## CISA Releases Guidance on new DDoS Mitigations

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has **release new guidance** to help federal agencies adopt distributed denial-of-service (DDoS) mitigations. The **guidance** is to help federal agencies prevent DDoS attacks and describe various DDoS mitigation services to help agencies services to help agencies make informed procurement decisions. According to CISA, the guidance focuses on DDoS attacks targeting websites and related web services, which are meant to deny user access to them. Before deciding which type of DDoS mitigation to adopt, federal agencies should make an inventory of agency-owned or operated webservices and analyze the impact a DDoS would have against those services. CISA also recommends when agencies are considering the adoption of mitigations against DDoS attacks, federal agencies should look at content delivery networks (CDNs), internet service providers (ISPs) and upstream providers, and cloud service provider hosted services.

## Beware of MalDoc in PDF

Researchers have discovered a **new antivirus evasion technique** that involves embedding a malicious Microsoft Word file into a PDF file. The sneaky method, dubbed 'MalDoc in PDF' by JPCERT/CC is said to have been deployed for over two months. A file created with MalDoc in PDF can be opened in MS Word even though it is a PDF document. Researchers state that the file has a configured macro and while in Word, it opened a visual basic script (VBS), which can run and perform malicious attacks. These types of files are called **polyglots** and are legitimate forms of multiple files types, such as Adobe PDF and Microsoft Word documents. This new technique has been used for different malicious campaigns, such as credential harvesting and social engineering attacks leveraging vishing and phishing tactics to gain unauthorized access to target systems.

## Parliament Approves Online Safety Bill

On 19 September, the UK Parliament approved the **Online Safety Bill**, that imposes a duty onto online platforms to shield young users from inappropriate or self-harm content wile exposing users to **potential criminal prosecution** for sending harmful and threating communications. The legislative now awaits the formality of royal assent before enactment, and grants British media and communication regulator Ofcom the power to fine violators up to 18 million pounds or 10% of their global annual revenue; whichever is greater.

## US Quietly Removes Botnet Infections

On 29 August, the US government **announced a coordinated crackdown** against QakBot malware. International law enforcement was involved in seizing control over the botnet's online infrastructure and quietly removing the malicious software from tens of thousands of infected computers. The internal operations called 'Duck Hunt' allowed the U.S. Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) to obtain court orders to remove Qakbot from infected devices, and to seize servers used to control the botnet. Authorities stated that Qakbot has been implicated in 40 different ransomware attacks over the past 18 months, and cost victims more than $58 million in losses. The FBI and DOJ worked with law enforcement partners in France, Germany, Latvia, the Netherlands, Romania and the United Kingdom and was able to seize more than 50 Internet servers connected to the malware network and close to $9 million in cryptocurrency.

# White House and DHS Look to Simplify Cyber Incident Reporting Rules

The Cyber Incident Reporting Council (CIRC) within the Department of Homeland Security (DHS) **released a report on 19 September** with recommendations for changing the many cyber incident reporting requirements faced by critical infrastructure institutions. This is part of efforts by the Biden administration to develop a more effective cyber policy. The report found that critical infrastructure institutions must comply with 45 different reporting requirements from 22 different federal agencies, excluding five additional requirements under consideration.

Recommendations from the report include making incident reporting requirements and the submission process as uniform as possible; creating a model definition, trigger, and timeline for a reportable cyber incident; creating a model cyber incident reporting form that can be adopted across all federal agencies; and streamlining the reporting and sharing of information on cyber incidents. Additionally, the Secretary for Policy and CIRC Chair Robert Silvers stated: "federal agencies should be able to receive the information they need without creating duplicative burdens on victim companies that need to focus on responding to incidents and taking care of their customers".

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner. This newsletter is not intended to replace the benefits of joining FS-ISAC. Learn more at fsisac.com.