Combating Hybrids

and The Modern Threatscape

Derek Manky
Project Manager, Cyber Security & Threat Research

YSTS 3.0: June 22nd, 2009

FORTINET®

Presentation Overview

- Modern Threats & Hybrids Intro
- Current Threat Profiles
  - Waledac
  - Conficker
- Virut: A Modern Hybrid
  - Prevalence & Impact
  - Live Demonstration
- Combating Modern Threats
- Q&A

Modern Threats & Hybrids Intro

Modern Threats

- Targeted Attacks: Documents Favored
  - Various Exploits Used
    - PDF, XLS, DOC
    - Soon: Migration to social networks, blogs
      - Profiling
  - Common Malware Dropped

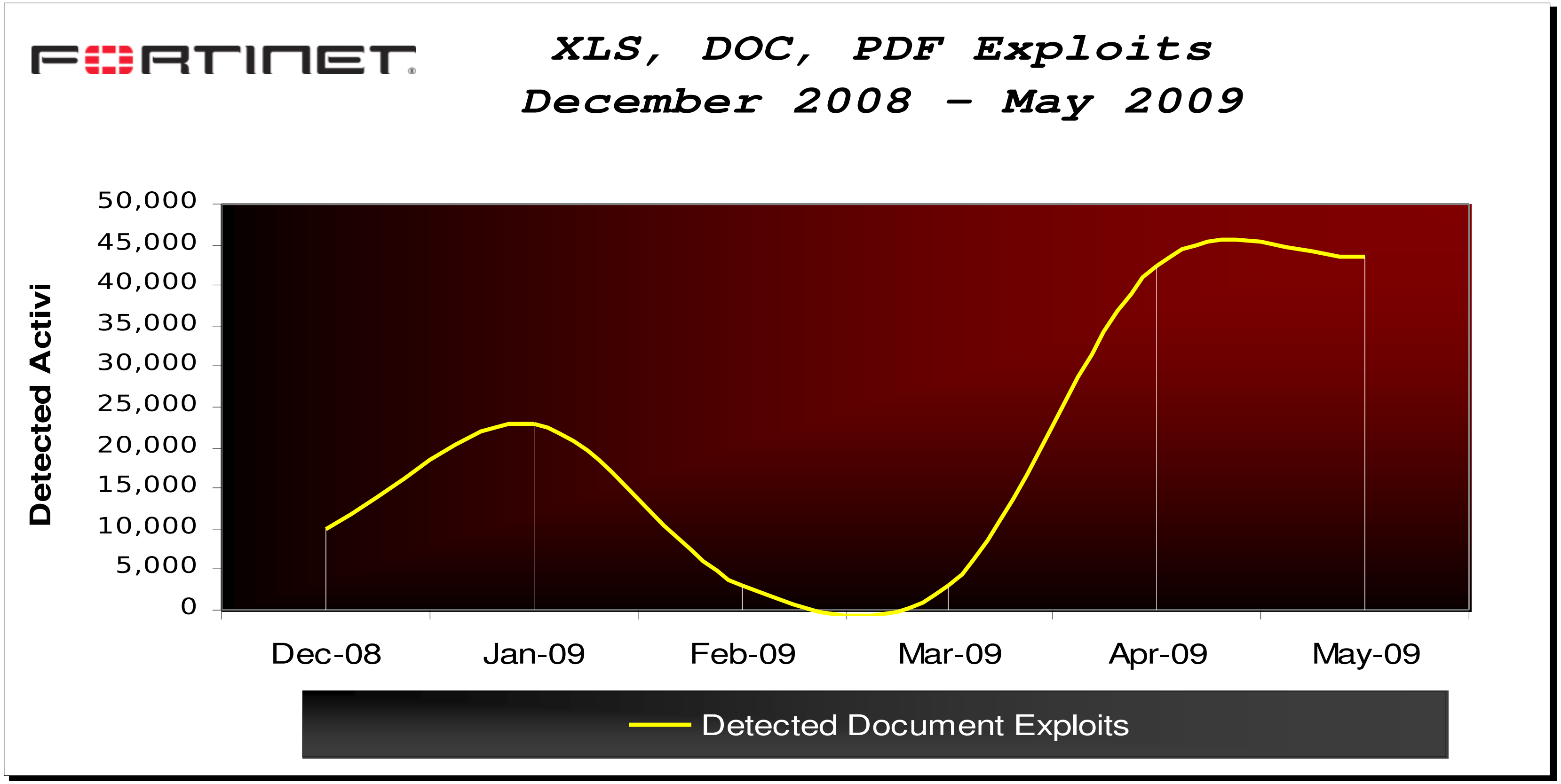
- Social Engineering 2.0
  - Location Based Services / geoIP
    - Waledac, Canadian Pharmacy
  - Profiling
  - Ransomware

- Obfuscated Scripting
- Packers++

Modern Threats & Hybrids Intro

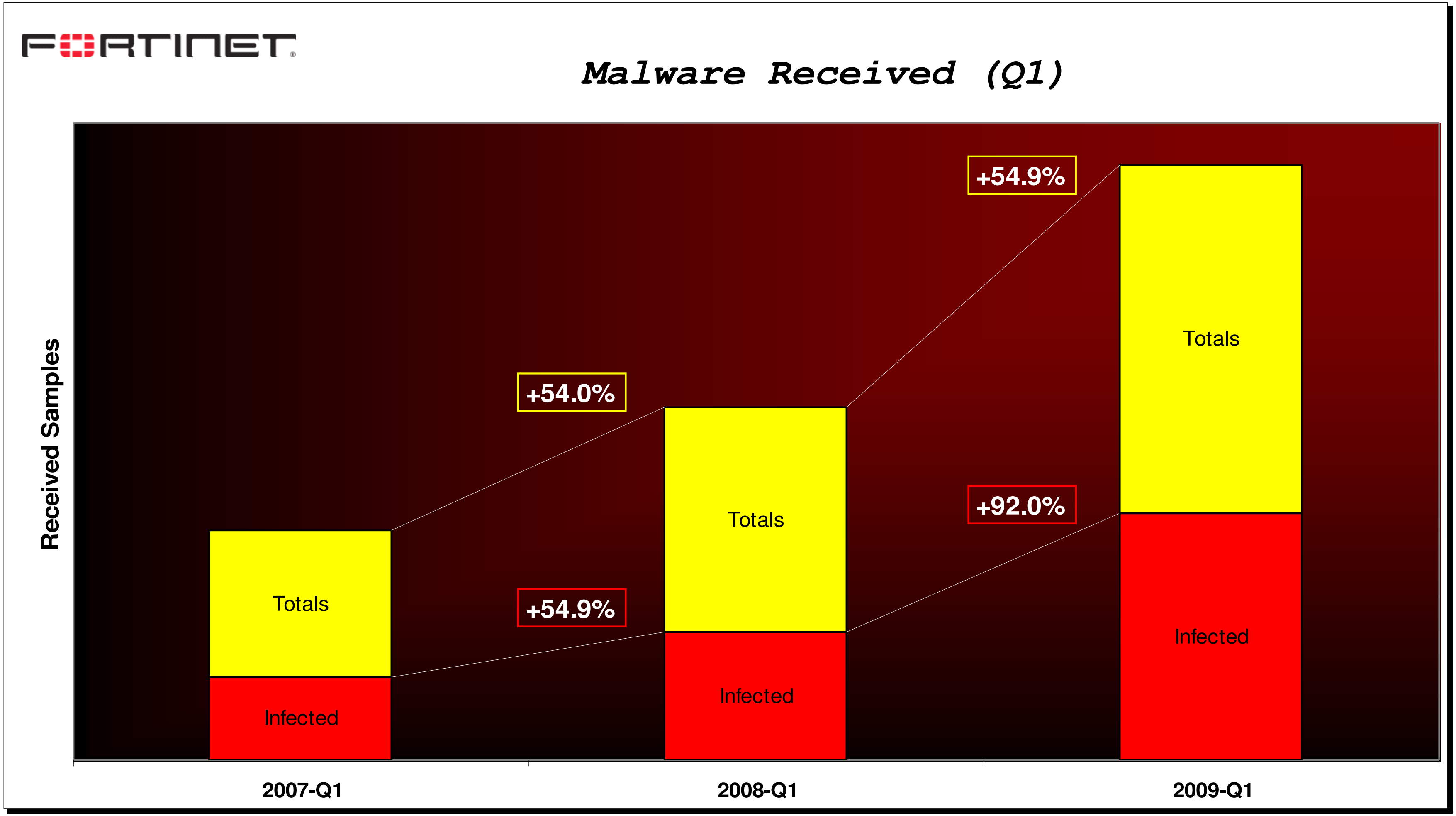
Modern Threats

- Targeted Attacks: Documents Favored



Modern Threats & Hybrids Intro

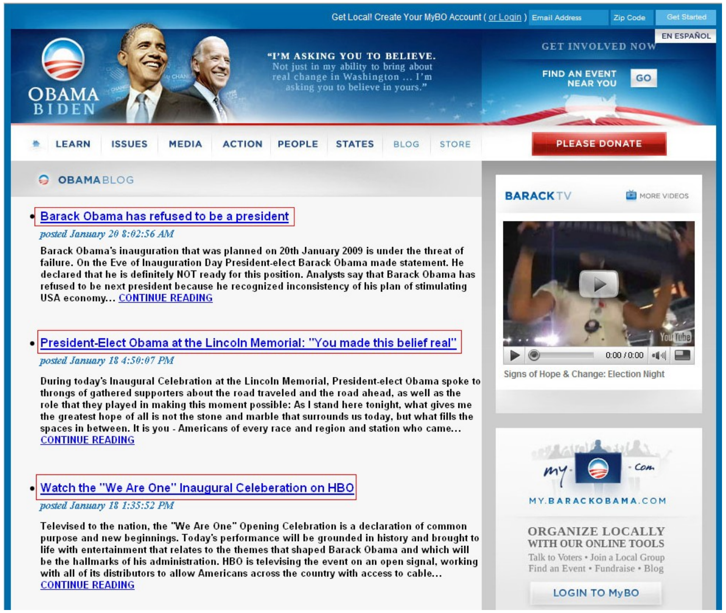
- 3 Quarter Increase in Received Samples



Current Threat Profiles

Waledac

- Malware Profile
- Routine Campaigns (5+ in 2009)
  - Botnet
    - Similar to Storm Worm
    - End Point / Server Nodes
    - HTTP Communication
      - Encrypted
      - Dynamic Session Keys
    - Initial Seed List in Binary
      - Node Updates Sent
  - Mass Mailer
    - Malicious Links
    - Affiliate Spam
      - Canadian Pharmacy


Get Local! Create Your MyBO Account (or Login)
Email Address
Zip Code
Get Started
EN ESPAÑOL
OBAMA BIDEN
"I'M ASKING YOU TO BELIEVE. Not just in my ability to bring about real change in Washington ... I'm asking you to believe in yours."
GET INVOLVED NOW
FIND AN EVENT NEAR YOU
GO
LEARN
ISSUES
MEDIA
ACTION
PEOPLE
STATES
BLOG
STORE
PLEASE DONATE
OBAMABLOG
BARACKTV
MORE VIDEOS
0:00 / 0:00
MY.BARACKOBAMA.COM
ORGANIZE LOCALLY WITH OUR ONLINE TOOLS
Talk to Voters • Join a Local Group
Find an Event • Fundraise • Blog
LOGIN TO MyBO

- Barack Obama has refused to be a president

  posted January 20 8:02:56 AM

  Barack Obama's inauguration that was planned on 20th January 2009 is under the threat of failure. On the Eve of Inauguration Day President-elect Barack Obama made statement. He declared that he is definitely NOT ready for this position. Analysts say that Barack Obama has refused to be next president because he recognized inconsistency of his plan of stimulating USA economy... CONTINUE READING

- President-Elect Obama at the Lincoln Memorial: "You made this belief real"

  posted January 18 4:50:07 PM

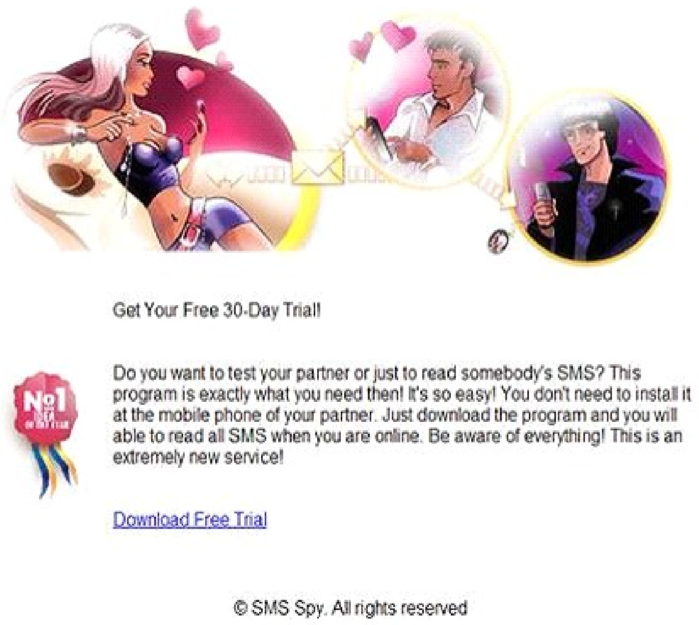
  During today's Inaugural Celebration at the Lincoln Memorial, President-elect Obama spoke to throngs of gathered supporters about the road traveled and the road ahead, as well as the role that they played in making this moment possible: As I stand here tonight, what gives me the greatest hope of all is not the stone and marble that surrounds us today, but what fills the spaces in between. It is you - Americans of every race and region and station who came... CONTINUE READING

- Watch the "We Are One" Inaugural Celeberation on HBO

  posted January 18 1:35:52 PM

  Televised to the nation, the "We Are One" Opening Celebration is a declaration of common purpose and new beginnings. Today's performance will be grounded in history and brought to life with entertainment that relates to the themes that shaped Barack Obama and which will be the hallmarks of his administration. HBO is televising the event on an open signal, working with all of its distributors to allow Americans across the country with access to cable... CONTINUE READING

Signs of Hope & Change: Election Night



Get Your Free 30-Day Trial!

Do you want to test your partner or just to read somebody's SMS? This program is exactly what you need then! It's so easy! You don't need to install it at the mobile phone of your partner. Just download the program and you will able to read all SMS when you are online. Be aware of everything! This is an extremely new service!

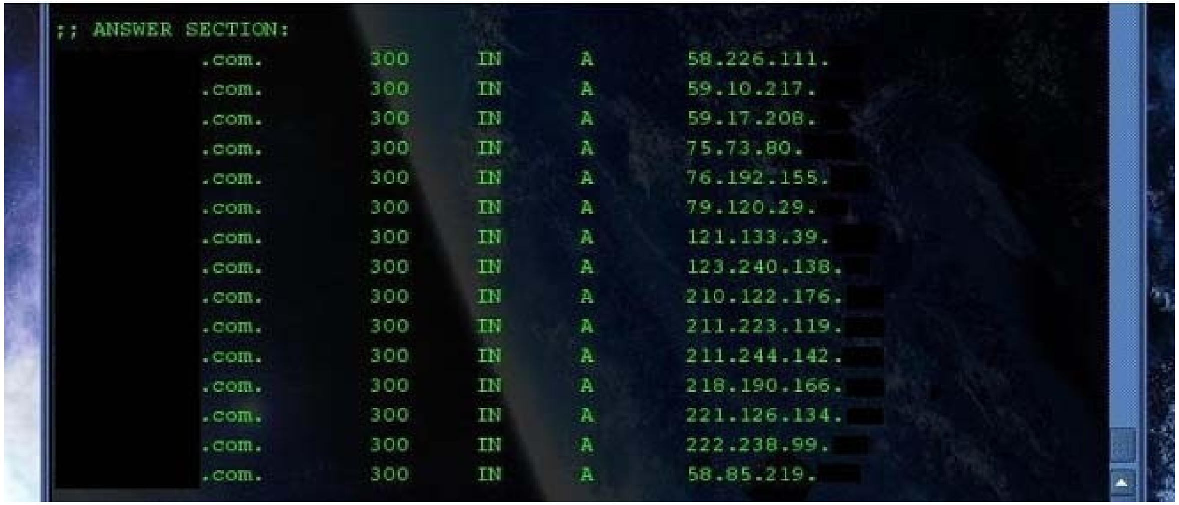
Download Free Trial

© SMS Spy. All rights reserved

Current Threat Profiles

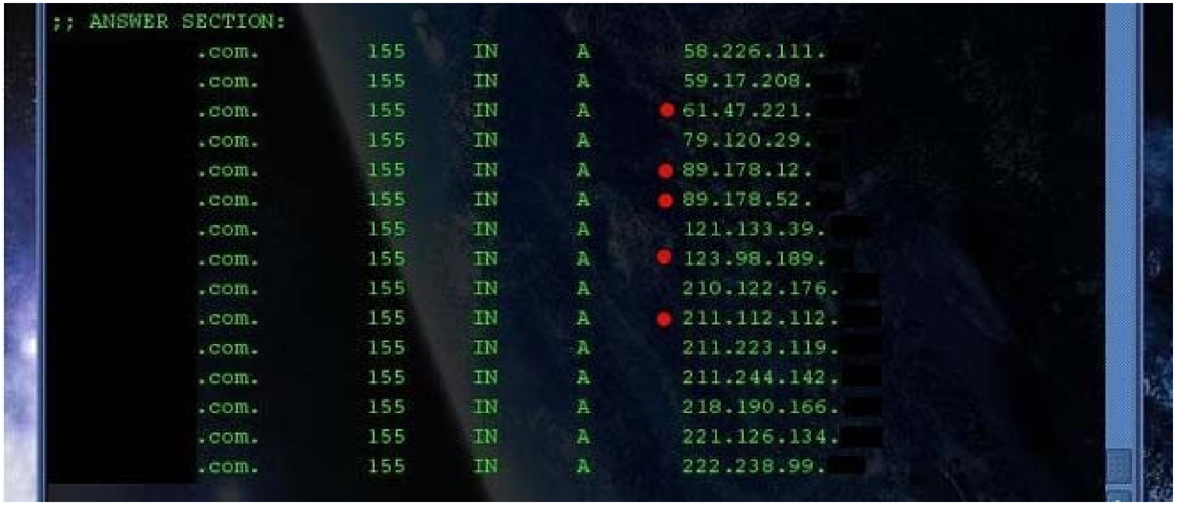
Waledac

- **Fast Flux Botnet**
  - Small TTL
  - Choice Weapon
    - Anonymous
  - Widely Adopted
  - Thousands of Domains
  - Various Campaigns
  - P2P



```
;; ANSWER SECTION:
[redacted]      .com.    300    IN    A    58.226.111.[redacted]
                .com.    300    IN    A    59.10.217.[redacted]
                .com.    300    IN    A    59.17.208.[redacted]
                .com.    300    IN    A    75.73.80.[redacted]
                .com.    300    IN    A    76.192.155.[redacted]
                .com.    300    IN    A    79.120.29.[redacted]
                .com.    300    IN    A    121.133.39.[redacted]
                .com.    300    IN    A    123.240.138.[redacted]
                .com.    300    IN    A    210.122.176.[redacted]
                .com.    300    IN    A    211.223.119.[redacted]
                .com.    300    IN    A    211.244.142.[redacted]
                .com.    300    IN    A    218.190.166.[redacted]
                .com.    300    IN    A    221.126.134.[redacted]
                .com.    300    IN    A    222.238.99.[redacted]
                .com.    300    IN    A    58.85.219.[redacted]
```

… 445 Seconds Pass …

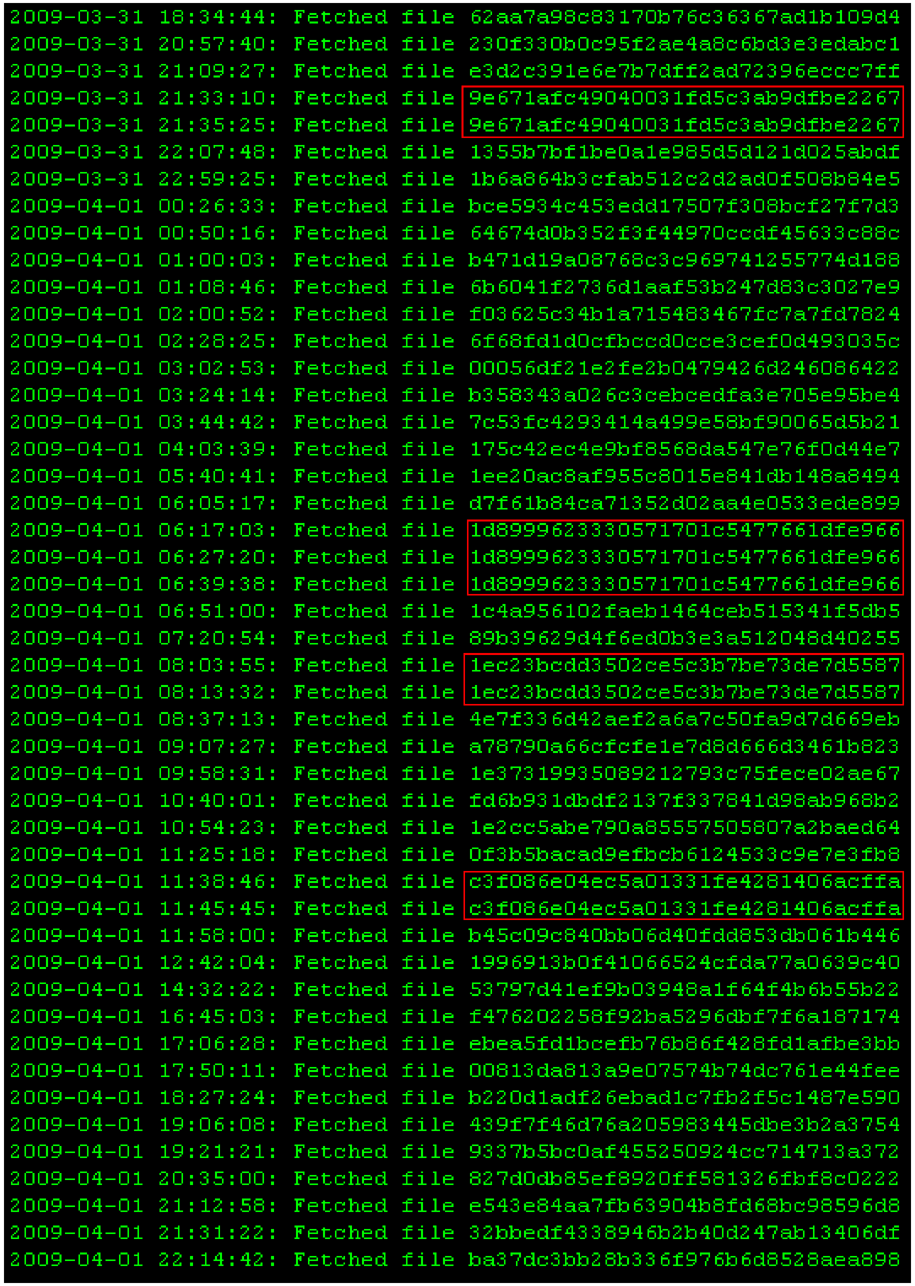


```
;; ANSWER SECTION:
[redacted]      .com.    155    IN    A      58.226.111.[redacted]
                .com.    155    IN    A      59.17.208.[redacted]
                .com.    155    IN    A    ● 61.47.221.[redacted]
                .com.    155    IN    A      79.120.29.[redacted]
                .com.    155    IN    A    ● 89.178.12.[redacted]
                .com.    155    IN    A    ● 89.178.52.[redacted]
                .com.    155    IN    A      121.133.39.[redacted]
                .com.    155    IN    A    ● 123.98.189.[redacted]
                .com.    155    IN    A      210.122.176.[redacted]
                .com.    155    IN    A    ● 211.112.112.[redacted]
                .com.    155    IN    A      211.223.119.[redacted]
                .com.    155    IN    A      211.244.142.[redacted]
                .com.    155    IN    A      218.190.166.[redacted]
                .com.    155    IN    A      221.126.134.[redacted]
                .com.    155    IN    A      222.238.99.[redacted]
```

Current Threat Profiles

Waledac

- **Server Side Polymorphism**
  - One Domain: 10 Days
    - One Malicious File
    - 275+ Variations
  - One Domain: 50 Days
    - One Malicious File
    - 1440+ Variations
  - < 1 Hour Changes
    - Consistent For ~2 Months

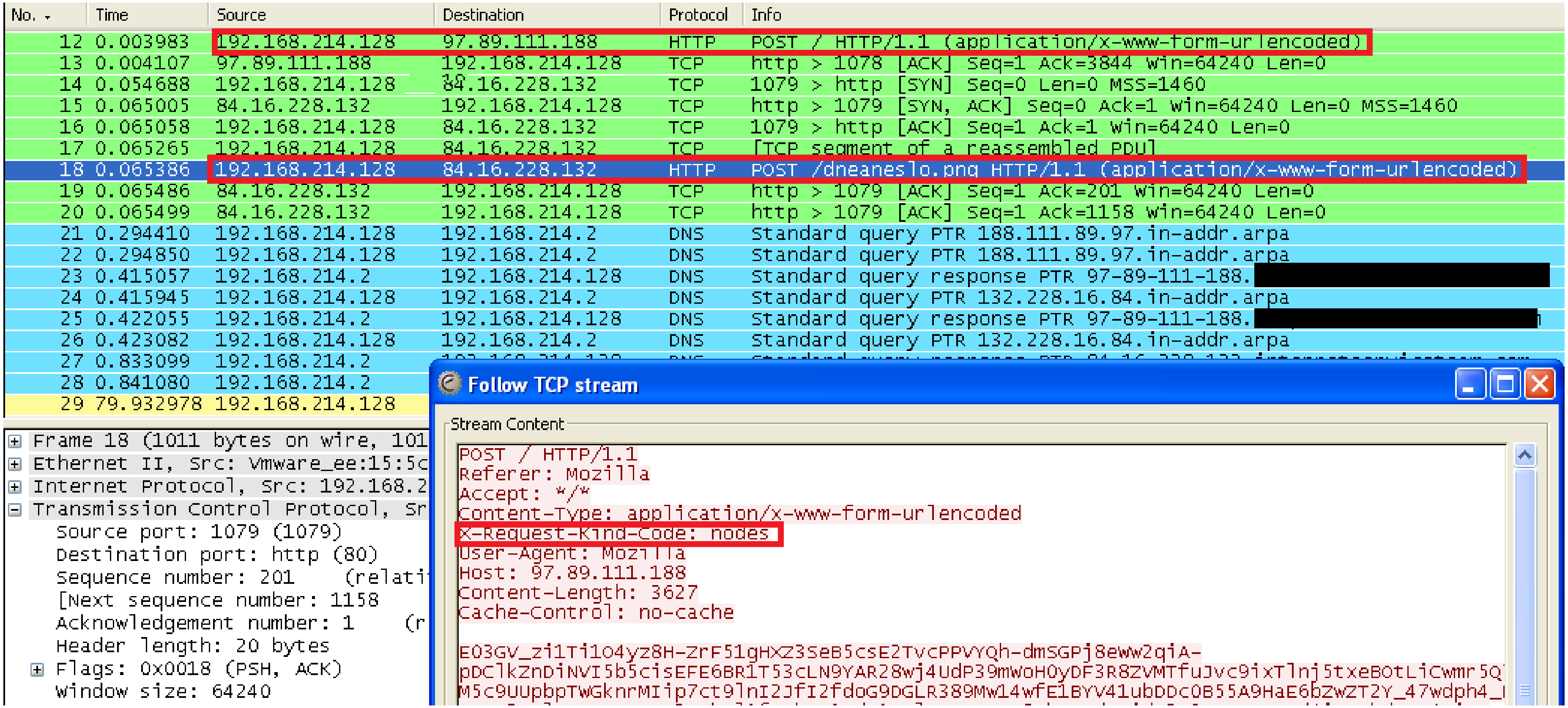


```
2009-03-31 18:34:44: Fetched file 62aa7a98c83170b76c36367ad1b109d4
2009-03-31 20:57:40: Fetched file 230f330b0c95f2ae4a8c6bd3e3edabc1
2009-03-31 21:09:27: Fetched file e3d2c391e6e7b7dff2ad72396eccc7ff
2009-03-31 21:33:10: Fetched file 9e671afc49040031fd5c3ab9dfbe2267
2009-03-31 21:35:25: Fetched file 9e671afc49040031fd5c3ab9dfbe2267
2009-03-31 22:07:48: Fetched file 1355b7bf1be0a1e985d5d121d025abdf
2009-03-31 22:59:25: Fetched file 1b6a864b3cfab512c2d2ad0f508b84e5
2009-04-01 00:26:33: Fetched file bce5934c453edd17507f308bcf27f7d3
2009-04-01 00:50:16: Fetched file 64674d0b352f3f44970ccdf45633c88c
2009-04-01 01:00:03: Fetched file b471d19a08768c3c969741255774d188
2009-04-01 01:08:46: Fetched file 6b6041f2736d1aaf53b247d83c3027e9
2009-04-01 02:00:52: Fetched file f03625c34b1a715483467fc7a7fd7824
2009-04-01 02:28:25: Fetched file 6f68fd1d0cfbccd0cce3cef0d493035c
2009-04-01 03:02:53: Fetched file 00056df21e2fe2b0479426d246086422
2009-04-01 03:24:14: Fetched file b358343a026c3cebcedfa3e705e95be4
2009-04-01 03:44:42: Fetched file 7c53fc4293414a499e58bf90065d5b21
2009-04-01 04:03:39: Fetched file 175c42ec4e9bf8568da547e76f0d44e7
2009-04-01 05:40:41: Fetched file 1ee20ac8af955c8015e841db148a8494
2009-04-01 06:05:17: Fetched file d7f61b84ca71352d02aa4e0533ede899
2009-04-01 06:17:03: Fetched file 1d8999623330571701c5477661dfe966
2009-04-01 06:27:20: Fetched file 1d8999623330571701c5477661dfe966
2009-04-01 06:39:38: Fetched file 1d8999623330571701c5477661dfe966
2009-04-01 06:51:00: Fetched file 1c4a956102faeb1464ceb515341f5db5
2009-04-01 07:20:54: Fetched file 89b39629d4f6ed0b3e3a512048d40255
2009-04-01 08:03:55: Fetched file 1ec23bcdd3502ce5c3b7be73de7d5587
2009-04-01 08:13:32: Fetched file 1ec23bcdd3502ce5c3b7be73de7d5587
2009-04-01 08:37:13: Fetched file 4e7f336d42aef2a6a7c50fa9d7d669eb
2009-04-01 09:07:27: Fetched file a78790a66cfcfe1e7d8d666d3461b823
2009-04-01 09:58:31: Fetched file 1e373199350892127930c75fece02ae67
2009-04-01 10:40:01: Fetched file fd6b931dbdf2137f337841d98ab968b2
2009-04-01 10:54:23: Fetched file 1e2cc5abe790a8555750580 7a2baed64
2009-04-01 11:25:18: Fetched file 0f3b5bacad9efbcb6124533c9e7e3fb8
2009-04-01 11:38:46: Fetched file c3f086e04ec5a01331fe4281406acffa
2009-04-01 11:45:45: Fetched file c3f086e04ec5a01331fe4281406acffa
2009-04-01 11:58:00: Fetched file b45c09c840bb06d40fdd853db061b446
2009-04-01 12:42:04: Fetched file 1996913b0f41066524cfda77a0639c40
2009-04-01 14:32:22: Fetched file 53797d41ef9b03948a1f64f4b6b55b22
2009-04-01 16:45:03: Fetched file f476202258f92ba5296dbf7f6a187174
2009-04-01 17:06:28: Fetched file ebea5fd1bcefb76b86f428fd1afbe3bb
2009-04-01 17:50:11: Fetched file 00813da813a9e07574b74dc761e44fee
2009-04-01 18:27:24: Fetched file b220d1adf26ebad1c7fb2f5c1487e590
2009-04-01 19:06:08: Fetched file 439f7f46d76a205983445dbe3b2a3754
2009-04-01 19:21:21: Fetched file 9337b5bc0af45525092 4cc714713a372
2009-04-01 20:35:00: Fetched file 827d0db85ef8920ff581326fbf8c0222
2009-04-01 21:12:58: Fetched file e543e84aa7fb63904b8fd68bc98596d8
2009-04-01 21:31:22: Fetched file 32bbedf4338946b2b40d247ab13406df
2009-04-01 22:14:42: Fetched file ba37dc3bb28b336f976b6d8528aea898
```

Current Threat Profiles

Waledac

- Common Channels & Cloaked Commands



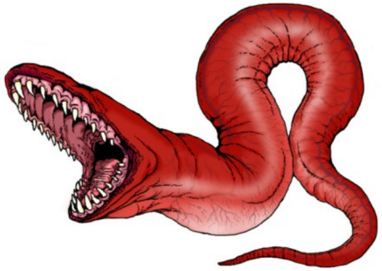
No.	Time	Source	Destination	Protocol	Info
12	0.003983	192.168.214.128	97.89.111.188	HTTP	POST / HTTP/1.1 (application/x-www-form-urlencoded)
13	0.004107	97.89.111.188	192.168.214.128	TCP	http > 1078 [ACK] Seq=1 Ack=3844 Win=64240 Len=0
14	0.054688	192.168.214.128	84.16.228.132	TCP	1079 > http [SYN] Seq=0 Len=0 MSS=1460
15	0.065005	84.16.228.132	192.168.214.128	TCP	http > 1079 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16	0.065058	192.168.214.128	84.16.228.132	TCP	1079 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
17	0.065265	192.168.214.128	84.16.228.132	TCP	[TCP segment of a reassembled PDU]
18	0.065386	192.168.214.128	84.16.228.132	HTTP	POST /dneaneslo.png HTTP/1.1 (application/x-www-form-urlencoded)
19	0.065486	84.16.228.132	192.168.214.128	TCP	http > 1079 [ACK] Seq=1 Ack=201 Win=64240 Len=0
20	0.065499	84.16.228.132	192.168.214.128	TCP	http > 1079 [ACK] Seq=1 Ack=1158 Win=64240 Len=0
21	0.294410	192.168.214.128	192.168.214.2	DNS	Standard query PTR 188.111.89.97.in-addr.arpa
22	0.294850	192.168.214.128	192.168.214.2	DNS	Standard query PTR 188.111.89.97.in-addr.arpa
23	0.415057	192.168.214.2	192.168.214.128	DNS	Standard query response PTR 97-89-111-188.[redacted]
24	0.415945	192.168.214.128	192.168.214.2	DNS	Standard query PTR 132.228.16.84.in-addr.arpa
25	0.422055	192.168.214.2	192.168.214.128	DNS	Standard query response PTR 97-89-111-188.[redacted]
26	0.423082	192.168.214.128	192.168.214.2	DNS	Standard query PTR 132.228.16.84.in-addr.arpa
27	0.833099	192.168.214.2			
28	0.841080	192.168.214.2			
29	79.932978	192.168.214.128			

```
⊞ Frame 18 (1011 bytes on wire, 101
⊞ Ethernet II, Src: Vmware_ee:15:5c
⊞ Internet Protocol, Src: 192.168.2
⊟ Transmission Control Protocol, Sr
    Source port: 1079 (1079)
    Destination port: http (80)
    Sequence number: 201    (relati
    [Next sequence number: 1158
    Acknowledgement number: 1    (r
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 64240
```

```
POST / HTTP/1.1
Referer: Mozilla
Accept: */*
Content-Type: application/x-www-form-urlencoded
x-Request-Kind-Code: nodes
User-Agent: Mozilla
Host: 97.89.111.188
Content-Length: 3627
Cache-Control: no-cache

E03GV_zi1Ti1O4yz8H-ZrF51gHXZ3SeB5csE2TvcPPVYQh-dmSGPj8eWw2qiA-
pDClkZnDiNVI5b5cisEFE6BR1T53cLN9YAR28wj4UdP39mWoHOyDF3R8ZVMTfuJvc9ixTlnj5txeBOtLiCwmr5Q
M5c9UUpbpTWGknrMIip7ct9lnI2JfI2fdoG9DGLR389Mw14wfE1BYV41ubDDc0B55A9HaE6bZwZT2Y_47wdph4_
```

Current Threat Profiles



The Conficker Timeline[2]

- **Aug 20, 2008**: First exploit seen, Gimmiv Trojan
- **Oct 23, 2008**: Microsoft Issues MS08-067 Patch
- **Oct 26, 2008**: PoC Widely Available
- **Nov 20, 2008**: Conficker.A observed
  - **Nov 26, 2008**: Time Bomb #1 (DGA – 250)
  - **Dec 01, 2008**: Time Bomb #2 (TrafficConverter)
- **Dec 28, 2008**: Conficker.B observed
  - **Jan 01, 2009**: Time Bomb #3 (DGA – 250)
- **Feb 16, 2008**: Conficker.B++ observed
- **Mar 05, 2008**: Conficker.C updates B/B++
  - **Apr 01, 2009**: Time Bomb #4 (DGA – 50k)
- **Apr 08, 2009:** P2P updates spread through Conficker.C
  - Connected to Waledac Servers

Current Threat Profiles

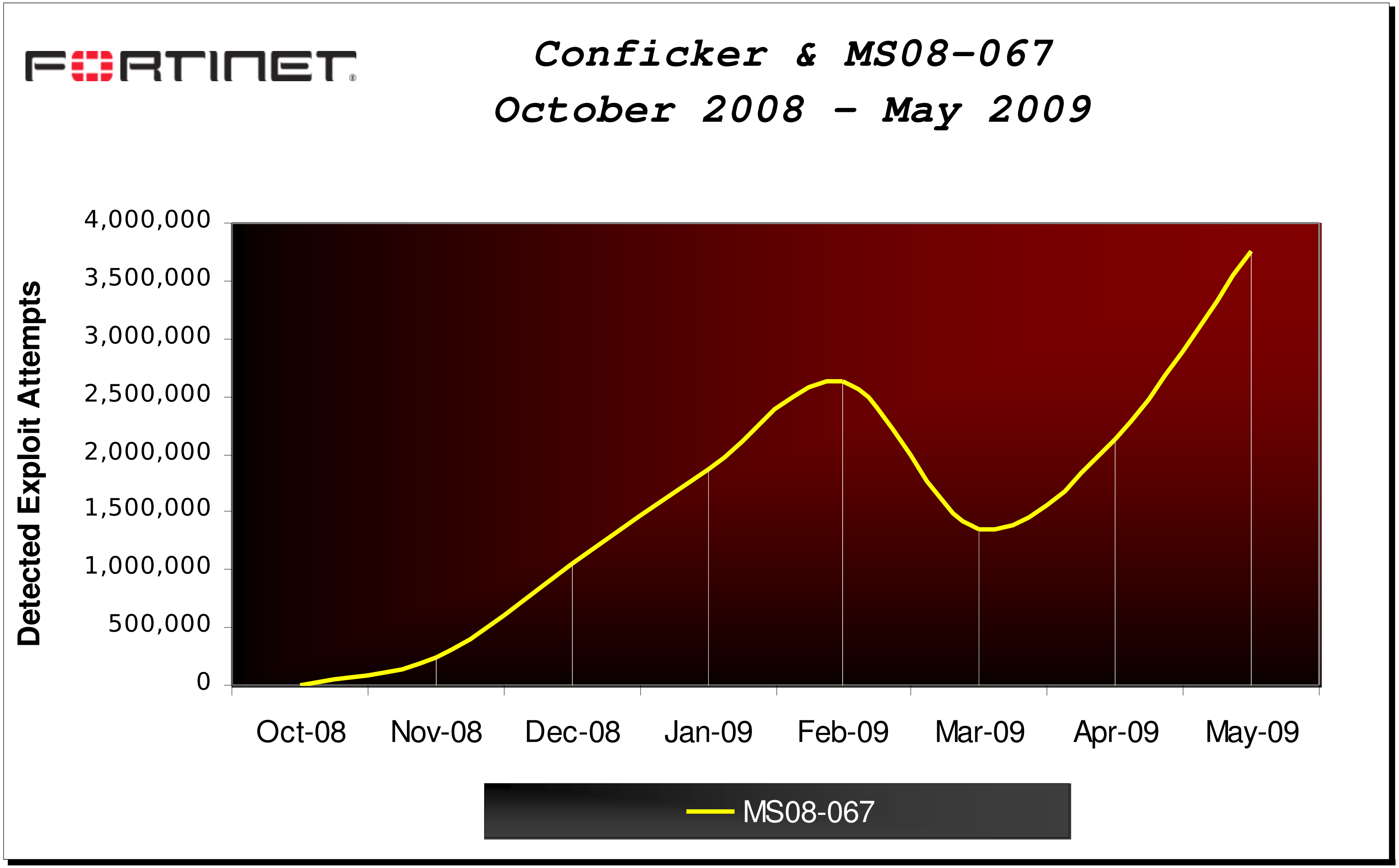
Notable Conficker Incidents[2]

- **Dec 29, 2008**: Sheffield Hospitals
  - 800+ Systems Infected
- **Jan 06, 2009**: UK Ministry of Defense
  - 2 Weeks Damage Control
- **Jan 15, 2009**: French Navy Computer Network[3]
  - Grounds aircrafts, flight plans cannot be downloaded
- **Feb 13, 2009**: German Federal Defense[3]
  - 100 Est. Systems Infected
- **Mar 2009**: CBS News Infected
- **Mar 24, 2009**: British Director of Parliamentary ICT[3]

- ***Millions Impacted Worldwide***
  - Denial of Service
  - Administrative Overtime

Current Threat Profiles

- Seven Month Peak After Disclosure / Patch[1]



Virut: A Modern Hybrid

Profile

- Parasitic file infector
  - Infects EXE, SCR
  - Entry Point Obscuring
  - Targets Servers - Infects web documents (Virut.CE)
    - HTM, PHP, ASP
  - Newer variants use cavities
  - Infecting Your Files Since 2007
- C&C Channels
  - Hardcoded IRC
  - Downloads multiple components / spambots

Virut: A Modern Hybrid

Profile: Virut's Evolution

- **Virut.A** (May 2006)
  - Highest detected activity in September 2008
    - *Most Prevalent Virus 2008-2009*
    - *Here We Go Again – May 2009*
  - Searches & Infects Executables
  - Simple Decrypting Loop (XOR)
  - Hardcoded C&C Channel (IRC)
    - Random Username
    - Accepts Instructions (GET)

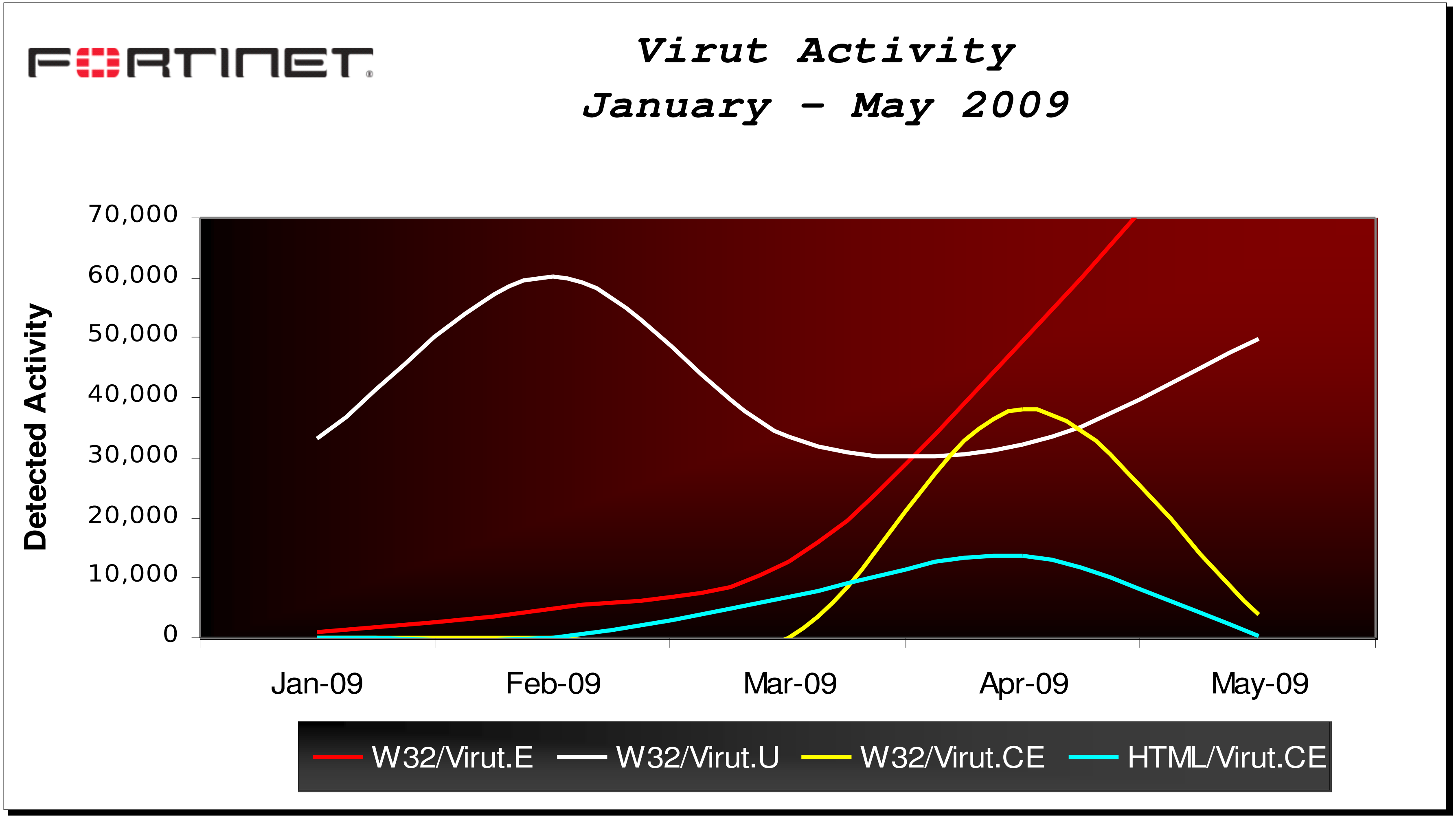
Virut: A Modern Hybrid

Profile: Virut's Evolution

- **Virut.CE** (Feb 2009)
  - Highest detected activity in April 2009
  - Multiple Appending Infection Routines
    - *Type 1* – EPO, Multiple Decoders (Cavity)
    - *Type 2* – Non-EPO, Multiple Decoders (Cavity)
    - *Type 3* – EPO, Single Decoder (Non-Cavity)
    - *Type 4* – Non-EPO, Single Decoder (Non-Cavity)
  - Targets Client & Servers
    - Injects IFrame into HTM, PHP, ASP
  - Memory Resident
    - Hooks NTDLL APIs
    - Injects into winlogon.exe
  - More Hardcoded C&C Servers (IRC)

Virut: A Modern Hybrid

- **Prevalence & Impact:** Gearing Up



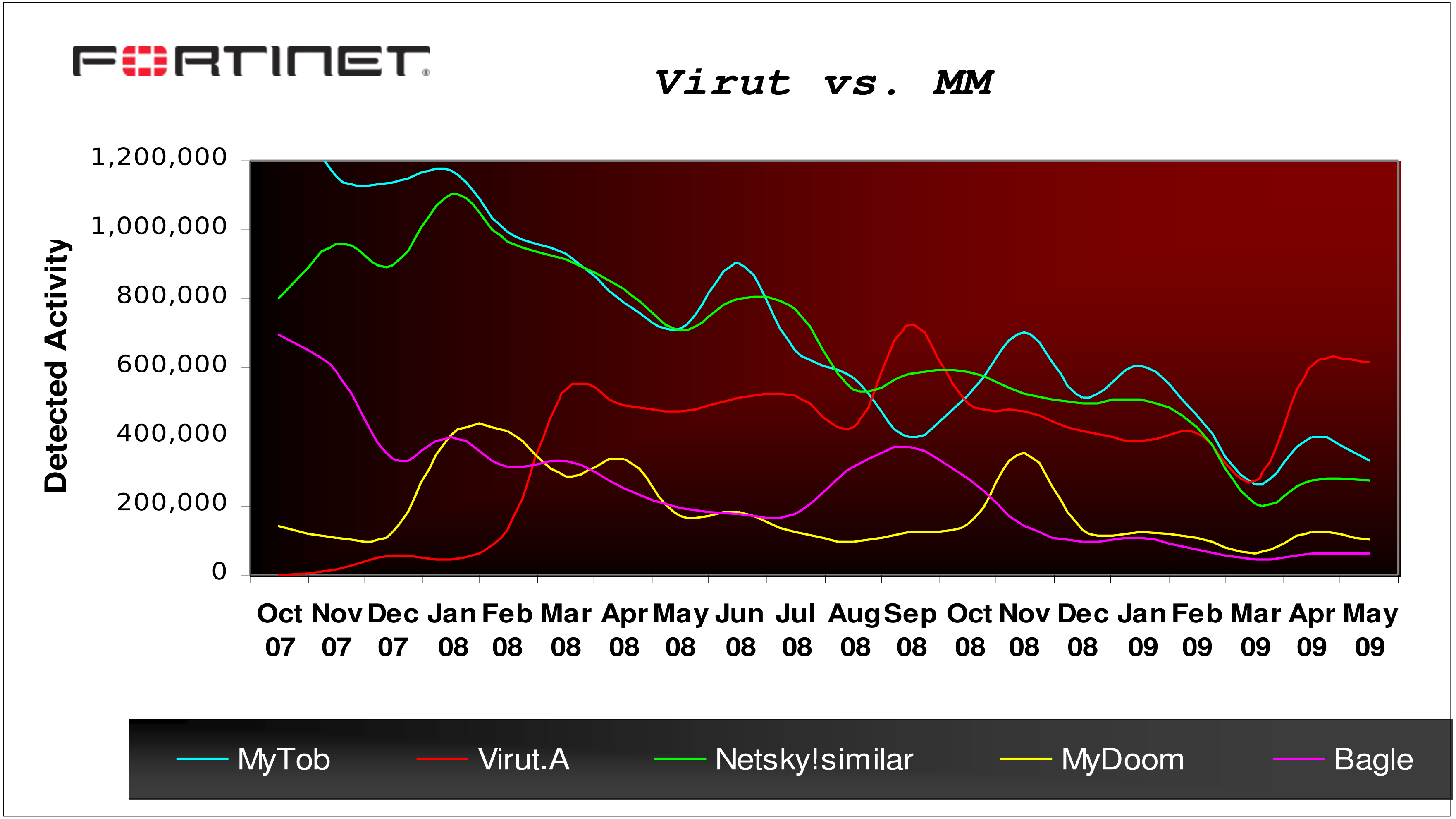
Virut: A Modern Hybrid

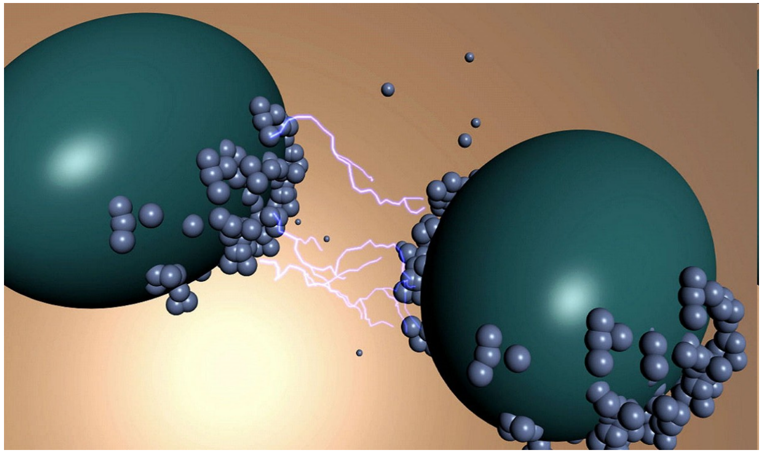
Prevalence & Impact

- Virut vs. Mass Mailers
  - Mass Mailing Hybrids Created
    - Netsky, Bagle, MyDoom, MyTob
  - Outbreak in Korea (W32/Virut.A)
  - Uses Mass Mailing Worms as Catalyst
    - ++Zombies
    - ++Profit
    - Any executables through spam templates / spambots

Virut: A Modern Hybrid

- **Prevalence & Impact:** Mass Conquered





W32/Virut.CE

Hybrid Demonstration

Combating Modern Threats

Conficker, Waledac et al: Layered Security

- Webfiltering: DGA, Fast Flux
  - High Capacity, Real Time
- Effective Antivirus: Reassembly, Server Polymorphism
  - End Point & **Gateway**
    - *Conficker Disables Host Security*
- Intrusion Prevention
  - MS08-067 & Future Exploits
- Antispam
  - Spam still very prevalent (McColo, 3FN)
  - Waledac node / server proxy technique
- Firewall
  - *Trojan Downloaders on Unwanted Ports*
  - End Point & Gateway

Conficker Case Study Sources
1: Fortinet's FortiGate and Worldwide Intelligence Systems
2: Byron Acohido: http://lastwatchdog.com/evolution-conficker-globe-spanning-worm
3: Wikipedia: http://en.wikipedia.org/wiki/Conficker

Combating Modern Threats

Policies & Education

- Incidence Response
  - Guidelines / Response Scenarios
  - Practice
    - Cyber Storm
- Memos/Seminars
  - Common Attacks
  - Security Bulletins / RSS
- Patch Management
  - OS & Browser Critical
- Browser Lockdown
  - ActiveX, Javascript, Flash, etc
- Wireless Lockdown
  - Inherently Insecure

Combating Modern Threats

Policies & Education

- Data Leak Prevention
  - Very Broad Area
  - UTM & IT Administration
    - Password Enforcement
- Mobile Devices
  - Roaming Policies
  - Connectivity Guidelines
    - Bluetooth, etc.
    - Autorun
- Encryption
  - VPN
  - SSL/TLS/(Open)PGP
  - CryptoFS
    - TrueCrypt

Bonus Slide

Top Malware in Brazil

January 01 – May 31 2009

Rank	Detection	Description
#1	W32/Netsky.X@mm	Netsky variant, DoS attacks three websites
#2	HTML/Virut.CE	Infected server pages (HTM, PHP, ASP) from W32/Virut.CE
#3	JS/Feebs.fam@mm	Attaches .HTA file (4kb). Spreads through encrypted JS instructions.
#4	Adware/AdClicker	General Adware Family
#5	JS/Agent.AOI!tr	JS trojan downloader

Questions ?

Thank You!