Cyberint

Capital One

CAPITAL ONE DATA BREACH

CyberInt's Take | July 2019

FACTS

On July 29th, 2019 Capital One Financial Corporation, a US-based bank holding company specializing in banking, credit cards, loans and savings, today released a statement[1] regarding the detection of a breach resulting in unauthorized access to personal data pertaining to over 100 million Canadian and US credit card applicants and customers.

- The breach is believed to be one of the largest in the history of the banking industry;
- According to the statement, Capital One do not believe the compromised data has been used fraudulently;
- Capital One became aware of the breach following a responsible disclosure email alerting them to potentially leaked data on a GitHub account associated with the alleged threat actor (TA);
- The breach reportedly exploited a configuration vulnerability in Capital One's infrastructure, including at least one known firewall misconfiguration, permitting access to customer data stored on Amazon Web Services' (AWS) cloud;
- US Law Enforcement arrested an alleged TA, 'Paige Adele Thompson', a former Amazon Inc. employed S3 Systems Engineer[2], also known as 'Erratic', in Seattle, WA (US) on suspicion of 'Computer Fraud and Abuse' as filed[3] in a criminal complaint with the US District Court for the Western District of Washington at Seattle;
- The hack is expected to cost the company up to $150 million in the near term, including paying for credit monitoring for affected customers.

[Scope of breach]

- Personal data of more than 100 million US and 6 million Canadian customers (consumers and small businesses) including approximately:
  - 140,000 US Social Security numbers
  - 1 million Canadian Social Insurance Numbers (SIN);
  - 80,000 US bank account details;
  - Names, addresses, phone numbers & dates of birth;
  - Self-reported income;
  - Credit scores, limits, balances & payment history.
- Stolen information pertained to credit card applications from 2005 through to 2019.

[Timeline]

- 12 March – 17 July 2019 – Period in which unauthorized access to Capital One's infrastructure likely occurred;
- 22 March 2019 – Capital One access logs confirm unauthorized access to AWS from a compromised account;
- 21 April 2019 – Timestamp associated with leaked data hosted on GitHub in addition to unauthorized activity recorded by Capital One logs;
- 26 June 2019 – Posts on a Slack channel associated with, and using an alias of, the TA include screenshots and directory listings of files belonging to Capital One and other potential victims;
- 17 July 2019 – Responsible disclosure email received by Capital One, alerting them to 'leaked s3 data' hosted on a GitHub Gist account believed associated with the threat actor;
- 18 July 2019 – Direct messages posted by the TA suggest that they were prepared to distribute the stolen data;
- 29 July 2019 – US FBI agents arrested the TA and Capital One release a public statement about the breach (also establishing a dedicated data breach webpage[4] with an FAQ for potentially affected customers).

1 http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043
2 https://www.linkedin.com/in/PaigeAdeleThompson
3 https://www.justice.gov/usao-wdwa/press-release/file/1188626/download
4 https://www.capitalone.com/facts2019/

CYBERINT RESEARCH LAB INSIGHTS

Technical data shared within the criminal complaint, combined with intelligence gathered by CyberInt Research Lab from social media and chat servers associated with the alleged threat actor (TA) allows the following to be determined:

- TA attempted to mask their identity and IP address when accessing Capital One by connecting to 'IPredator', a Sweden-based VPN provider, and using the 'Tor' anonymity network;
- An account, 'ISRM-WAF-Webrole', was compromised, potentially through a configuration vulnerability, to gain access to Capital One's cloud infrastructure hosted by Amazon Web Services (AWS);
- Once access to the AWS account was established, a storage gateway was configured and an EC2 snapshot (backup) taken before being transferring to the TA's server using 'dd', the Linux command-line copy utility;

Screenshots and posts (Figure 1) sent by the alleged TA on their Slack server suggest that other organizations are likely to have been breached, potentially using similar techniques. Whilst the TA specifically mentions Capital One, Michigan State University, Ohio Department of Transportation and Vodafone, other victims may be inferred from filenames.

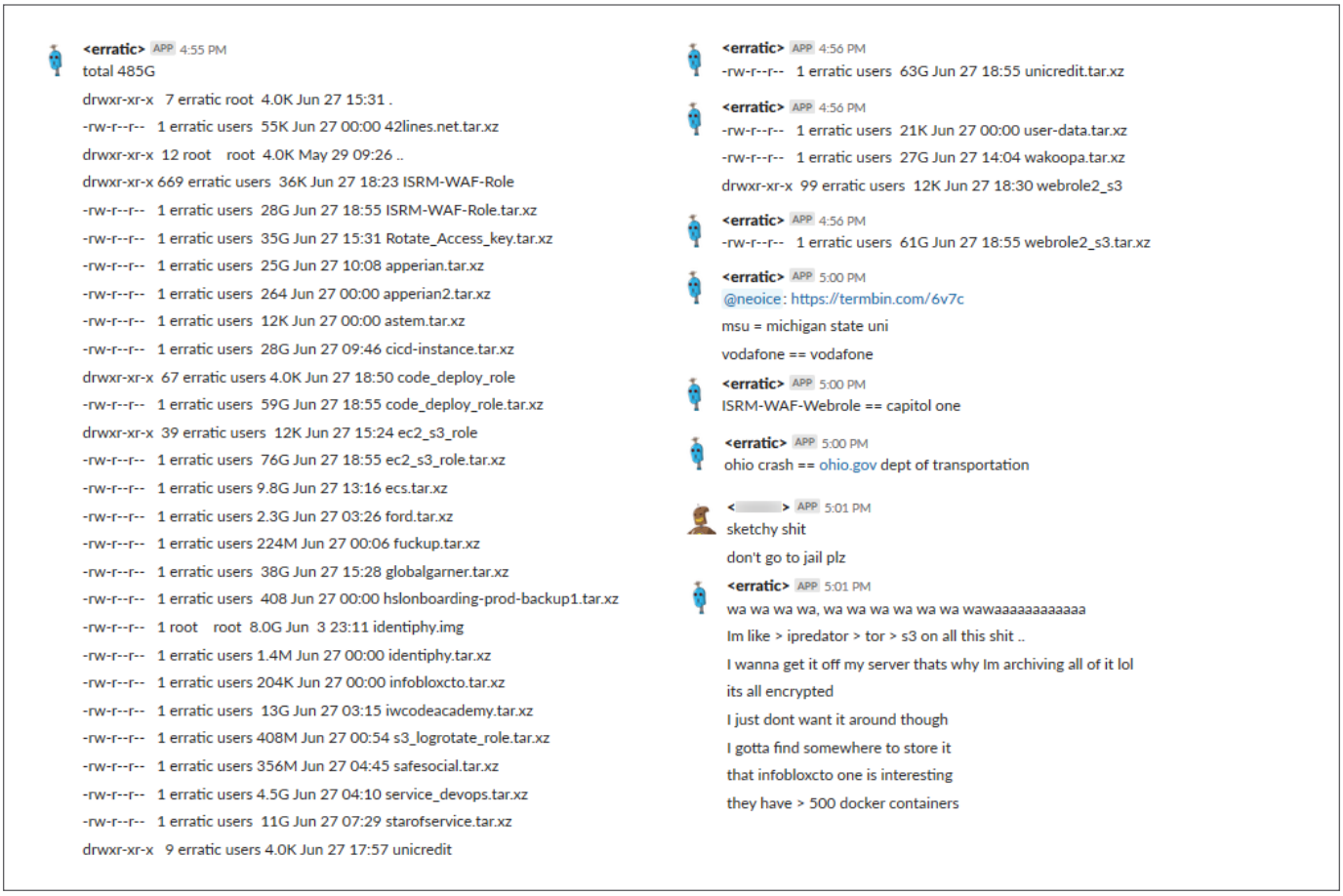

Figure 1 - Slack channel posts by alleged TA 'erratic'

RECOMMENDATIONS

- Organizations using cloud-based services, such as Amazon S3, should ensure that assets are correctly configured to prevent inadvertent or unauthorized access to sensitive data. Cloud providers will provide documentation detailing identity and access policy configurations that can restrict access, be that by user, file, bucket or organization.
- Existing users of cloud services should consider auditing current deployments to ensure that access permissions are correctly configured. Digital risk protection services, such as CyberInt's My Digital Presence[5], provide automated discovery and monitoring of digital assets including cloud storage instances and identify those that are left 'open' or at risk.
- In addition to logging activity on cloud services, logs should be regularly monitored to ensure that incidents of this nature are detected and acted upon as they occur rather than after-the-fact.

5 https://www.cyberint.com/product/my-digital-presence/

CONTACT INFORMATION

Cyberint

www.cyberint.com | sales@cyberint.com | The Cyber Feed: blog.cyberint.com

UNITED KINGDOM
Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068, London

USA
Tel: +1-646-568-7813
214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

ISRAEL
Tel: +972-3-728677717
Ha-Mefalsim St, 4951447, Kiriat Arie, Petah Tikva

SINGAPORE
Tel: +65-316-357-6010
Anson Road, #33-04A, International Plaza

LATAM
Tel: +507-395-1553
Edificio Corporativo Cable Onda/TeleCarrier, Panama City