10
OCT

THREAT INTEL REPORT 2024

CONVERGE
TECHNOLOGY SOLUTIONS

Prepared by: Converge Cybersecurity Practice
convergetp.com/cybersecurity | 800.747.8585

Observations for October 2024

October marks **Cybersecurity Awareness Month**, a time dedicated to reinforcing the importance of staying vigilant in the face of evolving cyber threats. As our digital world continues to grow, so do the risks that businesses and individuals face. The recent 23andMe data breach serves as a stark reminder that today's cybersecurity challenges have far-reaching consequences. Beyond the immediate impact, breaches like this can lead to prolonged financial, reputational, and operational setbacks. Cybersecurity isn't just about reacting to threats—it's about building resilience to secure our future.

This month, we dive into the evolving landscape of session hijacking. Once a network-focused threat, it has now shifted towards targeting identities in cloud-based environments. Attackers are increasingly bypassing multi-factor authentication using token replay attacks and advanced phishing techniques. This transformation in tactics underscores the need for innovative defenses and a deeper understanding of these modern methods to safeguard against the growing risks.

We also explore the discovery of a sophisticated side-channel attack known as RAMBO, which exploits electromagnetic emissions to exfiltrate data from air-gapped systems. This development highlights the ongoing innovation in cyber attacks, even against the most secure environments. As cyber threats continue to evolve, it's crucial to recognize that cybersecurity is a shared responsibility. The focus must remain on proactive strategies and collective efforts to defend against these threats, not only to protect our data today but to secure the innovations of tomorrow.

RETURN

Executive Overview

Cybersecurity Awareness Month - After Effects of a Security Incident

Audience

- CISO
- IT Managers
- Risk Management Professionals
- Cybersecurity Professionals and Analysts
- C-Suite Executives
- Business Organizations

SUMMARY: October is Cybersecurity Awareness Month, a crucial period for highlighting the ever-growing significance of cybersecurity in our interconnected world. This report aims to emphasize that cybersecurity is not only about responding to current threats but also about mitigating their long-term impact. The recent developments in the 23andMe data breach case exemplify the long-lasting consequences of cybersecurity lapses on businesses and individuals. The breach's aftermath highlights how vulnerabilities can lead to financial, reputational, and operational challenges that persist far beyond the initial incident. As cyber threats continue to evolve, the report stresses the collective responsibility that all individuals and organizations share in safeguarding against these risks.

Tactical guidance >> Cybersecurity Awareness Month

The Evolution of Session Hijacking: Modern Threats in an MFA-Dominated Landscape

Audience

- CISO
- Security Managers
- Cybersecurity Professionals

SUMMARY: Session hijacking, once reliant on network-based attacks, has evolved into an identity-centric threat targeting cloud-based services. With a surge in token replay attacks, attackers leverage phishing toolkits and infostealer malware to compromise session cookies, effectively bypassing multi-factor authentication (MFA). The analysis explores the modern methods of session hijacking, examines the shift in attacker tactics, and offers strategic, operational, and tactical insights for detection and mitigation. It also highlights the implications of these attacks on organizations and provides hypotheses for proactive threat hunting.

Tactical guidance >> The Evolution of Session Hijacking

RETURN

Audience

- Cybersecurity Professionals
- IT Engineering Teams
- C-Suite Executives
- Network and IT Administrators

RAMBO: Novel Side-Channel Attack Targeting Air-Gapped Systems

SUMMARY: A new and sophisticated side-channel attack, known as RAMBO (Radiation of Air-gapped Memory Bus for Offense), has been discovered, leveraging electromagnetic emissions from a computer's RAM to exfiltrate sensitive data from air-gapped systems. Developed by Dr. Mordechai Guri from Ben-Gurion University of the Negev, this attack can bypass physical isolation by using radio signals emitted from the RAM to transmit data. This development highlights the evolving nature of cyber threats targeting even the most secure environments. Effective mitigation strategies will need to address both the technical aspects of the RAMBO attack and the broader issue of securing air-gapped systems against similar covert threats.

Tactical guidance >> RAMBO: Novel Side-Channel Attack Targeting Air-Gapped Systems

Tactical Guidance

Cybersecurity Awareness Month - After effects of a Security Incident

Due to the breach, 23andMe settled

for $30 million compensation

Overview & Impact

The 23andMe data breach, which involved a credential stuffing attack, affected approximately 6.9 million individuals, resulting in significant financial and reputational damage to the company. The settlement of $30 million aims to provide compensation to those affected while also covering identity and genetic monitoring services. However, the case also serves as a stark reminder of the broader impact such breaches can have on an organization's future stability, the trust of its customers, and its market valuation.

Observations

- **Cybersecurity Awareness Month:** Since its inception in 2004, Cybersecurity Awareness Month has been a collaborative effort to promote cybersecurity best practices and risk mitigation across sectors.
- **2024 Theme:** The 2024 theme, "Secure Our World," encourages continuous daily actions to protect against online threats, reinforcing that cybersecurity is a shared responsibility.
- **Data Breach Summary:** Breaches often involve unauthorized access to user accounts through methods like credential stuffing, which can compromise sensitive information.

RETURN

- **Targeted Attacks:** Specific groups within affected populations may be targeted based on demographic factors, making data security and privacy protection even more critical.

Guidance

Strategic Intelligence

- **Business Impact:** The financial consequences of data breaches can be severe, with organizations often experiencing a significant decline in market value and investor confidence post-incident.

- **Cyber Resilience:** Investing in cyber resilience strategies is essential to mitigate future risks and minimize long-term operational disruptions, ensuring business continuity and stability.

- **Regulatory Compliance:** Compliance with data privacy laws and regulations is increasingly becoming a focal point for organizations, especially those handling sensitive information.

- **Proactive Preparation:** Anticipating and preparing for evolving regulatory requirements can help mitigate legal risks and enhance an organization's ability to protect customer data effectively.

Operational Intelligence

- **Credential Stuffing:** Cyber attacks often exploit poor password hygiene, where compromised credentials from other breaches are used to gain unauthorized access.

- **Authentication Measures:** Implementing multi-factor authentication (MFA) and advanced user behavior analytics can significantly reduce the risk of these attacks.

- **Incident Communication:** Delays in disclosing the full scope of data breaches can damage credibility and erode customer trust.

- **Transparent Strategies:** Transparent communication strategies during incident response are critical to maintaining trust and minimizing the impact on the organization's reputation.

Tactical Intelligence

- **Cyber Insurance:** Organizations that invest in cyber insurance can better manage the financial impact of data breaches, using the coverage to offset legal costs and settlement expenses.

- **Policy Coverage:** It is crucial to ensure that cyber insurance policies are comprehensive and aligned with the specific risks associated with an organization's operations.

- **Security Measures:** Encouraging the adoption of strong, unique passwords and enabling MFA are foundational steps in defending against credential-based attacks.

- **Awareness Training:** Regular security awareness training can empower employees to recognize and respond to phishing attempts and other social engineering tactics.

RETURN

Threat Hunting Hypotheses

Data Exfiltration via High Network Traffic Spikes

- **Hypothesis:** Large volumes of outbound traffic, particularly over short periods, may indicate ongoing data exfiltration efforts by threat actors using tools such as rclone or WinSCP. These activities are likely to cause noticeable spikes in network traffic, especially in critical sectors.
- **Investigation Approach:**
  - **Network Monitoring:** Monitor outbound network traffic for unusual spikes exceeding normal data flow, particularly volumes over 150 GB.
  - **Data Transfer Controls:** Use network security controls to flag data transfers involving external cloud storage services like Mega or AWS S3.
  - **Alert Setup:** Set up alerts for sudden, large transfers to new or previously unused external endpoints.
  - **Correlation Analysis:** Correlate the timing of traffic spikes with other indicators of compromise, such as suspicious login activity or the presence of known data transfer tools.

Exploitation of Known Vulnerabilities

- **Hypothesis:** Threat actors often exploit publicly disclosed vulnerabilities in critical infrastructure, such as CVE-2023-3519 (Citrix NetScaler) and CVE-2023-46747 (F5 BIG-IP). Unpatched systems are at a heightened risk of compromise through these vulnerabilities.
- **Investigation Approach:**
  - **Vulnerability Scanning:** Conduct regular scans for systems running vulnerable software versions, particularly Citrix and F5 appliances.
  - **Log Review:** Review security logs for exploit attempts targeting these CVEs.
  - **Patch Management:** Prioritize patching for systems identified with vulnerabilities that are actively exploited in the wild.
  - **Abnormal Activity Detection:** Set up alerts to detect abnormal access attempts or configuration changes on critical systems.

Suspicious Lateral Movement Across the Network

- **Hypothesis:** Adversaries frequently use lateral movement techniques, leveraging tools like PsExec, Cobalt Strike, and Metasploit to expand their reach within compromised networks. Unexpected lateral movements, especially from lower-privileged accounts, could indicate an ongoing attack.
- **Investigation Approach:**
  - **Execution Monitoring:** Monitor for unusual or unauthorized PsExec executions, particularly on critical servers.
  - **Pattern Analysis:** Track lateral movement patterns within the network, including the use of remote desktop protocols (RDP) and suspicious service creations.
  - **Tool Detection:** Set up detection rules to identify Cobalt Strike beacons or Metasploit usage.

RETURN

Sources

- Malwarebytes: 23andMe to pay $30 million in settlement over 2023 data breach
- HIPAA Journal: 23andMe Class Action Data Breach Settlement
- USA Today: 23andMe Class Action Lawsuit Settlement
- InformationWeek: 23andMe $30M Data Breach Settlement - How Valuable is Genetic Data?
- The Verge: 23andMe Settlement DNA Data Breach Lawsuit
- CNET: 23andMe Agrees to $30M Settlement That Could Pay $10,000 to Data Breach Victims
- Reuters: 23andMe Settles Data Breach Lawsuit for $30 Million

  - **Privilege Escalation Detection:** Analyze logs for the use of Windows Management Instrumentation (WMI) for privilege escalation and antivirus deactivation.

Use of Anonymizing Tools for Persistence and Evasion

- **Hypothesis:** Threat actors may deploy VPNs, proxy servers, or TOR to mask their true location and evade detection. These tools are often used to maintain persistence while accessing compromised systems.
- **Investigation Approach:**
  - **Traffic Analysis:** Analyze network traffic for signs of VPN or proxy tool usage that might indicate an adversary attempting to obfuscate their actions.
  - **Login Correlation:** Correlate login activity with known VPN and anonymization tool usage, especially when accessing sensitive systems.
  - **Persistent Connection Flagging:** Flag persistent connections to TOR exit nodes or proxy servers associated with high-risk activities.
  - **Geofencing Implementation:** Implement geofencing to detect access attempts from unexpected or masked locations.

The Evolution of Session Hijacking: Modern Threats in an MFA-Dominated Landscape

Overview & Impact

Session hijacking has transformed from traditional Man-in-the-Middle (MitM) tactics to sophisticated attacks that exploit the vulnerabilities in identity management for cloud services. This shift reflects an increase in both the frequency and effectiveness of these attacks, bypassing even advanced security controls such as MFA.

Statistics Highlighting the Threat:

- Microsoft reported a 111% increase in token replay attacks in 2023, totaling 147,000 incidents.

Increase in frequency and effectiveness

of Man-in-the-Middle (MitM) tactics

- Google indicated that attacks on session cookies now rival the prevalence of password-based attacks.

Modern session hijacking methods primarily involve targeting browser-based data through infostealers or using advanced phishing toolkits like AitM (Adversary-in-the-Middle) and BitM (Browser-in-the-Middle). These methods allow attackers to circumvent MFA, taking advantage of cloud-based applications that rely on identity as the new security perimeter.

Observations

- **Shift from Network to Identity-Based Attacks:**
  - **Legacy Attacks:** Historically, session hijacking relied on intercepting unencrypted network traffic.
  - **Modern Techniques:** Now predominantly involve identity-centric attacks over the public internet targeting cloud applications.
- **Phishing Toolkits (AitM and BitM):**
  - **AitM:** Acts as a proxy, capturing authentication material including session tokens as users complete MFA checks.
  - **BitM:** More sophisticated; involves tricking the victim into controlling the attacker's browser remotely.
- **Infostealers:**
  - Primarily opportunistic, targeting all session cookies saved in the victim's browser, potentially compromising multiple accounts and services.
  - Can evade detection by endpoint detection and response (EDR) solutions, especially when infecting unmanaged devices.
- **Malware-Enabled Session Hijacking:**
  - Infostealers like EvilProxy and Emotet have been increasingly used to exfiltrate session data from infected devices.
  - Malware infections often lead to long-term, undetected access to corporate networks.

Guidance

Strategic Intelligence

- **Adapting to the Identity-Driven Threat Landscape:**
  - Organizations need to shift their security focus to identity-based defenses as attackers increasingly target session tokens to bypass traditional controls like MFA.
- **Importance of Visibility into Session Management:**
  - Enhanced monitoring and proactive session validation can help identify unauthorized sessions, reducing the risk of data breaches.
  - Investing in tools that detect anomalous use of session tokens is critical to thwarting these advanced attacks.

RETURN

- **Balancing User Experience with Security:**
    - Solutions like passkeys offer a potential way forward but need to be integrated with robust session monitoring to counteract infostealers.

Operational Intelligence

- **Detection Techniques:**
    - Monitor for unusual sign-ins or session activity, particularly from new devices or locations inconsistent with the user's profile.
    - Employ conditional access policies to limit access based on device compliance and IP address reputation.
- **Mitigation Strategies:**
    - Enforce multi-factor authentication (MFA) with phishing-resistant options.
    - Regularly review session expiration policies to ensure timely invalidation of tokens.
- **Incident Response Enhancements:**
    - Quickly invalidate tokens upon detecting any suspicious session activity.
    - Implement automated password resets and session terminations when compromised credentials are detected.

Tactical Intelligence

- **Tools and Techniques Utilized by Attackers:**
    - **Advanced Phishing Kits:** AitM and BitM have become the preferred tools due to their ability to harvest both credentials and session tokens.
    - **Infostealers:** Typically deployed through phishing, malvertising, or malicious software, targeting browsers to extract session data.
- **EDR and AV Evasion:**
    - Attackers are using customized malware to avoid detection, indicating a need for advanced behavioral analysis in endpoint protection.
- **Recommended Defensive Controls:**
    - Increase reliance on user and entity behavior analytics (UEBA) to detect anomalous session behavior.
    - Ensure web applications enforce strong encryption for session cookies and robust session management practices.

Threat Hunting Hypotheses

Session Hijacking through Infostealer Malware

- **Hypothesis:** Threat actors are utilizing infostealer malware to exfiltrate session tokens from compromised devices, allowing them to bypass authentication mechanisms such as MFA and gain unauthorized access to cloud-based services.

RETURN

- **Investigation Approach:**
  - Monitor endpoint logs for indicators of infostealer malware activity, focusing on anomalous downloads or executables associated with known infostealers.
  - Analyze browser activity logs for signs of session cookie exportation or unauthorized session token usage across different IP addresses.
  - Cross-reference instances of unusual sign-ins with known Indicators of Compromise (IOCs) linked to infostealer malware campaigns.
  - Set up alerts for any sudden changes in device or location of session initiation that does not align with established user behavior.

Phishing Toolkits (AitM and BitM) Bypassing MFA

- **Hypothesis:** Threat actors are employing advanced phishing techniques using AitM (Adversary-in-the-Middle) and BitM (Browser-in-the-Middle) toolkits to intercept MFA challenges and session tokens.
- **Investigation Approach:**
  - Monitor network traffic for signs of proxy-based phishing attacks, focusing on requests that mimic legitimate authentication flows.
  - Audit user account activity to identify instances where MFA was successfully completed but the originating IP address or device is inconsistent with known user patterns.
  - Analyze authentication logs for unusual spikes in MFA challenges or repeated MFA attempts from unfamiliar locations.
  - Implement alerts for sudden changes in user agent strings or session initiation from browsers with unfamiliar configurations.

Cross-Device Session Syncing Leading to Credential Exposure

- **Hypothesis:** Infostealer malware on personal or unmanaged devices is exfiltrating synchronized corporate credentials stored in browser profiles, resulting in session hijacking or further credential abuse.
- **Investigation Approach:**
  - Review synchronization logs across devices to identify discrepancies where corporate credentials appear on unmanaged or personal endpoints.
  - Investigate patterns of session token reuse from unexpected devices or IP addresses, especially those linked to BYOD environments.
  - Analyze any unusual browser profile sync activity that occurs shortly before or after a known infostealer infection.
  - Set up alerts for unauthorized session token imports into browsers that are not part of the corporate device fleet.

Use of Malware-Enabled Session Tokens for Persistent Access

- **Hypothesis:** Attackers are leveraging stolen session tokens to maintain persistent access to corporate networks, evading detection by bypassing MFA and traditional authentication mechanisms.

RETURN

- **Investigation Approach:**
  - Monitor cloud service activity logs for prolonged sessions with consistent token reuse that lacks fresh authentication challenges.
  - Correlate session data with known compromised endpoints to identify potential re-import of session tokens by unauthorized actors.
  - Implement real-time alerts for instances of session activity originating from IP addresses or devices that have not been previously seen within the environment.
  - Examine cases where legitimate session tokens are used from geographic locations significantly different from where the session was initially established.

Collaboration with Ransomware Actors for Session Exploitation

- **Hypothesis:** After initial compromise via session hijacking, threat actors are collaborating with ransomware groups (e.g., EvilProxy, Emotet) to leverage stolen session tokens in orchestrating ransomware deployment across the network.
- **Investigation Approach:**
  - Monitor for suspicious session activity linked to known ransomware affiliates' TTPs (Tactics, Techniques, and Procedures), especially the use of tools for remote access and lateral movement.
  - Analyze logs for any attempt to establish encrypted tunnels or backdoors that could facilitate data exfiltration and ransomware deployment.
  - Investigate unauthorized changes in session policies or cloud application configurations that may indicate preparation for a ransomware attack.
  - Implement alerts for abnormal file encryption events on systems where session tokens were recently hijacked or re-imported by attackers.

Sources

- Microsoft: Overcoming the Rising Threat of Session Hijacking
- The Hacker News: Session Hijacking 2.0
- Dark Reading: Addressing Session Hijacking Vulnerabilities
- LinkedIn: Credential Abuse and Session Hijacking Trends
- Fuse Technology: Protecting Microsoft Accounts from Session Hijacking

RAMOB bypasses physical isolation by using radio signals.

RAMBO: Novel Side-Channel Attack Targeting Air-Gapped Systems

Overview & Impact

A new and sophisticated side-channel attack, known as RAMBO (Radiation of Air-gapped Memory Bus for Offense), has been discovered, leveraging electromagnetic emissions from a computer's RAM to exfiltrate sensitive data from air-gapped systems. Developed by Dr. Mordechai Guri from Ben-Gurion University of the Negev, this attack can bypass physical isolation by using radio signals emitted from the RAM to transmit data. This development highlights the evolving nature of cyber threats targeting even the most secure environments. Effective mitigation strategies will need to address both the technical aspects of the RAMBO attack and the broader issue of securing air-gapped systems against similar covert threats.

Observations

- **Attack Methodology:**
  - Uses On-Off Keying (OOK) and Manchester encoding techniques to manipulate RAM operations and generate controlled electromagnetic emissions.
  - Leverages software-defined radio (SDR) technology for signal reception, allowing attackers to decode the emissions into readable data.
- **Transmission Range:**
  - Slow transmissions can achieve nearly zero error rates up to 7 meters (23 feet).
  - Fast transmissions reach up to 3 meters (10 feet) but suffer from a 2-4% bit error rate.
- **Performance Limitations:**
  - At 1,000 bps, it takes around 2.2 hours to exfiltrate 1 megabyte of data, making the technique more suited for small data exfiltration like passwords or keylogging.
- **Vulnerabilities:**
  - Even systems with robust physical isolation measures are susceptible due to electromagnetic emissions from their components.
  - Air-gapped systems relying solely on physical isolation need to address these emission-based covert channels.

RETURN

Guidance

Strategic Intelligence

- **Trend Analysis:**
    - RAMBO represents a continued evolution in attack strategies targeting air-gapped systems, challenging the notion of complete security through isolation.
    - Historical precedence shows Dr. Guri's consistent innovation in air-gap attack techniques, including SATAn, GAIROSCOPE, and AirKeyLogger, indicating a trend toward exploiting physical properties of computer components.
- **Implications for Critical Infrastructure:**
    - The potential compromise of systems in critical sectors such as defense and energy highlights the importance of updating security frameworks to include defenses against electromagnetic and side-channel attacks.
    - State actors and advanced persistent threats (APTs) are likely to exploit such techniques for cyber espionage and sabotage.

Operational Intelligence

- **Attack Vectors:**
    - Requires prior infection of the air-gapped system via physical media (USB drives), supply chain compromises, or malicious insiders.
    - Once malware is in place, it leverages system RAM to modulate electromagnetic emissions to transmit sensitive data.
- **Detection Challenges:**
    - Standard security solutions fail to monitor the electromagnetic emissions used in RAMBO, making it difficult to detect with traditional intrusion detection systems.
    - Anomalous memory access patterns caused by the attack are subtle and often indistinguishable from legitimate processes.

Tactical Intelligence

- **Mitigation Strategies:**
    - **Physical Security:** Employ Faraday cages and electromagnetic shielding around sensitive systems to prevent the leakage of radio signals.
    - **Intrusion Detection Systems (IDS):** Implement hypervisor-level memory monitoring and electromagnetic intrusion detection to detect anomalous memory operations.
    - **Data Encryption:** Encrypt sensitive data to render it unreadable even if exfiltrated through RAMBO.
    - **Access Controls:** Strengthen access controls to air-gapped systems, utilizing biometric verification and physical security measures.
    - **Signal Jamming:** Deploy signal jammers to disrupt radio frequencies that RAMBO relies on for data transmission.

RETURN

- **Preventive Measures:**
  - Regularly update supply chain security protocols to prevent initial malware installation.
  - Conduct regular security audits and drills focusing on side-channel and electromagnetic threats.

Threat Hunting Hypotheses

Data Exfiltration via RAMBO Attack on Air-Gapped Systems

- **Hypothesis:** Threat actors may leverage the RAMBO attack to exfiltrate sensitive data from air-gapped systems by manipulating electromagnetic emissions from the RAM, targeting environments with highly sensitive information, such as defense installations or critical infrastructure.
- **Investigation Approach:**
  - **Monitor Electromagnetic Emissions:** Deploy electromagnetic signal analyzers to continuously monitor for unusual emissions patterns near air-gapped systems, focusing on signals that correspond to known frequencies of RAM operation.
  - **Analyze Memory Access Patterns:** Review system logs and telemetry for anomalies in memory read/write operations that could indicate an attempt to manipulate RAM to generate encoded electromagnetic signals.
  - **Cross-Reference Physical Security Logs:** Correlate any detected electromagnetic signals with physical security logs to identify unauthorized personnel or devices within proximity to the air-gapped systems.
  - **Set Up Alerts for Suspicious Activity:** Configure alerts for sudden spikes in electromagnetic emissions or unexpected RAM activity, especially during off-hours, that could indicate potential covert data transmission attempts.

Sources

- Arxiv.org - Research on RAMBO Attack
- HackRead - RAMBO Attack Uses RAM in Air-Gapped Systems to Steal Data
- TechRadar - RAMBO Attack Explained
- eSecurity Planet - RAMBO Attacks Explained
- SecurityWeek - New RAMBO Attack Allows Air-Gapped Data Theft
- Bleeping Computer - New RAMBO Attack Steals Data from Air-Gapped Systems
- The Hacker News - RAMBO Attack Uses RAM Radio Signals

RETURN

CONVERGE
TECHNOLOGY SOLUTIONS

Contact the Converge Threat Intel Group at cybersecurity@convergetp.com

convergetp.com/cybersecurity