

MARCH 2025 MONTHLY BULLETIN



Key Takeaways

CyberForceIQ continues to work diligently to detect the latest threats within the cyber landscape. We are excited to share our most recent Monthly Bulletin to cover the most prominent security incidents over the past month and discuss new Digital Forensics and Incident Response measures used by both adversaries and security professionals.

- Conduct regular phishing awareness training for all employees, emphasizing the risks of QR codes, suspicious links, and social engineering tactics.
- HR impersonation and credential harvesting tactics represents an evolving threat that uses advanced techniques such as email spoofing, embedded HTML forms, and QR code phishing to bypass traditional security measures.
- Medusa Ransomware exploits public-facing vulnerabilities, particularly in Microsoft Exchange Servers, to gain access to victim networks.

Case Study

Phishing Campaigns Impersonating Internal HR Department

Overview

Recently, CyberForceIQ's Security Operation Center has observed an influx in a targeted phishing campaign, in which attackers impersonate a company's internal HR department to harvest user credentials. The phishing emails typically present a malicious link or QR code, purporting to lead to an updated employee handbook or internal documents. Upon user interaction, attackers capture credentials through embedded HTML forms or redirect users to fake login pages. This campaign utilizes several techniques to bypass traditional email security and target trusted internal resources.

Campaign Overview

The phishing emails are crafted to look legitimate, appearing as communications from the company's HR department. These emails employ social engineering to:

- **Harvest credentials:** Direct users to fake login pages or trick them into submitting credentials via HTML forms.
- **Evade detection:** Use techniques like embedded QR codes and spoofed sender addresses to evade traditional email security systems.

The subject lines typically contain phrases such as "New Company Handbook" or "HR Update," urging the user to open attachments or click links urgently.

Attack Vectors

1. Email Spoofing (T1071.001):

- Attackers use email spoofing to make phishing emails appear as though they come from trusted internal sources such as HR personnel. The email addresses often mirror legitimate addresses with slight modifications (e.g., hr-updates@company.com instead of hr@company.com).

2. Embedded HTML Forms (T1566.001):

- The phishing emails contain HTML attachments that resemble internal company login forms. These forms are designed to capture user credentials when submitted. The attackers may use JavaScript to capture login data or submit the credentials to an external server.

3. QR Code Phishing (T1566.001):

- QR codes embedded within the emails redirect users to fraudulent login pages when scanned. These malicious sites are crafted to look like the company's internal portals and are optimized for mobile devices, making it more likely that users will fall for the scam when using their smartphones.

4. Credential Harvesting via Fake Login Pages (T1071.001):

- The phishing emails often include links that point to fake login portals designed to mimic the company's legitimate login systems. These fake pages capture credentials entered by the victim, potentially harvesting usernames, passwords, and multi-factor authentication (MFA) tokens.

Observed Techniques and Tools

- **Spoofed Sender Address:** The attacker's emails are crafted to resemble internal HR department communications, using slight variations in domain names to bypass email filters (e.g., hr-update@company.com).
- **HTML Form Fields:** The HTML attachments include hidden form fields designed to capture user input when submitting credentials (e.g., <input type="hidden" name="username">).
- **Phishing Links:** The email includes links that lead to fake login pages with URLs that may look similar to the organization's legitimate web address but contain slight variations (e.g., company-login.hr-update.com).
- **QR Code Redirect:** QR codes are embedded to lead users to external phishing sites. Scanning the code with a mobile device often bypasses traditional email filtering mechanisms, making this method harder to detect.

MITRE ATT&CK Techniques

- **Phishing (T1566):** The campaign uses spear-phishing emails as the primary vector for credential harvesting.
- **Spearphishing via Service (T1193):** The inclusion of QR codes provides a new vector for phishing, redirecting users to malicious websites when scanned.
- **Input Capture (T1056.001):** Malicious login pages capture credentials through JavaScript keyloggers or form submissions to external servers.
- **Credential Dumping (T1003):** Once credentials are harvested, they are potentially used to access internal systems and escalate privileges.

Impact

The primary impact of this phishing campaign is the theft of user credentials, which may lead to:

- **Account Compromise:** Successful credential harvesting could allow attackers to gain unauthorized access to sensitive internal resources.
- **Privilege Escalation:** Stolen credentials may provide attackers with elevated access to critical internal systems.
- **Lateral Movement:** Attackers could use stolen credentials to move laterally within the network and compromise additional accounts or systems.
- **Malware Deployment:** After credential theft, attackers could potentially deploy further malicious payloads such as ransomware or other forms of malware.

Detection and Mitigation Recommendations

1. Email Filtering and Detection:

- Utilize email security tools that integrate machine learning and advanced filtering techniques to detect email spoofing, domain anomalies, and embedded phishing links.
- Block or flag emails containing QR codes or HTML attachments from untrusted senders.
- Configure anti-spoofing technologies (SPF, DKIM, and DMARC) to ensure that emails purporting to come from internal sources are properly validated.

2. Multi-Factor Authentication (MFA):

- Enforce multi-factor authentication (MFA) for all internal systems, especially for applications that handle sensitive data or access critical resources.

3. User Behavior Analytics:

- Monitor and flag unusual login behavior, such as multiple failed login attempts, logins from unexpected locations, or abnormal access patterns.
- Use anomaly detection to identify login attempts that deviate from typical user behavior.

4. Web Application Firewall (WAF):

- Deploy a WAF to block access to malicious external sites that host fake login pages or phishing forms.
- Prevent access to unapproved domains masquerading as internal resources.

5. Security Awareness Training:

- Conduct regular phishing awareness training for all employees, emphasizing the risks of QR codes, suspicious links, and social engineering tactics.
- Encourage users to verify any unexpected communications from internal departments by contacting them through official channels before acting on links or attachments.

6. Incident Response:

- Implement a robust incident response plan for phishing attempts, including immediate password resets and account reviews for employees who report phishing attempts.
- Use EDR (Endpoint Detection and Response) tools to detect and investigate any keylogging or credential exfiltration activities.

Conclusion

The observed phishing campaign targeting internal users through HR impersonation and credential harvesting tactics represents an evolving threat that uses advanced techniques such as email spoofing, embedded HTML forms, and QR code phishing to bypass traditional security measures. Prompt implementation of detection mechanisms, user training, and multi-layered defenses can mitigate the risk and prevent further exploitation of stolen credentials.

External Trend

Medusa Ransomware Threat in 2025

Overview

In 2025, the Medusa ransomware group has intensified its attacks, impacting over 40 organizations within the first two months. The group demands ransoms ranging from \$100K to \$15M and has primarily targeted sectors such as healthcare, government, and finance. Medusa employs a double extortion approach, stealing data as a health care, government, and finance. Medusa employs a double extortion approach, stealing data as health care, government, and threatening it unless the ransom is paid. Vulnerabilities in Microsoft Exchange Servers remain a primary attack vector for initial access.





Tactics, Techniques, and Procedures (TTPs)

- **Exploitation of Vulnerabilities:** The group exploits public-facing vulnerabilities, particularly in Microsoft Exchange Servers, to gain access to victim networks.
- **Use of Remote Management Tools (RMM):** Tools like AnyDesk, SimpleHelp, and MeshAgent are deployed for remote access and persistence.
- **Data Exfiltration:** Before deploying ransomware, Medusa steals sensitive data using tools like Rclone and RoboCopy, which facilitates large-scale data exfiltration.
- **Lateral Movement:** Attackers leverage PDQ Deploy for lateral movement and deploy tools like KillAV to disable antivirus software and evade detection.

Impact

Medusa's aggressive tactics and high ransom demands make it a significant threat. Its attacks are strategically aimed at high-value targets, and the ransomware continues to evolve, becoming more sophisticated in its exploitation of vulnerabilities and evasion techniques.

Recommendations

-  **Patch Vulnerabilities:** Ensure Microsoft Exchange Servers are fully updated and securely configured to mitigate initial access risks.
-  **Monitor Remote Access Tools:** Detect and block unauthorized RMM software to prevent attackers from maintaining persistent access.
-  **Network Segmentation:** Isolate critical systems to prevent lateral movement and limit the scope of infections.
-  **Endpoint Protection:** Deploy advanced anti-malware solutions to identify and block tools like KillAV and Rclone used for evasion and data exfiltration.

The rise of Medusa ransomware underlines the continued need for organizations to stay vigilant in securing their systems and preventing ransomware attacks, especially those targeting public-facing vulnerabilities.

How CyberForceIQ Can Help

For 29 years, CyberForceIQ has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForceIQ, in collaboration with our participants, is protecting the cyber realm.

Contact Us For More Information

248-837-1400 • solutions@cyberforceiq.com

