Cybersecurity Blog

Thought leadership, Threat analysis, Cybersecurity news and alerts.

What Is Phishing-As-A-Service and How to Protect Your Organization

9/23/2021 0 Comments

What Is Phishing-As-A-Service and How to Protect Your Organization
Microsoft 365 Defender Threat Intelligence Team recently published their findings on a large-scale phishing-as-a-service operation called "BulletProofLink."

What Is Phishing-as-a-Service?

Phishing-as-a-service follows the software-as-a-service model in which cybercriminals pay an operator to launch an email-based phishing campaign.

In an email-based phishing campaign, the target receives an email from a seemingly legitimate origin. The email, however, is a malicious one, masquerading as coming from a legitimate source. Clicking a link on this malicious email will lead to a compromised or fake website. The login details entered by the target who believes he or she is logging into a legitimate website will then be harvested for criminal activities.

BulletProofLink

BulletProofLink, also known as BulletProftLink and Anthrax, is an example of a phishing-as-a-service. This phishing-as-a-service was first reported by OSINT Fans in October 2020. According to OSINT Fans, the phishing campaign launched by BulletProofLink started with a phishing email impersonating a Sydney-based accounting firm. The email looked legitimate, with no sign of broken English or a spoofed email sender.

Inside this email is the Remittance Advice receipts.pdf link. Clinking this link, OSINT Fans said, leads to a pixel-perfect clone of the Microsoft 365 login page. "If a victim enters their password on this page, the login credentials are sent straight to the criminals rather than Microsoft," OSINT Fans said.

In the blog post "Catching the big fish: Analyzing a large-scale phishing-as-a-service operation," Microsoft 365 Defender Threat Intelligence Team said BulletProofLink offers phishing-as-a-service at a relatively low cost, offering a wide range of services, including email templates, site templates, email delivery, site hosting, credential theft, credential redistribution, and "fully undetected" links/logs.

Microsoft 365 Defender Threat Intelligence Team said BulletProofLink has over 100 available phishing templates that mimic known brands and services. The BulletProofLink operation, the Team said, is responsible for many of the phishing campaigns that impact enterprises today.

The Team also reported that BulletProofLink used a rather high volume of newly created and unique subdomains – over 300,000 in a single run. The Team added that BulletProofLink is used by multiple attacker groups in either one-off or monthly subscription-based business models, creating a steady revenue stream for BulletProofLink's operators.

BulletProofLink's monthly service costs as much as $800, while the one-time hosting link costs about $50 dollars. The common mode of payment is Bitcoin.

Infinite Subdomain Abuse

According to Microsoft 365 Defender Threat Intelligence Team, the operators behind BulletProofLink use the technique, which the Team calls "infinite subdomain abuse." The Team said infinite subdomain abuse happens when attackers compromise a website's DNS or when a compromised site is configured with a DNS that allows wildcard subdomains.

Microsoft 365 Defender Threat Intelligence Team said infinite subdomain abuse is gaining popularity among attackers for the following reasons:

"It serves as a departure from previous techniques that involved hackers obtaining large sets of single-use domains. To leverage infinite subdomains for use in email links that serve to redirect to a smaller set of final landing pages, the attackers then only need to compromise the DNS of the site, and not the site itself.

"It allows phishing operators to maximize the unique domains they are able to use by configuring dynamically generated subdomains as prefix to the base domain for each individual email.

"The creation of unique URLs poses a challenge to mitigation and detection methods that rely solely on exact matching for domains and URLs."

Double Theft

Microsoft 365 Defender Threat Intelligence Team said that BulletProofLink's phishing-as-a-service is reminiscent of the ransomware-as-a-service model. Today's ransomware attacks involve, not just data encryption, but exfiltrating or stealing data as well. In a ransomware-as-a-service scenario, the ransomware operator doesn't necessarily delete the stolen data even if the ransom has already been paid.

In both ransomware and phishing, Microsoft 365 Defender Threat Intelligence Team said that operators supplying resources to facilitate attacks maximize monetization by assuring stolen data are put to use in as many ways as possible. Victims' credentials, the Team said, are likely to end up in the underground economy. "For a relatively simple service, the return of investment offers a considerable motivation as far as the email threat landscape goes," Microsoft 365 Defender Threat Intelligence Team said.

Cybersecurity Best Practices

To protect Microsoft 365 users from phishing-as-a-service operations, Microsoft 365 Defender Threat Intelligence Team recommends the following cybersecurity best practices:

Use anti-phishing policiesto enable mailbox intelligence settings
Configure impersonation protection settings for specific messages and sender domains
Enable SafeLinksto ensure real-time protection by scanning at time of delivery and at time of click
Secure the Azure AD identity infrastructure
Enable multifactor authentication
Block sign-in attempts from legacy authentication

Nome (richiesto)

E-mail (non pubblicato)

Sito Web

Commenti (richiesto)

Notifica i nuovi commenti a questo post per e-mail

INVIA

Author

Steve E. Driz, I.S.P., ITCP

View my profile on LinkedIn

Archives

Categories

Cyber Security Threats
Data Breach
Data Governance
Data Leak
Data Leak Prevention
DDoS
Email Security
Fraud
GDPR
Hacking
IoT
Malware
MFA
Microsoft Office
Mobile Security
Network Security Threats
Phishing Attack
Privacy
Ransomware
Remote Access
SaaS Security
Social Engineering
Supply Chain Attack
Third-Party Risk
Virtual CISO
Vulnerability
Vulnerability Assessment
Web Applcation Security
Web-applcation-security
Web Application Firewall
Web Application Protection
Web Application Security
Web Protection
Windows Security
Zero Trust

RSS Feed

1.888.900.DRIZ (3749)

Managed Services
Web Application Security
Compliance
Vulnerability Assessment
Free Vulnerability Assessment

About us
Testimonials
Meet the Team
Subsidiaries
Contact us
Blog

Resources & Tools
Incident Management Playbook

Sophos Authorized Partner

Privacy Policy | CASL