مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploiting Browser Isolation Using QR Codes

Tracking #:432316611

Date:10-12-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a recent research has revealed a novel method for bypassing browser isolation to establish C2 channels.

TECHNICAL DETAILS:

Browser isolation is a crucial cybersecurity technique that helps prevent web-based attacks by running web browsers in isolated, secure environments (cloud, on-premises, or local containers). This security mechanism is particularly effective in protecting users from phishing, malware, and command-and-control (C2) operations that typically rely on web traffic to compromise devices. However, recent research has revealed a novel method for bypassing browser isolation to establish C2 channels. The technique leverages machine-readable QR codes to send commands from a remote server to a compromised device, even when browser isolation is used.

The New C2 Technique:

1. Mechanism:
    - Attackers send a web page containing a QR code from the C2 server.
    - A malicious implant on the victim's device uses a local headless browser to render this page and capture a screenshot.
    - The implant decodes the QR code to retrieve commands, allowing attackers to control compromised systems.
2. Technical Specifications:
    - Data Capacity: QR codes can hold up to 2,189 bytes of data due to visual quality limitations.
    - Latency: Approximately 5 seconds per request due to browser rendering times.
    - Throughput: Around 438 bytes per second for payload transfer.
3. Proof of Concept: Mandiant developed a proof-of-concept implant using Puppeteer and Google Chrome in headless mode, which integrates with Cobalt Strike's External C2 feature.

Risks and Implications:

1. Circumvention of Browser Isolation: This novel technique demonstrates a way to bypass the protective measures of browser isolation, which is typically employed to safeguard against phishing, remote code execution, and malicious C2 operations.
2. Increased Attack Surface: The method allows attackers to maintain command-and-control over compromised devices, even when isolation mechanisms are in place. The attack is resilient against all three types of browser isolation: remote, on-premises, and local.
3. Latency and Bandwidth Limitations: While the technique is effective, it requires substantial latency and bandwidth, as each request involves multiple HTTP requests and QR code scanning, which may limit its feasibility for high-speed, high-volume attacks.
4. Detection Risks: The low-bandwidth nature of the attack makes it harder to detect using traditional network monitoring methods, increasing the risk of prolonged undetected intrusions.

RECOMMENDATIONS:

1. **Monitor Network Traffic**:
   - Implement systems to detect anomalous network patterns, particularly frequent HTTP requests that may indicate C2 activity.
2. **Detect Automated Browser Usage**:
   - Monitor for browsers running in automation mode by inspecting process command lines for specific flags like --enable-automation and --remote-debugging-port.
3. **Enhance Web Traffic Analysis**:
   - Utilize advanced web traffic analysis tools to identify suspicious patterns or content, including potential QR code transmissions.
4. **Implement Defense-in-Depth**:
   - While browser isolation is valuable, organizations should adopt a comprehensive cybersecurity strategy that includes multiple layers of protection.
5. **Regular Security Assessments**:
   - Conduct frequent security audits and penetration tests to identify vulnerabilities in browser isolation implementations.
6. **Employee Training**:
   - Educate staff about the risks of browser-based attacks and the importance of reporting suspicious activities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://cloud.google.com/blog/topics/threat-intelligence/c2-browser-isolation-environments/