Advanced Adversary SSO Abuse

The prevalence and efficacy of advanced adversary abuse of Single Sign-On (SSO) services has been steadily increasing over the past several years. Telltale signs of adversary targeting arose years ago with a notable series of BGP hijacks impacting major SSO service provides and their infrastructure (e.g., 2020 Rostelecom BGP hijacking incident impacting more than 200 CDNs and cloud providers), and since that time consistently larger waves of SSO abuse (e.g., Uber) provide evidence and speak to the growing maturity of actors' capabilities in this domain.

In August and September 2022, Red Sense observed a number of malicious devices broadly attacking prominent Western organizations' infrastructure via advanced SSO probing and exploitation attempts, e.g. potential early abuse of recent Microsoft Exchange 0days.

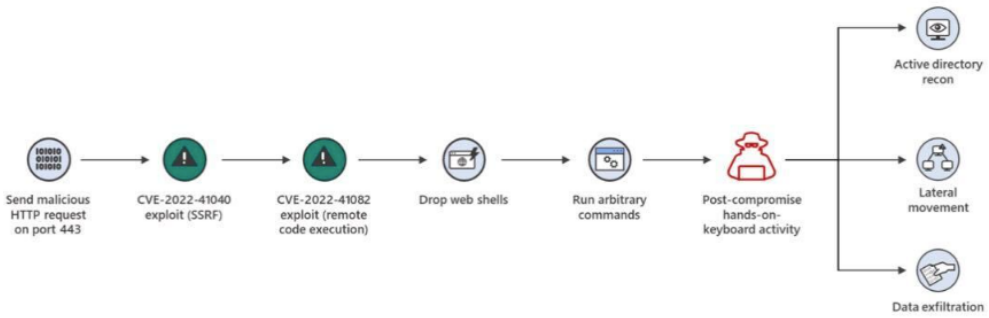

figure 1. advanced adversary attack vector

These devices were noted as primarily conducting low and slow MFA bypass attacks against SSO chokepoints with broad targeting a mix of financial, government, and academia targets. One such device, 52.55.50.201 was a compromised AWS machine running a reverse shell tor proxy.

start_time	src_ip_addr	dst_ip_addr	proto	src_port	dst_port
9/29/22 9:48	52.88.50.201	172.105.47.96	6	33359	9001
9/29/22 10:22	52.88.50.201	5.199.162.114	6	25225	9001
9/29/22 11:28	52.88.50.201	172.105.47.96	6	51579	9001
9/29/22 12:12	52.88.50.201	176.126.70.55	6	33187	9001
9/29/22 13:07	52.88.50.201	172.105.47.96	6	39526	9001
9/29/22 13:30	52.88.50.201	195.230.23.248	6	45684	9001
9/29/22 14:53	52.88.50.201	5.199.162.114	6	13656	9001
9/29/22 16:27	52.88.50.201	176.126.70.55	6	29205	9001
9/29/22 17:53	52.88.50.201	195.230.23.248	6	3345	9001
9/30/22 8:02	52.88.50.201	94.46.171.221	6	28066	9001
9/30/22 8:02	52.88.50.201	46.165.253.196	6	21175	9001
9/30/22 8:02	52.88.50.201	83.171.236.7	6	26322	9001
9/30/22 8:02	52.88.50.201	46.165.253.196	6	5554	9001
9/30/22 8:03	52.88.50.201	188.166.31.252	6	11638	9001
9/30/22 8:03	52.88.50.201	188.166.31.252	6	11638	9001
9/30/22 8:07	52.88.50.201	188.166.31.252	6	11770	9001
9/30/22 8:12	52.88.50.201	94.46.171.221	6	38277	9001
9/30/22 8:19	52.88.50.201	94.46.171.221	6	38277	9001
9/30/22 8:20	52.88.50.201	188.166.31.252	6	40016	9001
9/30/22 8:23	52.88.50.201	94.46.171.221	6	63086	9001
9/30/22 8:32	52.88.50.201	46.165.253.196	6	5554	9001
9/30/22 10:44	52.88.50.201	94.46.171.221	6	39645	9001
9/30/22 11:09	52.88.50.201	188.166.31.252	6	63523	9001
9/30/22 11:38	52.88.50.201	46.165.253.196	6	52897	9001
9/30/22 12:07	52.88.50.201	83.171.236.7	6	48797	9001
9/30/22 13:08	52.88.50.201	188.166.31.252	6	13655	9001

figure 2. tor proxy activity

Leveraging the tor proxy, low and slow MFA exploitation activity clearly impacted dozens of significant target organizations. One such target is an undisclosed “University Medical Center”, see below.

start_time	src_ip_addr	dst_ip_addr	proto	src_port	dst_port
9/22/22 23:57	52.88.50.201	redacted	6	64064	443
9/24/22 9:59	52.88.50.201	redacted	6	57194	443
9/24/22 10:29	52.88.50.201	redacted	6	16963	443
9/24/22 14:57	52.88.50.201	redacted	6	15599	443
9/24/22 14:57	52.88.50.201	redacted	6	15599	443
9/24/22 14:57	52.88.50.201	redacted	6	16606	443
9/24/22 17:58	52.88.50.201	redacted	6	51679	443
9/24/22 19:34	52.88.50.201	redacted	6	48096	443
9/24/22 19:57	52.88.50.201	redacted	6	1359	443
9/25/22 16:27	52.88.50.201	redacted	6	13497	443
9/25/22 16:27	52.88.50.201	redacted	6	22663	443
9/25/22 17:03	52.88.50.201	redacted	6	56311	443
9/25/22 17:06	52.88.50.201	redacted	6	5817	443
9/25/22 21:59	52.88.50.201	redacted	6	15434	443
9/26/22 12:49	52.88.50.201	redacted	6	41514	443
9/26/22 15:25	52.88.50.201	redacted	6	13600	443
9/26/22 15:25	52.88.50.201	redacted	6	11139	443
9/26/22 15:25	52.88.50.201	redacted	6	65025	443
9/26/22 21:38	52.88.50.201	redacted	6	51363	443
9/27/22 1:09	52.88.50.201	redacted	6	62750	443
9/27/22 17:20	52.88.50.201	redacted	6	30981	443
9/27/22 20:11	52.88.50.201	redacted	6	18438	443
9/27/22 20:28	52.88.50.201	redacted	6	59318	443
9/27/22 20:28	52.88.50.201	redacted	6	47516	443
9/27/22 20:28	52.88.50.201	redacted	6	12211	443
9/27/22 21:51	52.88.50.201	redacted	6	18518	443
9/27/22 21:51	52.88.50.201	redacted	6	18518	443
9/28/22 19:47	52.88.50.201	redacted	6	38637	443
9/29/22 13:51	52.88.50.201	redacted	6	28745	443
9/29/22 13:51	52.88.50.201	redacted	6	38465	443
9/29/22 13:51	52.88.50.201	redacted	6	38465	443
9/29/22 15:58	52.88.50.201	redacted	6	64694	443
9/30/22 0:28	52.88.50.201	redacted	6	35665	443

figure 3. low and slow MFA exploitation

The targeted device hosts this organizations central authentication services (cas.<redacted>[.]edu) and a Duo security application integration. (Note: this activity was tipped off to affected target organization as it was discovered).

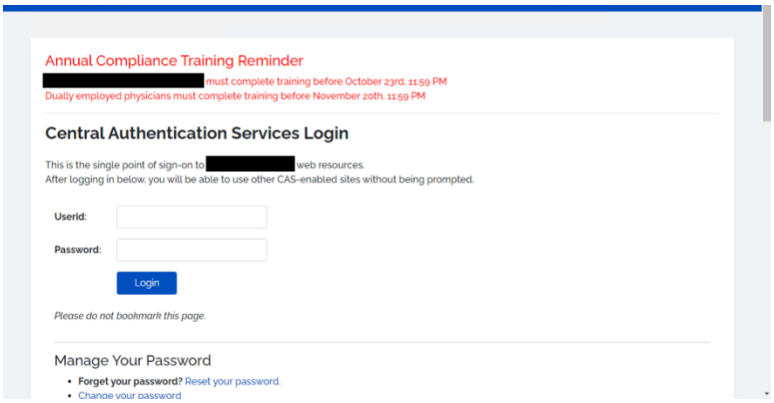

figure 4. Targeted central authentication services

Chokepoints like centralized authentication services remain a critical target for adversaries; take note of the growing maturity of their (adversaries’) operational capabilities for SSO abuse and exploitation.