All You Need to Know About AutoCAD SecureLoad

Fenton Webb, Autodesk

Agenda

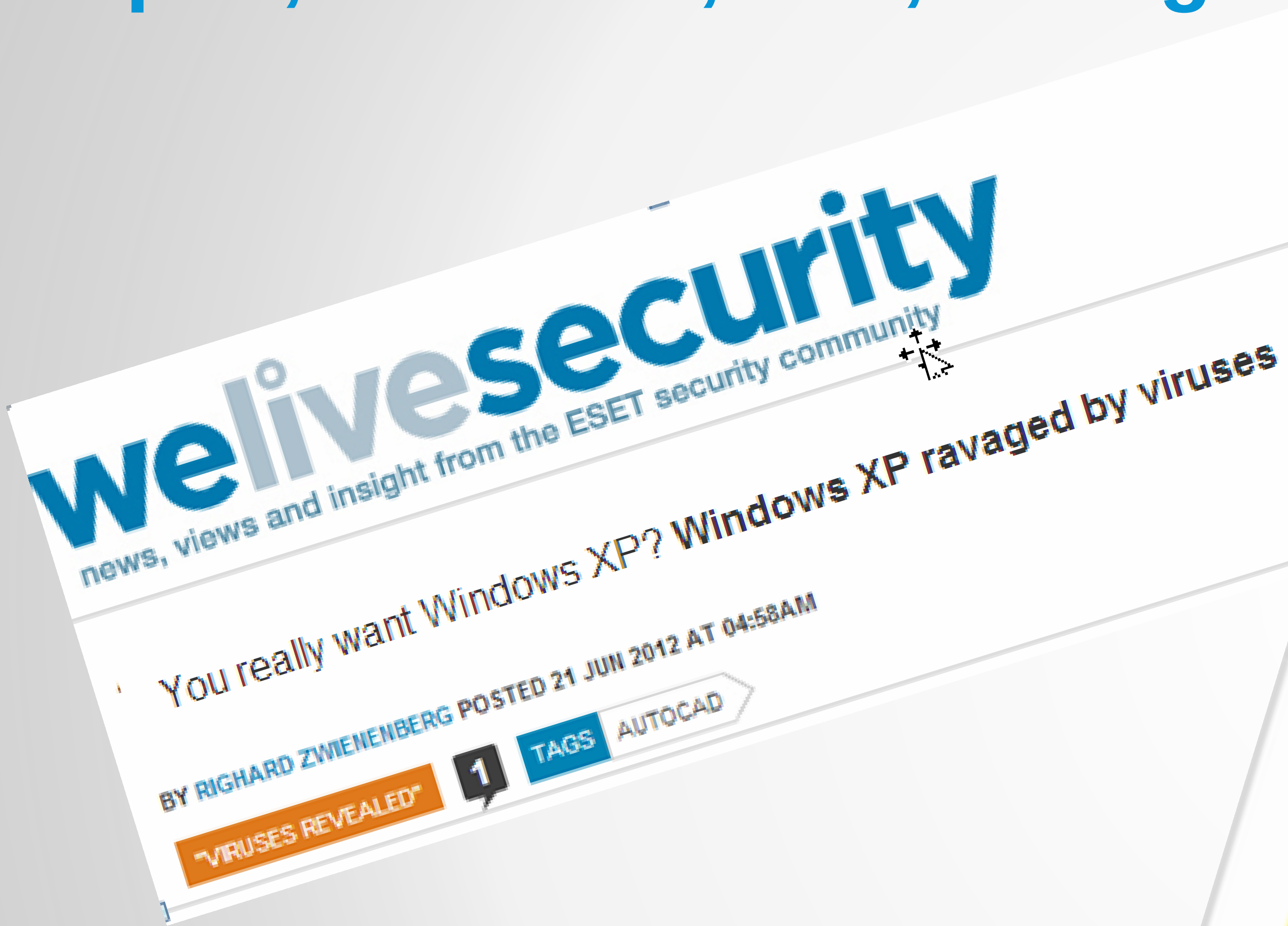
- Brief look at Virus History
- AutoCAD 2012 - First Response
- AutoCAD 2013 sp1/2014 - Enter SECURELOAD
- Questions

Agenda

- Brief look at Virus History
- AutoCAD 2012 - First Response
- AutoCAD 2013 sp1/2014 - Enter SECURELOAD
- Questions

Windows XP

Open, Powerful, and, Ravaged!



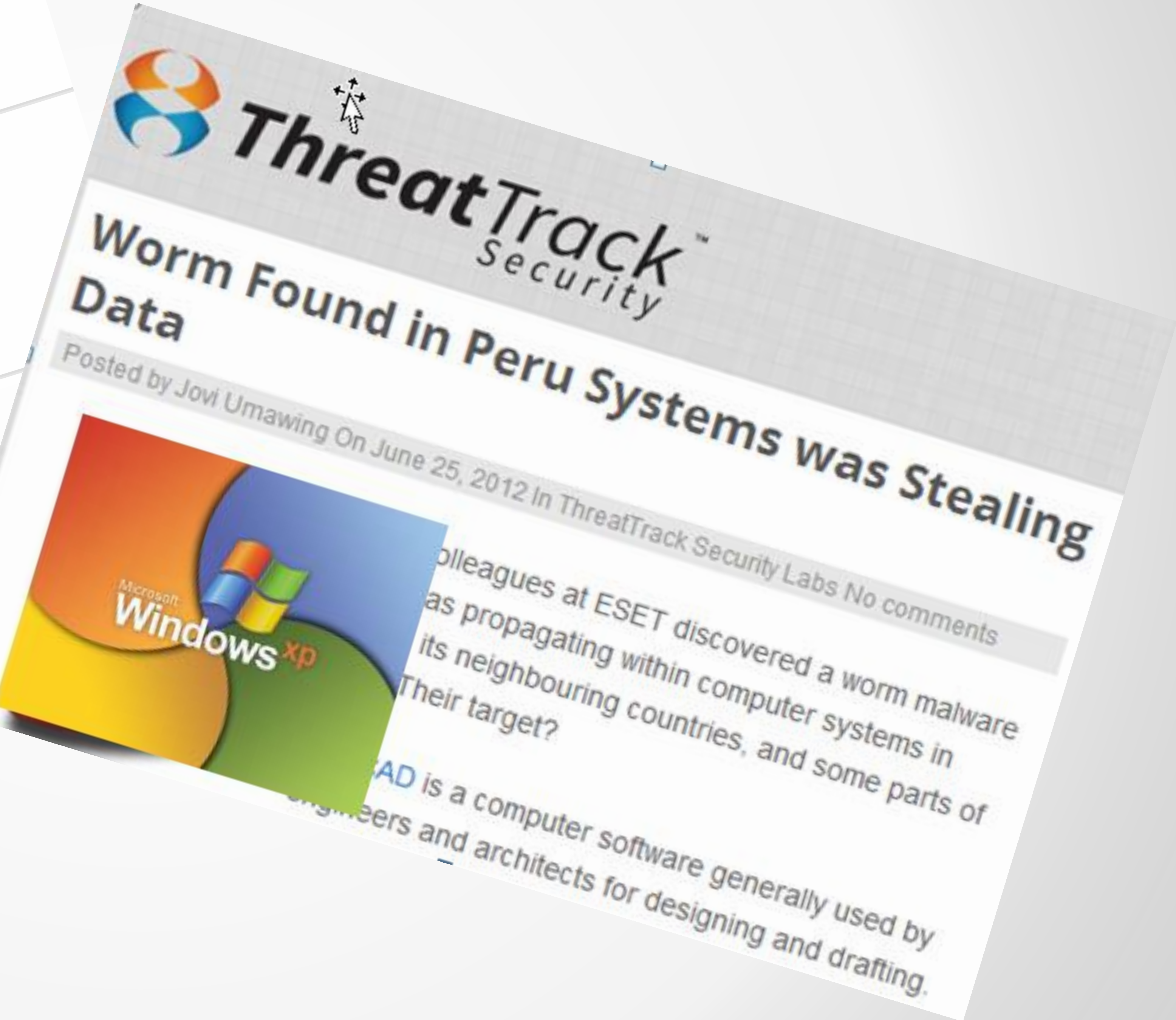
welivesecurity

news, views and insight from the ESET security community

You really want Windows XP? **Windows XP ravaged by viruses**

BY RICHARD ZWIENENBERG POSTED 21 JUN 2012 AT 04:58AM

"VIRUSES REVEALED" 1 TAGS AUTOCAD



ThreatTrack Security™

Worm Found in Peru Systems was Stealing Data

Posted by Jovi Umawing On June 25, 2012 In ThreatTrack Security Labs No comments

olleagues at ESET discovered a worm malware as propagating within computer systems in its neighbouring countries, and some parts of Their target?

AD is a computer software generally used by gineers and architects for designing and drafting.

Windows Vista

The ‘Cure’ for Windows XP users – Se’cure’

- Introduction of UAC (User Access Control)
  - Realization that you can’t detect all virus’s
    - Warn the user that something is about to run, OK?
  - Lock down System files, folders and registry
    - %windir%,%programfiles%, etc – administrator w+
    - Sandboxing of apps run from untrusted locations and domains
      - USB drive, temp folder, etc
    - HKLM - administrator w+

    - Most XP programs stopped working ☹

Windows Vista

Too strict

- Vista Failed
  - Too controlling
  - Too Restrictive
  - Too many UAC warning dialogs
  - Hard migration from XP
- Hello Windows 7!
  - We all learned a valuable lesson

History of AutoCAD Exploits

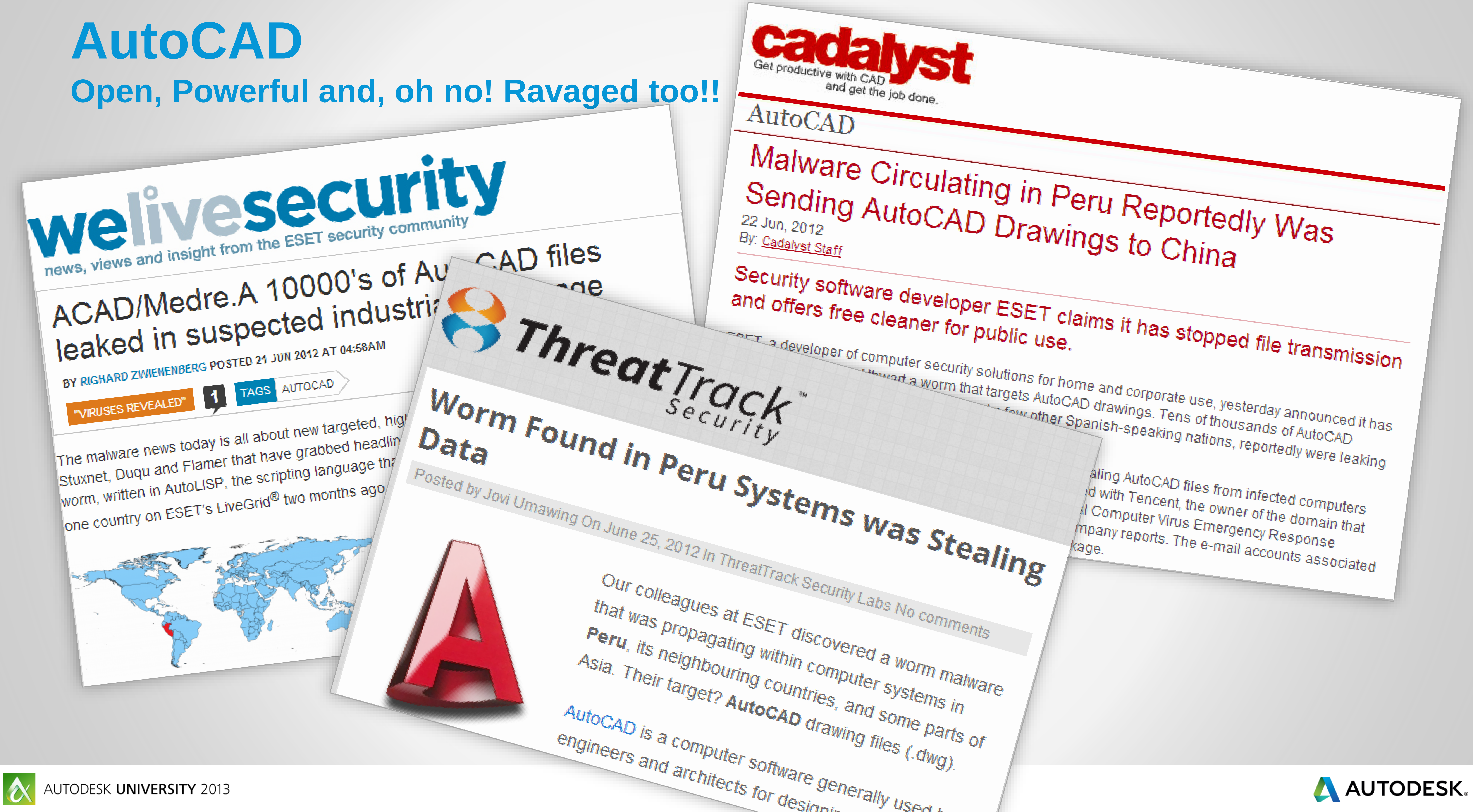
- 2000 - Kaspersky announces the discovery of the first computer virus to affect AutoCAD
  - Classified as a “First try”
  - Low threat

- 2003 – ASL Bursted
- 2009 – acad.vlx, acaddoc.lsp
  - Low threat

- 2012 – ACAD/Medre
  - High threat!!

AutoCAD

Open, Powerful and, oh no! Ravaged too!!



welivesecurity

news, views and insight from the ESET security community

ACAD/Medre.A 10000's of Au CAD files leaked in suspected industria ge

BY RICHARD ZWIENENBERG POSTED 21 JUN 2012 AT 04:58AM

"VIRUSES REVEALED" 1 TAGS AUTOCAD

The malware news today is all about new targeted, hig Stuxnet, Duqu and Flamer that have grabbed headlin worm, written in AutoLISP, the scripting language tha one country on ESET's LiveGrid® two months ago

cadalyst

Get productive with CAD and get the job done.

AutoCAD

Malware Circulating in Peru Reportedly Was Sending AutoCAD Drawings to China

22 Jun, 2012

By: Cadalyst Staff

Security software developer ESET claims it has stopped file transmission and offers free cleaner for public use.

ESET, a developer of computer security solutions for home and corporate use, yesterday announced it has thwart a worm that targets AutoCAD drawings. Tens of thousands of AutoCAD a few other Spanish-speaking nations, reportedly were leaking

aling AutoCAD files from infected computers d with Tencent, the owner of the domain that l Computer Virus Emergency Response mpany reports. The e-mail accounts associated kage.

ThreatTrack Security™

Worm Found in Peru Systems was Stealing Data

Posted by Jovi Umawing On June 25, 2012 In ThreatTrack Security Labs No comments

Our colleagues at ESET discovered a worm malware that was propagating within computer systems in **Peru**, its neighbouring countries, and some parts of Asia. Their target? **AutoCAD** drawing files (.dwg).

AutoCAD is a computer software generally used engineers and architects for design

The Exploit

- The AutoCAD Autoload Feature
  - Load the first acad/acaddoc/acad20xx/acad20xxdoc.lsp/fas/vlx or acad.dvb found in the Support path

- The Problem
  - Zip file containing DWG file (and virus lsp file) unzipped and autoloaded without control
    - Perfect for exploitation!

Agenda

- Brief look at Virus History
- AutoCAD 2012 - First Response
- AutoCAD 2013 sp1/2014 - Enter SECURELOAD
- Questions

First Response

AutoCAD 2012 Service Pack 1

- New system variables
  - LISPENABLED, AUTOLOAD, AUTOLOADPATH
- New command line startup switch
  - /nolisp
- Change load rules for acad20xx.lsp and acad20xxdoc.lsp
- Minor Options Dialog updates

First Response

AutoCAD 2012 Service Pack 1

New system variables

- LISPENABLED
  - Controls whether LISP is enabled for the AutoCAD session (includes LSP, FAS, VLX)
- AUTOLOAD
  - Controls whether or not AutoCAD autoloads LSP, FAS, VLX, DVB files
- AUTOLOADPATH
  - Controls where AutoCAD autoloads acad.lsp/fas/vlx, acaddoc.lsp/fas/vlx, acad.dvb files from

First Response

AutoCAD 2012 Service Pack 1

New Command Line Startup Switch /nolisp

- disables Lisp (.lsp, .fas and .vlx) in AutoCAD
- Turns off new **LISPENABLED**
- Useful for isolation

First Response

AutoCAD 2012 Service Pack 1

Change load rules for acad20xx.lsp and acad20xxdoc.lsp

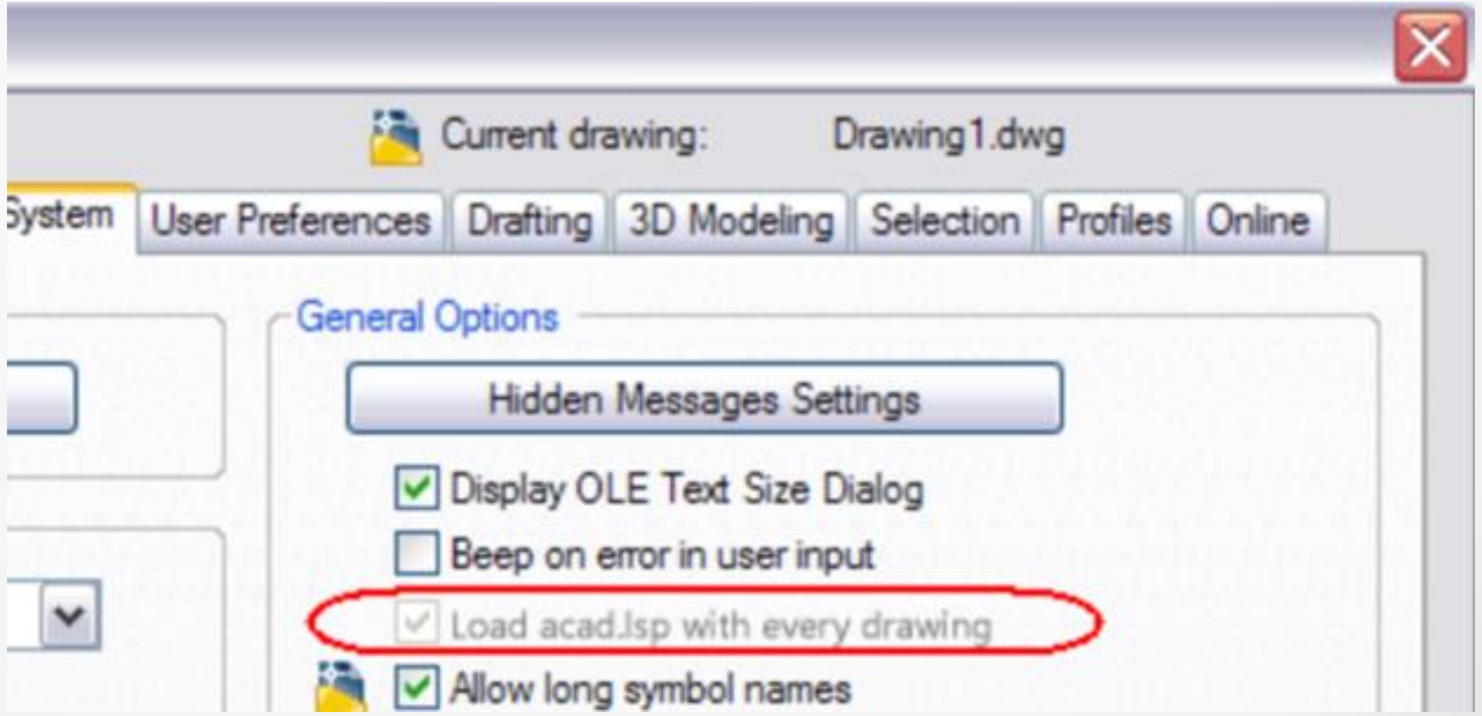
- acad20??.lsp and acaddoc20??.lsp no longer be autoloaded
  - Can now only be run from the AutoCAD install/Support path
    - e.g. Program Files\Autodesk\AutoCAD 2012\Support

First Response

AutoCAD 2012 Service Pack 1

Minor Options Dialog updates

- “Load acad.lsp with every drawing”
  - disabled when AUTOLOAD=0
  - and/or disabled when LISPENABLED=0.



Current drawing: Drawing1.dwg

☑ Display OLE Text Size Dialog

□ Beep on error in user input

☑ Load acad.lsp with every drawing

☑ Allow long symbol names

Agenda

- Brief look at Virus History
- AutoCAD 2012 - First Response
- AutoCAD 2013 sp1/2014 - Enter SECURELOAD

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

- Expanded default file types that are detected by SECURELOAD (formally AUTOLOAD)
- Split AUTOLOADPATH into 2 sysvars (TRUSTEDPATHS, TRUSTEDDOMAINS)
- Added new settings to Options dialog
- Implicitly “trust” digitally signed executable files (DLL, EXE, ARX, DBX, etc.)
- “/safemode” startup switch, SAFEMODE & SAFEMODEAPPS system variables
- New warning dialog to warn users when executable files are detected that are not included in TRUSTEDPATHS & TRUSTEDDOMAINS
- Change Loading for CUIx/MNL files
- Add warning message to warn users when writable locations are specified in TRUSTEDPATHS
- New LISP function (findtrustedfile) as opposed to (findfile)
- Add new settings to Network Deployment Wizard

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

Expanded default file types that are detected by SECURELOAD

- Previously, AUTOLOAD supported LSP, FAS, VLX, DVB
  - AUTOLOAD renamed to SECURELOAD
- SECURELOAD now supports
  - ARX/DBX/CRX
  - LSP/FAS/VLX/MNL
  - .NET assemblies
  - VBA macros, acad.rx, acVBA.arx, acad.dvb
  - Javascript
  - DLL
  - SCR files (located on network)

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

- SECURELOAD SYSVAR Settings
  - 0 - Load without warning (Legacy Behavior).
  - 1 - Load without warning if the file is also in TRUSTEDPATHS & TRUSTEDDOMAINS. If not in TRUSTEDPATHS & TRUSTEDDOMAINS, display warning dialog before loading. Applies to autoloading & manual loading.
  - 2 - Load without warning if the file is also in TRUSTEDPATHS & TRUSTEDDOMAINS. If not in TRUSTEDPATHS & TRUSTEDDOMAINS, do not display warning dialog. Applies to autoloading & manual loading.

- If a file found is not trusted, the command line displays the same error message as selecting “Do Not Load” in the File Loading - Security Concern task dialog. File load canceled: <path\filename>"

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

Split AUTOLOADPATH into 2 sysvars (TRUSTEDPATHS, TRUSTEDDOMAINS)

2012 sp1 AUTOLOADPATH renamed to TRUSTEDPATHS

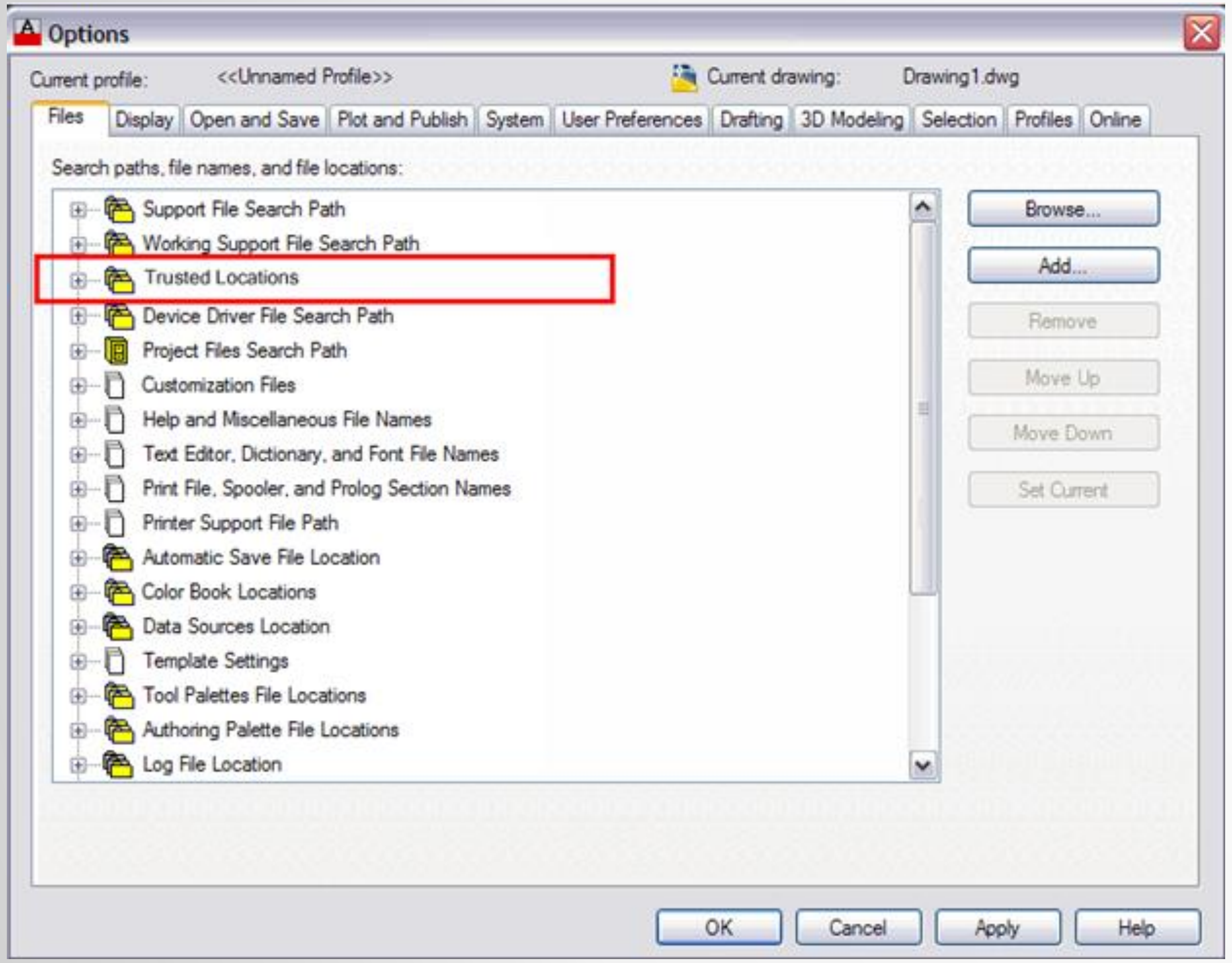
- TRUSTEDPATHS
  - Specifies the folders from where AutoCAD can load and execute files that contain code.
  - Used in conjunction with SECURELOAD= 1 or 2

- TRUSTEDDOMAINS
  - Specifies the domain names or URLs from which AutoCAD can run JavaScript code.
  - Users can specify multiple URLs for JavaScript servers.
    - The URLs support wildcards e.g.:
      - *.autodesk.com/* // trust anything from Autodesk
      - *.autocadws.com/* // trust anything from AutoCAD WS
      - *.codeplex.com/site/MyProject/* // trust anything from a subdomain
      - https://144.111.123.123/* // trust only https protocol from a specific IP address

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

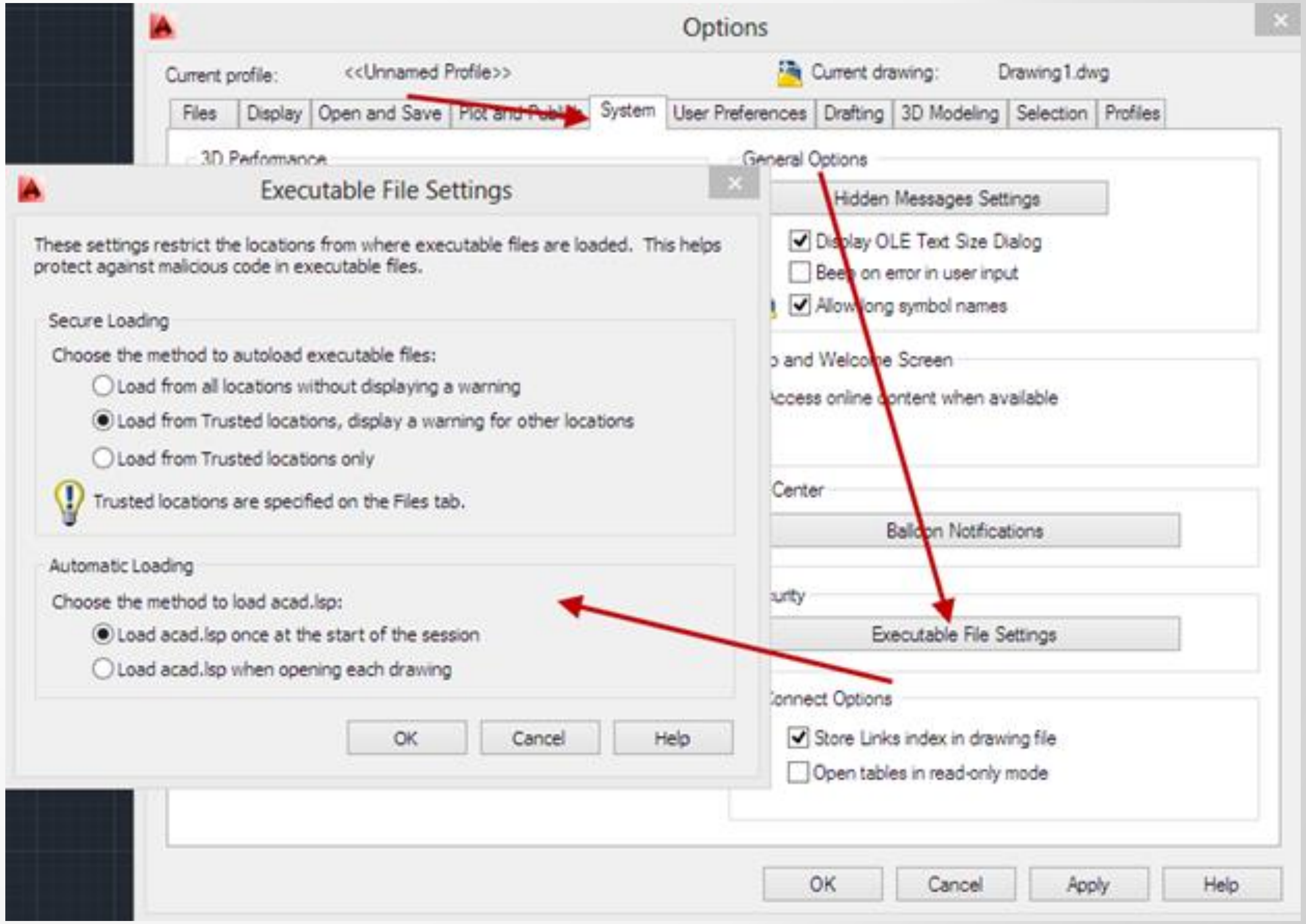
Added new settings to Options dialog



Current profile: <<Unnamed Profile>> Current drawing: Drawing1.dwg

Search paths, file names, and file locations:

- Support File Search Path
- Working Support File Search Path
- Trusted Locations
- Device Driver File Search Path
- Project Files Search Path
- Customization Files
- Help and Miscellaneous File Names
- Text Editor, Dictionary, and Font File Names
- Print File, Spooler, and Prolog Section Names
- Printer Support File Path
- Automatic Save File Location
- Color Book Locations
- Data Sources Location
- Template Settings
- Tool Palettes File Locations
- Authoring Palette File Locations
- Log File Location



Current profile: <<Unnamed Profile>> Current drawing: Drawing1.dwg

☑ Display OLE Text Size Dialog

☐ Beep on error in user input

☑ Allow long symbol names

Access online content when available

☑ Store Links index in drawing file

☐ Open tables in read-only mode

Executable File Settings

These settings restrict the locations from where executable files are loaded. This helps protect against malicious code in executable files.

Secure Loading

Choose the method to autoload executable files:

○ Load from all locations without displaying a warning

● Load from Trusted locations, display a warning for other locations

○ Load from Trusted locations only

Trusted locations are specified on the Files tab.

Automatic Loading

Choose the method to load acad.lsp:

● Load acad.lsp once at the start of the session

○ Load acad.lsp when opening each drawing

OK Cancel Help

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

Implicitly “trust” digitally signed executable files (DLL, EXE, ARX, DBX, etc.)

- All Digitally Signed modules are trusted
  - Regardless of location

- You can obtain Digital Signatures from VeriSign.com

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

“/safemode” startup switch, SAFEMODE & SAFEMODEAPPS system variables

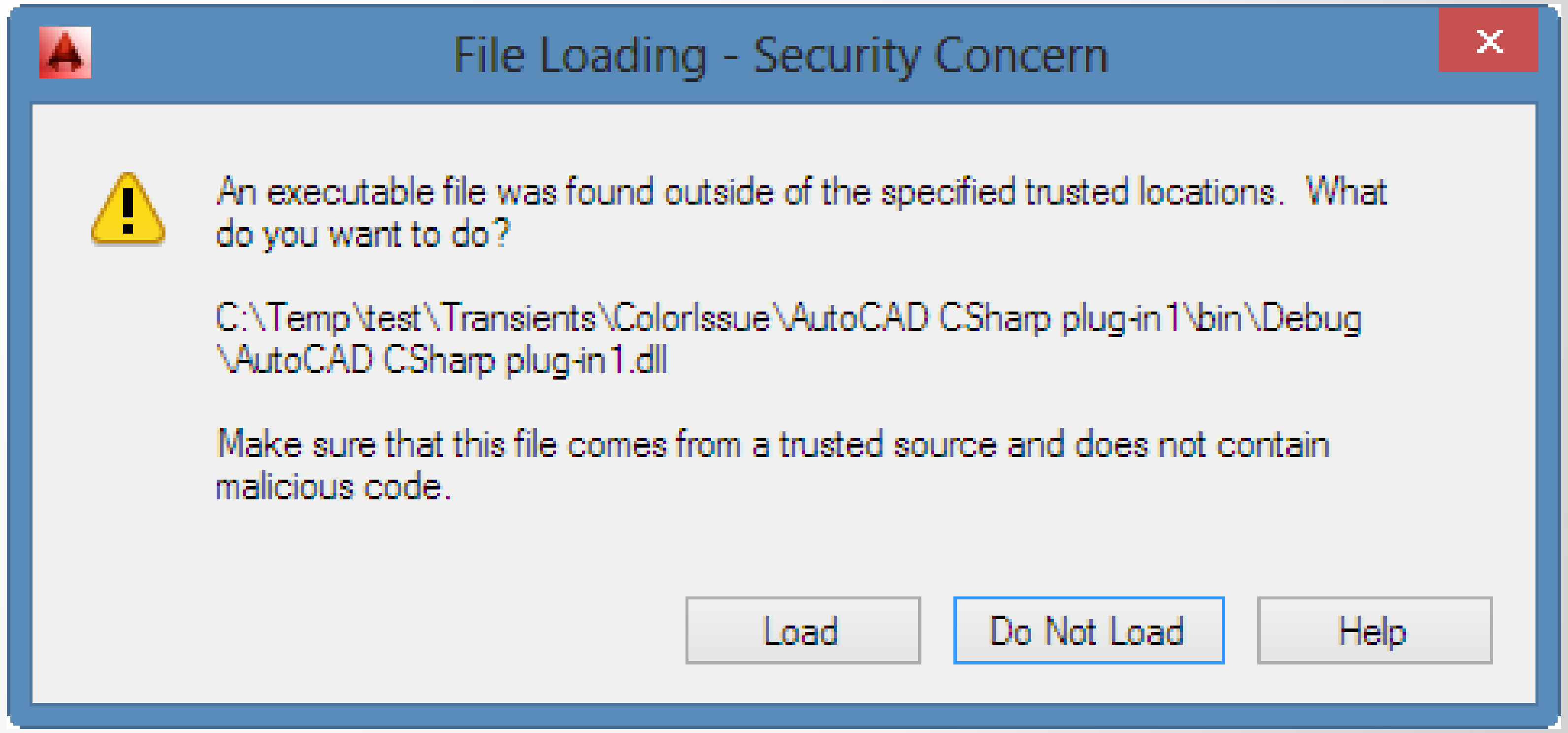
- 2012 /nolisp startup switch renamed to ‘/safemode’
  - /safemode now includes all executable code files too
  - Starts AutoCAD in a ‘bare minimum state’ to allow users to change AUTOLOADPATH in Options dialog without risking loading unsafe modules
- SAFEMODE
  - Specifies whether executable code can be loaded and executed for the AutoCAD session 0 or 1
- SAFEMODEAPPS
  - Specifies which apps can be loaded in safemode.
  - Semi-colon split multiple paths

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

New warning dialog: warn users when executable files are detected that are not included in TRUSTEDPATHS & TRUSTEDDOMAINS

- Dialog appears only when SECURELOAD = 1
- Best way for users to find out something is loading – tell them!



File Loading - Security Concern

An executable file was found outside of the specified trusted locations. What do you want to do?

C:\Temp\test\Transients\ColorIssue\AutoCAD CSharp plug-in1\bin\Debug \AutoCAD CSharp plug-in1.dll

Make sure that this file comes from a trusted source and does not contain malicious code.

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

Change Loading for CUIx/MNL files

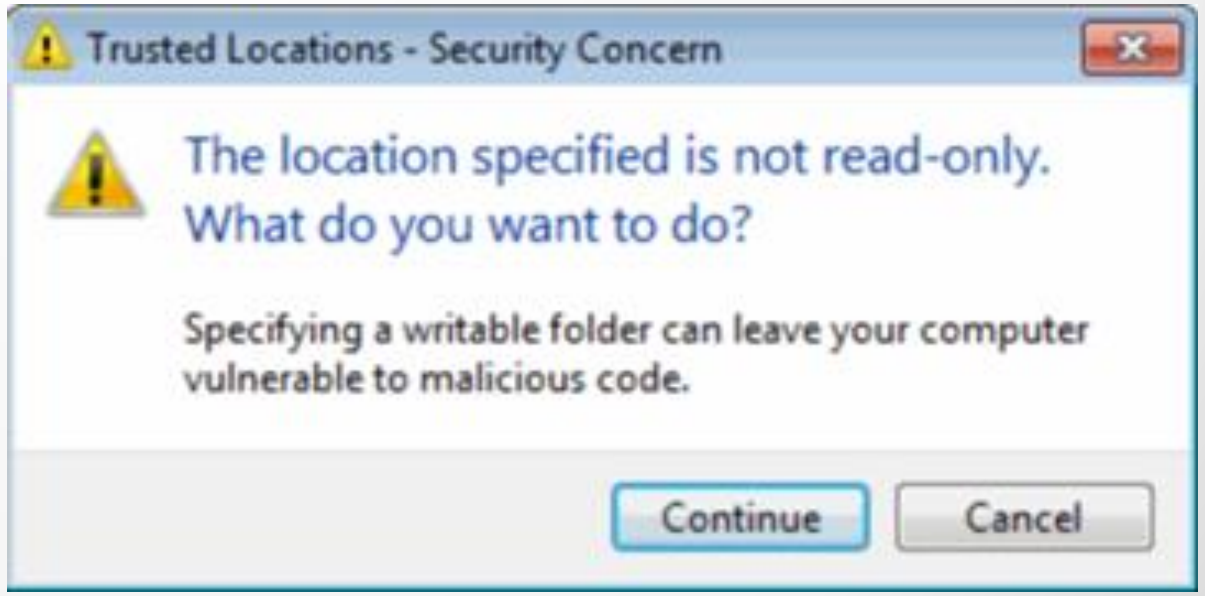
- Previously in the user’s roamable support folder: %appdata%\Autodesk\AutoCAD 20xx - <*lang*>\R19.0\enu\Support
  - **MNL -** moved to the localized Support folder of the Install Dir: C:\Program Files\Autodesk\AutoCAD 20xx\Support\en-us.
  - **CUIX -** staying in the user’s roamable support folder because they need to be easily edited.

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

Add warning message: to warn users when writable locations are specified in TRUSTEDPATHS

- If your Trusted Path is writable under your current login
  - You risk a virus writing itself to that folder
  - Get warned!



The location specified is not read-only.
What do you want to do?

Specifying a writable folder can leave your computer vulnerable to malicious code.

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

New LISP function (findtrustedfile) as opposed to (findfile)

- Behaves the same as the existing (findfile) function except it searches the Trusted Locations (TRUSTEDPATHS)
    - Even your own LISP modules can be protected!

The SECURELOAD Solution

AutoCAD 2013 sp1/2014

Add new settings to Network Deployment Wizard

- Allows the setting of the “Trusted Locations” & “Trusted Domain” Locations
- Deploy the same settings across your Enterprise
  - Without the risk of missing a machine!

Trustworthy Computing

- 2002 - Bill Gates – *“In the past, we've made our software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible.*

  We've done a terrific job at that, but all those great features won't matter unless customers trust our software… when we face a choice between adding features and resolving security issues, we need to choose security.”

- 2012 – Microsoft was the only company that managed to report fewer vulnerabilities in 2012 than its 10-year average, according to a study of vulnerability data by NSS Labs. (eWeek)

Agenda

- Brief look at Virus History
- AutoCAD 2012 - First Response
- AutoCAD 2013 sp1/2014 - Enter SECURELOAD
- Questions?

AUTODESK®