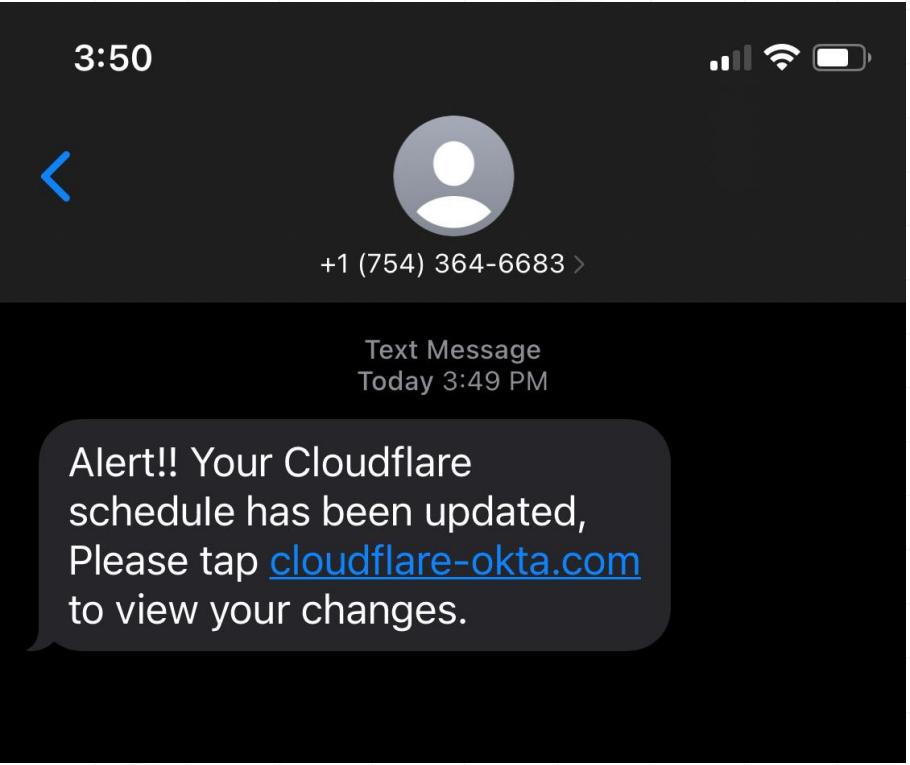
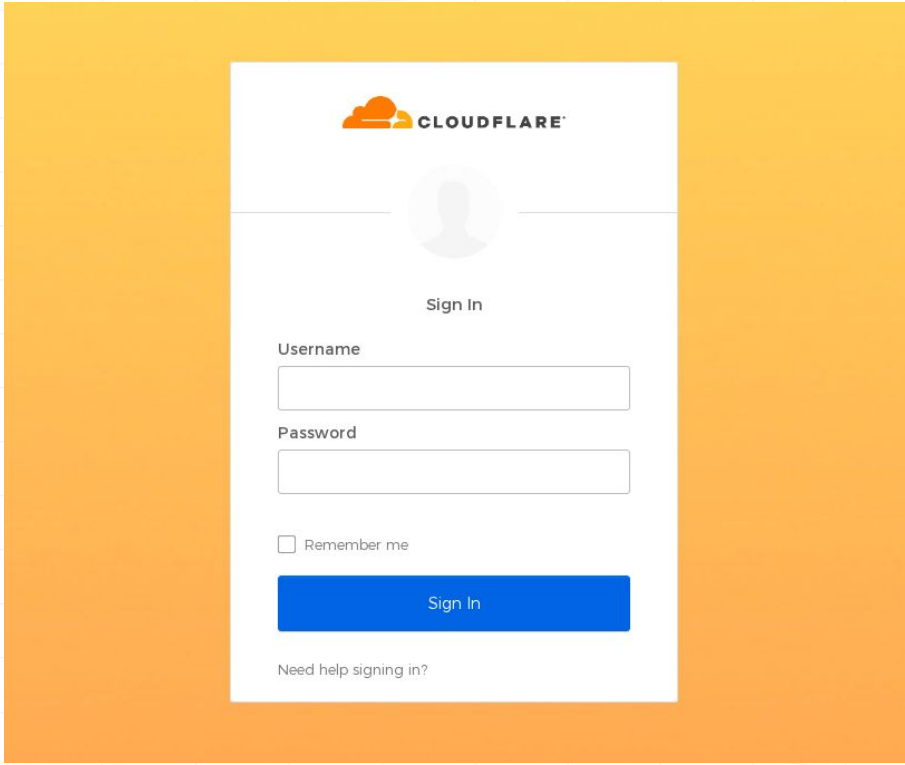
CLOUDFLARE

How Cloudflare stopped a targeted attack and you can too

What Cloudflare employees saw



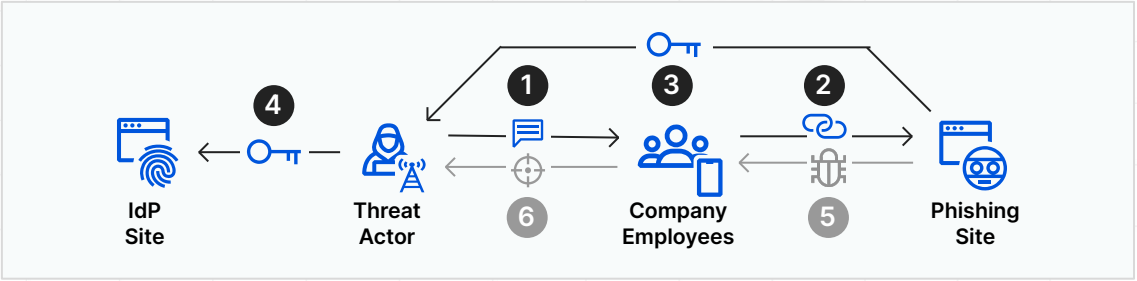


Threat actor attempted credential harvesting playbook
but was unsuccessful gaining full access

[1-2] Targeted text messages

[3-4] Sophisticated real-time phishing

[5-6] Remote access payload



#	What happened
1a	Threat actor sent legitimate-looking malicious SMS **100+ messages sent from four T-Mobile-SIMs**
1b	76+ Company employees and family members received SMS on personal & work phones
2a	Message included a legitimate-looking newly registered domain (cloudflare-okta.com)
2b	Clicking link opened a legitimate-looking phishing site (Cloudflare Okta login page) Domain registered via "Porkbun" <40 min before phishing campaign to avoid automated detection
3a	Victim's entered credentials were immediately relayed to the threat actor via Telegram
4a	Threat actor enters credentials received into actual identity provider (IdP) login site; sending TOTP codes to victims via SMS or mobile app
3b	Victim enters TOTP code on the phishing site, and it too would be relayed to the threat actor **3 employees reached this step, but did not go further as security keys don't use TOTP**
4b	Threat actor enters code in IdP site before it expires: Defeats most 2FA implementations
5	Phishing site initiated download of a phishing payload (may have been due to a misconfigured kit)
6	Once software installs, threat actor controls victims' machine remotely

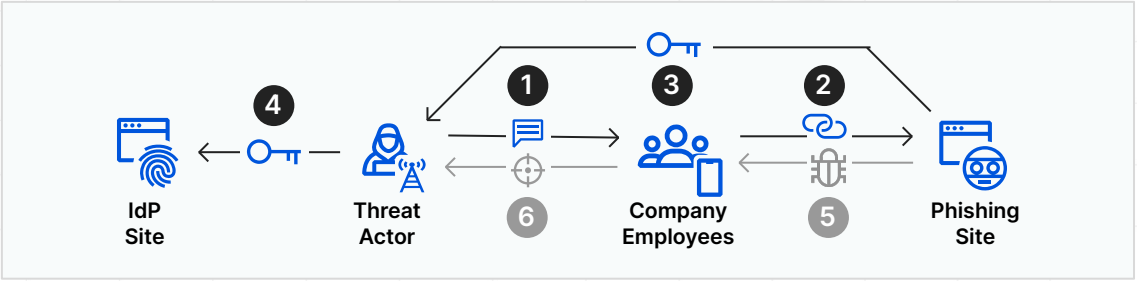
CLOUDFLARE

Threat actor attempted credential harvesting playbook
but was unsuccessful gaining full access

[1-2] Targeted text messages

[3-4] Sophisticated real-time phishing

[5-6] Remote access payload



#	Our response
1	• **1 min after attack**, SIRT was informed; no evidence of compromise via directory provider logs • **9 min after attack**, SIRT sent an internal warning to all employees across chat & email
2	• **3 min after attack**, SIRT added domain to SWG to block access. Later, isolated access to all newly registered domains and seized control of domain. • **37 min after attack**, DigitalOcean shutdown the attacker's server via our collaboration
3	• **1-37 min after attack**, SIRT killed active sessions via ZTNA, plus 48 min after attack, SIRT reset credentials & initiated scans for the identities & devices with unverified 2FA per our activity logs
4	• Intel from server indicated actor was targeting other orgs, including Twilio, and SIRT shared intel • SIRT blocked IPs used by threat actor from accessing any Cloudflare service
5	n/a
6	Note: Endpoint security used by Cloudflare would have stopped the installation

CLOUDFLARE

Reinforced the importance of what we're doing well, and everything you can do, too

1. **Adopt a phishing-resistant MFA**
   Not all MFA provides the same level of security

2. **Implement selective enforcement**
   with identity- and context-centric policies

3. **Enforce strong auth everywhere**
   All users and apps; even legacy non-web systems

4. **Adopt Zero Trust via one platform**
   Easier, faster operations & improved security posture

5. **Establish paranoid, blame-free culture**
   Report suspicions early and often

CLOUDFLARE