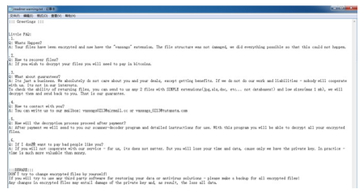
安天智甲有效防护 Makop 勒索软件变种

近日，安天 CERT 在梳理网络安全事件时发现一个 Makop 勒索软件新变种。该勒索软件隶属于 Makop 勒索软件家族，该变种最早于 2021 年 2 月被发现，主要通过垃圾邮件进行传播，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 Makop 勒索软件新变种的加密行为。

该勒索软件样本运行后，删除系统卷影副本和本地计算机的备份目录，以防止恢复加密文件。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，在被加密文件的文件名后追加名为“.[USER_ID].[联系邮箱].vassago”的后缀。并在加密文件所在的文件夹中创建一个名为“readme-warning.txt”的勒索信，该勒索信具体内容包含了勒索说明以及联系邮箱等信息。



▲Makop 勒索信

Makop 勒索软件采用“AES + RSA”加密算法加密文件，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、动态（Win XP）鉴定器、动态（Win7 x86）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、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	41A1FA524A93929A68B58064BB1F86F7
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	281 KB
MD5	41A1FA524A93929A68B58064BB1F86F7
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Makop
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=41A1FA524A93929A68B58064BB1F86F7

◆危险行为对比

行为描述	危险等级	动态 (WinXP)	动态 (Win7 x86)
dll 劫持	★★★★★	√	√
检测虚拟机	★★★★★	√	√
删除全盘所有卷影副本	★★★★	√	x
延时	★★★	x	√
查询系统硬盘大小	★★★	x	√

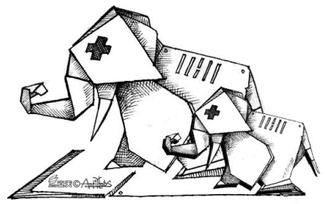
◆常见行为对比

行为描述	危险等级	动态 (WinXP)	动态 (Win7 x86)
疑似查找浏览器进程	★★	√	x
读取自身	★★	√	√
敏感位置创建快捷方式	★★	√	x
获取当前激活的窗口	★★	√	√
创建挂起进程	★★	x	√
WMIC 调用执行	★★	x	√
文档篡改	★★	x	√
设置文件属性为隐藏	★★	x	√
感染文件	★★	x	√
疑似桌面控制	★	√	x
加载运行时 DLL	★	√	√
获取驱动器类型	★	√	√
获取驱动加载权限	★	√	x
打开自身进程文件	★	√	√
创建快捷方式	★	√	√
……	……	……	……

◆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03月01日(总第267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

“幼象”组织针对巴基斯坦国防制造商的攻击活动分析报告



“幼象”组织是一个来自南亚次大陆方向的 APT 攻击组织，其最早由安天在 2020 年 1 月 15 日发布的《“折纸”行动：针对南亚多国军政机构的网络攻击》[1] 报告中所披露。“幼象”组织攻击活动最早可追溯到 2017 年 7 月，其主要攻击目标为巴基斯坦、孟加拉、斯里兰卡和马尔代夫等南亚国家的政府、军事、国防、外交、核能、金融、教育、电信等部门及行业。“幼象”组织使用的木马武器既有开源工具，如：Empire 渗透框架和 Exploit Pack 漏洞攻击平台。同时也有自研 C++ 编写的窃密木马（可借助 U 盘进行横向移动突破隔离网络，窃取隔离网络主机文件）、Python 语言编写的木马以及 Go 语言编写的木马。

安天 CERT 近期在 APT 组织攻击活动狩猎工作过程中，捕获到一起“幼象”组织针对巴基斯坦国防制造商的攻击活动。在本次攻击活动中“幼象”组织主要使用恶意 LNK 文件下载执行远程 HTA 投递自研的 Shell 后门恶意软件“WRAT”，该样本与我们之前披露的“幼象”样本十分相似。在对“WRAT”恶意软件进行分析发现，该木马不仅有后门功能，同时具有窃取移动磁盘文件和感染新接入存储设备的能力（将自身伪装成文件夹复制到磁盘根目录），尝试进行横向移动扩大感染范围。

（原文连接：https://mp.weixin.qq.com/s/y2kRbYCt94yPu-5jtcZ_AA）

扫描上方二维码阅读原文

首个 D 语言勒索软件，安天智甲有效防护

近日，安天 CERT 捕获到一种通过伪装为常见 Windows 应用的安装程序进行传播的 Vovalex 勒索软件。该勒索软件最早出现于 2021 年 1 月，它是目前发现的首个使用 D 语言编写的勒索软件。

防护建议

针对该勒索软件安天建议个人及企业采取如下防护措施：

● 个人防护

（1）安装终端防护：安装反病毒软件。建议安天智甲用户开启勒索病毒防御工具模块（默认开启）；

（2）加强口令强度：避免使用弱口令，建议使用 16 位或更长的密码，包括大小写字母、数字和符号在内的组合，同时避免多个服务器使用相同口令；

（3）及时更新补丁：建议开启自动更新功能安装系统补丁，服务器应及时更新系统补丁；

（4）关闭高危端口：如无使用需要，建议关闭 3389、445、139、135 等高危端口；

（5）定期数据备份：定期对重要文件进行数据备份，备份数据应与主机隔离；

（6）下载正版软件：建议使用官方网站下载的正版软件。如无官方网站，建议使用可信来源进行下载，下载后使用反病毒软件进行扫描。

● 企业防护

（1）开启日志：开启关键日志收集功能（安全日志、系统日志、PowerShell 日志、IIS 日志、错误日志、访问日志、传输日志和 Cookie 日志），为安全事件的追踪溯源奠定基础；

（2）设置 IP 白名单规则：配置高级安全 Windows 防火墙，设置远程桌面连接的入站规则，将使用的 IP 地址或 IP 地址范围加入规则中，阻止规则外 IP 进行暴力破解；

（3）主机加固：对系统进行渗透测试及安全加固；

（4）灾备预案：建立安全灾备预案，确保备份业务系统可以快速启用；

（5）安天服务：若遭受勒索软件攻击，建议及时断网，并保护现场等待安全工程师对计算机进行排查。安天 7*24 小时服务热线：400-840-9234。

（原文连接：https://mp.weixin.qq.com/s/sl1b7u0FczcZFqicE9HQGg）

扫描上方二维码阅读原文

每周安全事件

类 型	内 容
中文标题	专家警告 QuickBooks 文件数据盗窃事件明显增加
英文标题	Experts Warns of Notable Increase in QuickBooks Data Files Theft Attacks
作者	Ravie Lakshmanan
内容概述	QuickBooks 是一款由 Intuit 公司开发和销售的会计软件包。一项新的研究发现，使用社会工程技巧部署恶意软件并利用会计软件，导致 QuickBooks 文件数据盗窃事件大幅度增加。来自 ThreatLocker 的研究人员的一份报告中表示：“大多数情况下，攻击涉及的是经过签名的基本恶意软件，因此很难使用杀毒软件或其他威胁检测软件进行检测。”
链接地址	https://thehackernews.com/2021/02/experts-warns-of-notable-increase-in.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	Microsoft Windows TCP/IP 远程执行代码漏洞（CVE-2021-24074）	高	攻击者可以通过构造特殊 IP 数据包触发该漏洞而获得在目标主机上执行任意代码能力。
	Microsoft Windows TCP/IP 安全漏洞（CVE-2021-24086）	高	攻击者可以通过构造特殊 IP 数据包触发漏洞而导致目标主机发生蓝屏故障。
	Microsoft .NET Framework 安全漏洞（CVE-2021-24111）	高	Microsoft .NET Framework 中存在拒绝服务漏洞，该漏洞源于程序没有正确的处理 XML 文档。远程攻击者通过向 .NET 应用程序利用该漏洞造成拒绝服务。
较为活跃样本家族	Trojan/Win32.Yakes	中	此威胁是一种木马类程序。该家族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.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[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[Ransom]/Win32.Blocker	中	此威胁是一种赎金类木马家族。该家族木马运行后会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。
	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[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。

企业最严重的云基础架构风险

安天技术公益翻译组 / 译

Accurics 公司透露，随着越来越多的企业开始使用托管云基础架构服务，新型云水坑攻击随之出现。

在发现的所有攻击中，有 23% 针对配置不当的托管服务，其中大部分针对默认的安全配置或提供过高权限的配置。

最容易遭受水坑攻击的云环境

最近，一起黑客攻击引发了人们的关注。该攻击表明，攻击者会不断利用最终用户的漏洞，向其传播恶意软件、未经授权地访问生产环境或数据，甚至完全破坏目标环境。这种攻击方法被称为“水坑攻击”。研究人员发现，此类攻击已经开始针对云环境，这会造成更严重的破坏。

此类攻击开始针对云环境的一个原因是，云中开发流程利用托管服务，并不像在本地环境中那样隐藏在企业内部。实际上，它们在很大程度上已经暴露。

一旦犯罪分子能够利用开发管道中的错误配置，不仅会给企业带来灾难，还会给客户带来灾难。为了应对此类风险，企业应假设整个开发流程都能够被访问，并将访问权限设置为“仅限需要的用户访问”。

Accurics 首席技术官（CTO）和首席信息安全官（CISO）欧姆·穆尔坎丹尼（Om Moolchandani）表示：“如今，云原生应用程序和服务比以往任何时候都更为重要，基础架构中的任何风险都会带来严重的影响。”

“我们的研究表明，企业的安全团队正在迅速采用托管服务，这能够提高生产力，保持开发速度。但是，不幸的是，这些团队无法应对相关的风险，他们依赖于默认的安全配置（这会导致访问权限过高）。

就像几年前的存储桶一样，消息服务和“函数即服务”（FaaS）的使用已经进入危险阶段。如历史所揭示的那样，利用这些服务不安全配置的攻击会越来越多。”

在所有环境中，攻击的“平均修复时间”（MTTR）为 25 天。

研究表明，在所有环境中，攻击的 MTTR 为 25 天——对于潜在攻击者而言这是一个福音。需要注意的是，MTTR 也会出现偏离：如果运行时发生配置更改，云风险就会偏离已建立的安全基线。在偏离既定安全基础架构配置的情况下，MTTR 为 8 天。

正如一起广为人知的攻击所揭示的那样，即使企业在创建基础架构时设立了安全基线，但是随着时间的流逝，MTTR 也会出现偏离。在这起攻击事件中，企业在 2015 年将 AWS S3 存储桶添加到环境中并进行了正确配置，5 个月后为解决问题进行了配置更改，但是在工作完成后未正确地进行重置。直到近 5 年后，配置更改被攻击者利用，这一问题才被发现并得以解决。

云基础架构的风险

- 尝试实现“基于角色的访问控制”（RBAC）的 Kubernetes 用户，通常无法以适当的粒度定义角色。这增加了凭证重用和滥用的可能性——实际上，在接受评估的企业中，有 35% 正在努力解决该问题。
- 在 Helm 图表中，有 48% 的问题是由不安全的默认配置引起的。最常见的错误是：默认名称空间（系统组件在其中运行）的使用不当，这使攻击者得以访问系统组件或机密。
- 我们首次在生产环境中看到通过“基础架构即代码”（IaC）定义的身份和访问管理；在检测到的“身份识别与访问管理”（IAM）偏离中，超过三分之一（35%）源于 IaC。这表明，企业正在迅速采用“IAM 即代码”解决方案，这会导致角色配置错误。
- 在已发现的攻击中，近 10% 针对硬编码的机密，23% 针对配置不佳的托管服务。
- 在接受评估的企业中，有 10% 购买了从未启用的高级安全功能。
- 虽说基础架构错误配置的 MTTR 约为 25 天，但修复基础架构中最关键的部分通常需要花费更多的时间——例如，负载平衡服务的 MTTR 为 149 天。由于所有面向用户的数据都流过这些资源，因此理想情况下，应该以最快的速度来修复它们。

保护云基础架构需要一种全新的方法，该方法必须在开发生命周期的早期阶段就考虑到安全性，并始终保持安全状态。企业必须在运行时持续监控云基础架构的配置更改，并评估相关风险。

如果配置更改会带来风险，企业必须根据安全基线重新部署云基础架构。这样一来，企业就可以确保，任何意外或恶意更改都会被自动覆盖。

随着新攻击不断出现，各种风险不断困扰着企业，云网络弹性比以往任何时候都更加重要了，而配置安全则是重中之重。

原文名称	Top cloud infrastructure risks faced by real-world organizations
原文信息	2021 年 02 月 23 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/02/23/top-cloud-infrastructure-risks/
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。