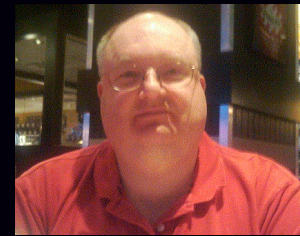


# Tech Tidbits

**Scott Quimby**

**January 2017**



# Microsoft Ends Security Bulletins



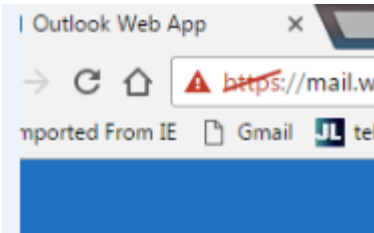
- **Microsoft is no longer going to have security bulletins emailed out starting in February.**
- **Supposedly there will be detailed descriptions on-line in a database that you can query.**



- **TLS 1.0 is now considered an insecure encryption protocol.**
- **SSL 2.0 considered insecure protocol**
- **SSL 3.0 considered insecure protocol**
- **Weak DH Key Exchange**
- **Weak RC4 ciphers**
- **Test your HTTPS sites yourself:**
  - <https://www.ssllabs.com/ssltest/>
- **Often IIS or other server based changes vs. the actual SSL.**



# SSL Security Issue



Google Chrome

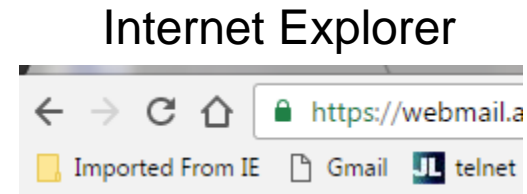
**Security Overview**

This page is insecure (broken HTTPS).

**SHA-1 Certificate**  
The certificate for this site expires in 2017 or later, and the certificate chain contains a certificate signed using SHA-1.  
[View certificate](#)

**Secure Resources**  
All resources on this page are served securely.

**Obsolete Connection Settings**  
The connection to this site uses a strong protocol (TLS 1.2), a strong key exchange (ECDHE\_RSA with P-384), and an obsolete cipher (AES\_256\_CBC with HMAC-SHA1).



## Internet Explorer

**Security Overview**

**This page is secure (valid HTTPS).**

**Valid Certificate**  
The connection to this site is using a valid, trusted server certificate.  
[View certificate](#)

**Secure Resources**  
All resources on this page are served securely.

**Obsolete Connection Settings**  
The connection to this site uses an obsolete protocol (TLS 1.0), a strong key exchange (ECDHE\_RSA with P-256), and an obsolete cipher (AES\_256\_CBC with HMAC-SHA1).

# SSL Security



## Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



# TLS 1.0 Issue growing

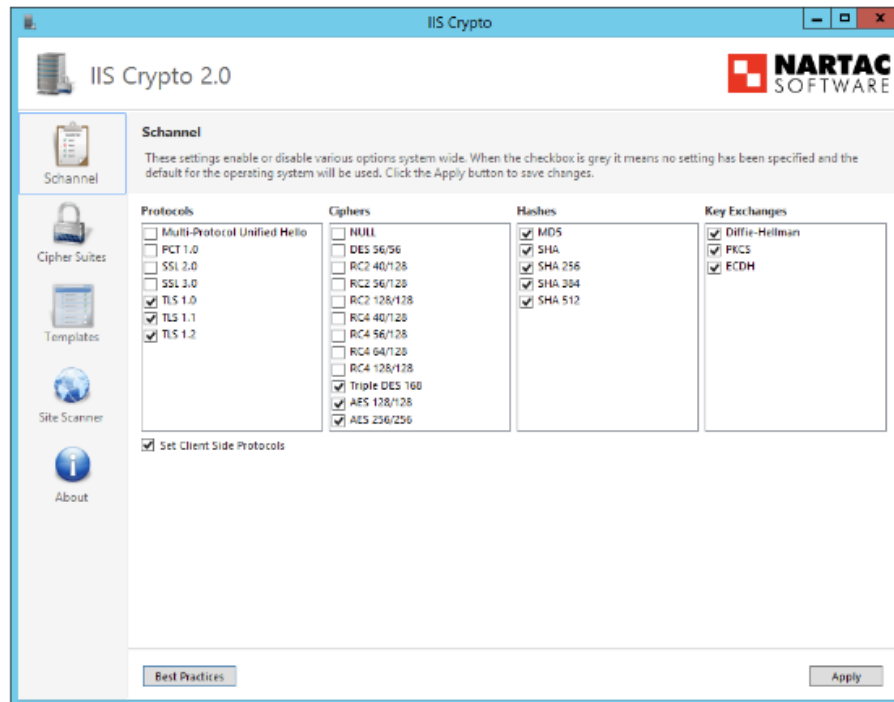


- **Showing up on wireless authentication**
- **Showing up on Microsoft ADFS connections.**



## GUI Tool Exposes Settings in IIS

- <https://www.nartac.com/Products/IISCrypto>



## I Ransomware Spora

- Offline encryption to get around command and control web-sites being blocked via firewalls to prevent criminals from getting money.
- Files encrypted with local key.
- Victim uploads key to site for criminal analysis with payment.
- Criminal downloads decryptor that matches the key provided.
  - <http://www.networkworld.com/article/3156603/security/professionally-designed-ransomware-spora-might-be-the-next-big-thing.html>





## ■ Pay the ransom and you won't get your data back anyway (because these guys are criminals)

- [http://www.infoworld.com/article/3156573/security/pay-the-ransom-you-wont-get-your-data-back.html?idg\\_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm\\_source=Sailthru&utm\\_medium=email&utm\\_campaign=InfoWorld%20Daily:%200Afternoon%20Edition%202017-01-11&utm\\_term=infoworld\\_daily](http://www.infoworld.com/article/3156573/security/pay-the-ransom-you-wont-get-your-data-back.html?idg_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm_source=Sailthru&utm_medium=email&utm_campaign=InfoWorld%20Daily:%200Afternoon%20Edition%202017-01-11&utm_term=infoworld_daily)
- Criminal A infects and encrypts your data.
- Criminal B infects your system and realizes criminal A was here. They delete the encrypted data replacing it with empty files and flip the payment to criminal B to get your data back.
- However, the data is gone because only criminal A knew how to decrypt the data.



# Ransomware variations



- **Cryptowall – What most of us have seen.**
- **SAMSAM – Cryptoworm. Once inside your network, it spreads without user interaction like a real virus would.**
- **Jigsaw - You have an hour to pay. If you don't, it will start deleting your files and increases the number of files it deletes every hour up to 72 hours when it deletes everything.**
- **Chimera – Decryptors available**
- **Cerber – Uses VBScripts (Ransomware as a service affiliate program available)**
- **Crylocker – If you don't pay in 24 hours, it encrypts your data and takes all your personal, security/social media info and publishes it on-line.**
- **HDD Cryptor – Finds every drive or path you have or have ever used and encrypts**
- **TeslaCrypt – Free decryptor from ESET**
- **Locky - Spread via spam and SVG images in Facebook and fake Flash Player update screens.**
  - Source: <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016/#.WG69CnHHGDE.email>



- **A new variant of ransomware encrypts your files. It then demands payment of \$780 in seven days to decrypt *OR* you can share an infection link with two people. If they get infected from your link, the ransomware creator will send you a free decryptor!**
  - <http://www.zdnet.com/article/new-ransomware-decrypts-your-files-if-you-infect-your-friends/>



# Ransomware that publishes you



- Lookout for the one that copies all the files to the cloud in the background before encrypting them, and then when you don't pay the ransom, they publish all the files on the internet.
- Possible partial solution
  - Password protect your files.



# Smart TVs get ransomware!



- This Christmas brought one of the first documented cases of an Android-based smart TV being infected with ransomware
  - <http://www.computerworld.com/article/3153953/security/ransomware-arrives-on-smart-tvs.html>



# Site to look for ransomware decryptors



■ <https://www.nomoreransom.org/>



# Ransomware Early Warning Honeypot



- ❑ **Create a \$honeypot Windows share**
  - This will be before “A” in the list of directories
- ❑ **Get the security so anyone can put files in this folder (i.e. authenticated or anonymous users R/W)**
- ❑ **File it with trash files like text files.**
- ❑ **Setup File Resource Scanning to alert if there is any file activity in this folder.**
- ❑ **The hope is that the crypto variants generally look for shares they can access and start at the top of the directory. If they follow their normal operations, they will find this as the easiest and first share and start to do what they do. That will alert FRS which will hopefully email and text page you to immediately intervene and mitigate the damage.**



# Microsoft Extending Server and SQL support years



- **Microsoft will add six more years of support to Windows Server 2008 and later and SQL Server 2008 and later if you have “Software Assurance” now and you buy “Premium Assurance” starting in March 2017.**
- **Premium assurance will continue to provide only security updates labeled as Critical and Important after the end of life date.**
  - <http://www.networkworld.com/article/3150252/software/why-microsoft-added-6-years-to-windows-server-support.html>





## <https://support.microsoft.com/en-gb/help/10164/fix-windows-update-errors>

- Source:

[http://www.networkworld.com/article/3152602/windows/microsoft-launches-a-windows-error-code-troubleshooting-site.html?idg\\_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm\\_source=Sailthru&utm\\_medium=email&utm\\_campaign=NWW%20Daily%20PM%20Alert%202016-12-21&utm\\_term=networkworld\\_daily\\_news\\_alert#tk.NWW\\_nlt\\_networkworld\\_daily\\_news\\_alert\\_2016-12-21](http://www.networkworld.com/article/3152602/windows/microsoft-launches-a-windows-error-code-troubleshooting-site.html?idg_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm_source=Sailthru&utm_medium=email&utm_campaign=NWW%20Daily%20PM%20Alert%202016-12-21&utm_term=networkworld_daily_news_alert#tk.NWW_nlt_networkworld_daily_news_alert_2016-12-21)



## Microsoft Report Says Hackers 'Weaponizing' Cloud Virtual Machines

- Gain foothold on virtual machines in cloud. The attacker can then use those machines to attack either that public cloud or other public clouds.
  - <http://fw.to/o8uMJYP>



- Why are phishing attacks so difficult to diagnose and stop? Perhaps this stat explains the problem:
  - Roughly 84 percent of phishing sites exist for less than 24 hours, according to [Webroot](#). In other words, phishing attacks are like guerrilla warfare. By the time you realize you may have been attacked, the hackers have moved on to another location...
- This goes right along with the discussion at our security event about the DNS names that are computer generated and live for several hours then die.
  - OpenDNS knows how to kill most of this so that the sites don't resolve and the attack can't really be successful.



## Google Docs hides malware

- <http://www.pcworld.com/article/2015169/malware-uses-google-docs-as-proxy-to-command-and-control-server.html>

## Android 4.0 and 5.0 infected a million Google Accounts

- Gmail
- Google Docs
- Photos
  - <http://www.channelnewsasia.com/news/business/international/android-malware-steals-million-google-accounts-researchers/3332010.html>

## Major cloud is infested with malware:

- <http://www.networkworld.com/article/3137260/security/major-cloud-is-infested-with-malware-researchers-say.html>

# IBM warns of VoIP cyber-attacks



- Cyber-attacks using the VoIP protocol Session Initiation Protocol (SIP) have been growing this year accounting for over 51% of the security event activity analyzed in the last 12 months, according to a [report from IBM's Security Intelligence](#) group this week.
  - <http://www.networkworld.com/article/3146095/security/ibm-warns-of-rising-voip-cyber-attacks.html>



# Mozilla discontinues XP support



## I September 2017

- [http://www.computerworld.com/article/3153392/internet/mozilla-to-scrap-firefox-support-on-windows-xp-and-vista-in-2017.html?idg\\_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm\\_source=Sailthru&utm\\_medium=email&utm\\_campaign=Computerworld%20Wrap-Up%202016-12-26&utm\\_term=computerworld\\_dailynews](http://www.computerworld.com/article/3153392/internet/mozilla-to-scrap-firefox-support-on-windows-xp-and-vista-in-2017.html?idg_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm_source=Sailthru&utm_medium=email&utm_campaign=Computerworld%20Wrap-Up%202016-12-26&utm_term=computerworld_dailynews)



- A new research report reveals that popular wearable devices may leak information as you use them. Researchers discovered that the motions of your hands as you use PIN pads, which is continually and automatically recorded by your device, can be hacked in real time and used to guess your PIN with more than 90 percent accuracy within a few attempts.
  - <https://www.sciencedaily.com/releases/2016/07/160711000130.htm>



# Headphones can be used to record you



- <https://www.engadget.com/2016/11/23/hijacked-headphones-could-be-used-to-listen-in-on-your-life/>





- **Microsoft Office 2007 support ends October 2017**
  - <http://www.zdnet.com/article/microsoft-wont-provide-extended-support-for-office-2007-products-beyond-october-2017-deadline/>



# vSphere 6.5 Released



- <http://defaultreasoning.com/2016/10/18/whats-new-vsphere-6-5/>



## Windows Server 2016 is supported on:

- ESXi 6.0
- 6.0 U1
- 6.0 U2
- 6.5
  - <https://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=16>



- **Check to see if your internet facing device is on Shodan and available for hackers:**
  - <http://iotscanner.bullguard.com/>



# Introducing Microsoft Teams



- **Microsoft Teams is the new chat-based workspace in Office 365.**
  - <https://blogs.office.com/2016/11/02/introducing-microsoft-teams-the-chat-based-workspace-in-office-365/>



# Boomerang for Office 365 and Google Apps



- Boomerang helps its customers focus on email that matters, when it matters. Our tools allow for reading and responding to messages faster and more decisively than before.
- Context-aware.** The next revolution in productivity software will come from software that analyzes the context of what we are working on and adds value on top of it. Leading the shift will require technical skills that few teams have. Fortunately, we have these skills, and cloning the functionality will remain difficult for years to come.
  - Sensible defaults. Context-aware systems will not be perfect, and spending time trying to make them so is a task for academic researchers. Instead, the system needs to supply an easy way for users to change mistakes, without imposing too heavy a burden on them. Designing this interaction properly will be a major challenge, which our team is well suited to conquer.
  - Persuasive Software. Research in practical psychology continues to uncover surprising truths about how our minds work. Our productivity software will incorporate the results of that research into broad, horizontal products. Designing these interactions will require significant skill and discretion, as we have learned from The Email Game.
  - Communication first. Applying our core productivity themes to communication and collaboration software will result in the greatest impact. We will not make the mistake of trying to build a competitor to all of Microsoft Office in one fell swoop, and we will likely never make a spreadsheet.
  - Data-Driven. We believe that data is the closest approximation to the truth. We will base our decisions, wherever possible, on the results of statistically-significant measured data.



# Windows 7 Professional OEM Gone



## ■ The only pre-load OS is Windows 10

- <http://www.networkworld.com/article/3137470/computers/microsoft-stops-sales-of-windows-7-professional-to-oems.html>



# Browser Auto Fill Can Fill Out Phishing Attack



## Things like LastPass and autofill:

- <https://flipboard.com/@flipboard/flip.it%2F101kxM-browser-autofill-used-to-steal-personal/f-141d5ff505%2Ftheguardian.com>





# Ipads unlock with too many characters



- [http://www.csiny.com/2017/01/flaw-allows-thieves-to-open-locked-ipads/?utm\\_source=dlvr.it&utm\\_medium=facebook](http://www.csiny.com/2017/01/flaw-allows-thieves-to-open-locked-ipads/?utm_source=dlvr.it&utm_medium=facebook)
- Fixed in future iOS update.



# FBI Accused of Paying Geek Squad to search through your PCs



- [http://www.csiny.com/2017/01/flaw-allows-thieves-to-open-locked-ipads/?utm\\_source=dlvr.it&utm\\_medium=facebook](http://www.csiny.com/2017/01/flaw-allows-thieves-to-open-locked-ipads/?utm_source=dlvr.it&utm_medium=facebook)



# Google Chrome Shutting Down Flash



- [http://www.csiny.com/2016/12/html5-trumps-flash-in-google-chrome/?utm\\_source=dlvr.it&utm\\_medium=facebook](http://www.csiny.com/2016/12/html5-trumps-flash-in-google-chrome/?utm_source=dlvr.it&utm_medium=facebook)



- [http://www.csiny.com/2017/01/flaw-allows-thieves-to-open-locked-ipads/?utm\\_source=dlvr.it&utm\\_medium=facebook](http://www.csiny.com/2017/01/flaw-allows-thieves-to-open-locked-ipads/?utm_source=dlvr.it&utm_medium=facebook)



# EqualLogic SAN Theory of Operation



- For example I allocate a volume as 500GB and label it as thin. That means it lies to the OS and says 500, but in fact provisions only 50GB because that is what is actually being used. It continues to add space on the fly -without intervention - up to the 500GB. However, if the server, only grows to 125GB, the remaining 375GB remains on the SAN to be used elsewhere. This over giving of disk is called over-subscription.
- As long as everyone's actual use is under the actual space available on the SAN, life is good.
- At some point the math starts getting tight. The SAN will then alert. At that point you can impose hard limits (i.e. Thick) and/or plan to add more space.
- Once the thin is approaching the fully provisioned amount, it functionally isn't thin.
- If the server size is likely to stay static, then changing it to thick eliminates the alert (and fully provisions the remaining space). This eliminates the warning.
- If it will continue to grow beyond your original configuration for the server, adding space and keeping it thin may be the best strategy.
- Thick is committing 500GB and provisioning it all immediately all at once. Technically there is some overhead/delay for provisioning thin on the fly so thick is always the fastest disk, but in our world the difference is minuscule. Technically domain controllers and database volumes are recommended thick, but for little improvement in performance and losing all that space we often don't bother.



## ■ Isis victim's families sue Twitter for being a weapon of terrorists

- [http://www.infoworld.com/article/3156611/social-networking/families-of-isis-victims-sue-twitter-for-being-weapon-for-terrorism.html?idg\\_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm\\_source=Sailthru&utm\\_medium=email&utm\\_campaign=InfoWorld%20Daily:%20Afternoon%20Edition%202017-01-11&utm\\_term=infoworld\\_daily](http://www.infoworld.com/article/3156611/social-networking/families-of-isis-victims-sue-twitter-for-being-weapon-for-terrorism.html?idg_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm_source=Sailthru&utm_medium=email&utm_campaign=InfoWorld%20Daily:%20Afternoon%20Edition%202017-01-11&utm_term=infoworld_daily)



- **MalwareBytes got in an electronic war with PC-Matic (those TV AV people on cable news). They started uninstalling PC-Matic leaving the machine without AV!**
  - <http://www.networkworld.com/article/3155113/security/when-anti-malware-vendors-get-into-a-slap-fight-users-lose.html>



# How to disable auto updates in Flash



- **If you are pushing Adobe flash updates out, you may want to force clients to not ask for auto updates.**
- **There is no GPO to turn off Flash auto updates.**
- **There is no registry key to turn off Flash auto updates.**
- **Instead you need to replace the `C:\windows\syswow64\macromed\flash\mms.cfg` file and reboot.**
- **The contents of the Flash `mms.cfg` file are:**
  - `SilentAutoUpdateEnable=0`
  - `AutoUpdateDisable=1`





- **HTML 5 bug locks up web page with fake Microsoft support message and often disables taskmgr.exe.**
  - [https://blog.knowbe4.com/tech-support-scammers-abuse-bug-in-html5-to-freeze-computers?utm\\_content=43053252&utm\\_medium=social&utm\\_source=linkedin](https://blog.knowbe4.com/tech-support-scammers-abuse-bug-in-html5-to-freeze-computers?utm_content=43053252&utm_medium=social&utm_source=linkedin)



- **People would rather have wi-fi than sex, chocolate or alcohol. 40% said it is the most important daily item!**
  - <http://www.ibtimes.co.uk/most-people-would-rather-have-wi-fi-sex-chocolate-alcohol-study-finds-1591644>



- <http://www.computerworld.com/article/3138095/virtual-reality/ibm-engineer-sees-ar-trumping-vr-for-data-visualization.html>



- | We are still waiting for Veeam to announce support for VMware vSphere 6.5**



# Fake Support Site Fined \$10M



- [https://www.channele2e.com/2016/12/23/it-service-providers-pay-10-million-fine/?utm\\_medium=email&utm\\_source=sendpress&utm\\_campaign](https://www.channele2e.com/2016/12/23/it-service-providers-pay-10-million-fine/?utm_medium=email&utm_source=sendpress&utm_campaign)

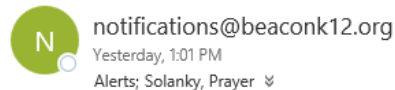


# Office 365 Labels vs. Categories



- In Office 365, a message can only live in one folder. However, you can assign multiple categories to the message. For example, in this screenshot I have the message categories as CSI and Forefront.

Forefront Status | BCSD



■ Forefront ■ CSI

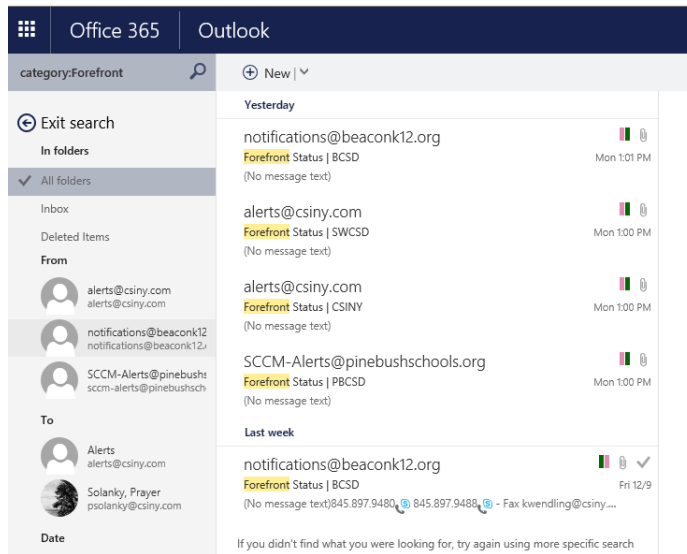
- In message listing, it looks like this.



# Office 365 Labels vs. Categories



- You can create rules to automatically categorize messages. Within the web interface, the rule can only apply one category but you can manually assign it more than one category. With the Outlook client, the rule can assign multiple categories.**



- To do a search for messages assigned to a category. You put in 'category:name' which will find the relevant messages.**



# Office 365 Troubleshooting Tool



- <http://www.infoworld.com/article/3143651/microsoft-windows/microsoft-enhances-troubleshooting-support-for-onedrive-for-business.html>










# Microsoft's New Docs site



**<https://docs.microsoft.com/en-us/>**

docs.microsoft.com

docs.microsoft.com is our new unified technical documentation experience; to learn more check out our [blog](#). For additional documentation on Microsoft products or services, please visit [MSDN](#) or [TechNet](#).

 Windows	Microsoft Azure	 Visual Studio	 Office
.NET	ASP.NET	Dynamics 365	Enterprise Mobility + Security
 nuget	SQL	 Xamarin	



## ■ Middle School student says:

- They use Google Docs
- Lots of tests by teachers are in Google Docs.
- Kids take a picture of the study guide and put it in a Google Doc.
- When they take the test, they open the second Google Doc with the study guide and flip back and forth.
- The teacher never picks up on this because on the Chromebooks (in a 1 to 1 initiative) the screens are so small.
- That makes it effectively an open book test.



# Ask Apple to pre-configure for MDM



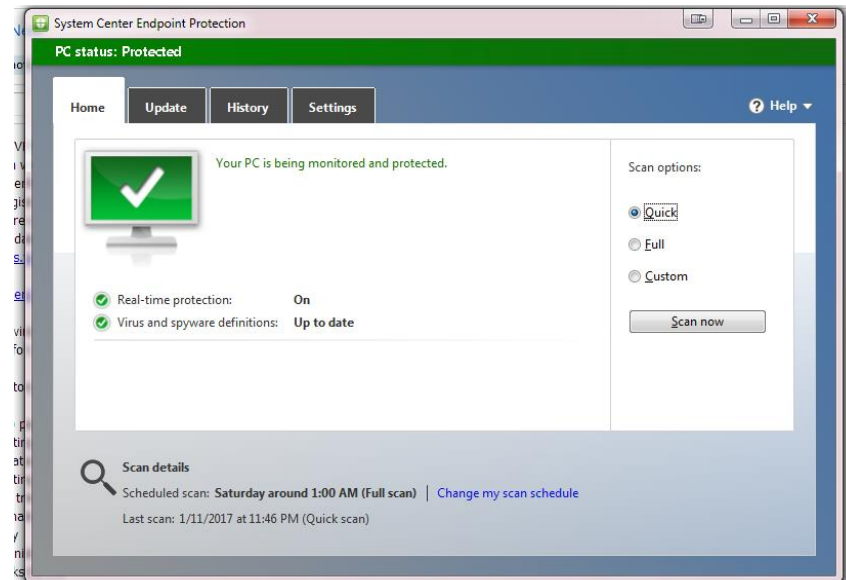
- Apple can pre-configure your iPads or iPhones for your MDM solution, saving you deployment time.**



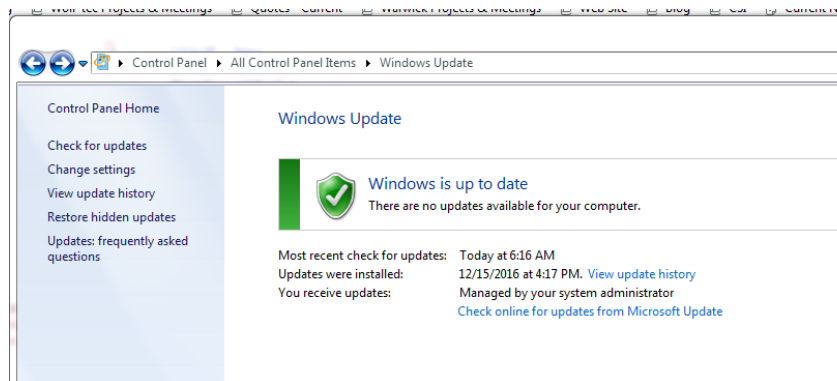
# SCCM Endpoint Excludes



- Make sure that you exclude this folder from your SCCM Endpoint Scans
  - `c:\windows\system32\config\systemprofile`
- There is endless WSUS CAB files that are opened in an SCCM Endpoint scan in this location. Scans can take days/weeks to complete in some cases!



# Windows Updates



## Choose how Windows can install updates

**i** Some settings are managed by your system administrator. [More information.](#)

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

[How does automatic updating help me?](#)

### Important updates

Install updates automatically (recommended)

Install new updates: Every day at 6:00 AM

### Recommended updates

Give me recommended updates the same way I receive important updates

### Who can install updates

Allow all users to install updates on this computer

### Microsoft Update

Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows

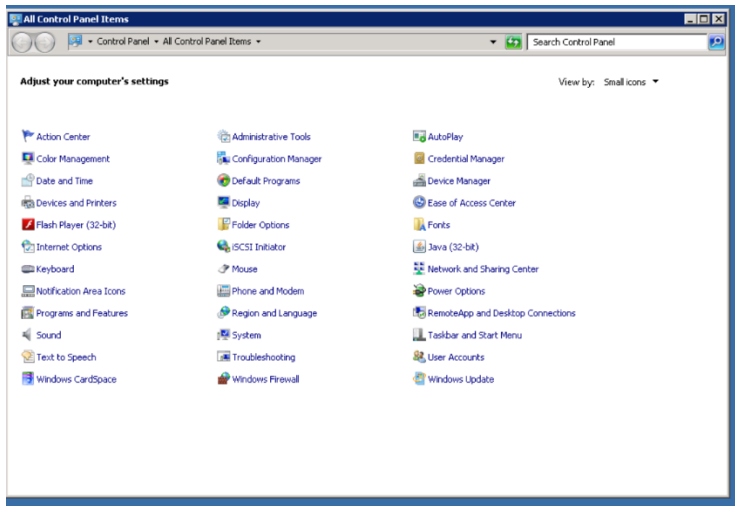
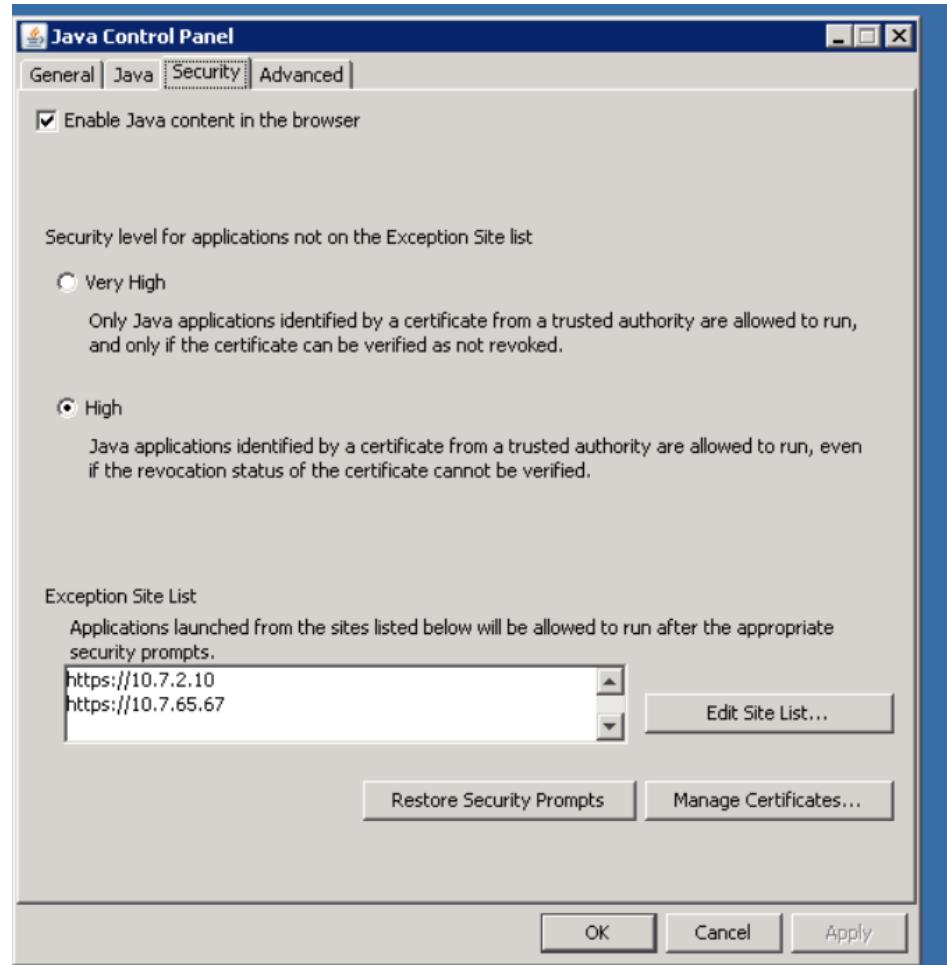
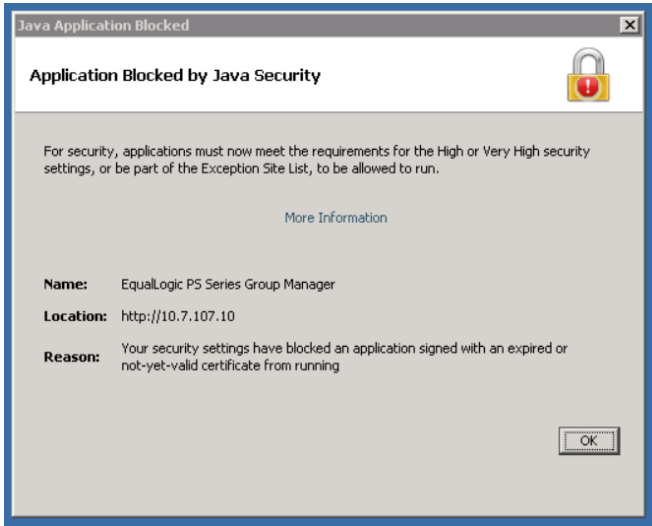
### Software notifications

Show me detailed notifications when new Microsoft software is available

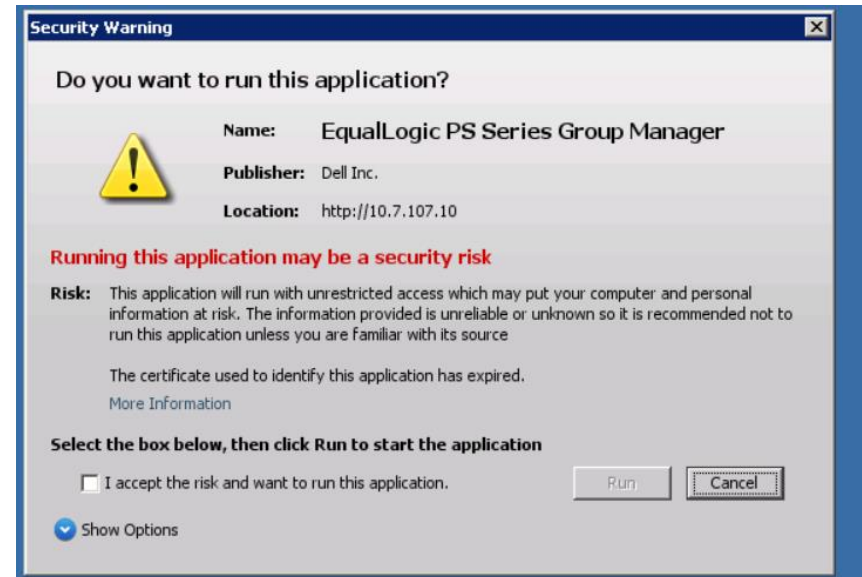
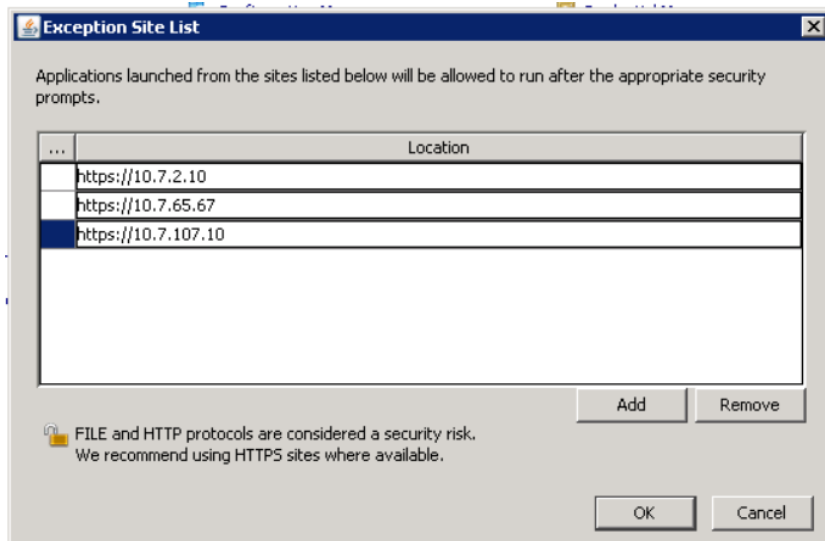
Note: Windows Update might update itself automatically first when checking for other updates. Read our [privacy statement online.](#)



# Java Security



# Java Security



# Phishing Email



Re: 10/31/2016

Inbox x



People (2)



**Robert Knapp** <rknapp@csiny.com>

Oct 31 (3 days ago) ☆



to me



**Robert Knapp**

Follow

Can you

from: **Robert Knapp** <rknapp@csiny.com>

request?

Robert

reply-to: Robert Knapp <ceouscellular@email.com>

Sent

to: metta@csiny.com

date: Mon, Oct 31, 2016 at 11:46 AM

subject: Re: 10/31/2016

Important mainly because of the people in the conversation.

Mail from this week

10/31/2016



# Phishing Email



Delivered-To: metta@csiny.com  
Received: by 10.157.46.109 with SMTP id c42csp197911otd;  
Mon, 31 Oct 2016 08:46:18 -0700 (PDT)  
X-Received: by 10.98.1.200 with SMTP id 191mr32250898pfb.102.1477928778016;  
Mon, 31 Oct 2016 08:46:18 -0700 (PDT)  
Return-Path: <axapar@axapar.com>  
Received: from p3plwbeout11-04.prod.phx3.secureserver.net (p3plsmtp11-04-2.prod.phx3.secureserver.net. [173.201.192.40])  
by mx.google.com with ESMTPS id 14si11631715pfk.287.2016.10.31.08.46.17  
for <metta@csiny.com>  
(version=TLS1\_2 cipher=AES128-SHA bits=128/128);  
Mon, 31 Oct 2016 08:46:17 -0700 (PDT)  
Received-SPF: neutral (google.com: 173.201.192.40 is neither permitted nor denied by best guess record for domain of axapar@axapar.com) client-ip=173.201.192.40;  
Authentication-Results: mx.google.com;  
spf=neutral (google.com: 173.201.192.40 is neither permitted nor denied by best guess record for domain of axapar@axapar.com) smtp.mailfrom=axapar@axapar.com  
Received: from localhost ([173.201.192.13])  
by p3plwbeout11-04.prod.phx3.secureserver.net with bizsmtp  
id 2FmH1u0020HoDz901FmHSm; Mon, 31 Oct 2016 08:46:17 -0700  
X-SID: 2FmH1u0020HoDz901  
Received: (qmail 25552 invoked by uid 99); 31 Oct 2016 15:46:17 -0000  
Content-Transfer-Encoding: quoted-printable  
Content-Type: text/html; charset="utf-8"

X-Originating-IP: **108.62.48.212**  
User-Agent: Workspace Webmail 6.5.3  
Message-Id: <20161031084615.3ecb96883911cf90e09e9e7d0a821bcb.0d7138c653.wbe@email11.godaddy.com>

**From: "Robert Knapp " <rknapp@csiny.com>**  
**X-Sender: axapar@axapar.com**  
**Reply-To: "Robert Knapp " <ceouscellular@email.com>**  
**To: metta@csiny.com**

Subject: Re: 10/31/2016  
Date: Mon, 31 Oct 2016 08:46:15 -0700  
Mime-Version: 1.0



# Phishing Whois Record



```
| Whois IP 108.62.48.212
| Updated 1 second ago
| #
| # ARIN WHOIS data and services are subject to the Terms of Use
| # available at: https://www.arin.net/whois_tou.html
| #
| # If you see inaccuracies in the results, please report at
| # https://www.arin.net/public/whoisinaccuracy/index.xhtmll
| #
|
| #
| # The following results may also be obtained via:
| # https://whois.arin.net/rest/nets;q=108.62.48.212?showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ext=netref2
| #
|
| # start
|
| NetRange: 108.62.48.0 - 108.62.55.255
| CIDR: 108.62.48.0/21
| NetName: NETBLK-UBIQUITY-NEW-YORK-108-62-48-0
| NetHandle: NET-108-62-48-0-1
| Parent: NETBLK-NOBIS-TECHNOLOGY-GROUP-09 (NET-108-62-0-0-1)
| NetType: Reallocated
| OriginAS: AS15003
|
| Organization : Ubiquity Server Solutions New York (NTGL-2)
| RegDate: 2011-02-07
| Updated: 2011-02-07
| Comment: Addresses in this block are non-portable.
| Comment: For security issues, abuse reports, and
| Comment: technical issues, please contact the
| Comment: Nobis Technology Group NOC at email@nobistech.net
| Ref: https://whois.arin.net/rest/net/NET-108-62-48-0-1
|
| OrgName: Ubiquity Server Solutions New York
| OrgId: NTGL-2
| Address: 200 Webro Road
| City: Parsippany
| StateProv: NJ
| PostalCode: 07054
```



# Ccleaner Uninstalls Default Windows 10 Apps



Windows 10 Pro 64-bit  
Intel Core i7-4800MQ CPU @ 2.70GHz, 8.0GB RAM, Intel HD Graphics 4600

Select a program from the list you want to remove from your computer

Programs to Remove	Publisher	Install Date	Size	Version
Sports	Microsoft Corporation	10/14/2016		4.16.17.0
Store	Microsoft Corporation	11/3/2016		11610.1001.1...
Store Purchase App	Microsoft Corporation	9/28/2016		11608.1000.2...
Sway	Microsoft Corporation	9/13/2016		17.7369.4514...
Synaptics Pointing Device Driver	Synaptics Incorporated	10/28/2016	46.4 MB	19.0.19.1
Synaptics WBF DDK S011 (Advanced)	Synaptics	7/4/2016	15.5 MB	4.5.507.0
System Requirements Lab Detection	Husdawg, LLC	8/18/2015	1.31 MB	6.1.6.0
Thinkpad USB 3.0 Ethernet Adapter Driver	Lenovo	10/18/2014	975 KB	8.8.911.2013
ThinkVantage Password Manager	Lenovo Group Limited	12/27/2014	86.3 MB	4.70.2.0
Thunderbolt(TM) Software	Intel(R) Corporation	10/18/2014	5.38 MB	1.4.0.1
Twitter	Twitter Inc.	9/27/2016		5.3.5.0
UltraVnc	uvnc bvba	10/28/2016	5.86 MB	1.2.1.2
Visual Studio 2012 x64 Redistributables	AVG Technologies	10/28/2014	13.0 MB	14.0.0.1
Visual Studio 2012 x86 Redistributables	AVG Technologies CZ, s.r.o.	10/28/2014	3.38 MB	14.0.0.1
VMware Horizon Client	VMware, Inc.	10/16/2016	206 MB	4.2.0.2831
VMware vSphere CLI	VMware, Inc.	8/1/2016	102 MB	6.0.0.8149
VMware vSphere Client 5.1	VMware, Inc.	5/2/2015	423 MB	5.1.0.2669
VMware vSphere Client 6.0	VMware, Inc.	3/7/2016	329 MB	6.0.0.5959
Voice Recorder	Microsoft Corporation	8/26/2016		10.1608.2211.0
Weather	Microsoft Corporation	10/20/2016		4.16.15.0
WinDirStat 1.1.2		8/13/2016		
Windows Driver Package - Intel (e1dexpress...	Intel	8/13/2016		07/02/2013 1...
Windows Driver Package - Intel Corporation ...	Intel Corporation	8/13/2016		11/15/2013 1...
Windows Driver Package - Lenovo 1.67.04.0...	Lenovo	8/13/2016		12/17/2013 1...
Windows Driver Package - Synaptics (SmbDR...	Synaptics	8/13/2016		02/25/2014 1...
Windows Driver Package - Synaptics (SynTF...	Synaptics	8/13/2016		02/25/2014 1...
Windows DVD Player	Microsoft Corporation	8/13/2016		3.6.13291.0
Xbox	Microsoft Corporation	10/7/2016		19.22.6017.0
Xbox Identity Provider	Microsoft Corporation	8/13/2016		11.19.19003.0

Uninstall  
Repair  
Rename  
Delete

Search

Save to text file...

Check for updates

# Dell OpenManage Web Page Fails



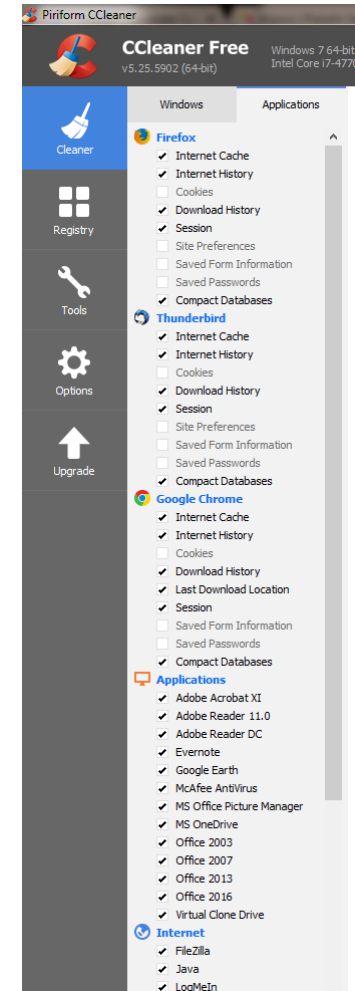
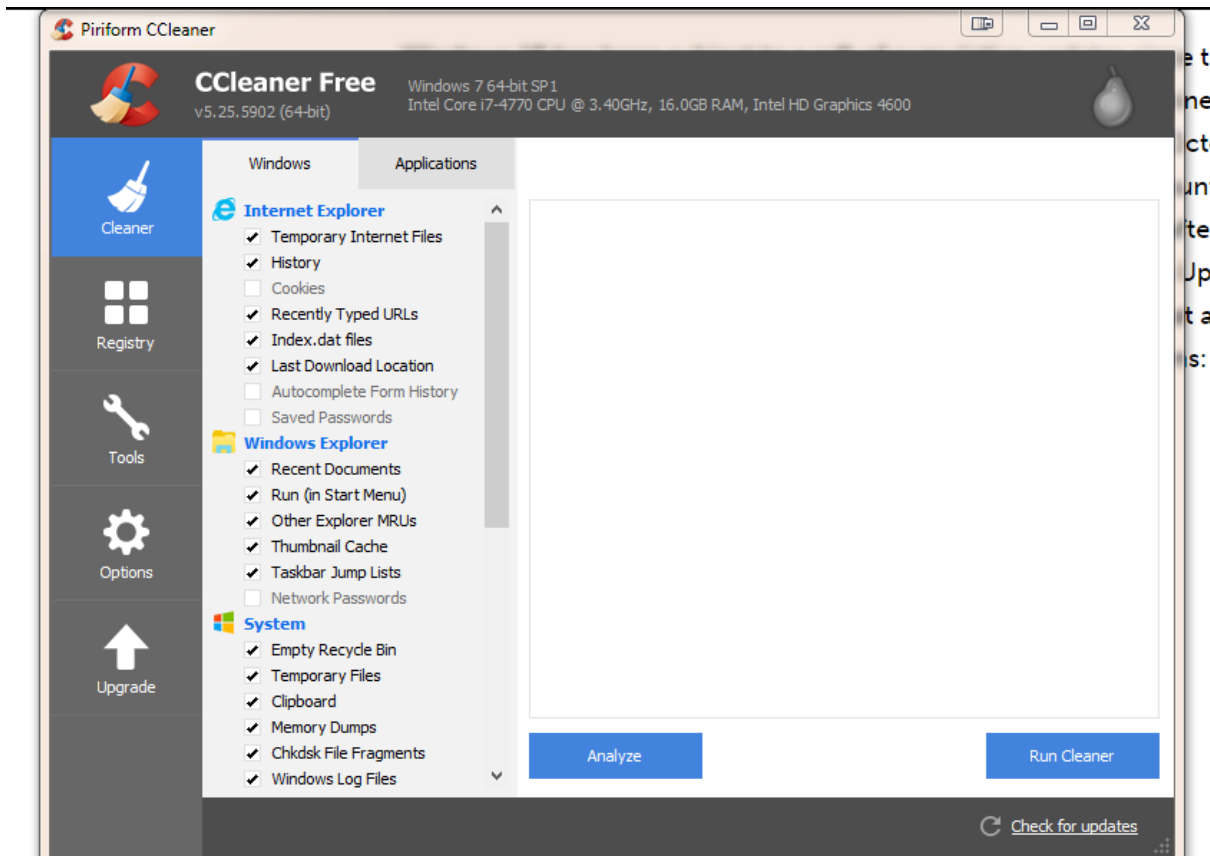
- **If the Dell OpenManage web page fails to load, re-install a newer version of Dell OpenManage Server Administrator on the server.**



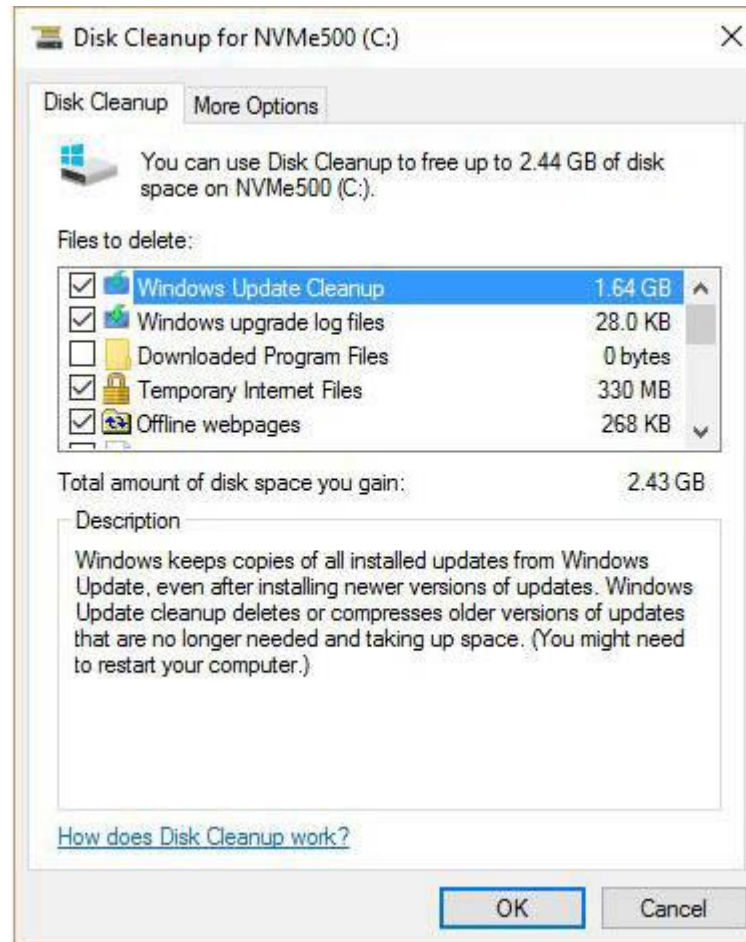
# Cleaning Up Installations



## Ccleaner – Generic files



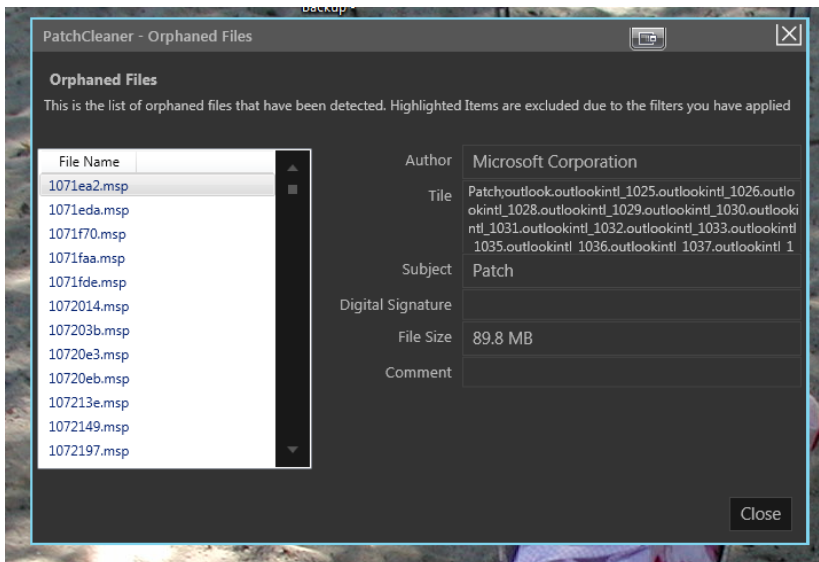
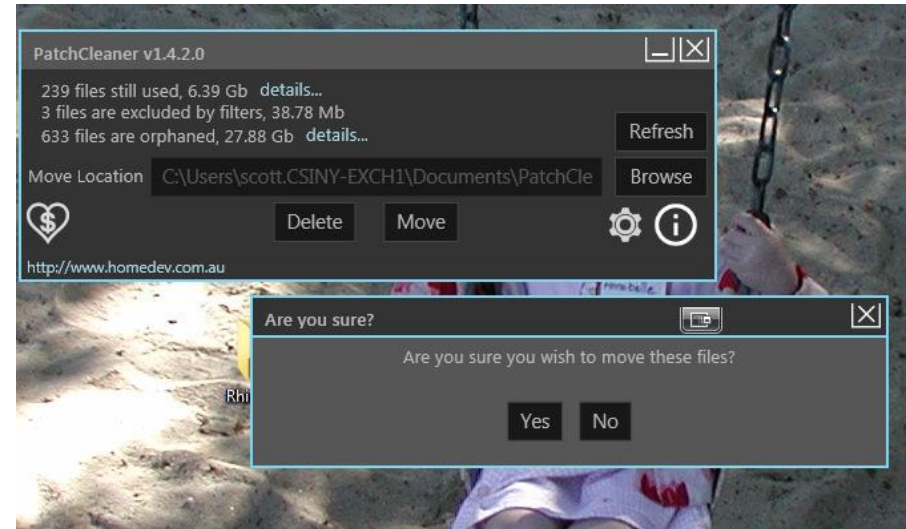
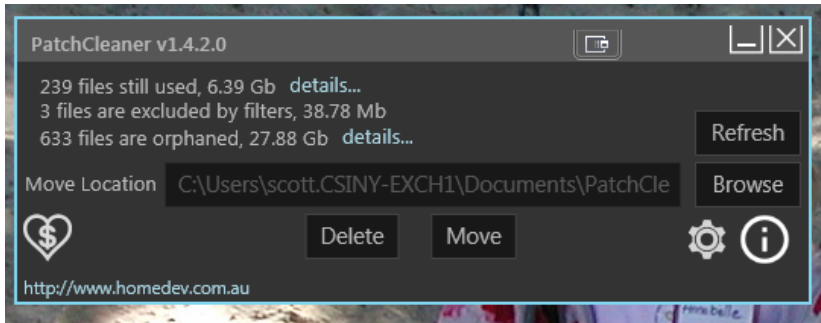
# Disk Clean-Up System Files



- <http://www.homedev.com.au/free/patchcleaner>
- **Awesome utility to go after C:\WINDOWS\Installer files in a responsible way.**
  - Looks for orphan files
  - Lists what it thinks can go responsibly.
  - Allows you to move the location to prove that nothing in that list is needed.
  - If nothing bad happens, you can delete the moved files and get the space back.



# PatchCleaner Running





- Due to the changing nature of Windows Updates it is not always in Automatic mode turned on. Therefore, we no longer alert on Windows Updates Automatic mode being off.**
- This has cut down on a ton of MBSA reports.**
- You are left with the MBSA reports that list security updates, and services packs required to be current for that day.**



# Down Detector



Verizon 3:35 PM

downdetector

FAVORITES

OTHER

- Comcast
- eBay
- Frontier
- Gmail
- Google
- Google Drive
- Instagram
- Mediacom

Verizon 3:36 PM

Google Drive

PROBLEMS AT GOOGLE DRIVE

REPORTS OVER THE LAST 24 HOURS

1777

-24h -12h Now

MOST PROBLEMS REPORTED WITH

- 44% Can't access files online
- 38% App not loading
- 17% File syncing

Report a problem

CONTACT

Facebook

Regain Control of Your Network

Details Tweets Comments

# Symantec+Chrome+Flash=BAD



- After reviewing this case and the available data (primarily the provided WPP logs) I have found that this is a known-issue with the SEP 12.1 and SEP 14 products. SEP is attempting to obtain a hash of the Adobe Flash Player file 'pepflashplayer.dll'; however, during the hash operation, Chrome is attempting to move the file from a temporary folder (where SEP is performing the hash) to Chrome's plugin folder; since SEP has a lock on the file, Chrome's move operation fails and the plugin update process aborts.
- Symantec has identified a fix for this issue and is planning on including a resolution in the next release of SEP 12.1 and SEP 14, both due out early next year.
- It is possible to work around this issue by disabling deferred scanning for AutoProtect; however, this is not generally recommended in production unless absolutely needed, as it disables scan throttling based on I/O activity.
- For more information on disabling deferred scanning, please see the following KB document:
- How to disable deferred scanning in Auto-Protect for Symantec Endpoint Protection
  - [https://support.symantec.com/en\\_US/article.TECH224108.html](https://support.symantec.com/en_US/article.TECH224108.html)
- It is also possible to work around the issue by temporarily disabling SEP; however, this is a potential security issue, as you will be temporarily disabling the product from being able to scan files.

<https://bugs.chromium.org/p/chromium/issues/detail?id=651945>

# Why WSUS & SCCM clients are reaching out to Microsoft



## <https://blogs.technet.microsoft.com/windowsserver/2017/01/09/why-wsus-and-sccm-managed-clients-are-reaching-out-to-microsoft-online/>

- Updating Windows App Store Updates that don't follow normal Microsoft Patch Tuesday style updates
- Proxy server configuration and restrictions



# Microsoft Office 365 Discontinuing Office 2013



- **Microsoft has decided the time has come to force everyone to Office 2016 via Office 365 downloads. Therefore, they are removing all on-line ability to download Office 2013 starting February 28<sup>th</sup>.**
- **No more feature updates to Office 2013**
- **No support via Customer Service Support or Premier Support!**
- **If you want Office 2013, you have a month to deploy it.**



- **Microsoft has announced that Windows 7 is an insecure OS (as compared to Windows 10)**
- **They are reminding people that some newer AMD, Intel and Qualcomm chipsets**
- **They are reminding people that the Windows Store Apps are for Windows 10.**
- **Windows 7 support ends January 14<sup>th</sup>, 2020.**
- **Use Windows 7 “ at your own risk, at your own peril.”**



## I Symantec reports:

- Windows execution policies are ineffective in preventing malicious PowerShell script launching. Hackers can easily bypass them.
- Always use the latest PowerShell version and enable extended logging and monitoring.
- PowerShell scripts can execute directly from memory making it harder to even see that bad things are happening.

## I Source:

- <http://m.mspmentor.net/technologies/experts-warn-powershell-security-threat?eid=forward>



# Adobe Installs Spyware in Chrome!



## Adobe Reader DC installs browser attachment without asking or warning in Chrome that tracks your surfing habits!

- [http://www.infoworld.com/article/3157420/microsoft-windows/adobe-acrobat-reader-dc-security-update-installs-chrome-spyware.html?idg\\_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm\\_source=Sailthru&utm\\_medium=email&utm\\_campaign=InfoWorld%20Daily:%20Afternoon%20Edition%202017-01-13&utm\\_term=infoworld\\_daily](http://www.infoworld.com/article/3157420/microsoft-windows/adobe-acrobat-reader-dc-security-update-installs-chrome-spyware.html?idg_eid=73261dcec9d3d8b52c7344e7a5e2afc1&utm_source=Sailthru&utm_medium=email&utm_campaign=InfoWorld%20Daily:%20Afternoon%20Edition%202017-01-13&utm_term=infoworld_daily)





# Fake Email Phishing Scam



## I Google Apps

- Someone's email gets hacked.
- Finds someone the compromised person emailed to
- Finds a subject line they used to email that person
- Finds an attachment name that they previously sent that person
- Embeds a graphic in the email that looks like the exact attachment they previously received.
- Clicking on the attachment takes you to Google Drive.
- A fake Google Apps sign on screen comes up in a Google Doc asking you to sign into Google Drive to get your shared attachment.
- You are hacked!
  - [Source: http://www.businessinsider.com/hackers-fake-email-attachment-scam-spoof-subject-lines-break-into-accounts-2017-1](http://www.businessinsider.com/hackers-fake-email-attachment-scam-spoof-subject-lines-break-into-accounts-2017-1)



# Is Antivirus getting worse?



- **More things getting through despite excellent testing results of major antivirus products.**
- **Malware/viruses using different techniques to evade detection.**
- **Need to use a multi-level approach and newer technologies such as Cisco AMP**
- **Source:**
  - <http://www.networkworld.com/article/3159469/computers/is-antivirus-getting-worse.html>



# Group Policy Troubleshooting Tip



- ❑ **Click on each group policy object under Group Policy Objects in Group Policy Management Console**
- ❑ **If a GPO object is corrupted, it will tell you it isn't there.**
- ❑ **If the rights are corrupted, it will ask you whether you want to fix the SYSVOL rights. Say yes to resolve the issue.**



**csiny.com**