UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

Video-Conference Calls are Target for Cybercriminals

QUANTICO, VA (April 15, 2020) – During the COVID-19 pandemic, more people have turned to video-teleconferencing to stay in touch with loved ones, collaborate with coworkers, and even attend medical appointments. The increase in video-conferencing browsing trends has garnered the attention of hackers who are looking for innovative ways to infiltrate computer software systems.

"Cybercriminals are conducting sophisticated phishing campaigns and exploiting vulnerabilities within various Video-Teleconferencing platforms to steal sensitive data," said Edward Labarge, director, Major Cybercrime Unit (MCU). "A lot of this stolen data is already being sold on the darkweb. This highlights the importance of using only approved Department of Defense software, tools, and platforms for official government business."

The use of collaboration tools enhances the military's mission attainment and day-to-day business process capabilities. However, the use of unauthorized collaboration tools on Government Furnished Equipment (GFE) has the potential to expose critical information or introduce vulnerabilities. Commands should remind personnel that use of unauthorized commercial collaboration tools or using commercial email for official business could be a violation of Army policy.

"Official Army business should only be done on Government Furnished Equipment," said Labarge. "Even though many of us are working from home, that doesn't mean our duties to protect Army information stops. Emails containing sensitive data must be encrypted and we should never use personal email for official business."

Labarge explained, cybercriminals are able to exploit VTC software—whether it's a paid service

-MORE-

or free—to obtain sensitive information or even eavesdrop on conference calls and virtual meetings. To gain access, cybercriminals may employ phishing, spoofed links or mobile applications that appear to come from legitimate VTC vendors.

CID officials also stated some VTC software companies may not have the user's best interest in mind. One well-known VTC company is currently being sued for allegedly selling user data to third parties, including a popular social media company. According to the lawsuit, a VTC company has provided the third-party with customer information, including details of the device used.

"Like all online accounts, it's important to use complex passwords coupled with two-factor authentication," said Labarge. "The majority of online platforms offer two-factor authentication in the form of SMS text messages or even through the use of an Authenticator App. Additionally, it's important to never use the same password for all your accounts."

As always, you should apply cyber best practices and weigh associated risks to ensure privacy and protect critical information. Consider the following steps:

- Verify the link to the meeting you attend is legitimate.
- Make sure to download the VTC software from the correct website.
- Verify the meeting ID and dial-in information is legitimate.
- Do not make meetings public.
- Do not share a link to a teleconference in an unrestricted, publicly available social media post. Provide the link directly to specific people.
- Avoid remote desktop sharing.

Below is a list of approved collaboration software for Army personnel to use for official telework purposes. Contact a system administrator for additional guidance on approved VTC software.

- DISA Global Video Service (GVS)
- Defense Collaboration Services (DCS)
- Skype for Business
- Intelink
- milSuite
- DoD Commercial Virtual Remote (CVR) Environment

According to CID officials, there is also an approved option of "Zoom for Government," still available for DOD use with prior approval.

-30-

For more information about computer security, other computer-related scams, and to review previous cybercrime alert notices and cyber-crime prevention flyers visit the Army CID MCU

website at https://www.cid.army.mil/mcu-advisories.html. To report a crime to Army CID, visit www.cid.army.mil