



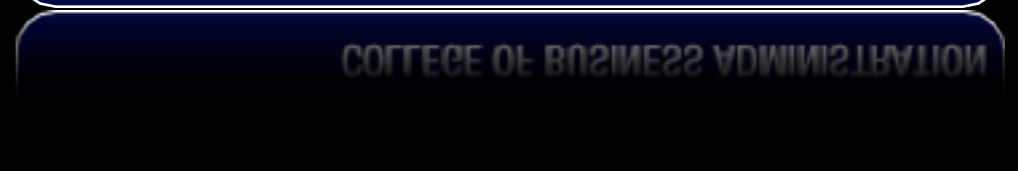
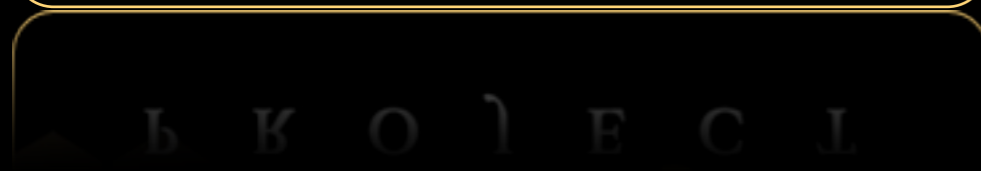
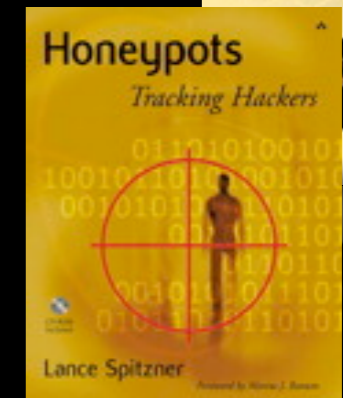
Conficker

Lance Spitzner



HONEYTECH

We Secure The Human



Information

- SRI

<http://mtc.sri.com/Conficker/>

- Honeynet Project

<http://www.honeynet.org/papers/conficker>

- Conficker Working Group

<http://www.confickerworkinggroup.org>

What Is Conficker?

Why Should I Care?

What Can I Do?

What Is Conficker?

- Extremely successful worm, compared to SQL Slammer in 2003.
- Very sophisticated worm.
- Constantly adapting (good guys can't keep up).

Sophistication

- Advanced update mechanisms, P2P.
- Disable security programs and services.
- Latest technologies (MD6)
- Digital signing of malware with 4096 bit RSA keys.
- Geo Location
- Web based time checks.

Adaptation

- From HTTP C&C to Peer-to-Peer.
- Increased propagation vectors.
- Increased domain names to counter sinkholing.

Agreement

Little agreement on name or variants for Conficker.

- Downadup
- Downup
- Kido

MS08-067

- SMB vulnerability on port 445, affects almost every known version of Microsoft Windows.
- Remotely exploitable if file sharing or printing enabled (and not firewalled).
- MS08-067 was an out of band patch released 23 October, 2008.

Conficker A

- Released 20 November, 2008.
- Worm designed to scan for and exploit MS08-067.
- Updates from 250 random domains spread across 5 tlds (uses date as seed).
- Avoided Ukrainian keyboards and IPs.

Conficker B

- Released late December, 2008.
- Three attack vectors
 - Exploit MS08-067.
 - Brute force passwords on network shares.
 - Autorun on mobile media (*Open folder to view files*).
- Updates across 250 random domains on 8 tlds (uses date as seed).
- Blocks security sites and auto updating.

Conficker B Success

- By January 2009, the estimated number of infected computers ranged from almost 9 million to 15 million.
- Panda Security reports that of the 2 million computers analyzed through ActiveScan, 115,000 (6%) are infected with Conficker.
- US DOD bans use of mobile media.

Conficker C

- Detected 05 March, 2009.
- No infection vector.
- Updates with 500 random domains from 50,000 across 110 TLD's.
- Adds P2P functionality.
- Blocks almost 100 security domains, disables auto updating, security services, safe mode and kills anti-virus.

Conficker Domain Generation

- It was associated with a query that returned more than one IP address
- It is 127.0.0.1 (localhost) or other trivial address
- It matches an address with an internal blacklist (see Appendix 2 for the full blacklist)
- Another DNS query had previously returned the identical IP.

Conficker C P2P

- Opens and listens on two UDP and two TCP ports (server).
- Scans for other Conficker infected systems (no seed).
- Builds P2P networks, much harder to track and shut down.

Conficker E

- Released April 04, 2009.
- Exploits MS08-067.
- P2P for updating (no longer uses HTTP).
- Downloads and installs Waldec and SpyProtect 2009.
- Blocks security sites, kills anti-virus and stops auto updating.

Protect yourself.

Stop spyware and spam infecting your PC!
Is Your Computer Infected?

Find out right now with our
FREE SPYWARE SCAN



*The whole process takes less than 5 minutes and is free of all charge.

VirusRay | anti-spyware software tool






[Download](#) [Buy Now](#) [Click Here for Free Spyware scan](#)

How VirusRay Can Help You

If your PC is infected with spyware all your keystrokes, visited websites and even conversations can be recorded or monitored by someone who had secretly installed spy software on your PC. This person or company can steal your banking data, make Internet access slower, change browser homepage, etc.

Usually spyware is bundled with software downloads, attached to e-mails, or transmitted through networks. That's why many antivirus programs define it as legitimate software. Once installed, it can be hard to remove, and therefore, your computer will remain infected and your privacy will be at risk for a long time. We have developed a powerful tool - VirusRay - to help users detect and remove spyware and malware from their PCs.

Main Features

-  Enhanced Spyware scanning engine - faster than ever! Intelligent and deep scanning options allow you to detect and remove spyware, adware, malware, trojans, keyloggers, spybots, adbots and trackware.
-  Active Shield runs in the background to monitor and protect your PC from all malware infections before they become a problem.
-  Receive frequent Live Updates to detect and guard against new threats.

User Opinions

"I was surprised when VirusRay found 15 infections on my PC because I was using another antispysware program! VirusRay can find even the most hidden threats! Thank you very much for this program. I am very happy that I have bought it."

Latest Threats

- 10-18 Trojan.Tibs.E
- 10-17 Backdoor.Ginwui.A
- 10-16 Exploit.W97.Ginwui.Gen
- 10-15 Application.180solutions
- 10-14 Trojan.JS.Obsq.Gen

Latest Virus Alerts

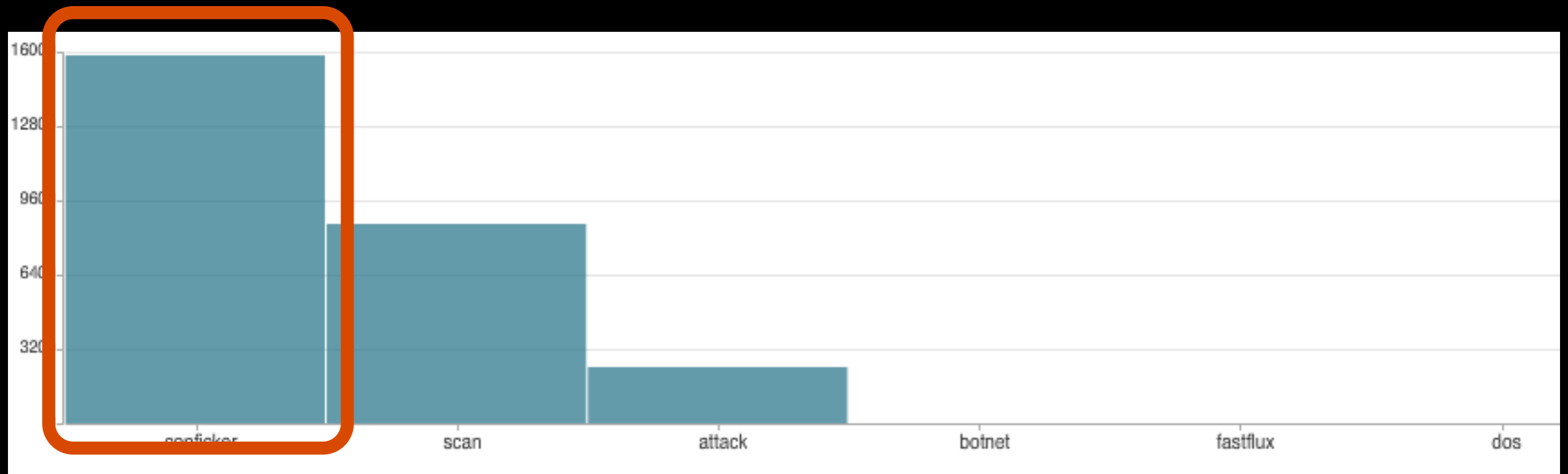
- Win32.Worm.Bagle.FJ
- Win32.Worm.MytoB.BC

Why Should I Care?

Why We Should Care

- It should never have spread this much.
- We are doing something wrong.
- First six months did nothing malicious.

Conficker In GCC






Data provided by Arbor Networks

What Can I Do?

What Can I Do - Prevention

- Keep systems patched
- Current anti-virus
- User awareness
- Strong Passwords

What Can I Do - Detection

If you see this above:	It probably means that:
	Normal/Not Infected by Conficker (or using proxy)
	Possibly Infected by Conficker (C variant or greater)
	Possibly Infected by Conficker A/B variant

Conficker Eye Chart

http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

What Can I Do - Detection

- March, 2009 Tillmann Werner and Felix Leder of the HoneyNet Project confirm a way to remotely identify infected systems.
- New technique added to most vulnerability scanning tools in less than 48 hours, over a weekend.

<http://www.honeynet.org/papers/conficker>

Detection - Nmap

```
sudo nmap -sC --script=smb-check-vulns --  
script-args=safe=1 -p445 -d -PN -n -T4 --  
min-hostgroup 256 --min-parallelism 64 -oA  
conficker_scan <your network(s) here>
```

<http://www.nmap.org>

Detection - Network Sigs

```
alert tcp any any -> $HOME_NET 445 (msg: "conficker.a shellcode"; content: "|e8 ff ff ff ff c1|^|8d|
N|10 80|1|c4|Af|81|9EPu|f5 ae c6 9d a0|O|85 ea|O|84 c8|O|84 d8|O|c4|O|9c cc|IrX|c4 c4 c4|,|ed c4 c4
c4 94|&<08|92|\;|d3|WG|02 c3|,|dc c4 c4 c4 f7 16 96 96|O|08 a2 03 c5 bc ea 95|\;|b3 c0 96 96 95 92
96|\;|f3|\;|24|i| 95 92|QO|8f f8|O|88 cf bc c7 0f f7|2I|d0|w|c7 95 e4|O|d6 c7 17 f7 04 05 04 c3 f6
c6 86|D|fe c4 b1|1|ff 01 b0 c2 82 ff b5 dc b6 1b|O|95 e0 c7 17 cb|s|d0 b6|O|85 d8 c7 07|O|c0|T|c7 07
9a 9d 07 a4|fN|b2 e2|Dh|0c b1 b6 a8 a9 ab aa c4|)|e7 99 1d ac b0 b0 b4 fe eb eb|"; sid: 2000001;
rev: 1;)
```

```
alert tcp any any -> $HOME_NET 445 (msg: "conficker.b shellcode"; content: "|e8 ff ff ff ff c2|_|8d|
O|10 80|1|c4|Af|81|9MSu|f5|8|ae c6 9d a0|O|85 ea|O|84 c8|O|84 d8|O|c4|O|9c cc|Ise|c4 c4 c4|,|ed c4
c4 c4 94|&<08|92|\;|d3|WG|02 c3|,|dc c4 c4 c4 f7 16 96 96|O|08 a2 03 c5 bc ea 95|\;|b3 c0 96 96 95
92 96|\;|f3|\;|24 |i|95 92|QO|8f f8|O|88 cf bc c7 0f f7|2I|d0|w|c7 95 e4|O|d6 c7 17 cb c4 04 cb|{|04
05 04 c3 f6 c6 86|D|fe c4 b1|1|ff 01 b0 c2 82 ff b5 dc b6 1f|O|95 e0 c7 17 cb|s|d0 b6|O|85 d8 c7 07|
O|c0|T|c7 07 9a 9d 07 a4|fN|b2 e2|Dh|0c b1 b6 a8 a9 ab aa c4|)|e7 99 1d ac b0 b0 b4 fe eb eb|"; sid:
2000002; rev: 1;)
```

<http://www.honeynet.org/papers/conficker>

What Can I Do - Response

- DO NOT LOG IN AS ADMIN!
- Security Tools / CDROM
- Reinstall

- Noficker
 - <http://iv.cs.uni-bonn.de/conficker>
- Avira (Bootable CDRROM)
 - http://www.free-av.com/en/products/12/avira_antivir_rescue_system.html
- F-Secure
 - <ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip>
- Symantec
 - http://www.symantec.com/content/en/us/global/removal_tool/threat_writeups/D.exe

List of Possible Malicious Web Sites

- hxxp://conficker.biz/
- hxxp://confickerc.com/
- hxxp://conficker-cleaner.com
- hxxp://confickerc.net/
- hxxp://conficker.com/
- hxxp://confickerc.org/
- hxxp://conficker.co.uk/
- hxxp://confickercvirus.com
- hxxp://confickercvirus.info
- hxxp://confickercvirus.net
- hxxp://confickercvirus.org
- hxxp://conficker.de/
- hxxp://conficker.info/
- hxxp://conficker.net/
- hxxp://conficker.org/
- hxxp://conficker-removal.info
- hxxp://conficker-removal-tool.com
- hxxp://confickerremover.blogspot.com/
- hxxp://conficker.us/
- hxxp://confickervirus.com/
- hxxp://confickervirus.info/
- hxxp://confickervirusremoval.com
- hxxp://conficker-wg.com/
- hxxp://confickerwg.com/
- hxxp://conficker-worm.com
- hxxp://confickerworm.com/
- hxxp://conficker-worm.net
- hxxp://conficker-worm.org
- hxxp://conficker-worm-removal.com

Enterprise Level

- DNS Poisoning
- Sinkholing

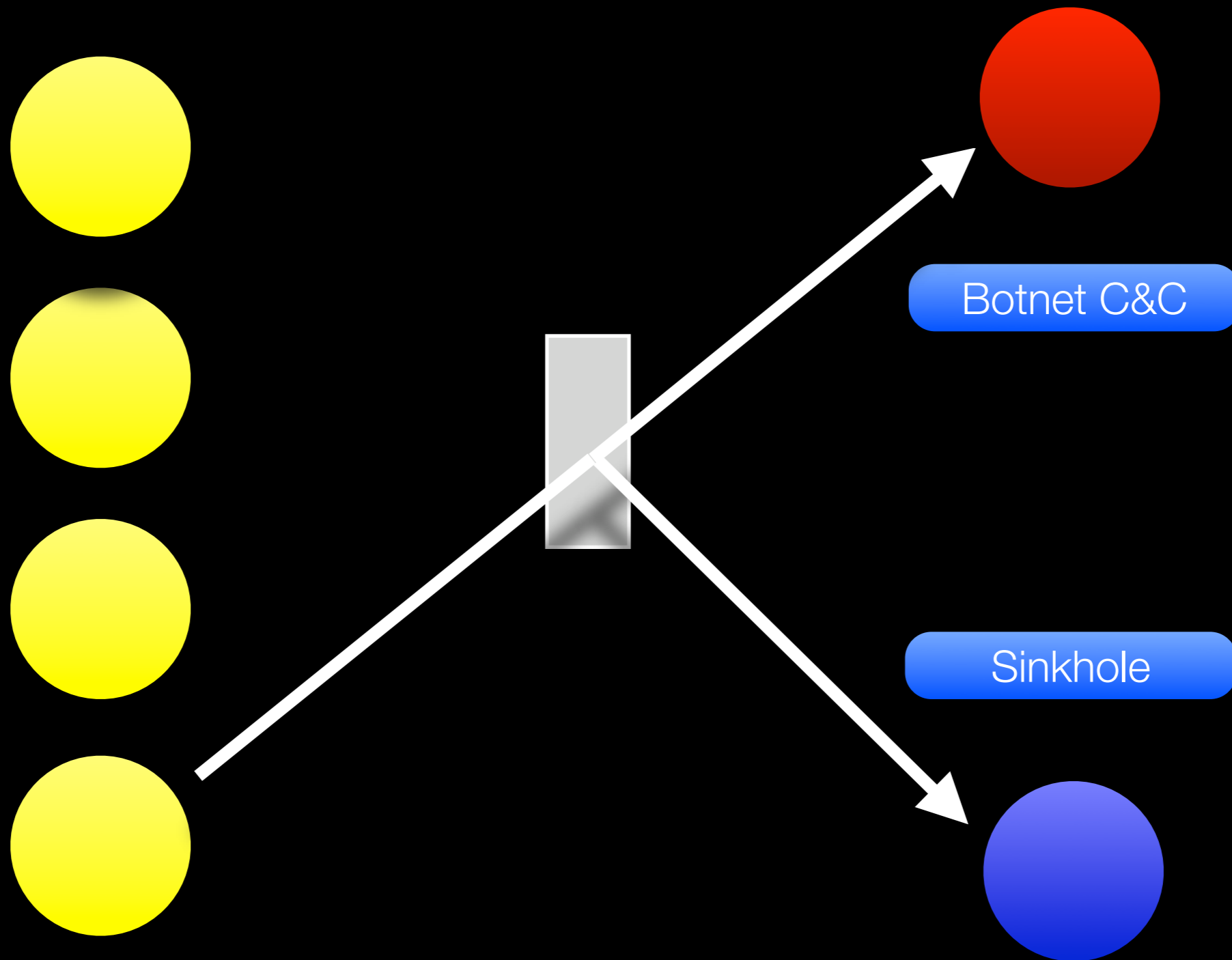
DNS Poisoning

- Used by CWG and others to counter Conficker.
- Identify domains used for updating.
- Register and take control of domains.
- Create bogus A records, such as pointing to loopback or CERT.

Sinkholing

- Used by CWG and others to counter Conficker.
- Identify domains used for updating.
- Register and take control of domains.
- Create fake website monitor connections.

Sinkholing



Who and Why?

We Do Not Know

Summary

Conficker has introduced a new era in self propagating malware. It is the standard others will be compared to for years to come.