SOPHOS

Multi-Component Malware - How To Name, Share and Report It

Sean McDonald
Virus Researcher

Nick FitzGerald
Independent Antivirus Consultant

www.sophos.com

Ancient History

SOPHOS

- Win32/Ska (aka Happy99)
  - early self e-mailing virus
  - early multi-component virus
- Arrives as e-mail attachment Happy99.exe
- Copies itself to system directory as SKA.EXE
- Drops SKA.DLL in system directory
- Patches WSock32.DLL to call SKA.DLL
- Win32/Ska replicates as user sends e-mail, posts to USENET News

Recent History

SOPHOS

- JS/Flea.A (aka JS/Fortnight.D)
  - e-mail-using virus
  - multi-component virus
- Arrives embedded in HTML e-mail message
- <IFRAME> tag grabs HTML from remote server
- Script in HTML executes
  - IE security flaw provides elevated privileges
  - script alters registry, drops files
- JS/Flea replicates as user sends e-mail

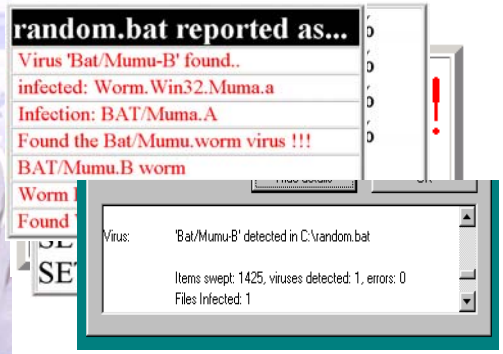
Reporting Problem

SOPHOS

File	Reported as...
muma.bat	Found Virus [BAT_MUMU.A] (1)
ipcpass.txt	Found Virus [BAT_MUMU.A] (1)
start.bat	Found Virus [BAT_MUMU.A] (1)
psexec.exe	
random.bat	Found Virus [BAT_MUMU.A] (1)
nwize.ini	

A Real Virus (apparently)

SOPHOS



How Big A Problem Is this

SOPHOS

- How could a single component or just a few end up on a system anyway?
  - using multiple scanners
  - switching scanner
  - using antivirus software for the first time
  - incomplete replication

Incorporating Context

SOPHOS

- Incorporate context to determine whether execution is possible
- Look at all factors that help achieve this objective:
  - number of components present
  - functionality of only those components present
  - can components communicate
  - correct operating systems
  - required registry entries

Difficulties Incorporating Context

SOPHOS

- Where should context be considered? Consider the following:
  - scanning network drives
  - scanning e-mail at the gateway
  - memory-borne virus in tcpdump data
- Boot sector in a file
- Archives
- Base64 encoding outside MIME boundaries

Benefits Incorporating Context

SOPHOS

- Infection statistics would be more accurate
- Consider what “currently” running and “not runnable” mean to the user
- What does the user have to do if one thinks the malware is active:
  - disconnect machines from network
  - replace deleted files
  - call support for help
  - perform security audit

Benefits Incorporating Context - Cont.

SOPHOS

- What does the same user have to do if the malware is believed to be not running:
  - delete malware files
  - possibly check for signs of previous infection
- What if the malware is not relevant to the machine:
  - delete malware files
  - possibly advise others

Using States

SOPHOS

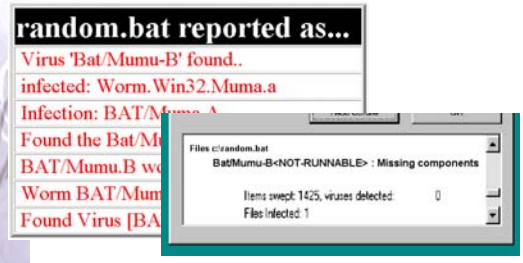
- States can be used to convey the results of incorporating context into reports
- Basic states might be:

ACTIVE	currently executing in memory
DORMANT	not executing however no reason why not
NOT-RUNNABLE	not executing and cannot execute in current climate

Using States - Cont.

SOPHOS

- The states reported could be followed by a descriptive reason:



To Finish…

SOPHOS

- Please contact us and let us know:
  - whether anything suggested has merit
  - why it does not
  - suggestions of your own
  - whether you are interested in furthering the matter
- nick@virus-l.demon.co.uk
- sean.mcdonald@sophos.com.au