Cyber Criminals Don’t Brake for Pandemics

By Stephen Murphy, DC3 Public Affairs

The ongoing COVID-19 pandemic has resulted in disruptions to everyday life for many with shelter-in-place and other social distancing requirements implemented throughout the United States and around the rest of the world.

Even though many supplies, services and leisure activities have slowed down or have come to a screeching halt, the one thing that has remained the same, or even gained momentum – is cyber espionage.

From the average citizens who encounter ransomware and malware scams via fraudulent stimulus check scams, all the way up to DoD-level organizations encountering attempted cyber intrusions/compromises from advanced persistent threat (APT) groups, cyber criminals and APT groups are actively working to exploit the COVID-19 pandemic.

The DoD Cyber Crime Center (DC3), located in Linthicum Heights, Md., and serving as the operational focal point for the Defense Industrial Base (DIB) Cybersecurity (CS) program, is keeping ahead of APT groups who exploit the COVID-19 pandemic in an attempt to infiltrate and exploit DIB and DoD networks. Its DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) maintains close situational awareness regarding the use of COVID-19 themed social engineering and email phishing scams by cyber actors—from criminal actors employing ransomware to more sophisticated nation-state operators conducting cyber espionage.

As the operational arm of the DIB Cybersecurity (CS) program, DCISE shares relevant information with more than 700 Cleared Defense Contractors (CDCs) who participate in the program. DCISE fosters a cyber-threat information sharing partnership with DIB participants by performing cyber analysis, offering mitigation and remediation strategies, providing best practices, conducting analyst-to-analyst exchanges, and holding cyber threat sharing meetings and technical exchanges with DIB participants.

"The public-private partnership that exists between the DIB partner companies and the DoD is built upon a foundation of trust, which is vital to critical cyber threat information sharing,” said DCISE director, Krystal Covey. “This crowd-sourced threat sharing allows for near real-time collaboration; enabling members of the partnership, as well as U.S. Government (USG) agencies, to potentially detect/deter, and remediate before an incident occurs or escalates."

The DCISE has processed multiple DIB reports specific to COVID-19-themed schemes during the past month. Domain masquerading is heavily used in these schemes; one partner company reported receiving an e-mail from the Center for Disease Control and Prevention with a link to a credential-harvesting site.

A DIB CS voluntary partner notified DCISE in late March that a USG Central Authentication Service (CAS) login service was using a web service as an open redirect (proxy) to commit COVID-19 phishing.

The DIB partner requested DCISE alert the USG for remediation. DCISE informed USG points of contact (POC) the same day. The USG entity advised March 26, that the asset in question

was taken offline and an investigation was underway. The same entity also requested DIB CS Partner POC information to engage and ensure they had all relevant technical details.

“This scenario highlights that the DIB CS Voluntary Program provides critical communication and benefits beyond its immediate scope and mission—such as identifying issues with USG Information Technology assets and ensuring notification to the correct USG POC, even during an unprecedented pandemic,” said Covey.

DCISE monitors evolving cyber activities that exploit the pandemic and will ensure the DIB Partnership and USG are fully informed to better protect their respective network environments. The DCISE will continue processing all submissions from its partners and encourage maximum cyber threat collaboration during this challenging time. This type of public-private communication demonstrates DCISE and the DIB CS Program’s role in protecting critical DoD assets.

For more information about DCISE, visit https://www.dc3.mil/cyber-security.

For more information on the DIB CS Program, visit https://dibnet.dod.mil/portal/intranet/.

For more information about the DoD Cyber Crime Center, visit https://www.dc3.mil/.