Heureka!

The suspicious thing is that it's not suspicious

#define BUHERATOR

- void* S2
- bPenTester
- bBlogger
- rgdwYear[2013] = AV || TEST || BREAK
- !bCppCoder && !bWindowsCoder

  // Trying to change that though :)

#include "past.h"

- *"Unfortunately, the general problem of discerning between viral and non-viral programs is unsolvable." – Symantec*
- AV-comparatives 2013 March
  - Real World Protection Test: 90.3% - 100% success
  - Heuristic Behavioural Tests: 66.4% - 97.5% success
- **A**verage **P**oisonIvy **T**hreats
  - Yes, you can still pwn with off-the-shelf RATs…
  - See FireEye's PIVY report
  - .. and the great counterpwnage by malware.lu&itrust

virustotal

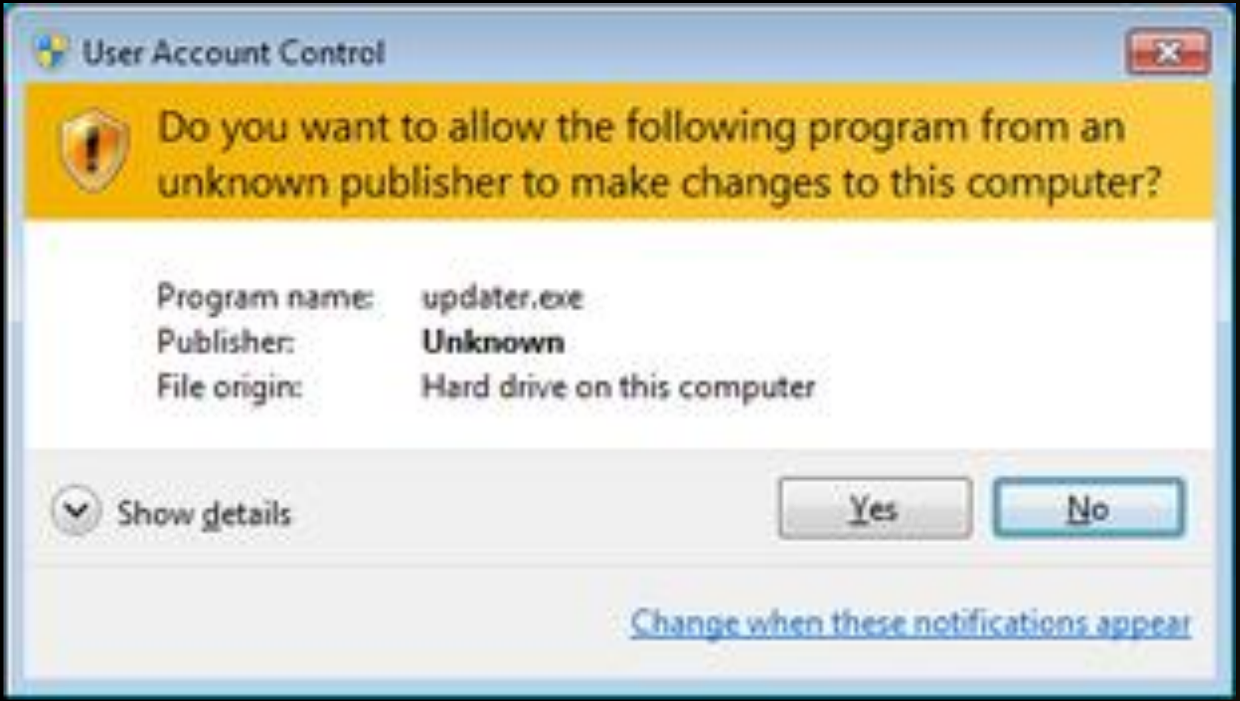
"VirusTotal AV engines are commandline versions, so depending on the product, they will not behave quite like the desktop versions: for instance, in such cases when ***desktop solutions use techniques based on behavioral analysis and count on personal firewalls that may decrease entry points and mitigate propagation, etc.****"*

http://blog.virustotal.com/2012/08/av-comparative-analyses-marketing-and.html

#define HEUREKA

- A toolset to assess the behavioral capabilities of AV/HIPS software
- Target audience:
  1. AV customers
  2. AV vendors
  3. AV hackers
  4. Pentesters tend to start writing malware
     - Gunter Ollman - Penetration Testing With Honest-To-Goodness Malware (VB2013)
     - Alberto Garcia Illera – Enterprise Malware (Infiltrate2013)
     - Dr. Markku-Juhani O. Saarinen – Developing a Grey Hat C2 and RAT for APT Security Training and Assessment (GreHack2013)
     - Stephan Chenette - Building Custom Android Malware for Penetration Testing (BruCON2013)

#define THREAT_MODEL



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: updater.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

#define DESIGN_GOALS

- An open toolset to assess the behavioral capabilities of AV/HIPS software
- "Modular" design
  - Different needs => different solutions
- Single executable
  + optional standalone components

Autonomous binaries with unique functionality

#define HEUREKA

- 32-bit Windows PE executable
- C++ (Visual Studio)
- KISS
  - – 1 function/Task
  - – Configuration with a single .h file
    - Preprocessor directives (#define, #if …)
    - Unwanted functionality doesn't get into the compiler

#define FEATURES

- Network communication - HTTP
- File access
- Registry access
- *Other*

Mostly sufficient

#define FEATURES

- **Network communication – HTTP**
  - Shellcode
  - Download & Execute
  - Leak information
- **File access**
  - Look for sensitive data
  - Hosts file hijack
  - Logging
- **Registry access**
  - Autorun
  - DLL injection
- ***Other***
  - DLL injection
    - Man-in-the-Browser
    - Download&Execute
  - API hooking
    - Keylogging

TEST RESULTS

Candidates

- **"Free" Tier (as in free beer)**
  - Avast
  - AVG
- **Newcomer Tier**
  - Emsisoft
  - G Data
  - Threatfire (Aquired by Symantec)
- **Hotshot Tier**
  - ESET
  - F-Secure
  - Kaspersky
  - Symantec

My poor excuse for demo effects

AV is non-deterministic :(

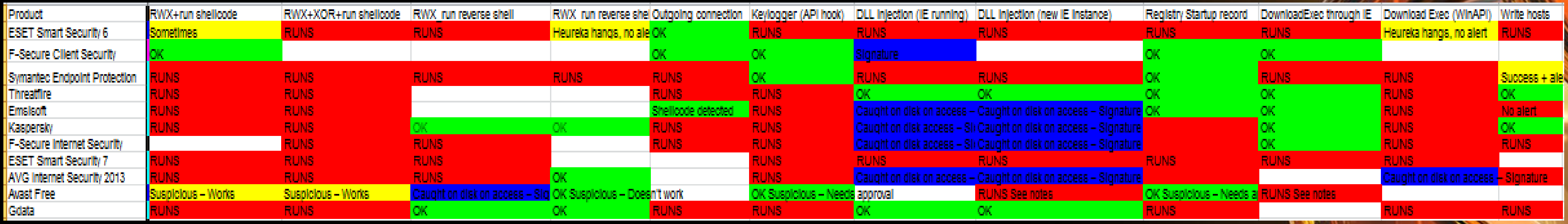
Expectations vs. Reality

- Task 1: Set automatic startup in Registry
- Task 2: Write new domain-IP record to the hosts file

Expectations vs. Reality

- Task 1: Set automatic startup in Registry
  - Caugth by 4/10 products
- Task 2: Write new domain-IP record to the hosts file
  - Caught by 4/10 products
- Both
  - Caugth by 3/10 products

Test results - in Excel!



Product	RWX+run shellcode	RWX+XOR+run shellcode	RWX_run reverse shell	RWX run reverse she	Outgoing connection	Keylogger (API hook)	DLL Injection (IE running)	DLL Injection (new IE instance)	Registry Startup record	DownloadExec through IE	Download Exec (WinAPI)	Write hosts
ESET Smart Security 6	Sometimes	RUNS	RUNS	Heureka hangs, no ale	OK	RUNS	RUNS	RUNS	RUNS	RUNS	Heureka hangs, no alert	RUNS
F-Secure Client Security	OK				OK	OK	Signature		OK	OK		
Symantec Endpoint Protection	RUNS	RUNS	RUNS	RUNS	RUNS	OK	RUNS	RUNS	OK	RUNS	RUNS	Success + ale
Threatfire	RUNS	RUNS			RUNS	RUNS	OK	OK	OK	OK	RUNS	OK
Emsisoft	RUNS	RUNS			Shellcode detected	RUNS	Caught on disk on access –	Caught on disk on access – Signature	OK	OK	RUNS	No alert
Kaspersky	RUNS	RUNS	OK	OK	RUNS	RUNS	Caught on disk access – Sh	Caught on disk on access – Signature		OK	RUNS	OK
F-Secure Internet Security		RUNS	RUNS		RUNS	RUNS	Caught on disk access – Sh	Caught on disk on access – Signature		OK	RUNS	RUNS
ESET Smart Security 7	RUNS	RUNS	RUNS			RUNS	RUNS	RUNS	RUNS	RUNS	RUNS	
AVG Internet Security 2013	RUNS	RUNS	RUNS	OK		RUNS	Caught on disk on access –	Caught on disk on access – Signature			Caught on disk on access – Signature	
Avast Free	Suspicious – Works	Suspicious – Works	Caught on disk on access – Sig	OK Suspicious – Doesn't work		OK Suspicious – Needs approval		RUNS See notes	OK Suspicious – Needs a	RUNS See notes		
Gdata	RUNS	RUNS	OK	OK	RUNS	RUNS	OK	OK	RUNS		RUNS	RUNS

A few words about scoring

"… an IDS should not view the task of detecting misuse as a binary decision problem, i.e. >>saw an attack<< vs. >>did not see an attack<<. It should be recognized that different forms of attack technique are not equally complex and consequently not equally complex to detect; succinctly, the intrusion detection problem is not a binary (discrete), but rather an n-valued (variable) problem."

– lifeline & sasha, Phrack #56 – 2000.

DEMO TIME!

Set Autostart in Registry

- "I want to load every time you log in"
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Harmless programs do this
  - We can't whitelist them
  - An alert would be nice though

Download and Execute

- "Let's grab the real/most-recent payload"
  - See also ALLOC_RWX
- Harmless programs do this
  - We have application-aware host-based firewalls!

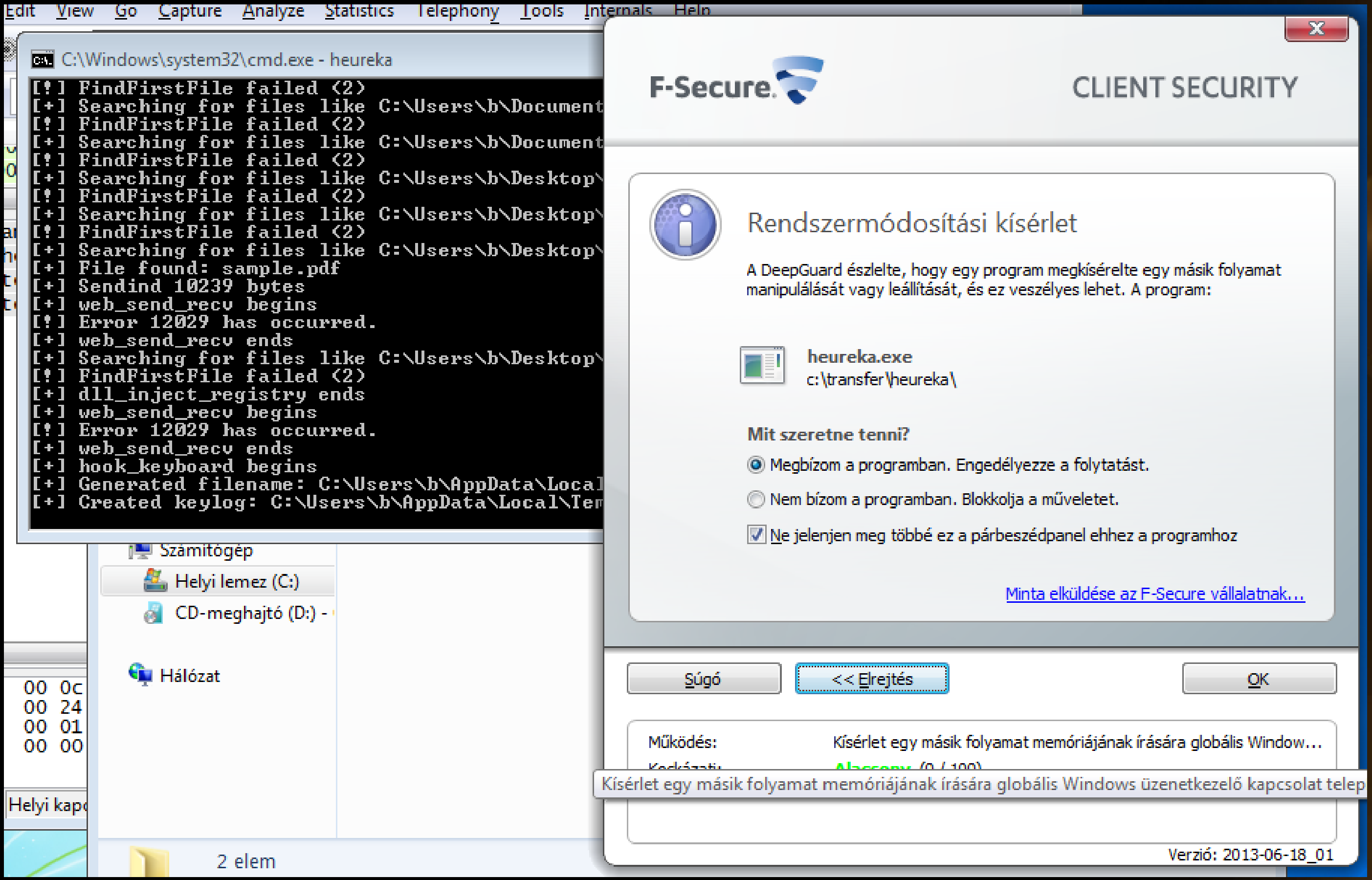
Write to hosts file

- "Let's hijack some hostnames!"
- Harmless programs don't do this very often
  - Say hello to the warez teams though!
- Requires administrative privileges
  - Think XP…
- Sounds trivial to detect

Hook the Low-Level Keyboard API

- Other purpose than keylogging?
- Limited with user privileges
  - Snooping into the winlogon process requires SYSTEM
  - User level is usually good enough
  - See also Brett More @ Ruxcon 2011, mubix @ DerbyCon 2013

#fail – Can't reproduce :(



```
[!] FindFirstFile failed (2)
[+] Searching for files like C:\Users\b\Document
[!] FindFirstFile failed (2)
[+] Searching for files like C:\Users\b\Document
[!] FindFirstFile failed (2)
[+] Searching for files like C:\Users\b\Desktop\
[!] FindFirstFile failed (2)
[+] Searching for files like C:\Users\b\Desktop\
[!] FindFirstFile failed (2)
[+] Searching for files like C:\Users\b\Desktop\
[+] File found: sample.pdf
[+] Sendind 10239 bytes
[+] web_send_recv begins
[!] Error 12029 has occurred.
[+] web_send_recv ends
[+] Searching for files like C:\Users\b\Desktop\
[!] FindFirstFile failed (2)
[+] dll_inject_registry ends
[+] web_send_recv begins
[!] Error 12029 has occurred.
[+] web_send_recv ends
[+] hook_keyboard begins
[+] Generated filename: C:\Users\b\AppData\Local
[+] Created keylog: C:\Users\b\AppData\Local\Tem
```

```
00 0c
00 24
00 01
00 00
```

Rendszermódosítási kísérlet

A DeepGuard észlelte, hogy egy program megkísérelte egy másik folyamat manipulálását vagy leállítását, és ez veszélyes lehet. A program:

heureka.exe
c:\transfer\heureka\

Mit szeretne tenni?

● Megbízom a programban. Engedélyezze a folytatást.

○ Nem bízom a programban. Blokkolja a műveletet.

☑ Ne jelenjen meg többé ez a párbeszédpanel ehhez a programhoz

Minta elküldése az F-Secure vállalatnak...

Működés: Kísérlet egy másik folyamat memóriájának írására globális Window...

Kockázati: Alacsony (0 / 100)

Kísérlet egy másik folyamat memóriájának írására globális Windows üzenetkezelő kapcsolat telep

Verzió: 2013-06-18_01

DLL injection (in-memory)

- Man-in-the-Browser malware
- Firewall bypass
- Security software do this
- The devil is in the details
  - Target process?
  - Existing vs. New?

Vendor reactions?

ping timed out :(

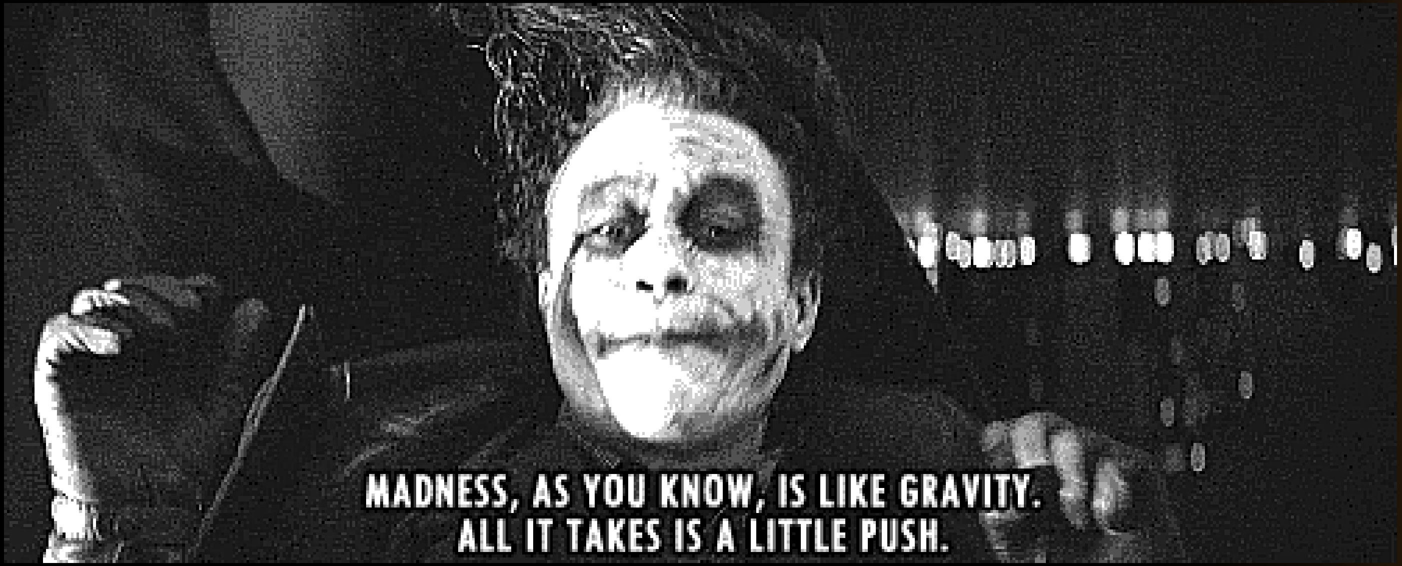
Anyway, thank you for the cooperation:
ESET (HU)
Symantec (HU)
G-Data (HU)
F-Secure (FI)

Conclusion?

- The time of democratic security systems is over
- Let's build police states!
  - Reputation databases
  - Trained whitelists
- Learn from other police states!

The Call for Arms

- Lots of Tasks to implement
  - Privilege escalation
  - Virtualization detection
  - Anti-AV techniques
- Testing, testing, testing
  - New Task => Many new test cases
- Encourage vendor cooperation
- Fully automated testing?
- Architectural redesign?


MADNESS, AS YOU KNOW, IS LIKE GRAVITY.
ALL IT TAKES IS A LITTLE PUSH.

http://git.io/heureka

Questions?

Come out and play!

buherator@silentsignal.eu

http://silentsignal.eu

http://buhera.blog.hu

@buherablog

Greetz: S2crew, hekkcamp, CampZer0, GCS

Links

- https://www.symantec.com/avcenter/reference/heuristc.pdf
- https://www.sans.org/reading_room/whitepapers/malicious/about-heuristics_141
- http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf
- http://www.wired.com/threatlevel/2012/06/internet-security-fail/
- http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- http://phrack.org/issues.html?issue=56&id=12#article
- http://www.slideshare.net/mubix/windows-attacks-at-is-the-new-black-26665607
- Encyclopaedia Of Windows Privilege Escalation - https://www.youtube.com/watch?v=kMG8IsCohHA