okta Security

Go to Okta.com ↗

November 10, 2022

Detecting Real-Time Phishing Attacks

Brett Winterford and Defensive Cyber Operations

In the last two installments in our series on phishing resistance, we discussed phishing resistant authenticators and how to gather signals about phishing lures directly from your users. Now let's drill down into detection and response: what signals does Okta's System Log provide that are indicative of in-flight phishing campaigns?

Okta's Defensive Cyber Operations team routinely identifies phishing infrastructure configured to imitate an Okta sign-in page and proactively notify Okta customers when suspicious infrastructure we detect appears to be targeting their users. Since March 2020, we have delivered over 1000 notifications to customers.

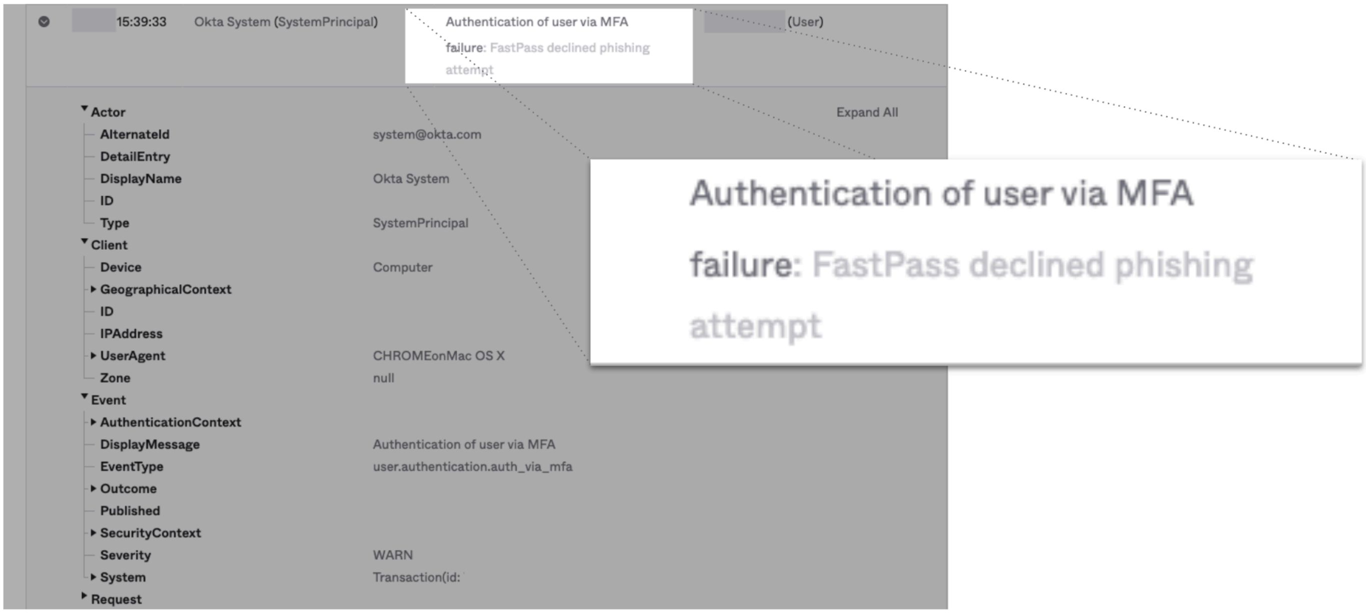
Proactive alerts provides customers opportunities to:

- Deny outbound requests to phishing infrastructure from managed devices,
- Request takedowns when the infringing site goes live, and
- Adjust access policies accordingly.

There are no guarantees, however, that every phishing domain will be detected in advance of a campaign. And even when they are, there is often a short window of exposure before takedowns take effect.

So the harder problem for defenders is how to quickly identify threat actor activity and remediate any exposure while users are under attack.

When your users are enrolled in FastPass, Okta can provide defenders a high-fidelity signal for when user applications are being targeted by attackers wielding real-time (AiTM) proxies.



```
[redacted] 15:39:33   Okta System (SystemPrincipal)   Authentication of user via MFA   [redacted] (User)
                                                      failure: FastPass declined phishing
                                                      attempt

▾Actor                                                                                Expand All
   AlternateId              system@okta.com
   DetailEntry
   DisplayName              Okta System
   ID
   Type                     SystemPrincipal
▾Client
   Device                   Computer
  ▸GeographicalContext
   ID
   IPAddress
  ▸UserAgent                CHROMEonMac OS X
   Zone                     null
▾Event
  ▸AuthenticationContext
   DisplayMessage           Authentication of user via MFA
   EventType                user.authentication.auth_via_mfa
  ▸Outcome
   Published
  ▸SecurityContext
   Severity                 WARN
  ▸System                   Transaction(id:
▸Request
```

Authentication of user via MFA

failure: FastPass declined phishing attempt

This Early Access feature is available for self-service on Okta Identity Engine - select "Phishing Resistance for FastPass" under **Settings > Features** in the Admin Console.

If one or more users enrolled in FastPass is targeted using AiTM phishing kits, Okta Identity Engine identifies the failed origin check and generates a unique event in Okta System Log:

eventType eq "user.authentication.auth_via_mfa" AND outcome.result eq "FAILURE" AND outcome.reason eq "FastPass declined phishing attempt"

The utility of that single system log event can't be understated. In many scenarios, it's likely to be the earliest available signal about an in-flight attack, and includes key details about the phishing infrastructure used by the adversary.

Why are those details so important? As we previously discussed in this series, there are relatively few organizations today that are 100% passwordless. Even in organizations where a majority of users are protected by phishing resistant factors, there are often groups of users with little choice but to rely on authenticators that are less resistant to phishing.

So any early detection offers opportunities to:

- Prevent other users from accessing (or authenticating via) the attacker’s infrastructure,
- Evaluate if other users were previously targeted via the same infrastructure,
- Evaluate if other users have entered credentials, and
- Evaluate if any of the phishing activity resulted in an account takeover.

Many of these actions can be automated using Okta Workflows (or using a third-party SOAR solution).

Okta Workflows can be used, for example, to:

- Extract the IP of the attacker’s proxy server.
- Assess the reputation of the IP (by checking the ratio of successful to unsuccessful authentication events from that IP over the weeks or months prior to the incident).
- Search System Log to check whether any other users successfully authenticated via a suspicious IP. If any value is returned, the flow can automatically clear the user’s sessions.
- If users entered a password as part of the authentication flow (irrespective of whether they successfully authenticated), the flow can call System Log to check whether the user’s corporate email application was accessed during the session in question. This can help determine whether to reset the user’s password.
- Raise a request to add the IP to an org-wide blocklist (network zone) to prevent future authentication requests via the attacker’s infrastructure.

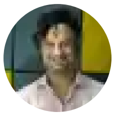
To see these ideas in action, we recommend catching up on the recorded sessions delivered on FastPass phishing resistance at this week's Oktane22 conference [Registration Required]:

- Security Deep Dive: Preventing Credential Phishing Attacks with Passwordless and Phishing Resistant Authenticators
- Security Deep Dive: Achieving Frictionless and Enhanced Credential Phishing Resistance with Okta FastPass

Updated detection query to include the missing outcome required in the outcome.result field.

1.0 - Nov 20, 2022

Original Version Published



Brett Winterford

Regional CSO, Okta APJ

Brett Winterford is the regional Chief Security Officer for Okta in the Asia Pacific and Japan.
He advises business and technology leaders on evolving threats and helps them harness advances in identity technology to drive business outcomes and mitigate risk.
Prior to Okta, Brett held a senior security leadership role at Symantec, and helmed security research, awareness and education at Commonwealth Bank.
Brett is also an award-winning journalist, having long ago been the editor-in-chief of iTnews Australia and a contributor to ZDNet, the Australian Financial Review and the Sydney Morning Herald. Most recently, he was the founding editor of the Srsly Risky Biz newsletter, a companion to the Risky Business podcast, providing the cybersecurity, policy, defense and intelligence communities with a weekly brief of the news that shapes cyber policy.

Defensive Cyber Operations

The Defensive Cyber Operations (DCO) team is responsible for detecting and responding to cyber threats that impact Okta or our customers via the Okta platform. Our intelligence-driven capability identifies the adversaries most likely to impact Okta and our customers, and prioritises our defensive capabilities based on the threats most likely to be realised.