VF-Atak

Virus Flood Attack on Desktop Anti-Virus Programs

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

Urban legend

- On-access anti-virus program failed to stop (detect) an old and already known virus
  - 99.99% an user error
  - Definition or engine problem
  - Anti-virus program updating
- If problem exists window of opportunity is very short

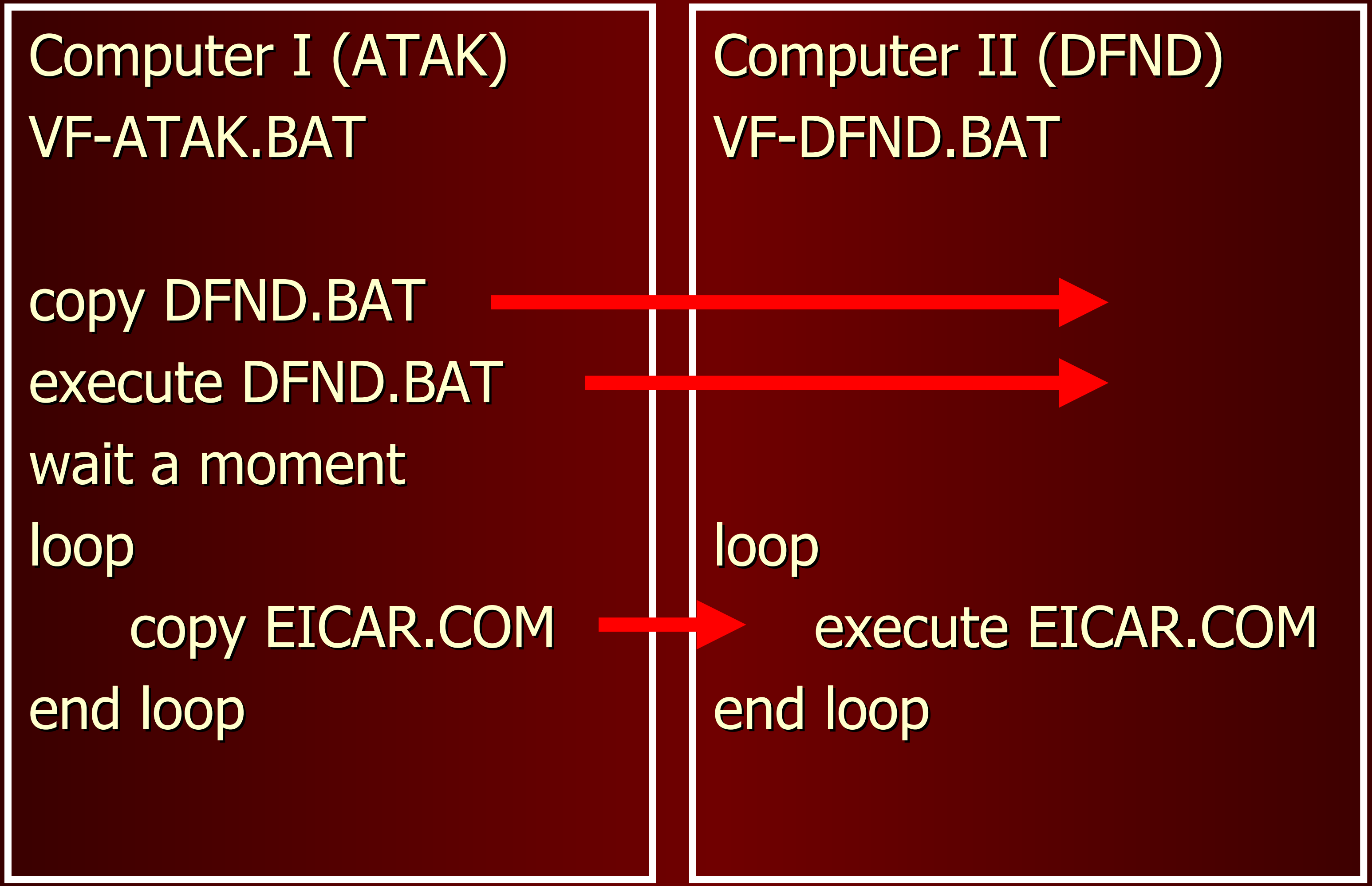
Birth of VF-Atak

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

So we decided to try

- Two computers
  - ATAcKer
  - DeFeNDer
- Windows XP Professional
  - SP2
  - Fully patched with latest patches

So we decided to try



Computer I (ATAK)

VF-ATAK.BAT

```
copy DFND.BAT
execute DFND.BAT
wait a moment
loop
    copy EICAR.COM
end loop
```

Computer II (DFND)

VF-DFND.BAT

```
loop
    execute EICAR.COM
end loop
```

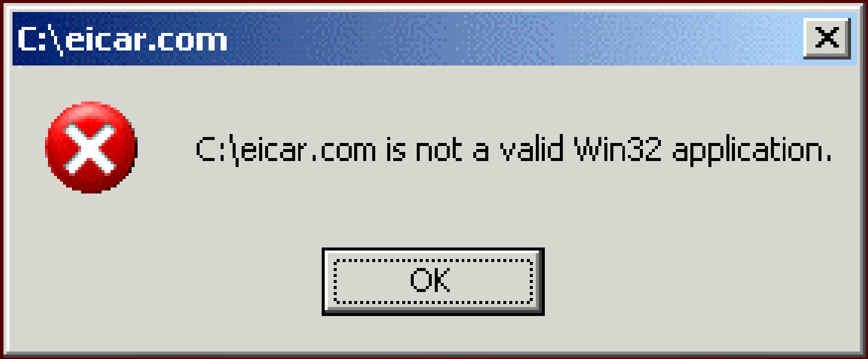
VF-Atak (Caric & Sombolac, QUBIS d.o.o.)

WWW.QUBIS.HR

Oops – it works!

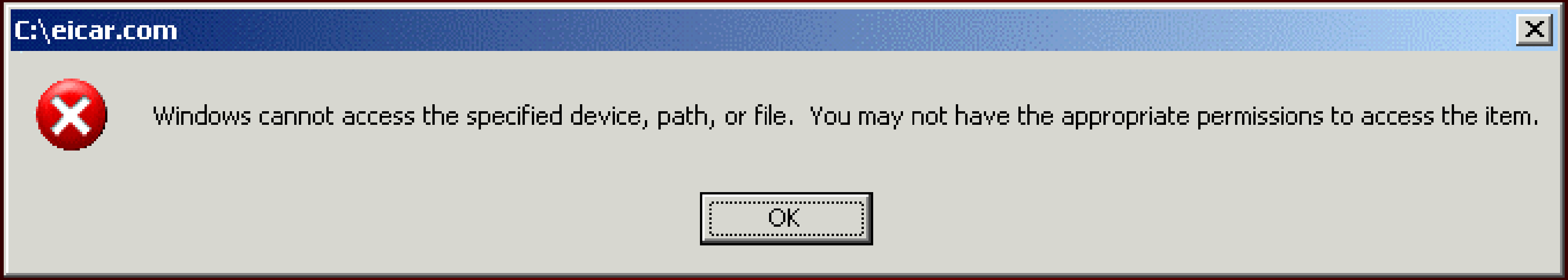
Access denied Access denied Access denied Access denied Access denied Access denied Access denied Access denied Access denied Bad Command or file name EICAR-STANDARD-ANTIVIRUS-TEST-FILE!Access denied Access denied Bad Command or file name Access denied Access denied Access denied Access denied Access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

Attack was not "smooth"



C:\eicar.com

C:\eicar.com is not a valid Win32 application.



C:\eicar.com

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

VF-Atak (Caric & Sombolac, QUBIS d.o.o.)

WWW.QUBIS.HR

“Naughty” errors

General failure reading drive C

Abort, Retry, Fail?

Retry – same error again

Abort – continue attack

Fail – end script

Be warned

- Attack requires attacker to have administrative rights on defender computer
  - Is that a *problem* at all?
  - Not required for “standalone” version
- Desktop alerting set to off

Testing

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

VF-Atak (Caric & Sombolac, QUBIS d.o.o.)

WWW.QUBIS.HR

Anti-virus programs performance

- One consistently passing
  - Passed all trials
- One consistently failing
  - Failed all trials
- Other failing more or less often
- Some programs displayed erratic behaviour

Anti-virus programs performance

- Time to complete the test was from several minutes to two hours
- From one to several hundred infections

VF-Atak (Caric & Sombolac, QUBIS d.o.o.)

WWW.QUBIS.HR

Testing issues

- Consistency
  - Number of passes/fails
  - “Seriousness” of fails
  - Performance over time
- No live viruses
- Use of Command Prompt
- .COM executable
  - Not a true Windows application
  - File size

More testing issues

- Each anti-virus program unique
- Default program configuration
- Number of anti-virus programs used
- Personal firewall
  - Circumvented with modified, “binary” attack
- Anti-virus programs should not upgrade during test

Evolution of ATAKs

- Simple
- Multi-stream
- Binary
- One computer only
- Could be written in script, Java, C, etc.
- Web/Internet based attack

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 something about performance
- Could pose a risk and could be exploited

VF-Atak (Caric & Sombolac, QUBIS d.o.o.)

WWW.QUBIS.HR

What Microsoft thinks?

I have reviewed your paper and noticed it says, "Everything was done under administrative account to simulate real world - too many desktop users already work under power or admin rights. Also, virus writers are quite capable of finding a way to elevate privileges." 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. I agree too many users run with administrative privileges, but that does not make a vulnerability. Also, if an attacker has some other method of elevating privileges, then that may constitute a vulnerability and we would investigate that vector separately.

VF-Atak (Caric & Sombolac, QUBIS d.o.o.)

WWW.QUBIS.HR

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 also mentioned in the essay to which I linked yesterday, and 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.

What do we think?

- This is most probably a problem of integration of the anti-virus program and Microsoft OS
- Also, it could be a problem of quality control
- Anti-virus companies should test and remedy the issue

What do you think?

VF-Atak (Caric & Sombolac, QUBIS d.o.o.)

WWW.QUBIS.HR

VF-Atak

Virus Flood Attack on Desktop Anti-Virus Programs

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