Ransomware Case Study - Infosys McCamish Systems

A Third-Party Breach of Bank of America

BY: LISA BOETTCHER

DATE: MARCH 21, 2024

Ransomware Hack

- Between October-November 2023 a data breach attack targeted Bank of America's third-party vendor Infosys McCamish Systems LLC (IMS).
- The cybercriminal syndicate known as LockBit Ransomware Group (LRG) claimed responsibility for the breach.
- Vulnerable open ports and a malicious ransomware software tool, LockBit 3.0, was used in the attack.
- The group encrypted over 2000 systems of Infosys McCamish's during the attack.
- To unlock IMS systems and data, hackers demanded $500,000 in cryptocurrency.
- LockBit instructed McCamish to message them on tox chat platform.

REUTERS FILE PHOTO 2017

Timeline

Infosys McCamish Systems Attack

1. More than 57,000 customers affected by breach as their personally identifiable information (PII) was exposed.
2. Infosys McCamish hired external data forensics experts who confirmed the breach impacted deferred compensation plan accounts for employees of Bank of America.
3. The attack vector and infrastructure included malicious traffic directed at Infosys McCamish' open ports and compromised credentials.
4. The data exposed included names, addresses, social security numbers, DOB, banking accounts, credit card info.
5. February 1, 2024 Infosys sent out data breach letters to anyone who was affected by the data security incident.
6. Affected customers were offered free 2-year membership to Experian identity protection services.

Vulnerabilities

There was no plan in place if an attack occurred.

Infosys McCamish had to hire a cybersecurity products provider to launch an independent Investigation to assess the extent of the breach.

Even worse, there was a delay in notifying customers their personal identifiable information (PII) was exposed. And a Class Action Lawsuit has been filed by Console & Associates, P.C

Vulnerability #1

Open Ports

68 IP addresses identified as malicious communicated with Infosys' 16 IP addresses on open port 22 (SSH) to gain initial access into Infosys McCamish' network.

Vulnerability #2

RDP Exploitation

Infosys BPM IP addresses communicated 182 times with attacker's IP addresses via remote desktop protocol (RDP) exploitation during the brute-force attack which gave them lateral movement within portions of the network.

Vulnerability #3

Vulnerable Infrastructure

According to SecurityScorecard's Attack Surface Intelligence (ASI) model, Hackers used a compromised MikroTik router which enabled them to route traffic through it — unpatched CVE-2023-32154 (2023).

Vulnerability #4

Weak Passwords

McCamish' lack of use of strong passwords and multi-factor authentication (MFA) gave Hackers access to no less than 23 login credentials.

Costs

- Infosys McCamish Systems LLC (IMS) reported financial losses of approximately roughly £25 million and facing disruptions due to the unavailability of critical applications and systems.
- This type of data breaches (that originate from third parties) typically costs an average of $4.45 million USD.
- Lockbit Ransomware Group (LRG) ‘s ransom bid started at $500K USD.
- McCamish offered to pay $50K USD.
- LRG threatened that if demand not met, all available data from last 365 days that was exfiltrated will be published.

Prevention

- IMS recently hired Celent, an IT research and consulting to assist with patching CVE’s, implementing two-factor (2FA) or multi-factor authentication (MFA), removing unnecessary permissions implementing tokenization, more robust encryption, tighter access controls and data monitoring mechanisms, and segmenting networks to prevent widespread environment proliferation.
- According to the DOJ, if an organization that holds your personal information experiences a data breach, it must inform you of your rights.
- Infosys McCamish offering affected customers a free two-year membership to Experian IdentityWorks. This identity theft protection program includes daily credit report monitoring from Experian, Equifax and TransUnion, internet surveillance, and identity theft resolution, among other services.

LOCKBIT RANSOMWARE GROUP ("LRG")

- ⇒ LRG used LockBit 3.0; an advanced version of the LockBit ransomware-as-a-service (RaaS) known for its highly sophisticated encryption techniques and targeted attacks. LockBit 3.0 is designed to infiltrate computer systems, encrypt valuable files, and render them unusable until a ransom is paid.
- ⇒ LRG is believed to be originated in Russia based on their communication style and syntax; and their propensity to not attack countries bordering Russa (except for Ukraine).
- ⇒ LRG uses affiliates like "LockBit Black" or "BlackCat" or "Bitwise Spider" or "LostTrust" to conduct attacks.
- ⇒ LRG have been highly active in deploying models such as double extortion exfiltration, initial access broker affiliates methods and Diamond Model of Intrusion to name a few.
- ⇒ LRG utilizes a modular approach and encrypts the payload until execution, which presents significant obstacles to malware analysis and detection.
- ⇒ LRG's preferred form of payment is privacy coin that cannot be tracked such as Monero cryptocurrency or ZCash cryptocurrency.
- ⇒ LockBit ransomware developers were secretly building a new version of their file encrypting malware, dubbed LockBit-NG-Dev - likely to become LockBit 4.0, when law enforcement took down the their servers in February 2024.

SOURCES

https://twitter.com/DarkWebInformer/status/1720868655037120602

https://blackkite.com/data-breaches-caused-by-third-parties/

https://www.1arabia.com/2024/03/it-services-industry-grapples-with.html

https://www.americanbanker.com/news/data-breach-affects-57-000-bank-of-america-accounts

https://www.linkedin.com/pulse/redefining-cybersecurity-insights-from-infosys-ransomware-1xzec/?trk=organization_guest_main-feed-card_feed-article-content

https://www.forbes.com/advisor/personal-finance/data-breach-affects-bank-of-america-customers/

https://apps.web.maine.gov/online/aeviewer/ME/40/c2da936e-14f0-421a-833e-a24cbdd79cfa.shtml

https://vulncheck.com/blog/mikrotik-foisted-revisited

https://www.identitytheft.gov/#/Info-Lost-or-Stolen

https://www.infosecurity-magazine.com/news/bank-america-customers-risk-data/

https://www.infosys.com/newsroom/press-releases/2012/producer-services-strategic-business-unit.html

https://www.myinjuryattorney.com/infosys-mccamish-systems-data-breach-class-action-investigation-and-lawsuit-assistance/

https://www.jdsupra.com/legalnews/infosys-mccamish-systems-announces-data-5328584/

https://securityscorecard.com/blog/infosys-mccamish-systems-third-party-breach/

https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

https://www.resecurity.com/blog/article/lockbit-30s-bungled-comeback-highlights-the-undying-risk-of-torrent-based-data-leakage

https://panorays.com/blog/boa-data-breach-2024/#:~:text=The%20data%20breach%20targeted%20and,an%20average%20of%20%244.45%20million

https://www.spiceworks.com/it-security/data-security/news/bank-of-america-data-breach-third-party-risk/

https://socradar.io/lockbit-3-another-upgrade-to-worlds-most-active-ransomware/

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-secretly-building-next-gen-encryptor-before-takedown/

https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program/#google_vignette

https://darkfeed.io/ransomwiki/

https://www.solutions4it.co.uk/lockbit-3-0-ransomware-attacks/

https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf

https://go.crowdstrike.com/global-threat-report-2024.html?utm_campaign=cao&utm_content=crwd-cao-amer-us-en-psp-x-wht-gtr-tct-x_x_x_x-x&utm_medium=sem&utm_source=goog&utm_term=current%20cyber%20security%20threats&cq_cmp=1705069828&cq_plac=&gad_source=1&gclid=CjwKCAjwkuqvBhAQEiwA65XxQM1cvQ5QGqpWxfdeRxkO0ZLcIKOb-kEUg_SeH-YZXHKVAupgaMIOuxoCe5UQAvD_BwE

https://www.virustotal.com/gui/file/c244ab74a7436cfcef4725474761a0996a8b3c66b8a67da675620382c2be962a

https://www.virustotal.com/gui/file/8d7a7439c4317f52b5bd3bb12a54e7f445c1b015d3dd027821daffa08fd892dc