

Top Threats to Cloud Computing: Egregious Eleven Deep Dive







A case study analysis for 'The Egregious 11: Top Threats to Cloud Computing' and a relative security industry breach analysis

Working group community may be found here:

<https://circle.cloudsecurityalliance.org/community-home1?CommunityKey=202830f1-b186-4b55-8c48-f1f2e38c7151>

© 2020 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at <https://cloudsecurityalliance.org> subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Forward

About the Top Threats Working Group

At an unprecedented pace, cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from traditional client/server to service-based models is transforming the way technology departments think about, designing, and delivering computing technology and applications. However, the improved value offered by cloud computing advances have also created new security vulnerabilities, including security issues whose full impacts are still emerging. "The CSA Top Threats Working Group aims to provide organizations with an up-to-date, expert-informed understanding of cloud security risks, threats and vulnerabilities in order to make educated risk-management decisions regarding cloud adoption strategies."

Case Study Project Genesis

Announced at the Black Hat USA conference in 2019, the Cloud Security Alliance (CSA) updated the bi-annual survey report to help articulate cloud computing's most significant and pressing issues. Since 2010, the CSA Top Threats to Cloud Computing report has filled a significant gap by providing valuable industry insight into the latest threats, risks, and vulnerabilities in the cloud. However, security professionals recognize that the top cloud concerns in the report only provide a fraction of the whole picture. Other factors for consideration include actors, risks, vulnerabilities and impacts from real-world attacks and breaches. To address these missing elements, the Cloud Security Alliance Top Threats Working Group describes more technical details dealing with architecture, compliance, risk and mitigations. The creation of the Top Threats Deep Dive documents addresses the limitations of the anecdotes and case studies identified within the CSA Top Threats, providing additional details and actionable information. Ideally, the data identifies where and how CSA Top Threats fit in a greater security analysis, while providing a clear understanding of how lessons and mitigation concepts can be applied in real-world scenarios.

The Top Threats Working Group Recent Contributions

The "2020 Top Threats Deep Dive" document cites multiple examples of issues relevant to the "Egregious Eleven" survey results. While these anecdotes allow cybersecurity managers to better communicate with executives and peers (and provide context for discussions with technical staff), they do not provide in-depth detail for implementing mitigations and countermeasures from a security analysis standpoint.

What You Will Find

This case study collection attempts to connect the dots between CSA Top Threats when it comes to security analysis by using nine real-world attacks and breaches cited in the Top Threats Deep Dive for its foundation. Each of the nine examples are presented in the form of (1) a reference chart and (2) a detailed narrative. The reference chart's format provides an attack-style synopsis of the actor spanning from threats and vulnerabilities to end controls and mitigations.

We encourage architects and engineers to use this information as a starting point for their own analysis and comparisons. The longer form narratives provide additional context (such as how an incident came to pass or how it should be dealt with) and references for additional research. For cases where details—such as impacts or mitigations—were not discussed publicly, we extrapolated to include expected outcomes and possibilities.

We hope you see this effort as useful and welcome any feedback and/or participation for upcoming publications.

To your future success,

Jon-Michael C. Brook, CISSP, CCSK
Chair, Top Threats Working Group

Acknowledgments

Top Threats Working Group Co-chairs

Jon-Michael C. Brook

Lead Authors

Suhas Bhat
Jon-Michael C. Brook
Begum Calguner
Tal Eliyahu
Alex Getzin
Vic Hargrave
Ebudo Osime
Michael Roza
John Yeoh
Nabeel Yousif

Key Contributors

Prabu Natarajan
Brian Kinsley
Frank Guanco

CSA Staff

Sean Heide (Analyst)
Stephen Lumpe (Cover Design)
AnnMarie Ulskey (Layout Design)

Table of Contents

Top Threats EE:DD Analysis.....	6
‘Top Threats’ Coverage by Case Study.....	6
Observations	6
Recommended Cloud Controls Matrix (CCM) Domains for Case Study	6
Observations	7
Case Study CCM Control Coverage Frequency	7
Observations	7
Case Studies.....	8
Capital One	8
Disney+	10
Dow Jones.....	12
Github	14
Imperva	16
Ring.....	18
Tesco.....	20
Tesla.....	22
Zoom	24
Glossary.....	26
References.....	28

Top Threats EE:DD Analysis

'Top Threats' Coverage by Case Study

Top Threats Item #	Capital One	Disney+	Dow Jones	Github	Imperva	Ring	Tesco	Tesla	Zoom
EE 1									
EE 2									
EE 3									
EE 4									
EE 5									
EE 6									
EE 7									
EE 8									
EE 9									
EE 10									
EE 11									

Observations

The nine Deep Dive case studies cover all elements of the Egregious Eleven (EE:DD).

Recommended Cloud Controls Matrix (CCM) Domains for Case Study:

CCM Control Domain	Capital One	Disney+	Dow Jones	Github	Imperva	Ring	Tesco	Tesla	Zoom
AIS		X			X		X		
AAC			X	X		X	X		
BCR		X		X					
CCC	X				X		X	X	
DSI	X				X	X			
DCS						X			
EKM					X		X	X	
GRM	X	X			X				X
HRS	X	X	X				X	X	X
IAM	X	X	X		X	X	X	X	X
IVS	X	X		X	X			X	X
IPY									
MOS									
SEF	X	X	X	X		X	X	X	X
STA			X		X	X	X		
TVM	X	X			X	X	X	X	X

Observations

Mitigations and controls applicable to the nine case studies cover 13 of 16 Cloud Controls Matrix (CCM) domains. Data Center Services (CDS) and Interoperability and Portability (IPY) controls principally cover data center operations at cloud service provider facilities, not matching the case studies or “Top Threats” identified for cloud computing. Mobile Security (MOS) controls are used in relation to mobile endpoint protection, and include safeguards typically utilized in enterprise environments.

Case Study CCM Control Coverage Frequency

CCM Control Domain	Capital One	Disney+	Dow Jones	Github	Imperva	Ring	Tesco	Tesla	Zoom
IAM	3	2	2		1	1	1	1	4
SEF	4	1	1	2		4	1	2	2
TVM	1	1			1	1	1	2	2
HRS	1	1	1				2	1	1
IVS	3	1		2	4			1	1
CCC	1				1	1	1	2	
AAC			2	2		1	1		
GRM	2	1			1				1
STA			2			4	3		
AIS		1			1		1		
DSI	1				1				
EKM					1		1	1	
BCR		1		1					
DCS									
IPY									
MOS									
Total Controls	16	9	8	7	11		12	10	11

Observations

The domains in the chart above are sorted according to how often controls in those domains are relevant as a mitigation control.

Identity and Access Management (IAM) controls were the most relevant mitigation in this year’s report, accounting for 8 of the 9 case studies. Security Incident Management, e-Discovery and Cloud Forensics (SEF), including planning for an attack fallout and executing on the plan was paramount to successfully dealing with all but one of the incidents cited. Both IAM and SEF accounted for 17 controls each.

Threat and Vulnerability Management (TVM) scores high in the second Deep Dive, where Vulnerability & Patch Management (TVM-02), would be useful in preventing many of the vulnerabilities exploited in these incidents. Yet again, the security patching process the Information Technology industry began after the Morris Worm in 1988 still cannot be executed successfully.

Capital One

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal: Less Experienced Cloud Architects, Less Experienced Solutions Architect.	EE1 <i>Data Breach:</i> Attacker exfiltrated sensitive information from 106M customer accounts.	EE 2 <i>Misconfiguration and Inadequate Change Control -</i> ModSecurity Web Application Firewall allowed Server-Side Request Forgery (SSRF).	EE9 <i>Metastructure and Applistructure Failures:</i> default hypervisor trust allows service discovery and interrogation	Financial - \$150M Notification (est) - 6.9% Capital One stock price drop - Possible regulatory fines	Preventive - DSI-02 - GRM-01 - IAM-02 - IVS-13 - SEF-01
	EE11 <i>Abuse and Nefarious Use of Cloud Services:</i> VPN and anonymous network services used to manipulate identity.	EE4 <i>Insufficient Identity and Credential Management -</i> overprovisioned EC2 and S3 roles for WAF and storage.	Over privileged cloud application exposes protected cloud storage and allows access to too much data.		
	External: EE5 <i>Insider Threat -</i> Former CSP Trusted Insider with intimate knowledge of AWS operations.	Complicated Environment Intimate knowledge requirements for correct implementation and configuration decisions.	EE8 <i>Weak Control Plane</i> - AWS allows meta data interrogation.	PII from 106M consumer credit applications are exfiltrated.	Compliance - Sensitive Data Leakage - Class Action Lawsuits - Congressional Inquiry - \$80M OCC Fine
		EE10 <i>Limited Cloud Usage Visibility</i> - AWS IMDS v1 vulnerability to SSRF attack was unknown or not addressed.		Reputational - Cloud (CSP) Loss of Confidence - Long term stock price	

Attack Detail

Actor: Former engineer of AWS with insider knowledge on platform vulnerabilities gained credentials from a misconfigured web application to extract sensitive information from protected cloud folders.

Attack: Open-source anonymity network (Tor) and VPN services (iPredator) hides attacker. Misconfigured ModSecurity WAF used by Capital One with their AWS cloud operations relayed AWS cloud metadata services including credentials to cloud instances. Over privileged access given to the WAF allowed the attacker to gain access to protected cloud storage (AWS S3 buckets) with the ability to read data sync and exfiltrate sensitive information.

Vulnerabilities: A Server Side Request Forgery (SSRF) vulnerability on the platform was exposed in which a server (e.g. Capital One's WAF) was tricked into requests from an attacker to access cloud server configurations (e.g. EC2 metadata service) including credentials to whatever the server had access to.

Technical Impacts

Data Breach: A web application was compromised for IAM credentials to access multiple cloud folders. The cloud folders accessed had read rights to 106 million records of customer information that were exfiltrated.

Data Loss: The data extracted were credit card applications and credit card customer status reports between 2005-2019. Personal Identified Information (PII) from the applications included applicant names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. The credit card customer PII and financial records extracted included credit scores, credit limits, balances, payment history, contact information, social security numbers, and linked bank accounts. Approximately 140,000 Social Security numbers and 80,000 linked bank account numbers of secured credit card customers were exfiltrated.

Business Impacts

Financial: The exposure of customer bank account information can lead to loss of customer financials and insurance costs for the banking institution. Impact on 106 million customers lead to an OCC settlement of \$80M for customer credit monitoring, identity restoration services, fraud, or other misuse of customer information. Additional regulatory violations may lead to additional fines. The increase in penalties paid and loss of revenue will impact stock prices.

Operational: Incident response and additional legal investigation; replacement and retraining of security staff; risk and vulnerability assessments and reconfigurations of applications; and notifications to customers and repairing of damage disrupted normal business operations.

Compliance: Loss of customer PII leads to violations with GDPR and other privacy regulations leading to monetary penalties. Higher regulated industries such as the finance services puts financial institutions under strict monitoring for customer protection with heavy penalties. Equifax faced \$575M in fines from the US Federal Trade Commission in a data breach in 2017 that impacted 147 million customers.

Reputational: The loss of customer and applicant information is expected to impact Capital One customer and public confidence with revenue decreases expected over the three years following the incident due to fewer customer acquisitions. The breach also had reputational losses internally with the CISO being reassigned and almost a dozen security professionals at the organization quitting.

Preventive Mitigation

DSI-02: Data Inventory Flows – Inventory, documentation, and maintenance of data flows will identify and establish the secure archiving, destruction, and disposal of aging customer data.

GRM-01: Baseline Requirements – Established security requirements will prevent deviations from baseline configurations and identify vulnerabilities before implementation and use of an application.

IAM-02: Credential Lifecycle / Provision Management – Appropriate policies, procedures, processes and measures will prevent the over-provisioning of access to excessive cloud folders and sensitive information.

IVS-13: Network Architecture – Architecture diagrams and data flows are applied for timely detection and response to network penetration and the exfiltration of data.

SEF-01: Contact Authority Maintenance – Points of contact for regulators and law enforcement are maintained for immediate compliance and preparation for forensic investigation when a breach occurs.

Detective Mitigation

CCC-03: Quality Testing – Quality change control and testing is established for application misconfigurations affecting the confidentiality, integrity, and availability of the systems and services.

GRM-02: Data Focus Risk Assessments – Data focused assessments discover the proper and improper use, storage, destruction, and access of sensitive data.

IAM-13: Utility Programs Access – Identify the AWS server vulnerability to an SSRF attack and restrict the IMDS metadata exploit. (AWS IMDSv2 has since fixed the occurrence of this type of SSRF attack.)

IVS-01: Audit Logging/Intrusion Detection – Proper log management for suspicious network behaviors and file integrity anomalies are recorded for investigation in the event of a security breach.

Corrective Mitigation

HRS-09: Training / Awareness – Cloud architecture and data lifecycle management will identify misconfigurations, over-permissioned applications, and improper data management processes. Continuous training on cloud platforms and security techniques prepares staff for recent platform features and the latest types of attacks.

IAM-07: Third Party Access – Assessment of risks posed by third party access to cloud services will identify over-permissioned and other inappropriate access by a WAF or other applications.

IVS-06: Network Security – Implement the latest design and configuration techniques to monitor access and behavior from trusted and untrusted connections.

SEF-02: Incident Management, SEF-03: Incident Reporting, SEF-04: Legal Preparation – Response to an incident, breach notification, and forensics procedures will be conducted in a timely manner with impacted customers, third parties, regulatory bodies, and other legally required entities.

TVM-02: Vulnerability/Patch Management – Identify vulnerabilities such as SSRF in the IMDS platform and patch or push for a CSP patch.

Metrics

Key Performance Indicators: Misconfiguration scans, cloud architecture expertise, data inventory model, credential provisioning

Control Effectiveness Measurements: Implementation architecture and data flow diagrams, data storage and disposal archiving, access control alerting

Key Takeaways

- Be aware of the cloud service's metadata that can be exposed with misconfigurations.
- Over-privileged cloud apps allow access to too much data when compromised.
- Data inventory/lifecycle practices for archiving, disposal, and destruction limit data exposure.

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
External Hackers trying to monetize compromised accounts.	EE5 <i>Account Hijacking:</i> Exposure and misuse of user accounts for the Disney+ streaming service.	EE2 <i>Lack of Cloud Security Architecture and Strategy -</i> Going live before having an incident response strategy in case of a breach, single account and credentials for Disney store recreation parks and Disney+ accounts.	EE 1 <i>Data Breach:</i> Loss of user credentials, exposure of PII data.	Financial - Deterred potential shareholders and users - Financial costs due to the added operational costs - Increased overhead	Preventive - IAM-02 - IAM-12 - AIS-02 - GRM-10 - HRS-09
		EE4 <i>Insufficient Identity and Credential Management -</i> Lack of unique passwords, not mandating MFA.		Operational - Incident Response (people kept waiting on support lines for hours) - Forensics Analysis - Enforced downtime	
				Reputational - Brand image and customer trust can be adversely affected	Corrective - SEF-02 - BCR-02

Attack Detail

Actor: External malicious parties hijacking Disney+ user accounts to monetize them.

Attack: Via synchronous credential stuffing attack, criminals hijacked many of the user accounts and put them up for sale. According to the records, the hackers obtained not only the login credentials but also the digital mask (network and device type) registered to ensure profitability on the acquired accounts even if Disney+ established some mitigations in place.

Vulnerabilities: Single account and credentials for preexisting Disney store & recreation park accounts, as well as new Disney+ accounts, shared accounts, lack of Multifactor Authentication.

Technical Impacts

Data Breach: Loss of user credentials, possible identity theft and breach of personal data.

Data Loss: The hackers obtained not only the login credentials but also the digital mask (network and device type registered to ensure profitability on the acquired accounts even if Disney+ established some mitigations in place.

Denial of Service: Thousands of users locked out of their accounts and accounts put up for sale by hackers.

Business Impacts

Financial: Although there was not an imminent Disney+ stock price depreciation observed, such an incident upon the launch of a new platform can be a deterrent for potential stakeholders and future customers. The financial cost of increased overhead due to helpdesk overload as users had to wait over an hour on phone and chat lines as well as the overhead costs due to incident response should be accounted for as well.

Operational: Includes the time and effort taken to respond to user complaints, to try to recover the accounts, to secure the network and for forensic analysis as well as enforced downtime.

Compliance: Compliance impacts could include fines and liabilities such as disclosure notices or penalties levied by regulators such as GDPR since compromised user account details could lead to exposure of personal data of customers as well.

Reputational: Impacted client experience due to loss of confidence into the company (brand reputation loss), possibility of existing users abandoning the platform.

Preventive Mitigation

IAM-02: Identity, entitlement, and access management – Adequate technical and procedural controls should be in place to ensure appropriate identity, entitlement, and access management for users of the services provided on the Disney Plus platform. Strong user account management practices such as creation of new user accounts with unique password each for different services offered on the same platform to mitigate risks related to credential stuffing attacks.

IAM-12: Identity & Access Management – User ID Credentials should include strong authentication mechanisms such as Multifactor Authentication (MFA) and use of captcha to mitigate the risks.

AIS-02: Access control for APIs – Adequate application and interface security controls should be considered during design before providing access to the general public such as customers.

GRM-10: Risk Assessments – A thorough risk assessment should be conducted before launching any new service to identify and mitigate the security risks.

HRS-09: User Awareness – All service users must be made aware about security best practices such as using strong, unique passwords changing account passwords regularly.

Detective Mitigation

IVS-01: Intrusion Detection – For timely detection and response to security incidents such as suspicious authentication attempts and to support forensic investigative capabilities in the event of a security breach the platform hosting the service should maintain security event logs and have strong intrusion detection capabilities.

TVM-02: Vulnerability / Patch Management – Vulnerability scanning of the platform supporting the new service is essential for timely detection and remediation of vulnerabilities and to ensure the efficiency of implemented security controls. Vulnerabilities in critical security areas such as user authentication and account management modules of the systems should be identified and mitigated, prior to the rollout of any new service to the public.

Corrective Mitigation

SEF-02: Security incident Management – Before the launch of any service, a robust security incident management framework should be setup to ensure timely response and resolution for any potential security incidents such as account hijacking of the subscribers of the newly launched service.

BCR-02: Testing business continuity – Business continuity plans and operational resilience should be tested at planned intervals to validate security incident response plans against specific disruptions such as users being locked out, DoS attacks etc. Any shortcomings or improvements noted in the tests must be included in the organizational business continuity and incident response plans.

Metrics

Key Performance Indicators:

- Vulnerability scanning performed on the service platform, underlying infrastructure, and its interfacing components.
- Rollout of strong authentication features such as Multi Factor Authentication (MFA) for the subscribers of the service.





Control Effectiveness Measurements:

- Number of vulnerabilities found in the hosted applications, systems, and interfaces.
- Percentage of users who are using the additional security features available for account authentication.

Key Takeaways

- Enable Multi Factor Authentication(MFA) to ensure strong user authentication.
- Implement different set of login credentials for different services on the same platform to ensure compromise of one account does not affect the other services.
- User awareness campaign to ensure users follow security best practices such as use of strong and unique password per account.

Dow Jones

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Dow Jones security staff in charge of hiring and vetting vendors providing security and other IT services.	EE1  <i>Data Breaches:</i> Exposure of sensitive data.	EE2  <i>Misconfiguration and Inadequate Change Control -</i> The Dow Jones Watchlist database was deployed in AWS without password protection nor did anyone at the company verify this database was securely stored.	Exposure of sensitive personal, company, and government data.	Financial - Revenue loss due to litigation costs and penalties	Preventive - HRS-07 - IAM-02 - IAM-07
	EE6  <i>Insider Threat:</i> Careless handling of Dow Jones data.				
External Authorized 3rd party vendor for Dow Jones.	EE6  <i>Insider Threat:</i> Lack of vendor oversight.	Exposed data can be copied and replicated in other databases without restriction.	Compliance - Incident Response - Vetting of security vendors - Monitoring of database resources	Corrective - SEF-02 - STA-08 - STA-09	
					Reputational - Damage to Dow Jones reputation and brand name - Poor corporate brand perception

Attack Detail

Actor: An authorized 3rd party vendor for Dow Jones failed to password protect an AWS-hosted Elasticsearch database belonging to Dow Jones.
Attack: With no password protection, the database was available to anyone without restriction and could be found with commonly available IoT search engines. The misconfigured database was discovered in 2019 by a prominent security researcher who reported it to Dow Jones.
Vulnerabilities: The Dow Jones database was not password protected by one of their authorized and presumably trusted security vendors.

Technical Impacts

Data Breach: The database contained 2.4 million Watchlist records detailing information on Politically Exposed Persons (PEP), their associates and companies to which they are linked, national and international government sanction lists, people suspected or convicted of high-profile crime, and notes citing federal agencies and law enforcement sources. The exposed data was discovered by a prominent security researcher who reported it to Dow Jones technical staff.
Data Loss: The Dow Jones data was tagged, indexed, and stored unencrypted making it easily viewed, retrieved, and replicated. Beyond the security researcher who discovered the exposure, it was not documented who else accessed the database. But its ready availability posed a significant risk to the privacy of parties mentioned in the data.

Business Impacts

Financial: The financial and compliance impacts of the Dow Jones data breach are intertwined. From a financial perspective there could have been considerable costs for litigation taken against Dow Jones by people or organizations who could claim they were materially damaged by the exposure of their personal information.
Operational: To avoid incidents like this in the future, Dow Jones has to put in place better policies and procedures to vet security vendors and make sure they follow standard security practices. Developing the standards and procedures to improve data security will increase Dow Jones technical operations cost. Since Dow Jones is responsible for incident remediation, responding to this incident, and others like it in the future, will increase their incident response costs.
Compliance: Storing data in the cloud without at least password protection and unencrypted, leaves the data exposed and easily accessible, which violates the privacy of people and organizations whose information is contained in the data.
Reputational: Damage to corporate and brand reputation is a potential outcome for any company that experiences data breaches of a significant magnitude. The Dow Jones data breach in 2019 was not first time this happened. They had a similar incident take place in 2017.

Preventive Mitigation

HRS-07: Roles/Responsibilities – Roles and responsibilities of security team members both inside a company and those in 3rd party security providers must be clearly documented. Of particular importance is the identification of the responsibilities for deploying, maintaining, and securing cloud services that are shared between an organization and its third-party cloud/security support parties or contractors.

IAM-02: Credential Lifecycle/Provision Management – Data should never be stored in the cloud without password protection, as Dow Jones' third-party provider did. Further, there should be a separate account for each user that is authorized to access data in the cloud. Levels of access based on role should be implemented. System administrators can have full access whereas other users should be granted read-only privileges. Data access, even if it is read-only, should be limited to the users who require it to do their jobs. Whenever possible, data should be stored in encrypted form. In the Dow Jones case, everybody inside and outside the company had unrestricted access to their data.

IAM-07: Third Party Access – The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to data should be identified before enlisting third-party services. Third-party security and managed service providers should be rigorously vetted to make sure they follow standard security practices. It is also important to investigate the reputation of third-parties to make sure they have not failed to provide adequate service. In short, an organization should determine what they are getting themselves into, before enlisting the services of any third-party.

Detective Mitigation

AAC-01: Audit Planning – After a company deploys a cloud service, whether it was done by the company or a third-party, there should be a plan in place to regularly check whether the service is running properly, from a functional standpoint, and securely. Audits should be conducted that check to make sure databases in the cloud are stored with password protected user accounts and is visible to only the users who require access to the data. Accounts for users that are no longer with a company or who no longer require access to the data should be deleted. These audits should be done more than once a year. In the Dow Jones incident, a security audit would have caught the fact that their Watchlist data was stored insecurely.

AAC-02: Independent Audits – Although an organization may have a vigorous auditing scheme in place, it is a good idea to have independent audits by reputable auditing companies done to make sure an organization's security team has not missed anything. The key word here is "reputable". Independent security auditors are third-party contractors or companies who pose their own security risks. In a sense, the security researcher who discovered the vulnerable Dow Jones database took the actions of an independent auditor, he was not hired by the company for this purpose.

Corrective Mitigation

SEF-02: Incident Management – Procedures for responding to security incidents must be in place to efficiently resolve issues and maintain data security and business continuity. This is where HRS-07 really comes into play. When there is a security incident involving a company's cloud data that is maintained by a third-party service, a question of responsibility for remediating the incident can arise. If the company who owns that data assumes the third-party will handle the incident and the third-party assumes otherwise, the service will remain compromised. The responsibility of incident management must be clearly spelled out in any service agreement between a company and its third-party service providers.

STA-08: Third Party Assessment – Dow Jones should have insisted that their third-party provider provide written assurances that they follow sound security practices and that they verify their methods on a regular basis.

STA-09: Third Party Audit – Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. This is an important aspect of deciding whether to use certain third-party security and managed service providers. Third-party providers must adhere to standard security practices before data can be placed in their care.

Metrics

Key Performance Indicators: Regular and periodic incident reports demonstrating that minor or no damage to database infrastructure has taken place.

Control Effectiveness Measurements: Vulnerability scanning and security audits to verify data remains secure.

Key Takeaways

- Data stored in the cloud should be secured through encryption and the use of IAM facilities.
- 3rd party security service providers should be vetted to make sure they are trustworthy and follow standard security practices.

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal N/A	Delivery of UDP packets with amplification payload.	EE2 <i>Misconfiguration and Inadequate Access Control - Open Port</i>	EE 2 <i>Misconfigurations of the memcached servers</i>	Financial None-Reported	Preventive - IVS-04 - BCR-09 - IVS-06
		EE3 <i>Lack of Cloud Security Architecture and Strategy - Deficient architectural design</i>	EE 3 <i>Lack of architecture and knowledge of memcached servers exposed to the public internet.</i>		
EE3 <i>Lack of Cloud Security Architecture and Strategy - Poor Corporate Strategy</i>		EE9 <i>Metastructure and Applistructure Failures: Integrity</i> None Reported	Compliance None Reported	Corrective - SEF-02 - SEF-03	
<i>Insiders</i> Insufficient Training		Availability System Down			Reputational None Reported
External Unknown	<i>Software</i> Outdated Version				

Attack Detail

Threat Actor - An unknown external actor seeks to knock Github offline interrupting their operations.

Threat Source/Event - The actor used a technique known as Memcrashing to create a DDoS attack. Memcrashing works by exploiting memcached database servers that have been left open to the public internet with no authentication requirements in place.

The DDOS amplification attack works as follows: an actor sends a small database command to an open memcached server, and, in the UDP packet for that request, sets the source internet address Github servers. The memcached database fires back about 50,000 times the amount of data it received in the command - a 203-byte request results in a 100MB response. Github Inbound network traffic peaked at 1.35Tbps, or 126.9 million packets per second, The sheer volume of data overwhelmed GitHub's computers, causing them to stop responding to normal users.

Vulnerabilities: Insiders - Employees, consultants, etc., with access rights, improperly trained to question or are neglectful when presented with potentially malevolent email.

Technical Impacts

Confidentiality: There was no loss of confidentiality.

Integrity: There was no loss of integrity.

Availability: The System and its data was unavailable for around five minutes which was insufficient time to have any material effect reported by Github. Had the system been unavailable for a longer period, Github a collaborative platform for software development, might have had any number of projects significantly delayed.

Business Impacts

Financial: No Financial impacts were reported. However, should the disruption have lasted for an extended period revenue generated by the platform could have been severely impacted as projects would have not been able to proceed.

Operational: While the Systems and Data were unavailable no material effect was reported. Should the unavailability have lasted longer numerous projects could have been interrupted causing delays in completion.

Compliance: There were no reported compliance issues. However, GDPR Recitals 32 and 49 address availability and DDoS attacks, respectively so had there been issues GDPR fines and penalties could have come into effect.

Reputational: While no financial loss was reported, disrupted operations can affect brand value by undermining confidence in management's ability to successfully manage the company's operations and security.

Preventive Mitigation

IVS-04: Infrastructure and Virtualization Security – Network Architecture - Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

IVS-06: Infrastructure and Virtualization Security – Network Security - Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.

BCR-09: Business Continuity Management & Operational Resilience – Impact Analysis - There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: Identify critical products and services, Identify all dependencies, including processes, applications, business partners, and third party service providers, Understand threats to critical products and services, Determine impacts resulting from planned or unplanned disruptions and how these vary over time, Establish the maximum tolerable period for disruption, Establish priorities for recovery, Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption, Estimate the resources required for resumption.

Detective Mitigation

AAC-01: Audit Planning – Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the efficiency and effectiveness of the implementation and continuous performance of security/operations including incident plans, router, firewall and port configurations and network and filtering capacity.

AAC-02: Independent Audits – Independent reviews and assessments shall be performed at least annually to promote best practice and ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations. Independent and internal audits need to be coordinated to ensure efficient and effective coverage of operations including incident plans, router, firewall and port configurations and network and filtering capacity.

Corrective Mitigation

SEF-02: Incident Management – Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage Github security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.

SEF-03: Incident Management Reporting – Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all Github information security events in a timely manner. Github Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.

Metrics

Key Performance Indicators: Recovery Time Objective (RTO) Recovery Point Objective (RPO), Mean-Time-to-Detect (MTD), Mean-Time-to-Respond (MTR), untrusted risk classified connections attempted / All Connections, % of untrusted risk classified connections allowed on a continuous basis, incident priority, status (not processed, in process, resolved) and time elapsed for each step in the incident process and for the incident resolution process as whole.

Control Effectiveness Measurements: Reduction in number and severity of issues, reduction in detection time and response and recovery time.

Key Takeaways

Github Cloud Takeaways

- Advance arrangements for additional network and filter capacity in an emergency
- Have a detailed, tested incident response plan at the ready
- Return shutdown \ r \ n", o "flush_all \ r \ n" command to Memcached servers
- Ensure router and firewall configurations stop all invalid IP addresses
- Block UDP traffic from memcached server port 11211

Memcached Server Takeaways

- Place memcached servers inside a trusted network
- Install a new memcached version that disables the UDP protocol by default

Imperva

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Design and Human error by an internal cloud team.	EE1 <i>Data Breach:</i> Compromise of AWS server instance and AWS access key in production AWS, which led to an exposure of a database snapshot containing sensitive data.	EE2 <i>Misconfiguration and Inadequate Change Control -</i> A server with access to sensitive database snapshots was configured to be internet accessible.	EE1 <i>Data Breach:</i> Subset of Incapsula customers' email addresses, passwords, API keys and certificates were disclosed.	Financial - No data available	Preventive - DSI-05 - EKM-04 - IVS-07 - IVS-06
		<i>Undisclosed Server Vulnerability -</i> The attacker was able to pivot from an internet facing cloud server, meaning he was able to compromise it via some undisclosed vulnerability or gross misconfiguration.			
External - Unknown threat actor - Undisclosed bug bounty hunter	<i>Cloud Server and Credentials Compromise:</i> An attacker was able to compromise an AWS EC2 service instance and abuse credentials that he found on that server.	EE3 <i>Lack of Cloud Security Architecture and Strategy -</i> A server with access to production database snapshot was used for testing. It was internet facing and used AWS API keys rather than roles (temporary credentials).	<i>Cloud Instance Compromised:</i> An attacker was able to compromise an AWS EC2.	Compliance -GDPR driven breach notifications issued.	Detective - IVS-06 - IVS-01 - TVM-02
		<i>Cloud Access Key Credentials Compromised.</i>	Reputational N/A		

Attack Detail

Actor: External unknown threat actor and undisclosed bug bounty hunter.

Attack: Compromise of an Imperva cloud server led to unauthorized use of an administrative API key in one of the production AWS accounts in October 2018, which led to an exposure of a database snapshot containing emails and hashed and salted passwords.

Vulnerabilities: Internal design and human error by an internal cloud team introduced server weakness (**Undisclosed Server Vulnerability**) and conditions enabling the breach, specifically - making the server internet accessible (**EE2 - Misconfiguration and Inadequate Change Control**) and setting up access to production database snapshots from this server via AWS API access keys (**EE3 - Lack of Cloud Security Architecture and Strategy**).

Technical Impacts

Cloud Instance Compromised: An attacker was able to compromise an AWS EC2 server operated by Imperva for testing purposes.

EE1 - Data Breach: A subset of Incapsula customers' email addresses, passwords, API keys and certificates were exfiltrated by an attacker.

Cloud Access Key Credentials Compromised: An AWS API access key on the compromised server was leveraged by the attacker for data exfiltration and is therefore compromised as well.

Business Impacts

Financial: Imperva became a privately held company as of 2018, so there is no data available on financial impacts or impacts on Imperva's valuation.

Operational:

- Marketial, Security & Operations teams incident response efforts.
- Re-issuing and re-rolling tens of thousands of customer certificates, passwords and API keys.

Compliance: GDPR driven breach notifications were issued, as is required by privacy laws.

Reputational: Communications on the breach were made to Client, media, global law enforcement organizations and regulators, additionally the news media covered this failure and incident at length.

Business: The Imperva CEO stepped down in wake of the breach, though formally the company discredited any correlation between this and the breach.

Preventive Mitigation

DSI-05: Production data shall not be replicated or used in non-production environments (alternatively, testing shall not be conducted on sensitive production data). Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and scrubbing of sensitive data elements.

EKM-04: Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. The sensitive data considered compromised was not encrypted in this case.

IVS-07: Operating systems shall be hardened to provide only necessary ports, protocols, and services and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging. An exposed service on the server allowed it's compromise, server security solutions could assist in prevention and detection.

IVS-06: Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. The breach was possible as a server was internet accessible, which it did not necessarily need to be.

Detective Mitigation

IVS-01: Identity and Credentials compromise and use monitoring should be employed to identify anomalous use and compromise as was this case. Host Intrusion Detection solution shall be employed to identify and respond to compromise of workloads or attempts at such.

IVS-06: Controls in place designed to restrict and monitor (network) traffic between trusted and untrusted connections.

TVM-02: Timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficacy of implemented security controls and remediation of flaws, even if just one of the several flaws in this case could make the difference between a data breach and an incident.

Corrective Mitigation

CCC-03: A defined quality change control and testing process, with a focus on confidentiality, of systems and services could have shed light on the data security concerns with replicating sensitive production data and establishing access to it from an internet facing server.

AIS-04: Considerations for data security should be made when creating new interfaces for server and applications to (a) the internet and (b) data stores. This could prevent data breach.

GRM-02:

- Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:
- Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure
- Compliance with defined retention periods and end-of-life disposal requirements
- Data classification and protection from unauthorized use, access, loss, destruction, and falsification.

A proactive approach to assessing which data is stored where, why and whether it is at risk can prevent it's misuse and mishandling.

IAM-08: Consideration of permissible storage and access of identities used for authentication to ensure the practice of least privilege and secure handling could prevent the use of AWS API access keys where AWS Roles would be a better practice (harder to exploit and misuse).

Metrics

Key Performance Indicators: Cloud misconfigurations count declining, Access to sensitive data and production datastores reduced, external attack surface IP addresses number reduced.

Control Effectiveness Measurements: Data classification and tagging in conjunction with e-discovery and continuous attack surface and cloud misconfiguration reduction. Identity and access compromise detection testing. Server compromise detection testing. External vulnerability scanning.

Key Takeaways

- The agility of cloud services enables more human error, design flaws and policy violations. More investments into control and correction of existing and planned states are necessary.
- Cloud services and assets exhibit a broader external attack surface, its discovery and reduction is key.
- Sound architecture & design of cloud systems, networks, accounts and identities, as well as other defence in depth considerations are beneficial even for smaller cloud-using organizations and environments.

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Potential malicious insiders that could leverage the collected data for personal objectives.	EE1 <i>Data Breach:</i> of consumer PII via third-party trackers.	Inadequate privacy risk assessment that could have discovered the potential to violate user's privacy.	EE 1 <i>Data Breach</i> of consumer PII via third-party trackers.	Financial - Possible risk of lawsuits that could result in financial loss	Preventive - IAM-07 - STA-01 - STA-05 - STA-06 - STA-08
External Potential threat actors that might gain unauthorized access to customer PII.				Operational - Incident Response: Additional resources to remediate the incident	
	EE2 <i>Misconfiguration</i> stemming from the absence of the capability that seeks user content and provides the option to block the company from sharing their data.	EE11 <i>Abuse and Nefarious Use of</i> consumer PII for advertising, data mining, profiling, surveillance purposes.	Compliance - Pre-discloser audit findings - Post disclosure fines	Detective - AAC-02 - CCC-03 - DSI-02 - STA-04 - TVM-02	
				Reputational - Ring loss of Confidence - Long term market share impact - Potential impact to Amazon share price. Amazon owns Ring.	Corrective - SEF-02 - SEF-03 - SEF-04 - SEF-05 - STA-02

Attack Detail

Actor: Third-party trackers on the Ring doorbell app for Android that could be leveraged by malicious external threat actors and insiders to exploit consumers.

Attack: The Ring Android app was discovered by the EFF team to contain third-party trackers sending out customers' personally identifiable information (PII) to four Analytics and Marketing companies. Thus, providing the possibility of abusing data for nefarious purposes such as profiling, surveillance and data theft etc.

Vulnerabilities: The trackers did not provide users with meaningful notifications about this functionality nor the ability to provide consent on data collection and transfer.

Technical Impacts

Data Breach: Unauthorized 3rd parties gained access to customers' PII leading to a breach of user privacy. Information such as user full names, email addresses, OS version and model, Bluetooth activity, local IP addresses etc were being collected and transferred for possible analytics and data mining activity.

Abuse and Nefarious Use of Cloud Services: Given the type of data collected, there is a possible risk of this data being used for advertising, data mining, user profiling, nation state surveillance, data mismanagement, theft by threat actors for social engineering purposes etc.

Business Impacts

Financial: This data breach provides the possibility of financial loss from regulatory fines and class action lawsuits being filed by angry customers for inappropriately handling their data.

Operational: The time and effort taken by the Incident Response team to remediate the incident. There is also a risk that sharing customer data with third party organizations could lead to the data breaches and abuse.

Compliance: Possible regulatory fines for non-compliance and potential law suits from aggrieved consumers

Reputational: The discovery provided negative publicity for the company and may likely have eroded consumer trust in the ability of Ring to protect the privacy of their data.

Preventive Mitigation

IAM-07: Third Party Access – Proper due care must be taken when providing access to third parties who requires access to organizational or customer data.

STA-01: Data Quality and Integrity – Ring should ensure that proper data quality is maintained and any error should be mitigated.

STA-05: Supply Chain Management – Agreement - Supply chain agreement/contract should explicitly and clearly state information security requirements to safe guard customer data.

STA-06: Governance Reviews – Organizations should review the governance and risk management policies of their partners to ensure risks transferred from other members of that partner's cloud supply chain are accounted for.

STA-08: Third Party Assessment – Annual third-party assessments should be performed to ensure compliance and efficacy of policies and procedures. This is a control measure that can detect inappropriate practices from third parties that could put an organization at risk.

Detective Mitigation

AAC-02: Independent Audits – Independent reviews and risk assessments performed at least annually should have been able to detect and correct nonconformities with established privacy compliance obligations

CCC-03: Quality Testing – Proper testing should be done to detect problems with critical features that could impact consumer confidentiality and trust.

DSI-02: Data Inventory / Flows – Policies should be established to review data flows of application. In Ring's case, proper inventory and review of data flows should have revealed the missing requirements: that customer consent should be obtained before collecting and transferring data.

STA-04: Internal Assessment – Third party should perform internal assessment of effectiveness and conformance of internal controls. Provide a copy of the assessment to Ring.

TVM-02: Vulnerability / Patch Management – Timely detection of weaknesses within applications including missing critical features.

Corrective Mitigation

SEF-02: Incident Management – Organizations should ensure they have defined Incident Response processes.

SEF-03: Incident reporting – Third party should contractually agree to report any data breaches or security incidents.

SEF-04: Incident response legal preparation – In the event of a data breach involving a third party, proper forensic procedures should be followed for evidence collection to support potential legal actions.

SEF-05: Incident Response Metrics – For accounting and future budget ramifications, each incident should be tracked according to time and resources spent.

STA-02: Incident Reporting – All customers who have been impacted by a security incident should be notified and adequate provisions made to respond to customers seeking additional information through RFIs (Requests for Information).

Metrics

Key Performance Indicators: Number of third-party related incidents, number of customers RFIs, number of feature gaps detected during quality testing, presence of privacy feature assessments during application development etc.

Control Effectiveness Measurements: Automated scans to reveal weaknesses in applications before deployment to production, regular performance of internal and third party risk assessments, customer satisfaction surveys.

Key Takeaways

- Ring has benefit from the customer data that is available to them by handing over to third party trackers and data miners. Ring has added a privacy dashboard allowing customers to manage privacy and security settings.
- Consumers have to be aware of the hidden dangers of installing apps into their mobile devices without understand the true impact to their privacy.

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Third party service provider maintaining the web application.	EE1 <i>Data Breach:</i> Exposure of personal data of users.	EE2 <i>Misconfiguration and Inadequate Change Control -</i> A publicly accessible cloud storage containing personal data was left unsecured.	EE1 <i>Data Breach:</i> Resulting in exposure of millions of images containing personal data of users across 19 locations in the UK.	Financial - Application downtime expenses - Operational costs to fix the vulnerability - Possible fines levied by regulators - Affected users can sue for damages	Preventive - AIS-01 - CCC-02 - EKM-03 - HRS-09 - HRS-07 - IAM-02
		EE4 <i>Insufficient Identity, Credential and Access Management -</i> The parking validation web app had no authentication controls.			
External Any external user accessing the unsecured data.	EE6 <i>Insider Threat:</i> Handling of personal data by untrained staff of the application maintenance team.	EE7 <i>Insecure Interfaces and APIs -</i> Insecure implementation of a web interface exposed personal data.		Compliance - Personal Data Leakage - Regulatory fines and inquiry	Corrective - SEF-02 - STA-02 - STA-09

Attack Detail

Actor: A third party service provider maintaining a web application for Tesco, stored personal data of customers i.e. ANPR images in a public cloud storage platform without any authentication.

Attack: External users accessing images stored on the public cloud and harvesting the images in bulk for illicit use.

Vulnerabilities: Lack of authentication mechanism to access data stored on public cloud used by the web application. Inadequate security checks in the data migration process. Poor vendor risk management practices such as inadequate oversight and review mechanism.

Technical Impacts

Data Breach: Images of customer cars and vehicle number plates taken using ANPR software is publicly exposed. Violation of customer privacy as the exposed images are time stamped and the aggregated data history can be used to track customer location and activity.

Data Loss: Tens of millions of images of license plates and cars taken in 19 locations across the UK.

Regulatory Breach: Breach of personal data of customers visiting the supermarket. Violation of privacy regulations i.e. GDPR regulation requires user personal data of users to be adequately protected.

Business Impacts

Financial: Depending on the extent of the exposure and publicity in the media, the business impact could be significant in the short term, if customers choose not to visit the supermarket. Affected users may sue the company for damages in case the data breach leads to any adverse consequences. It could lead to regulatory fines as both data controller and data processor are responsible for protecting personal data of users as per GDPR obligations.

Operational: The parking app was shut down once the data exposure was made public. The operational impacts include the time and effort taken to secure the vulnerable app.

Compliance: Compliance impacts could include fines and liabilities such as disclosure notices or penalties levied by regulators such as GDPR.

Reputational: The coverage in the media may result in users unwilling to trust the supermarket with their personal data in the near future. The organizational brand may also take a hit owing to the bad publicity.

Preventive Mitigation

AIS-01: Application and Interface Security – The organization should ensure that secure SDLC practices are followed while designing, developing, testing, and deploying publicly exposed applications and programming interfaces (APIs).

CCC-02: Change and Configuration Management in Outsourced Development – Outsourced service provider should adhere to secure procedures for change management, release, and testing; especially while handling customer data such as during a data migration activity.

EKM-03: Protection of personal data – The organization should protect personal data of users by using technical means such as encrypting data at rest, in transit or during use to prevent unauthorized access.

HRS-09: Security awareness training for contractors – All contractors & third-party service providers should be provided appropriate security awareness, training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.

HRS-07: Roles and Responsibilities of contractors – Roles & responsibilities of contractors and third-party service providers to be documented in work contracts as they relate to information security.

IAM-02: Identity, entitlement, and access management – Adequate technical and procedural controls to be implemented to ensure that only authorized users and processes are able to access the sensitive data based on the principle of least privilege.

Detective Mitigation

AAC-02: Audit Assurance and Compliance – Organizations should ensure that independent audits of their IT processes & systems are conducted at planned intervals and findings or gaps identified with respect to information security and compliance are closed at the earliest.

STA-08: Vendor Assessments – Organizations should perform an annual review of the operational and security processes followed by vendors and outsourced service providers to get reasonable assurance about the security practices followed across their information supply chain

TVM-02: Vulnerability / Patch Management – Regular vulnerability scanning of publicly exposed applications and interfaces is essential for timely detection and remediation of vulnerabilities such as applying missing patches within organizational applications, systems, or network components.

Corrective Mitigation

SEF-02: Security Incident Management – Maintaining a security incident management procedure and implementing adequate technical controls to manage the incidents would ensure that the organization is able to provide timely and adequate response to security incidents such as a data breach.

STA-02: Service Provider Incident Reporting – In case of a data breach involving customer data, the service providers should make security incident information available to all affected customers through electronic methods.

STA-09: Audit of third party services – Audits of all third party service providers should be conducted at least once a year, to verify compliance against contractual obligations related to information security.

Metrics

Key Performance Indicators:







- Security awareness trainings detailing the security responsibilities for third party service provider personnel to be conducted.
- Vulnerability scanning performed on the publicly exposed application, underlying infrastructure, and its interfacing components.

Control Effectiveness Measurements:

- Number of security incidents reported related to the applications maintained by third-party service provider.
- Number of vulnerabilities found in the publicly hosted applications, systems, and interfaces.

Key Takeaways

- Service provider agreements should clearly state security responsibilities of the supplier.
- Conduct periodic security assurance audits to verify vendor conformance against organizational policies, procedures and standards.
- Always protect sensitive data storage via encryption, especially when its accessible over the internet.

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Failure to secure access to admin console by unintentional insider.	EE5  Account Hijacking of AWS access credentials.	EE2  Misconfiguration of Kubernetes administrative interface.	EE1  Data Breach: Resulting in the exposure of vehicle telemetry data.	Financial - Possible increase in the cost of resources consumed for mining cryptocurrency. - Possible risk of exfiltrating and auctioning valuable intellectual property to the company's competitors.	Preventive - CCC-04 - EKM-03 - IAM-02 - HRS-09 - TVM-02
	Installation of evasive cryptocurrency mining scripts.	EE4  Insufficient Identity and Credential Management likely caused by failure to protect AWS access credentials, lack of multifactor authentication.			
External Malicious hacker	Inadequate security monitoring to detect intrusions.	EE7  Insecure Kubernetes Interfaces exposed AWS access credentials.	EE11  Abuse and Nefarious Use of unsecured Kubernetes instances for cryptocurrency mining.	Operational - Time and effort taken by the Incident Response team to remediate the incident.	Detective - CCC-03 - IVS-01 - TVM-01
	Inadequate antimalware solution to prevent the execution of malicious scripts.			Compliance - Exposure of sensitive data	

Attack Detail

Actor: External malicious hacker(s) gained access to an unsecured Kubernetes administrative interface. This was discovered by security researchers and reported to Tesla.

Attack: The attackers gained access to AWS access credentials via the unsecured Kubernetes administrative interface. These credentials further provided access to S3 buckets containing non-public vehicle telemetry data. In addition, the attackers installed mining scripts on the hijacked Kubernetes instance to mine cryptocurrency.

Vulnerabilities: Misconfiguration of secure authentication mechanisms within the Kubernetes console provided access to confidential data including credentials.

- Insufficient credential management and effective encryption measures possibly facilitated lateral movement across the network.
- Inadequate antimalware and security monitoring failed to detect and prevent the installation of mining scripts.

Technical Impacts

Data Breach: The attackers were able to gain access to AWS S3 buckets housing intellectual property related to internally-used engineering test cars.

Malware infection: The intrusion allowed the attackers to install evasive cryptocurrency mining scripts. In addition to stealing computing resources, these nefarious scripts provide an avenue for attackers to persist within the environment if not properly detected and remediated.

Business Impacts

Financial: Possible increases in the cost of cloud computing resources could be realized depending on the length of time the attackers spent mining crypto currency within the compromised network.

- Possible risk of exfiltrating and selling valuable intellectual property to highest bidding competitor

Operational: Time and effort taken by the Digital Forensic and Incident Response (DFIR) team to manage malware infections, revoke access credentials and ensure reconfiguration of the Kubernetes administrative instance.

Compliance: This attack may not have direct impacts from non compliance since confidential data such as customer PII was not exposed. However, there was a loss of confidentiality of sensitive data that could be possibly related to trade secrets.

Reputational: The data breach may have led to a reduction of consumer confidence and a diminished perception of brand value.

Preventive Mitigation

CCC-04: Unauthorized Software Installations – Organizations should have application whitelisting policies in place to restrict the installation of unauthorized software (including malware) on end-points and servers.

EKM-03: Sensitive Data Protection – Encryption should be enforced for sensitive data in stored in the cloud. CSPs should provide customers with the option to select client side or server-side encryption. Where possible, customers should select encryption mechanisms that complement the value and use of data being protected.

IAM-02: Credential Lifecycle/Provision Management – Establishment of user access control policies supporting business processes and technical controls that ensure appropriate identity and access management for all users with access to data.

HRS-09: Employee training – Intelligence driven security awareness training should be provided to DevOps teams on secure development practices. This can help mitigate the risk of security misconfiguration.

TVM-02: Vulnerability / Patch Management – Timely detection of weaknesses within configurations of applications, infrastructure, network and system components can ensure efficacy of implemented security controls. For example, penetration testing of applications can reveal the presence of weak authentication mechanisms that need to be corrected before being exploited by attackers.

Detective Mitigation

CCC-03: Quality Testing – Organizations should have defined change control and testing processes to test applications and before being deployed into production. This can help in detecting misconfigured services that can affect the confidentiality, integrity and availability of systems and services.

IVS-01: Audit Logging / Intrusion Detection – CSP's should provide customer's the capability to detect potentially suspicious network behaviours/ anomalies within their environment. Furthermore, the CSP needs to ensure the confidentiality, integrity and availability of audit logs are maintained at all times to aid forensic investigations.

TVM-01: Anti-Virus / Malicious Software – Some endpoint detection and response (EDR) solutions are capable of detecting and mitigating the effects of malware intrusions. Although not fully encompassing, these solutions at the very least can help in detecting and preventing the execution of commodity malware or publicly known tools which are still currently being used in the wild by adversaries.

Corrective Mitigation

SEF-02: Incident Management – An Incident Response Team will be required to triage/investigate suspicious security events and ensure timely and thorough management of incidents, as established within the Incident Response process.

SEF-05: Incident Response Metrics – Each incident should be tracked in order to provide justification for time and resources spent to manage incidents. This will aid Management in making investment decisions needed to improve the Incident Response process.

Metrics

Key Performance Indicators: Number of malicious events generated by the antivirus solution installed on affected servers, presence of suspicious alerts generated by the user behavioural analytics system, CPU usage trends overtime, tailored user security awareness training etc.

Control Effectiveness Measurements: Automated scans to reveal weaknesses in configuration before deployment to production, regular rotation of credentials, enforcement of least privilege access, utilization of antimalware solution on critical assets etc.

Key Takeaways

- Have a detailed, tested incident response plan at the ready, including arrangements for additional network and filter capacity in an emergency
- Perform appropriate threat modeling
- Lower attack surface through best practice network design (ACLs, Firewalls, port and protocol blocking, deny invalid IP addresses)

Zoom

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Third party service provider maintaining the web application.	EE1 <i>Data Breach:</i> Zoombombers steal sensitive information through Zoom's lack of security protections .	EE2 <i>Misconfiguration and Inadequate Change Control -</i> Zoom accounts resulted in easily guessed (or non-existent) passwords and publicly displayed meeting info.	EE11 <i>Abuse and Nefarious Use of Cloud Services:</i> Zoombombers incite general mayhem.	Financial - Incident stock price drops were overcome due to CoVID-19 work from home necessity - Possible Fines - Fast turn code releases	Preventive - IAM-02 - IAM-05 - IVS-13 - TVM-02
		EE4 <i>Insufficient Identity, Credential and Access Management -</i> Inadequate testing of credential reuse and weak password hash checks allowed for credential stuffing attack.	Data Loss: UNC leaks bypass network connection protections in Windows enterprise environments.		
		EE7 <i>Insecure Interfaces and APIs -</i> Company looked for simplified operations and use, or performed poor threat modeling.	State Secret Exposure: German and UK Governments both incur high profile incidents.	Compliance -Sensitive Data Leakage -Multiple Class Action Lawsuits -US Government mandated a "Zoom for Government" offering	Corrective - SEF-02 - STA-02 - STA-09
External Any external user accessing the unsecured data.	EE5 <i>Account Hijacking:</i> Lack of credential stuffing protections allow account credential harvesting.			Reputational - Product Confidence Tested - Multiple municipalities banned Zoom	

Attack Detail

Actor: Script Kiddies Zoombombing. External attacker harvesting accounts.

Attack: Uninvited guests log into accounts. Credential stuffing harvests 500M user accounts.

Vulnerabilities: With the CoVID-19 pandemic, Zoom experienced a huge user uptick with multiple incidents throughout early 2020. Several issues crept in, including poorly randomized, easily guessed or widely broadcast meeting room information without sufficient detective or preventive security controls. Customer credential reuse was rampant, without appropriate Zoom corrective security controls. Lastly, attackers could use the Zoom Windows client's group chat feature to share links that leak Windows network credentials. This happens when Zoom converts Windows UNC paths into clickable links.

Technical Impacts

Data Breach: There is a potential breach of confidentiality by attackers of company intellectual property during virtual meetings. Such information can include source code, trade secrets or other highly sensitive information.

Data Loss: Universal Naming Convention (UNC) leaks within chat sessions allow network protection bypass, threatening enterprise organizations using Windows sharing.

State Secrets Exposure: The UK's Prime Minister, Boris Johnson, used his permanent Personal Meeting ID (PMI) instead of a separate, per meeting code for government business during the CoVID-19 crisis. In posting a screenshot to Twitter, Johnson compromised the forum and potentially discussions of state business.

Credential Compromise: Zoom lost over 500M usernames and passwords throughout their user base with the external account harvesting.

General Mayhem: Attackers defaced company & school meetings with racially incendiary and sexually explicit graffiti.

Business Impacts

Financial: Depending on the systems compromised, the business impact could be significant, ranging from loss of IP to premature strategic planning disclosure. Several organizations banned Zoom as a communications platform, resulting in direct lowered revenues for monthly subscriptions.

Operational: Operational impacts includes the time and effort taken reset user details. Zoom instituted new security controls for meeting locking, waiting rooms and general privacy. Within 6 months of the situations, Zoom rolled out password requirements for all meetings, hid all meeting codes in settings menus and defaulted to secure configurations for all new meetings.

Compliance: Compliance impacts could include fines and liabilities such as breach disclosure notices (for PII) or penalties levied by regulators. Multiple government organizations asked for tailored products, with Zoom for Government reaching FedRAMP Authority To Operate in the US.

Reputational: The affected Zoom users might suffer reputational impacts from negative publicity based on the verbiage and visuals presented. Multiple organizations immediately banned Zoom meetings, including New York State Schools, Google and Germany. Such impacts are visible and noticeable by the organization's' customers and the general public.

Preventive Mitigation

IAM-02: Credential Lifecycle / Provision Management - Implementing single use meeting IDs and random meeting pins minimizes attackers replaying previous meeting invites or guessing new meetings.

IAM-05: Segregation of Duties - Separating meeting access (connecting to a meeting) and administrative duties (sharing screens or allowing admittance from a waiting room) controls zoombombing capabilities.

IVS-13: Network Architecture - Technical measures, including Security and privacy controls should be designed through threat modelling, including not publicly displaying meeting info and proper random numbering sequences.

TVM-02: Vulnerability / Patch Management - Threat testing did not uncover vectors surrounding uninformed employees, which should allow stringent policy implementation and, system defaults for meeting password, no join before host, participant screen sharing, lock meeting after start.

Detective Mitigation

IAM-02: Credential Lifecycle / Provision Management - Check account credentials against compromised password lists. Password hash and rainbow table testing for credential reuse. Monitor for account password abuse, including resets, privilege use and possible credential stuffing.

IAM-12: User Access Reviews - Data analysis for personal meeting rooms use, anomalous account behavior, significant profile changes and audit admin settings for deviations Account creation, deletion and inactive account monitoring. Track Metrics - meetings created, IDs used by guests, where they join from.

GRM-02: Data Focus Risk Assessments - Data exfiltration shared through chat or other virtual environment methods. Audit/Logging - Consider third party CASB monitoring tools.

Corrective Mitigation

EF-02: Incident Management - The Incident Response Team will be charged with immediate clean-up. Common playbooks minimize errors and speed resolution time for events.

SEF-04: Incident Response and Legal Preparation - Forensic investigations need accurate and admissible evidence. Several cases are pending throughout the US, ranging from meeting disruptions to the display of child pornography.

HRS-09: Training / Awareness - Zoom quickly implemented several new security features. Training users of new security changes including creating waiting rooms, settings adjustments such as disabling the 'join before host feature' and enabling meeting passwords by default.

TVM-02: Vulnerability / Patch Management - Zoom is a software product, and cybercriminals are more apt to target old versions.

Metrics

Key Performance Indicators:

- Credential database testing size
- Percent credentials tested
- User behavioral analysis

Control Effectiveness Measurements:

- Helpdesk complaints
- Customer satisfaction surveys

Key Takeaways

- Proper threat modelling allows security architects and developers time to evaluate control gaps
- Security Protections built in not bolted on
- Agile development may quickly respond to feature requirements

Glossary

Capital One

EC2 - Amazon Elastic Compute Cloud
GDPR - European Union General Data Protection Regulation
IMDS - Amazon Web Services Instance Meta Data Service version 1
S3 - Amazon Simple Storage Service
SSRF - Server Side Request Forgery
VPN - Virtual Private Network
WAF - Web Application Firewall

Disney+

Credential stuffing - is a cyberattack method in which attackers use lists of compromised user credentials to breach into a system. The attacker uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services.

Dow Jones

Elasticsearch - Elasticsearch is an open-source, distributed data search and analytics engine built on Apache Lucene. You can send data in the form of JSON documents to Elasticsearch using the RESTful API or ingestion tools such as Logstash. Elasticsearch automatically stores the original document and adds a searchable reference to the document in the cluster's index. You can then search and retrieve the document using the Elasticsearch API. Amazon provides fully managed Elasticsearch services that enables you to deploy, secure, and run Elasticsearch at scale.

IoT Search Engine - Internet of Things (IoT) search engine which enables you to find physical devices with embedded computing capabilities - such as webcams, home appliances, medical devices - that are connected to and can exchange data over the Internet. Two examples of IoT search engines are Thingful (<https://www.thingulf.com>) and Shodan (<https://www.shodan.io>).

Politically Exposed Person - Someone who, through their prominent position or influence, is more susceptible to being involved in bribery or corruption.

Github

Amplification Attack - any attack where an attacker causes more resource usage than what a single connection should be capable of. The amplification factor multiplies the attack's power through asymmetry, where a low level of resources causes a large level of target failures.
Memcached server - General purpose distributed memory caching system used for increasing speed on dynamic database-driven websites.
Memcrashing - utilizing a weakness in Memcached server on UDP port 11211 to execute an Amplification Attack and paralyze the hosting server
Port 11211 - Memcached clients use client-side libraries to contact servers. By default, Memcached servers expose their service at port 11211 on both TCP and UDP.
UDP - (User Datagram Protocol) is a communications protocol primarily used for establishing low-latency and loss-tolerating connections between applications on the internet.

Imperva

Unknown threat actor - unauthorized access was confirmed, but the identity of the attacker, nor any information on the attacker was not made available. It is doubtful whether much is known at all.

GDPR - General Data Protection Regulation

AWS EC2 - the amazon web services server workloads (elastic compute) service, mostly used for virtual machines run by customers on AWS infrastructure.

AWS API Access Key - the credentials pair of an AWS user, different to username/password credentials as they are intended for programmatic use with AWS API.

Ring

None.

Tesco

Unknown threat actor - unauthorized access was confirmed, but the identity of the attacker, nor any information on the attacker was not made available. It is doubtful whether much is known at all.

GDPR - General Data Protection Regulation

AWS EC2 - the amazon web services server workloads (elastic compute) service, mostly used for virtual machines run by customers on AWS infrastructure.

AWS API Access Key - the credentials pair of an AWS user, different to username/password credentials as they are intended for programmatic use with AWS API.

Tesla

Kubernetes - An open-source container-orchestration system for automating deployment, scaling, and management of containerized applications across multiple hosts.

Zoom

Zoombombing - the practice of hijacking video conversations by uninvited parties to disrupt the usual proceedings.

Credential Stuffing - Attackers take a database of known usernames and passwords and try to "stuff" those credentials into the login page of other digital services. Because of password reuse across multiple sites, attackers can often use one piece of credential info to unlock multiple accounts.

UNC - Universal Naming Convention provided by Windows as an early method of identifying systems within an enterprise environment.

References

Capital One

Capital One Breach Details

1. <https://cloudsecurityalliance.org/blog/2019/10/10/cloud-penetration-testing-the-capital-one-breach/>
2. <https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach/>
3. <https://www.capitalone.com/facts2019/>
4. <https://www.scmagazine.com/home/security-news/capital-one-breach-exposes-not-just-data-but-dangers-of-cloud-misconfigurations/>
5. <https://krebsonsecurity.com/tag/capital-one-breach/>
6. <https://krebsonsecurity.com/tag/paige-a-thompson/>
7. <http://web.mit.edu/smadnick/www/wp/2020-07.pdf>

SSRF

8. <https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SS>
9. <https://blog.appsecco.com/server-side-request-forgery-ssrf-and-aws-ec2-instances-after-instance-meta-data-service-version-38fc1ba1a28a>

Estimated cost of Capital One breach

10. <https://fortune.com/2019/07/31/capital-one-data-breach-2019-paige-thompson-settlement/>
11. <https://www.forbes.com/sites/greatspeculations/2019/09/11/how-could-the-recent-data-breach-affect-capital-ones-stock/#f2faa4437b79>
12. <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html>

Job Loss at Capital One

13. <https://www.bankinfosecurity.com/following-massive-breach-capital-one-replacing-ciso-report-a-13385>

Regulatory Breach Fines and Penalties

14. <https://techcrunch.com/2019/07/22/equifax-fine-ftc/#:~:text=FTC%20slaps%20Equifax%20with%20a%20fine%20of%20up,M%20for%202017%20data%20breach&text=Credit%20agency%20Equifax%20will%20pay,a%20data%20breach%20in%202017.>

Disney+

15. <https://www.wired.com/story/disney-plus-hacks-credential-stuffing/>
16. <https://www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/>
17. <https://blog.eccouncil.org/disney-plus-accounts-hacked-within-hours-of-its-most-awaited-launch-heres-how/>
18. <https://popculture.com/streaming/news/quarantine-disney-plus-users-hacked-accounts/>
19. <https://medium.com/online-io-blockchain-technologies/thousands-of-disney-plus-accounts-got-hacked-heres-why-f2f0b7b569a2>
20. <https://www.imperva.com/learn/application-security/credential-stuffing/#:~:text=Credential%20stuffing%20is%20a%20cyberattack,and%20passwords%20across%20multiple%20services.>

Dow Jones

21. [Amazon Elasticsearch Service](#)
22. [Cloud Leak: WSJ Parent Company Dow Jones Exposed Customer Data](#) - Dan O'Sullivan
23. [Data Breaches/Privacy](#) - Justia
24. [Dow Jones Risk Screening Watchlist Exposed Publicly in a Major Data Breach](#) - Bob Diachenko
25. [Dow Jones Watchlist of risky businesses exposed on public server](#) - Lisa Vaas
26. [Dow Jones' watchlist of 2.4 million high-risk individuals has leaked](#) - Zack Whittaker
27. [The what, why and how of IoT search engine](#) - Futurelo Editors
28. [What is a Politically Exposed Person \(PEP\)?](#) - Accuity

Github

29. https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/
30. https://www.theregister.co.uk/2018/03/01/github_ddos_biggest_ever/
31. <https://www.globaldots.com/memecached-servers-ddos-attacks-complete-analysis/>
32. <https://www.geekwire.com/2018/memcached-servers-used-launch-record-setting-ddos-attacks/>
33. <https://memcachedscan.shadowserver.org/stats/>

Imperva

34. <https://www.imperva.com/blog/ceoblog/>
35. <https://krebsonsecurity.com/2019/08/cybersecurity-firm-imperva-discloses-breach/>

Ring

36. <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers>
37. <https://www.geekwire.com/2020/ring-customers-cameras-breached-hackers-sue-amazon-proposed-class-action-lawsuit/>
38. <https://www.eff.org/deeplinks/2019/12/ring-throws-customers-under-bus-after-data-breach>
39. <https://www.businessinsider.com/amazon-ring-passwords-credit-card-exposure-leak-hack-2019-12>
40. <https://securitytoday.com/articles/2019/12/23/ring-faces-intense-scrutiny-after-hacks.aspx>
41. <https://www.securitymagazine.com/articles/91469-amazon-ring-leaks-thousands-of-customer-data>
42. <https://abcnews.go.com/US/amazon-ring-face-million-proposed-class-action-lawsuit/story?id=67948687>

Tesco

43. https://www.theregister.co.uk/2019/09/20/tesco_parking_app_10s_millions_anpr_photos_exposed/
44. <https://cyware.com/news/unsecured-microsoft-azure-blob-exposes-millions-of-automatic-number-plate-recognition-images-9b04c528>
45. <http://securitydive.in/2019/09/how-the-tescos-parking-app-exposed-millions-of-automatic-number-plate-recognition-images/>
46. <https://thedataprivacygroup.com/blog/2019/9/23/tesco-shutters-parking-app-following-license-plate-image-leak>
47. <https://www.techradar.com/news/tesco-shutters-parking-app-following-license-plate-image-leak>
48. <https://www.anprcameras.com/about-us/understanding-anpr/>
49. <https://panopticonblog.com/2016/11/10/anpr-personal-data/>

Tesla

50. https://info.redlock.io/hubfs/WebsiteResources/RedLock_CSI_report_May2018.pdf
51. <https://www.zdnet.com/article/tesla-systems-used-by-hackers-to-mine-cryptocurrency/>
52. <https://www.osradar.com/tesla-cloud-account-data-breached/>
53. <https://fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/>
54. <https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>
55. <https://kubernetes.io/>
56. <https://github.com/kubernetes/kubernetes>

Zoom

57. <https://www.npr.org/2020/04/03/826129520/a-must-for-millions-zoom-has-a-dark-side-and-an-fbi-warning>
58. <https://www.sumologic.com/blog/zoom-security-challenges/>
59. <https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/>
60. <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/>
61. <https://www.npr.org/2020/04/03/826968159/senator-zoom-deceived-users-over-its-security-claims>
62. <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>
63. <https://www.lawfareblog.com/prosecuting-zoom-bombing>
64. <https://www.pcworld.com/article/3535213/how-to-prevent-zoom-bombing-by-being-smarter-than-boris-johnson.html>

