**AL2025\_38 Microsoft and Cloudflare Disrupt Massive RacoonO265 Phishing Operation (September 20th , 2025)**

**Description**

A large phishing operation known as **RaccoonO365** has been taken down through a joint effort by **Microsoft**, **Cloudflare**, and law enforcement. This phishing-as-a-service (PhaaS) platform helped cybercriminals steal **tens of thousands of Microsoft 365 credentials** from victims around the world, including individuals, businesses, and government organizations.

RaccoonO365 worked by creating fake login pages that looked like real Microsoft 365 login screens. Victims were tricked into entering their usernames and passwords, which were then sent to attackers in real-time. Some phishing kits even allowed criminals to **bypass multi-factor authentication (MFA)** by capturing session tokens.

**Attack Details**

* RaccoonO365 was offered as a **subscription service** to cybercriminals, making it easy for non-technical users to run phishing campaigns.
* Attackers used email and SMS messages to lure victims to **fake login pages** hosted on domains that looked like real Microsoft services.
* Once a user entered their login info, it was immediately **sent to the attacker**. Some attacks also captured **MFA codes** or session cookies to gain access even with MFA enabled.
* **Thousands of victims** across multiple industries and regions were affected before the service was disrupted.

**Remediation**

* **Verify Links Before Logging In**: Always check the website address before entering your Microsoft credentials.
* **Enable Strong MFA**: Use phishing-resistant multi-factor authentication (MFA) (like biometrics or authentication apps), not just SMS codes.
* **Monitor Account Activity**: Check your Microsoft 365 account for recent logins or unfamiliar activity in the Microsoft 365 Security Center.
* **Educate Users**: Train employees and users to recognize phishing emails and fake login pages.
* **Block Malicious Domains**: Ensure DNS filtering and firewalls block access to known phishing infrastructure.
* **Use Conditional Access Policies**: Restrict login by location, device, and risk level using Microsoft’s built-in security tools.
* **Report Phishing Attempts**: Users should report suspicious messages to their IT or security teams immediately.

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

**References**

* Microsoft. (2025, September 16). Microsoft seizes 338 websites to disrupt rapidly growing “RaccoonO365” phishing service. Retrieved from Microsoft. <https://blogs.microsoft.com/on-the-issues/2025/09/16/microsoft-seizes-338-websites-to-disrupt-rapidly-growing-raccoono365-phishing-service/>
* Abrams, L. (2025, September 19). Microsoft and Cloudflare disrupt massive RaccoonO365 phishing service*.* Retrieved from BleepingComputer. <https://www.bleepingcomputer.com/news/security/microsoft-and-cloudflare-disrupt-massive-raccoono365-phishing-service/>