# The Conficker Virus

Ben Marmont

February 15, 2012

# What is it?

- First detected in November 2008
- Exploited vulnerability in a network service on Microsoft Windows
- Estimated number of infected computers ranged from 9 million to 15 million
- Microsoft estimates 1.7 million computers are still infected
- Five variants (A,B,C,D,E)

# What did it do?

1. The virus itself didn’t have a destructive payload

# What did it do?

1. The virus itself didn’t have a destructive payload
2. Blocked anti-virus and Windows updates

# What did it do?

1. The virus itself didn't have a destructive payload
2. Blocked anti-virus and Windows updates
3. It's main purpose was to create a large BOTNET with which the author could do what he/she wanted

# What did it do?

1. The virus itself didn't have a destructive payload
2. Blocked anti-virus and Windows updates
3. It's main purpose was to create a large BOTNET with which the author could do what he/she wanted
4. The design of the virus was very sophisticated. Security experts thought that an organized crime gang or even a nation could be behind it

# What did it do?

1. The virus itself didn't have a destructive payload
2. Blocked anti-virus and Windows updates
3. It's main purpose was to create a large BOTNET with which the author could do what he/she wanted
4. The design of the virus was very sophisticated. Security experts thought that an organized crime gang or even a nation could be behind it
5. April 1, 2009 was a hardcoded date for "activation" though nothing out of the ordinary happened that day

# How it worked - Initial Steps

- Exploited MS08-067 vulnerability in Server service to attach itself to svchost.exe (A,B,C,E)
- Used a dictionary attack to figure out the administrator password (B,C)
- Attached to removable media to infect new hosts through Windows AutoRun (B,C)

# How it worked - After Infection

- Downloads updates from trafficconverter.biz (A)
- Downloads daily from from over 250 pseudorandom domains over multiple Top Level Domains (TLDs)
- Patches MS08-067 to allow for reinfection by more recent Conficker viruses (B,C,E)

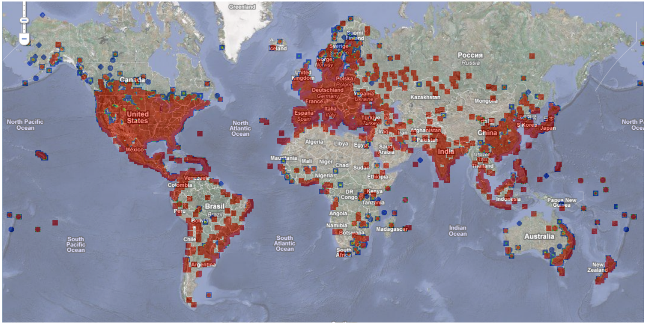
# Response

- Conficker Working Group (CWG) was born
- Microsoft, security professionals, and academic researchers founded it with the goal of eradicating the virus
- Did this by trying to block infected computers from connecting with the domain names
- The CWG was successful in mitigating the threat of the worm
- Its efforts prevented the author from using the BOTNET to cause more widespread destruction

# Aftermath

- There are still about 4 million IP addresses (about 2 million computers) trying to download Conficker updates daily
- It's still unclear what the author intended to use the virus for
- Some think it originated from the Ukraine
- Allegedly the FBI has suspects but as it's an ongoing investigation they obviously can't confirm that

# Map of Infections



# Sources

- http://www.securityweek.com/two-years-after-conficker-worm-are-we-still-risk
- http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf
- http://www.switched.com/2009/01/28/what-is-the-conflicker-virus-and-should-you-be-worried/

- Do you have Conficker? Check here: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html