Studentnet Analysis of the Impact of BigBear 2.0 Attacks

Recently, researchers at CloudSEK discovered a phishing toolkit called BigBear 2.0 that bypassed multi-factor authentication at 258 organisations and stole over 5,000 Microsoft 365 credentials. It operates an adversary-in-the-middle (AiTM) framework which places a malicious proxy between the victim and their legitimate authentication infrastructure.

The proxy intercepts usernames, passwords, multi-factor authentication data and session cookies as the victim signs in, so attackers can replay the credentials to access the victim's mailbox and applications without triggering re-authentication. See report.

Impact on Non-Microsoft Authentication Services

Industry analysts have observed that any service using MFA and session tokens may be vulnerable, as the actual login page is irrelevant to the malicious proxy. It shows a copy of the real page to the victim, forwards their input, forwards the challenge response, and keeps the session data. Displaying a different login page instead of Microsoft's requires only a small configuration change.

Studentnet Approach

Kevin Karp, Studentnet MD, sees the issue as a question of *observed attacks* (those mounted against Microsoft authentication services) vs *potential attacks* (whether they can successfully penetrate a Studentnet authenticated SSO service in the future). Hence:

1. What does the analysis of the *observed attack* reveal about the likelihood that it will succeed (or fail) against a Studentnet authenticated SSO service?
2. What improvements can Studentnet implement to better protect our client schools from *potential attacks?*

Attack Analysis

Jaye Steward from Studentnet writes: internally, we've been discussing this issue in two distinct aspects – one, current attacks as outlined against Microsoft, and two, what happens if the attack is turned against Studentnet specifically.

Observed Attacks against Studentnet Authenticated SSO

The attack works by setting up a transparent proxy that presents a different domain to the user and copies their client credentials, tokens and cookies. But inside a well-configured SAML environment such as Studentnet, where authentication is handed off to Studentnet services, this attack fails. Studentnet does NOT send the response back to the proxied domain, but redirects the user to the Assertion Consumer Service (ACS) included in the SAML request.

Thus the attacker never sees the successful login, so it can't scrape cookies or credentials. If the attacker tries to manipulate the login request to change the ACS URL the attack still fails because the attacker's domain will not be part of the configuration at Studentnet's end, as we verify ACS URLs against the service configuration.

For an additional layer of security, schools could require Studentnet to validate the cryptographic signature in the SAML request, thus further tightening restrictions against tampering with the login request.

OpenID Connect responses similarly are only provided to whitelisted response URLs. Protection against forged requests is more difficult, due to specific use-cases of OpenID Connect (eg, local applications that keep authentication details on-device), but Studentnet still provides responses only to authorised URLs.

Potential Attacks Against Studentnet Authenticated SSO

If the BigBear code was rewritten to specifically attack Studentnet, the service would be no more unique than Microsoft in this case, and our response needs to be much the same: requiring schools to use *Phishing Resistant MFA* (PR-MFA).

If schools enforce FIDO2/WebAuthn, authentication is cryptographically bound to the login origin, so a proxy on another domain cannot obtain a usable login. In this case the domain name presented to the end-user becomes part of the cryptographic verification, thus invalidating the possibility of proxy attacks.

Studentnet has already developed the capability for schools to be able to lock down specific cohorts and require them to strictly use PR-MFA Passkeys or FIDO/WebAuthn authentication – users would then access services with biometrics, Windows Hello, Yubikeys, and so on. Ideally all accounts would have to login with PR-MFA, but at minimum all IT and admin staff, and other privileged accounts, should use it.

Currently Studentnet is also researching other measures to protect against these types of attack, however Phishing Resistant MFA is the industry standard response to threats such as BigBear.