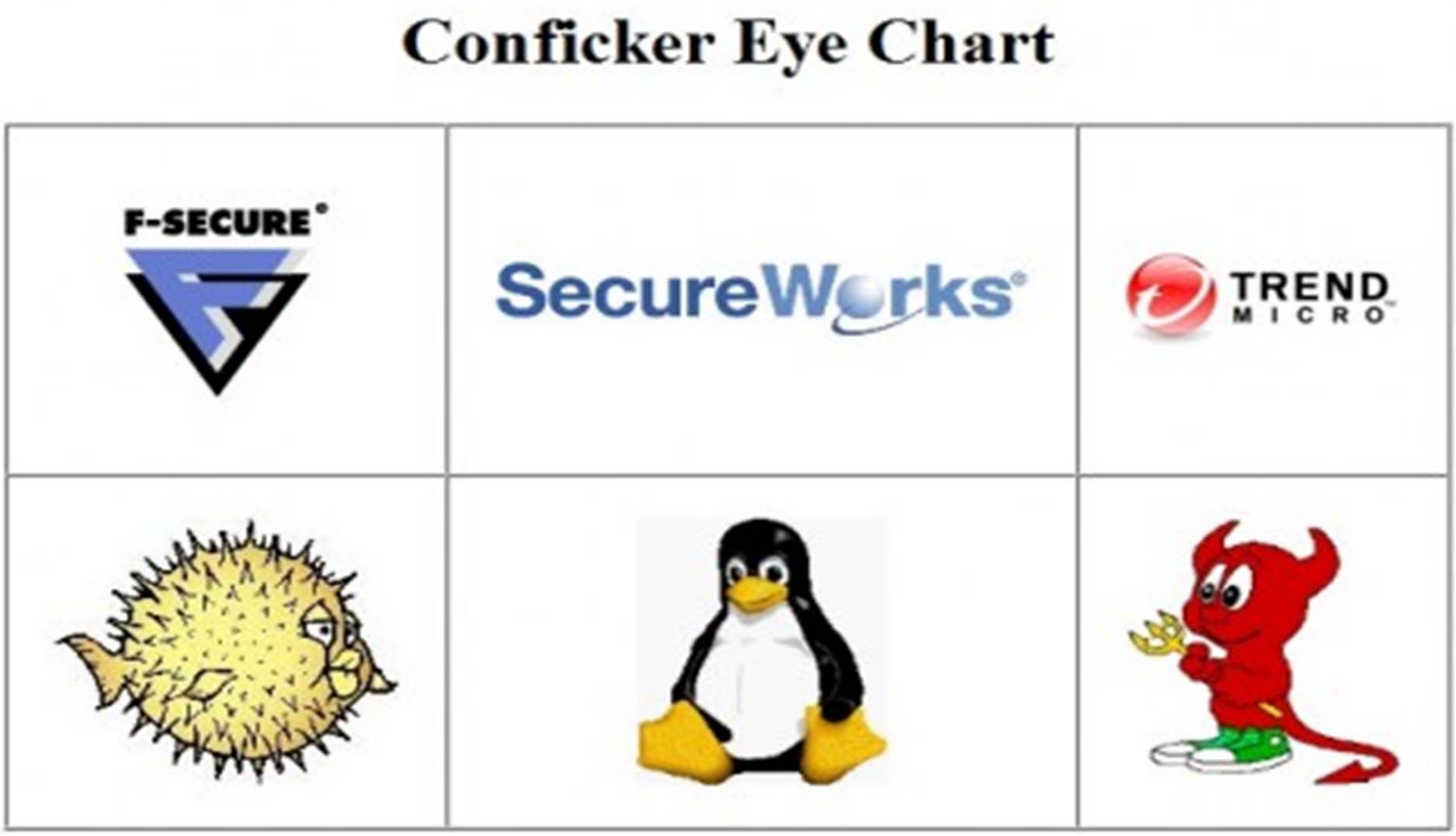
CONFICKER

Colin Cole



What is it?

- Worm, released in 2008, by unknown creators. Thought to originate from Eastern Europe, specifically the Ukraine
- 5 different versions
- Exact number of infected computers is not known. Microsoft estimates at around 1.5 million as of mid 2011. Others have estimated from 9 million to 15 million
- Although there has been an unprecedented effort in containing the worm (Conficker Cabal), it still remains prevalent in computer systems worldwide

How does it propagate?

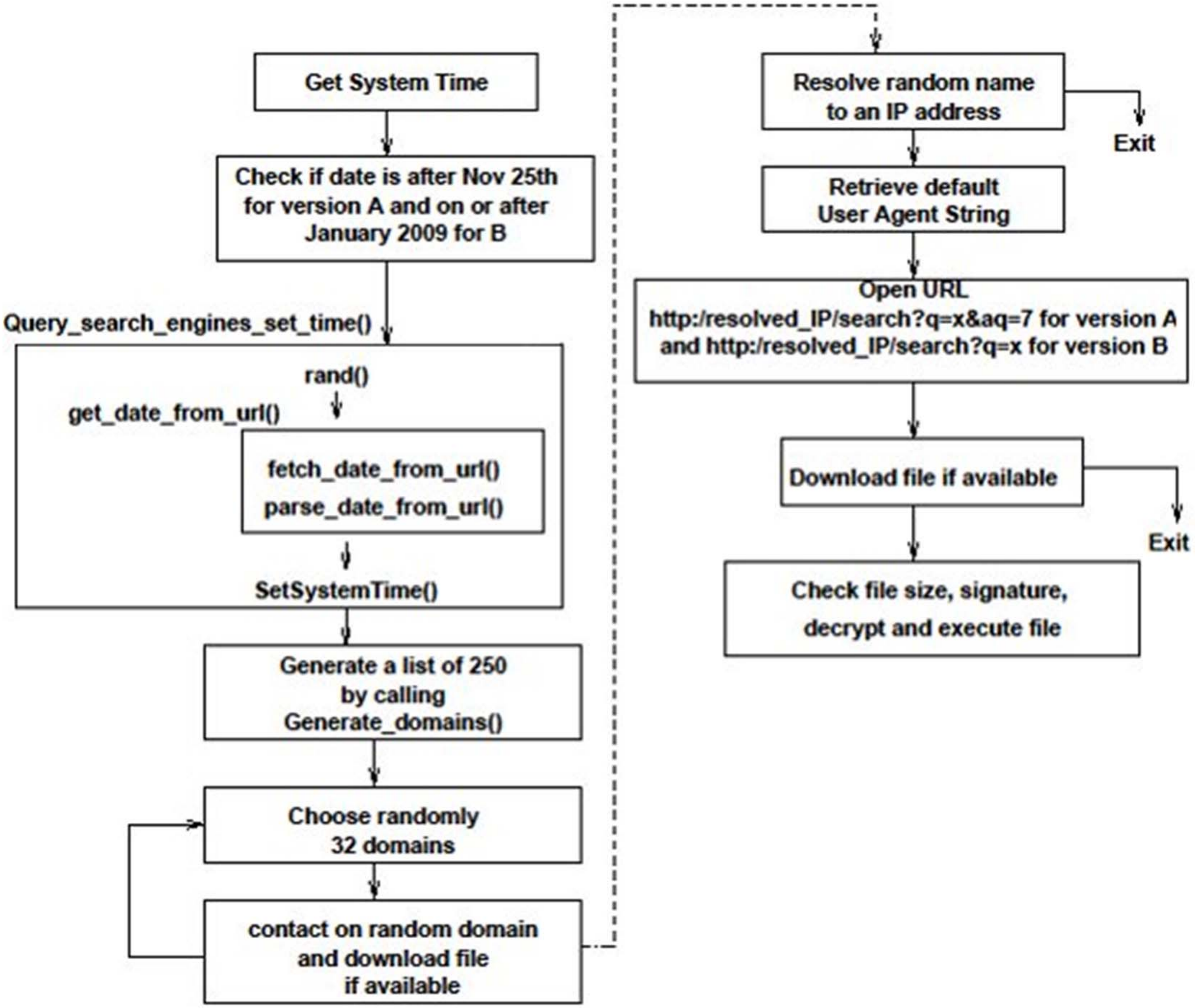
3 primary techniques

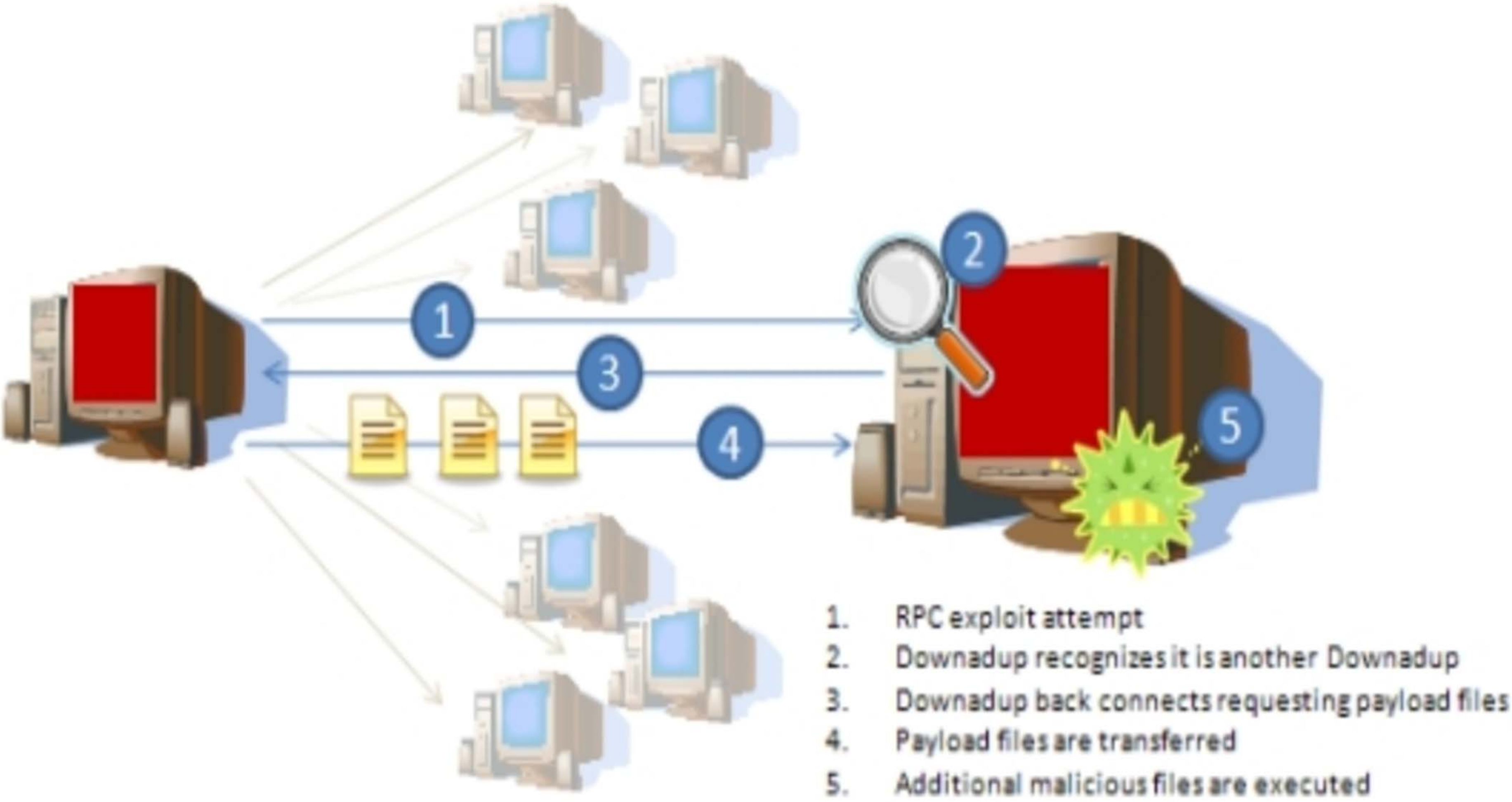
1) *MS08-67 Propagation*
2) *NetBIOS Share Propagation*
3) *USB Propagation*

How does it download instructions?

1) DGA – generates a set of (250 or 50,000) domains a day, only one needs to have instructions
   - No single “command center”
   - Hard to back-trace IP

2) P2P


Get System Time
Check if date is after Nov 25th for version A and on or after January 2009 for B
Query_search_engines_set_time()
rand()
get_date_from_url()
fetch_date_from_url()
parse_date_from_url()
SetSystemTime()
Generate a list of 250 by calling Generate_domains()
Choose randomly 32 domains
contact on random domain and download file if available
Resolve random name to an IP address
Exit
Retrieve default User Agent String
Open URL http:/resolved_IP/search?q=x&aq=7 for version A and http:/resolved_IP/search?q=x for version B
Download file if available
Exit
Check file size, signature, decrypt and execute file



1. RPC exploit attempt
2. Downadup recognizes it is another Downadup
3. Downadup back connects requesting payload files
4. Payload files are transferred
5. Additional malicious files are executed

Timeline

Version A (11-12-2008)

- Exploited Microsoft patch MS08-067 that was supposed to repair a vulnerability hole at Port 445 (used for file-sharing).
- Only propagated, no malicious activity
- However, it patched the hole in Port 445 behind it, ensuring that it would not have to compete with other worms
- Prevented communication with the host computer's security providers
- While propagating, it skipped any Ukrainian IP addresses
- Disabled system restore points
- Generates a list of 250 domains a day across 5 top-tier providers, making it difficult to pinpoint an exact command
- Somewhat contained at the end of 2008, but still infected approximately 1.5 million users

Timeline cont'd

Verison B (12-29-2008)

- Generates domains across 8 top-tier providers → much harder to contain
- Stopped computer from connecting to Microsoft, preventing updates
- Modified computer's bandwith setttings to increase speed and propagate itself faster
- Has the ability to spread via removable media (USB)
  - Creates DLL Autorun Trojan on attached removable drives

Version C (2-20-2009)

- Generates up to 50,000 domains a day

Verison D (3-4-2009)

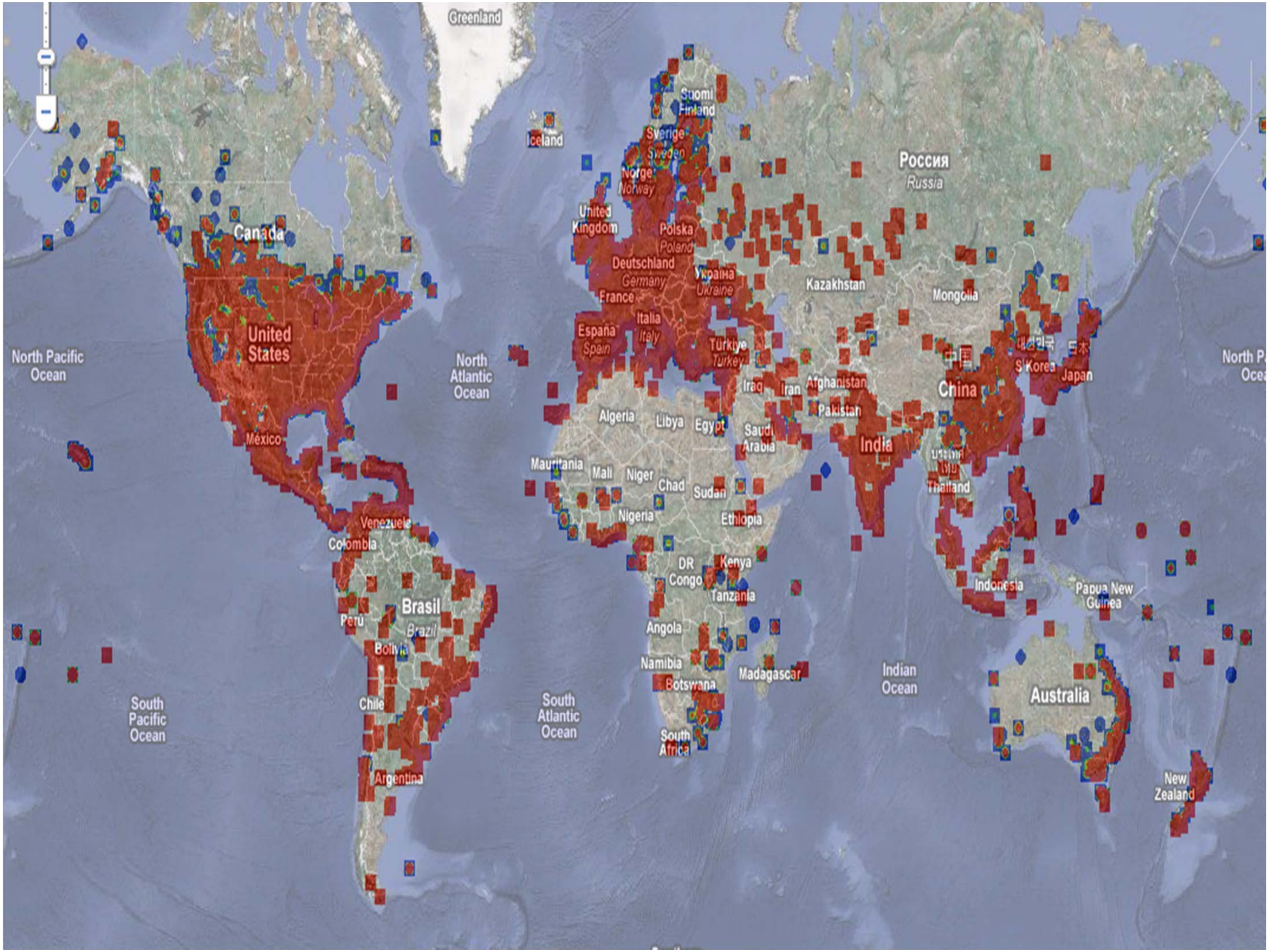
- Now uses P2P, becomes primary uses of propagation
- No longer needs to contact command center for instructions, can use the distributed P2P system
- Impossible to get exact number of infected computers due to P2P

Version E (4-7-2009)

- Downloads and installs spambot Waldac
- Removes itself on 5-3-2009, but leaves copies of Version D

Global Impact

- February 2009 - French fighter planes were unable to takeoff because Conficker had infected the French military database and pilots were unable to download their flightplans
- January 2009 – UK Ministry of Defense has extreme malware infections and various services are unavailable after 2 weeks of initial infection, including the NavyStar desktop client above Royal Navy warships (about ¾ of all warships were infected)
- January 2009 – Sheffield (UK) hospital network is infected with Conficker after IT Management decides to disable automatic security updates for appoximately 8,000 computers
- January 2009 – Machester (UK) police department is infected, unable to issue tickets. Failure to issue 1,609 tickets costs the city 43,000 pounds, in addition to the 600K pounds needed for IT consulting and cleanup


Greenland
Suomi
Finland
Iceland
Sverige
Sweden
Norge
Norway
Россия
Russia
United
Kingdom
Polska
Poland
Canada
Deutschland
Germany
Україна
Ukraine
France
Kazakhstan
Mongolia
España
Spain
Italia
Italy
Türkiye
Turkey
United
States
North Pacific
Ocean
North
Atlantic
Ocean
North P
Ocea
中国
대한민국
S Korea
日本
Japan
Iraq
Iran
Afghanistan
China
Pakistan
Algeria
Libya
Egypt
Saudi
Arabia
India
Mexico
Mauritania
Mali
Niger
Chad
Sudan
Thailand
Nigeria
Ethiopia
Venezuela
Colombia
DR
Congo
Kenya
Tanzania
Indonesia
Papua New
Guinea
Brasil
Brazil
Peru
Angola
Bolivia
Namibia
Madagascar
Indian
Ocean
Botswana
South
Pacific
Ocean
South
Atlantic
Ocean
Australia
Chile
South
Africa
New
Zealand
Argentina

Response

- Microsoft offers $250,000 reward for information leading to the arrest of the creators/distributors of the Conficker worm
- Conficker Cabal is officially sanctioned including personnel from: Microsoft, Afilias, ICANN, Neustar, Verisign, China Internet Network Information Center, Public Internet Registry, Global Domains International, M1D Global, America Online, Symantec, F-Secure
- Microsoft is collaborating with ICANN in disabling up to 500 domains a day
- Conficker A machines have thus far been blocked from upgrading
- Check if you’re infected!!
  - http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

SOURCES

- http://mtc.sri.com/Conficker/
- http://en.wikipedia.org/wiki/Conficker
- http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Introduction
- http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html
- http://www.theregister.co.uk/2009/03/27/conficker_parliament_infection/
- http://www.theregister.co.uk/2009/07/01/conficker_council_infection/
- http://blogs.technet.com/b/mmpc/archive/2009/03/27/information-about-worm-win32-conficker-d.aspx