Bypassing MFA: A Forensic Look at Evilginx2 Phishing Kit

aon.com/cyber-solutions/aon_cyber_labs/bypassing-mfa-a-forensic-look-at-evilginx2-phishing-kit/

Is MFA Enough?

Recently, Stroz Friedberg Incident Response Services encountered an uptick in compromises where multi-factor authentication ("MFA") was not effective in keeping the threat actor out of the environment. Attack patterns to bypass MFA have been around for years, but some methods are becoming increasingly mainstream due to the increase in organizations adopting and implementing MFA. While there are dozens of ways for a threat actor to breach an account with MFA enabled, the post below covers the technical details of one technique that is easy to exploit, but difficult to prevent – proxy phishing sites.

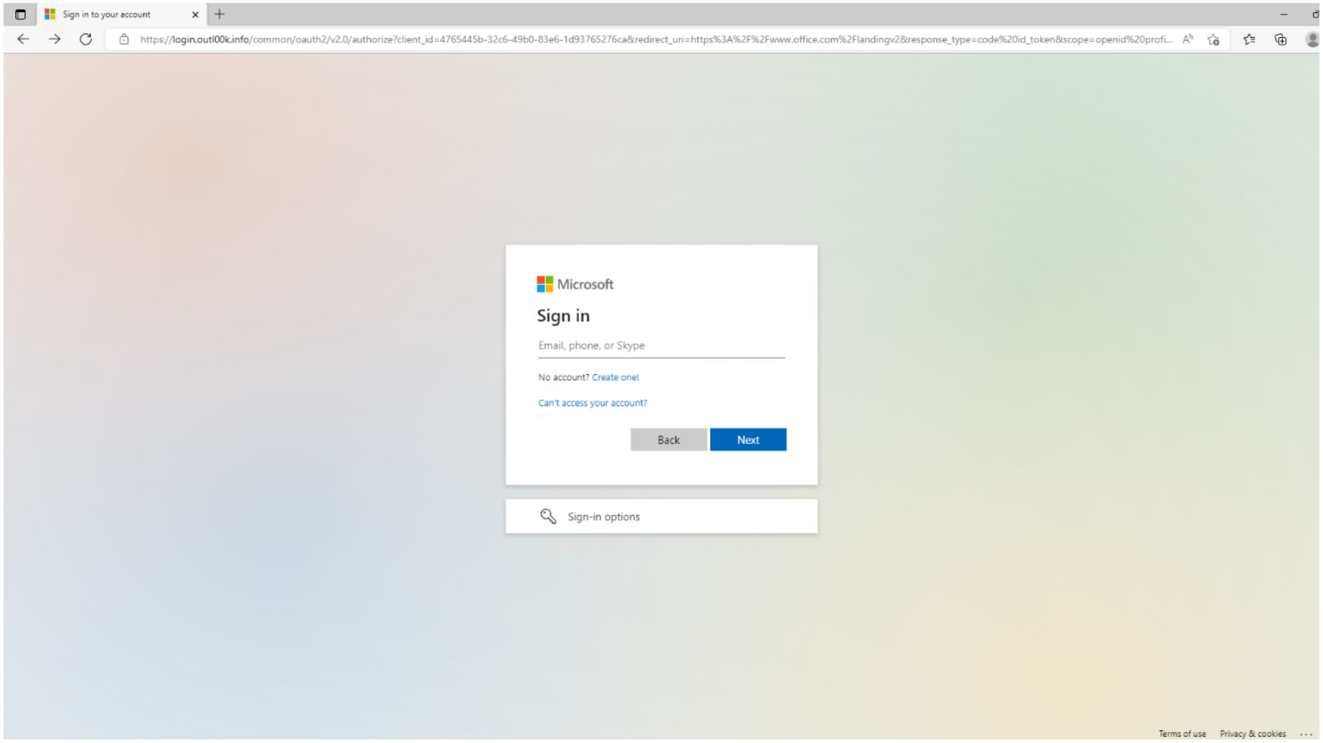
Proxy phishing sites are more advanced versions of the typical credential harvesting phishing page, as they enable interception of authentication tokens. Such sites are known as Man-in-the-Middle/Machine-in-the-Middle ("MitM") or Adversary-in-the-Middle ("AitM") sites as they stand between the victim user and a legitimate service that a threat actor is impersonating.

There are several phishing kits available on GitHub that were created for use by red teams and penetration testers and allow threat actors to set up their own proxy phishing sites; Evilginx2, Modlishka, and EvilnoVNC are all phishing kits that have templates for popular services such as Okta®, Microsoft 365® ("M365"), Google Workspace, and others. Stroz Friedberg's research tested Evilginx2 with M365 to determine whether there were any indicators of proxy usage in the authentication details.

Evilginx2: An Operational Overview

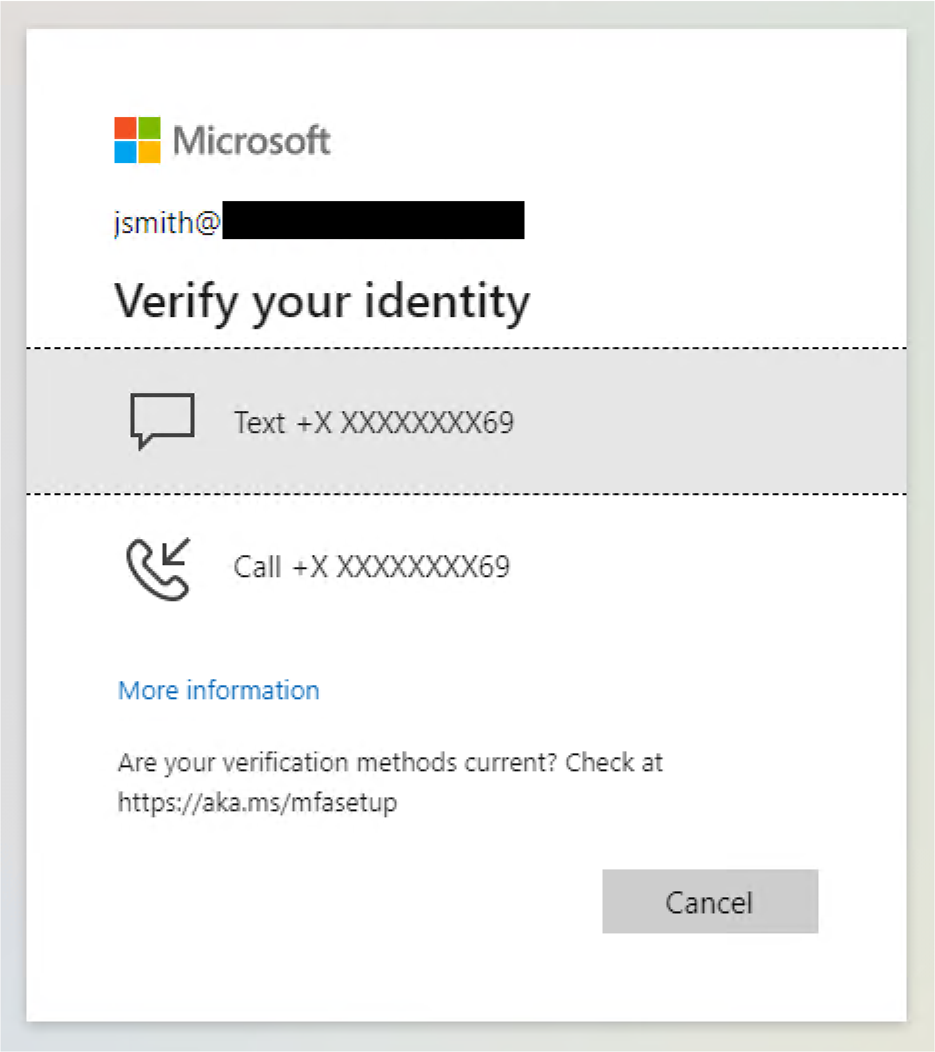
Developed between 2018 and 2021, Evilginx2 is an open-source phishing framework that is built on an earlier framework, EvilGinx. Evilginx2 is written in Go and comes with various built-in "phishlets" to mimic login pages for Citrix, M365, Okta, PayPal, GitHub, and other sites. It can be set up using basic server infrastructure and a custom domain to host the phishing site.

For this testing, we purchased a domain, configured DNS, and ran a handful of commands to stand up a phishing site on a test server with the built-in O365 phishlet. Once the site is up and running, any users who visit the phishing link generated by Evilginx2 will be met with a page that looks identical to a legitimate Microsoft login page. Common security advice maintains that pages without the TLS lock icon in the URL bar should be a red flag of malicious activity – Evilginx2 requests an TLS certificate from Let's Encrypt, a free certificate authority, meaning that its communications are secured with HTTPS, resulting in phishing sites that do have this lock icon. The only way for a regular user to tell this page apart from a legitimate login page is the URL.


Sign in to your account
https://login.outl00k.info/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=https%3A%2F%2Fwww.office.com%2Flandingv2&response_type=code%20id_token&scope=openid%20profi...
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Sign-in options
Terms of use
Privacy & cookies
...

Fraudulent login page displayed to victim from built-in Evilginx2 O365 phishlet

When the unsuspecting user enters their credentials into the fraudulent login page, the phishing site checks these with Microsoft to ensure that valid credentials were entered. After providing the correct credentials, the user is then prompted with a regular MFA challenge, in whatever methods they normally have enabled for their M365 account. In our test case, the account had SMS and calling options for MFA verification.



Microsoft

jsmith@[redacted]

Verify your identity

Text +X XXXXXXXX69

Call +X XXXXXXXX69

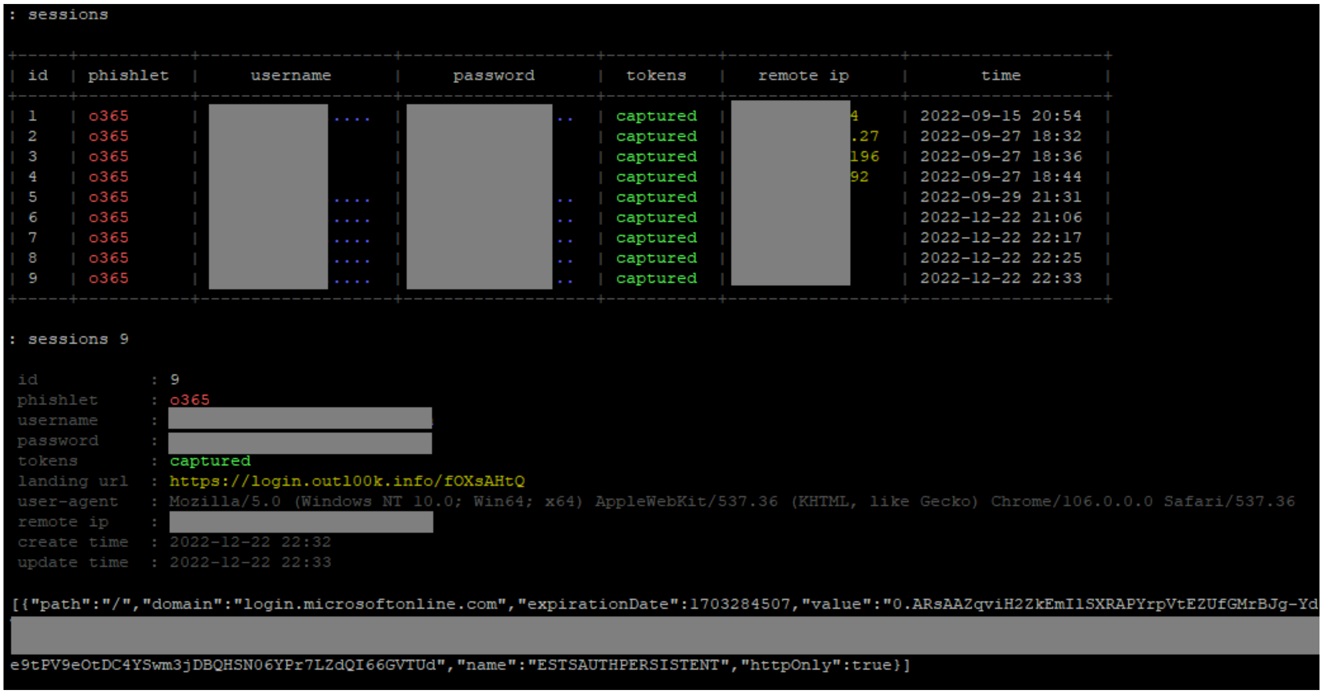
More information

Are your verification methods current? Check at https://aka.ms/mfasetup

MFA challenge provided to victim by Evilginx2 phishing site

If MFA is successfully approved, it will appear to the victim that they are logged in with their credentials. Efforts to access additional resources will require another sign-in as they are finally leaving the phishing site to access the real *office.com*. The user may be tipped off by the additional request for authentication, or by the fact that whatever was promised to them in the phishing email was not available, but many users may still not realize they were phished.

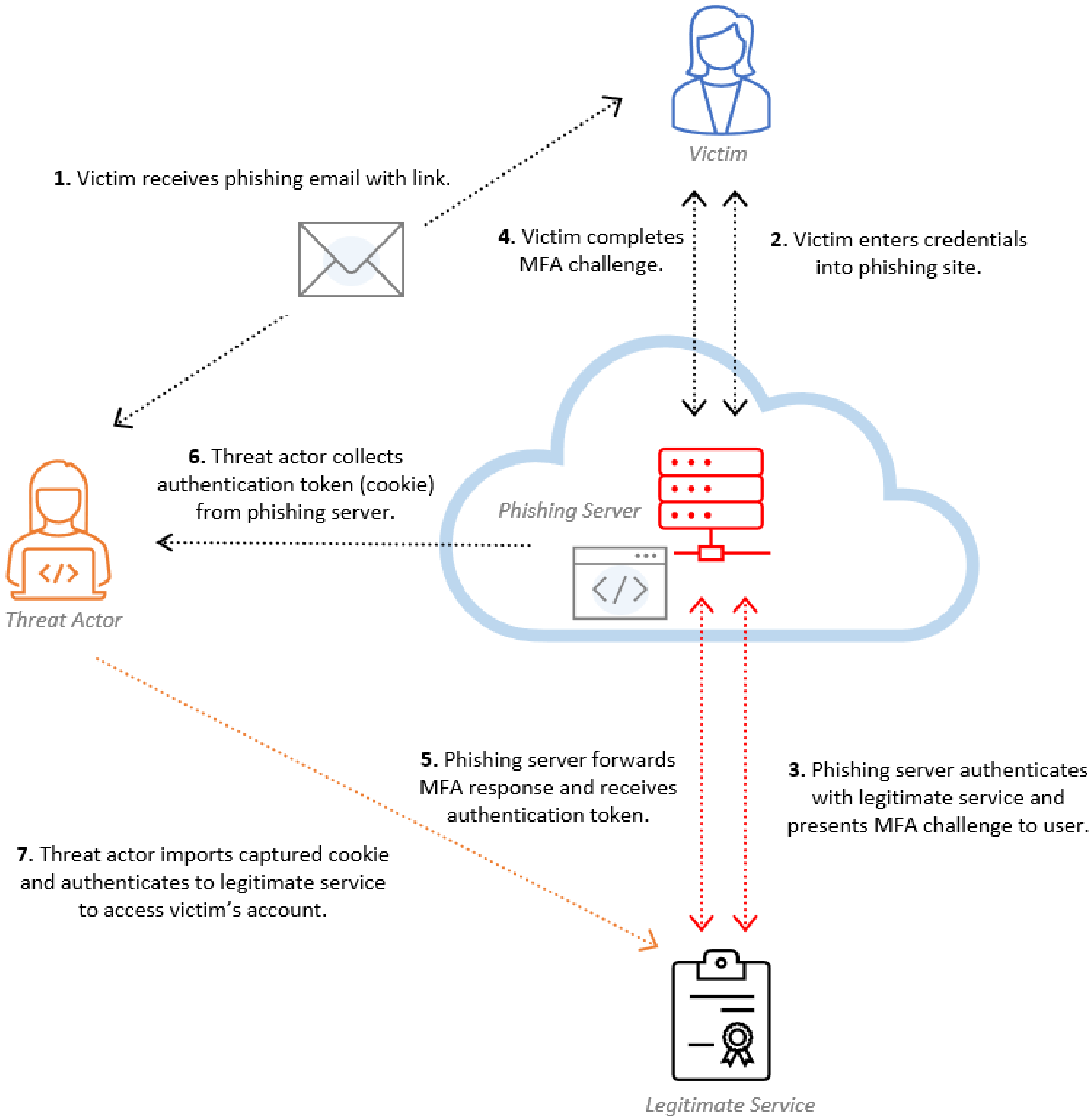
On the other side of the scheme, the phishing site operator can run the *sessions* command from their Evilginx2 instance and view all captured credentials as well as details about any specific session and associated tokens.



```
: sessions

+-----+-----------+-------------------+-------------------+------------+----------------+-----------------+
| id  | phishlet  |     username      |     password      |   tokens   |   remote ip    |      time       |
+-----+-----------+-------------------+-------------------+------------+----------------+-----------------+
| 1   | o365      | [redacted]....    | [redacted]..      | captured   | [redacted]4    | 2022-09-15 20:54 |
| 2   | o365      | [redacted]        | [redacted]        | captured   | [redacted].27  | 2022-09-27 18:32 |
| 3   | o365      | [redacted]        | [redacted]        | captured   | [redacted]196  | 2022-09-27 18:36 |
| 4   | o365      | [redacted]        | [redacted]        | captured   | [redacted]92   | 2022-09-27 18:44 |
| 5   | o365      | [redacted]....    | [redacted]..      | captured   | [redacted]     | 2022-09-29 21:31 |
| 6   | o365      | [redacted]....    | [redacted]..      | captured   | [redacted]     | 2022-12-22 21:06 |
| 7   | o365      | [redacted]....    | [redacted]..      | captured   | [redacted]     | 2022-12-22 22:17 |
| 8   | o365      | [redacted]....    | [redacted]..      | captured   | [redacted]     | 2022-12-22 22:25 |
| 9   | o365      | [redacted]....    | [redacted]..      | captured   | [redacted]     | 2022-12-22 22:33 |
+-----+-----------+-------------------+-------------------+------------+----------------+-----------------+

: sessions 9

 id           : 9
 phishlet     : o365
 username     : [redacted]
 password     : [redacted]
 tokens       : captured
 landing url  : https://login.out100k.info/fOXsAHtQ
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
 remote ip    : [redacted]
 create time  : 2022-12-22 22:32
 update time  : 2022-12-22 22:33

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1703284507,"value":"0.ARsAAZqviH2ZkEmIlSXRAPYrpVtEZUfGMrBJg-Yd
[redacted]
e9tPV9eOtDC4YSwm3jDBQHSN06YPr7LZdQI66GVTUd","name":"ESTSAUTHPERSISTENT","httpOnly":true}]
```

Attacker view of sessions collected by Evilginx2

The threat actor can then copy the text of the cookie that is provided at the bottom of the session information and import it into a browser using any cookie modification plugin, such as EditThisCookie. When the threat actor refreshes the Microsoft sign in page, they are logged in as the phished user.The diagram below shows the workflow of the attack at a high level.


Victim
1. Victim receives phishing email with link.
4. Victim completes MFA challenge.
2. Victim enters credentials into phishing site.
6. Threat actor collects authentication token (cookie) from phishing server.
Phishing Server
Threat Actor
5. Phishing server forwards MFA response and receives authentication token.
3. Phishing server authenticates with legitimate service and presents MFA challenge to user.
7. Threat actor imports captured cookie and authenticates to legitimate service to access victim's account.
Legitimate Service

Sample attack diagram

Forensic Findings

While it may be difficult to positively identify the use of a proxy phishing site such as Evilginx2, there are fact patterns that examiners can rely on to indicate that an attacker may have stolen a user's cookies through a phishing site. The following subsections will discuss Stroz Friedberg's main observations, including:

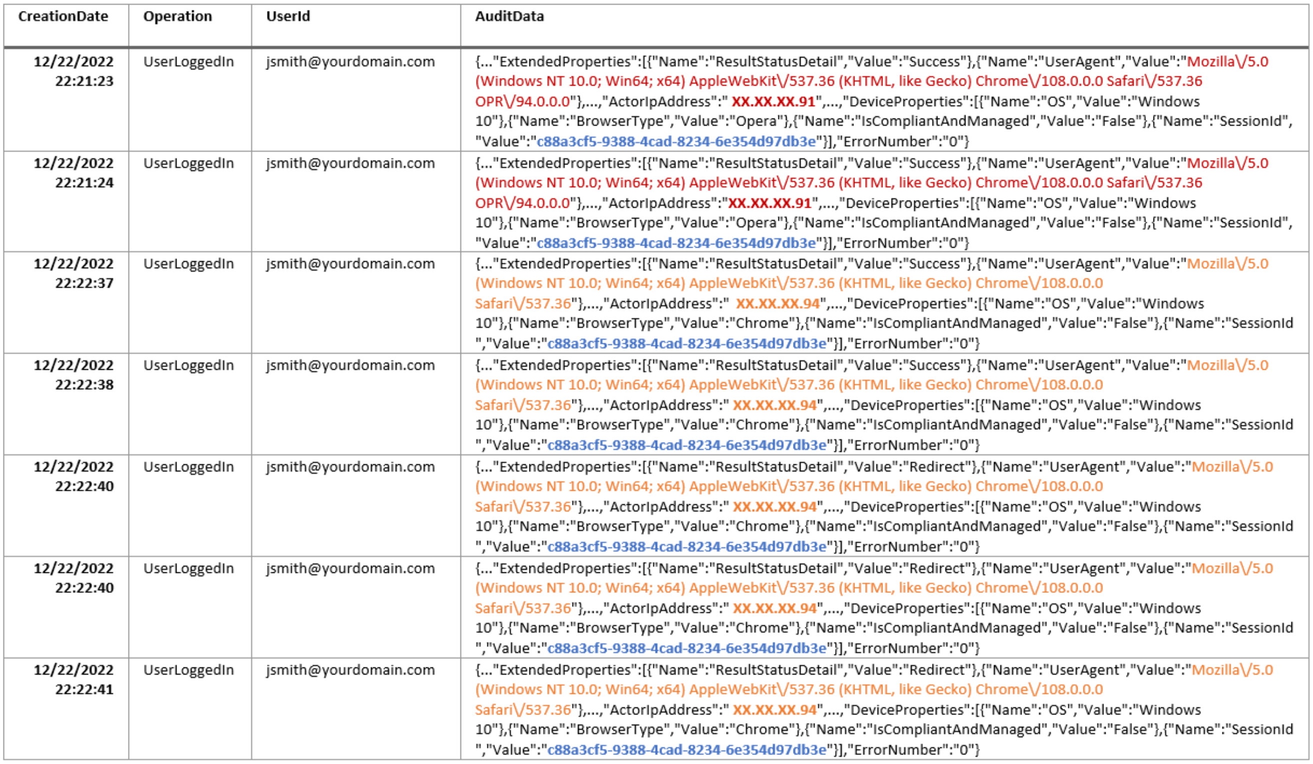
1. Logins will still originate from **anomalous IP addresses**.
2. All attacker activity will have the **same SessionId**, even if the cookie is moved off the phishing server to be imported into a browser on another system.
3. Initial logins from the phishing server will appear as the **victim's legitimate user agent string**.

Anomalous IPs

The typical methods of identifying email compromise still apply in this situation. Although it looks to the user like they are logging in through Microsoft, their credentials are being sent to Microsoft through the phishing site, so it is the phishing server's IP address, and not the IP of the user's system, that will appear in the logs for the initial login.

Consistent Session ID

While the phishing server IP address will show up for the first login through the phishing site, the IP address may change with subsequent logged activity. In typical adversary-in-the-middle attacks, the login occurs on the phishing server, and the threat actor will then move the cookie to a different machine to import into a browser. Because the cookie is the same, the SessionId in the Unified Audit Log ("UAL") will be consistent between logins, even though they are coming from different IP addresses and/or user agents. The SessionId can be found under "DeviceProperties" for UserLoggedIn events in the UAL.



CreationDate	Operation	UserId	AuditData
12/22/2022 22:21:23	UserLoggedIn	jsmith@yourdomain.com	{..."ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Success"},{"Name":"UserAgent","Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.0.0 Safari\/537.36 OPR\/94.0.0.0"},...,"ActorIpAddress":" **XX.XX.XX.91**",...,"DeviceProperties":[{"Name":"OS","Value":"Windows 10"},{"Name":"BrowserType","Value":"Opera"},{"Name":"IsCompliantAndManaged","Value":"False"},{"Name":"SessionId", "Value":"**c88a3cf5-9388-4cad-8234-6e354d97db3e**"}],"ErrorNumber":"0"}
12/22/2022 22:21:24	UserLoggedIn	jsmith@yourdomain.com	{..."ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Success"},{"Name":"UserAgent","Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.0.0 Safari\/537.36 OPR\/94.0.0.0"},...,"ActorIpAddress":"**XX.XX.XX.91**",...,"DeviceProperties":[{"Name":"OS","Value":"Windows 10"},{"Name":"BrowserType","Value":"Opera"},{"Name":"IsCompliantAndManaged","Value":"False"},{"Name":"SessionId", "Value":"**c88a3cf5-9388-4cad-8234-6e354d97db3e**"}],"ErrorNumber":"0"}
12/22/2022 22:22:37	UserLoggedIn	jsmith@yourdomain.com	{..."ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Success"},{"Name":"UserAgent","Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.0.0 Safari\/537.36"},...,"ActorIpAddress":" **XX.XX.XX.94**",...,"DeviceProperties":[{"Name":"OS","Value":"Windows 10"},{"Name":"BrowserType","Value":"Chrome"},{"Name":"IsCompliantAndManaged","Value":"False"},{"Name":"SessionId","Value":"**c88a3cf5-9388-4cad-8234-6e354d97db3e**"}],"ErrorNumber":"0"}
12/22/2022 22:22:38	UserLoggedIn	jsmith@yourdomain.com	{..."ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Success"},{"Name":"UserAgent","Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.0.0 Safari\/537.36"},...,"ActorIpAddress":" **XX.XX.XX.94**",...,"DeviceProperties":[{"Name":"OS","Value":"Windows 10"},{"Name":"BrowserType","Value":"Chrome"},{"Name":"IsCompliantAndManaged","Value":"False"},{"Name":"SessionId","Value":"**c88a3cf5-9388-4cad-8234-6e354d97db3e**"}],"ErrorNumber":"0"}
12/22/2022 22:22:40	UserLoggedIn	jsmith@yourdomain.com	{..."ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Redirect"},{"Name":"UserAgent","Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.0.0 Safari\/537.36"},...,"ActorIpAddress":" **XX.XX.XX.94**",...,"DeviceProperties":[{"Name":"OS","Value":"Windows 10"},{"Name":"BrowserType","Value":"Chrome"},{"Name":"IsCompliantAndManaged","Value":"False"},{"Name":"SessionId","Value":"**c88a3cf5-9388-4cad-8234-6e354d97db3e**"}],"ErrorNumber":"0"}
12/22/2022 22:22:40	UserLoggedIn	jsmith@yourdomain.com	{..."ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Redirect"},{"Name":"UserAgent","Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.0.0 Safari\/537.36"},...,"ActorIpAddress":" **XX.XX.XX.94**",...,"DeviceProperties":[{"Name":"OS","Value":"Windows 10"},{"Name":"BrowserType","Value":"Chrome"},{"Name":"IsCompliantAndManaged","Value":"False"},{"Name":"SessionId","Value":"**c88a3cf5-9388-4cad-8234-6e354d97db3e**"}],"ErrorNumber":"0"}
12/22/2022 22:22:41	UserLoggedIn	jsmith@yourdomain.com	{..."ExtendedProperties":[{"Name":"ResultStatusDetail","Value":"Redirect"},{"Name":"UserAgent","Value":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/108.0.0.0 Safari\/537.36"},...,"ActorIpAddress":" **XX.XX.XX.94**",...,"DeviceProperties":[{"Name":"OS","Value":"Windows 10"},{"Name":"BrowserType","Value":"Chrome"},{"Name":"IsCompliantAndManaged","Value":"False"},{"Name":"SessionId","Value":"**c88a3cf5-9388-4cad-8234-6e354d97db3e**"}],"ErrorNumber":"0"}

Abbreviated export of Unified Audit Log showing threat actor logins

In the example shown above, the IP address of the phishing server is shown in red and ends in .91, while the IP address of the mock threat actor system is shown in orange and ends in .94. The subsequent logins with the .94 IP address are logins that occurred when the mock threat actor imported the captured cookie from the phishing server into a Chrome browser and continued interacting with the victim account. The SessionId shown in blue is consistent throughout all activity because the same authentication cookie is used.

User Agent Pattern

For many unauthorized email access investigations, the investigator can often differentiate malicious activity from legitimate logins by the user agent, which represents the device type and client being used to access the account. Typically, threat actor activity will have a different user agent than the legitimate user because the threat actor is logging in from their own infrastructure. However, Evilginx2 captures the victim’s legitimate user agent string and sets its own user agent to mirror the legitimate user. This means that although the phishing site may be running on a Linux system, if the victim clicks the link using Firefox on a Windows 10 machine, the user agent recorded in the logs will reflect the Firefox on Windows 10 user agent string.

In the sample UAL logs shown above, the mock victim during our testing accessed the phishing site using Windows 10 and the Opera browser – the same user agent that is reflected in the initial logins originating from the phishing server IP address.

This attempt at blending into legitimate logins in authentication logs has substantial implications for investigators. Without a clearly anomalous user agent, the only clear indicator of compromise in the login event is the anomalous IP address. In a situation where the threat actor employs a botnet or other infrastructure belonging to regular residential internet service providers (“ISPs”), detection of this activity would be very difficult.

In the second phase of the attack, once the cookies are captured, they can be imported into the threat actor’s browser. A threat actor may view the user agent from the captured session within Evilginx2 and spoof the user agent of their browser to match, but Stroz Friedberg has identified many occasions where threat actors have not bothered to continue matching their user agent to the victim’s. As such, there may be a detection opportunity when the threat actor imports cookies into their own browser and the user agent switches while the SessionId remains the same.

Prevention

Prevention against MFA bypass techniques is non-trivial, but there are several ways that organizations can lower the risk of successful compromise:

Implement FIDO2 Authentication

Hardware-based authentication mechanisms using FIDO2 protocols currently appear to be the best way to mitigate the risk of threat actors bypassing MFA in all forms. FIDO2 authentication uses cryptographic keys that are pre-registered with a service such as M365 to allow the user to authenticate to that site. The challenge presented to the FIDO2 device by the service includes details about the origin of the request, such as the URI of the site. Because of this, attempts to authenticate to a fraudulent phishing site using this authentication mechanism should fail. Examples of FIDO2 authentication include hardware tokens such as Yubikeys or a built-in solution on a user’s laptop such as Windows Hello.

There is a risk of downgrade attacks on FIDO2 authentication, where alternative authentication methods are also made available. For example, an organization may have FIDO2 authentication as their primary method but may also allow one-time passwords (OTP) to be delivered via SMS or email as an alternative. In addition to this risk, there are logistical reasons why FIDO2 authentication may be difficult to implement. Switching to FIDO2 authentication is a big change for most users, and it comes with additional costs to organizations in many cases.

Limit External Access

Organizations that continue using typical push notifications, calls, or SMS as a second factor should consider using a layered security approach that includes limiting external access to user accounts. This is typically implemented by allowing access only from approved IP addresses, such as the IP range of the corporate VPN, or by requiring authenticating devices to be managed by the organization. These types of security controls can be very effective measures in making life difficult for threat actors.

Other Layered Security Protocols

Other important aspects of layered security that help to minimize the risk of this attack occurring in its earlier stages include spam filtering — either using your email platform's built-in filtering functionality or using a third-party solution — and the use of a web proxy for filtering users' web traffic. With web filtering, users can be blocked from visiting known phishing sites or other sites in categories that are considered risky. Additionally, organizations can also help guard against attacks by providing user training on how to better identify phishing emails and malicious websites.

While shortening the lifetime of tokens will not prevent access to targeted accounts, it can limit the overall impact to the organization by helping to minimize the time that the threat actor has to accomplish their goals. In M365 specifically, administrators can modify the session lifetime – this can also be done for particular groups of users, such as administrators, through conditional access. Password resets in M365 will invalidate old persistent tokens, so this is an effective remediation step for accounts that have suffered this attack pattern.

Closing Thoughts

Cybersecurity is always evolving, and the abilities of threat actors to circumvent MFA does not come as a surprise. The concepts of token theft or adversary-in-the-middle attacks are not new, but with the number of organizations moving to secure their systems with MFA, threat actors are forced to use newer methods to obtain access to targeted accounts. These attacks threaten more than just email environments, as other services such as Okta, Citrix, and others are at risk of the same types of attack. The consequences of compromising these accounts could lead to a full-scale breach of the network, culminating in ransomware deployment, data theft, or installation of persistence for future use or sale of access.

Threat actors can bypass MFA even without possessing the technical skills required to set up a proxy phishing site. Phishing-as-a-Service solutions are available for threat actors to subscribe to for a couple hundred dollars per month — much less than threat actors typically earn from even a single redirected wire transfer. Even simpler for threat actors, some users may just accept push notifications on their phone even when they did not initiate the login attempt. Threat actors have many methods for MFA circumvention at their disposal, and while MFA may at this time be a non-negotiable, must-have tool in cyber defense, it is not a bulletproof solution to security.

Author: Carly Battaile

February 10, 2023

While care has been taken in the preparation of this material and some of the information contained within it has been obtained from sources that Stroz Friedberg believes to be reliable, Stroz Friedberg does not warrant, represent, or guarantee the accuracy, adequacy, completeness or fitness for any purpose of the article and accepts no liability for any loss incurred in any way whatsoever by any person or organization who may rely upon it. It is for informational purposes only. You should consult with your own professional advisors or IT specialists before implementing any recommendation or following the guidance provided herein. Further, we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. Further, this article has been compiled using information available to us up to 02/10/2023.

About Cyber Solutions
Cyber security services are offered by Stroz Friedberg Inc., its subsidiaries and affiliates. Stroz Friedberg is part of Aon's Cyber Solutions which offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates. Aon UK Limited is authorised and regulated by the Financial Conduct Authority in respect of insurance distribution services. FP.AGRC.238.JJ The following products or services are not regulated by the Financial Conduct Authority:

- Cyber risk services provided by Aon UK Limited and its affiliates
- Cyber security services provided by Stroz Friedberg Limited and its affiliates.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates. Aon UK Limited is authorised and regulated by the Financial Conduct Authority in respect of insurance distribution services. FP.AGRC.238.JJ The following products or services are not regulated by the Financial Conduct Authority:

- Cyber risk services provided by Aon UK Limited and its affiliates
- Cyber security services provided by Stroz Friedberg Limited and its affiliates.