June 2012

Feature article: ACAD/Medre: 10ks of AutoCAD Designs Leaked in Suspected Industrial Espionage

Table of Contents

ACAD/Medre: 10ks of AutoCAD Designs Leaked in Suspected Industrial Espionage

Recently the worm, ACAD/Medre.A, showed a big spike in Peru on ESET's Live Grid® (a cloud-based malware collection system utilizing data from ESET users worldwide). ESET's research shows that the worm steals AutoCAD drawings and sends them to email accounts located in China. ESET has worked with Chinese ISP Tencent, Chinese National Computer Virus Emergency Response Center and Autodesk, the creator of AutoCAD, to stop the transmission of these files. ESET confirms that tens of thousands of AutoCAD drawings, primarily from users in Peru, were leaking at the time of the discovery.

"After some configuration, ACAD/Medre.A sends opened AutoCAD drawings by e-mail to a recipient with an e-mail account at the Chinese 163.com internet provider. It will try to do this using 22 other accounts at 163.com and 21 accounts at qq.com, another Chinese internet provider."

"ACAD/Medre.A represents a serious case of possible industrial espionage. Every new design is sent automatically to the operator of this malware. Needless to say this can cost the legitimate owner of the intellectual property a lot of money as the cybercriminals have access to the designs even before they go into production. They may even have the guts to apply for patents on the product before the inventor has registered it at the patent office."

The Story

The malware news today is all about new targeted, high-tech, military grade malicious code such as Stuxnet, Duqu and Flamer that have grabbed headlines. So imagine our surprise when an AutoLISP virus, AutoLISP is the scripting language that AutoCAD uses, suddenly showed a big spike in one country on ESET's Live Grid® two months ago, and this country is Peru.

We have seen other small number of infections of ACAD/Medre.A in other countries, but they are all in countries that are near Peru or have a large Spanish speaking contingent. The odd one out in the infection table would be the People's Republic of China, but not quite so weird when we started to analyze the virus based on this sudden spike. More about China will follow later.

Of course it does not mean much that we see high detection numbers because they may not all be live infections. But watching ESET's Live Grid®, where we can also see detections at specific URLs, which made it clear that a specific website supplied the AutoCAD template that appears to be the basis for this localized spike as this template was also infected with ACAD/Medre.A. If it is assumed that companies which want to do business with the entity have to use this template, it seems logical that the malware mainly shows up in Peru and neighboring countries. The same is true for larger companies with affiliated offices outside this area that have been asked to assist or to verify the – by then – infected project and then infecting their own environment. Other information that is described later also points to live infections.

So what exactly is ACAD/Medre.A?

ACAD/Medre.A is a worm written in AutoLISP, a dialect of the LISP programming language used in AutoCAD.

ESET detects it as ACAD/Medre.A worm, however the malware also has characteristics which are attributed to a virus or a trojan. It's a worm, because it aids its spreading by copying its

body into the folder of any opened AutoCAD drawing on the infected system (similarly to the way worms create autorun.inf entries on removable media), so if the user would compress the AutoCAD project folder and send it to someone else, they would be sending the worm along with it.It's a trojan, as it mostly relies on the user to - inadvertently, but manually – download it onto his system. It sneaks in alongside legitimate AutoCAD drawings. Or, in a way, it's also a virus, as it infects the installed AutoCAD environment (similarly to the way the Win32/ Induc virus infected the Delphi environment). But it doesn't infect executable files like a common parasitic virus.

But terminology aside, let's take a look at what the Medre malware does.

Conclusion

ACAD/Medre.A is a serious example of suspected industrial espionage. Every new design created by a victim is sent automatically to the authors of this malware. Needless to say this can cost the legitimate owner of the intellectual property a lot of money as the cybercriminals will have designs before they even go into production by the original designer. The attacker may even go so far as to get patents on the product before the inventor has registered it at the patent office. The inventor may not know of the security breach until his patent claim is denied due to prior art.

If there is one thing that becomes obvious from our experience with this piece of malware it is that reaching out to other parties to minimize damage is not only the right thing to do, it really works. We could have tried to clean up the problem without the assistance of Autodesk, Tencent and CVERC and solely focus on removal of the malware from the infected machines. By working with Autodesk, Tencent and CVERC, we were able to not only alert and inform users but also defeat the e-mail relay system used by the attackers and deny them access to the e-mail boxes, so the damage is now contained.

To see an infographic about ACAD/Medre.A go to the annex – image 1

To read the white paper of ACAD/Medre.A visit ESET webpage.

Practical Implications of Malware Analysis

David Harley, ESET Senior Research Fellow

When antivirus researchers such as myself are asked to write about security threats we tend to emphasize the technical details of the threats that we deal with in the virus labs on a day-to-day basis. As a result, we sometimes pay less attention to issues of more immediate and practical concern to a non-technical audience. I thought I would balance this emphasis this by providing a closer look at some practical implications of a threat called ZeroAccess.

My colleague Aleksandr Matrosov recently published an excellent technical analysis of changes to the ZeroAccess rootkit family. This is written for an audience that has a high level of technical understanding, intended to share technical information and stimulate informed discussion. For a technical analysis, we usually have to assume that our readers have a good understanding of the underlying technologies and terminology; otherwise we would have to go into detailed considerations of basic principles that would have technical readers, such as other virus researchers, drumming their fingers in irritation while we go over old ground.

Sometimes, though, even a highly technical article has serious

implications for people who ordinarily may not read such an article. For example, some ESET Threat Blog readers might not have been too interested in the finer points of Aleksandr's earlier article on CVE2012-1889: MSXML use-after-free vulnerability but the problem it describes is already being exploited out there in the wild. In practical terms, the reader didn't have to understand the underlying technology to appreciate the need to install the 'Fix it' patch on systems where the affected software was installed (see Microsoft Security Advisory 2719615). My colleague at Securing Our eCity, Liz Fraumann, refers to this as answering the question: "What does this mean for the end user?"

In the case of ZeroAccess, after some discussion between Stephen Cobb, Aleks and myself, we thought that it might be useful to expand on the way in which ZeroAccess earns a dishonest crust for the criminals behind it. Like many other malware families, ZeroAccess (or Sirefef) sells itself to its partners or affiliates on the strength of the way in which it substitutes its own choices for the results of popular search engines–a form of click fraud.

ZeroAccess uses a P2P (Peer-to-Peer) network protocol for communicating with the C&C (Command and Control server) used by the gang to exploit infected machines by giving instructions to the local malware that allows it to generate illicit income. This income is generated by a 'clicker module' that implements a number of malicious techniques:

- 'Blackhat' SEO (search engine optimization) or index hijacking that helps drive people using search engines like Bing and Google to malicious links.
- Clickjacking – hijacking the user's mouse clicks and redirecting them invisibly to another site for its own malicious purposes
- Substitution of its own choice of URLs for the legitimate results that a search engine would generate for an uncompromised system: in this case, to implement click fraud. We considered another interesting example of click fraud with respect to Cycbot: and the 'Ready to Ride' cybercrime group.

The C&C not only issues commands, but also updates payload modules (what the malware actually does) and lists of malicious URL's in the form of an XML-based configuration file. Aleks points out that the TDL3/TDL4 rootkit/bootkit family is also capable of implementing clickjacking and changes in search results, while Stephen observes that monetizing malware via fake search results is essentially what DNSchanger was doing, albeit by a different process.

Absorbing though the mechanical detail can be, we shouldn't lose sight of the fact that complex malware is created for a reason – i.e. profit – and the way in which a rootkit or bootkit can provide persistent infection (that is, infection over an extended period that survives rebooting) provides a substantial profit for the criminals behind the bot. When it's installed, they make a percentage of the profit on every click or redirection.

Continued and aggressive distribution of ZeroAccess through driveby downloads (where just landing on a malicious URL can result in infection without any action on the part of the victim), offers of fake software downloads and so on, mean that their revenue stream isn't showing signs of drying up for a while yet. And although that revenue stream is not coming out of the pockets of the people infected with this malware—either consumers or corporate users—that revenue stream could be used by the criminals behind the botnet to fund future malicious activity that uses the same infection to steal personal or corporate data and perhaps execute spam and DDoS attacks.

(Note that ESET products will detect and block attempts to infect systems with ZeroAccess, detected as Win32/Sirefef and Win64/Sirefef.)

ESET at Bled: a Wider View of Research

David Harley, ESET Senior Research Fellow

Bled, in Slovenia, is perhaps more associated with gorgeous scenery and the famous Bled cream cake than IT conferences. However, it's been hosting a major European conference for many years, and ESET was represented in some force at the 25th Bled eConference in Slovenia this month.

See annex – image 2

The conference was organized by the Faculty of Organizational Sciences at the University of Maribor, the conference theme being:

- eDependability: Reliable and Trustworthy eStructures, eProcesses, eOperations and eServices for the Future

The conference attracted academics, politicians, representatives of the European Commission and researchers in a wide variety of disciplines from all over the world, including Europe, Australia and the US, addressing an equally wide range of topics from eHealth informatics to data mining, from electronic publications to Smart Cities, from social media to business processes and eco-tourism.

ESET North America's David Harley was one of the keynote speakers, presenting on the topic of 'Targeted Attacks? Everyone is a Target!': after his presentation, he was interviewed for Slovenian television, as he blogged here. Later in the conference, ESET Ireland's Urban Schrott chaired a Panel Session on 'eSecurity: the Evolution and Near Future of Cyberthreats', the other participants being David Harley, ESET Slovenia's Gregor Mustar, and Milan Gabor of Viris.

See annex – Image 3

As you may be able to see from the slide in the background, the scope of the discussion was pretty wide, including topics like:

- How much has the threat landscape really changed in 30 years?
- How important is security software to a modern enterprise security strategy?
- Is it easy to select appropriate security software for your environment?
- Is anti-virus software worth paying for?
- Do highly-publicized botnet takedowns stop malware propagation?
- How relevant is targeted phishing for those of us who aren't RSA or Lockheed?
- What does Stuxnet tell us about threats to national infrastructures and SCADA sites?
- Why is the Conficker botnet still relevant?
- What are the differences in impact between drive-bys, 0-days, 1-days and Forever-days?

- Is the cost-saving of BYOD worth the security issues?
- Has the term social engineering been seriously misused. What do you think?

In the course of the discussion, the panelists each presented on key topics such as:

- Malware as a moneymaker
- Increasing volumes of malware
- Social engineering
- Complex systems and organisation of cybercrime
- Malware in action
- The evolution of malware

Following the presentations, the participants faced a barrage of questions from the floor that lasted until the hotel crew insisted that the session be closed so that they could prepare for the next day's sessions... However, discussion continued with questions later in the lobby as well as sporadically throughout the next day, so that Urban Schrott had to provide an unofficial session for a group of Russian IT students on piracy and malware, white-hat vs. black-hat hacking and cybercrime in general, that lasted nearly an hour. This indicated that the topic of cybersecurity is under-represented even among the academic IT (or ICT) crowd, where even the basic concepts of current cyber threats are often unfamiliar to many. Because of the interest sparked by our input to the conference, the organisers have expressed an interest in hosting ESET as expert contributors again in the future.

The Top Ten Threats

1. INF/Autorun

Previous Ranking: 1
Percentage Detected: 6.28%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://blog.eset.com/?p=94 ; http://blog.eset.com/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

2. Win32/Conficker

Previous Ranking: 4
Percentage Detected: 3.65%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://blog.eset.com/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

3. HTML/ScrInject.B

Previous Ranking: 3
Percentage Detected: 3.57%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

4. HTML/Iframe.B

Previous Ranking: 2
Percentage Detected: 3.55%

Type of infiltration: Virus
HTML/Iframe.B is generic detection of malicious IFRAME tags embedded in HTML pages, which redirect the browser to a specific URL location with malicious software.

5. JS/Iframe

Previous Ranking: 5
Percentage Detected: 2.72%

JS/Iframe.AS is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

6. Win32/Sirefef

Previous Ranking: 6
Percentage Detected: 2.57%

Win32/Sirefef.A is a trojan that redirects results of online

search engines to web sites that contain adware.

7. JS/TrojanDownloader.Iframe.NKE

Previous Ranking: 9
Percentage Detected: 2.10%

It is a trojan that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

8. Win32/Sality

Previous Ranking: 8
Percentage Detected: 1.87%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.
It modifies EXE and SCR files and disables services and process related to security solutions.
More information relating to a specific signature:
http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

9. Win32/Dorkbot

Previous Ranking: 7
Percentage Detected: 1.83%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX.
The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

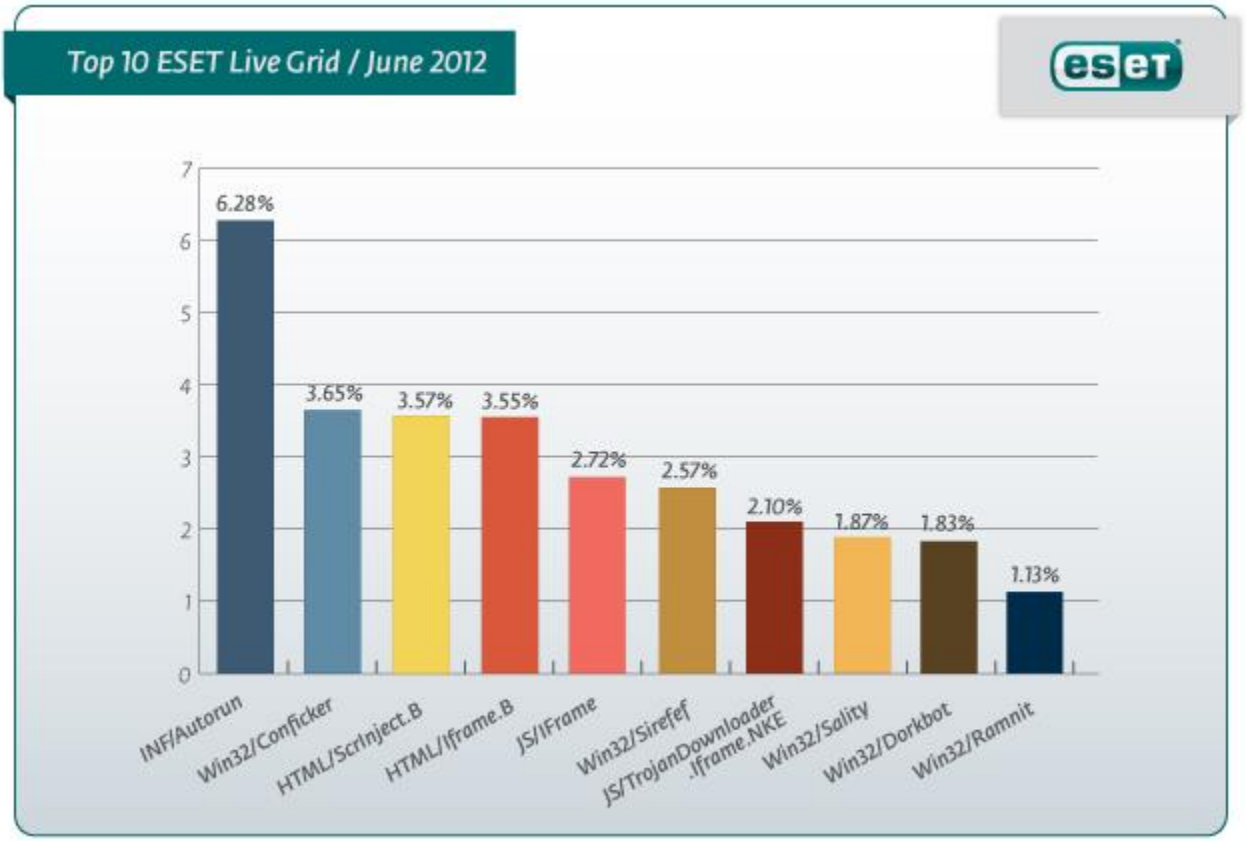
10. Win32/Ramnit

Previous Ranking: 10
Percentage Detected: 1.13%

It is a file infector. It's a virus that executes on every system start.It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer

Top Ten Threats at a Glance (graph)

Analysis of ESET Live Grid, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 6.28% of the total, was scored by the INF/Autorun class of threat.



Annex

Image 1 - ACAD/Medre.A infographic

Image 2 - Pilgrimage Church of the Assumption of Mary, Lake Bled

Image 3 - David Harley, Urban Schrott, Gregor Mustar, and Milan Gabor

About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- ESET Blog
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation