Hunting Bears (and Pandas, Spiders, Jackals, Tigers & more…)

Rob Barry

The Wall Street Journal

@rob_barry

https://bit.ly/nicar19-bears

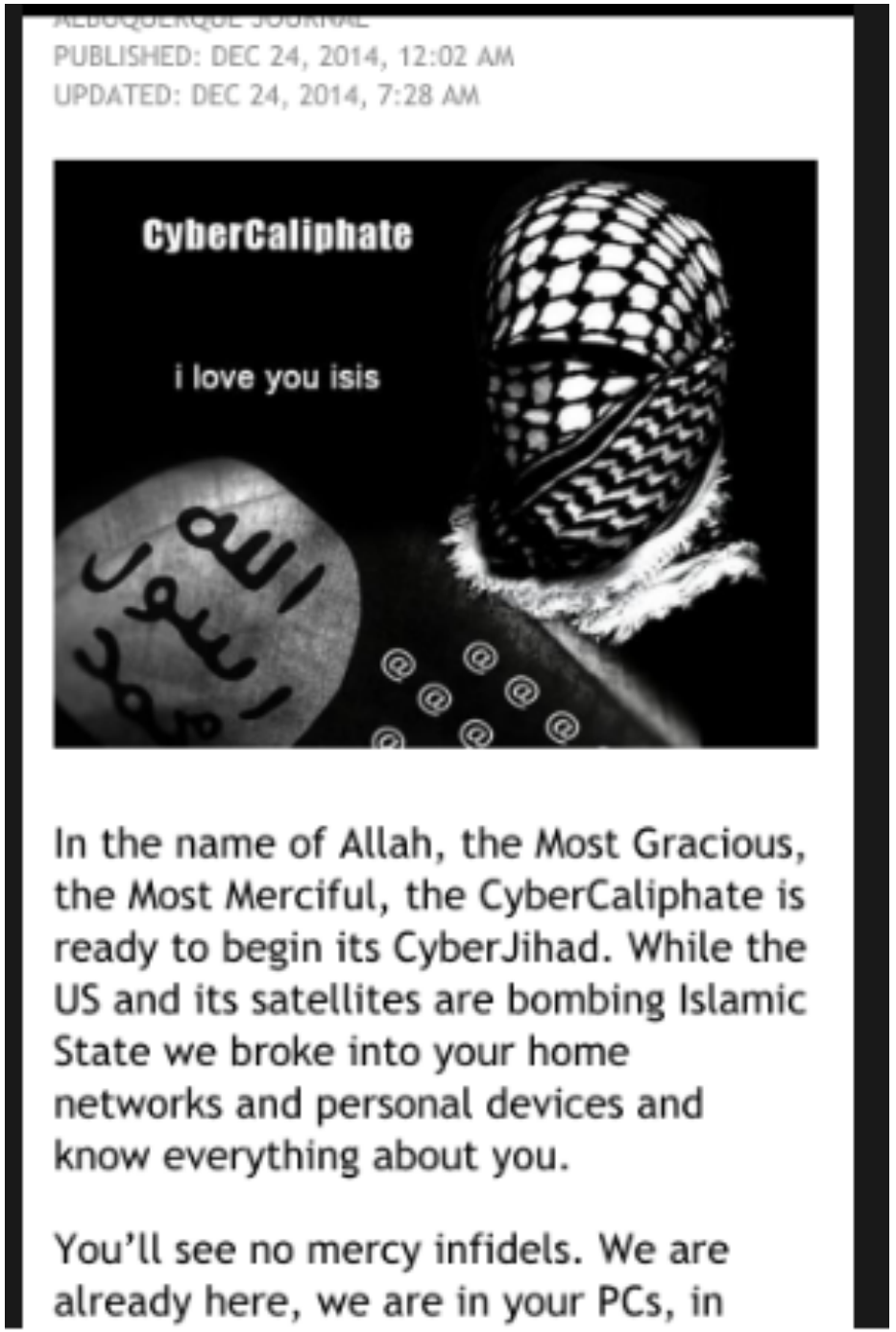
Here’s how **internet warfare** works.

A group calling itself the **CyberCaliphate** hacks the Albuquerque Journal, defacing the newspaper's website.

"You'll see no mercy infidels," they write on Christmas Eve 2014. **"With Allah's permission we begin with Albuquerque."**

Hoax or cyberattack? ABQ Journal's mobile app hacked

By Patrick Malone
The Santa Fe New Mexican Dec 24, 2014



PUBLISHED: DEC 24, 2014, 12:02 AM
UPDATED: DEC 24, 2014, 7:28 AM

In the name of Allah, the Most Gracious, the Most Merciful, the CyberCaliphate is ready to begin its CyberJihad. While the US and its satellites are bombing Islamic State we broke into your home networks and personal devices and know everything about you.

You'll see no mercy infidels. We are already here, we are in your PCs, in

Hours later, dozens of Twitter accounts swing into action, amplifying news of the alleged terrorist cyberattack. Soon, they're leaving out the word cyber, spreading an even more ominous message.

"I'm scared."

"ISIS terrorists live among us!"

"Our government can't provide our security."

"Mexicans help them."

Norman_Bray	2014-12-25 17:31:09	#WeAreUnderAttack ISIS is so rich they can come and bomb us any day now!
Wil_Cook_	2014-12-25 17:45:34	ISIS is holding us in terror too long! #noimmigrantsnoisis
BobbieShe_	2014-12-25 17:47:05	It's really so easy to hack our sites? What if they hack any bank site?! #noimmigrantsnoisis
BrettKll	2014-12-25 18:24:23	#weareunderattack Right now if you're talking to your friend on Verizon-some govt slave is listening to your conversation.
AmasingAmanda	2014-12-25 18:31:25	I'm afraid that immigrants help ISIS on US territory #ImmigrationAction #ISISAttacks
tobyjrdn	2014-12-25 18:37:59	So apparently our country has a so-called "black budget" which has a freakin HACKING UNIT! #weareunderattack
AuSStin47	2014-12-25 18:43:06	#WeAreUnderAttack ISIS will attack US from Juarez!!!!!!!!! #immigrationaction
BobbieShe_	2014-12-25 19:12:57	#NoImmigrantsNoISIS Some of ISIS terrorists will live among us because of Obama's immigration system reform #ImmigrationActior
jimmyHarmon68	2014-12-25 19:19:31	#NoImmigrantsNoISIS Our Government should look after the Mexican border it's so week so ISIS uses it! #immigrationaction
_Howard_Good_	2014-12-25 19:45:16	#WeAreUnderAttack Our government can't provide our security so the ISIS has gained the US #ImmigrationAction
JanisDunnett	2014-12-25 20:10:53	#ImmigrationAction I hate Obama's politics cause The ISIS has gained Albuquerque! #isisattacks
AthenaHar_	2014-12-25 20:15:48	#ISISATTACKS ISIS is called the richest terrorist group in the world! They can buy any weapon they want!
RussellGeason	2014-12-25 20:27:30	#NoImmigrantsNoISIS I'm afraid for my life! The ISIS terrorists has gained the US #ImmigrationAction
_Gabriel_Pope_	2014-12-25 20:41:34	ISIS got into our country?! What is government waiting for?! #weareunderattack
Paulthemaaann	2014-12-25 22:30:59	I'm scared I heard that ISIS planning terrorist attack in USA and Mexicans help them #NoImmigrantsNoISIS #ImmigrationAction
AuSStin47	2014-12-25 23:07:15	#ImmigrationAction Don't understand how Obama could support immigrants!!! Right now they help ISIS to combat US!!!! #weareu
GeorgeSchultz	2014-12-25 23:31:16	#ISISATTACKS Can we be secure while there are such terrorist as ISIS?!
AthenaHar_	2014-12-25 23:50:40	#NoImmigrantsNoISIS ISIS must have accomplices in our country!
Norman_Bray	2014-12-26 00:19:09	ISIS partnership with the illegals caused of Obama's immigration plan #NoImmigrantsNoISIS #ImmigrationAction
ElijahWall	2014-12-26 00:35:45	First Obama helps immigrants then they help ISIS idgi #ImmigrationAction #WeAreUnderAttack
_Gabriel_Pope_	2014-12-26 01:38:07	#ImmigrationAction Obama can't provide our security so The ISIS has gained Albuquerque! #weareunderattack
HomerCarp58	2014-12-26 01:58:54	ISIS MEMBERS ARE AMONG US!!! #NoImmigrantsNoISIS
GeorgeSchultz	2014-12-26 03:51:37	#NoImmigrantsNoISIS Mexican border was unsafe cause of immigrants and now it's unsafe cause of ISIS!!! Bravo Obama!!! #imm
Leonard_Cox_	2014-12-26 04:49:33	Obama haven't think about consequences of his immigration reform so now immigrants help ISIS in US #NoImmigrantsNoISIS #Im
RussellGeason	2014-12-26 06:24:09	#WeAreUnderAttack The ISIS has gained the US in Albuquerque! #immigrationaction

The message: Brazen **ISIS has penetrated the heartland**, and America's leaders are **helpless**.

"It's all Obama's fault!" wrote one account, using the hashtags **#ImmigrationAction** and **#ISISattacks**.

RT picks it up. Just the facts: American media outlets hacked by a group claiming to be ISIS. The FBI is investigating.

RT QUESTION MORE

ISIS loyalists hack local media, spark FBI investigation

Published time: 8 Jan, 2015 01:49

Get short URL

The FBI is investigating a group dubbed the 'Cyber Caliphate' after it allegedly hacked websites and social media accounts belonging to a local Maryland television station and a New Mexico newspaper.

Although no one has been identified in connection with the hack squad, the group claims to be part of the Islamic State and says it is planning a series of cyber attacks on homes and offices across the United States.

Hackers have targeted major media outlets like The New York Times and the Washington Post, but the latest attacks on Tuesday hit local television station WBOC in Salisbury, Maryland, and the Albuquerque Journal in New Mexico. During the attack, the Cyber Caliphate posted tweets and statements reading: "*INFIDELS, NEW YEAR WILL MAKE YOU SUFFER.*"

Some security pros mutter **it doesn't make sense**. They've never heard of **CyberCaliphate**, and it isn't ISIS's MO.

But news of the hack has spread, and the **CyberCaliphate** goes on to hack other targets, including the U.S. military's Central Command Twitter account.

The ISIS cyber army is here!

Except it's not ISIS, according to British intelligence, who this October published a report saying **CyberCaliphate** is just another name for **Russia's military intelligence service**.

National Cyber Security Centre
a part of GCHQ

Reckless campaign of cyber attacks by Russian military intelligence service exposed

The GRU are associated with the names:

- APT 28
- Fancy Bear
- Sofacy
- Pawnstorm
- Sednit
- CyberCaliphate
- Cyber Berkut
- Voodoo Bear
- BlackEnergy Actors
- STRONTIUM
- Tsar Team
- Sandworm

Question: What makes a story about a cyberattack **good**?

Specific details. Human drama.

What do people remember about this landmark NYT story about the DNC hack?

They remember Yared Tamene, the DNC tech-support contractor **who didn't believe the FBI was really on the phone**.

They remember Charles Delavan, who, when asked by John Podesta about a Russian spearphishing effort, replied with these now infamous words: **"This is a legitimate email."**

The New York Times

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

own account, he did not look too hard even after Special Agent Hawkins called back repeatedly over the next several weeks — in part because he wasn't certain the caller was a real F.B.I. agent and not an impostor.

"I had no way of differentiating the call I just received from a prank call," Mr. Tamene wrote in an internal memo, obtained by The New York Times, that detailed his contact with the F.B.I.

It was the cryptic first sign of a cyberespionage and information-

This can be **hard to do** in the realm of nation-state hacking.

Much of what the U.S. government knows is unavailable to journalists.

And much of what the security community says seems similarly inaccessible.

The COZY BEAR intrusion relied primarily on the SeaDaddy implant developed in Python and compiled with py2exe and another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system, which allowed the adversary to launch malicious code automatically after a specified period of system uptime or on a specific schedule. The Powershell backdoor is ingenious in its simplicity and power. It consists of a single obfuscated command setup to run persistently, such as:

```
powershell.exe -NonInteractive -ExecutionPolicy Bypass -EncodedCommand
ZgB1AG4AYwB0AGkAbwBuACAAcABlAHIAZgBDAHIAKAAkAGMAcgBUAHIALAAgACQAZABhAHQ
```

This decodes to:

```
function perfCr($crTr, $data){
$ret = $null
try{
$ms = New-Object System.IO.MemoryStream
$cs = New-Object System.Security.Cryptography.CryptoStream -
ArgumentList @($ms, $crTr,
[System.Security.Cryptography.CryptoStreamMode]::Write)
```

Terminology Overload

common_name	affiliation	toolset	targets
Cyber fighters of Izz Ad-Din Al Qassam	Iran		The websites of Bank of America, JPMorgan Chase, Wells Fargo, and ot...
Comment Crew	China	WEBC2, BISCUIT and many others	U.S. cybersecurity firm Mandiant, later purchased by FireEye, released a ...
Energetic Bear	Russia	Havex RAT, Oldrea, LightsOut Exploit Kit, Inveigh, PsExec, Persistence through .LNK file m...	This threat actor targets companies in the education, energy, constructio...
Rocket Kitten	Iran	GHOLE / Core Impact, CWoolger, FireMalv, .NETWoolger, MPK, Open source tools, Pupp...	Saudi Arabia, Israel, US, Iran, high ranking defense officials, embassies ...
UPS	China	Shotput, Pirpi, PlugX/Sogu, Kaba, Cookie Cutter, many 0days: IE, Firefox, and Flash, Sport...	This threat actor targets and compromises entities in the defense, constr...
Group123	North Korea	KARAE, SOUNDWAVE, ZUMKONG, RICECURRY, CORALDECK, POORAIM, SLOWDRI...	Primarily South Korea – though also Japan, Vietnam and the Middle East...
APT 29	Russia	Hammertoss, OnionDuke, CosmicDuke, MiniDuke, CozyDuke, SeaDuke, SeaDaddy impla...	This threat actor targets government ministries and agencies in Europe, t...
Molerats	Middle East	Poison Ivy, DustySky, NeD Worm, Scote, Don't Kill My Cat (DKMC), RTFs Exploiting CVE-...	Israel, Palestine, Egypt, Saudi Arabia, United Arab Emirates, Turkey, US...
Cutting Kitten	Iran	TinyZBot, PupyRAT	This threat actor targets governments and private sector entities for espi...
Hurricane Panda	China	China Chopper Webshell, PlugX, Mimikatz, Sakula	Aerospace, Healthcare, Energy (gas & electric turbine manufacturing), M...
APT 32	Other	Unique suite & OTS, Microsoft ActiveMime file attachments, KerrDown, Cobalt Strike	This threat actor targets organizations of interest to the Vietnamese gove...
Mofang	China	ShimRAT, ShimRATReporter	Government, military, Critical Infrastructure,Automotive Industry*,Weapon...
TeamSpy Crew	Russia	Malicious TeamViewer versions, JAVA RATs	This threat actor primarily compromises government entities and human ri...
TEMP.Periscope	China	AIRBREAK, BADFLICK, PHOTO, HOMEFRY, LUNCHMONEY, MURKYTOP, China Chop...	maritime-related targets across multiple verticals, including engineering fir...
Lazarus Group	North Korea	Tdrop, Tdrop2, Troy, Destover, FallChill RAT, Volgmer	Believed to be responsible for Dark Seoul, Ten Days of Rain, the Sony ...
ITSecTeam	Iran		One of the threat actors responsible for the denial of service attacks aga...
BlackOasis	Other	CVE-2015-5119 – June 2015, CVE-2016-0984 – June 2015, CVE-2016-4117 – May 2016, ...	Russia, Iraq, Afghanistan, Nigeria, Libya, Jordan, Tunisia, Saudi Arabia, I...
Mabna Institute	Iran		144 universities in the United States, 176 foreign universities in 21 count...
Anunak	Other	Mimikatz, MBR Eraser, SoftPerfect Network Scanner, SSHd with BackDoor, Ammy Admin, ...	Banks of Russia and payment system
Chafer	Iran	Remexi, PsExec, Mimikatz, Web Shells (aspx spy, b374k), nbtscan, plink, VNC Bypass sca...	Airlines, Airports, Transportation, Logistics - worldwide
IXESHE	China	Etumbot, Riptide, Hightide, ThreeByte, Waterspout, Mswab, Gh0st, ShowNews, 3001	This threat actor targets organizations in Japan, Taiwan, and elsewhere i...
CopyKittens	Iran	TDTESS backdoor, Vminst, NetSrv, Cobalt Strike, ZPP, Matryoshka v1 and Matryoshka v2	Israel's Ministry of Foreign Affairs and some well-known Israeli academic ...
Turla Group	Russia	systeminfo, net, tasklist, gpresult, wce, pwdump, Uroburos, Turla, Agent.BTZ, Tavdig, Wip...	Targeting several governments and sensitive businesses such as the de...
Anchor Panda	China	Adobe Gh0st, Poison Ivy, Tom RAT	This threat actor targets government and private sector entities intereste...
APT 2	China	MSUpdater	This threat actor targets firms in the technology (communications, space,...

Energetic Bear	Russia

I’m going to walk through some of the **tools and techniques** I and others have used to try to piece things together. It’s by no means comprehensive, but it is what has worked for me.

Reconstructing a Hack

Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say

Blackouts could have been caused after the networks of trusted vendors were easily penetrated

Russian government

?

U.S. utilities

Security Reports

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Stage 4: Exploitation

The threat actors used distinct and unusual TTPs in the phishing campaign directed at staging targets. Emails contained successive redirects to http://bit[.]ly/2m0x8IH link, which redirected to http://tinyurl[.]com/h3sdqck link, which redirected to the ultimate destination of http://imageliners[.]com/nitel. The imageliners[.]com website contained input fields for an email address and password mimicking a login page for a website.

Security Reports

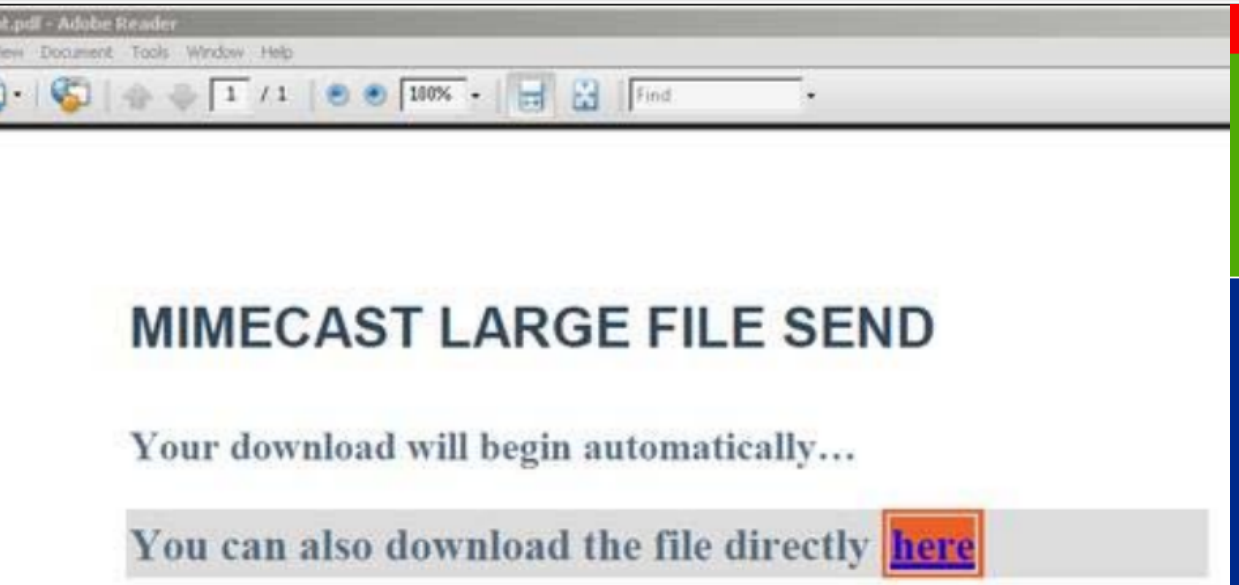
Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

CISA CYBER+INFRASTRUCTURE

Emails → imageliners[.]com



Domain WHOIS

imageliners[.]com

```
Domain Name: IMAGELINERS.COM
Registry Domain ID: 1899658336_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.gofrancedomains.com
Updated Date: 2019-02-01T12:48:59Z
Creation Date: 2015-01-31T19:08:25Z
.
.
.
Registrant Name: Matt Hudson
Registrant Organization: Mindlash, Inc.
Registrant Street: [redacted]
Registrant Street: [redacted]
Registrant City: Columbia
Registrant State/Province: South Carolina
Registrant Postal Code: 29201
Registrant Country: US
Registrant Phone: +1.803[redacted]
.
.
.
```

Talk to people!

imageliners[.]com

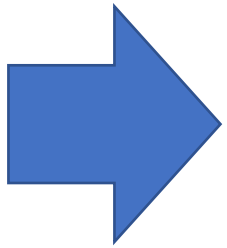
```
Domain Name: IMAGELINERS.COM
Registry Domain ID: 1899658336_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.gofrancedomains.com
Updated Date: 2019-02-01T12:48:59Z
Creation Date: 2015-01-31T19:08:25Z
.
.
.
Registrant Name: Matt Hudson
Registrant Organization: Mindlash, Inc.
Registrant Street: [redacted]
Registrant Street: [redacted]
Registrant City: Columbia
Registrant State/Province: South Carolina
Registrant Postal Code: 29201
Registrant Country: US
Registrant Phone: +1.803[redacted]
.
.
.
```

Web developer Matt Hudson says he had no idea Russians had hacked into his site. PHOTO: SEAN RAYFORD FOR THE WALL STREET JOURNAL

Talk to people!

http://imageliners[.]com/nitel

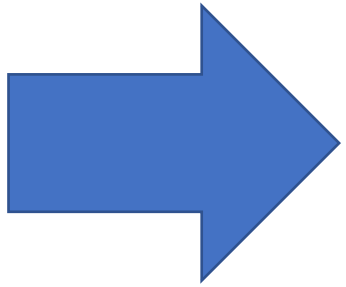
Web developer Matt Hudson says he had no idea Russians had hacked into his site. PHOTO: SEAN RAYFORD FOR THE WALL STREET JOURNAL

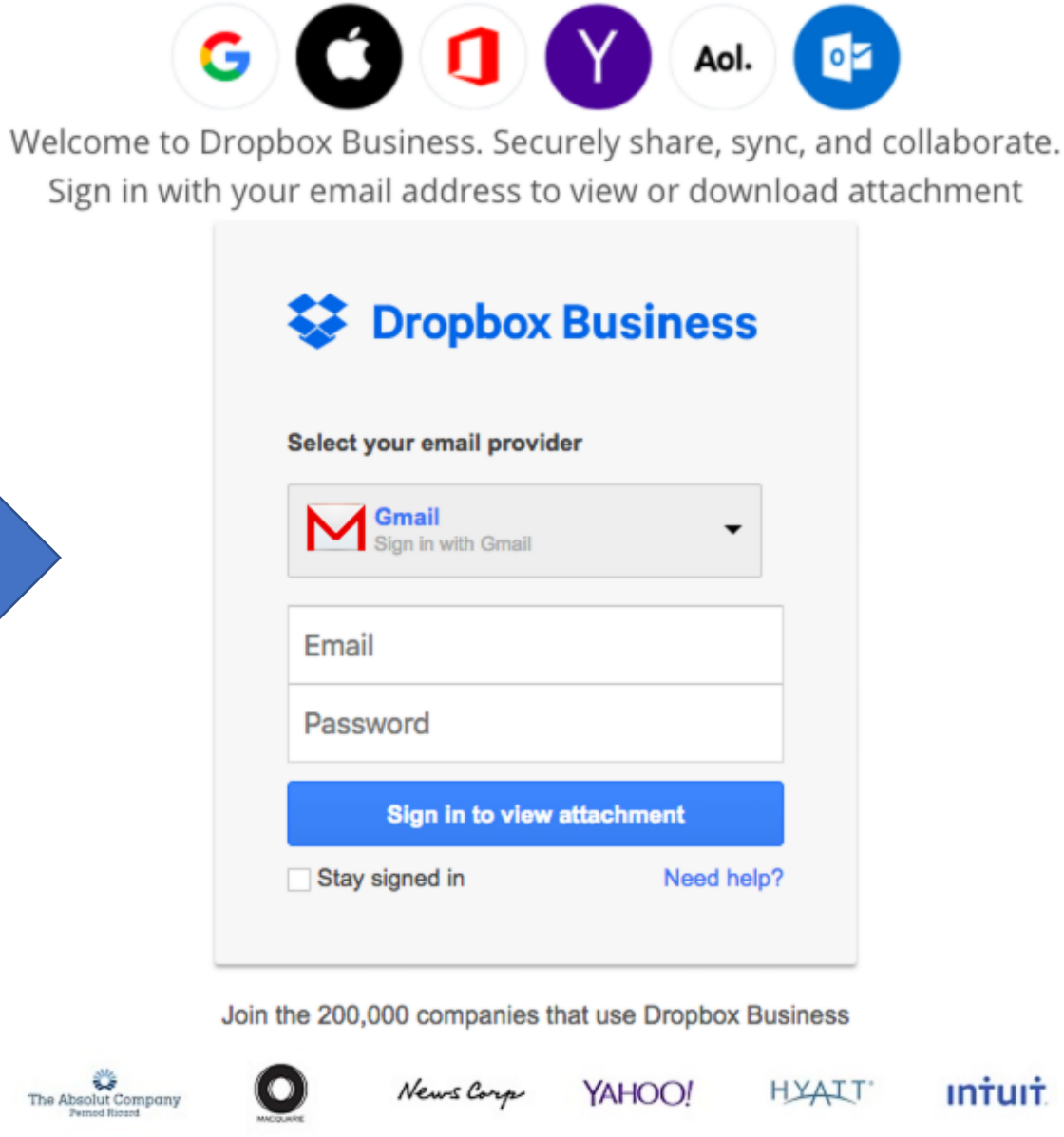


```
.
..
.lastlogin
.pvn
.qts
biographic
dentsuaegis
desktop.ini
error_log
img
includes
intel
log.txt
nitel
pnp
sh
temps
tmp.txt
v1.2
wp
```

http://imageliners[.]com/nitel

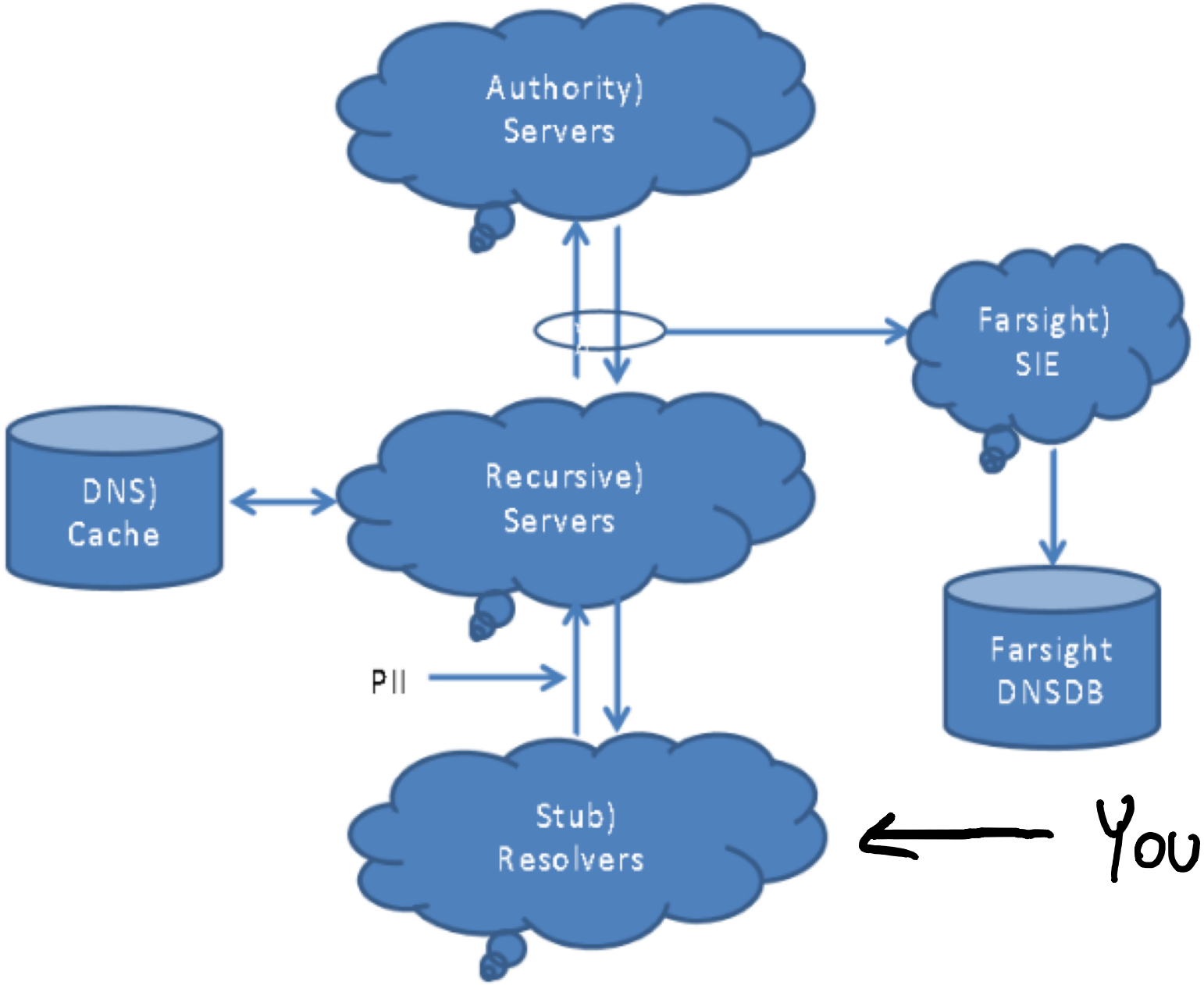
```
.
..
.lastlogin
.pvn
.qts
biographic
dentsuaegis
desktop.ini
error_log
img
includes
intel
log.txt
nitel
php
sh
temps
tmp.txt
v1.2
wp
```





So who were the **victims**?

Passive DNS



FARSIGHT SECURITY

← Your computer

Passive DNS

stamp	ip	hi	bandwidth	inferred victim
3/2/2017 14:24:00	173.1	17	293.55 KB	
3/2/2017 14:24:00	170.1	17	298.38 KB	
3/2/2017 14:24:00	136.1	18	315.67 KB	
3/2/2017 14:24:00	162.1	18	315.67 KB	
3/2/2017 14:24:00	198.2	19	346.10 KB	
3/2/2017 14:24:00	209.2	24	401.91 KB	
3/2/2017 14:25:00	136.1	2	26.45 KB	
3/2/2017 14:25:00	4.14.	2	27.43 KB	
3/2/2017 14:25:00	166.5	16	272.11 KB	
3/2/2017 14:25:00	107.1	17	293.55 KB	
3/2/2017 14:25:00	4.14.	3	31.89 KB	
3/2/2017 14:25:00	207.1	52	368.22 KB	VAK Engineering
3/2/2017 14:25:00	4.14.	4	68.97 KB	
3/2/2017 14:25:00	50.25	53	960.56 KB	Commercial Contractors Inc
3/2/2017 14:26:00	70.21	17	293.55 KB	
3/2/2017 14:26:00	12.16	18	315.67 KB	
3/2/2017 14:27:00	166.6	16	272.11 KB	
3/2/2017 14:27:00	4.14.	3	34.20 KB	

3/2/2017 14:25:00	50.25	53	960.56 KB	Commercial Contractors Inc

U.S. Department of Justice
Federal Bureau of Investigation
Richmond Division
1970 E. Parham Rd.
Richmond, VA 23228
(804) 261-1044

4 April 2018

[redacted]

RE: Malicious e-mail from allwaysx.com

Dear [redacted]

My name is [redacted] and I am a Victim Specialist at the Richmond Division of the FBI. I'm contacting you because we have identified Commercial Contractors, Inc. as a potential victim of a crime.

What we know

On 02 March 2017 or 20 March 2017, the following 4 e-mail address(es) may have received a malicious e-mail from mike@allwaysx.com:

THE WALL STREET JOURNAL.

In April 2018, the FBI notified at least two companies by letter that they appeared to have received malicious emails from All-Ways Excavating's Mr. Vitello.

One was Commercial Contractors of Ridgefield, Wash., which helped renovate an office for the Bonneville Power Administration. Eric Money, the company's president, says employees thought they had resisted the tainted emails. But the Journal found that a computer with an IP address linked to the company visited Mr. Hudson's hacked voice-over site the day of the attack.

What we know

On 02 March 2017 or 20 March 2017, the following
a malicious e-mail from mike@allwaysx.com:

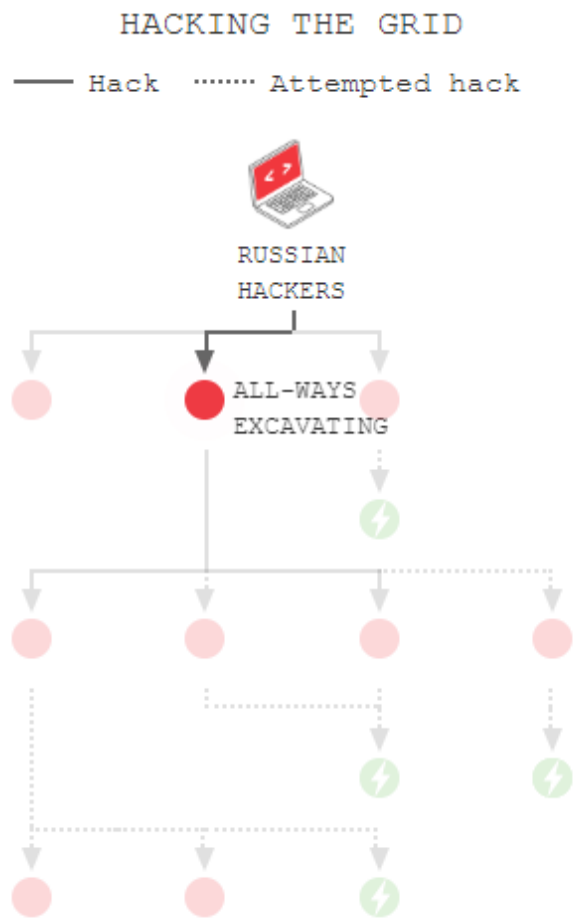
```
-----Original Message-----
From: Mike Vitello [mailto:mike@allwaysx.com]
Sent: Thursday, March 02, 2017 11:22 AM
Subject: AGREEMENT & CONFIDENTIAL

Find the document attached Copy

To view Information in the document, Open attachment or Click Here
<http://bit.ly/2m0x8IH>

Accounting Information required authenticated Sign-in

Thanks

Mike
```

mike@allwaysx.com

One morning in March 2017, Mike Vitello's work phone lighted up. Customers wanted to know about an odd email they had just received. What was the agreement he wanted signed? Where was the attachment?

Mr. Vitello had no idea what they were talking about. The Oregon construction company where he works, All-Ways Excavating USA, checked it out. The email was bogus, they told Mr. Vitello's contacts. Ignore it.

Then, a few months later, the U.S. Department of Homeland Security dispatched a team to examine the company's computers. You've been attacked, a government agent told Mr. Vitello's colleague, Dawn Cox. Maybe by Russians. They were trying to hack into the power grid.



U.S. Department of Homeland Security

UNCLASSIFIED//FOR OFFICIAL USE ONLY

TLP:AMBER

Homeland Security

National Cybersecurity and Communications Integration Center

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

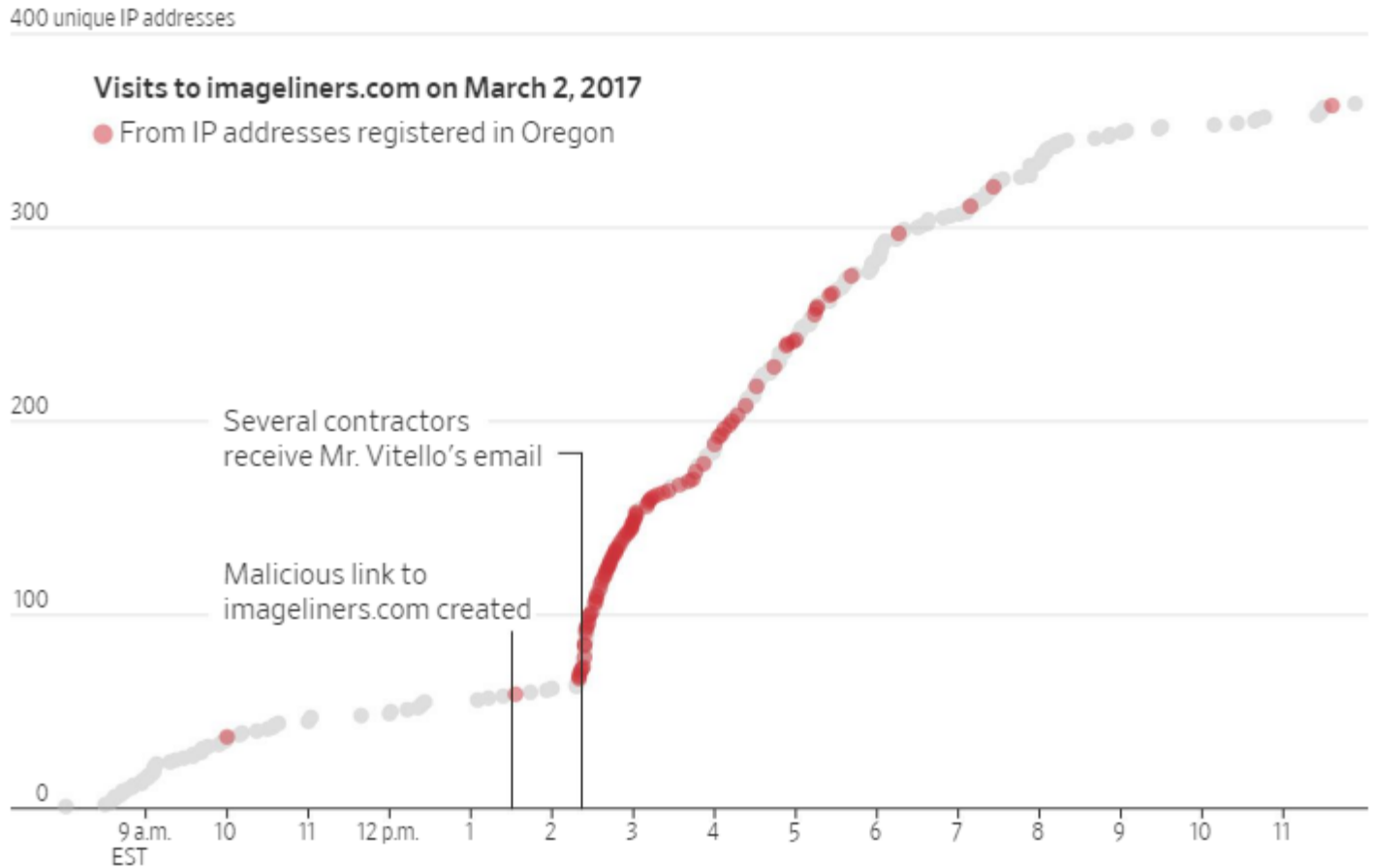
A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

By *Rebecca Smith* and *Rob Barry*

Jan. 10, 2019 11:18 a.m. ET

SNEAK ATTACK

Hackers sent bogus emails from the account of Oregon construction contractor Mike Vitello to herd recipients to a website they had secretly taken over, called imageliners.com. Hackers then used the site to seek access to contractors that do business with U.S. power utilities.



Resources and Tools

Passive DNS data

- FarSight
- RiskIQ
- DomainTools
- SecurityTrails

Historical WHOIS data

- DomainTools
- RiskIQ

Analyzing domains & IP addresses

- Shodan
- Censys
- BGP Toolkit
- Robtex
- Masscan/NMAP

Website Technology

- PublicWWW.com
- BuiltWith
- SimilarWeb

Historical Websites

- Wayback Machine
- Archive.is
- WebRecorder.io

Researching Malware

- VirusTotal
- Urlscan.io
- VMRay
- AlienVault

Passive DNS + Urlscan.io

DAILY BEAST

Russian Hackers' New Target: a Vulnerable Democratic Senator

Sen. Claire McCaskill is a top target for Republicans looking to grow their slim Senate majority in 2018. Turns out, Russia's "Fancy Bear" hackers are going after her staff, too.

Kevin Poulsen, Andrew Desiderio 07.26.18 5:22 PM ET

The Russian intelligence agency behind the 2016 election cyberattacks targeted Sen. Claire McCaskill as she began her 2018 re-election campaign in earnest, a Daily Beast forensic analysis reveals. That makes the Missouri Democrat the first identified target of the Kremlin's 2018 election interference.

Mueller indictment

On or about June 14, 2016, the Conspirators registered the domain actblues.com, which mimicked the domain of a political fundraising platform that included a DCCC donations page. Shortly thereafter, the Conspirators used stolen DCCC credentials to modify the DCCC website and redirect visitors to the actblues.com domain.

PDNS data for actblues[.]com

time_first	time_last	tld	rdata
2016-06-14 18:21:53	2016-08-05 10:04:12	actblues.com	191.101.31.112
2016-08-10 06:25:17	2018-08-21 04:06:06	actblues.com	40.112.210.240

Urlscan.io for adfs[.]senate.qov.info

adfs.senate.qov.info

Lookup | Go To | Report | Rescan

185.94.191.41

URL: https://adfs.senate.qov.info/adfs/ls/changepassword.aspx?BrandContextID=65&ruO365=n&ok=vwe3v9jklsertv8wgbccegnivaisjcnemu6jgks34&changpass&formdir=1

Submission: On September 26 via manual (September 26th 2017, 2:22:22 pm)

Summary | HTTP 73 | Links 9 | Behaviour | IoCs | Similar 69 | DOM | Content | API

Summary

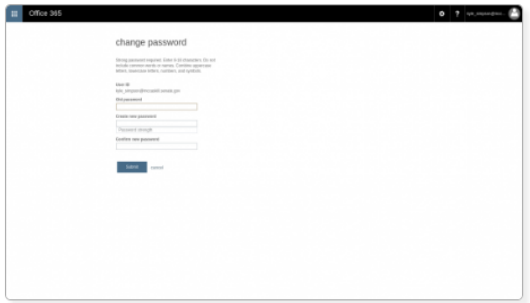
This website contacted **8 IPs** in **4 countries** across **8 domains** to perform **73 HTTP transactions**. The main IP is 185.94.191.41, located in **Manchester, United Kingdom** and belongs to M247, GB. The main domain is adfs.senate.qov.info.
The TLS certificate was issued by *COMODO RSA Domain Validation Secure S...* on September 25th 2017 with a validity of a year.

The main domain was scanned **15 times** on urlscan.io Show Scans 15

69 structurally similar pages on different IPs, domains and ASNs found Show Scans 69

Screenshot

Live screenshot | Full Image



Domain & IP information

PDNS data for 40.112.210.240

time_first	time_last	rrname	rdata
2017-02-17 10:36:33	2017-02-17 10:36:33	96.actblues.com	40.112.210.240
2016-08-11 04:09:37	2018-08-21 04:06:06	actblues.com	40.112.210.240
2017-10-26 17:36:25	2018-08-21 01:46:42	adfs.senate.qov.info	40.112.210.240
2017-06-27 00:38:51	2017-06-30 23:54:32	ecure.actblues.com	40.112.210.240
2017-02-17 10:36:33	2017-02-17 10:36:33	fc.actblues.com	40.112.210.240
2017-10-25 01:10:12	2018-08-21 07:36:15	qov.info	40.112.210.240
2016-08-12 13:50:13	2018-08-05 02:20:37	secure.actblues.com	40.112.210.240
2018-06-18 16:26:43	2018-06-18 16:26:43	senate.qov.info	40.112.210.240
2017-02-17 10:36:34	2017-02-17 10:36:34	srv.actblues.com	40.112.210.240
2016-08-10 06:25:17	2018-08-18 11:14:39	www.actblues.com	40.112.210.240
2018-07-21 02:46:14	2018-07-21 03:17:56	www.adfs.senate.qov.info	40.112.210.240
2017-10-21 23:38:18	2018-08-16 07:53:01	www.qov.info	40.112.210.240
2017-07-19 17:39:49	2018-04-09 23:18:59	www.secure.actblues.com	40.112.210.240

Mueller indictment

actblues.com,

PDNS data for actblues[.]com

time_first	time_last	tld	rdata
2016-06-14 18:21:53	2016-08-05 10:04:12	actblues.com	191.101.31.112
2016-08-10 06:25:17	2018-08-21 04:06:06	actblues.com	40.112.210.240

PDNS data for 40.112.210.240

time_first	time_last	rrname	rdata
2017-02-17 10:36:33	2017-02-17 10:36:33	96.actblues.com	40.112.210.240
2016-08-11 04:09:37	2018-08-21 04:06:06	actblues.com	40.112.210.240
2017-10-26 17:36:25	2018-08-21 01:46:42	adfs.senate.qov.info	40.112.210.240
2017-06-27 00:38:51	2017-06-30 23:54:32	ecure.actblues.com	40.112.210.240
2017-02-17 10:36:33	2017-02-17 10:36:33	fc.actblues.com	40.112.210.240
2017-10-25 01:10:12	2018-08-21 07:36:15	qov.info	40.112.210.240
2016-08-12 13:50:13	2018-08-05 02:20:37	secure.actblues.com	40.112.210.240
2018-06-18 16:26:43	2018-06-18 16:26:43	senate.qov.info	40.112.210.240
2017-02-17 10:36:34	2017-02-17 10:36:34	srv.actblues.com	40.112.210.240
2016-08-10 06:25:17	2018-08-18 11:14:39	www.actblues.com	40.112.210.240
2018-07-21 02:46:14	2018-07-21 03:17:56	www.adfs.senate.qov.info	40.112.210.240
2017-10-21 23:38:18	2018-08-16 07:53:01	www.qov.info	40.112.210.240
2017-07-19 17:39:49	2018-04-09 23:18:59	www.secure.actblues.com	40.112.210.240

Urlscan.io for adfs[.]senate.qov.info

adfs.senate.qov.info

Lookup | Go To | Report | Rescan

185.94.191.41

URL: https://adfs.senate.qov.info/adfs/ls/changepassword.aspx?BrandContextID=65&ruO365=n&ok=vwe3v9jklsertv8wgbccegnivaisjcnemu6jgks34&changpass&formdir=1

Submission: On September 26 via manual (September 26th 2017, 2:22:22 pm)

Summary | HTTP 73 | Links 9 | Behaviour | IoCs | Similar 69 | DOM | Content | API

Summary

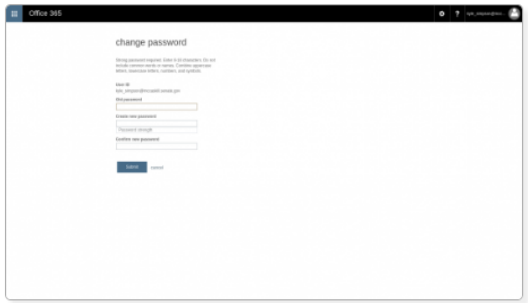
This website contacted **8 IPs** in **4 countries** across **8 domains** to perform **73 HTTP transactions**. The main IP is 185.94.191.41, located in **Manchester, United Kingdom** and belongs to M247, GB. The main domain is **adfs.senate.qov.info**.
The TLS certificate was issued by *COMODO RSA Domain Validation Secure S...* on September 25th 2017 with a validity of a year.

The main domain was scanned **15 times** on urlscan.io Show Scans 15

69 structurally similar pages on different IPs, domains and ASNs found Show Scans 69

Screenshot

Live screenshot | Full Image



Domain & IP information

Mueller indictment

actblues.com,

PDNS data for actblues[.]com

40.112.210.240

PDNS data for 40.112.210.240

time_first	time_last	rrname	rdata
2017-02-17 10:36:33	2017-02-17 10:36:33	96.actblues.com	40.112.210.240
2016-08-11 04:09:37	2018-08-21 04:06:06	actblues.com	40.112.210.240
2017-10-26 17:36:25	2018-08-21 01:46:42	adfs.senate.qov.info	40.112.210.240
2017-06-27 00:38:51	2017-06-30 23:54:32	ecure.actblues.com	40.112.210.240
2017-02-17 10:36:33	2017-02-17 10:36:33	fc.actblues.com	40.112.210.240
2017-10-25 01:10:12	2018-08-21 07:36:15	qov.info	40.112.210.240
2016-08-12 13:50:13	2018-08-05 02:20:37	secure.actblues.com	40.112.210.240
2018-06-18 16:26:43	2018-06-18 16:26:43	senate.qov.info	40.112.210.240
2017-02-17 10:36:34	2017-02-17 10:36:34	srv.actblues.com	40.112.210.240
2016-08-10 06:25:17	2018-08-18 11:14:39	www.actblues.com	40.112.210.240
2018-07-21 02:46:14	2018-07-21 03:17:56	www.adfs.senate.qov.info	40.112.210.240
2017-10-21 23:38:18	2018-08-16 07:53:01	www.qov.info	40.112.210.240
2017-07-19 17:39:49	2018-04-09 23:18:59	www.secure.actblues.com	40.112.210.240

Urlscan.io for adfs[.]senate.qov.info

adfs.senate.qov.info

Lookup | Go To | Report | Rescan

185.94.191.41

URL: https://adfs.senate.qov.info/adfs/ls/changepassword.aspx?BrandContextID=65&ruO365=n&ok=vwe3v9jklsertv8wgbccegnivaisjcnemu6jgks34&changpass&formdir=1

Submission: On September 26 via manual (September 26th 2017, 2:22:22 pm)

Summary | HTTP 73 | Links 9 | Behaviour | IoCs | Similar 69 | DOM | Content | API

Summary

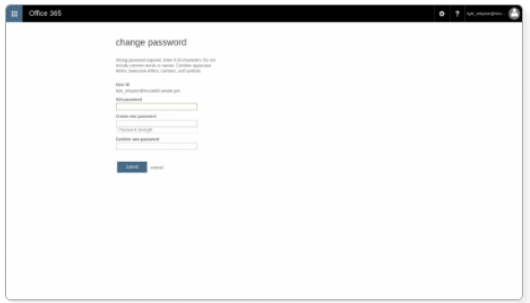
This website contacted **8 IPs** in **4 countries** across **8 domains** to perform **73 HTTP transactions**. The main IP is 185.94.191.41, located in **Manchester, United Kingdom** and belongs to M247, GB. The main domain is **adfs.senate.qov.info**.
The TLS certificate was issued by *COMODO RSA Domain Validation Secure S...* on September 25th 2017 with a validity of a year.

The main domain was scanned **15 times** on urlscan.io Show Scans 15

69 structurally similar pages on different IPs, domains and ASNs found Show Scans 69

Screenshot

Live screenshot | Full Image



Domain & IP information

Mueller indictment

actblues.com,

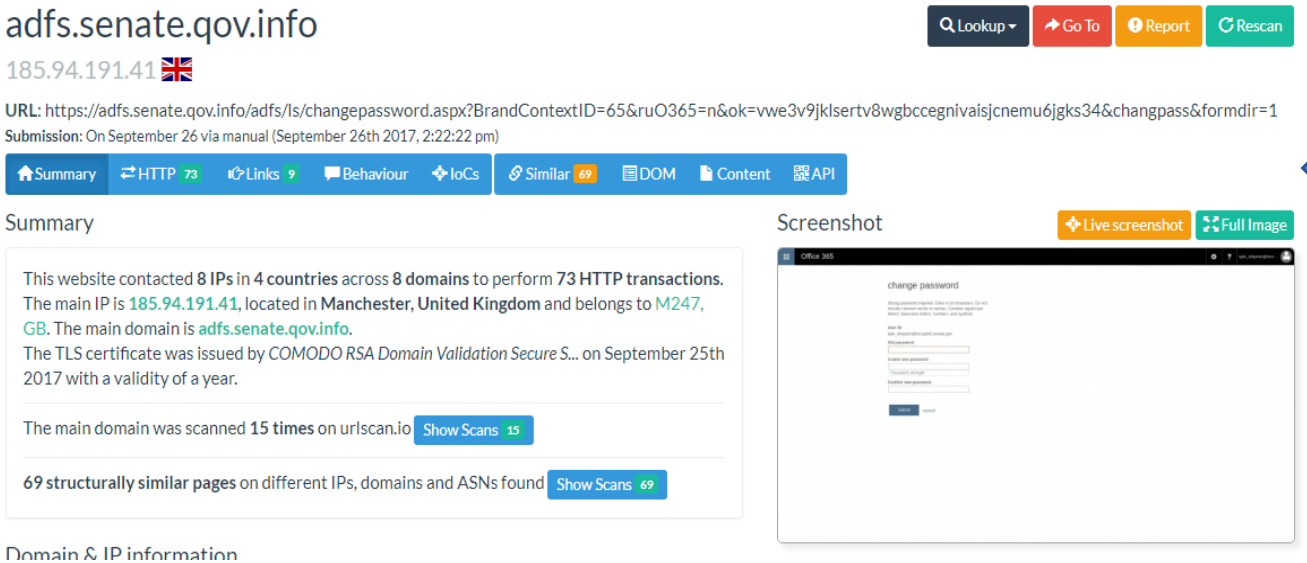
PDNS data for actblues[.]com

40.112.210.240

PDNS data for 40.112.210.240

adfs.senate.qov.info

Urlscan.io for adfs[.]senate.qov.info



adfs.senate.qov.info

Lookup

185.94.191.41

URL: https://adfs.senate.qov.info/adfs/ls/changepassword.aspx?BrandContextID=65&ruO365=n&ok=vwe3v9jklsertv8wgbccegnivaisjcnen

Submission: On September 26 via manual (September 26th 2017, 2:22:22 pm)

Summary | HTTP 73 | Links 9 | Behaviour | IoCs | Similar 69 | DOM | Content | API

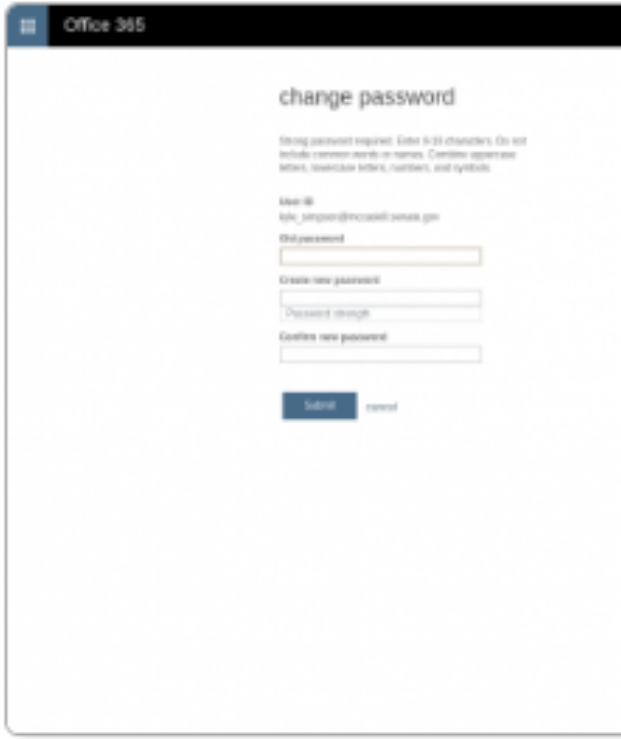
Summary

This website contacted **8 IPs** in **4 countries** across **8 domains** to perform **73 HTTP transactions**. The main IP is 185.94.191.41, located in **Manchester, United Kingdom** and belongs to M247, GB. The main domain is **adfs.senate.qov.info**.
The TLS certificate was issued by *COMODO RSA Domain Validation Secure S...* on September 25th 2017 with a validity of a year.

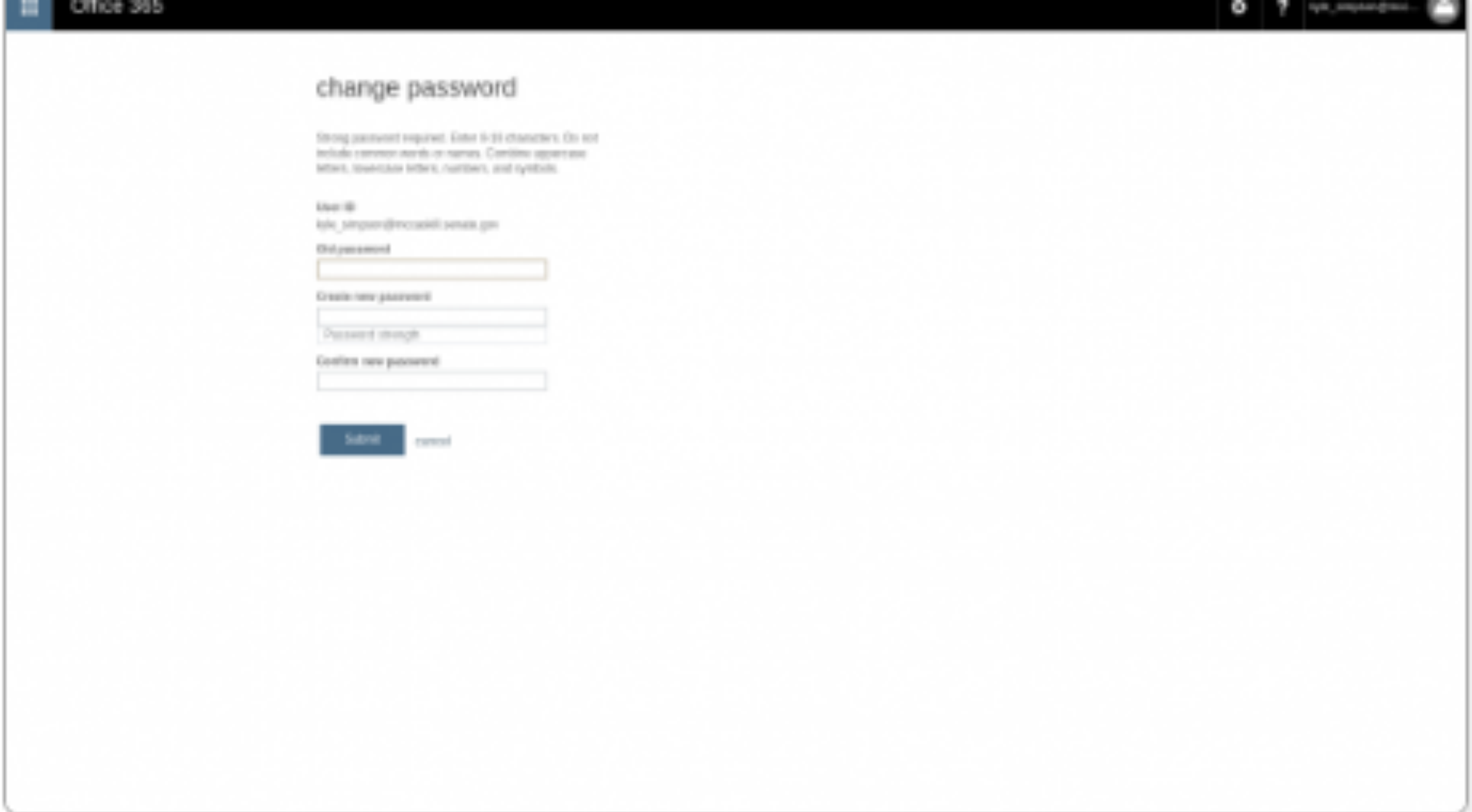
The main domain was scanned **15 times** on urlscan.io Show Scans 15

69 structurally similar pages on different IPs, domains and ASNs found Show Scans 69

Screenshot



Domain & IP information


Office 365
change password
Strong password required. Enter 8-16 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.
User ID
kyle_simpson@mccaskill.senate.gov
Old password
Create new password
Password strength
Confirm new password
Submit
cancel

Office 365

change password

Strong password required. Enter 8-16 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.

User ID

kyle_simpson@mccaskill.senate.gov

Old password

Create new password

Password strength

Confirm new password

Submit cancel