
AVG
Fighting Malware
How AV companies fight malware,
How malware fights AV companies,
And why…
Karel Obluk, Chief Scientist, AVG Technologies

Agenda

- Malware history
- Virus detection in a nutshell
- Current threats
- Fighting malware nowadays
- Web Threats
- Behavior Monitoring
- Mobile Malware

Malware History

- Good old times
  - 1987 – cca 1995
  - DOS viruses
  - Spreading fast – how fast? Within a month! Wow!
  - File infectors, memory-resident viruses, boot-sector viruses
  - E-mail? What e-mail?
  - No Linux viruses
- Windows
  - 'Eradication' of DOS viruses (well, not really)
  - Macro viruses – until the release of Office 2000
  - E-mail? Who uses e-mail?
  - First Linux virus (Staog – 1996)

Malware History - continued

- Mass-mailing worms
  - Cca 1999 – 2004
  - Who loves me? Hot tennis players…
  - E-mail scanning on gateways
  - ISPs scanning mails
- Bots and Worms, direct attacks
  - Cca 2001 – 2004
  - CodeRed anyone?
  - Directly attacking PCs
  - Windows XP SP2 released – with firewall on by default (and some other patches)
- Web based attacks
  - That's where the fun begins…
- And going mobile…

Why?

- First PC viruses:
  - Playing melodies
  - Screen effects
  - Computer freezes
  - Political statements
  - Erasing data
  - Blackmailing
- First virus authors:
  - Demonstrate skills

- Now:
  - **REAL MONEY!**

Why? Money Talks!

Good morning Sir,

When choosing a peniss stronger method, there are many MANY options these days. But very few are worth the money. In fact, most are scam! Don't get ripped off - you deserve the real thing!

Viagr Patches Shop are the newest, safest and absolutely most cheapest Shop with potent patchs you can buy here. No other shops even comes close to duplicating the prices found in our Viagr Patch Shop.

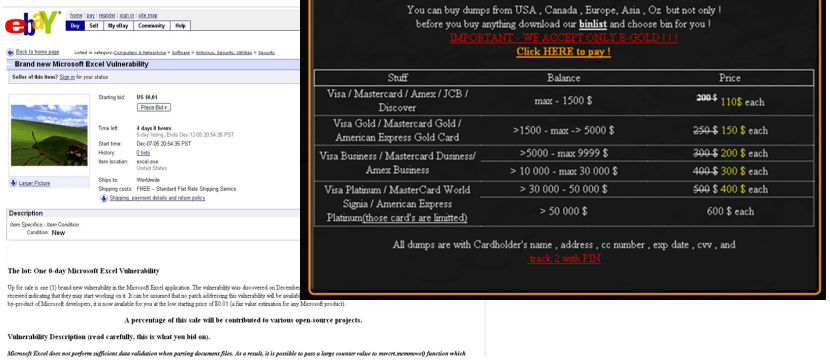
Try our Viagr Patches from our Shop and see how it can change your life!
<http://wwb.mj7f8nm1je4v1e7.jjplanularch.info>

Why? Money Talks!

- Get sensitive data
  - Access codes, passwords
  - Confidential information
- Bank accounts, credit card info
- Spying on you
- Industrial espionage
- Controlling your PC
  - SPAM *(Jeremy Jaynes, $24M, 9 years)*
  - Direct attacks – DDoS *(Estonia, 2007)*
  - Attacking other infrastructure
  - Anonymizing attackers
  - Hosting illegal content

Money Talks

- Highly profitable business
- Selling data, personal information
- Fraud As A Service



Stuff that we sell:

You can buy dumps from USA , Canada , Europe, Asia , Oz but not only !
before you buy anything download our **binlist** and choose bin for you !

IMPORTANT - WE ACCEPT ONLY E-GOLD ! ! !

Click HERE to pay !

Stuff	Balance	Price
Visa / Mastercard / Amex / JCB / Discover	max - 1500 $	~~200 $~~ 110$ each
Visa Gold / Mastercard Gold / American Express Gold Card	>1500 - max -> 5000 $	~~250 $~~ 150 $ each
Visa Business / Mastercard Dusiness/ Amex Business	>5000 - max 9999 $	~~300 $~~ 200 $ each
	> 10 000 - max 30 000 $	~~400 $~~ 300 $ each
Visa Platinum / MasterCard World Signia / American Express Platinum(those card's are limitted)	> 30 000 - 50 000 $	~~500 $~~ 400 $ each
	> 50 000 $	600 $ each

All dumps are with Cardholder's name , address , cc number , exp date , cvv , and track 2 with PIN

Malware, Viruses

- Virus:
  - *"A virus is a program that is able to infect other programs by modifying them to include a possibly evolved copy of itself"*

    Dr. Frederick Cohen, 1994
- Worm
- Trojan Horse, Dialer, Spyware, Adware…
- Infection types
  - File infectors
  - Boot sector, MBR
  - Deep integration into the hosting OS – register system extensions, redirect system functions, DNS changes, …

Virus Detection in a Nutshell

- Integrity checkers
  - First integrity checkers – file dates, …
  - Stealth techniques made it useless for virus detection
  - Even in DOS times (memory resident viruses, …)
  - Still useful as part of IDS
- Innoculation
  - And why it is a stupid idea
- Checksums
  - And how they can be defeated
- Too many files for a user to decide
- Document infection, media files, scripts, …

Virus Stealth Techniques

- Redirecting system calls, boot sector infection
- Preserving time stamp and file size
  - Compression
  - (Mis-)using file system structures
- Hiding within files (parasitic viruses)
  - Cavity viruses
  - Compressing viruses
  - Embedded decryptors (One_Half, Commander_Bomber)
  - Entry-Point Obfuscation (EPO)
- Avoid detection
  - Not trying to be stealth, rather avoid signature detection
  - Encryption
  - Server-side polymorphism

Current Threats

- File infectors still exist, but significantly fewer
- Files infecting the system
  - OS too complex for a typical user – social engineering
  - Deep integration in the system
- Social engineering attacks
  - Codecs, Rogue antivirus products
- Rootkits
  - MBR rootkits
  - virtualization
- Spearheaded attacks
- Combination of several techniques
- **HUGE** number of threats

Web Threats

- World War Web
  - Web currently the primary attack vector
- HTTP <=> GFBP
  - Generic Firewall Bypass Protocol
- Connection is made from the client
- Client actively downloads content
- Active content, lots of different data sources
- Browsers try to offer rich user experience

Web Threats

- Users nowadays somewhat educated – not to launch attachments, not to run unknown programs
- But visiting web sites is normal
- Nobody expects a 'trusted' website to be infected
- The result
  - Exploits for browsers, applications, OS
  - Social engineering attacks
- Exploit packs available

Even a security expert cannot – without proper tools – tell for sure if a website is safe

Social Networks

- Increasingly popular attack vector
- Key issue is **user trust**
  - *"I am among friends here!"*
  - *"What a great application this must be if Ian is using it!"*
- Not accessible to security crawlers
- Extremely fast spreading
- Combined with phishing / spam
- Social engineering techniques

Social Engineering

- Most popular type of attack
- 5x more attacks based on SE than exploits
- Rogue AV lead the pack
- Survey on social networks:
  - 21% users accept invitations from people they don't know
  - 52% allow their friends to access social networks from their computer
  - 64% will click on a link shared by others
  - 47% have experienced malware infection
  - 20% have experienced identity theft

- **EDUCATION!**

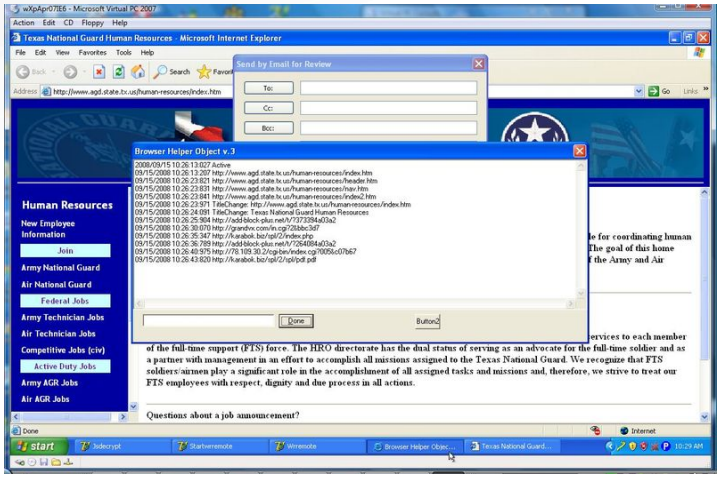
Some Numbers

- 1 out of 5 users infected every week
- 60 – 70 million detections every day
- 30 – 40 thousands new viruses every day
- More than 85% threats coming from web
- More than 85% web threats exist **< 1 day**
- 10 million sites blocked by AVG every day

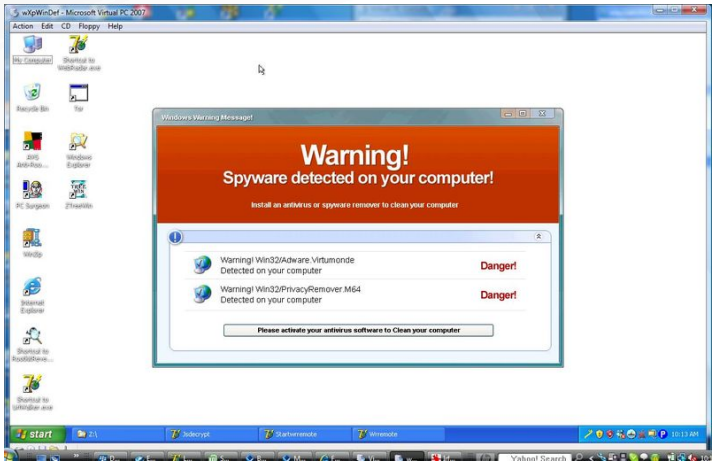
- Income from a single botnet $11,000 a day

Web Threats

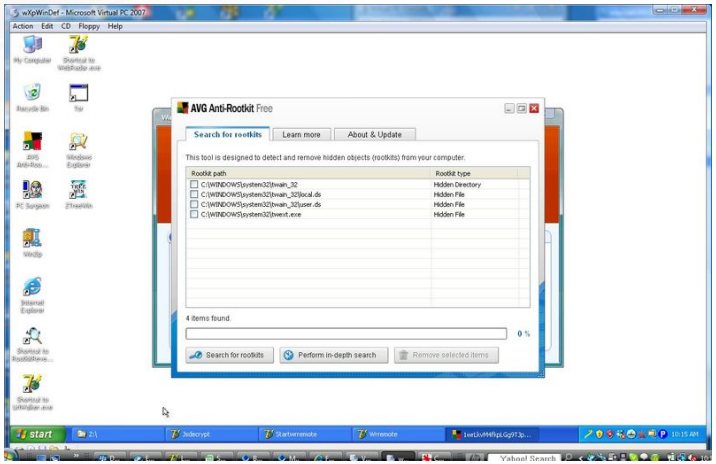
Web Threats – Texas NG



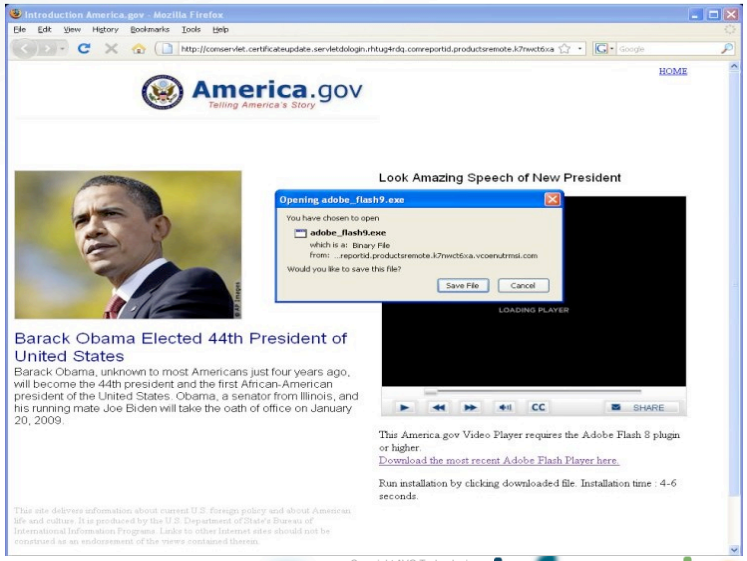
Web Threats – Texas NG



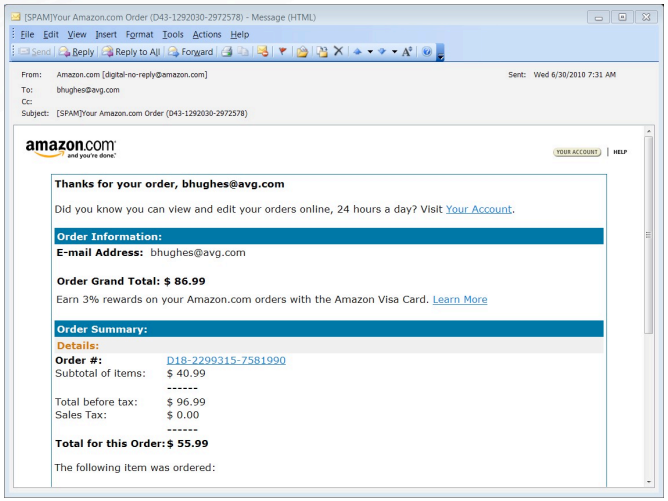
Web Threats – Texas NG



Web Threats – codecs



Fake e-mails



Fighting Malware Nowadays

- Simple checksums – ineffective since early 90s
  - Even though some 'antispyware' products used it
- Simple pattern matching – ineffective since early 90s
  - Even though some 'antimalware' products still use it!!!
  - Cannot cope with polymorphism, file infectors, new threats
- Sequences, generic detection
  - Similar to regexp but designed for code detection
- Patterns/checksums over some code ranges
  - Definition contains instructions on 'where to look', algorithmic

Fighting Malware Nowadays

- X-ray detections (cryptographic)
- Statistical methods
- Heuristics
- Emulators
  - Built-in virtual machine
  - Each executable run within this machine, observing actions and events
  - Also used to defeat encryptors or packers – scanning after some emulation (code decrypts itself)
- Behavior – not to be mistaken for emulation and heuristics!
  - More on behavior later

Detecting Web Threats

- Billions of web sites on the Net
- Database of good sites?
  - Huge! Ask Google
- Database of bad sites?
  - Inefficient! Ask Google
- Bad sites are highly transient
- Some threats active only at specific times
- Database approach:
  - Obsolete for most of threats
  - Outdated information for cleaned sites

Detecting Web Threats

- Threats are avoiding detection
  - Goal – maximize return on investment
  - Keep machines infected for as long as possible
  - Delay AV detection as much as possible
- Controlled distribution
  - Keeping below the radar, < 10k installations then different malware
- Avoiding crawlers
  - Different content for different geographies, IP blocks
  - Different content for different clients, marking clients
  - Different content based on where the user comes from
- Infected content in protected areas (behind login)
- Dynamically generated content, 3rd party content

Detecting Web Threats

- Detecting content!
  - Cca 40k new unique malware files / day
  - Only about 1000 exploits
- Centralized vs distributed approach
- Seeing what clients see

- Legitimate pages serving malware through 3rd party content
- Blended threats
  - Combining information theft with malware infection
  - Infrastructure attacks – DNS, fake certificates, …

Behavior Monitoring

When web threat gets in …
… or when user is tricked to launch malware …
… and signature scanner does not detect it …
the malware gets active!

Sending sensitive data, getting instructions from C&C, attacking other systems, …

- Behavior monitoring collects information about active processes
- Evaluates suspicious behavior
- Reports and remediates

Behavior Monitoring

- The good
  - Can detect completely new malware
  - Small footprint – very small database of rules
  - Detects what matters
- The bad
  - Cannot detect file infectors
  - Focused on malicious processes only
  - Lots of false positives

Let’s Go Mobile

- Mobile devices = ideal attack target
- Always online, increasing computing power
- Social engineering methods especially efficient
- New forms of monetization
  - Premium SMS
  - PIN and authentication eavesdropping
  - Sensitive data, GPS
- Android currently the most endangered

Android

- Not just mobile platform – GoogleTV etc.
- Very popular, also among developers
- Very well documented, based on Linux
- More open than iOS
  - Open appstore, yet high degree of trust
- Already numerous exploits
- Many attack vectors
- Need to check number of different data formats (media, wallpapers, …)
- Permission system does not guarantee 100% security
  - Known exploits, user is the weakest link

Some interesting attacks

- Estonia - 2007
  - Whole country without internet connectivity, economy severely damaged. DDoS, botnets as well as 'volunteers'
    http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
- Georgia - 2008
  - Severe disruptions in connectivity, attack on network infrastructure re-routed traffic. Performed and coordinated by RBN ('Russian Business Network)
    http://en.wikipedia.org/wiki/Cyberattacks_during_the_2008_South_Ossetia_war
- SCADA systems - 2010
  - Iran: Stuxnet worm, spread via USB sticks, focused on specific industrial equipment
  - Similar bugs discovered in Chinese SCADA systems (different vendor) – no known exploits
- Unintentional(?) attacks on the infrastructure
  - Hospital networks infected: London 2008, New South Wales Ambulance 2011 - http://www.bartsandthelondon.nhs.uk/formedia/press/release.asp?id=2077
    http://www.smh.com.au/technology/security/nsw-ambulance-service-back-online-after-virus-infection-20110214-1asv1.html
  - Power plant systemts infected: Cleveland 2003 - http://www.redorbit.com/news/technology/8586/computer_virus_may_have_caused_blackout/


http://member_cute-sexb6.systembars.com/index.html?Ref= - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://member_cute-sexb6.systembars.com/index.html?Ref=
Go
Links
SKIP
DO NOT PRESS
Done
Internet


AVG.