关于 CAD 盗图木马的紧急预警

广东省网络与信息安全通报中心

2022 年 06 月 04 日

编号：2022030

目录

一、安全预警

CAD（Computer Aided Design）是利用计算机及其图形设备帮助设计人员进行设计工作的简称。AutoCAD 是国际最知名的 CAD 设计软件。应用范围较广，因此威胁影响范围较大。

近期发现该木马对我国重要企业的渗透传播突然加剧，已有数十家央企单位遭受攻击。

鉴于该木马背后的黑客团伙不仅有明显的窃密倾向，而且逐步呈现与勒索组织和 APT 组织勾联的动态，请各企业网络安全部门高度重视，开展自查、清理和加固工作，避免重要设计文件失窃。

二、事件信息

（一）事件概要

事件名称	CAD 盗图木马		
威胁类型	水坑攻击、数据窃取、勒索攻击	**威胁等级**	高
受影响的应用版本			
• 使用 AutoCAD 软件的单位			

（二）攻击概述

攻击过程如下：

1、通过社会工程学方法向攻击目标发送植入木马的 CAD 项目文件或通过植入木马的 AutoCAD 破解软件下载站进行“水坑攻击”完成木马的初始化传播。

2、利用自身复制完成注册表持久化驻留；

一旦植入木马的 CAD 文件被 AutoCAD 打开，或植入木马的“破解版”AutoCAD 启动，就会自动加载木马所在的恶意 FAS 文件，然后将自身复制到以下三个位置：

(1)当前用户的 Documents 文件夹，即：

C:\Users\John Doe\Documents\acad.fas

(2)AutoCAD 的主 Support 文件夹，即：

C:\JohnDoe\ApplicationData\Autodesk\AutoCAD2019\R23.0\enu\Support\acad.fas

(3)AutoCAD 的主 Program Files 文件夹，即：

C:\Program Files\Autodesk\AutoCAD2019\acaddoc.fas

此后，修改注册表，将“dlr”和“dqs”的环境变量存入（HKCU\Software\Autodesk\AutoCAD\R23.0\ACAD-A001:409\FixedProfile\General）。

3、通过文件分享进行横向移动；

由于 CAD 文件往往随项目文件夹一同分享，该木马也随之传播。常见的传播途径包括 U 盘移动硬盘拷贝、共享文件夹、互联网网盘共享等。

4、与控制服务器通信完成窃密传输。

该木马会暗中通过 Http 协议连接到控制服务器（C2），其通信过程采用了混淆加密方法，加密过程中使用了“dqs”和“dlr”变量值、系统区域设置和实际 AutoCAD 构建的版本号等。以下是完整查询的示例，其中大写字母“O”用作分隔符：

hxxp://sl.szmr.org/cj/?9c5d97bba87f468b9237c9b160c36a43142898157 O 102156291 O 8264 O 23.0s%20(LMS%20Tech)

（三）危害影响

该攻击活动影响较大，攻击者会直接利用窃取工程蓝图进行间谍行为或放在暗网出售，甚至后期会针对重点目标发动勒索攻击。

（四）影响范围

使用 AutoCAD 软件的单位

三、防范建议

该木马的控制服务器主要使用如下域名，各单位可通过 DNS 服务器日志或流量检测设备自行监测、定位受木马控制的主机，同时在互联网边界采取封堵措施。

sq.szmr.org

sqer.szmr.org

sl.szmr.org

y.szmr.org

zxb.isdun.com

建议各单位通过防病毒软件对内网主机进行木马查杀，在主机上查找并清除 acad.fas、acaddoc.fas、acad.lsp、acadapp.lsp、acadappp.lsp 等文件

四、应急处置建议

一旦发现系统中存在被利用的情况，要第一时间上报我中心，同时开展以下紧急处置：

一是立即断开被入侵的主机系统的网络连接，防止进一步危害；

二是留存相关日志信息；

三是通过“防范建议”加固系统并通过检查确认无相关漏洞后再恢复网络连接。