CYBERSECURITY
RED TEAM, BLUE TEAM

OLLI Summer 2016

Tom Manteuffel

Slides: http://www.olligmu.org/~docstore

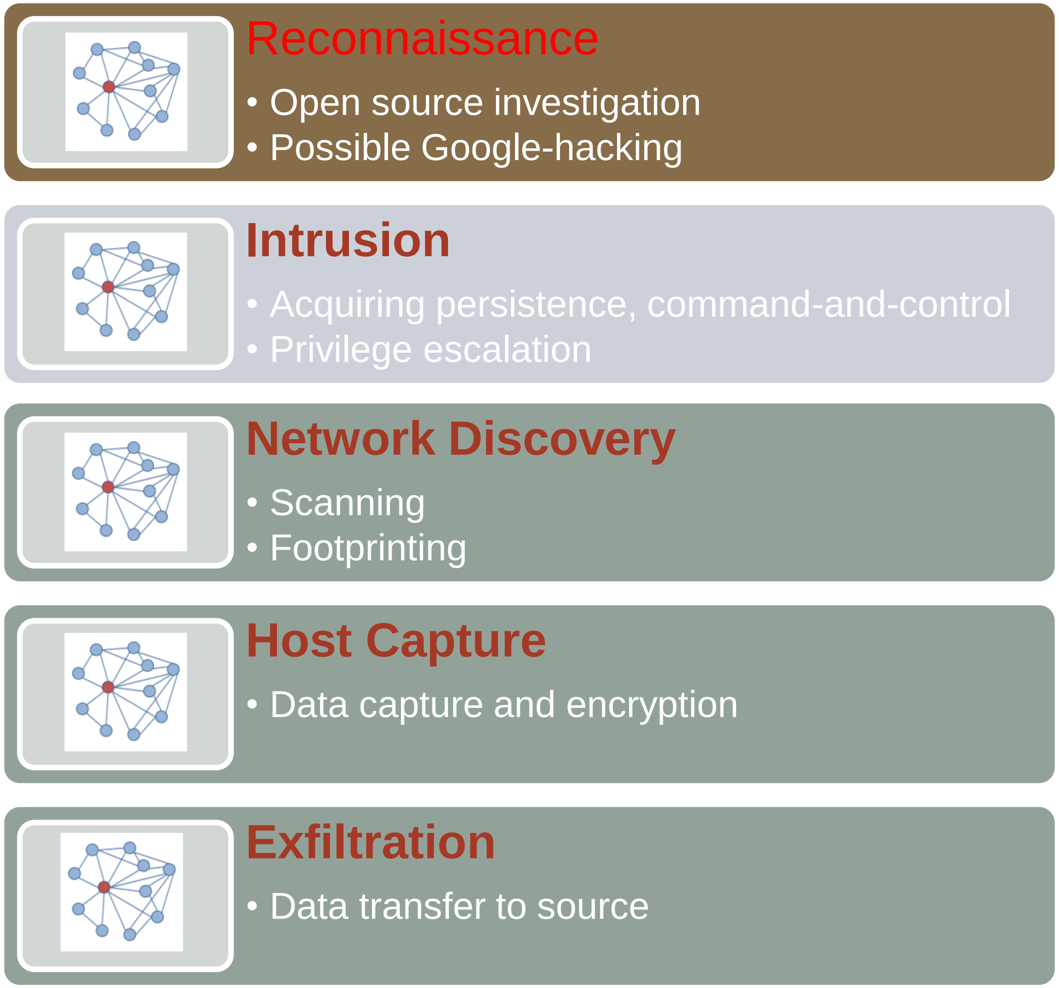
Plan of The Course

Week I - How did we get here?

Week II - Red Team: Hacking 101

Week III - Blue Team: Defending the home computers

Phases in a Major Attack



Reconnaissance

- Open source investigation
- Possible Google-hacking

Intrusion

- Acquiring persistence, command-and-control
- Privilege escalation

Network Discovery

- Scanning
- Footprinting

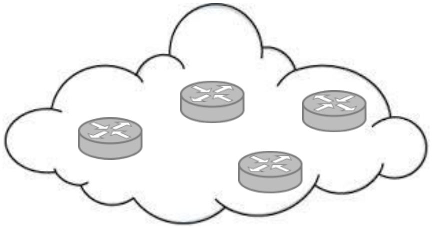
Host Capture

- Data capture and encryption

Exfiltration

- Data transfer to source

Cyberwarfare



Will there be a Cyberwar?

There already has…

FINLAND
SWEDEN
Helsinki
St.Petersburg
Tallinn
Stockholm
ESTONIA
BALTIC SEA
RUSSIA
Riga
LATVIA
LITHUANIA
RUSSIA
Vilnius
Warsaw
POLAND

Has among the highest Internet usage in the world

Has free Wi-Fi virtually everywhere

First nation to conduct voting purely online

Where Skype was invented

And it happens to be where the first cyberwar was launched…

Cyberwar 1.0?

April 2007

FINLAND
SWEDEN
Helsinki
St.Petersburg
Tallinn
Stockholm
ESTONIA
BALTIC SEA
RUSSIA
Riga
LATVIA
LITHUANIA
RUSSIA
Vilnius
Warsaw
POLAND

Denial of Service attacks targeted Estonian Parliament, banks, ministries, newspapers and broadcasters.

The attacks followed Estonian Parliament’s decision to relocate a bronze post-WW II Monument to the Red Army .

The attacks triggered militaries around the world to prepare for cyber attacks.

NATO established its Cyber Defense Center in Estonia in 2008.

Stuxnet

Malware targeting Iranian nuclear centrifuges
was developed by nation-state(s).

Was largely thought to be effective.
But…

Eventually escaped to the wild, causing
headaches for civilian infrastructure

Titan Rain

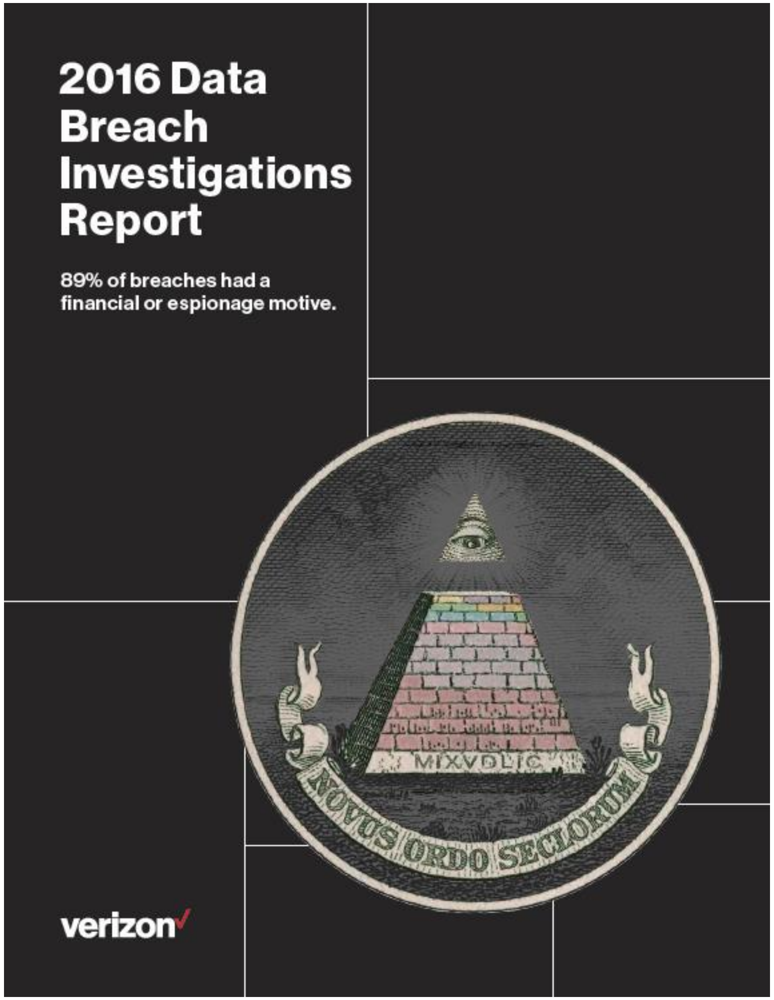
A long series of cyber attacks starting around 2001 targeting Lockheed Martin, Sandia Labs, DIA, Redstone Arsenal, etc.

Generally attributed to Chinese (PLA) entities

Billions of dollars worth of stolen intellectual property has been taken overall.

Attacks may have moderated since a September 2015 informal promise by Xi JinPing to Obama that China would constrain its attacks.

Verizon’s Annual DBIR

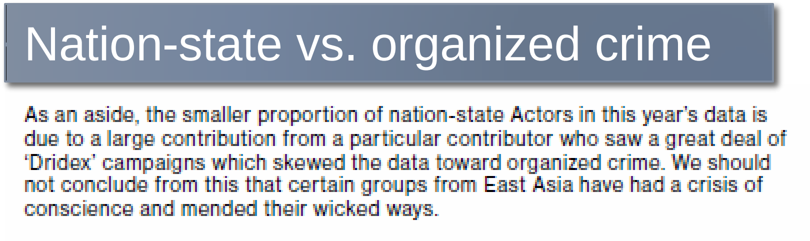


2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Verizon DBIR 2016

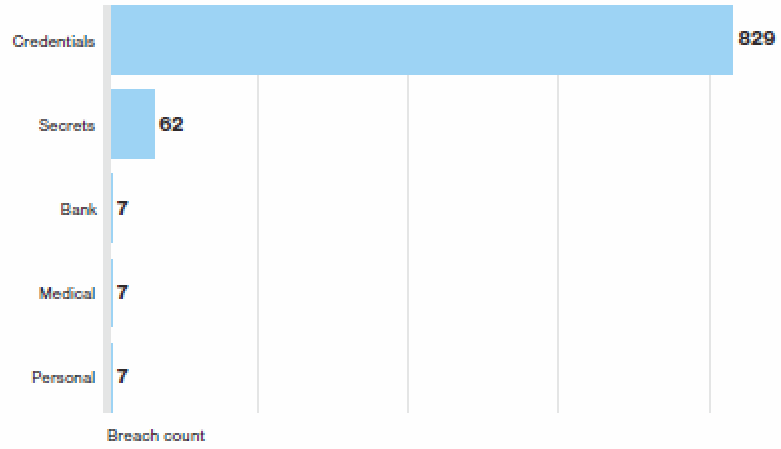


Nation-state vs. organized crime

As an aside, the smaller proportion of nation-state Actors in this year's data is due to a large contribution from a particular contributor who saw a great deal of 'Dridex' campaigns which skewed the data toward organized crime. We should not conclude from this that certain groups from East Asia have had a crisis of conscience and mended their wicked ways.

Who is responsible?

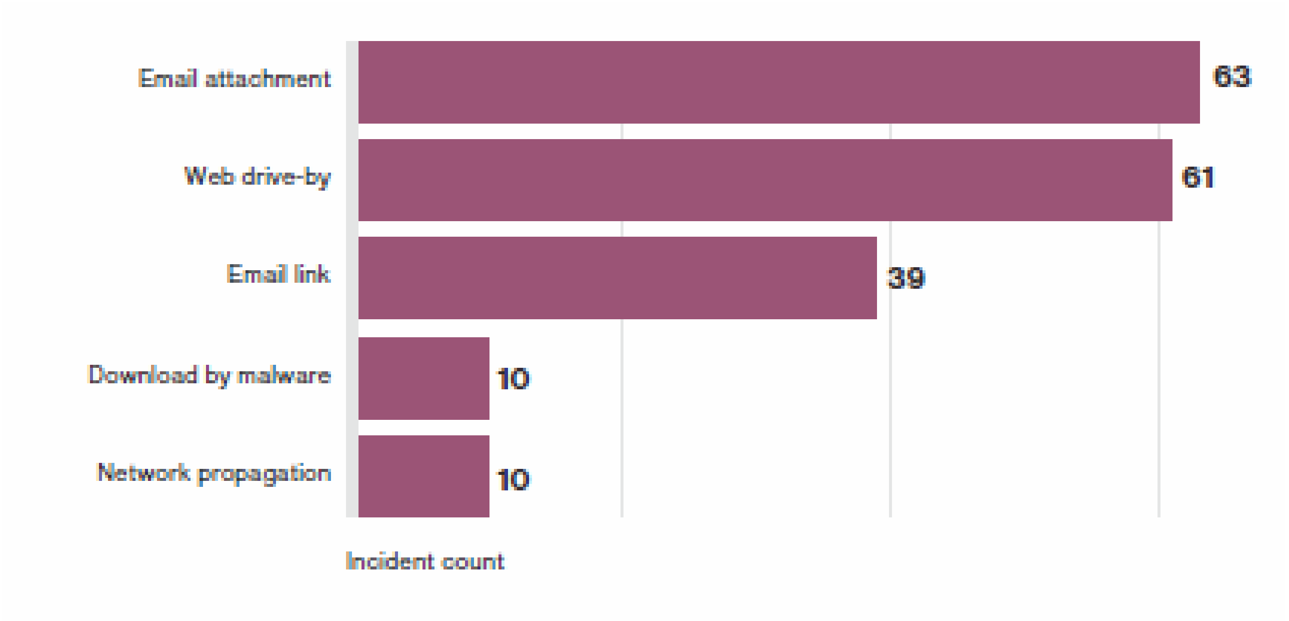
What are they after?



What do the attackers ultimately steal? A heck of a lot of credentials (mostly due to the large amount of opportunistic banking Trojans–beware of Greeks bearing gifts), but also trade secrets.

Verizon BDIR 2016

How does malware get in?



Research on Specific Threats

Recent cyber-espionage research published in 2015/2016

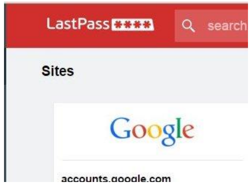
- APT28 (FireEye)
- APT30 (FireEye)
- Duqu Threat Actor (Kaspersky)
- Morpho Group (McAfee)
- Various Actors/Campaigns (Kaspersky)
- Project CameraShy (Threat Connect)
- Various Actors/Campaigns (CrowdStrike)

Arm yourself with information…

So What Can One Do to Protect Oneself?

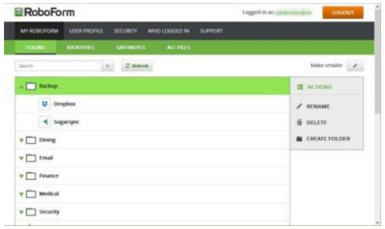
Be Password Savvy

Consider using a password manager



LastPass 4.0

RoboForm



Sticky Password

LogmeOnce

Use an Up-to-Date Antivirus

Avast Free Antivirus 2016

All these are free…

AVG AntiVirus Free (2016)

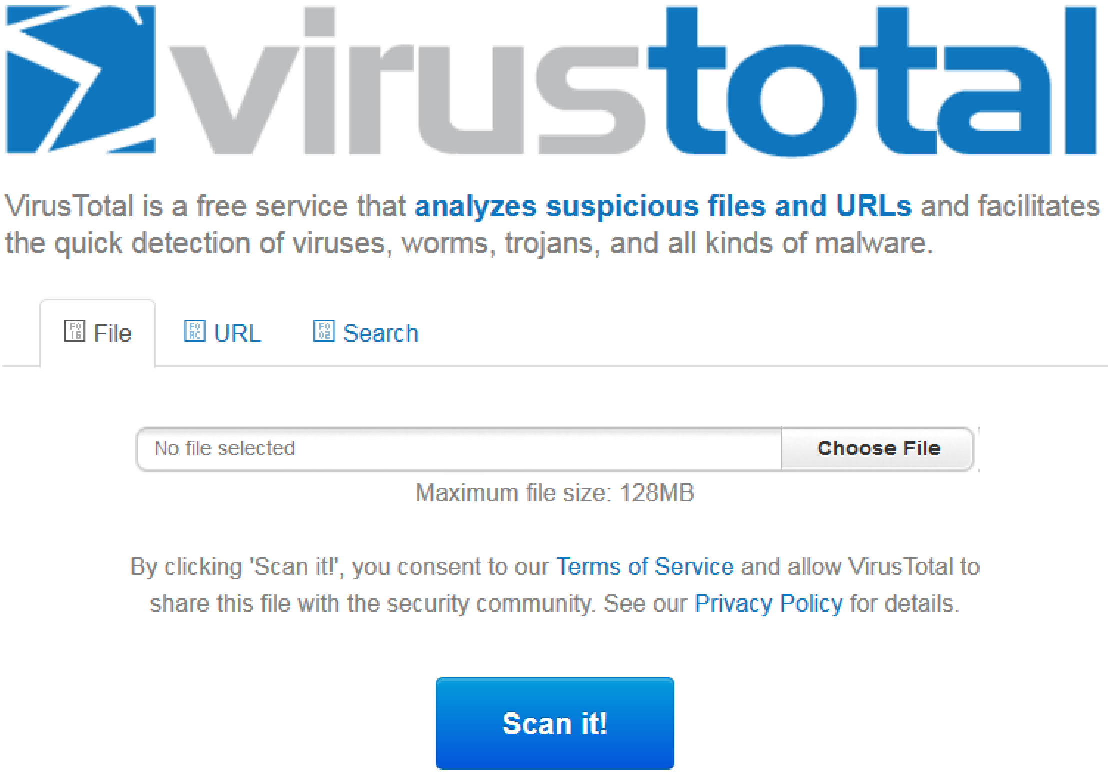
Panda Free Antivirus 2016

Sophos Home

Bitdefender Antivirus Free Edition (2014)

Check Point ZoneAlarm Free Antivirus + Firewall 2016

You Can Submit Malware Here

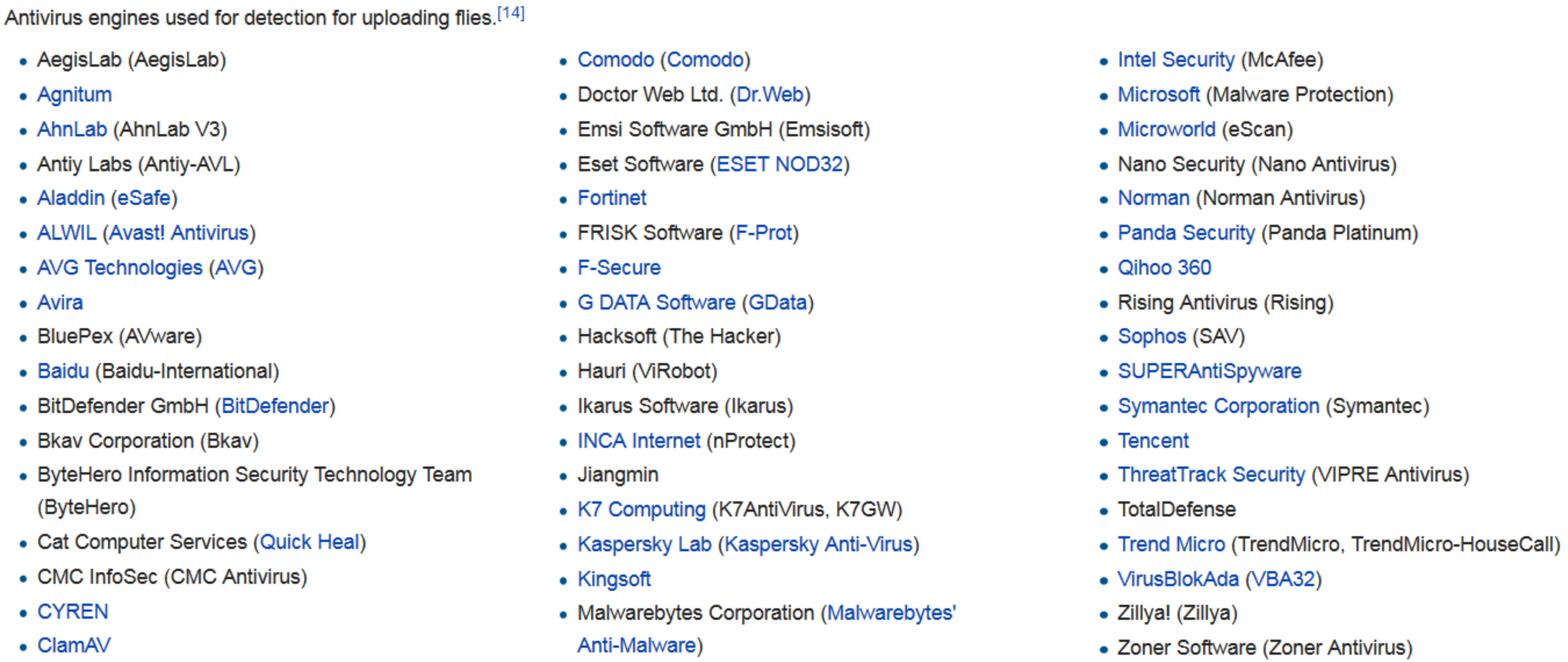


VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

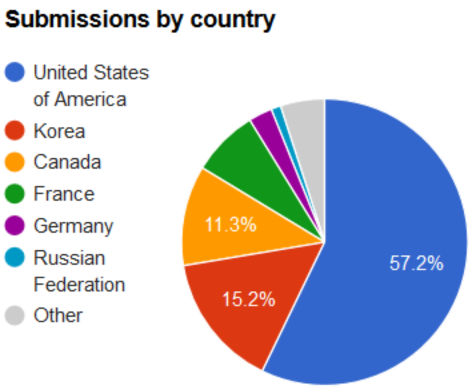
Antivirus Used on VirusTotal

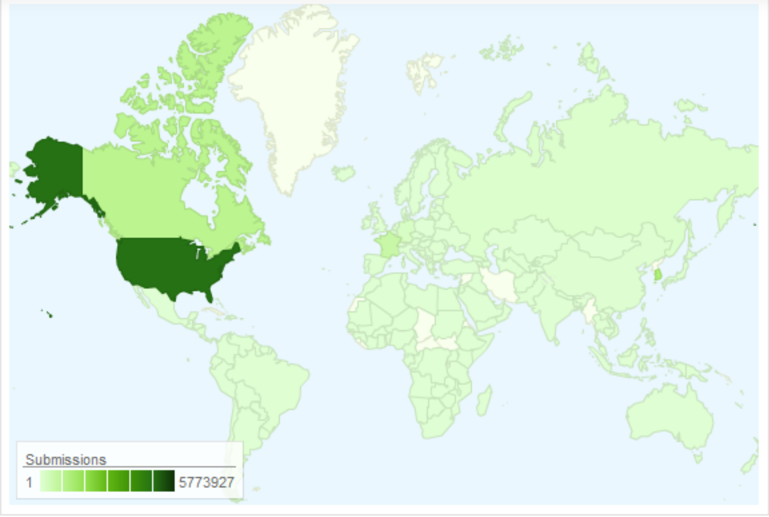


Antivirus engines used for detection for uploading flies.[14]

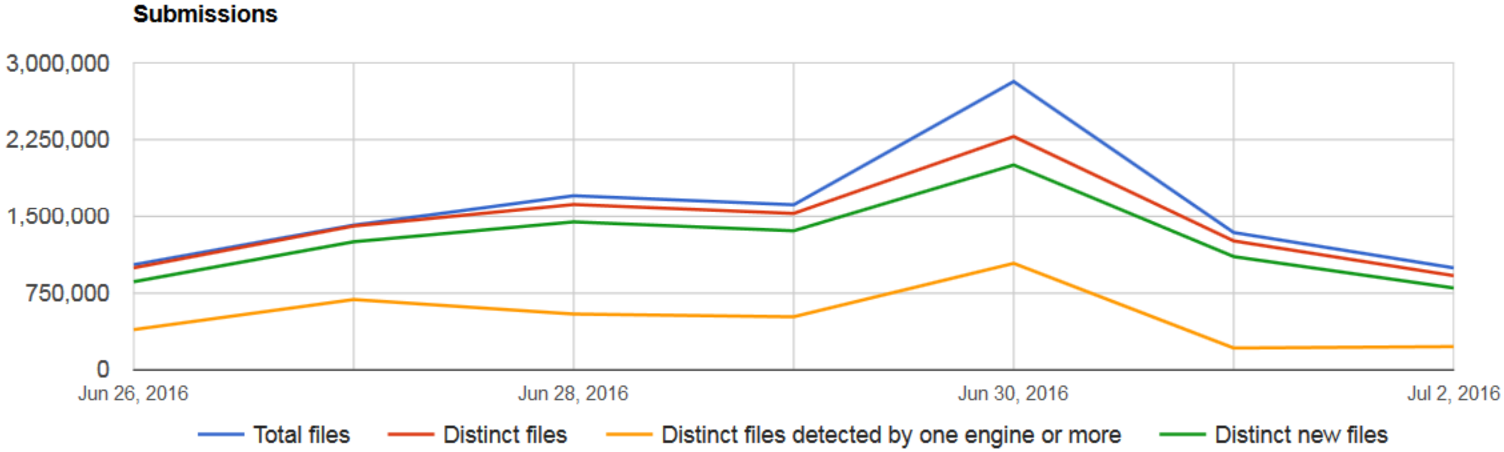
- AegisLab (AegisLab)
- Agnitum
- AhnLab (AhnLab V3)
- Antiy Labs (Antiy-AVL)
- Aladdin (eSafe)
- ALWIL (Avast! Antivirus)
- AVG Technologies (AVG)
- Avira
- BluePex (AVware)
- Baidu (Baidu-International)
- BitDefender GmbH (BitDefender)
- Bkav Corporation (Bkav)
- ByteHero Information Security Technology Team (ByteHero)
- Cat Computer Services (Quick Heal)
- CMC InfoSec (CMC Antivirus)
- CYREN
- ClamAV
- Comodo (Comodo)
- Doctor Web Ltd. (Dr.Web)
- Emsi Software GmbH (Emsisoft)
- Eset Software (ESET NOD32)
- Fortinet
- FRISK Software (F-Prot)
- F-Secure
- G DATA Software (GData)
- Hacksoft (The Hacker)
- Hauri (ViRobot)
- Ikarus Software (Ikarus)
- INCA Internet (nProtect)
- Jiangmin
- K7 Computing (K7AntiVirus, K7GW)
- Kaspersky Lab (Kaspersky Anti-Virus)
- Kingsoft
- Malwarebytes Corporation (Malwarebytes' Anti-Malware)
- Intel Security (McAfee)
- Microsoft (Malware Protection)
- Microworld (eScan)
- Nano Security (Nano Antivirus)
- Norman (Norman Antivirus)
- Panda Security (Panda Platinum)
- Qihoo 360
- Rising Antivirus (Rising)
- Sophos (SAV)
- SUPERAntiSpyware
- Symantec Corporation (Symantec)
- Tencent
- ThreatTrack Security (VIPRE Antivirus)
- TotalDefense
- Trend Micro (TrendMicro, TrendMicro-HouseCall)
- VirusBlokAda (VBA32)
- Zillya! (Zillya)
- Zoner Software (Zoner Antivirus)

Community Statistics Documentation FAQ About English Join our community Sign in





This is just the last seven days activities…



Keep Up-to-Date on Patches

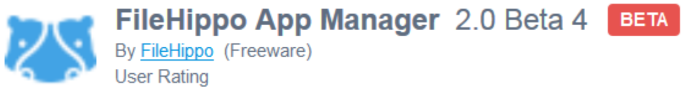
Always accept patches when offered, especially Adobe (including Flash), Java and Browsers

Consider using a tool to detect unpatched software

Microsoft Baseline Security Analyzer

FLEXERA SOFTWARE Personal Software Inspector

Appupdater keeping your software up to date

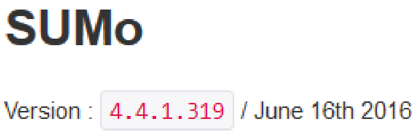


FileHippo App Manager 2.0 Beta 4 BETA

By FileHippo (Freeware)

User Rating

Ninite



SUMo

Version : 4.4.1.319 / June 16th 2016

HEIMDAL SECURITY

Free Endpoint Protection

Symantec.

KASPERSKY lab

SOPHOS

McAfee®

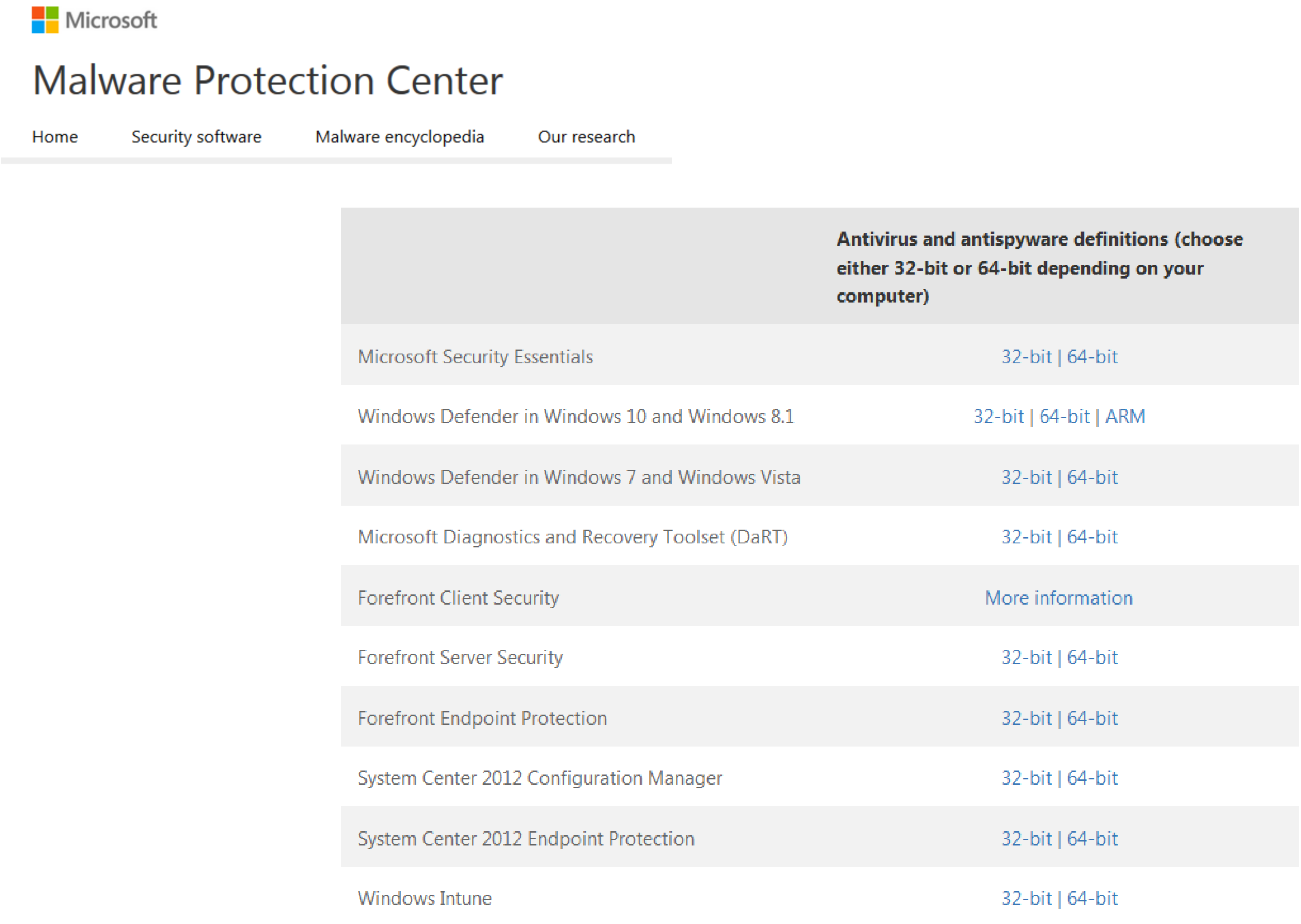
eset®

F-Secure.

PANDA SECURITY

Install one and see if it fits your needs…

Microsoft Tools

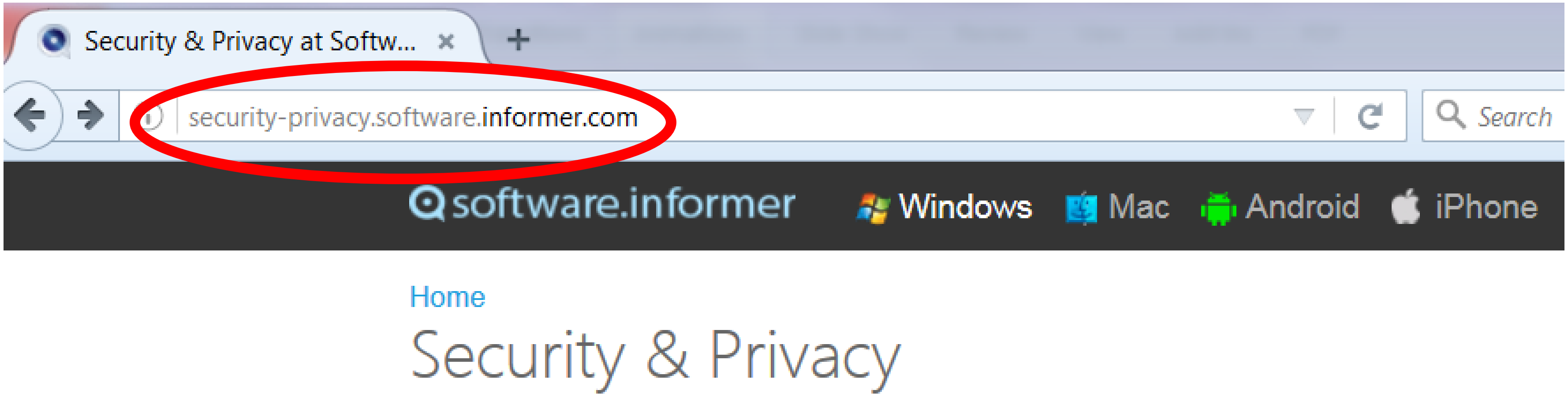


Microsoft

Malware Protection Center

	Antivirus and antispyware definitions (choose either 32-bit or 64-bit depending on your computer)
Microsoft Security Essentials	32-bit | 64-bit
Windows Defender in Windows 10 and Windows 8.1	32-bit | 64-bit | ARM
Windows Defender in Windows 7 and Windows Vista	32-bit | 64-bit
Microsoft Diagnostics and Recovery Toolset (DaRT)	32-bit | 64-bit
Forefront Client Security	More information
Forefront Server Security	32-bit | 64-bit
Forefront Endpoint Protection	32-bit | 64-bit
System Center 2012 Configuration Manager	32-bit | 64-bit
System Center 2012 Endpoint Protection	32-bit | 64-bit
Windows Intune	32-bit | 64-bit

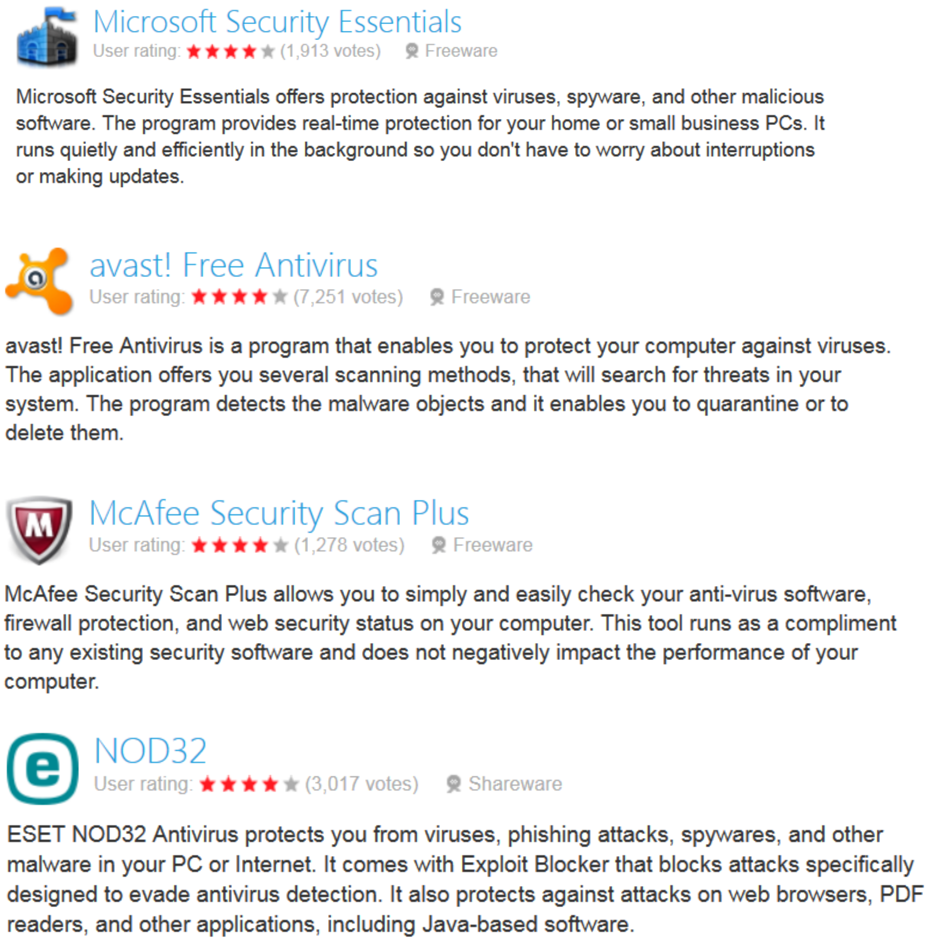
Good Source for Info/Downloads


Security & Privacy at Softw...
security-privacy.software.informer.com
Search
software.informer
Windows
Mac
Android
iPhone

Home

Security & Privacy

Other Tools



Microsoft Security Essentials

User rating: ★★★★☆ (1,913 votes) Freeware

Microsoft Security Essentials offers protection against viruses, spyware, and other malicious software. The program provides real-time protection for your home or small business PCs. It runs quietly and efficiently in the background so you don't have to worry about interruptions or making updates.

avast! Free Antivirus

User rating: ★★★★☆ (7,251 votes) Freeware

avast! Free Antivirus is a program that enables you to protect your computer against viruses. The application offers you several scanning methods, that will search for threats in your system. The program detects the malware objects and it enables you to quarantine or to delete them.

McAfee Security Scan Plus

User rating: ★★★★☆ (1,278 votes) Freeware

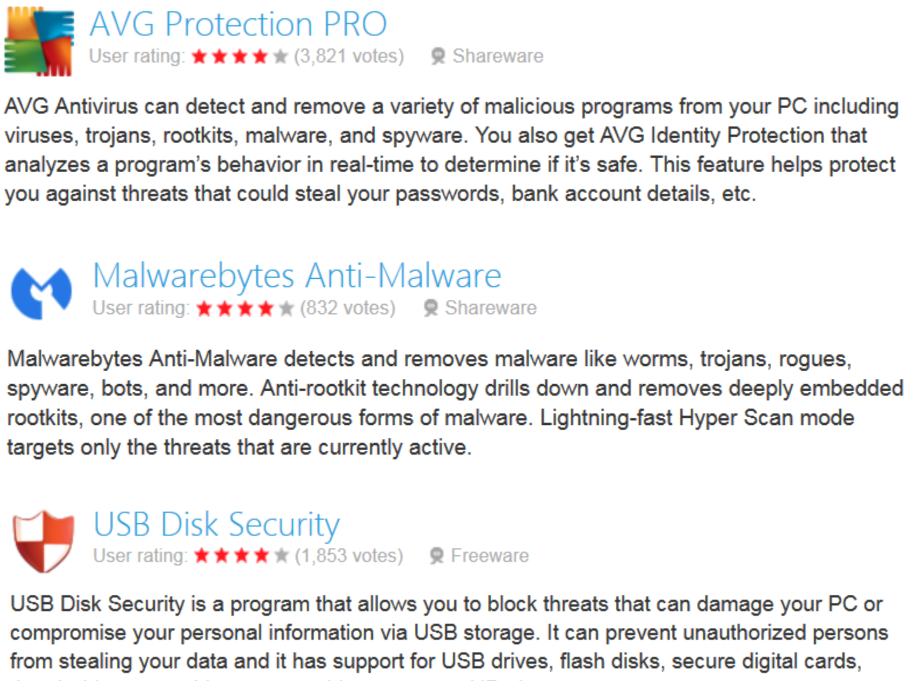
McAfee Security Scan Plus allows you to simply and easily check your anti-virus software, firewall protection, and web security status on your computer. This tool runs as a compliment to any existing security software and does not negatively impact the performance of your computer.

NOD32

User rating: ★★★★☆ (3,017 votes) Shareware

ESET NOD32 Antivirus protects you from viruses, phishing attacks, spywares, and other malware in your PC or Internet. It comes with Exploit Blocker that blocks attacks specifically designed to evade antivirus detection. It also protects against attacks on web browsers, PDF readers, and other applications, including Java-based software.

More Tools



AVG Protection PRO

User rating: ★★★★☆ (3,821 votes) Shareware

AVG Antivirus can detect and remove a variety of malicious programs from your PC including viruses, trojans, rootkits, malware, and spyware. You also get AVG Identity Protection that analyzes a program's behavior in real-time to determine if it's safe. This feature helps protect you against threats that could steal your passwords, bank account details, etc.

Malwarebytes Anti-Malware

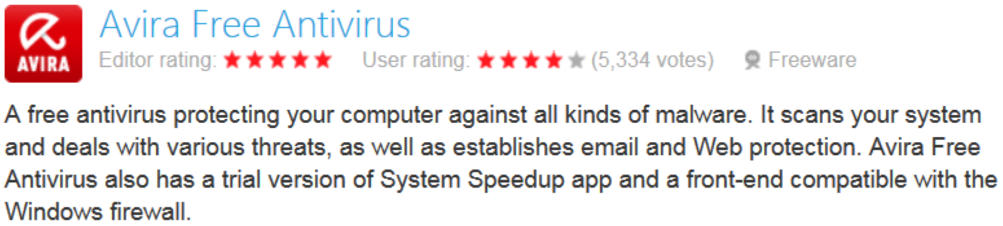
User rating: ★★★★☆ (832 votes) Shareware

Malwarebytes Anti-Malware detects and removes malware like worms, trojans, rogues, spyware, bots, and more. Anti-rootkit technology drills down and removes deeply embedded rootkits, one of the most dangerous forms of malware. Lightning-fast Hyper Scan mode targets only the threats that are currently active.

USB Disk Security

User rating: ★★★★☆ (1,853 votes) Freeware

USB Disk Security is a program that allows you to block threats that can damage your PC or compromise your personal information via USB storage. It can prevent unauthorized persons from stealing your data and it has support for USB drives, flash disks, secure digital cards,

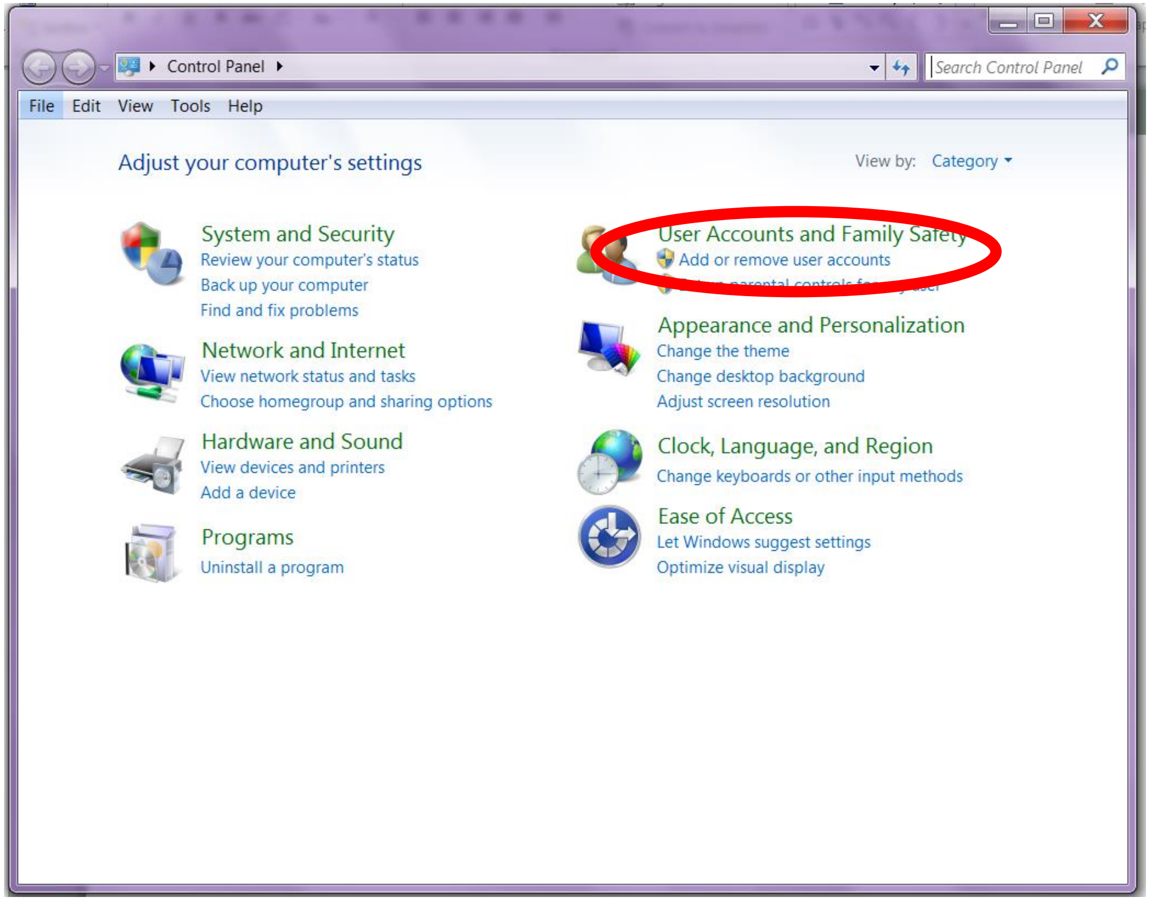


Avira Free Antivirus

Editor rating: ★★★★★ User rating: ★★★★☆ (5,334 votes) Freeware

A free antivirus protecting your computer against all kinds of malware. It scans your system and deals with various threats, as well as establishes email and Web protection. Avira Free Antivirus also has a trial version of System Speedup app and a front-end compatible with the Windows firewall.

Don’t Websurf as Administrator



Adjust your computer's settings

System and Security
Review your computer's status
Back up your computer
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

Hardware and Sound
View devices and printers
Add a device

Programs
Uninstall a program

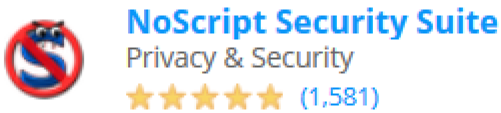
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user

Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution

Clock, Language, and Region
Change keyboards or other input methods

Ease of Access
Let Windows suggest settings
Optimize visual display

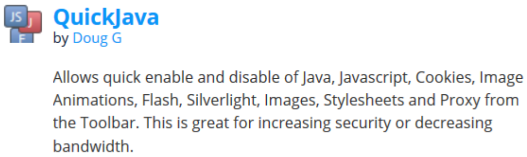
Browser Safety Habits



NoScript Security Suite
Privacy & Security
★★★★★ (1,581)

Disable automatic Javascript and other scripting languages

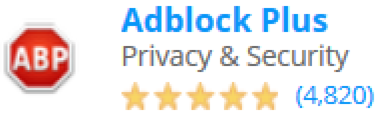
Or…



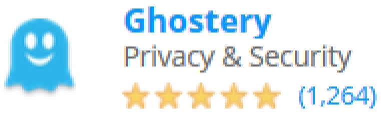
QuickJava
by Doug G

Allows quick enable and disable of Java, Javascript, Cookies, Image Animations, Flash, Silverlight, Images, Stylesheets and Proxy from the Toolbar. This is great for increasing security or decreasing bandwidth.

Suppress ads and popups



Adblock Plus
Privacy & Security
★★★★★ (4,820)



Ghostery
Privacy & Security
★★★★★ (1,264)

Minimize Tracking

To Fight Ransomware…

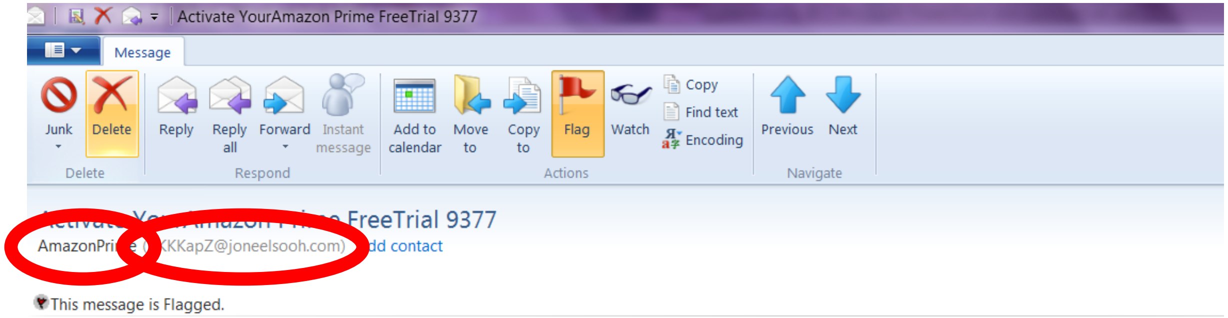
Backup!

And maybe try…

Trend Micro™ Anti-Ransomware Tool

Malwarebytes
ANTI-RANSOMWARE
BETA

Email Security

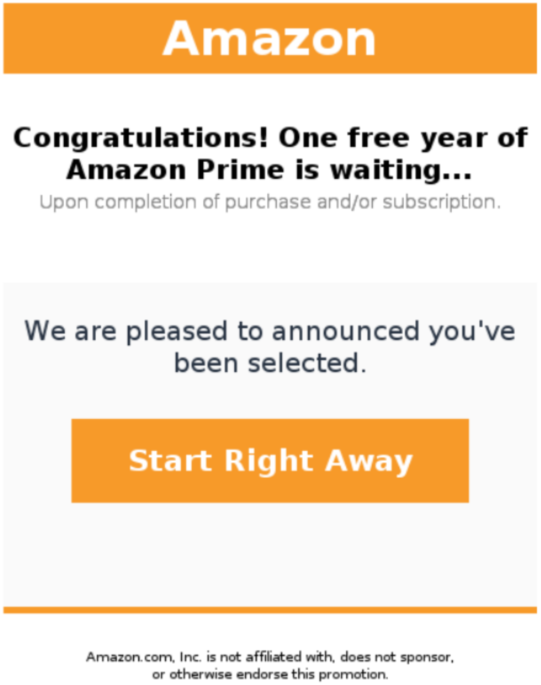


Activate YourAmazon Prime FreeTrial 9377

Activate YourAmazon Prime FreeTrial 9377

AmazonPri e (KKapZ@joneelsooh.com) dd contact

This message is Flagged.



Amazon

Congratulations! One free year of Amazon Prime is waiting...

Upon completion of purchase and/or subscription.

We are pleased to announced you've been selected.

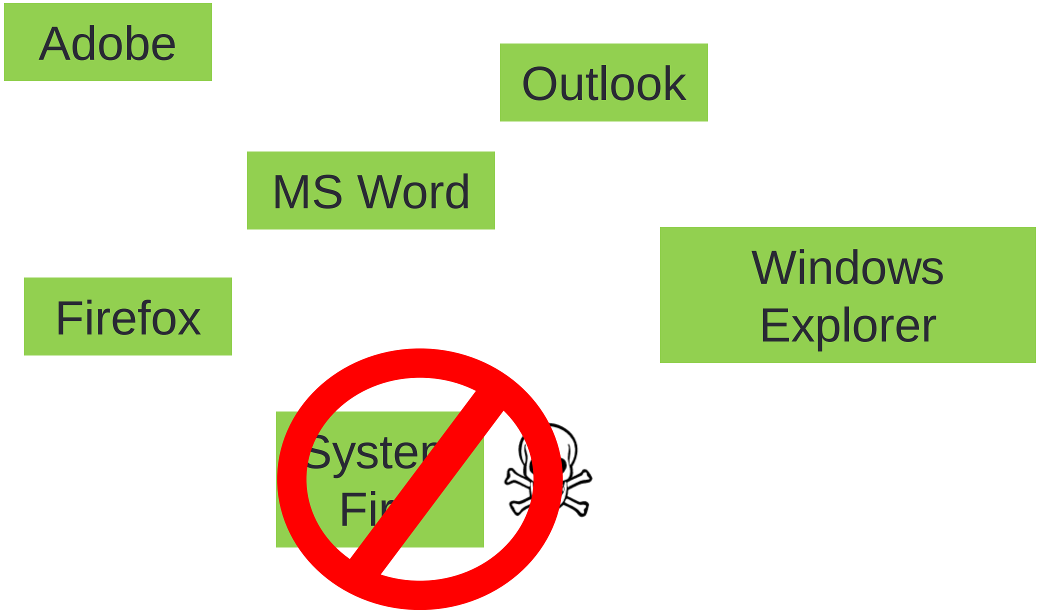
Start Right Away

Amazon.com, Inc. is not affiliated with, does not sponsor, or otherwise endorse this promotion.

Also be wary of email attachments!

If you are a bit tech savvy…

Try ***Application Whitelisting…***



Adobe

Outlook

MS Word

Firefox

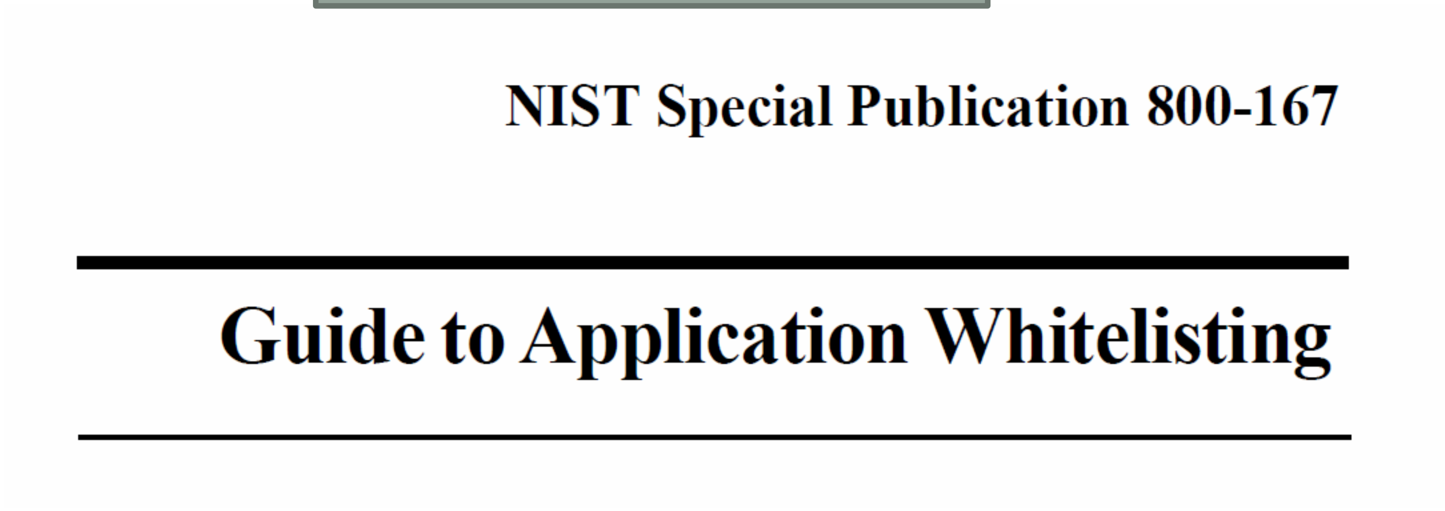
Windows Explorer

Syste Fi

Application Whitelisting

Application whitelisting is like the inverse of antivirus, which attempts to block known-bad programs. Whitelisting permits only known-good programs.

Recommended reading



NIST Special Publication 800-167

Guide to Application Whitelisting

Look up Windows Family Safety feature and use ‘child accounts.’

Some more ideas…

- Turn off the computer when not in use
- Occasionally examine Windows Task Manager
- Windows EMET is free, and helps---if you’re tech savvy
- Can try anti-rootkit freeware:

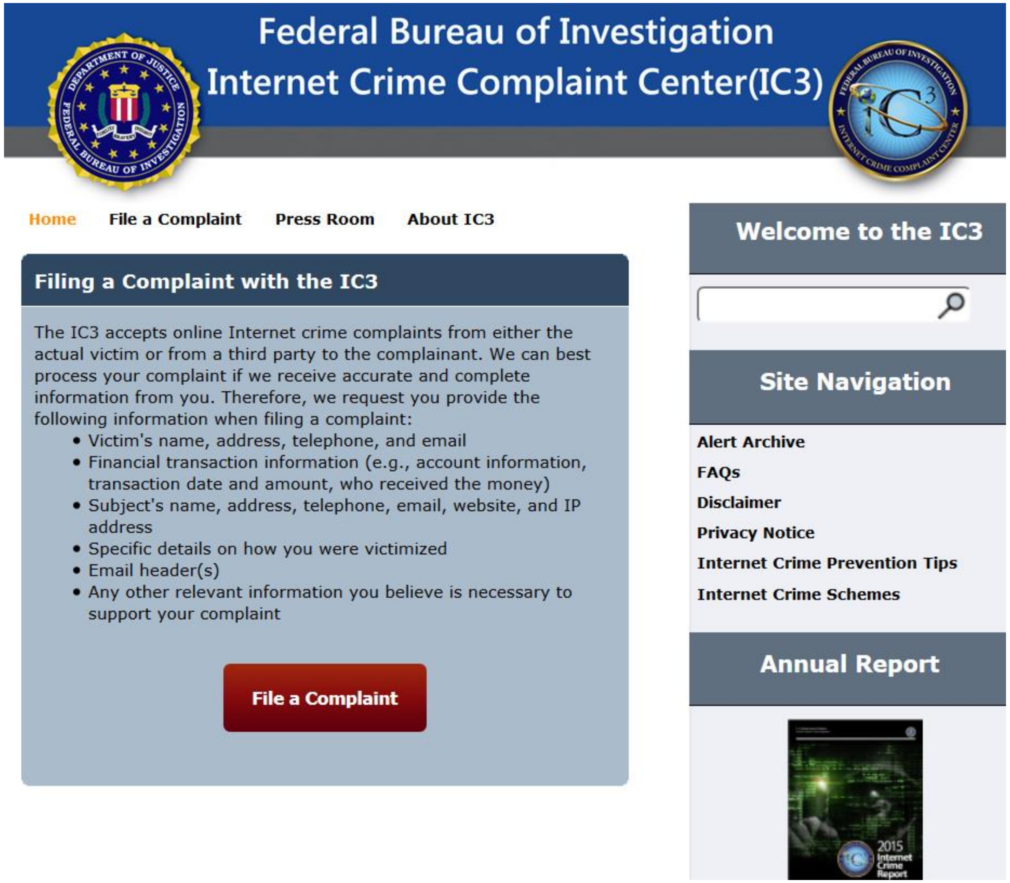
Vba32 Anti-Rootkit

Malwarebytes
Anti-Rootkit Beta

SOPHOS
Community BETA

Sophos Virus Removal Tool (SVRT)

What To Do If You’ve Been Hacked



Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Home File a Complaint Press Room About IC3

Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request you provide the following information when filing a complaint:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint

Welcome to the IC3

Site Navigation

Alert Archive
FAQs
Disclaimer
Privacy Notice
Internet Crime Prevention Tips
Internet Crime Schemes

Annual Report

Compared to those who defend corporate and governmental networks…

…you have a chance!

Happy surfing….

Questions

✉ manteuf@verizon.net