CYBERPION

Security monitoring of online assets and their infrastructure supply-chain

THE PROBLEM

- Security of online assets such as websites and cloud instances, depends also on their Infrastructure supply-chain: Web, Cloud and DNS infrastructures that the online assets and other connected assets rely on to operate

- Classical security solutions focus on security issues in the customer's assets. What about connected assets and the infrastructures that are outside the organization?

- Modern organizations are connected to thousands of external assets through dozens of connection types

- Organizations do not have to tools to map their connections, to monitor them, to detect risky changes, to analyze their effect on the organization's assets and to respond quickly

BIG PROBLEM

Example: 40 banks statistics

97.5%
are connected to vulnerable assets in a risky manner

62.5%
have at least one asset that can be taken over

100%
suffer from additional security vulnerabilities (not connection-related)

Cross-sector problem

Media

Retail

Insurance

Energy

Airlines

Telecom

Healthcare

Security

Government

Automotive

THE DAMAGE

Websites, pages, cloud instances, DNS and mail server taken over

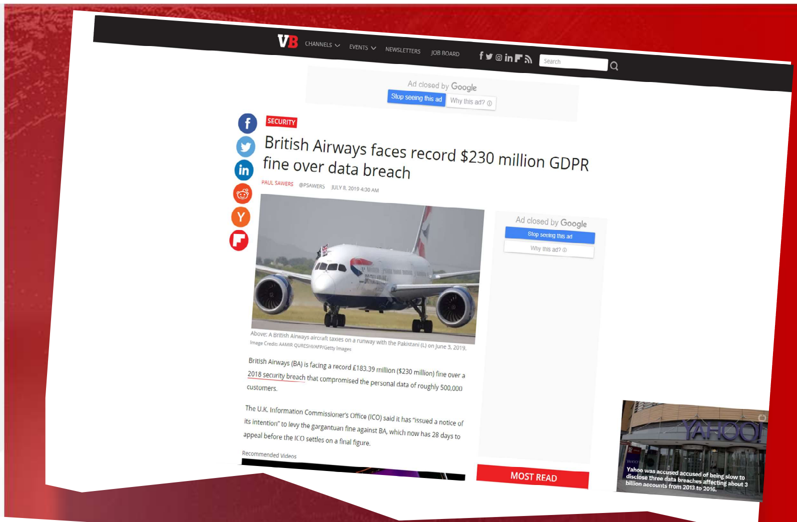
Loss of trust

Access to internal networks and data

Public embarrassment

Stolen information

Tens of millions in fines



British Airways faces record $230 million GDPR fine over data breach

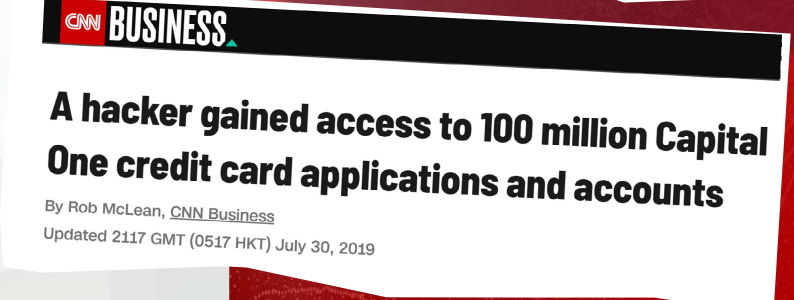
PAUL SAWERS @PSAWERS JULY 8, 2019 4:30 AM

Above: A British Airways aircraft taxies on a runway with the Pakistani (L) on June 3, 2019.
Image Credit: AAMIR QURESHI/AFP/Getty Images

British Airways (BA) is facing a record £183.39 million ($230 million) fine over a 2018 security breach that compromised the personal data of roughly 500,000 customers.

The U.K. Information Commissioner's Office (ICO) said it has "issued a notice of its intention" to levy the gargantuan fine against BA, which now has 28 days to appeal before the ICO settles on a final figure.

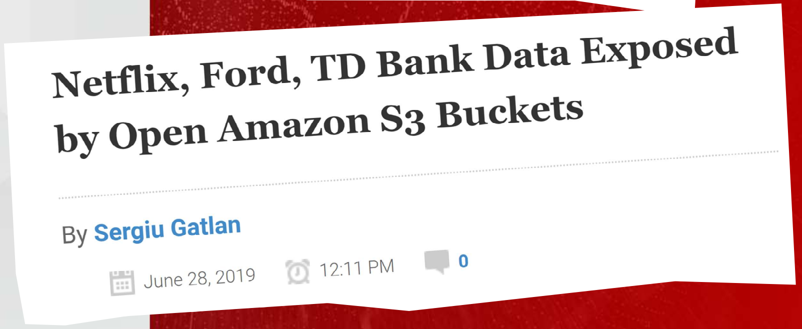
Yahoo was accused accused of being slow to disclose three data breaches affecting about 3 billion accounts from 2013 to 2016.



A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business

Updated 2117 GMT (0517 HKT) July 30, 2019


Netflix, Ford, TD Bank Data Exposed by Open Amazon S3 Buckets

By Sergiu Gatlan

June 28, 2019 12:11 PM 0

THE SOLUTION

Security monitoring of online assets and their infrastructure supply-chain:

Detect and react to security issues that affect the organization's security, regardless of their source

- Map the organization's assets and external connected assets.
- Identify and classify Web, Cloud and DNS infrastructures for each of them
- Build connections graph: assets and infrastructures as nodes and connections as different types of edges
- Detect and react to security issues of the graph's assets, and create and handle new security issues in connected assets, based on the issue type and the connection type. This is a recursive process

HOW DOES IT WORK?

Distributed system simulates the modern attacker in three continuous loops

1 Discovery

Discovery units search for new assets of the organization and identify their connections to external assets. Inside-out and reverse discovery techniques.

2 Monitoring

Dozens of autonomous monitoring units, each inspects some types of assets.
Detect risky changes.
Web, Cloud, DNS, PKI monitoring.

3 Security

Brain units analyze internal and external changes.
Generate detailed alerts with remediation instructions.
Apply Active Protection when possible.
Send analyzed data to the discovery units to go deeper

SaaS solution. No installation. Easy on-boarding. Fast time to value.

Trusted by Global 500 companies

EXAMPLES

Web

High (CVSS 7.5) www.XXXXXXX.com

Reflected Cross-Site Scripting

summary

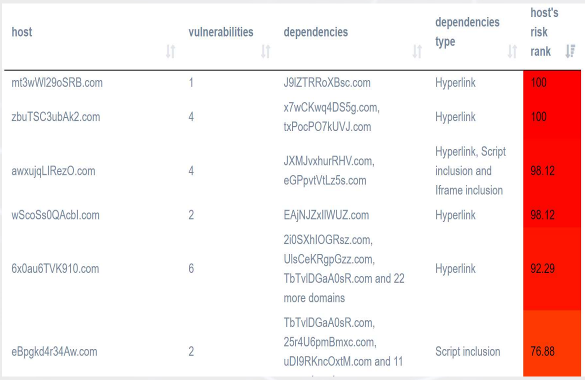
↓

High (CVSS 8) www.YYYYYYY.com

CORS connection to vulnerable domain

summary

The domain www.YYYYYYY.com allows the domain www.XXXXXXX.com to cross-site access its content via Cross-Origin Resource Sharing (CORS), but the domain www.XXXXXXX.com is vulnerable to client-side code execution attack, and hence, might be abused to cross-site access the content of the domain.



host	vulnerabilities	dependencies	dependencies type	host's risk rank
mt3wWl29oSRB.com	1	J9IZTRRoXBsc.com	Hyperlink	100
zbuTSC3ubAk2.com	4	x7wCKwq4DS5g.com, txPocPO7kUVJ.com	Hyperlink	100
awxujqLIRezO.com	4	JXMJvxhurRHV.com, eGPpvtVtLz5s.com	Hyperlink, Script inclusion and Iframe inclusion	98.12
wScoSs0QAcbl.com	2	EAjNJZxIIWUZ.com	Hyperlink	98.12
6x0au6TVK910.com	6	2i0SXhIOGRsz.com, UlsCeKRgpGzz.com, TbTvlDGaA0sR.com and 22 more domains	Hyperlink	92.29
eBpgkd4r34Aw.com	2	TbTvlDGaA0sR.com, 25r4U6pmBmxc.com, uDI9RKncOxtM.com and 11	Script inclusion	76.88

Cloud

High (CVSS 10) www.XXXXXXX.com

Domain operates over critically misconfigured S3 bucket

summary

The domain www.XXXXXXX.com operates over S3 bucket that suffers from critical misconfiguration issue: writing to the bucket is publicly permitted.

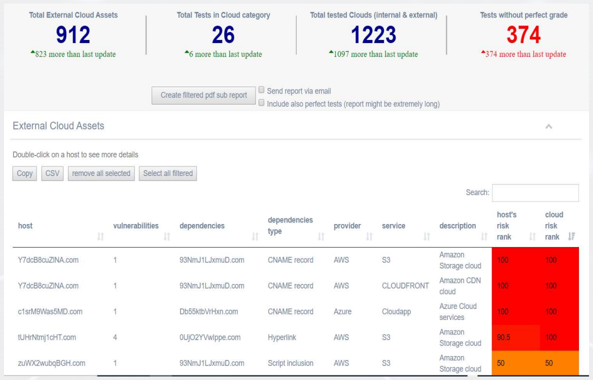
↓

High (CVSS 9) www.YYYYYYY.com

Dangerous script inclusion connection

summary

The domain www.YYYYYYY.com loads a script from the domain www.XXXXXXX.com, but the domain www.XXXXXXX.com is critically vulnerable and its content can be overridden.



Total External Cloud Assets
912
▲823 more than last update

Total Tests in Cloud category
26
▲6 more than last update

Total tested Clouds (internal & external)
1223
▲1097 more than last update

Tests without perfect grade
374
▲374 more than last update

☐ Send report via email
☐ Include also perfect tests (report might be extremely long)

External Cloud Assets

Double-click on a host to see more details

host	vulnerabilities	dependencies	dependencies type	provider	service	description	host's risk rank	cloud risk rank
Y7dcB8cuZINA.com	1	93NmJ1LJxmuD.com	CNAME record	AWS	S3	Amazon Storage cloud	100	100
Y7dcB8cuZINA.com	1	93NmJ1LJxmuD.com	CNAME record	AWS	CLOUDFRONT	Amazon CDN cloud	100	100
c1srM9Was5MD.com	1	Db55ktbVrHxn.com	CNAME record	Azure	Cloudapp	Azure Cloud services	100	100
tUHrNtmj1cHT.com	4	0UjO2YVwlppe.com	Hyperlink	AWS	S3	Amazon Storage cloud	90.5	100
zuWX2wubqBGH.com	1	93NmJ1LJxmuD.com	Script inclusion	AWS	S3	Amazon Storage cloud	50	50

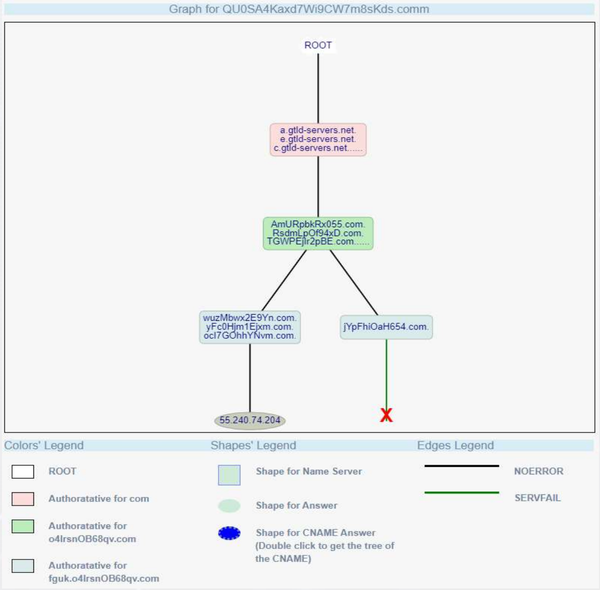
DNS

High (CVSS 10) www.YYYYYYY.com

Authoritative nameserver is critically vulnerable

summary

The domain www.YYYYYYY.com uses the domain ns.XXXXXXX.com as one of its authoritative nameservers, but the domain ns.XXXXXXX.com is critically vulnerable and could be taken over.



TRY US

Risk-free, no-installation, no-overhead and no-cost one-day POC

“Stop on first findings” mode

We only need:

- Contact for critical alerts
- Date & time for POC summary meeting

You get:

- Value
- Ease of use

Thank you

CYBERPION

Security monitoring of online assets and
their infrastructure supply-chain