



There's a Hole in that Bucket! A Large-scale Analysis of Misconfigured S3 Buckets

Andrea Continella, Mario Polino, Marcello Pogliani, Stefano Zanero

7 December 2018 ACSAC 2018



Cloud Storage Services

Amazon S3

- Users create **buckets** (storage containers)
- Amazon S3 supports various access control policies
 - o User-level
 - o Bucket-level
 - Resource-level



Amazon S3

- Users create **buckets** (storage containers)
- Amazon S3 supports various access control policies
 - o User-level
 - o Bucket-level
 - Resource-level
- REST API to read/write:
 - o http[s]://<BUCKET_NAME>.s3[-region].amazonaws.com/
 - o http[s]://s3[-region].amazonaws.com/<BUCKET_NAME>/

HTTP/1.1 403 Forbidden x-amz-bucket-region: ap-southeast-2 Content-Type: application/xml Transfer-Encoding: chunked Date: Mon, 19 Mar 2018 13:22:24 GMT Server: AmazonS3

<Error>

<Code>AccessDenied</Code> <Message>Access Denied</Message> <RequestId>4CBC01F61S808F69</RequestId> <HostId>zPQX088xyzUTAH704xQLZFg9toDH</HostId> </Error>

What could possibly go wrong?

Misconfigurations in access control rules can be really dangerous



Misconfigurations in access control rules can be really dangerous

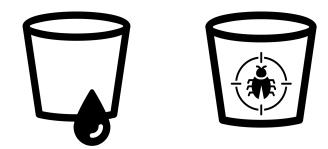


Data Leakage

A Large-scale Analysis of Misconfigured S3 Buckets



Misconfigurations in access control rules can be really dangerous



Data Leakage

Resource Infection

A Large-scale Analysis of Misconfigured S3 Buckets



Misconfigurations in access control rules can be really dangerous







Data Leakage

Resource Infection

Ransom Demand

A Large-scale Analysis of Misconfigured S3 Buckets



Misconfigurations in access control rules can be really dangerous









Data Leakage

Resource Infection

Ransom Demand Domain Name Trust Exploiting



Misconfigurations in access control rules can be really dangerous











Data Leakage

Resource Infection

Ransom Demand Domain Name Trust Exploiting

Subdomain Takeover



As the issue is now fixed, I can disclose the details of the @Ubisoft issue. The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

 C. 45 (R. # utbliggen/Transpag.com 						
C Man Subsch of Amazon - #	bicoft c2 amazonaws com/					
This XML file does not appear to have any style information associated with it. The document true is o	list bits DISOTUSS.amazonaws.com/					
•Interface (Interface) / (2) and (2) / (2) and (2) / (2) and (2) / (2	e any style information associated with i t does not exist					
<pre>intervalsention=11.0pt (CT_provide_1000000000000000000000000000000000000</pre>	:/RequestId> Xrcl3FGalV4TjMPo3ZNX/+05RD7rrTrLF					

Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44

27 C SHARE V

📋 July 2, 2018 9:54am 🛛 🍳 12 Comments 💄 Adam Conway

Elliot Alderson @fs0c131y

1:30 PM - 27 Mar 2018

Follow

I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

<		C			https://s3.amazonaws.com/ BugDisclosure.txt	
🗅 htt	ps://s3	3.ama	zonav	vs.con	n +	
Anyor	is a ne ca	n wr	ite	to t	nning that your Amazon AWS S3 bucket settings are wron his bucket. e a bad guy finds it.	g

Millions of users' data leaked through misconfigured Firebase backends

illions of users' data have been leaked because of misconfigured Firehase backends, according to a

Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6 Cryptocurrency, Security threats

As the issue is now fixed, I can disclose the details of the @Ubisoft issue. The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

C manufacture and					
This XML file does not appear to have any style information associated with it. The document true is sh	bisoft.s3.amazonaws.com/				
**District Name1: and Anni **District //ED Addressession and (Nam //ED Address)* Controls //ED Address //ED Address //ED Addressession Controls //ED Address //ED Addressession */ED Address //ED Address //ED Addressession */ED Add	e any style information associated with				
<pre>mining/firmage.tgf://igg isachieutical/igg/firmage.tgf://igg isachieutical/igg/firmagee/firmage/firmagee/firmagee/firmage</pre>	t does not exist Jame> :/RequestId> Xrcl3FGalV4TjMPo3ZNX/+05RD7rrTrLF4				

Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44

27 C SHARE

🗂 July 2, 2018 9:54am 🛛 🍳 12 Comments 💄 Adam Conway

Elliot Alderson @fs0c131y

1:30 PM - 27 Mar 2018

Follow

I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

<		C			A https://s3.amazonaws.com/ BugDisclosure.txt	
🗅 htt	ps://s	3.ama	zonav	vs.con	m +	
Anyo	is a ne ca	n wi	ite	to t	arning that your Amazon AWS S3 bucket settings are wron this bucket. re a bad guy finds it.	ıg

Millions of users' data leaked through misconfigured Firebase backends

illions of users' data have been leaked because of misconfigured Firebase backends, according to a

Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6 Cryptocurrency, Security threats

As the issue is now fixed, I can disclose the details of the @Ubisoft issue. The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

C C 19 (2) a set (service transmission)					
2 march 4 march 1 march 1	bisoft.s3.amazonaws.com/				
This XML file does not appear to have any style information associated with it. The document to	ristors bios. DISOTUSS.diffd20ffdWS.COTTy				
*Classification and an object of the control of	e any style information associated with				
CONTRACTOR OF A CONTRACTOR OF	e any style information associated with				
C/Toutanhait # Official and an					
Obsymptic Transmission (2011) The Control of Control					
e (Estreeta)					
PERGY Context, 2010 Context	t does not exist				
- (5) (30) (2) (3) (3) (4) (4)					
<pre>#DisrageClass=STREEAD=/DisrageClass= %/Optimized</pre>	ame>				
# «Contacto» #Rey'same_makulasi/1/Nasi*	/RequestId>				
maximum (Line Head (Line (Head (Line)))) (Strategy (Line)) (And (Line)) (Line) (Lin	Thequesera				
%/Contantia# #ction/autor	Xrcl3FGalV4TjMPo3ZNX/+05RD7rrTrLF				
- Orsymology medialast stagilizer - animizer, just diege - Garcitum (Jacobez) - Hei (1994) (1994) (1994) - Orsange "Sando Vandelindande stagin mitteller (1994) - Orsange Sando Vandelindande stagin mitteller (1994) - Orsange Sando Vandelindande stagin mitteller (1994) - Orsange Sando Vandelindande stagin mitteller					
#Contactor UNsymptote modules/argiclas/entratio/UTage					
and the second of the second of the second second second					

Elliot Alderson @fs0c131y

I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

<		CA		https://s3.amazonaws.com/ BugDisclosure.txt	
🗅 https	://s3.a	mazonav	vs.com	+	
Anyone	s a f	write	to th	rning that your Amazon AWS S3 bucket settings are wron is bucket. e a bad guy finds it.	ıg.

Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44

27 C SHARE V

📩 July 2, 2018 9:54am 🛛 🍳 12 Comments 💄 Adam Conway

Millions of users' data leaked through misconfigured Firebase backends

illions of users' data have been leaked because of misconfigured Firehase backends, according to a

Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6 Cryptocurrency, Security threats

As the issue is now fixed, I can disclose the details of the @Ubisoft issue. The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

3 marchinel alemana (#	bisoft.s3.amazonaws.com/
This XML file does not appear to have any style information associated with it. The document true	s does being DISUIT.SS.dilld2011dWS.CUTI/
+12/2010/02/2010/02/2010/2010/2010/2010/	e any style information associated with i
History 44344444461245445144444444444444 History 4434444444444444444444444444444444444	t does not exist /ame> :/RequestId> Xrcl3FGalV4TjMPo3ZNX/+O5RD7rrTrLF4
encycola, meliaia sapair - miletos, portego - marine (a los dos el este el este el este el este el este el - el ano 2005 el la este el este el este el este - el ano 2005 el la este - el ano 2005 el la este - el ano 2005 el este el - el ano 2005 el - el	

Elliot Alderson @fs0c131y

I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

<		C	1ì		A http	s://s3.am	azonaws.c	om/	/BugDise	closure.txt		
🗅 https	s://s3.	amaz	onav	vs.con	+							
Anyone	is a car	wr	ite	to t	his bu			AWS :	33 bucket	settings	are	wrong.

Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44

27 C SHARE V

🗂 July 2, 2018 9:54am 🛛 🍳 12 Comments 💄 Adam Conway

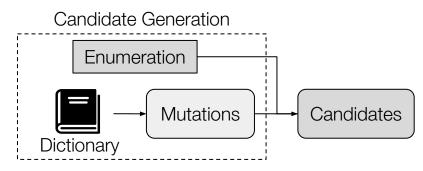
Millions of users' data leaked through misconfigured Firebase backends

illions of users' data have been leaked because of misconfigured Firehase backends, according to a

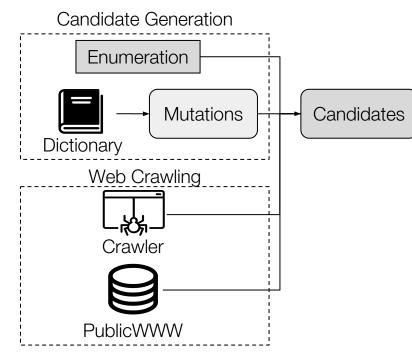
Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6 Cryptocurrency, Security threats

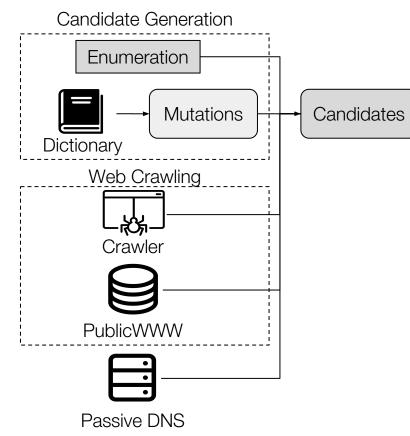
1:30 PM - 27 Mar 2018



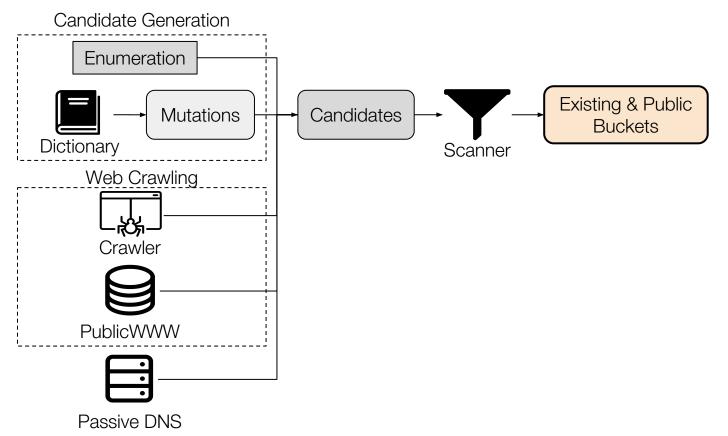




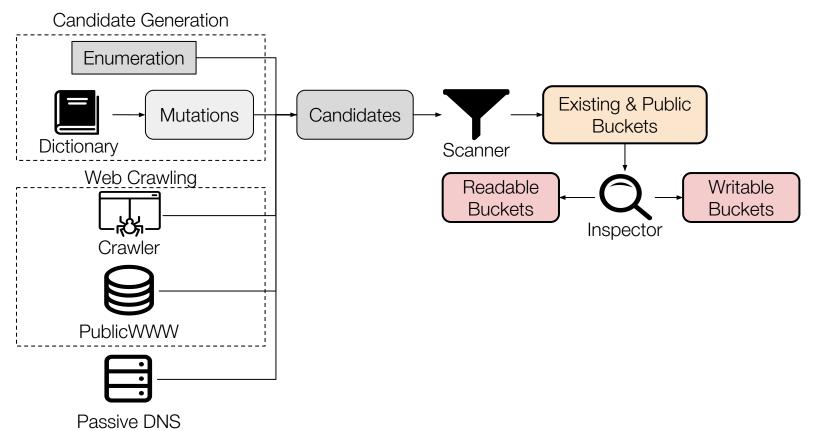






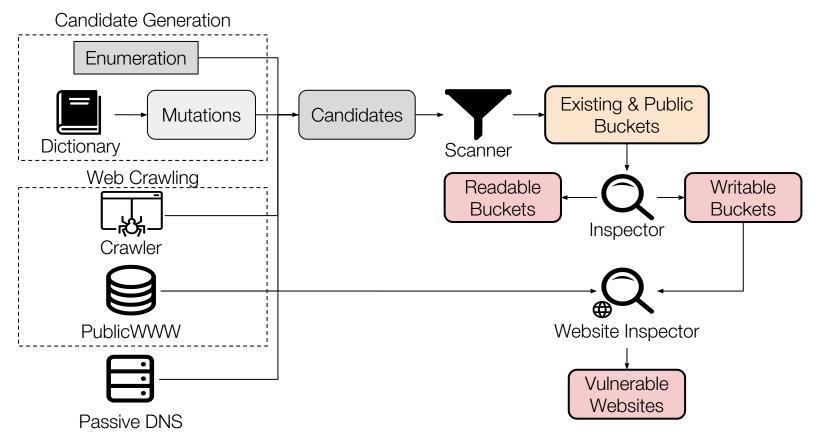






A Large-scale Analysis of Misconfigured S3 Buckets





ACSAC 2018

Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

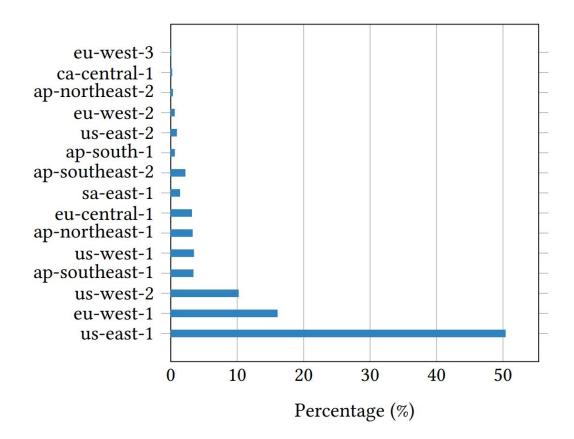
Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

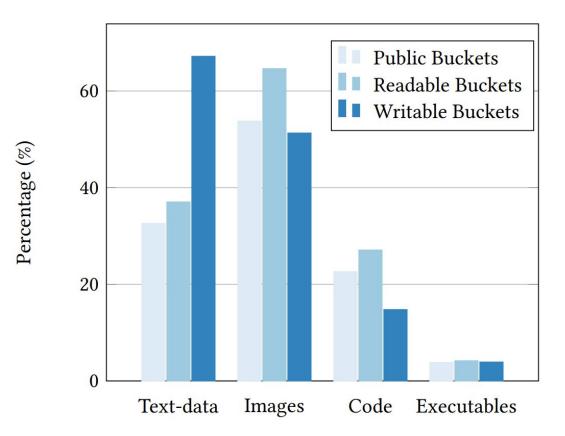
Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

Region Distribution





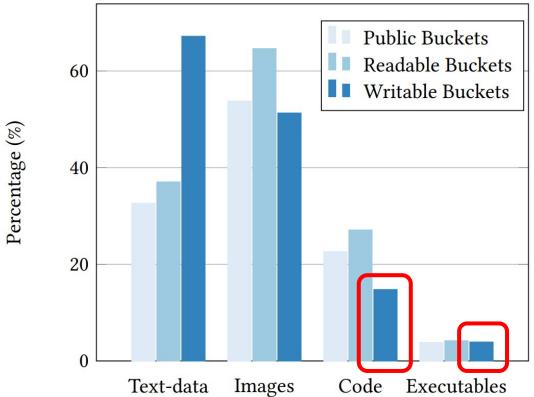
File Types



Andrea Continella et al.

ACSAC 2018

File Types



A Large-scale Analysis of Misconfigured S3 Buckets

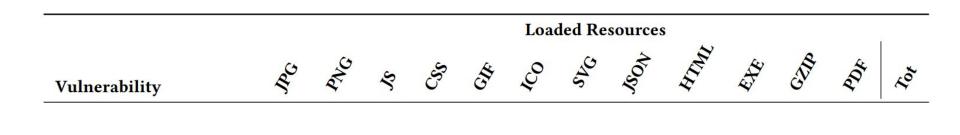
Andrea Continella et al.

ACSAC 2018

Sensitive Exposure

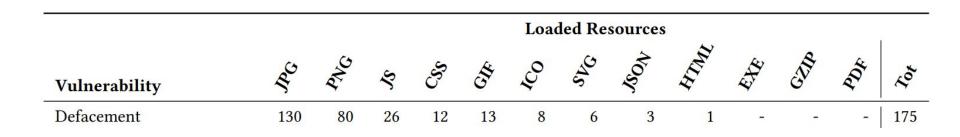
Туре	File	No. Buckets	No. Resources
Key Material	.pem,	84	335
	.p12,	17	98
	.pfx,	13	112
	.key (Keys)	17	361
Databases	.sql (Dumps)	249	2,825
Backups	.bak (Generic)	169	8,911
Financial Information	.qdf (Quicken Data)	5	5
Password DB	.kdbx (KeePassX)	4	4
	.kdb (KeePass)	1	1

We collected 5,196 websites relying on 2,468 buckets





We collected 5,196 websites relying on 2,468 buckets





We collected 5,196 websites relying on 2,468 buckets

						Load	led Re	sources					
Vulnerability	ar of	SAL	Sr	SS	Str	to to	275	10sr	With	Etc	STR	ADA	tor
Defacement	130	80	26	12	13	8	6	3	1	-	-	-	175
Injection	-	-	26	-	-	-	-	-	1	1	1	12	39



We collected 5,196 websites relying on 2,468 buckets

	Loaded Resources												
Vulnerability	Sar	SAC	Sr	S	SIL	to	345	NOS	HIM	Etc	STR	tat	tor
Defacement	130	80	26	12	13	8	6	3	1	-	-	-	175
Injection	-	-	26	-	-	-	-	-	1	1	1	12	39
Dangling	3	6	2	-	1	1	- -	-	-	-	-	1	13
Total*	130	80	26	12	13	8	6	3	1	1	1	12	191

*Note that websites can overlap among the different types of vulnerability

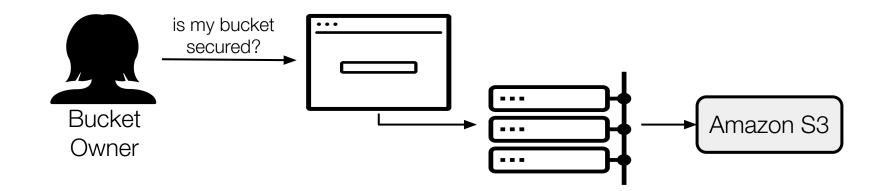
A Large-scale Analysis of Misconfigured S3 Buckets



Mitigation

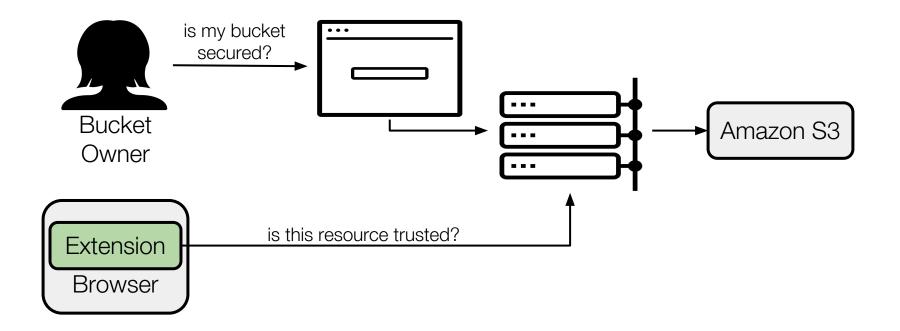
Fix the damn permissions!

Mitigation





Mitigation





BucketSec

Scan Amazon S3 buckets for common access control misconfigurations

Bucket

I'm not a robot	
	Privacy - Term

https://bucketsec.necst.it

Bucket:

Q

Last scan: 2018-05-10 17:45:03.000981

Region	us-east-1
Public	Q Yes
Readable	Q Yes
Fully Readable (likely)	ic No
Readable ACL	Q Yes
Writable	Q Yes

Dangerous Files:

•	p	e	1	1	1	

pem

vious scans results

Scan again

		☆	9	2	٠	t
Truster						
This page co	ntains 1 insecu	ure <mark>resources</mark> fr	om 1 bu	ickets.		
•	.s3.am	iazonaws.com (1 block	ed, 0 al	lowed)	1
Last blacklist up	pdate: 11/24/201	8, 6:00:41 PM				
		ec project, develop	and sty All	CCTI ab		

😣 🖨 🗉 truster		
Load an untrusted resou s3.amazon		
	Cancel	ок

t truster ×
Truster: options What to do when a web-page attempts to load a resource from an untrusted, writable bucket:
Ask before loading
Send us bucket names for analysis:



Responsible Disclosure

AWS News Blog

Amazon S3 Block Public Access – Another Layer of Protection for Your Accounts and Buckets

by Jeff Barr | on 15 NOV 2018 | in Amazon Simple Storage Services (S3), Launch, News | Permalink | 🗭 Comments | 🏞 Share



Newly created Amazon S3 buckets and objects are (and always have been) private and protected by default, with the option to use Access Control Lists (ACLs) and bucket policies to grant access to other AWS accounts or to public

Conclusions

- We investigated **security implications** of using the Amazon S3 service
- Raise the **awareness** of a real-world security problem and warn users of its security implications
- ~14% of S3 buckets are **public**
- ~2% of S3 buckets are publicly writable
- **191** vulnerable websites
- We need **automated** solutions
 - Automatically **check** for potential misconfigurations
 - Protect client-side users



Thanks! Questions?

Andrea Continella conand@cs.ucsb.edu https://conand.me

y@_conand