安天发布《Zloader 银行木马变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Zloader 的银行木马变种程序。Zloader 又名 Terdot，自 2016 年以来首次被发现，平均每周发布一至两个新版本。Zloader 的银行木马变种并非采用传统方式进行传播，攻击者采取通过网页广告重定向至恶意的下载站下载恶意代码，通常模仿 TeamViewer、Zoom、Discord 等流行应用程序。

当用户在 Google 浏览器中搜索 TeamViewer 安装程序，之后点击 Google 广告，重定向至攻击者网站下载恶意文件。Zloader 银行木马变种的 Dropper 从经典的恶意宏文档变为已签名的 MSI 恶意文件，并依靠后门程序和 LOLBAS 脚本绕过防御。该恶意代码通常窃取银行凭证。该恶意代码新增禁用 Windows Defender 服务等功能。下载的 msi 文件释放并执行相关脚本与载荷文件，其中 updatescript.bat 的功能是禁用 Windows Defender 所有模块、隐藏恶意软件的所有组件、下载可执行文件并通过 LOLBAS 脚本执行。nsudo.bat 功能为以系统最高权限禁用 Windows Defender 服务。载荷执行后，首先是在 %APPDATA% 内创建随机名称的目录，并在目录中创建自己的副本，然后通过修改注册表项自启动，之后创建名为 msiexec.exe 的傀儡进程并挂起，注入相关代码，当 msiexec.exe 进程恢复后实现窃取 Cookie、登录凭证和所有敏感信息等功能。

安天 CERT 提醒广大政企客户，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱密码，如果业务上无需使用远程桌面服务，建议将其关闭。目前，安天追影产品已经实现了对该类木马的鉴定；安天智甲已经实现了对该木马的查杀。

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、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、动态（Win7 x64）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	tim.exe
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	165 KB
MD5	3393BD9D04BE1FF4E537464E1B79D078
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	BD 静态分析

报告地址：https://1.119.163.6/vue/details?hash=3393BD9D04BE1FF4E537464E1B79D078

◆运行环境

操作系统	内置软件
Win7 x64 6.1.7601 Build 7601	默认、IE9、Google Chrome、Firefox、Office2007、Flash、WPS、FoxitReader、AdobeReader

◆危险行为

行为描述	危险等级
映射内存方式注入	★★★
自启动	★★★
执行解释型脚本	★★★
查询软件限制策略	★★★
在系统目录创建文件	★★★
创建互斥量	★★★
通过标记进程可执行堆绕过 DEP	★★★★★
混淆或加密数据	★★★★
注册或取消对象链接和嵌入控件	★★★

◆常见行为

行为描述	危险等级
获取当前激活的窗口	★★
检测自身是否被调试	★★
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09月27日(总第297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

Sodinokibi/REvil 勒索组织近期活动梳理与最新样本分析

概述

近日，安天 CERT 监测到消失约两个月的 Sodinokibi（又名 Revil）勒索组织重新活跃的迹象。2019 年 6 月，安天在《勒索软件 Sodinokibi 运营组织的关联分析》报告中提到，该勒索组织是一个不断套用、利用其他现有恶意工具作为攻击载体，传播勒索软件、挖矿木马以及窃密程序的具有一定规模的黑产组织，并在全球范围内实施普遍性、非针对性勒索、挖矿、窃密攻击。

9 月 16 日，安全厂商 Bitdefender 发布了免费的 Sodinokibi 勒索软件通用解密器，并声称解密器使用的密钥来自于某执法部门。Sodinokibi 勒索软件的受害者可以通过下载主解密器，一次性解密全部或指定文件夹下的数据。经过测试，该解密器可用于解密 2021 年 7 月 13 日之前版本的 Sodinokibi 勒索软件加密的数据，但对本次新发现的勒索软件新型变种无效。

事件对应的 ATT&CK 映射图谱

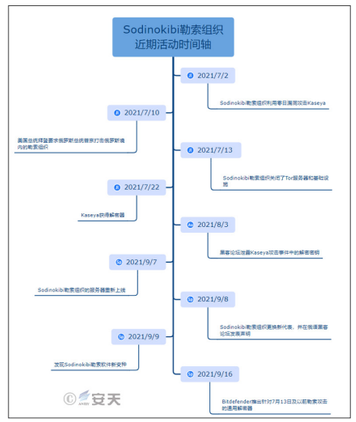
该事件对应的技术特点映射图谱如下：

▲ 该事件对应的 ATT&CK 技术特点映射图谱

活动分析

安天 CERT 通过关联分析，结合已知情报，梳理了 Sodinokibi 勒索组织近期活动时间轴如下：

2021 年 7 月 2 日，Sodinokibi 勒索组织针对美国 IT 管理软件制造商 Kaseya 发起大规模的供应链攻击，致使多个托管服务提供商及其一千多位客户受到影响。被攻击的 Kaseya VSA 是一个基于云的 MSP 平台，为客户提供补丁管理和客户端监控服务。由于该平台具有客户端的管理员权限，导致勒索软件可以在客户系统中快速传播。



▲ Sodinokibi 勒索组织近期活动时间轴

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：

1. 个人防护

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）；

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 .....

2. 企业防护

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提供基础；

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 .....

目前，安天智甲终端防御系统可实现对 Sodinokibi 勒索软件的查杀与有效防护。

样本分析

1. 样本标签

病毒名称	Trojan[Ransom]/Win32.Sodinokibi
MD5	21D01FA87DFCAF971FF7B63A1A6FDA94
处理器架构	Intel 386 or later, and compatibles
文件大小	137.50 KB (140,800 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2021-09-04 14:16:49
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2021-09-09 08:18:10
VT 检测结果	52/66

▲ 样本标签

2. 样本分析

该样本使用 RC4 算法加密存储静态字符串，并在执行时解密，解密函数共有 5 个参数，分别为：加密数据起始地址、待解密数据偏移量、密钥长度、加密数据长度、解密数据存放地址。

根据系统版本使用 bootcfg 或 bcdedit 指令修改系统引导项为带网络连接的安全模式，并添加启动项用于执行自身及恢复被修改的引导项，最后重启系统，以此达到规避安全软件检查及避免待加密文件被占用的目的。（原文链接：https://mp.weixin.qq.com/s/GsX1UbXnmwYIVfeXc-d5YQ）

扫描右侧二维码阅读全文

每周安全事件

类 型	内 容
中文标题	攻击者使用虚假的过期证书通知分发 TeamViewer
英文标题	Hacked sites push TeamViewer using fake expired certificate alert
作者	Sergiu Gatlan
内容概述	攻击者正在破坏 Windows IIS 服务器，以添加过期证书通知页面，提示访问者下载恶意的虚假安装程序。Malwarebytes 威胁情报安全研究人员观察到，该恶意软件是通过使用 Digicert 证书签名的虚假更新安装程序安装的。投放到受感染系统上的有效载荷是 TVRAT（又名 TVSPY、TeamSpy、TeamViewerENT 或 Team Viewer RAT），一旦部署到受感染的设备上，恶意软件将静默地安装并启动 TeamViewer 远程控制软件的一个实例。启动后，TeamViewer 服务器将与命令和控制 (C2) 服务器联系，让攻击者知道他们可以远程完全控制新受感染的计算机。
链接地址	https://www.bleepingcomputer.com/news/security/hacked-sites-push-teamviewer-using-fake-expired-certificate-alert/

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 Scripting Engine 远程代码执行漏洞（CVE-2021-26435）	高	Microsoft Windows Scripting Engine 存在远程代码执行漏洞。由于 Windows 脚本引擎中的边界错误，使得远程攻击者可以创建一个特制的文件，诱使受害者打开它，触发内存损坏并在目标系统上执行任意代码。
	Microsoft MPEG-2 Video Extension 远程代码执行漏洞（CVE-2021-38644）	高	Microsoft MPEG-2 Video Extension 存在远程代码执行漏洞。由于 Microsoft MPEG-2 Video Extension 中的输入验证不正确，使得远程攻击者可以在目标系统上执行任意代码。
	Microsoft HEVC Video Extensions 远程代码执行漏洞（CVE-2021-38661）	高	Microsoft HEVC Video Extensions 存在远程代码执行漏洞。由于 HEVC 视频扩展中的输入验证不正确，使得远程攻击者可以在目标系统上执行任意代码。
较为活跃样本家族	Trojan/Win32.Mansabo	中	此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。
	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.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.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.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[DDoS]/Linux.Xarcen	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要利用漏洞和弱口令对 IoT 设备进行攻击并组建僵尸网络，利用该僵尸网络对任意目标发动 DDoS 攻击。
	Trojan/Android.Fakeapp	中	此威胁是一种伪装类木马家族。该家族样本通常伪装为主要应用程序（Fackbook 等），诱导用户输入账号密码，通过 firebase 联网上传或发送短信等方式窃取用户的账号密码，造成用户隐私泄露和资费消耗。

特权访问管理（PAM）的六个优势

詹妮弗·格雷戈里 / 文 安天技术公益翻译组 / 译

当说到访问时，大家脑海中浮现的第一件事很可能是“口令”。当然，口令是访问管理的重要组成部分，但是还有其他方面需要考虑。企业在进行访问管理时，使用特权访问管理（PAM）解决方案会有所帮助。

如果企业不能正确地管理凭证和访问权限，就会面临遭受攻击的风险。根据 Verizon《数据泄露调查报告》，绝大多数网络安全问题（80%）与凭证被盗或弱凭证有关。

PAM 是什么？

PAM 是一种确定“谁”有权访问网络（包括基础设施和应用程序），然后有目的地管理该访问权限的战略方法。在大多数情况下，这涉及用户的单点登录，以及管理员的单点管理。

访问管理通常涉及用户，但是 PAM 还涵盖应用程序和进程。要想恰当地行使职能，每个用户、应用程序和进程都需要访问网络的不同区域以及其他应用程序。

PAM 既指访问管理工具，也指访问管理进程。企业需要首先购买 PAM 解决方案，然后部署 PAM 进程和工具。

通常，企业和机构会使用“最低权限”原则。即，仅授予每个用户、设备和应用程序完成工作所需的最低限度的访问权限。通过这种方法，企业和机构可以限制访问特权区域的人员，从而降低风险。

许多企业将 PAM 与零信任策略相结合。这意味着，他们需要对每个访问请求进行验证，并假设每个请求都是无效的。由于这两种方法具有相似的原则，因此这些策略可以很好地协同工作。

特权访问管理的优势

PAM 解决方案能够为企业提供诸多优势，包括：

（1）增强可见性。通过部署 PAM 解决方案，企业 IT 团队可以实时地了解“谁”在访问“哪个”网络、服务器、应用程序和设备，且无需手动维护高风险的电子表格。通过跟踪会话时间，企业可以确保供应商和承包商按照要求进行访问。

企业 IT 团队可以看到“谁”在尝试访问未经授权的区域，甚至可以设置告警，这可以为潜在的内部人员攻击提供线索。通过使用基于人工智能的 PAM 工具，一旦用户不遵循其典型行为，IT 团队就会收到告警，以发现可能的凭证窃取活动。

（2）增强合规性。许多行业（例如医疗和金融行业）必须实施最低权限原则，以遵守各项法规。通过部署 PAM 解决方案，企业可以降低审计风险，更轻松地实现合规性。

（3）提高工作效率。大多数 PAM 工具使用自动化技术来执行以往的手动任务，例如口令创建和口令保管，这样可以节省很多时间。

这些工具和结构化流程能够减少人为错误。这样一来，企业 IT 团队就不必花费太多时间来纠正错误，可以节省大量的时间和精力。此外，企业员工在管理口令和访问权限上花费的时间也会更少。

当前，很多企业都转向了混合办公模式。PAM 解决方案对这些企业也有帮助，可防止从多个位置和设备登录时出现访问问题。

（4）跨环境集成。网络安全的一个常见问题是无意中创建了“孤岛”，这会给安全流程增加新的问题。通过部署 PAM 解决方案，IT 团队可以轻松地在整个企业中集成其流程和工具。

企业可以选择与其系统集成的应用程序，并使用单个面板进行管理。此外，企业可以从单个工具创建详细的报告。

（5）减少恶意软件攻击。由于特权账户能够提供广泛的访问权限，攻击者通常会攻击这些账户（例如管理员账户），以更快地传播恶意代码。

通过部署 PAM 解决方案，企业可以更安全地控制访问并限制对企业的访问权限，有助于减少此类攻击。

（6）减少被解雇员工的攻击。通常，前员工可以使用旧凭证来获取访问权限。这些访问很难被发现，而且通常是有害的。

PAM 解决方案能够为企业提供一个内置流程，用于在员工离职时关闭其访问权限。如果确实发生了攻击，PAM 解决方案立即提供对攻击活动的洞察，有助于企业了解攻击造成的损害并迅速进行恢复。

通过部署 PAM 解决方案并关注基础安全措施，企业可以降低风险，同时提高工作效率。

原文名称	6 Benefits of Using Privileged Access Management
作者简介	詹妮弗·格雷戈里（Jennifer Gregory），是一位网络安全作家。
原文信息	2021 年 9 月 17 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/articles/six-benefits-privileged-access-management/
摘 要	PAM 是一种确定“谁”有权访问网络（包括基础设施和应用程序），然后有目的地管理该访问权限的战略方法。PAM 解决方案能够为企业提供诸多优势，包括：（1）增强可见性；（2）增强合规性；（3）提高工作效率；（4）跨环境集成；（5）减少恶意软件攻击；（6）减少被解雇员工的攻击。
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。