ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about a new Phishing-as-a-Service tool called Mamba 2FA which has the capability to easily get through email firewalls and, if successful, bypass MFA authentication altogether.

Why this matters

Two Factor Authentication (2FA) is commonly understood to deter against credential stealing attacks by adding an additional layer of security, usually via the "something you have" factor such as a Time-based one-time password(TOTP) generator like Microsoft Authenticator, Google Authenticator or Authy.

In order for a web service to not require that a user authenticates every action they want to take with a password and TOTP, the web service issues a cookie to the user that identifies them for the duration of the session. Should an attacker be able to gain hold of this cookie, they would be able to have full access to the user's account without the need for the credentials or TOTP.

Summary

Several reports dating as far back as June of this year have been laying out the workings of a new platform designed to facilitate as much as possible the planning and execution of phishing attacks capable of getting past most security controls.

Phishing–as-a-Service

Phishing-as-a-Service (PhaaS) is a model where cybercriminals sell recurring licenses for access to comprehensive phishing platforms, enabling even non-technical users to conduct phishing attacks. These platforms include tools such as email templates, fake websites, lists of targets, and detailed instructions, making it easier for malicious actors to execute sophisticated phishing campaigns.

Mamba 2FA Platform

This recently discovered platform differentiates itself from the rest by greatly facilitating the exploitation of adversary-in-the-middle (AiTM) methods. Should the user open the link embedded in the phishing email they will be presented with an accurately recreated microsoft login page where the user will be prompted to enter their credentials and 2FA token. The Mamba platform will be forwarding both to the actual Microsoft login manager with the intent being to capture session tokens. These allow attackers to bypass the second layer of security, such as two-factor authentication (2FA).
This approach enables unauthorized access to accounts without directly defeating the authentication itself, making conventional protective measures such as MFA redundant in fighting phishing attacks.

Mamba generated emails and web pages have mostly been seen used in conjunction with compromised email accounts. This gives the malicious actor two main benefits:

1. a list of email contacts that will be familiar with the sender and so won't be as suspicious of the phishing email;
2. an email address which is properly configured to pass email checks such as SPF, DKIM and DMARC.

The malicious actors will focus on gathering intelligence from the compromised accounts in order to recreate the phishing attack on the account's contacts and gain access to new targets.

Recommendations

Recommendation #1: Train users on identifying and reporting phishing attacks

ORNA recommends that organizations train their users on how to identify phishing attacks and report them.

Recommendation #2: Implement Zero Trust architecture where possible

ORNA recommends that organizations attempt to mitigate the damages that a compromised account can cause by implementing zero trust architecture, thus limiting the actions that any one user can do via their work account.

Recommendation #3: Develop incident playbooks for dealing with compromised accounts

ORNA recommends that organizations have playbooks ready and rehearsed for handling a compromised account in order to reduce the time that a malicious actor has within the organization's infrastructure as much as possible.

References

1. https://www.bleepingcomputer.com/news/security/new-mamba-2fa-bypass-service-targets-microsoft-365-accounts/
2. https://blog.sekoia.io/mamba-2fa-a-new-contender-in-the-aitm-phishing-ecosystem/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team