January, 2009

Malware Hash Registry

Harnessing the power of AntiVirus Aggregation

TEAM CYMRU
www.team-cymru.org

Stephen Gill
Chief Scientist
Team Cymru

© 2008 Team Cymru

Agenda

- Introduction
- Purpose
- Access
- Usage, Tools, Applications
- Statistics
- Looking to the Future
- Conclusion

© 2008 Team Cymru

Jeopardy: Who is “Team Cymru”?

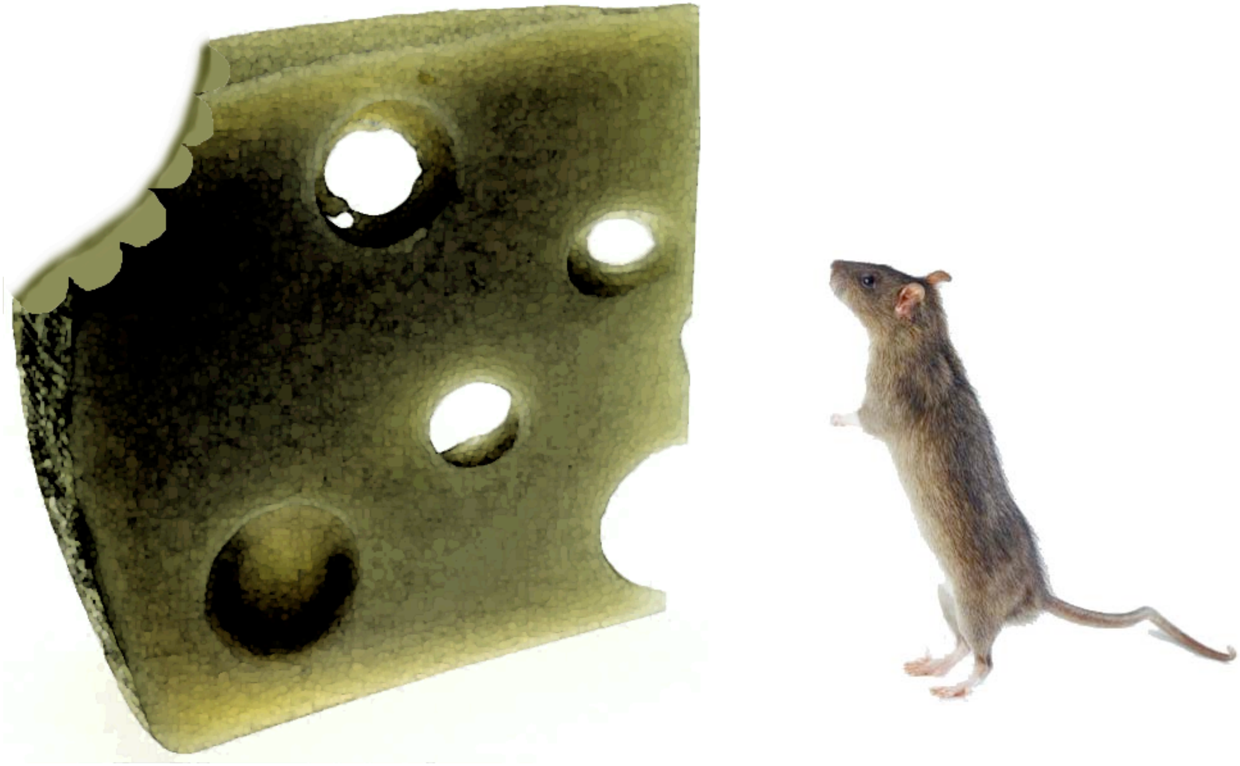
- Began as a hobby in 1998; Incorporated in 2004.
- Network of researchers dedicated to supporting the Internet community in maintaining security; non-profit
- Funded by multinational banks, CERTs/CSIRTS, security vendors… and you?
- Global investigators previously from Dutch NHTCC, UK Scotland Yard, Polish Police, USSS
- Our Mission: The WHO and the WHY

© 2008 Team Cymru

The Internet

© 2008 Team Cymru

Malware's Effect on the Internet



© 2008 Team Cymru

Malware

- Samples Skyrocketing: one new virus every 2 seconds
- Vectors:
  - people
  - mobile viruses
  - Drive By downloads
  - file infectors (ie virut)
  - USB drives. spreading like wildfire in AsiaPac
  - Office programs
  - Middle man: arp poisoning

© 2008 Team Cymru

Enter, the Malware Hash Registry

- In a nutshell: query our service for a computed MD5 or SHA-1 hash of a file
  - if it is known malware we display an AV detection Rate and last seen timestamp
- Similar to IP to ASN released several years ago:
  - http://www.team-cymru.org/Services/ip-to-asn.html
  - Translates Ips to BGP ASNs via Whois and HTTP
  - Highly successful

© 2008 Team Cymru

Enter, the Malware Hash Registry

- Complements AV extremely well.
  - Maintaining Hashes in signatures is impractical (1 (1GB+ size)
  - We take care of that by storing it in the cloud
  - Lets AV continue to do what it does best: detect malware based on signatures and heuristics.
- Free for non-commercial use

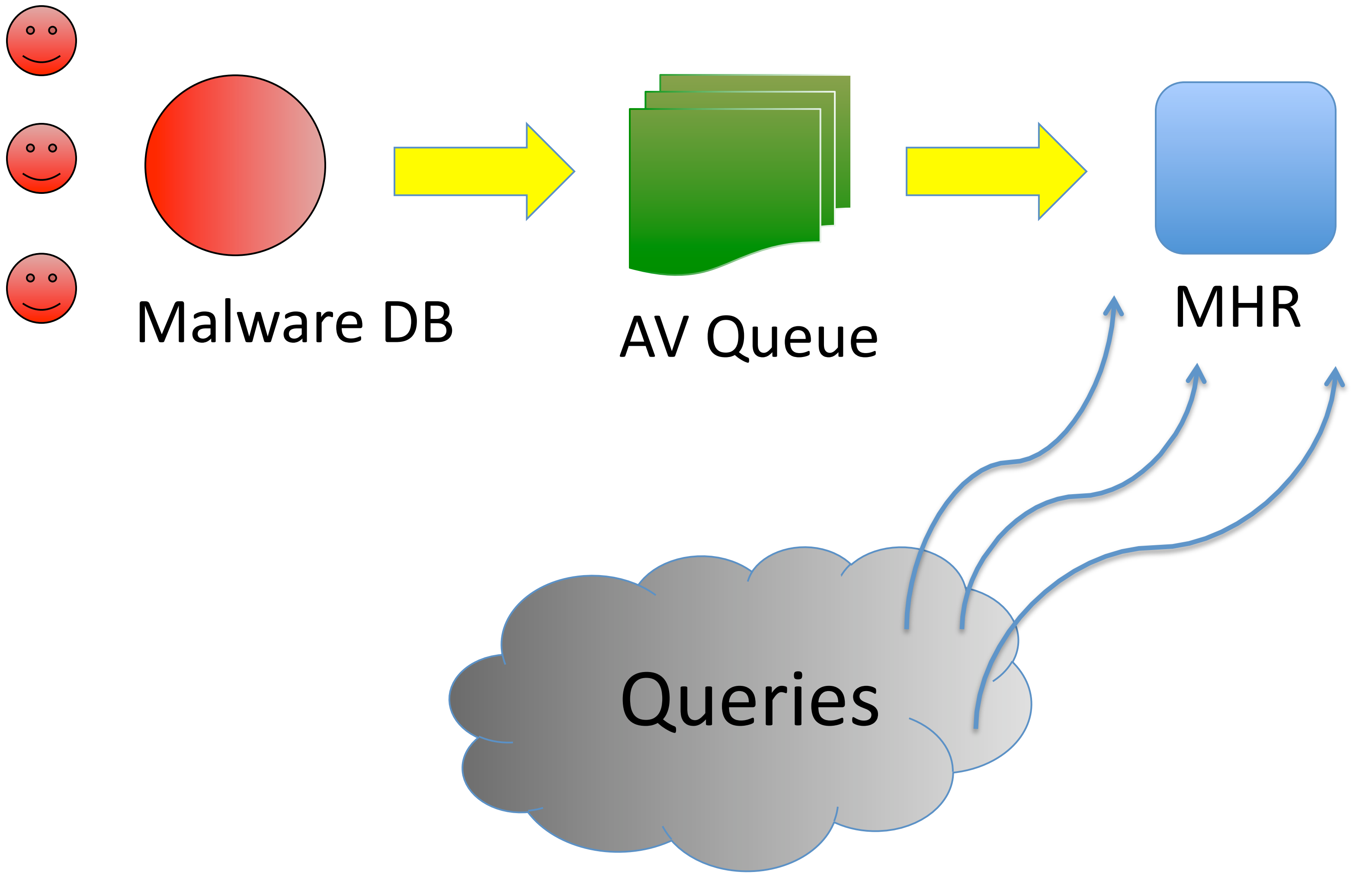
Access Methods

- Access is available over the Internet via:
  - Whois: TCP 43
  - Netcat: TCP 43 (bulk whois)
  - DNS: UDP 53

- Possibly coming later:
  - Instant Messaging
  - HTTP
  - Your ideas here …

© 2008 Team Cymru

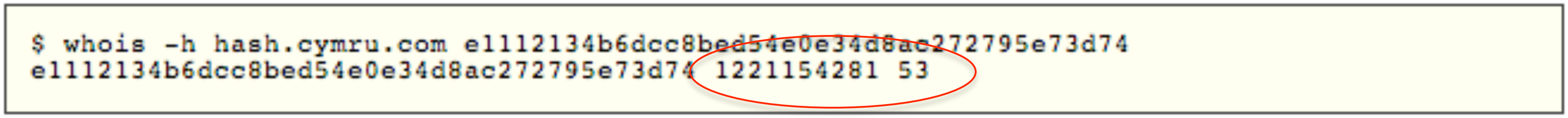
Architecture



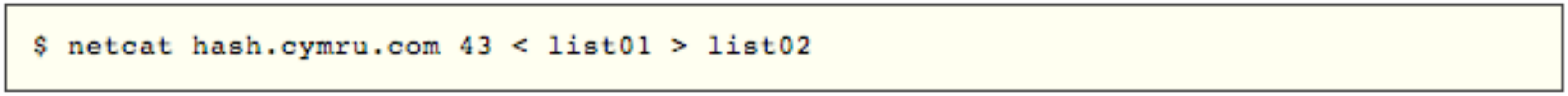
© 2008 Team Cymru

Usage

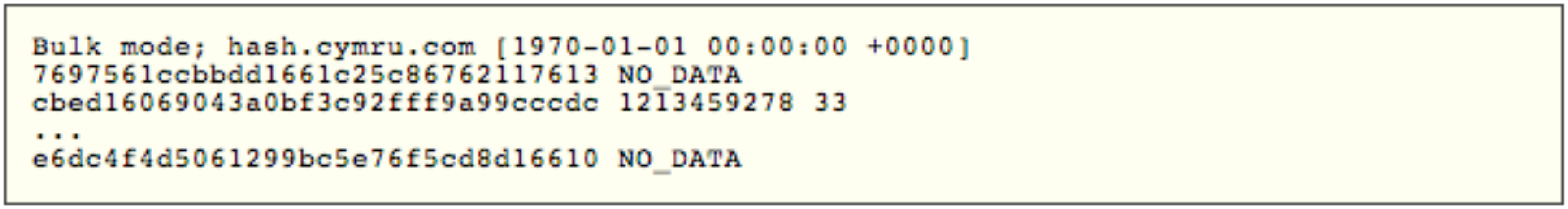
- Whois & Netcat



```
$ whois -h hash.cymru.com e1112134b6dcc8bed54e0e34d8ac272795e73d74
e1112134b6dcc8bed54e0e34d8ac272795e73d74 1221154281 53
```

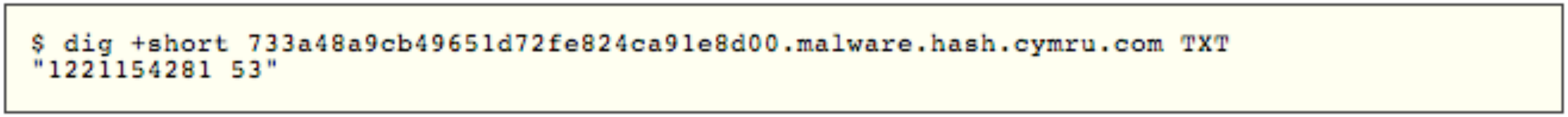


```
$ netcat hash.cymru.com 43 < list01 > list02
```

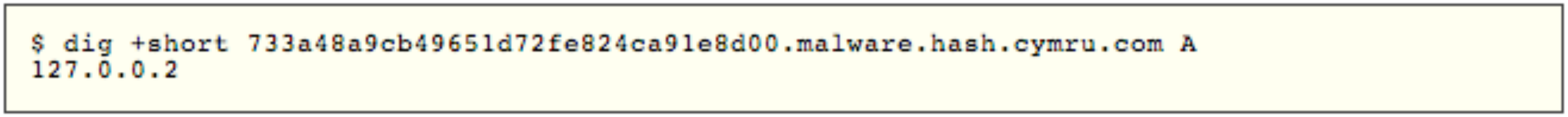


```
Bulk mode; hash.cymru.com [1970-01-01 00:00:00 +0000]
7697561ccbbdd1661c25c86762117613 NO_DATA
cbed16069043a0bf3c92fff9a99cccdc 1213459278 33
...
e6dc4f4d5061299bc5e76f5cd8d16610 NO_DATA
```

- DNS



```
$ dig +short 733a48a9cb49651d72fe824ca91e8d00.malware.hash.cymru.com TXT
"1221154281 53"
```



```
$ dig +short 733a48a9cb49651d72fe824ca91e8d00.malware.hash.cymru.com A
127.0.0.2
```

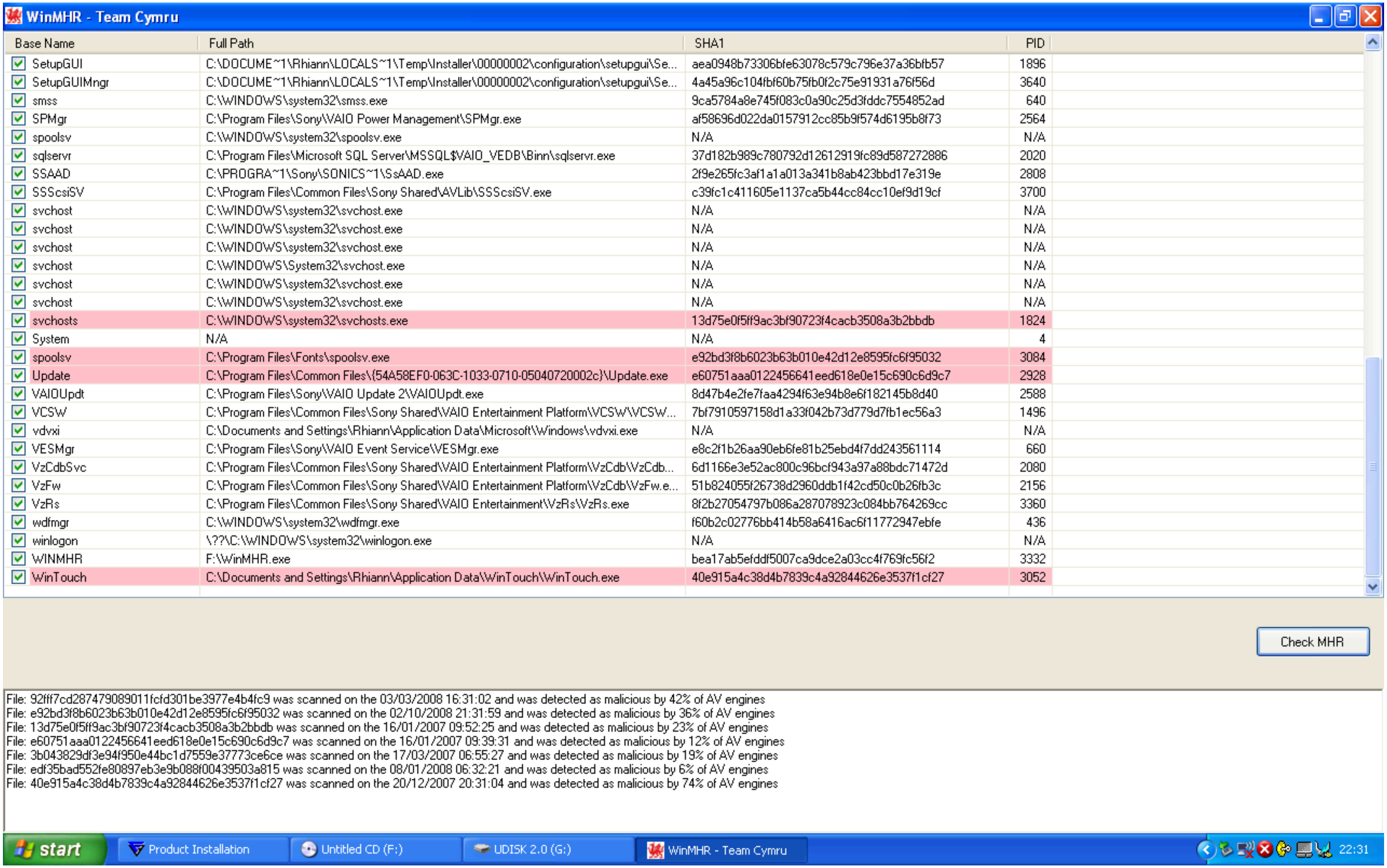
© 2008 Team Cymru

Applications

- Hardware
  - Coming soon to a router vendor near you…
  - BRO appliance
  - Your ideas here…
- Software
  - Mail Servers
  - Forensics
  - Poor man’s AV
  - The Sky’s the limit

© 2008 Team Cymru

Sneak Peek: WinMHR



Base Name	Full Path	SHA1	PID
☑ SetupGUI	C:\DOCUME~1\Rhiann\LOCALS~1\Temp\Installer\00000002\configuration\setupgui\Se...	aea0948b73306bfe63078c579c796e37a36bfb57	1896
☑ SetupGUIMngr	C:\DOCUME~1\Rhiann\LOCALS~1\Temp\Installer\00000002\configuration\setupgui\Se...	4a45a96c104fbf60b75fb0f2c75e91931a76f56d	3640
☑ smss	C:\WINDOWS\system32\smss.exe	9ca5784a8e745f083c0a90c25d3fddc7554852ad	640
☑ SPMgr	C:\Program Files\Sony\VAIO Power Management\SPMgr.exe	af58696d022da0157912cc85b9f574d6195b8f73	2564
☑ spoolsv	C:\WINDOWS\system32\spoolsv.exe	N/A	N/A
☑ sqlservr	C:\Program Files\Microsoft SQL Server\MSSQL$VAIO_VEDB\Binn\sqlservr.exe	37d182b989c780792d12612919fc89d587272886	2020
☑ SSAAD	C:\PROGRA~1\Sony\SONICS~1\SsAAD.exe	2f9e265fc3af1a1a013a341b8ab423bbd17e319e	2808
☑ SSScsiSV	C:\Program Files\Common Files\Sony Shared\AVLib\SSScsiSV.exe	c39fc1c411605e1137ca5b44cc84cc10ef9d19cf	3700
☑ svchost	C:\WINDOWS\system32\svchost.exe	N/A	N/A
☑ svchost	C:\WINDOWS\system32\svchost.exe	N/A	N/A
☑ svchost	C:\WINDOWS\system32\svchost.exe	N/A	N/A
☑ svchost	C:\WINDOWS\System32\svchost.exe	N/A	N/A
☑ svchost	C:\WINDOWS\system32\svchost.exe	N/A	N/A
☑ svchost	C:\WINDOWS\system32\svchost.exe	N/A	N/A
☑ svchosts	C:\WINDOWS\system32\svchosts.exe	13d75e0f5ff9ac3bf90723f4cacb3508a3b2bbdb	1824
☑ System	N/A	N/A	4
☑ spoolsv	C:\Program Files\Fonts\spoolsv.exe	e92bd3f8b6023b63b010e42d12e8595fc6f95032	3084
☑ Update	C:\Program Files\Common Files\{54A58EF0-063C-1033-0710-05040720002c}\Update.exe	e60751aaa0122456641eed618e0e15c690c6d9c7	2928
☑ VAIOUpdt	C:\Program Files\Sony\VAIO Update 2\VAIOUpdt.exe	8d47b4e2fe7faa4294f63e94b8e6f182145b8d40	2588
☑ VCSW	C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VCSW\VCSW...	7bf7910597158d1a33f042b73d779d7fb1ec56a3	1496
☑ vdvxi	C:\Documents and Settings\Rhiann\Application Data\Microsoft\Windows\vdvxi.exe	N/A	N/A
☑ VESMgr	C:\Program Files\Sony\VAIO Event Service\VESMgr.exe	e8c2f1b26aa90eb6fe81b25ebd4f7dd243561114	660
☑ VzCdbSvc	C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzCdb...	6d1166e3e52ac800c96bcf943a97a88bdc71472d	2080
☑ VzFw	C:\Program Files\Common Files\Sony Shared\VAIO Entertainment Platform\VzCdb\VzFw.e...	51b824055f26738d2960ddb1f42cd50c0b26fb3c	2156
☑ VzRs	C:\Program Files\Common Files\Sony Shared\VAIO Entertainment\VzRs\VzRs.exe	8f2b27054797b086a287078923c084bb764269cc	3360
☑ wdfmgr	C:\WINDOWS\system32\wdfmgr.exe	f60b2c02776bb414b58a6416ac6f11772947ebfe	436
☑ winlogon	\??\C:\WINDOWS\system32\winlogon.exe	N/A	N/A
☑ WINMHR	F:\WinMHR.exe	bea17ab5efddf5007ca9dce2a03cc4f769fc56f2	3332
☑ WinTouch	C:\Documents and Settings\Rhiann\Application Data\WinTouch\WinTouch.exe	40e915a4c38d4b7839c4a92844626e3537f1cf27	3052

```
File: 92fff7cd287479089011fcfd301be3977e4b4fc9 was scanned on the 03/03/2008 16:31:02 and was detected as malicious by 42% of AV engines
File: e92bd3f8b6023b63b010e42d12e8595fc6f95032 was scanned on the 02/10/2008 21:31:59 and was detected as malicious by 36% of AV engines
File: 13d75e0f5ff9ac3bf90723f4cacb3508a3b2bbdb was scanned on the 16/01/2007 09:52:25 and was detected as malicious by 23% of AV engines
File: e60751aaa0122456641eed618e0e15c690c6d9c7 was scanned on the 16/01/2007 09:39:31 and was detected as malicious by 12% of AV engines
File: 3b043829df3e94f950e44bc1d7559e37773ce6ce was scanned on the 17/03/2007 06:55:27 and was detected as malicious by 19% of AV engines
File: edf35bad552fe80897eb3e9b088f00439503a815 was scanned on the 08/01/2008 06:32:21 and was detected as malicious by 6% of AV engines
File: 40e915a4c38d4b7839c4a92844626e3537f1cf27 was scanned on the 20/12/2007 20:31:04 and was detected as malicious by 74% of AV engines
```

© 2008 Team Cymru

AV’s Effectiveness

- We collect approximately ~30K+ unique malware samples per day.
- Using current AV signatures and engines from 32 AV vendors, the detection rate is circa 28%.
- 30 days later the detection rate can be as high as 50%. Yay. :/

© 2008 Team Cymru

MHR’s Effectiveness

- According to One Private study:
  - MHR improved AV’s hit rate by 50%!

- Contributions Welcomed!!!
  - AV engines (from vendor)
  - Malware samples
  - Suggestions for improvement
  - Moral support
  - Coffee

MHR’s Adoption

- In the first 5 days, over 750k queries
- 10M+ queries in Jan 2009
- BRO Addon in the first day

http://wiki.github.com/sethhall/bro_scripts/the-malware-hash-registry-and-bro-ids

Realtime HTTP Monitoring

- Linux Host Active Scanning

© 2008 Team Cymru

Future Addons

- Kernel Driver to watch for new processes
- Monitoring of subprocesses and DLLs (svchost.exe)

© 2008 Team Cymru

FAQ

- How do I interpret the output?
  - It’s not too bad, just two numbers to worry about: timestamp (unix), and detection rate
- How do you collect malware?
  - *How don’t we collect malware...*
- Can I download your hash registry database?
  - *It is not publically available, but you may contact us about a data sharing agreement.*
- Can I have a sample of the file …?
  - *Please see the FAQ ☺*

© 2008 Team Cymru

FAQ

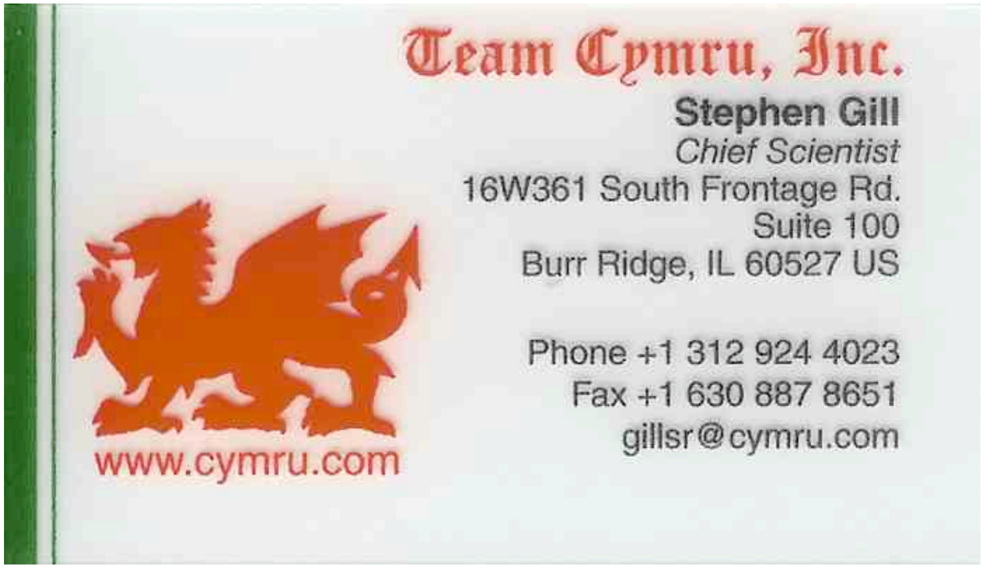
- Which AV Engines?
  - *Undisclosed*
- Tell me more about your malware database?
  - *Talk to me afterwards.*
- Should I just stop using an anti-virus package?
  - *NO! Please continue to use AV!*
- How up-to-date is your registry?
  - *Updated once, daily.*
- How do I report a False Positive?
  - *http://www.team-cymru.org/Services/MHR/*

Team Cymru can Help You!

- Detection
  - – Flows, Feeds, Compromised devices
  - – Have questions about your network or IPs? Talk to me afterwards.
- Investigation
  - – Cyber who dunnit?
- Prevention
- Mitigation
- Collaboration

© 2008 Team Cymru

Thank you for your time!



Team Cymru, Inc.

Stephen Gill
Chief Scientist
16W361 South Frontage Rd.
Suite 100
Burr Ridge, IL 60527 US

Phone +1 312 924 4023
Fax +1 630 887 8651
gillsr@cymru.com

www.cymru.com

© 2008 Team Cymru

Concluding Remarks

- Questions?

© 2008 Team Cymru

More Information

- http://www.team-cymru.org/Services/MHR/

TEAM CYMRU
www.team-cymru.org

© 2008 Team Cymru