汉、成都各属地成立党支部。2018 年，经上级党组织批准，成立集团党委。目前集团党委下设 6 个党支部。安天坚持以党建促发展，把党建作为集团发展的“红色引擎”。目前安天各地研发中心负责人中有半数都是由政治思想坚定，专业技术过硬的党员专家担任，充分发挥“红色引擎”产生的“红色动力”，激发企业科技研发、技术创新等能力全面提升，推动企业高效发展，切实担负起网络安全国家队的责任使命。

▲ 安天各地支部组织观看纪念大会直播

捍卫国家网络空间主权、确保网络安全，是新时代的重要使命和时代课题。值此伟大的中国共产党成立百年之际，安天作为战略创新企业，始终将国家安全作为唯一立场和第一视角。永远跟党走，坚守爱国初心、心怀报国之志，努力为祖国新时代发展做出新的更大贡献。（原文链接：https://mp.weixin.qq.com/s/m8vsGZBAH9BmbYM6uyFdng）

扫描右侧二维码阅读全文

防御勒索攻击即刻行动！安天垂直响应服务平台正式上线！

前不久，美国成品油管道运营商遭到勒索攻击，导致该公司为美国东部沿海主要城市输送油气的管道系统被迫下线，美国交通运输部联邦汽车运输安全管理局（FMCSA）发布区域紧急状态声明。安天前后发布 3 篇相关报告进行深度分析（点击这里阅读安天分析和总结）。面对一次又一次“勒索攻击”带来的不能承受之痛，事前的防御准备和事中的及时发现尤为重要，保护信息资产、防御勒索攻击，必须马上行动！

自 2015 年起，安天已将勒索软件视为需要重点布防的首要威胁之一，持续为用户提供全方位的解决方案。对于部分尚未建立有效安全策略的中小企业用户来说，因难于及时发现勒索攻击，随时面临勒索攻击的风险，急需专业的安全服务。面对这一需求，安天正式推出“安天垂直响应服务平台”，面向中小企业用户提供专业的安全服务，首批上线的功能之一就是勒索风险检测服务，面向个人用户和中小企业用户的 Windows 终端，下载即用，一键诊断，免费检测勒索风险，并提供专业知识和应对指导。

免费获取方式：

产品下载链接：https://vs.antiy.cn/service/rdt，或后台回复“勒索风险检测服务”，获取下载链接。（原文链接：https://mp.weixin.qq.com/s/3NTX_Gyz6Eg6r5MLJY_n8A）

扫描右侧二维码阅读全文

伪造盗版软件传播的窃密样本分析

近日，安天 CERT 监测到黑产组织利用伪造的盗版软件下载网站分发多个恶意程序的窃密攻击行动，目前共监测伪造相关虚假盗版（破解）软件数百个，我国已有近千台设备受其感染。虽然攻击者伪造了大量知名软件破解版本的下载页面，但实际这些下载地址文件均为相同类型的恶意代码，并非真正的破解程序或破解安装包。（原文链接：https://mp.weixin.qq.com/s/ykQRCzzWveunFbVs-IaAYQ）

有力保障神舟十二号载人飞行任务圆满成功，安天收到感谢信

2021 年 6 月 17 日，神舟十二号载人飞行任务获得圆满成功。在此次发射任务中，安天相关网络安全产品提供了安全检测防护能力，保障系统安全运行（点击这里阅读相关内容）。近日，中国人民解放军某部队向安天发来感谢信，感谢安天对此提供的技术支持和安全服务。（原文链接：https://mp.weixin.qq.com/s/W8bZwpzChH9au83BOG8Aow）

安天亮相 2021 上海网络安全博览会

2021 年 6 月 27 日，由上海市信息网络安全管理协会牵头，(ISC)² 上海分会、国家计算机网络应急技术处理协调中心上海分中心（SHCERT）等联合组织的“新耀东方 -2021 上海网络安全博览会暨高峰论坛”在上海新国际博览中心举办。众多业内顶级专家齐聚上海，围绕网络安全领域的热点内容和未来趋势进行探讨交流。（原文链接：https://mp.weixin.qq.com/s/5nGtnK28NuIPpwpN3HQjtQ）

每周安全事件

类 型	内 容
中文标题	DarkSide 2.0 针对托管 VMware 虚拟机的服务器
英文标题	DarkSide Created a Linux Version of Its Ransomware
作者	Prajeet Nair
内容概述	据 AT&T 的 Alien Labs 称，DarkSide 俄语网络犯罪组织于 2021 年 3 月 9 日在 XSS 俄罗斯网络犯罪论坛上发布了 Linux 版本的 DarkSide 2.0，旨在针对托管 VMware 虚拟机的 ESXi 服务器。研究人员表示，Linux 版本恶意软件支持通过执行 esxcli 命令关闭整个虚拟机。在执行时，恶意软件将其配置打印到终端，并包括要加密的根路径、RSA 密钥信息、要加密的目标文件扩展名和 C2 地址。然后恶意软件统计要加密的文件，并从受感染机器收集信息，加密后将其发送到 C2 服务器。一旦加密完成，恶意软件就会在每个文件被加密的文件夹中创建一张勒索信。研究人员没有报告说有任何组织正在使用该 Linux 恶意软件。
链接地址	https://www.inforisktoday.com/darkside-created-linux-version-its-ransomware-a-16941

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 Paint 3D 远程代码执行漏洞（CVE-2021-31946）	高	Microsoft Paint 3D 存在远程代码执行漏洞。由于 Paint 3D 在解析 GLB 文件时存在边界条件，使得攻击者可以创建一个特制的 GLB 文件，诱使受害者打开它，触发越界读取错误并执行任意代码。
	Microsoft VP9 Video Extensions 远程代码执行漏洞（CVE-2021-31967）	高	Microsoft VP9 Video Extensions 存在远程代码执行漏洞。由于 VP9 Video Extensions 中的输入验证不正确，使得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。
	Microsoft Office Graphics 远程代码执行漏洞（CVE-2021-31941）	高	Microsoft Office Graphics 存在远程代码执行漏洞。由于在 Microsoft Office Graphics 中处理 Excel 文件时出现释放后使用错误，使得攻击者可以创建一个特制的 Excel 文件，诱使受害者打开它，触发释放后使用错误并在系统上执行任意代码。
较为活跃样本家族	Trojan[Backdoor]/Win32.Salgorea	中	此威胁是一种可以下载恶意代码的木马类家族。该家族样本运行后连接网络下载恶意代码并执行。
	Trojan/Win32.Scar	中	此威胁是一种木马类程序，可以将某些金融网站重定向到攻击者设置的另一个地址，模仿登录界面从而窃取用户密码。
	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[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.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	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.Hqwar	中	此威胁是安卓平台上一种间谍类木马家族。该家族木马运行后，伪装成系统应用，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗。

重新思考威胁建模

特雷弗·杨 / 文 安天技术公益翻译组 / 译

传统的威胁建模方法非常有效，但是在当前的计算和威胁环境中，它们的扩展性不够好。随着越来越多的业务运营转向数字化，解决企业的所有高优先级威胁变得非常耗时，导致很多漏洞无法得到修复。

企业应如何精简这项工作呢？他们首先应意识到，他们目前是在反向进行威胁建模的，应对这种开发方式做出转变。

使威胁建模更加简单

从广义上讲，威胁建模涉及从日常的安全工作中后退一步，以了解企业的系统，评估网络和数字资源，识别威胁环境中的漏洞，并优先考虑涵盖保护、响应、补救和恢复的计划。在某些情况下，威胁建模团队主要由安全专家和架构师组成。在其他情况下，威胁建模团队可以涵盖各种利益相关者，包括应用程序所有者、服务台人员、管理员等等。

这些团队需要遵循许多已定义的框架，例如微软 1999 年开发的 STRIDE 模型。威胁建模会议通常以类似于“白板会议”的方式进行：安全专家和利益相关者聚在一起讨论风险因素，并就“如何应对这些风险因素”进行头脑风暴。这是必须要改变的。

如果企业的目标是跨应用程序扩展威胁建模，那么“在白板上绘制系统组件和架构图”的方式就是落后的。

在快速发展的云环境中，技术和数字系统越来越普遍。在这种情况下，安全专家坐在一个房间里花几个小时进行头脑风暴，已经无法与针对多个系统的、日益增加的威胁相抗衡。这是因为，大型企业可能拥有数百个系统。更麻烦的是，随着物联网（IoT）的发展，新的威胁向量不断出现——包括汽车和交通信号灯、工业控制系统，以及客厅中的联网设备等等。

从许多方面来说，硬件漏洞和 IoT 构成了全新的领域，带来了新的攻击目标，Colonial Pipeline 管道公司的攻击事件就是一个很好的例子。在这种情况下，企业应如何使用当前的劳动密集型方法，对如此众多的新攻击向量进行建模呢？他们是做不到的。

威胁建模的新趋势

安全行业出现了一个新的威胁建模趋势：企业可以扫描现有系统，整合有关当前和潜在威胁的数据，由此进行威胁建模；而非借助白板和满屋子的安全专家（他们被要求像黑客一样思考，试图识别潜在威胁）进行威胁建模。

这种转型是可行的，原因是：大多数系统都有一种公开数据的方法，可以帮助企业识别引入业务风险的组件或流程。借助结构化的数据和分析工具，安全从业人员可以快速生成不同的系统风险模型，以凸显整个企业的威胁、漏洞和弱点。

如果企业以可重复的自动化方式执行此操作，则他们不仅可以同时对数百个应用程序执行威胁建模，还可以近乎实时地进行建模，以持续监控企业的安全状况。

上述分析工具可以自动扫描系统中的元数据，对各领域（例如源代码库、云管理工具和配置管理数据库）的威胁进行建模。企业可以利用与各种技术组件相关的商业或开源漏洞数据库（例如 OWASP Top Ten 和 MITRE ATT&CK 框架），以及安全提供商整合的大量数据库。

将从这些系统扫描中发现的技术资产，与已知组件漏洞数据库相匹配，企业可以快速确定其基线安全状况。之后，企业可以在此基础上进行建模，确定哪些漏洞适合进行完整的“白板头脑风暴”会议。这样，企业可以创建一种更高效、更有效的方法，将威胁建模的优势应用于其认为会构成最大风险因素的所有威胁。

为未来建模

威胁建模的时代还没有过去——它仍然是应对风险和漏洞的非常有价值的工具。但是，如果企业想要对所有运营进行威胁建模，那么既定的建模方法会使整个过程大大减慢。

对于企业称之为“皇冠珠宝”的资产——例如保存支付信息或敏感个人数据的系统，由专家团队进行头脑风暴的方式仍然可行。关键是，在对整个企业进行风险评估的同时识别这些系统和漏洞。

通过逆转这一过程——首先使用自动化工具和大量可用的威胁信息来评估整个企业的风险状况，企业可以更快地解决所有高风险威胁，且不会漏掉任何威胁。

这就是安全行业出现的新趋势。考虑到计算和威胁形势的持续发展，如果这一趋势流行起来，对每个企业都会是有利的。

原文名称	Threat modeling needs a reset
作者简介	特雷弗 · 杨 （Trevor Young），是 Security Compass 公司的首席产品官。
原文信息	2021 年 6 月 30 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/06/30/threat-modeling-process/
摘 要	安全行业出现了一个新的威胁建模趋势：企业可以扫描现有系统，整合有关当前和潜在威胁的数据，由此进行威胁建模；而非借助白板和满屋子的安全专家（他们被要求像黑客一样思考，试图识别潜在威胁）进行威胁建模。
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。