NEWS RELEASE

FOR IMMEDIATE RELEASE
March 25, 2021

CONTACT:
Brian Weiss (USTelecom): (202) 326-7226
Jennifer Drogus (CTA): (571) 527-6193

Council to Secure the Digital Economy Releases 2021 Botnet and IoT Security Guide

Leading global technology companies outline security strategies to protect digital economy from growing botnet attacks

Global botnet threat accelerated during the COVID-19 pandemic with phishing campaigns running rampant across the internet

10 million denial of service attacks launched in 2020; 542 percent increase in these attacks during pandemic-mandated work from home protocols

WASHINGTON, DC – The Council to Secure the Digital Economy (CSDE), a partnership between global technology, communications and internet companies supported by USTelecom—The Broadband Association and the Consumer Technology Association (CTA)®, today released the International Botnet and IoT Security Guide 2021.

CSDE's third annual report includes an update on the global threat of botnets, malware and distributed attacks, as well as recommendations for government and industry to detect vulnerabilities and malicious traffic against shared digital infrastructure, software and the rapidly growing Internet of Things (IoT) segment.

Botnets are large networks of compromised, internet-connected computers and devices that malicious actors can command to commit distributed denial of service (DDoS) attacks, spread ransomware, phishing attacks and disinformation campaigns amplifying inauthentic social media, and commit other harmful acts against the networks and platforms comprising the global digital economy.

CSDE's 2021 report includes an analysis of how the global COVID-19 pandemic has accelerated the botnet threat. Among the findings:

- There were 10 million DDoS attacks in 2020. These attacks increased by 542 percent from Q4 2019 to Q1 2020, a surge correlating with pandemic-mandated work from home protocols.

- During the pandemic, malicious actors increasingly aimed DDoS attacks at health and research facilities, as well as essential government and private sector services around the world.

- Botnets are spreading via fake virtual private network (VPN) clients and installers as the workforce migrates to remote working.

- Botnets are exploiting public demand for information about the pandemic to spread phishing lures; botnets also regularly targeted online retailers, including vendors of sanitizers and face masks.

- In the face of these increased threats, industry accelerated 'baseline' IoT cybersecurity requirements, deployed new technical standards, and launched new cybersecurity certification programs.

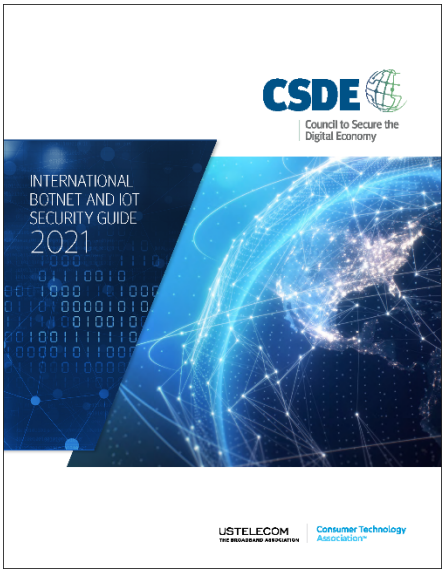
Robert Mayer, Senior Vice President of Cybersecurity and Innovation, USTelecom said: "This is a good news/bad news story. The bad news: criminals and bad actors have capitalized on the disruption of the pandemic to launch increasingly destructive and sophisticated attacks against the digital ecosystem at precisely the time the world was relying on that infrastructure more than ever. The good news: internet innovators have gone on the offensive and our ability to predict both botnet attacks and develop countermeasures is improving daily. There are ways to reduce the threat, and our CSDE report has some excellent guidance and concrete strategies to fight this clear and present cyber risk to our connected economy."

Mike Bergman, vice president of technology and standards, CTA said: "Connected technology is essential for us to work, learn and meet during the pandemic – but that dependence poses risk. This report puts a spotlight on the severity of the situation, then lays out the critical steps the major stakeholders – including enterprises, software developers, infrastructure providers, device makers and system installers – should be taking."

According to the report, IoT connected devices will outnumber the human population tenfold – 80 billion devices by 2025. As the number of connected people, businesses and devices grows, so does the potential for malicious attacks. By 2022, cyber-crimes alone are estimated to cost businesses $8 trillion (in fines, loss of business, remediation costs, etc.).

Infrastructure costs are also escalating, as companies must continuously invest to maintain and build excess capacity to ensure reliable service. The intangible costs are also detrimental, as these threats undermine fundamental confidence and trust in the digital economy.

CSDE's International Botnet and IoT Security Guide 2021 is available **HERE**.



About the Council to Secure the Digital Economy (CSDE)
CSDE brings together leading global enterprises from across the information technology, communications, and cybersecurity sectors. Its founding partners include Akamai, AT&T, Cisco, Ericsson, IBM, Intel, Lumen, NTT, Oracle, Samsung, SAP, Telefónica and Verizon. The CSDE's Secretariat includes USTelecom and CTA. For more information visit: www.securingdigitaleconomy.org.

About Consumer Technology Association
As North America's largest technology trade association, CTA® *is* the tech sector. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the most influential tech event in the world. Find us at CTA.tech. Follow us @CTAtech.

About USTelecom
USTelecom is the national trade association representing technology providers, innovators, suppliers, and manufacturers committed to connecting the world through the power of broadband. Visit us at www.ustelecom.org.

###