AL2024_43 New Rockstar 2FA Phishing Service Targets Microsoft 365 Accounts (4th December 2024)

Description

Rockstar 2FA is a new phishing-as-a-service (PhaaS) platform facilitating adversary-in-the-middle (AiTM) attacks to compromise Microsoft 365 accounts, bypassing multifactor authentication (MFA). This sophisticated platform, which builds on older kits like DadSec and Phoenix, exploits session cookies to gain unauthorized access to accounts, underscoring the evolution of phishing tactics and the persistent risks associated with PhaaS ecosystems.

Attack Details

Rockstar 2FA uses adversary-in-the-middle (AiTM) techniques to deceive users with fake login pages that mimic Microsoft 365, tricking victims into entering their credentials. These credentials are proxied to legitimate Microsoft servers, allowing the attacker to intercept valid session cookies and bypass multifactor authentication (MFA) to access accounts without needing additional verification. The Rockstar 2FA platform supports Microsoft 365, Hotmail, GoDaddy, and Single Sign-On (SSO) systems and employs stealth features like randomized code, Cloudflare Turnstile Captcha for bot filtering, and multiple login themes with automated branding. With over 5,000 phishing domains deployed since May 2024, attacks are distributed through malicious emails leveraging tools like QR codes, URL shorteners, and PDF attachments. The user-friendly admin panel offers real-time logs, branding customization, and API access. Phishing campaigns use lures like document-sharing prompts, IT notices, payroll alerts, and password reset requests, with the AiTM system redirecting researchers or bots to benign decoy pages, ensuring operational stealth.

Indicators of Compromise (IOCs)

- **Phishing Domains:** Look for unusual domains mimicking Microsoft services or similar high-profile targets.
- **Email Characteristics:** Suspicious attachments (PDFs) or QR codes. URLs redirecting to phishing pages via legitimate-looking short links. Language mimicking document-sharing or payroll notifications.
- **Session Cookie Behavior:** Unauthorized session replays or logins, even with MFA enabled.
- **IP Patterns:** Repeated login attempts from unrecognized geolocations or IPs flagged as risky.

Remediation

1. **User Awareness and Training:**

- Conduct phishing awareness campaigns to educate employees about identifying deceptive emails.

2. **Technical Measures:**
   - Implement Conditional Access Policies to restrict logins based on device and location.
   - Deploy phishing-resistant MFA methods such as FIDO2 security keys.
   - Monitor for unusual cookie behavior or account activities.
3. **Incident Response:**
   - Use endpoint detection tools to identify malicious activities.
   - Revoke suspicious sessions and force MFA re-authentication for all users upon detection of suspicious activity.
4. **Collaboration and Reporting:**
   - Report phishing attempts and domains to Microsoft, CIRT.GY and Cybercrime Unit.
   - Leverage threat intelligence platforms to stay updated on evolving tactics.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

1. Lakshmanan.R Phishing-as-a-Service “Rockstar 2FA” targets Microsoft 365 users with AITM attacks. (2024, November 29). Retrieved from The Hacker News. https://thehackernews.com/2024/11/phishing-as-service-rockstar-2fa.html
2. Toulas, B. (2024, November 29). The new Rockstar 2FA phishing service targets Microsoft 365 accounts. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-rockstar-2fa-phishing-service-targets-microsoft-365-accounts/