Press Release

2025 年 4 月 3 日（木）

Infoblox 株式会社

国境なきフィッシング：新世代 PhaaS の脅威

Morphing Meerkat が 100 以上のブランドを偽装し、認証情報を盗む。

2025 年 4 月 3 日（木） - Infoblox Threat Intel（DNS 脅威インテリジェンスチーム）は、世界中の企業に重大な脅威をもたらす高度なフィッシング アズ ア サービス（PhaaS：Phishing as a Service） プラットフォームを発見したことを発表します。

Morphing Meerkat と名付けられたこれらのキャンペーンの背後にいる脅威アクターは、DNS メール交換（MX）レコードを巧みに利用して偽のログインページを動的に提供し、100 以上のブランドになりすまし、ログイン認証情報を不正に盗み出します。

被害者がフィッシングリンクをクリックすると、フィッシングキットは被害者のメールドメインの MX レコードを照会し、メールサービスプロバイダを特定します。この MX レコード情報に基づき、フィッシングキットは動的に偽のログインページを表示し、被害者の実際のメールサービスプロバイダのログインページを模倣します。この斬新な DNS テクニックは、他の目的で存在するメールコンフィギュレーションを使って、被害者向けにコンテンツをカスタマイズすることを可能にします。これは、脅威アクターが既存環境の正規の管理ツール、コマンド、機能等を利用して身を隠す「Living Off The Land」と呼ばれるテクニックの DNS バージョンです。

Morphing Meerkat は、サイバー犯罪者に巧妙なフィッシングキットを提供します。

- **認証情報の窃盗**：被害者が偽のページにログイン情報を入力すると、Morphing Meerkat はその情報を盗み出し、サイバー犯罪者に送信します。
- **リダイレクト**：怪しまれないように、何度かログインに失敗すると、被害者を本物のログインページにリダイレクトさせます。
- **多言語対応**：偽のログインページを日本語も含めて複数の言語に翻訳し、世界中のユーザーをターゲットにすることができます。
- **標的型の罠**：MX レコードを使用し、被害者のメールサービスプロバイダ（Gmail、Microsoft Outlook、Yahoo! など）を識別し、動的にカスタマイズされたフィッシングページを提供することで、フィッシングの試みをより説得力のあるものにします。
- **回避テクニック**：このプラットフォームは、アドテクサーバー上でオープンリダイレクトを使用し、コードを難読化して分析を妨げるなど、従来のセキュリティシステムを回避するための様々な回避テクニックを採用しています。

- **スケーラビリティ**：PhaaS プラットフォームは、非技術的なサイバー犯罪者でも大規模なフィッシングキャンペーンを展開できるため、大きな脅威となっています。

サイバー犯罪者が Morphing Meerkat のようなフィッシング詐欺でログイン認証情報を入手した場合、特に企業にとっては深刻な影響が及ぶ可能性があります。これらの認証情報を使って、企業ネットワークに侵入し、機密データを盗み、さらに攻撃を仕掛けることも可能です。これは、企業にとって大きな金銭的損失、風評被害、法的責任につながる可能性があります。さらに、侵害されたアカウントは、他の従業員や顧客にフィッシングメールを送信するために使用され、攻撃をさらに拡大し、広範囲に混乱を引き起こす可能性があります。

企業における効果的なサイバーセキュリティ対策には、可視化と監視が不可欠です。 Morphing Meerkat は、DNS クローキングやオープンリダイレクトのような高度なテクニックを使って、サイバー犯罪者がいかにセキュリティの盲点を突いているかを例証しています。組織は、システムに強力な DNS セキュリティレイヤーを追加することで、この種の攻撃から身を守ることができます。これには、ユーザーが DoH サーバーと通信できないように DNS 制御を強化したり、ビジネスに重要でないアドテクやファイル共有インフラへのユーザーアクセスをブロックしたりすることが含まれます。企業がネットワーク内の重要でないサービスの数を減らすことができれば、攻撃対象領域を減らすことができ、サイバー犯罪者が脅威を提供するための選択肢を減らすことができます。

ブログ（英語）の全文はこちら：
https://blogs.infoblox.com/threat-intelligence/a-phishing-tale-of-doh-and-dns-mx-abuse/

日本語ブログはこちら：
https://note.com/infoblox/n/n93b0fb5bf06e

Infoblox について
Infoblox はネットワークとセキュリティを統合し、比類のないパフォーマンスと保護を提供します。フォーチュン 100 の企業や新興のイノベーターに信頼され、ネットワークに接続するユーザー、デバイスおよびその接続先をリアルタイムで可視化し制御することで、組織の迅速な稼動と脅威の早期防御を実現します。
Infoblox.com をご覧いただくか、LinkedIn または X でフォローしてください。

【本プレスリリースに関するお問合せ】
Infoblox 株式会社
〒107-0062 東京都港区南青山 2-26-37 VORT 外苑前Ⅰ 3 階
Email：SalesJapan@infoblox.com
https://www.infoblox.com