Cyberattacks target international conference attendees

By Tom Burt

Published: 2020-10-28 · Archived: 2026-04-06 01:30:40 UTC

Today, we're sharing that we have detected and worked to stop a series of cyberattacks from the threat actor Phosphorus masquerading as conference organizers to target more than 100 high-profile individuals. Phosphorus, an Iranian actor, has targeted with this scheme potential attendees of the upcoming Munich Security Conference and the Think 20 (T20) Summit in Saudi Arabia. The Munich Security Conference is the most important gathering on the topic of security for heads of state and other world leaders, and it has been held annually for nearly 60 years. Likewise, T20 is a highly visible event that shapes policy ideas for the G20 nations and informs their critical discussions.

Based on current analysis, we do not believe this activity is tied to the U.S. elections in any way.

The attackers have been sending possible attendees spoofed invitations by email. The emails use near-perfect English and were sent to former government officials, policy experts, academics and leaders from non-governmental organizations. Phosphorus helped assuage fears of travel during the Covid-19 pandemic by offering remote sessions.

We believe Phosphorus is engaging in these attacks for intelligence collection purposes. The attacks were successful in compromising several victims, including former ambassadors and other senior policy experts who help shape global agendas and foreign policies in their respective countries.

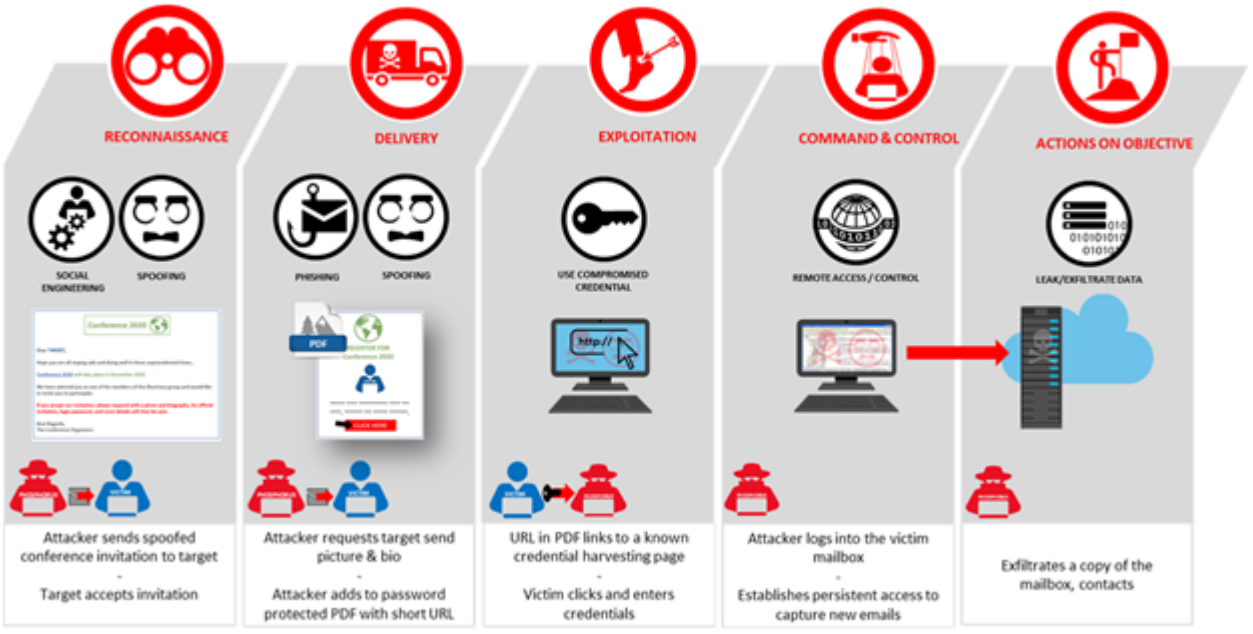

Figure 1: Flow of a typical Phosphorus attack in this campaign

This activity was uncovered by Microsoft's Threat Intelligence Center, or MSTIC, which tracks the world's nation-state and cybercrime actors so we can better protect our customers. MSTIC is also critical to the work of our Defending Democracy Program, powering our AccountGuard threat notification service available in 30 countries worldwide and fueling the intelligence we share to help keep elections secure. We build new protections into our products regularly based on the threats MSTIC uncovers.

We've already worked with conference organizers who have warned and will continue to warn their attendees, and we're disclosing what we've seen so that everyone can remain vigilant to this approach being used in connection with other conferences or events.

We recommend people evaluate the authenticity of emails they receive about major conferences by ensuring that the sender address looks legitimate and that any embedded links redirect to the official conference domain. As always, enabling multi-factor authentication across both business and personal email accounts will successfully thwart most credential harvesting attacks like these. For anyone who suspects they may have been a victim of this campaign, we also encourage a close review of email-forwarding rules in accounts to identify and remove any suspicious rules that may have been set during a successful compromise.

We are also sharing the indicators of compromise (IOCs) observed during these activities. We encourage IT teams to implement detections and protections to identify possible prior campaigns and prevent future campaigns against their users. These indicators include phony email accounts and domains or websites used to steal victims' credentials.

INDICATOR	TYPE	DESCRIPTION
t20saudiarabia[@]outlook.sa	Email	Masquerading as the organizer of the Think 20 (T20) conference
t20saudiarabia[@]hotmail.com	Email	Masquerading as the organizer of the Think 20 (T20) conference
t20saudiarabia[@]gmail.com	Email	Masquerading as the organizer of the Think 20 (T20) conference
munichconference[@]outlook.com	Email	Masquerading as the organizer of the Munich Security Conference
munichconference[@]outlook.de	Email	Masquerading as the organizer of the Munich Security Conference
munichconference1962[@]gmail.com	Email	Masquerading as the organizer of the Munich Security Conference
de-ma[.]online	Domain	Domain used for credential harvesting
g20saudi.000webhostapp[.]com	Subdomain	Subdomain used for credential harvesting
ksat20.000webhostapp[.]com	Subdomain	Subdomain used for credential harvesting

As we noted in our recent Digital Defense Report, nation-state cyberattackers routinely pursue think tanks, policy organizations and governmental and non-governmental organizations, seeking information that an attacker can use for their benefit. We will continue to use a combination of technology, operations, legal action and policy to disrupt and deter malicious activity, but nothing replaces vigilance from people who are likely targets of these operations.

Tags: cyberattacks, cybersecurity, Defending Democracy Program, Microsoft AccountGuard, Microsoft Threat Intelligence Center, MSTIC
