The Death of AV Defense in Depth ? - revisiting Anti-Virus Software

Sergio Alvarez – Director of Research
Thierry Zoller – Security Engineer

n runs professionals

Who are we ?

- Sergio Alvarez
  - > Director of Research @ n.runs AG
  - > Argentine
  - > Lives in Berlin since 2005

- Thierry Zoller
  - > Security Engineer @ n.runs AG
  - > Author of BTCrack, Secure-it, Harden-it
  - > Luxembourg

Revisiting AV Software ?

What will we talk about ?

- Attacking the Parsing Engines to Own the AV Software
  - > Sergio Alvarez
- Attacking the Parsing Engines to ByPass Detection
  - > Thierry Zoller (For reasons beyond his control couldn't be here today)

Death of AV Defense in Depth ? > TOC

Introduction

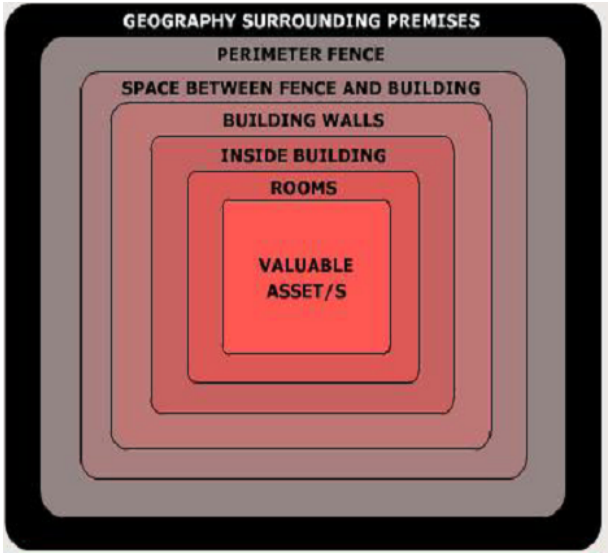
- This talk is **NOT** about the Death of DiD as a concept.

- This talk is about
  - > questioning real-life **implementations** of DiD, specifically as implemented for Anti-Virus solutions and Email Security (“AV DiD”)
  - > showing the threat is real (Demos)
  - > discovering new bugs =)

Death of AV Defense in Depth ? > Military

The Roots of „Defense In Depth“

- Defense in Depth (DiD) originally is a concept as used by ancient Military. Main Goal : Get more time



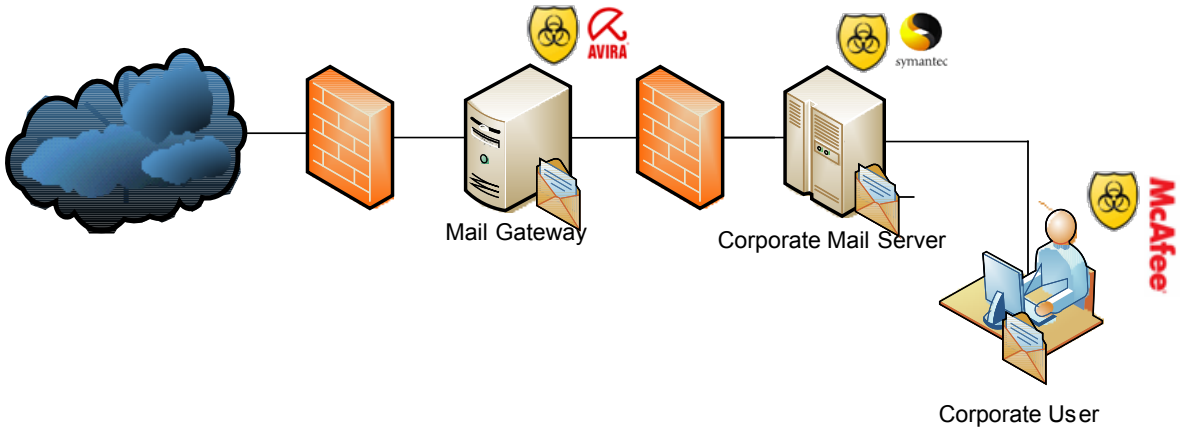
- In General “The paradigm describes an approach where you assume that individual (even multiple) elements of your defense fall, **in the worst possible way** “

n runs professionals

Death of AV Defense in Depth ? > IT Security

Transposing DiD to AV and IT Security in General

- IT Security DiD is about reducing the attack surface
- IT Security DiD is about having multiple redundant security measures
- **AV DiD** is generally being defined and promoted according to this logic (and best practices) :



- The Problem : You **think** you have implemented DiD when in reality **you have not** , you just created a much bigger problem. Let us explain.

nruns professionals

* Vendor names were chosen randomly

Death of AV Defense in Depth ? > Problem

Where is the Problem ?

- Recap : In General “The paradigm describes an approach where you assume that individual (even multiple) elements of your defense fall, **in the worst possible way** “
- Where is the Problem ?
  Current **AV DiD** implementations define “**the worst possible way”** an Anti-virus product may fail as “*Fails to detect a threat*” or “*Fails to detect a virus*” whereas in reality the *worst possible way* is a more severe one: Compromise of the underlying OS through the Anti-Virus Engine.

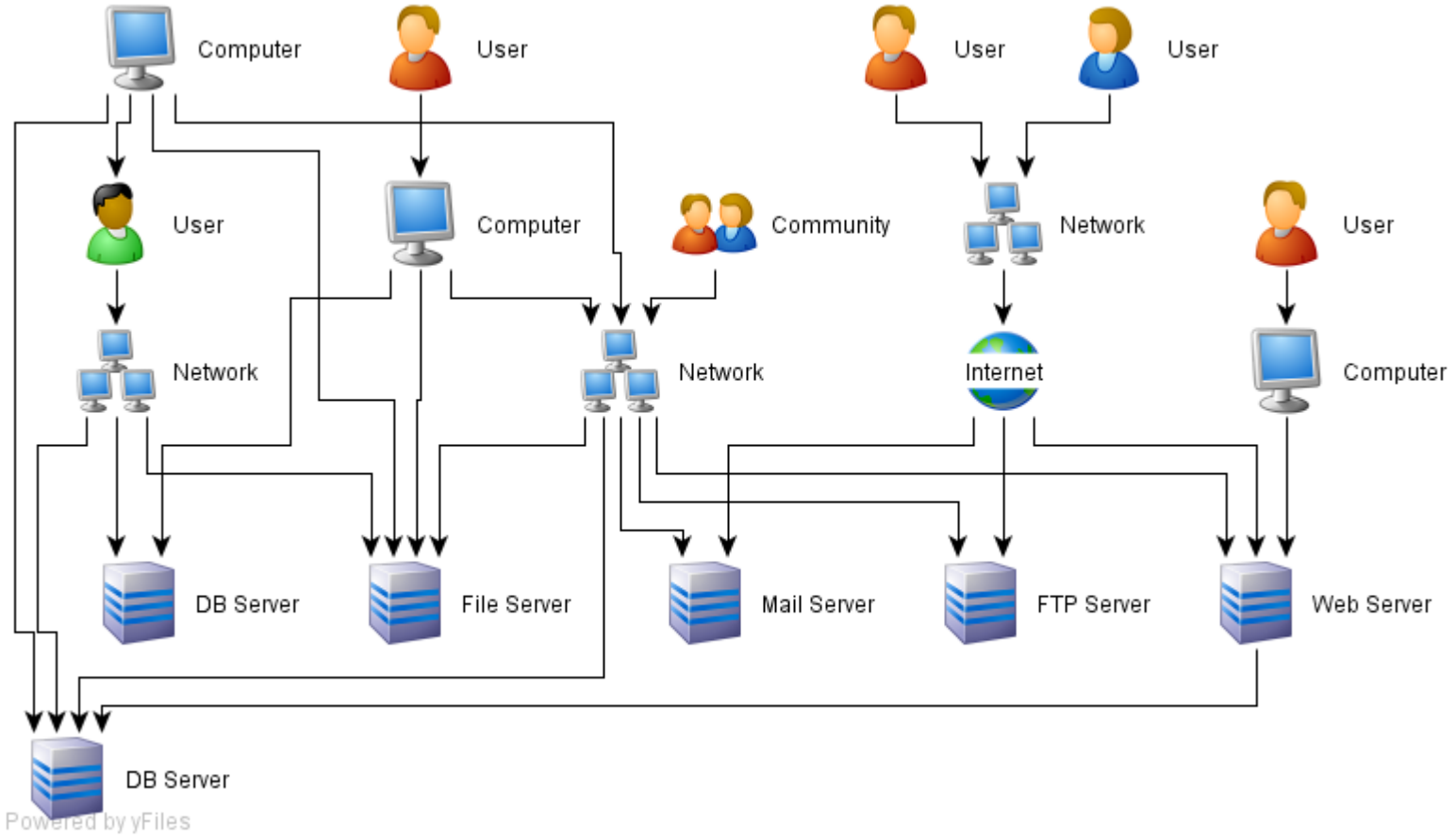
- **The result is that AV software itself is left with no protection at all, there is rarely any kind of mitigation.**
- Side-Note : “Worst possible Failure” in general for Security Software (IPS, IDS, AV..) is defined as “fails to detect/react/alert”. Attacks on the Defenses themselves are rarely taken into account.

- This has led the industry to deploy **AV DiD** in a way that is detrimental to the concept
  - Multiple AV engines running on critical Servers with high privileged rights
  - AV Engines everywhere, high privileges, unprotected.
    - Mail gateways
    - Servers (WWW, DB, Fileserver..)
    - Clients
    - …

[1] “Anti-Virus Defense in Depth” - Microsoft

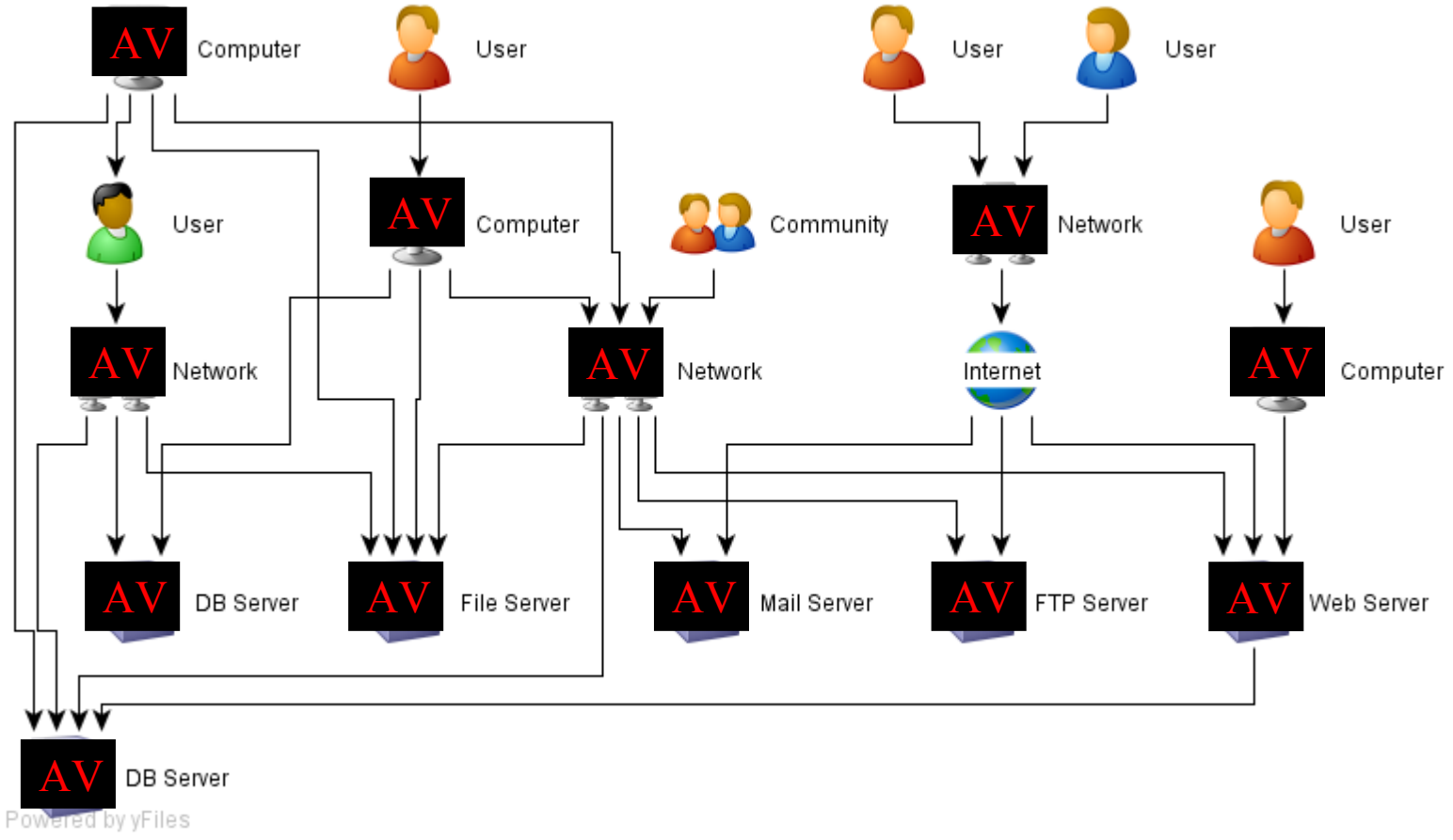
Anti-Virus Software > Anti-Virus Software is everywhere

So where is the problem ?



Anti-Virus Software > Anti-Virus Software is everywhere

So where is the problem ?



Anti-Virus Software > Myths

Why bother ? AV Software is secure by design…

- Antivirus Security Myths :
  - > Antivirus Software is secure
  - > Makes our network and systems more secure
- Antivirus Developers Myths :
  - > AV Software is developed by security experts
- Antivirus Detection Myths :
  - > I use Antivirus Software, I will not get infected
  - > My Antivirus Software detects even unknown viruses

nruns professionals

Anti-Virus Software > Facts

Here are the facts

- Antivirus Security Facts :
  - > HUGE Attack surface
  - > Parse thousands of formats (Kaspersky claims over 3000)
  - > Programmed in unmanaged languages (Performance)
  - > **It takes time and resources to re-create the AV engines from scratch In managed languages (read: bugs will stay here for a while)**
  - > The result : Antivirus have to deal with so many file formats that chances are good there is more than one security flaw

- Antivirus History
  - > First developed to protect against Boot Sector and Viruses
    - > Infection Vector : Disc
  - > Overhauled to protect against Worms
    - > Infection Vector : Network
  - > Overhauled yet again to work on Servers/Gateways
    - > Code ported, Logic not adapted (see Bypass)

- Code reused – 15 years
- Logic not adapted to new vectors
- Vulnerabilities ported over

Anti-Virus Software > Facts

Here are the Facts

- It gets even worse :
  - > More parsing code as AV software mutates to an All-in-one Solution
  - > They now start coming with IDS/IPS functions
  - > The more engines are involved, more potential bugs are involved, you are unknowingly increasing the attack surface by following best practices.

- A small sample from these widely supported formats (includes variants)
  - > Zip, Zip SFX, ARJ, ARJ, SFX, TAR, GZ, ZOO, UUEncode, TNEF, MIME, BINHEX, MSCompress, CAB, CAB SFX, LZH, LZH SFX, LHA, RAR, RAR SFX, JAR, BZ2, Base64, Mac Binary, ASPack, CHM, DOC, EML, EXE, FSG, HLP, PDF, Yoda, ELF, PPT, OPD, and many more.
  - > If the creators of these file types themselves have problems parsing them, what are the chances for the antivirus to get them all right? (scary, isn't it?)

nruns professionals

Anti-Virus Software > Facts

Here are the Facts

- Want to try it yourself? :
  - > Open your favourite AV in IDA Pro (4.9 is free)
  - > ALT+t and search for ‘RAR’
  - > Double click and check what file formats it supports.


```
.rdata:601EA638 String2        db '.rar',0          ; DATAXREF: sub_601CE320+165o
…
.rdata:601EA65C ; char aSfx[]
.rdata:601EA65C aSfx           db 'sfx',0           ; DATAXREF: sub_601CF6E0+88o
.rdata:601EA660 ; char aExe[]
.rdata:601EA660 aExe           db 'exe',0           ; DATAXREF: sub_601CF6E0+6Do
…
etc
```

- The following is a RAW output from a random AV solution:
  - > 7z, zip, exe, arj, tar, gz, bz, ace, tgz, uue, xxe, lzh, lha, ice, com, zoo, dat, ??_, cab, rar, jar, 386, ? HT*, ACM, ADE, ADP, ANI, APP, ASD, ASF, ASP, ASX, AWX, AX, BAS, BAT, BIN, BOO, CDF, CHM, CLASS, CMD, CNV, CPL, CRT, CSH, DLL, DLO, DO?, DOC, DRV, EMF, EML, FLT, FOT, HLP, HT*, INF, INI, INS, ISP, J2K, JFF, JFI, JFIF, JIF, JMH, JNG, JP2, JPE, JPEG, JPG, JS*, JSE, LNK, MD?, MDB, MOD, MS?, NWS, OBJ, OCX, OLB, OSD, OV?, PCD, PDF, PDR, PGM, PHP, PIF, PKG, PL*, PNG, POT, PPS, PPT, PRG, REG, RPL, RTF, SBF, SCR, SCRIPT, SCT, SH, SIS, SHA, SHB, SHS, SHTM*, SPL, SWF, SYS, TLB, TMP, TSP, TTF, URL, VB?, VCS, VLM, VXD, VXO, WIZ, WLL, WMD, WMF, WMS, WMZ, WPC, WSC, WSF, WSH, WWK, XL?, XML

Anti-Virus Software > Facts

Here are the Facts

Antivirus Software is a *must have*

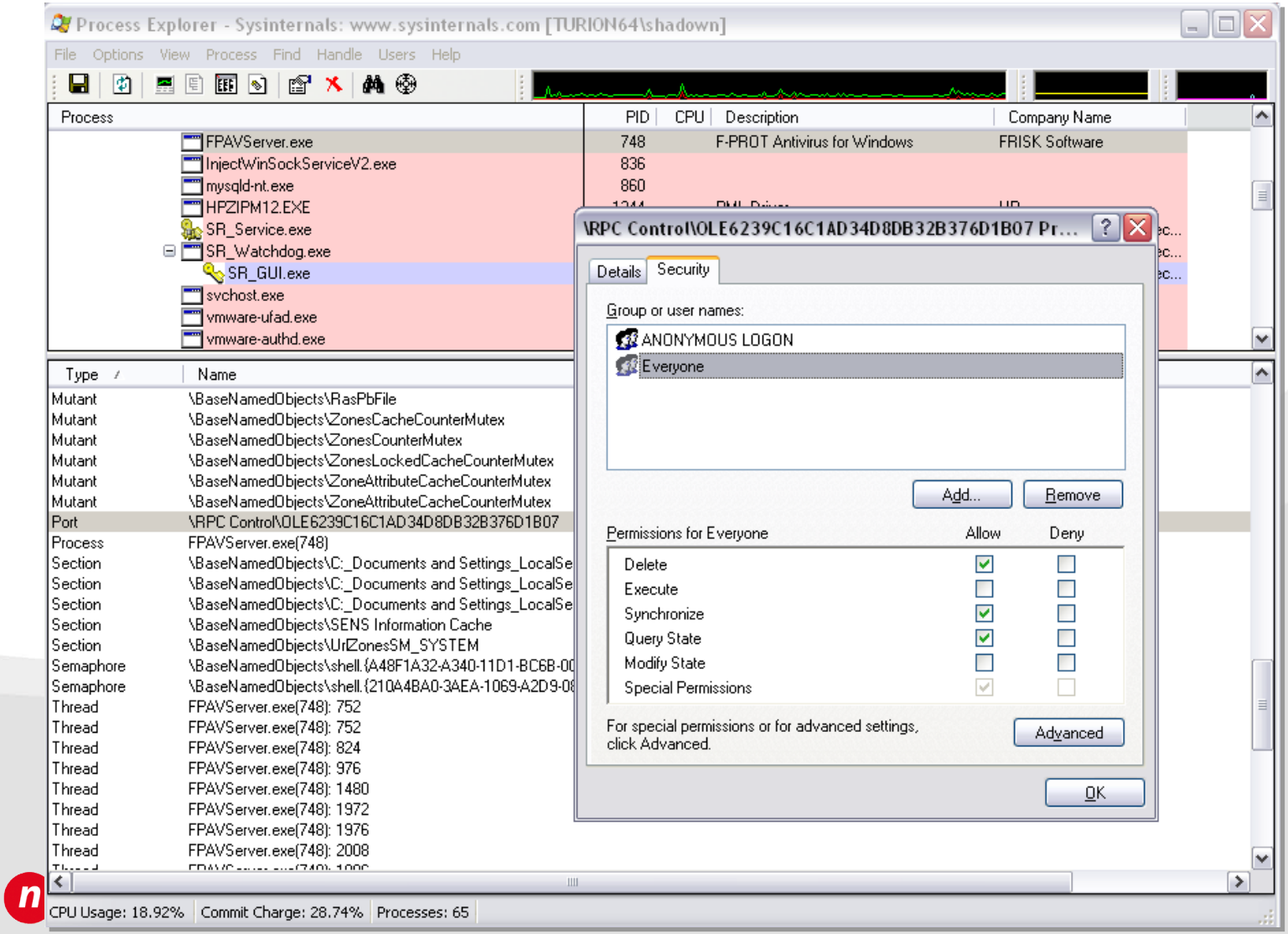
Death of Defense in Depth ? > TOC

Anti-Virus Software > General problems

Common Problems

- Communication Protocols Security by Obscurity
  - Hard coded passwords in the binaries
- Improper Password Handling
  - Storing the password of the administration console in the client's configuration file, too. (TrendMicro did this some time ago, 'encrypted' with a char depending on position mutation algorithm.)
- Client Listeners Standard Security Issues
- NULL DACLs
  - Registry for Settings
  - Configuration Files
  - Handles

Anti-Virus Software > General problems



Anti-Virus Software > General problems

Vulnerability Notification

- We report every bug to the vendor before publishing *any* Information
  - > It's difficult !
  - > Even finding the correct person to talk to
    - > secure@ / security@ - do not always exist
  - > Bugs are more often than not fixed quietly
  - > 10 Bugs reported transformed in 1 Bug being published ("Fixed Archive bypass")
  - > For Bypasses - Risk Rating is often a joke
    - > Don't make the difference between Client and Gateway Solutions
  - > We spent days explaining bugs :
    - > "It just crashes because it jump invalid memory location, EIP points to x41414141, that address does not exist, it's not a security Problem…
    - > Hey, but that exceptions is handled !

nruns professionals

Anti-Virus Software > General problems

Vendor Responses

Dear Thierry Zoller,

In keeping with our security policy, we have sent this note to provide you with information about the status of security investigation MFE-FW-20060227-01, which we have undertaken in response to the report you sent us in February 27 of 2006. Please advise if there is additional information you need. We will send the next status to you next week, typically Monday by close of business GMT-5.

. Date of this status report: October 15, 2007

. Current status of investigation: Patch is being developed

. Progress since last report: Investigation Completed

. Next steps: Patch is currently being developed

. Problems: None

Anti-Virus Software > General problems

Vendor Responses

> We cannot accept poc code that contains malicious code. Can you resend the poc using the Ecair test virus? Your original poc has been deleted.

Not possible, the Eircar string can be found in a ZIP file pretty easily as it is not compressable, it also has specific Lenght alltogether no realiable check for evasion.

I resend the POC13 with password

Anti-Virus Software > General problems

Vendor Responses

```
Hi Thierry,

I do not consider this to be an issue. If Microsoft's own tools can't
parse it then I am not too concerned about it.

[X:\crashes\2007\06-08-07-evasion-cab-1\1]cabarc x POC-#22-CAB-Version.cab

Microsoft (R) Cabinet Tool - Version 5.00.2134.1
Copyright (C) Microsoft Corp. 1981-1999.

FDIIsCabinet() failed: 'POC-#22-CAB-Version.cab' is not a cabinet
```

The Problem is Winrar & Winzip can extract that file – this makes it a security problem if this file is reported as clean.
Who here in this Room uses Winrar or Winzip ?

Anti-Virus Software > General problems

Vendor Responses

The detection bypass vulnerability in all Norman Antivirus products was discovered and reported by Sergio Alvarez. Here's the vendor response:

> *We have discussed your mail. It is not our company's policy to publish information about vulnerabilities or bugs in our software, unless they are extremely critical and/or can be worked around by the end-user. There are usually a large number of vulnerabilities/bugs in any software, and in our opinion it would only serve to unsettle user confidence in the products if the industry continually feeds information about such weaknesses, and we don't see that it would give the user any benefit in return.*
>
> *Instead we feel that it should be the supplier's responsibility to correct any errors and weaknesses and have them released to the user fast and silently, without alerting also the malware industry.*
>
> *Hence, there is no forum where we can credit you for your findings.*

Anti-Virus Software > General problems

Vendor Responses

It's hard to imagine that the respective fix would be directly related to your files because we haven't had them. Don't get me wrong, we have no problem crediting anyone who reports bugs to us, helping us to improve our software (just as we did e.g. in the case of version XXXXX where we credited XXX YYYY - see http://www.linktothecredit) but I don't think this applies here, really...

Sorry - maybe you can find some other overruns in the current build? (or, even better, in the build that's coming out in about a week - because that one has some new fixes in it, too [so it's theoretically possible you'd hit something that has already been fixed, too]).

Death of Defense in Depth ? > TOC

Anti-Virus Software > Hunting Bugs

Anti-Virus Bypass

- AV Bypass / Evasion
- Problem widely known since 2005, nearly no vendor reacted to early reports
  Wakeup call 3 months after revealed nearly none of them had patched the bypasses
- What is AV Evasion ?
  - > Key concept : AV engine cannot extract an archive, but the user can
  - > Why is this important ?
    - > Sneaking malicious code through gateways, hiding content in general, infected files on fileservers etc.
  - > Typical arguments from AV vendors :
    - > Argument 1 We will catch the malicious code at run-time (on-access) so bypasses are no threats.
    - > Problem: Your Gateway/Server Solutions do **NOT** execute the code, so there is **NO** on-access scan as there is no access/execution. As such the engine cannot scan the files inside and will generally flag the file as clean (Consequences might be: Mail is sent further and marked as clean, file is downloaded etc.)
    - > This is also a problem for AV clients if they are run in an environment where files are not executed (Fileservers, Mails, Web servers, Online Mail services etc.)
    - > Argument 2 “It’s the same than adding a Password to a Zip file, we can’t scan these either”
      This is why companies often choose to have GW Policies to generally forbid encrypted files (and have them allowed for specific addresses upon request), for the simple reason that they cannot be scanned. Furthermore for these encrypted files, AV engines in general add a Banner/Title to indicate the file was not scanned “File not scanned” indicating that it should be treated as such, this warning does not show for bypasses.

Anti-Virus Bypass

- Bypasses: F-Secure as of to-date is the only AV vendor we are aware of that estimates the risk in the advisories according to where and how the product is used
  - > Low Risk for Client Software
  - > High Risk for Gateway Products

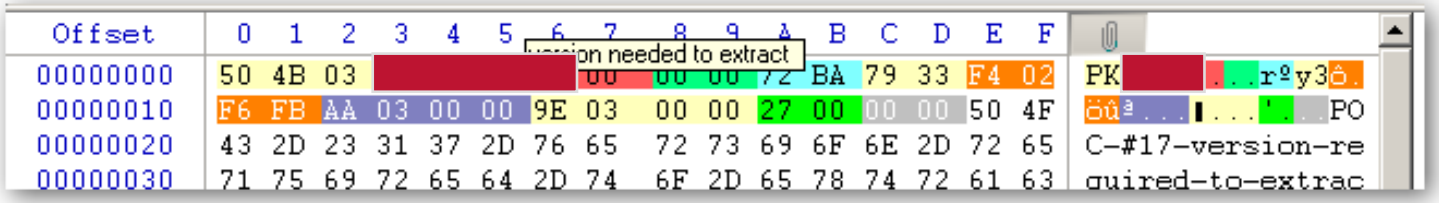
- Message to AV companies :

Your goal is to detect malicious code, do not flag supported archive formats as clean if you error on parsing them.

(Flag **supported** archive formats as unscanned/suspicious, **because** the engine wasn't able to scan the content)

Anti-Virus Bypass

- Example of a bypass
- Version_needed_to_extract Field (ZIP)
  - > Extracts without errors in Winrar (i.e. the user will execute whatever is inside)

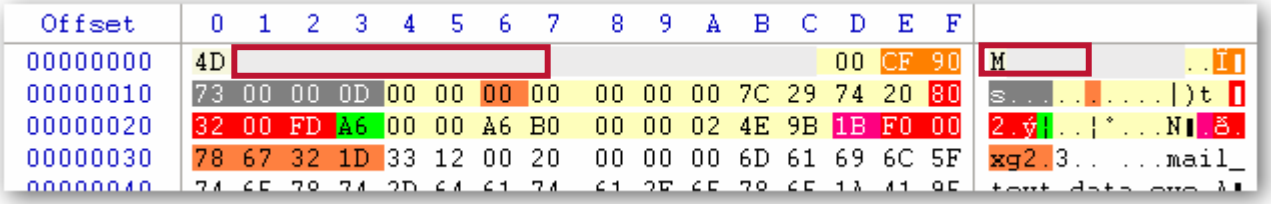


20 AV Vendors

"Vulnerable"

Anti-Virus Bypass

- Example of a bypass
- Adding a EXE header (MZ) to a RAR file
  - > Winrar extracts file without Errors



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	4D													00	CF	90
00000010	73	00	00	0D	00	00	00	00	00	00	00	7C	29	74	20	80
00000020	32	00	FD	A6	00	00	A6	B0	00	00	02	4E	9B	1B	F0	00
00000030	78	67	32	1D	33	12	00	20	00	00	00	6D	61	69	6C	5F

16 AV Vendors

"Vulnerable"

Addendum 11/2007:
TZO: It has come to my attention that this bug was a re-discovery, In OCT 2005 somebody by the nickname of fRoGGz found this issue and published the results: CVE | BID .

This also means that what you see is a list of vendors might not have reacted since 2005 or have introduced the same bug.

nruns professionals

Hunting Bugs

- Attack Vectors Testing
  - > Entry Points Runtime Analysis
    - > Wireshark
    - > Cdb
    - > OllyDbg
    - > Dum(b)ug
    - > PaiMei (win32)
    - > vtrace (multiplatform debugging framework)
    - > Sysinernals tools, etc
  - > Parsers Analysis (idem above – Wireshark + IDA)
  - > Fuzzing
    - > Peach, Sulley, custom scripts, etc.

Hunting Bugs

- Fuzzing Techniques (Generators + Publishers + Debug APIs)
  - Fuzzing Engine
    - Customizable structures to represent the datatypes
    - Supports structure recursions (embedded structures)
    - Add customized structures on the fly (responses based)
    - Function Call Interception (script on top of vtrace)
      - Argument/Return value manipulation in runtime
      - Allows to fuzz virtually (almost) anything
  - Runtime tracing (customised scripts on top of vtrace)
    - Automated Tracing
    - Function Call Hijacking
    - Multiplatform (Windows, Linux, MacOSX)
    - Easy to extend

Hunting Bugs

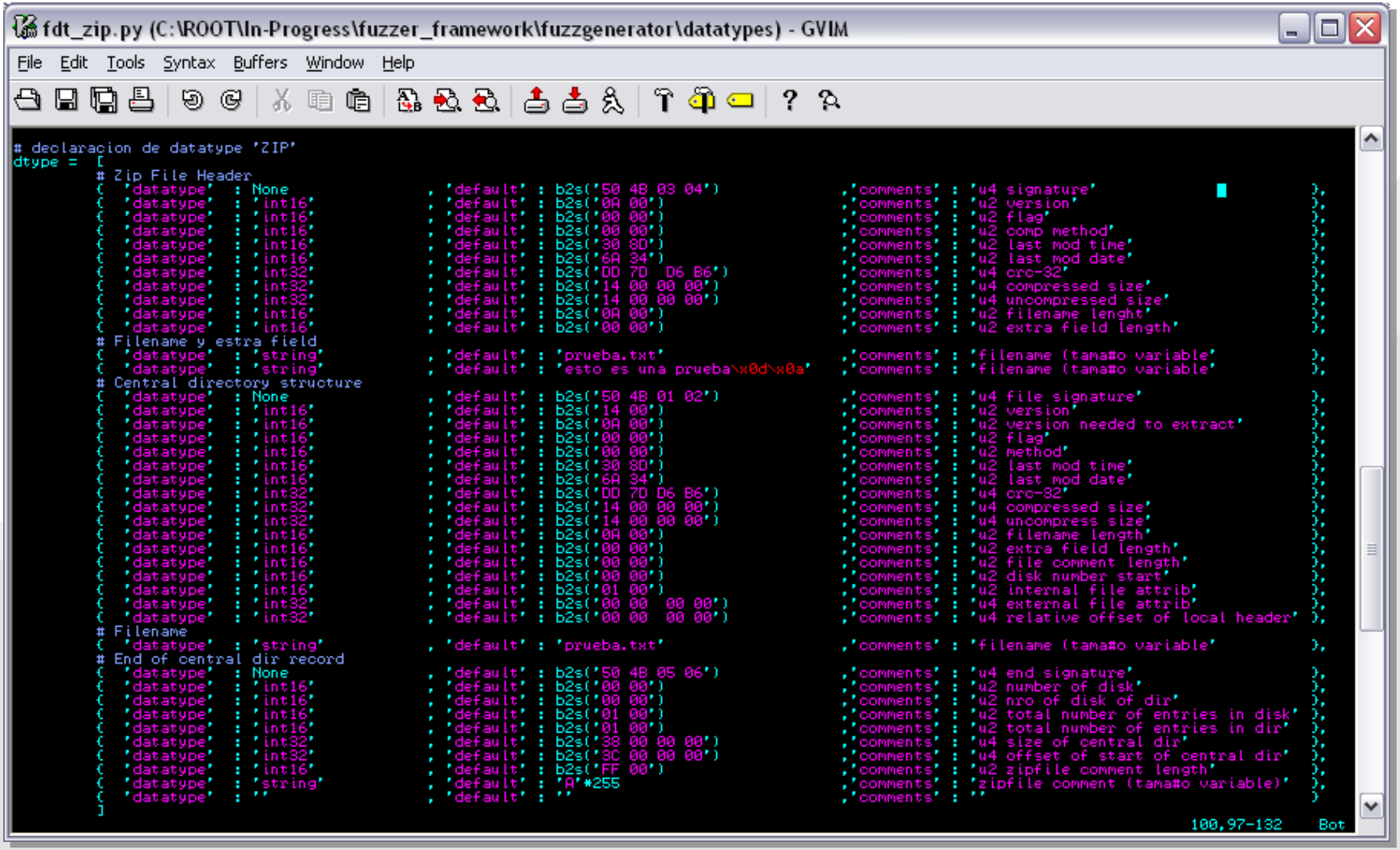
A. Local file header:	
local file header signature	4 bytes (0x04034b50)
version needed to extract	2 bytes
general purpose bit flag	2 bytes
compression method	2 bytes
last mod file time	2 bytes
last mod file date	2 bytes
crc-32	4 bytes
compressed size	4 bytes
uncompressed size	4 bytes
filename length	2 bytes
extra field length	2 bytes
filename	(variable size)
extra field	(variable size)
B. Data descriptor:	
crc-32	4 bytes
compressed size	4 bytes
uncompressed size	4 bytes
C. Central directory structure:	
central file header signature	4 bytes (0x02014b50)
version made by	2 bytes
version needed to extract	2 bytes
general purpose bit flag	2 bytes
compression method	2 bytes
last mod file time	2 bytes
last mod file date	2 bytes
crc-32	4 bytes
compressed size	4 bytes
uncompressed size	4 bytes

PKZIP

Principal Targets
- Size/Length fields
- String Fields

Anti-Virus Software > Hunting Bugs

Hunting Bugs



Hunting Bugs

- Some Tips
  - > Simultaneous fields fuzzing does give very good results
  - > When a file type has a TLV structure, don't fuzz only one stage only, it's always more effective to use multiple TLV instances.
  - > Look for Path-Flow Coverage, not for Code Coverage
  - > When exploiting heap massaging is easily accomplished with embedded compressed files ;), use it!
  - > If you want to target multiple engines at once, compress your exploits together in the same file
  - > Files names and files other IS IMPORTANT, the engines analyze them in that same order.

Hunting Bugs

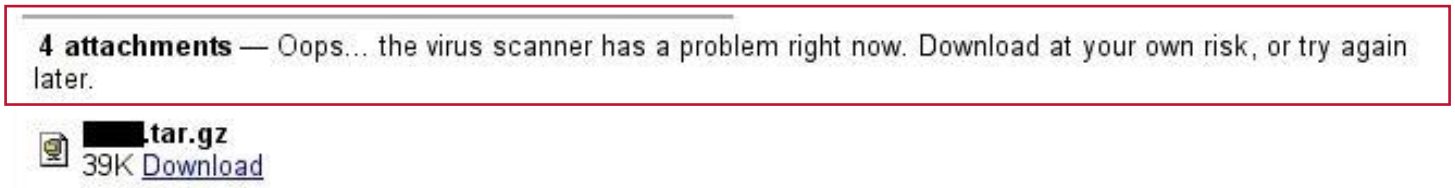
- Useful links with files specs
  - > http://www.wotsit.org/
  - > And Google a lot ;)
  - > Microsoft files type specs are available at Microsoft website.

Death of Defense in Depth ? > TOC

Anti-Virus Software > Facts

The Result

- End up in:
  - > Unprotected Settings (wrong DACLs)
  - > Detection Bypass / Evasion
    - > Low Impact for AV clients, Important for Gateways
  - > Privilege Escalation
  - > **DoS**
    - > AV dies, Mail service continues
    - > AV dies, takes OS with it, no more mails
    - > Blue Screen of Death
  - > **Remote Code Execution**



Question : Who recognizes this Email service ?

Anti-Virus Software > Facts

The Result

- The Result :

25.07.2007 CA eTrust - Denial of Service Advisory [CHM]
23.07.2007 Norman Antivirus - Denial of Service Advisory [DOC]
23.07.2007 Norman Antivirus - Detection Bypass Advisory [DOC]
23.07.2007 Norman Antivirus - Arbitrary Code Execution Advisory [LZH]
23.07.2007 Norman Antivirus - Arbitrary Code Execution Advisory [ACE]
20.07.2007 Panda Antivirus - Arbitrary Code Execution [EXE]
20.07.2007 ESET NOD32 - Denial of Service [ASPACK+FSG]
20.07.2007 ESET NOD32 - Denial of Service [ASPACK]
20.07.2007 ESET NOD32 - Arbitrary Code Execution [CAB]
04.06.2007 F-Secure Denial of Service [FSG]
04.06.2007 F-Secure Denial of Service [ARJ]
01.06.2007 F-Secure Remote Code Execution [LZH]
30.05.2007 Avira Antivir Infinite Loop [TAR]
29.05.2007 Avira Antivir Divide By Zero [UPX]
28.05.2007 Avira Antivir Abitrary Remote Code Execution [LZH]
25.05.2007 Avast ! Heap Overflow [SIS]
24.04.2007 Avast! Heap Overflow [CAB]

nruns professionals

+100 Vulnerabilities
reported just by Sergio
@40 fixed
@20 didn't even replay

Over 800 bypasses
some refuse to fix at all..

Anti-Virus Software > E-Mail

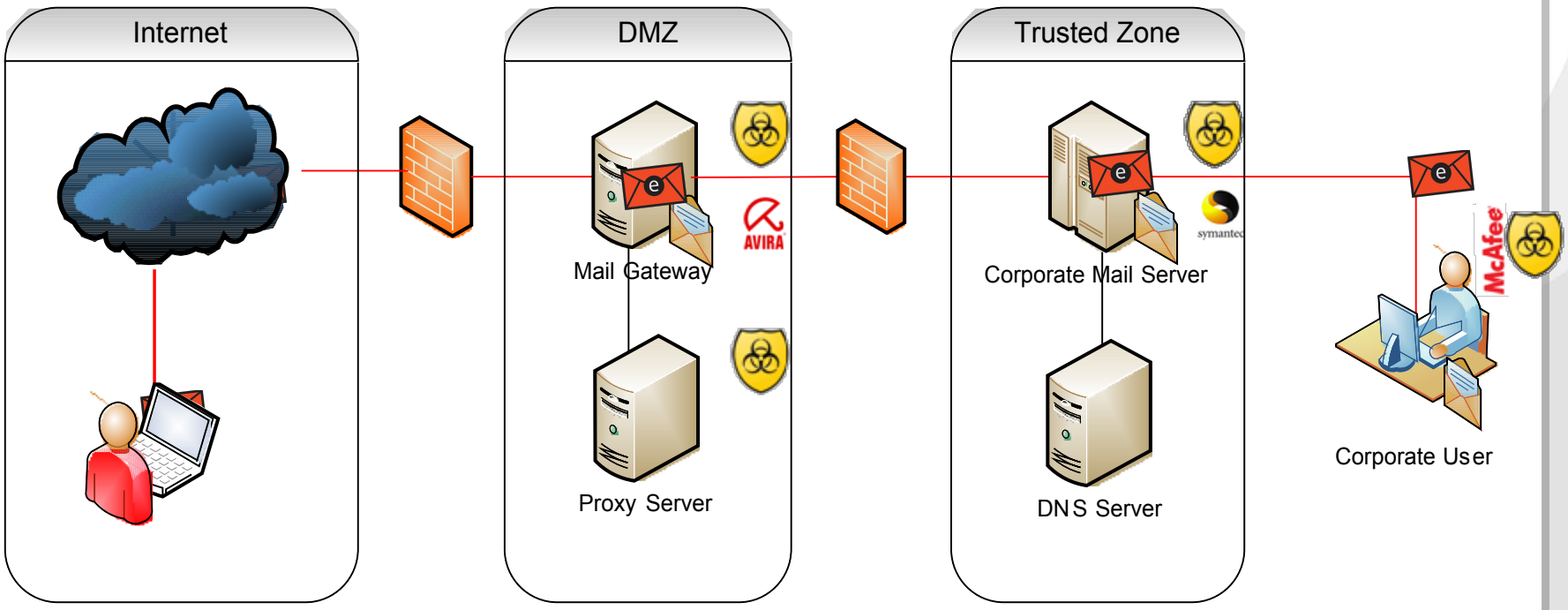
AV Vulnerabilities as related to Email traffic

- **Don't forget : AV Software runs also on your Email Architecture!**
  - > Gateway (MX)
  - > Corporate Mail Server (Real-time & Scheduled)
  - > Client
- Why does this change what is at stake?
  - > Email comes in from the outside
  - > Email travels through your internal network
  - > Email goes through your Firewalls

Oops, suddenly AV Vulnerabilities seem a lot more dangerous. What if non-trusted code gets executed on the Corporate Mail Server ?

Anti-Virus Software > Email

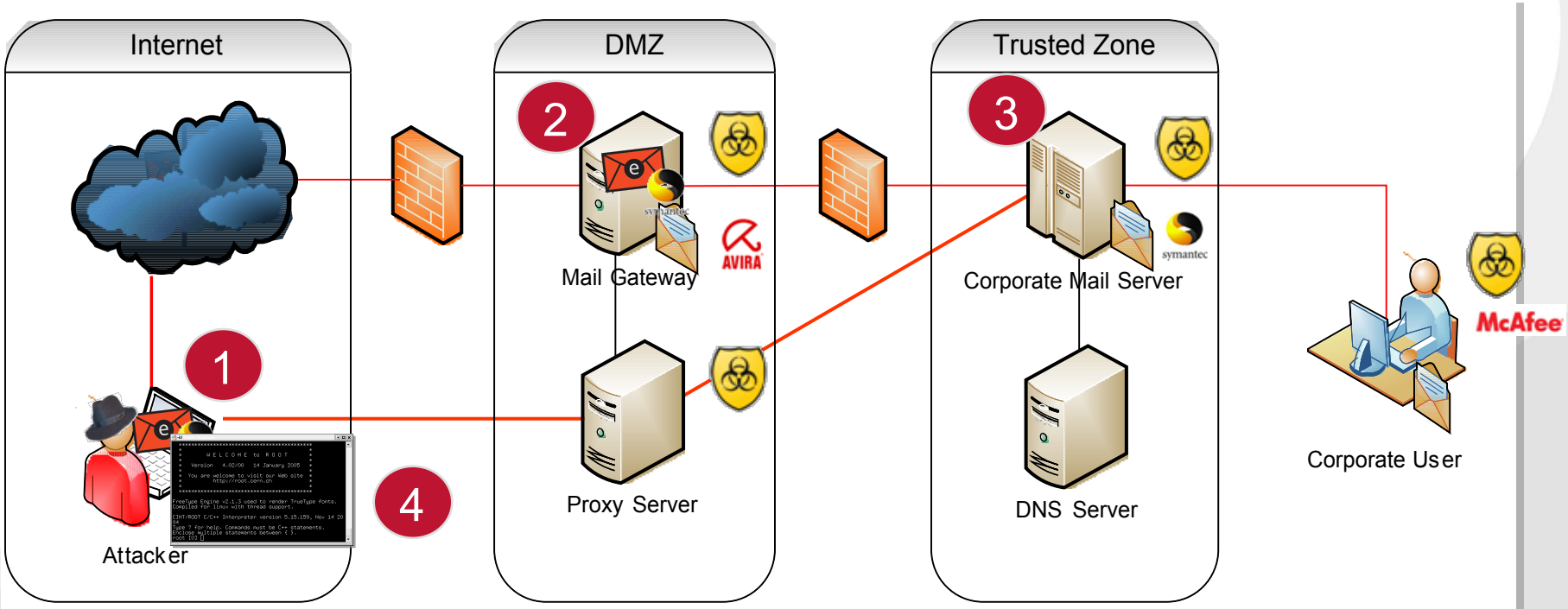
AV Vulnerabilities - Increase of Attack Surface



Multiple AV Engines, different vendors ->Increase of Attack surface
AV software running with privileged rights on critical parts of infrastructure.
Paradox: “The more you protect yourself the more vulnerable you become”

Anti-Virus Software > Email

Exploit Staging - Oversimplified



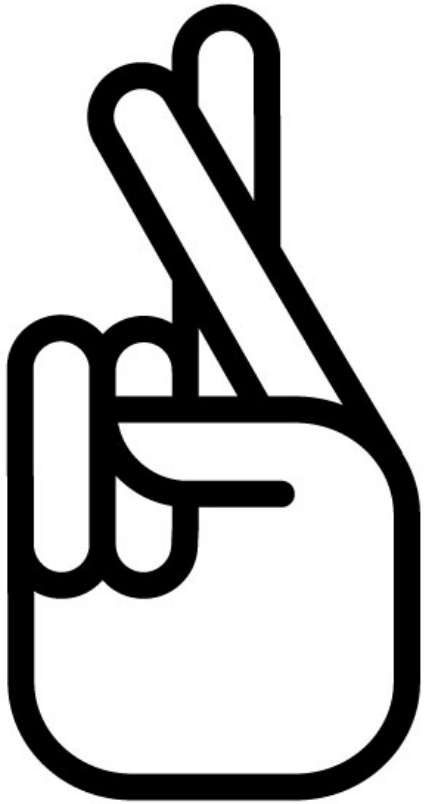
Oversimplification :

- Attacker sends an e-mail with a attachment targeting the Symantec Engine
- Avira on the Mail gateway does recognize a threat and the Mail is passed on
- The Attachment hits the Corporate Server where the exploit triggers
- Attacker gets a shell

nruns professionals

Demo

Demo



Final Words

- This is just the top of the iceberg
  - > IPSs/IDSs deal with +100 protocols
- Paradox
  - > “The **more** you **protect** yourself the **more vulnerable** you become”

Final Words

- n.runs opened a Pandora's Box
  - > There is no doubt things will get worse
  - > Lots of more bugs to come
- Before going public, n.runs looked for a Solution, there was no easy one, hence :

- n.runs is developing a secure system solution. The core of this solution is based on innovative architecture and software. The foundation for this development is based upon the years of consulting experience that n.runs has collected in IT security, infrastructure and processes.

- At this time the final tests are being performed. The market introduction begins in the 4th quarter of 2007.

Final Words

- The solution developed by n.runs under the code name "**ParsingSafe** " will build on and work **together with the customer antivirus products** that are already in place or that are planned to be put in place.
- Based on this, the **antivirus vendors are very important technology partners** for our solution. The goal of the customer is still primarily to have the highest rate of virus recognition possible but now embedded in a highly secure architecture that will prevent successful attacks on the AV products.

- **For more information, please contact:**

Torsten Pressel,

Director of Software Sales n.runs AG

Tel.: +49 6171 699-576

Email: parsingsafe@nruns.com

Web: http://www.nruns.com/ps

Final Words

Thank you for your Attention

Sergio Alvarez
Sergio.Alvarez@nruns.com

Thierry Zoller
Thierry.Zoller@nruns.com

References

- Vtrace, http://kenshoto.com/vtrace
- Paimei, http://code.google.com/p/paimei/
- n.bug, http://www.nruns.com/security_tools.php
- Peach Fuzzing Framework, http://peachfuzz.sourceforge.net
- SysInternals Tools, http://www.sysinternals.com
- Dum(b)ug, http://www.phenoelit-us.org/fr/tools.html
- Wireshark, http://www.wireshark.org
- Windows Debugging Tools, http://www.microsoft.com/whdc/devtools/debugging
- IDA Pro, http://www.hex-rays.com/idapro/
- OllyDbg, http://www.ollydbg.de