VF-Atak

Virus Flood Attack on Desktop Anti-Virus Programs

Lucijan Caric & Tomo Sombolac
2005, QUBIS d.o.o.
http://www.qubis.hr
qubis@qubis.hr

Urban legend

- On-access anti-virus program detects old and known viruses
- 99.99% an user error
- Bad or faulty definition
- Anti-virus program updating
- What about real-life?

Every man has his follies - and often they are the most interesting thing he has got.
(Josh Billings)

Birth of VF-Atak

- DoS probe
- How anti-virus programs behave under extreme load
- Remote attack

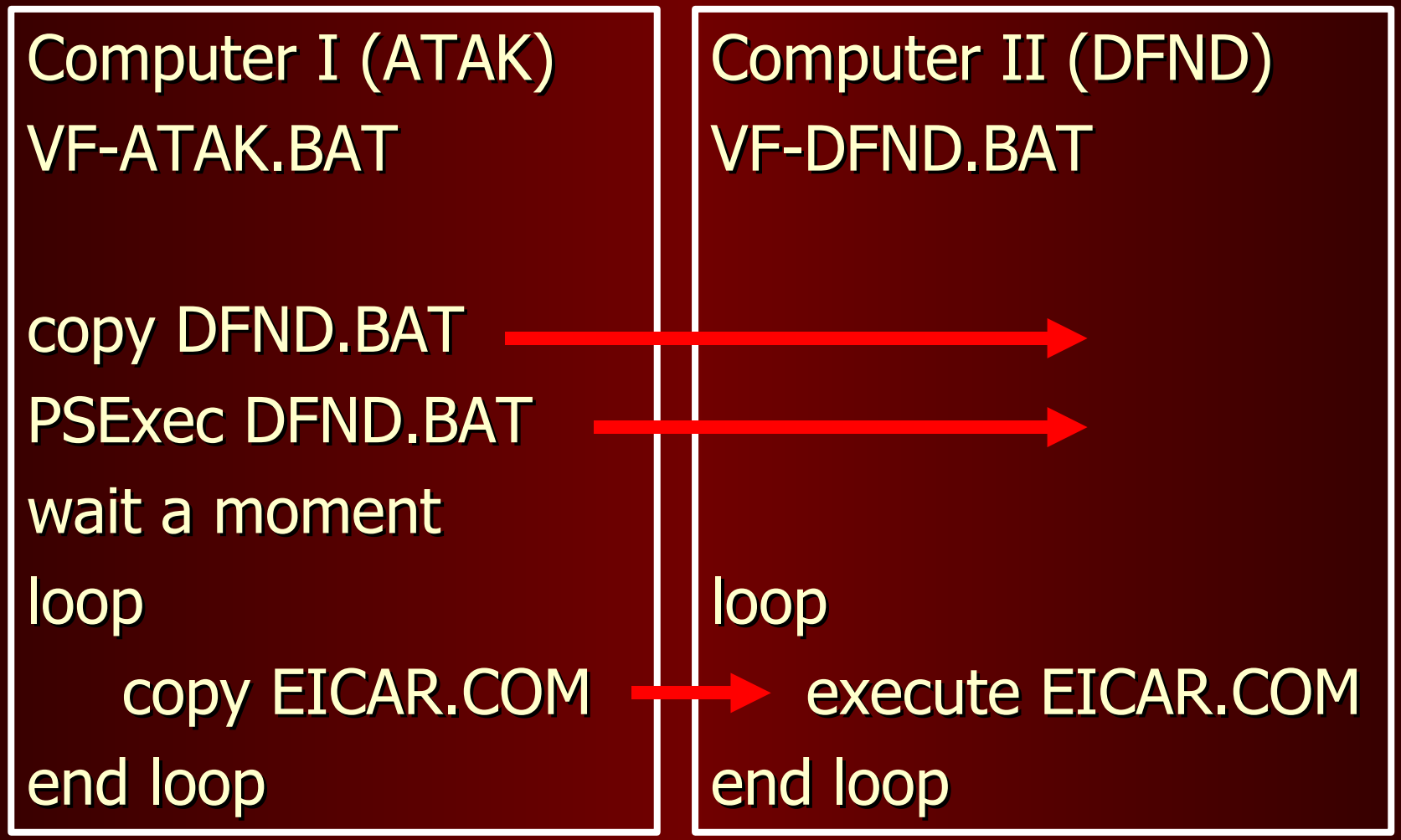
I must confess, I was born at a very early age.
(Groucho Marx)

So we decided to try

- Two computers
  - ATAcKer (ATAK)
  - DeFeNDer (DFND)
- Windows XP Pro
  - SP2
  - Fully patched
- AV: installed next-next
- Hardware – meet sys reqs

He who asks is a fool for five minutes, but he who does not ask remains a fool forever.
(Chinese proverb)

So we decided to try



I've got the brain of a four year old. I'll bet he was glad to be rid of it.
(Groucho Marx)

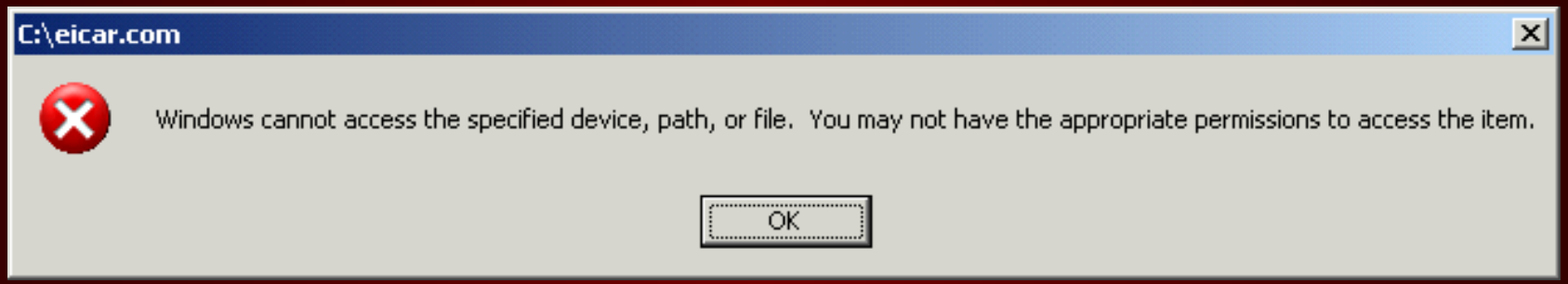
It works!

Access denied Access denied Access denied Bad Command or file name **EICAR-STANDARD-ANTIVIRUS-TEST-FILE!** Access denied Access denied Bad Command or file name Access denied Access denied Access denied Bad Command or file name...

Either he's dead or my watch has stopped.
(Groucho Marx)

Attack is not “smooth”

- Remote attack quite visible
- Local attack (trojan) faster and less visible



“Naughty” errors

General failure reading drive C

Abort, Retry, Fail?

Retry – same error / continue

Abort – continue attack

Fail – finish attack

Be warned

- Remote attack requires admin permission on defender
  - Is that really a problem?
- On-write scanning is safer
  - Could be default (resources?)
- Desktop alerting off

Testing

- 10.000 writes of EICAR.COM
  - Several times in a row
  - Two streams
- Clean OS image restored before each test

I remember the first time I had sex - I kept the receipt.
(Groucho Marx)

Anti-virus programs performance

- Rough calculation: 80% success
- Three AV consistently passing
  - Passed all trials
- One consistently failing
  - Failed all trials
- Other failing more or less often (more more than less)
- Some programs displayed erratic behaviour, DoS

A James Cagney love scene is one where he lets the other guy live.
(Bob Hope)

Anti-virus programs performance

- Time to complete the test: several minutes to two hours, some cancelled
- Many clicks, Enters, spaces, ...
- Sophisticated DoS test method: Start Notepad, qwe, File - Save
- AV menu accessibility during attack

I never forget a face, but in your case I'll be glad to make an exception.
(Groucho Marx)

Testing issues

- Consistency (proof of concept)
  - Number of passes/fails
  - "Seriousness" of fails
  - Performance over time
- No live viruses (Eicar)
- Batch script attack – slow
- Default AV configuration

I don't want to be a member of a club that would accept people like me for a member.
(Groucho Marx)

More testing issues

- Number of anti-virus programs tested (10 until now)
  - improvement
- Personal firewall
  - Circumvented with “split-virus”
- Anti-virus programs must not upgrade during test

...
(Groucho Marx)

Evolution of VF-ATAK

- Simple
- Multi-stream
- "Split-virus"
- One computer only
- Could be written in VB, Java, C, ... and performed from Internet

My mother buried three husbands - and two of them were only napping.
(Rita Rudner)

What VF-Atak means?

- This is not a test, but *proof of a concept*
- Method is simple, but could be improved
- It seems that a number of applications is affected
- Tells about performance
- Could pose a risk and could be exploited

A black cat crossing your path signifies that the animal is going somewhere.
(Groucho Marx)

What Microsoft thinks?

- "...If I understand correctly, this exploit requires the attacker to already have administrative privileges on the victim's machine. **If that is the case, the attacker already has full control of the system, would not need to use this particular vector, and could already cause any amount of damage.** ... but that does not make a vulnerability..."
- True, BUT... XP Security Center and other monitors stays silent on failed AV

You don't pay taxes - they take taxes.
(Chris Rock)

What Microsoft thinks?

- "...I believe I understand your methodology for non-administrative exploits. It seems to me, however, that it still requires a user to run code. If a user chooses to run code, that application or script can take any action the user is authorized to do. This ... is one of the reasons why we recommend running software only from trusted sources. **Trojan horses that attempt to run code are common and one of the reasons our email software blocks executable attachments**. In the event your exploit code is put on a machine through a dropper of some sort, that dropper may be exploiting a vulnerability, but would not be the vulnerability itself..."
- ActiveX, Java, VB, ...

Age is an issue of mind over matter. If you don't mind, it doesn't matter.
(Mark Twain)

What do we think?

- This is most probably a problem of integration between the anti-virus program and Windows OS
- Could it be a problem of quality control?
- Anti-virus companies should test and remedy the issue themselves
- The AV denial phase in progress:
  - AV1: "...an Eicar issue..."
  - AV2: "...did not test ... but doesn't work..."
  - AV3: "...did we fail?..."
  - AVx: "Retry? Ignore!"

Those are my principles, and if you don't like them... well, I have others.
(Groucho Marx)

VF-Atak

Virus Flood Attack on Desktop Anti-Virus Programs

Lucijan Caric & Tomo Sombolac
2005, QUBIS d.o.o.
http://www.qubis.hr
qubis@qubis.hr

I have two messages – one is bad, but the other one is worse.
(Dubravko Matakovic)