安天智甲有效防护 MountLocker 勒索软件

勒索软件名：MountLocker 勒索软件
传播方式：垃圾邮件
加密算法：ChaCha20+RSA
后缀：.ReadManual. 八位随机字符串
支付与金额：需通过暗网地址联系
免费解密工具：暂未发现

近日，安天 CERT 在梳理网络安全事件时发现一个名为 MountLocker 的勒索软件。该勒索软件最早于 2020 年 7 月被发现，在 2020 年 11 月上旬进行了更新，扩大加密文件类型的范围并增加逃避安全软件功能，主要通过垃圾邮件和 CobaltStrike Beacon 进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序。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 MountLocker 勒索软件的加密行为。

MountLocker 勒索软件样本运行后，通过批处理文件从受害主机中窃取敏感文档回传到指定的 FTP 服务器，随后创建多个线程，在短时间内完成对计算机上相关文件的加密，在被加密文件的后缀名后追加以“.ReadManual. 八位随机字符串”命名的后缀。加密完成后，删除系统卷影副本，以防止恢复加密文件，并在加密文件所在的文件夹中创建一个名为“RecoveryManual.html”的勒索信，该勒索信具体内容包含了勒索说明、暗网联系地址。为了迫使受害者尽快缴纳赎金，

▲MountLocker 勒索信

勒索信中威胁受害者如在接下来的几天不联系攻击者，其将在网上公布受害者数据。

MountLocker 勒索软件采用“ChaCha20+RSA”加密算法加密文件，并使用 RSA-2048 对文件加密密钥进行加密，目前被加密的文件在未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、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态(Win7 x64）鉴定器、信标检测鉴定器等鉴定分析。

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	5eae13527d4e39059025c3e56dad966cf67476fe7830090e40c14d0a4046adf0
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	95 KB
MD5	0BC638D8C24A8DBD1C17BCA989281624
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Zudochka
判定依据	反病毒引擎

◆操作系统

操作系统	内置软件
Win7 x64 6.1.7601 Build 7601	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
删除全盘所有卷影副本	★★★★
修改文件权限	★★★
删除自身	★★★★

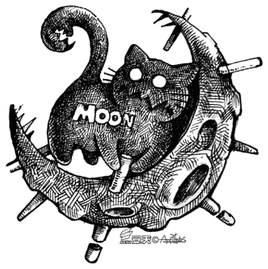
◆常见行为

行为描述	危险等级
获取计算机名	★
设置调试器权限	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
访问文件尾部	★
获取系统版本	★
获取驱动器类型	★
加载运行时 DLL	★

◆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01月04日(总第261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

“灵猫”组织针对中东地区的攻击活动分析报告



“灵猫”组织（又名 Moonlight、Molerats、Gaza Hackers Team、Gaza Cybergang）是一个来自加沙地区的 APT 攻击组织，其最早的攻击活动时间可追溯至 2012 年。国外安全厂商 ClearSky 曾在 2016 年所发的“Operation DustySky”报告中指出该组织的背后为哈马斯（伊斯兰抵抗运动组织的简称）。

安天 CERT 从 2020 年 10 月份开始陆续捕获到“灵猫”组织针对中东地区进行攻击的样本，在本次攻击活动中“灵猫”组织使用的工具更为丰富，不仅包括在既往活动中使用的通过 ENIGMA 打包的 Spark 恶意软件，还有在此前未发现被使用的 .NET 框架的 MoleStage 恶意软件，以及自研的 Python 后门恶意软件 MoleCloud。其中 MoleCloud 网络通讯全程利用正常网站的信息发布和存储服务进行指令交互、窃密数据上传和下载文件执行，通过利用合法的 Web 服务，MoleCloud 在抵达端点后可以在流量侧隐匿自身的攻击活动，若未被端点侧安全产品发现，则 MoleCloud 将能长期潜伏于目标端点中。

在使用 ATT&CK 框架对“灵猫”组织在本次攻击中所使用的技术进行总结时，安天采用的是最新版本的 ATT&CK 框架。在最新版本 ATT&CK 框架中，战术阶段由原来的 12 个变成了 14 个，增加了侦察以及资源开发这两个新的战术阶段。

（本文为报告节选，完整报告请扫描下方二维码查看）

川崎重工披露未经授权访问其系统的安全事件

日本川崎重工（Kawasaki Heavy Industries）披露了一项安全漏洞，该公司发现多个海外办事处对日本公司服务器的未授权访问。川崎重工在一次内部审计中发现了这一事件，其 IT 员工注意到“一个本不应该发生的从海外办事处（泰国）到日本服务器的连接。”川崎重工宣布，该公司受到了外部未经授权的访问。经过彻底的调查，该公司发现海外办事处的一些信息可能已经泄露给了外部各方。目前，该公司没有发现任何向外部网络泄露信息的证据。这家日本公司宣布已经加强了对海外办事处访问的监控操作，同时也限制了海外访问其日本服务器的权限。11 月 30 日，公司恢复了海外办事处与日本总部之间中断的网络通信。

（原文链接：https://securityaffairs.co/wordpress/112765/data-breach/kawasaki-heavy-industries-cyber-attack.html）

每周安全事件

类 型	内 容
中文标题	SolarWinds 黑客旨在访问受害者的云资产
英文标题	SolarWinds hackers aimed at access to victims’ cloud assets
作者及单位	Pierluigi Paganini
内容概述	微软 365 Defender 团队透露，SolarWinds 供应链攻击背后的威胁参与者的目标是，一旦 Sunburst/Solorigate 后门感染了受害者的网络，他们就会转移到受害者的云基础设施。只要部署了后门，威胁参与者就利用它来窃取凭证、提升权限，并在目标网络内进行横向移动，以获得创建有效 SAML 令牌的能力。微软专家报告说，攻击者通过窃取 SAML 签名证书或通过添加或修改现有联合身份验证信任来创建有效的 SAML 令牌。然后，攻击者创建了 SAML 令牌来访问云资源并窃取电子邮件和敏感数据。
链接地址	https://securityaffairs.co/wordpress/112773/hacking/solarwinds-solorigate-attack-chain.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 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	Struts2 远程代码执行漏洞（CVE-2020-17530）	高	Apache Struts2 存在远程代码执行漏洞。攻击者利用该漏洞，可通过构造特定参数，获得目标服务器的权限，实现远程代码执行攻击。
	Mozilla Firefox 内存破坏漏洞（CVE-2020-26969）	高	Mozilla Firefox 83 之前版本存在内存破坏漏洞。攻击者可利用该漏洞导致内存破坏并执行任意代码。
	Cisco IoT Field Network Director 存在 SQL 注入漏洞（CVE-2020-26075）	高	Cisco IoT Field Network Director 存在 SQL 注入漏洞。攻击者可利用该漏洞访问受影响设备的后端数据库，成功利用该漏洞可以使攻击者可利用该漏洞获得对受影响设备的后端数据库的访问。
较为活跃样本家族	Trojan[Banker]/Win32.Emotet	中	此威胁是一个具有窃取银行账户行为的木马家族。该家族木马在执行后会在后台对进程进行监控，监视登陆银行页面的进程并记录信息，回传攻击者服务器。
	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[Backdoor]/Win32.Delf	中	此威胁是一种后门类木马家族。该家族是通过开发语言 Delphi 来命名的。该家族样本运行后，会在被感染的电脑中打开后门，黑客利用后门窃取用户的隐私信息。
	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]/Win32.Tiny	中	此威胁是一种窃密类木马家族。该家族木马运行后连接远程服务器下载恶意代码并执行，可以窃取用户敏感信息。
	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。

2021 年的 SaaS 安全

埃瑞克·卡森布罗德 / 文 安天技术公益翻译组 / 译

今年，企业通过“软件即服务”（SaaS）业务模式转向基于订阅的服务已不是什么新鲜事。这是企业本地数据中心和应用程序等更大转变的一部分，而这些转变已经进行了数年。疫情加速了这一转变——随着公司寻求虚拟协同和会议工具，SaaS 订阅不断增长。

这导致员工与业务应用交互的方式发生变化，对全球的 IT 部门都带来了影响。因此，公司必须确保 SaaS 供应商能够保护其公司数据，且员工在未连接到办公室网络的情况下能够安全地使用这些 SaaS 解决方案。

2021 年，随着企业使用多个 SaaS 供应商，端点激增以及攻击技术的不断发展，企业的 IT 专家需要应对更大的安全风险。他们将通过以下三种方法来增强安全性。

IT 部门增强安全架构

员工与应用交互的方式发生变化，要求企业重新思考安全架构。只有当员工在访问云解决方案之前登录网络的情况下，SaaS 访问 IP 白名单才会起作用。但是，员工日益倾向于直接访问云解决方案。

IT 部门将使用云原生解决方案进行响应，以重新控制重要功能，例如补丁管理、配置管理和保护未连接到公司网络的设备。他们还将寻求“自带设备”（BYOD）安全策略，并采用更现代的安全架构方法，包括云安全和访问管理保护，例如多因子身份鉴别和与 SaaS 应用联合等。

在 2021 年，企业的安全架构措施可能还包括审查 SIEM 日志集成、与云访问安全代理合作等。通过安全架构在安全策略实施和业务需求之间取得平衡，对于 IT 部门至关重要。

通过多学科团队改善 SaaS 监管

IT 领导者很清楚，未经审查的 SaaS 解决方案（影子 IT）会带来各种风险，包括敏感信息泄露、数据所有权问题和合规性问题。企业需要考虑，谁能够更好地减轻这些风险。到 2021 年，更多的公司将采用多学科战略。

主动的监管方法需要已定义的流程，该流程涉及多学科的团队。该团队可以确保可见性并直接解决风险，以将风险保持在可接受的水平内。公司必须根据完整性、机密性和可用性对数据进行分类，以在安全性和成本之间找到理想的平衡，并确定可接受的风险水平。

云提供商与公司共同承担着确保数据安全的责任。因此，企业应明确双方分别应对哪些内容负责，这一点很重要。公司通常需要管理用户访问、端点设备和数据；而 SaaS 供应商则需要监管应用程序、虚拟机、数据库等。

为了实现监管目标，IT 领导者将寻求提供多种配置选项的 SaaS 提供商，包括口令设置 / 身份联合和授权模型，以及可用性计划（实现与恢复时间和恢复点相关的目标）等。

采用宏观方法评估 SaaS 供应商

考虑到员工所采用的云解决方案数量众多，将供应商的安全措施与公司各方面的要求进行对比并不容易。2021 年，通过审查诸如供应商安全认证和保证报告（ISO 27001，SOC1/SOC2）等因素，公司将更有可能从宏观角度评估或重新评估供应商。

IT 领导者还可以通过问卷调查来获取安全实践，使用诸如 Cloud Security Alliance 等组织的最佳实践来定义需求。此外，测试也将发挥重要的作用，企业可以通过两种方法进行测试：（1）供应商共享的第三方渗透测试；（2）供应商按照其要求执行测试。

公司应意识到，许多 SaaS 提供商将使用子提供商（例如 AWS、Micosoft Azure 或 Google Cloud）来托管其服务。这样一来，SaaS 提供商就可以利用子提供商的安全功能，这会带来许多优势。同时，SaaS 用户应评估，SaaS 供应商在与子云提供商进行交互时是否能够确保数据安全。

此外，IT 部门将要求供应商升级客户能力，包括识别联合或口令设置、定义用户角色、分配职责等能力。IT 部门还应在必要时以安全方式进行系统间集成，并确保数据存储位置符合任何适用的法规要求，例如 GDPR。

结论

疫情期间，SaaS 解决方案的使用激增。在 2021 年，这一趋势将会持续下去。对于 IT 团队来说，在保护数据的同时快速扩展对设备、解决方案和信息的访问是非常严峻的挑战，这样可以确保企业在疫情期间保持业务连续性。在过去的几个月中，数百万公司的 IT 领导者及其团队做了大量的工作。

随着 2021 年的到来，IT 部门将寻求巩固收益并确保安全运营。富有远见的 IT 专家将通过升级安全架构、采用更广泛的监管方法和更有效地评估供应商来满足新要求。这些措施将使其公司享受 SaaS 环境的优势，同时更有效地减轻风险。

原文名称	SaaS security in 2021
作者简介	埃瑞克 · 卡森布罗德（Eric Kaasenbrood）。埃瑞克 · 卡森布罗德是 Unit4 的安全专家。
原文信息	2020 年 12 月 28 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/12/28/2021-saas-security/
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。