On-demand Webcast: CrowdStrike Experts on COVID-19 Cybersecurity Challenges and Recommendations

By Michael Busselen

Archived: 2026-04-02 12:19:40 UTC

A new on-demand webcast, "Cybersecurity in the Time of COVID-19," features CrowdStrike® CTO Mike Sentonas, VP of Intelligence Adam Meyers and Sr. Director of Product Management Brian Trombley as they discuss ways for companies to overcome the cybersecurity challenges they're facing during this worldwide crisis. Along with recommendations, they also detail new programs CrowdStrike has introduced to help organizations support and secure a newly remote workforce. In setting a context for the webcast, Sentonas says, "The cybersecurity considerations organizations are facing at this time are as varied as they are complex, and we are going to try and touch on as many of them as possible."

Challenges of Working From Home

Sentonas points out that while CrowdStrike has been working remotely since the company began, many companies are not prepared to pivot rapidly and enable a large-scale remote workforce. This is especially challenging as more regions establish guidelines and regulations to enforce social isolation and keep people at home. He cites some of the issues that enabling a remote workforce can entail:

- In addition to security considerations, a fast migration to employees using personal computers creates more complex connectivity problems.
- Although there are many organizations that already enable remote workers and are somewhat prepared for the current crisis, many more are struggling to make this transition at speed.
- A lack of IT resources is a perpetual complaint in many organizations, but it's significant in this case. The number of helpdesk calls goes way up when you are connecting from a home device — what do you troubleshoot? We're getting this feedback from a lot of organizations.

Sentonas also has some suggestions for how companies can help make a smoother and more secure transition to a remote workforce. If the following key factors aren't already a part of your security strategy, they should be part of your planning going forward:

- Make sure you have current cybersecurity policies that include remote working.
- Plan for BYOD devices connecting to your organization.
- Know that sensitive data may be accessed through unsafe WiFi networks.
- Cybersecurity hygiene and visibility will be critical.
- Continued education is important as COVID-19 schemes escalate.
- Crisis management and IR plans need to be executable by a remote workforce.

Adversaries Are Exploiting the COVID-19 Crisis

In the webcast, Meyers summarizes the CrowdStrike Intelligence team's observations on nation-state and eCrime actors that are leveraging the pandemic to further their own criminal objectives. "What we're seeing from a threat intelligence perspective is that threat actors have been using and are continuing to use the COVID-19 pandemic as themes and to help enable their operations." Recent adversary activity his team has observed includes the following:

- **MUMMY SPIDER**, an eCrime adversary originating out of Eastern Europe or the Russian Federation, is linked to the core development of the malware most commonly known as Emotet or Geodo. This adversary has been observed targeting a wide range of organizations globally and capitalizing on the ongoing coronavirus outbreak by using the pandemic as a theme for email system attacks. "Emails were sent using a technique that we call email thread hijacking, where the adversary gets into a victim machine and is able to access their email," Meyers explains. "They look for a thread they can jump into and send, and inject content in order to increase the chances that somebody will trust that email enough to click on a link or open an attachment."
- **PIRATE PANDA**, also known as APT23, KeyBoy and Tropic Trooper, was last observed in February. This adversary typically targets India, Japan, Mongolia, the Philippines, Taiwan and Vietnam. Recently the threat actor has been observed using an English-language lure that appears to be from Mongolia's ministry of health, and is formatted to look like a World Health Organization daily report. "Though we can't see exactly who was targeted, based on the content, we can see the types of entities that they would have targeted, such as governmental organizations and non-governmental organizations (NGOs)," Meyers says.
- **Ransomware Big Game Hunting (BGH)** — Meyers says his team has observed adversaries using ransomware BGH attacks with COVID-19 lures against organizations that have a particularly critical need to stay operational, such as healthcare entities and state and local governments. He adds, "We're in a state of high alert when it comes to information pertaining to COVID-19. We're tracking threat actors that are rapidly trying to adopt this into their operations."

CrowdStrike Programs to Support Remote Workers

In his presentation, Trombley outlines two free programs that CrowdStrike has initiated to help customers move rapidly to a remote workforce model, while ensuring security across their enterprises and keeping costs low. These include a Burst Licensing program for organization-owned devices and a new version of CrowdStrike Falcon Prevent™ next-generation antivirus protection for Home Use for employee-owned devices. The Burst Licensing program is designed to help customers alleviate concerns associated with licensing the CrowdStrike Falcon® platform to protect a surging number of new systems being deployed for use by remote workers. This program is particularly vital because these systems may only be needed for a short period of time. Falcon Prevent for Home Use provides organizations with a low-cost option for securing employees' home Windows devices. For more information on these programs, read this blog: CrowdStrike Announces Two New Programs to Help Organizations Secure Remote Workers During COVID-19 Crisis. Both of these programs are being offered at no additional cost to existing CrowdStrike customers for a limited period of time. Don't miss this important on-demand webcast: **"Cybersecurity in the Time of COVID-19."**

Additional Resources

- *Read a blog on COVID-19 cybersecurity from CrowdStrike CEO George Kurtz.*
- *Learn about adversary activities around the COVID-19 crisis and get weekly updates in this blog: "Situational Awareness: Cyber Threats Heightened by COVID-19 and How to Protect Against Them."*
- *Learn more about the cybersecurity challenges during COVID-19 and recommendations for securing your remote workforce in blogs by CrowdStrike CTO Mike Sentonas and Chief Product and Engineering Officer Amol Kulkarni.*
- *Access resources to help you ensure the security of your organization and remote workers by visiting the CrowdStrike COVID-19 resource webpage.*
- *Download the CrowdStrike 2020 Global Threat Report.*
