BLOG POST

mimecast

Human Risk Roundup: A City Attacked, Salesloft Fallout, and VerifTools Thwarted

Baltimore loses money to BEC, the fallout from the Salesloft breach continues, and authorities believe they have taken down VerifTools

SEPTEMBER 5, 2025

Key Points

- A fraudster stole over $1.5 million from the city of Baltimore by impersonating a vendor and manipulating staff to change bank account details.
- A breach at Salesloft, an AI chatbot maker, resulted in the theft of authentication tokens, compromising data from nume rous corporate Salesforce instances and other integrated services.
- A joint U.S.-Dutch law enforcement operation has dismantled VerifTools, a major platform for creating fake identification documents used in various cybercrimes.

In this edition of the Human Risk Roundup, we dive into three high-profile recent newsworthy events – keep reading for more information.

Fraudster stole over $1.5 million from city of Baltimore

A fraudster stole over $1.5 million from the city of Baltimore by impersonating a vendor and manipulating staff to change bank account details, exploiting weak internal controls in a business email compromise (BEC) attack. Despite recovering part of the funds, the incident highlights ongoing vulnerabilities in the city's accounts payable processes, which have faced similar scams in the past.

What happened

This scheme, a classic BEC attack, occurred between February and March 2025, with two fraudulent payments totaling $1,524,621.04. The scammer accessed the vendor's Workday account and altered bank details, which were approved by accounts payable employees without proper verification. While the city recovered $721,236.60, the remaining $803,384.44 is still unrecovered, and an insurance claim has been filed. The investigation revealed weak internal controls and a lack of safeguards in the accounts payable department, which had failed to implement corrective measures after previous fraud cases. This incident follows two other vendor scams in Baltimore since 2019.

Why it matters

This attack highlights a significant cybersecurity incident where a fraudster exploited weak internal controls. The attacker used a common BEC tactic, posing as a vendor and altering bank account details to redirect payments. This

case underscores the critical need for robust verification processes and safeguards in financial systems to prevent such fraud. It also reveals a pattern of recurring vulnerabilities, as Baltimore has faced similar scams in the past, emphasizing the importance of learning from previous incidents. For cybersecurity personnel, this serves as a reminder to prioritize employee training, implement multi-factor authentication, and enforce strict document verification protocols. The incident demonstrates how lapses in basic security measures can lead to substantial financial and reputational damage.

Four practical tips for security leaders

1. Ensure that all changes to vendor bank details are thoroughly verified. Require multiple levels of approval and cross-check documentation, such as voided checks, to confirm authenticity.
2. Educate employees on recognizing phishing attempts and BEC schemes. Regular training can help staff identify red flags, such as unusual requests or discrepancies in documentation.
3. Conduct regular audits of accounts payable processes and implement safeguards to detect and prevent fraudulent activities. This includes adopting corrective measures after any fraud incidents to avoid repeat vulnerabilities.
4. Invest in advanced fraud detection systems that can flag suspicious activities, such as repeated attempts to change vendor details or access accounts from unusual locations.

The Ongoing Fallout from a Breach at AI Chatbot Maker Salesloft

A breach at Salesloft, an AI chatbot maker, resulted in the theft of authentication tokens, compromising data from numerous corporate Salesforce instances and other integrated services like Google Workspace and Amazon S3. The attack, attributed to the group UNC6395, has led to widespread data theft and raised concerns about the security of centralized identity platforms, prompting urgent remediation efforts from affected organizations.

What happened

Hackers stole authentication tokens, compromising not only Salesforce data but also integrations with services like Slack, Google Workspace, and Amazon S3. Google's Threat Intelligence Group revealed that the breach allowed attackers to exfiltrate sensitive data, including credentials for cloud services, potentially enabling further compromises. The breach, linked to UNC6395, has led to widespread warnings for companies to invalidate all tokens connected to Salesloft integrations. The incident is part of a broader trend of social engineering attacks, with groups like ShinyHunters and Scattered Spider exploiting access tokens to infiltrate systems. Salesloft has hired Mandiant to investigate the breach, but the root cause remains unclear.

Why it matters

This breach highlights critical vulnerabilities in authentication token security, affecting not just Salesforce but also integrations with major platforms like Google Workspace, Slack, and Microsoft Azure. Cybersecurity personnel must act swiftly to mitigate risks, as attackers have already exploited stolen tokens to access sensitive corporate data, including credentials for cloud services like AWS and Snowflake. This incident underscores the dangers of "authorization sprawl," where attackers leverage legitimate user access to move undetected across systems. The breach also reveals the growing sophistication of threat groups like UNC6395, who use social engineering and token theft to bypass traditional security measures. This case serves as a stark reminder of the cascading risks posed by third-party integrations in modern IT ecosystems.

Four practical tips for security leaders

1. Proactively invalidate and reissue authentication tokens, especially for third-party integrations, to minimize the risk of token theft and unauthorized access.
2. Implement strict controls to prevent "authorization sprawl," where attackers exploit legitimate user access tokens to move undetected between systems. Regular audits of access permissions and token usage can help mitigate this risk.

3. Evaluate and secure third-party integrations, as they can be a weak link in your security chain. Assume that data connected to compromised integrations may be at risk and take immediate remediation steps.
4. Train employees to recognize and respond to social engineering tactics, such as voice phishing, which attackers use to gain access to sensitive systems. Regular simulations and awareness campaigns can bolster defenses against these threats.

Law Enforcement Operation Seizes Fake ID Platform VerifTools

A joint U.S.-Dutch law enforcement operation has dismantled VerifTools, a major platform for creating fake identification documents used in various cybercrimes, including phishing and cryptocurrency theft. Authorities seized servers and domains, and investigations are ongoing to identify the platform's administrators and users, marking a significant step in combating identity fraud and cybercrime.

What happened

The operation involved seizing servers in Amsterdam and domain names in the U.S., which were used to generate counterfeit IDs for as little as $9. These fake IDs were exploited in various cybercrimes, including phishing, help desk fraud, and bypassing financial verification systems. Investigators are now analyzing the seized data to identify the platform's administrators and users. The FBI's investigation, which began in 2022, linked VerifTools to at least $6.4 million in illicit profits. Authorities emphasized the importance of targeting such platforms to combat fraud and identity theft effectively.

Why it matters

The takedown of VerifTools is a significant development for cybersecurity personnel. This platform enabled criminals to bypass identity verification systems, facilitating phishing, cryptocurrency theft, and other cybercrimes. By seizing its servers and domains, law enforcement disrupted a key tool in the cybercrime-as-a-service ecosystem. The operation highlights the importance of targeting not just cybercriminals but also the infrastructure that supports their activities. For cybersecurity teams, this underscores the need to strengthen identity verification processes and monitor for fraudulent activity. Additionally, the investigation's success demonstrates the value of international collaboration in combating cyber threats.

Four practical tips for security leaders

1. Ensure that your identity verification processes are robust enough to detect and prevent the use of fake IDs. This includes leveraging advanced technologies like AI and machine learning to identify anomalies in submitted documents.
2. Build strong partnerships with law enforcement agencies to share intelligence and collaborate on investigations targeting cybercrime platforms and their users.
3. Stay informed about the evolving cybercrime-as-a-service economy, which provides tools like fake IDs, malware, and bulletproof servers. Understanding these trends can help in anticipating and mitigating emerging threats.
4. 4. Conduct regular training and awareness programs for employees and customers to recognize and report phishing attacks, help desk fraud, and other scams that exploit fake identification documents.