May 10, 2024

MFA Bypass Techniques: The Evolving Threat

Jamie Tolles ZeroFox

Kamran Salour Lewis Brisbois









Jamie Tolles

VP Response ZeroFox



Kamran Salour

Partner Lewis Brisbois

Agenda

- MFA Overview
- Bypass methods
 - Social Engineering MFA codes
 - Social Engineering Replacement MFA Devices
 - Phish Kits
 - \circ Infostealers
- Recommendations



Bypass methods: MFA Overview



Common Forms of MFA:

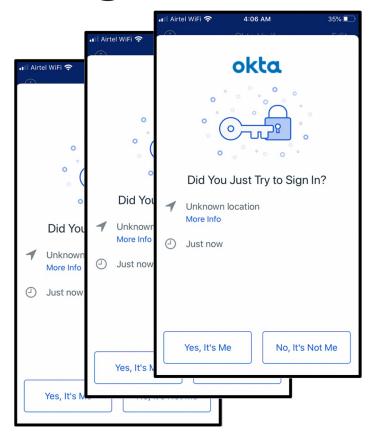
- Push notifications
- SMS
- Authenticator apps/soft tokens
- Voice
- Email
- Hardware token



Bypass methods: Social Engineering MFA Codes



MFA Fatigue Attack:



(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it 6:47 PM

And well, he accepted and I added my device $_{6:47\ PM}$

Source: community.arubanetworks.com

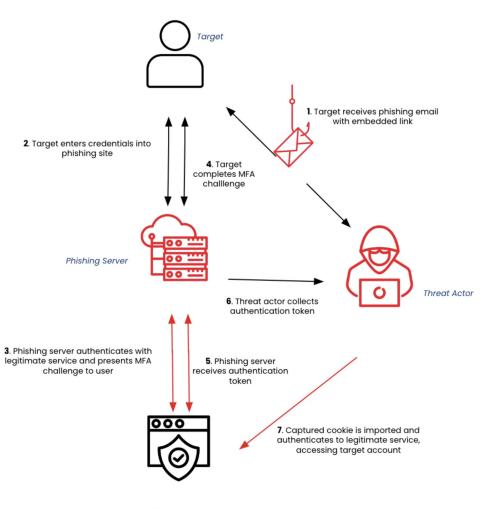
Source: bleepingcomputer.com

Bypass methods: Social Engineering MFA Codes



Token theft example:

<complex-block></complex-block>	Sign in to your account × +		✓ - □ X
Microsoft Sign in Email, phone, or Skype No account? Create one! Can't access your account? Back Next	$\epsilon \rightarrow \mathbf{C}$ in login.logincyberdemo.com/common/oauth	2/v2.0/authorize?cliert_id=4765445b-32c6-49b0-83e6-1d93765276ca&re	direct_uri=https%3A%2F%2Fwww
Sign in Email, phone, or Skype No account? Create one! Can't access your account? Back Next	login.logincyberc	emo.com/common/oauth2/v2.0	0/authorize?clier
Q Sign-in options		Sign in Email, phone, or Skype No account? Create one! Can't access your account?	
Terms of use Privacy & cookies ····		🔍 Sign-in options	



Legitimate Service Source: ZeroFox Intelligence

Source: jeffreyappel.nl

Bypass methods: Social Engineering Replacement MFA Devices

Privacy+ Security Forum

Call to help desk

- Broken/lost phone
- Urgent task needing to be done
- Request to enroll new MFA device



EvilGinx Demo

C -> C -= login.microsottonine.com/common/oautta/v2.u/auttonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/common/oautta/v2.u/auttonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b3443b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/builtonize/client_id=4/b344b-32cb-4900-83eb-1093/b32/bca8dredirect_uri=https/sa4%2/b22/boldirect_uri=https/sa4%2/b22/boldirect_uri=https/sa4%2/ballect_uri=https/sa4%2/ba	n%2Handingv 🔓	9 U	
Microsoft Pick an account i jtolles@ Use another account			
	Ø		
	Terms	of use Privac	cy & cookies





Bypass methods:

Phish Kits (EvilGinx)

Bypass methods:

Infostealers (SapphireStealer)

Infostealer Example

-								-		<u>_</u>
	Data :	SendLog.cs	Program.cs + × Chro			oackages.config			Solution Explorer	×
Miterescolifi	Source	Sapphire 10	using System.Threa	Sapphire.Program	+ 🗊 Main()			• ÷		- 2
ladere	e a	10	Lasting System. milet	ading. rasks,						
			Enamespace Sapphire	e					▲ Solution 'Sapphire' (1 of 1 project)	
X	Ac		0 references		I				B C Sapphire Properties	
A Studio	Sa		Class Program						▷ and References	
(Catio			{ 0 references						✓ Modules	
				atic async Task Main()				. —	Þ 🛅 Auth	
			{						Grabbers	
7		180 ⁴ 19		<pre>ium.Get(); // Get Passw ium.GetCookies(); // Get</pre>					Helpers	
DE BROWERE		20	Crirom.	Ium.GetCookies(); // Ge					 Information Others 	
(Sell(cipher))				nshot.Make(); // Screen					D Ctners	
	H			.Grab(); // grab docs p					a 🗋 .gitignore	
		23 24	Filen	anager.ArchiveDirectory	(); // zip				App.config	
DBBrowers		25		SendLogS3.Send(); // s					a packages.config	
(Sollika)									♦ 6 C# Program.cs	
_		27 28	//File	eManager.DeleteDirector	y("all");				A README.md	
1		28							o ∰ Sapphire_TemporaryKey.pfx	
			[]							
CorolNi=0	H									
-										
		100 % 🝷	No issues found			▶ Ln: 18 Cł	h: 39 SPC (CRLF		
Girdiox		Output						ų ×		
	H	Show output from	m: Debug		[등 등 등 돌 😫 😫					
				apphire.exe): Loaded 'C:\						
				apphire.exe): Loaded 'C:\ apphire.exe): Loaded 'C:\						
Uker/Date		'Sapphire.ex	e' (CLR v4.0.30319: Si	apphire.exe): Loaded 'C:\	Users\vboxuser\Docum	ents\Sapphire	\bin\Debug\S	Sy:		
Sharitani				apphire.exe): Loaded 'C:\ ' has exited with code 0		t\assembly\GA	C_MSIL\Syste	em		
		the program	Cartool sopprize ever							
		4 Developer Report	Shell Error List Output							
7		Developer Powers	Output							

Privacy+ Security Forum

Planet Stealer | #1 Affordable, Modern, Effective Infostealer by PlanetStealer Sunday March 3. 2024 is 0.444 PM Image: Stealer Image: Stealer Steale Code of the Stealer of the market, completely made in Go, and has lots of useful features. Image: March 2. 2024 Steals Code of the Stealer on the market, completely made in Go, and has lots of useful features. Image: Stealer is a new info-stealer on the market, completely made in Go, and has lots of useful features. Image: Steale Crypto wallet files both software wallets and browser extension wallets Image: Steale Crypto wallet files both software wallets and browser extension wallets Image: Steale Crypto wallet files for Tox, Signal, Telegram, Steam, Minecraft Launcher config files and also third party launcher config files Image: Steale Code wall Self Deletion Ability Image: Steale Code wall and builder Image: Steale Code wall and builder

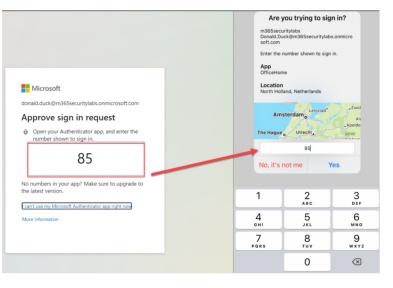
Sponsored S

Source: zerofox.com/blog/stealing-the-show-top-5-infostealer-trends/

Recommendations

- 1. Implement MFA using the strongest available method:
 - a. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn/Passkeys)
 - Mobile app soft tokens (preferably push notification with number matching)
 - c. MFA via SMS or voice (when no other options are possible)
- 2. Disable legacy protocols and leverage conditional access policies
- 3. Managed devices should be required for authentication
- 4. Properly vet MFA enrollment requests. Extra scrutiny for privileged accounts!
- 5. Do not allow credential storage in browsers or allow browsers to sync with non-corporate devices







Questions & Contacts





Jamie Tolles

VP Response, ZeroFox jtolles@zerofox.com



Kamran Salour

Partner, Lewis Brisbois Kamran.Salour@lewisbrisbois.com