BUSINESSAFE

BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 20-164 **July 2020, Issue #30**

BusinesSafe Threat Topic: DDoS Attacks

A distributed denial of service, or DDoS, attack occurs when a malicious cyber actor attempts to disrupt a website or online service by sending an overwhelming amount of internet traffic to a targeted server. These attackers typically use multiple hacked computers operating in unison, known as botnets, to carry out these attacks. The traffic used to overwhelm these systems may include incoming messages, requests for connections, or other data inputs. Signs of a DDoS attack include unusually slow network performance, unavailability of a website or application, and an inability to access certain websites.

DDoS attacks have increased in recent years as the number of devices connected to the internet has increased. Today, devices that make up the Internet of Things, like smart appliances, smart vehicles, and smart industrial devices, can also be compromised and used as components in a botnet. These devices may have default passwords set or weaker security measures, creating an opportunity for exploitation by cyber criminals. The malicious cyber actors behind a DDoS attack may be difficult to identify because the true source of the attack may be masked through the compromised devices within the botnet.

- In February 2020, Amazon Web Services reportedly experienced the largest DDoS attack in history caused by a "reflection attack". This type of DDoS attack occurs when a vulnerable third-party server is used to amplify the amount of traffic being sent to the target's IP address. The attack volume was 44% larger than any network event detected by Amazon Web Services with a volume of 2.3 terabytes per second. The attack was reportedly mitigated by a protection service.
  Amazon Says it Mitigated the Largest DDoS Attack ever Recorded

- In March 2020, the U.S. Department of Health and Human Services experienced a DDoS attack that attempted to disrupt the department's operations. Department officials stated that the attempt was unsuccessful and no data was accessed although the agency had experienced increased activity on their cyber infrastructure.
  HHS Says DDoS Attack Failed to Cause Disruption

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1

Ways to protect yourself from DDoS Attacks:

- **Institute firewalls and antivirus protection.** Prevent your devices from becoming compromised by installing and maintaining antivirus software and firewalls on any internet connected device or system. Ensure that your network security is configured to protect against illegitimate requests.
- **Monitor your website's traffic.** Malicious cyber actors may initially launch multiple low-volume attacks on a target before initiating a larger attack. By monitoring your network traffic patterns, you may be able to detect irregularities before a serious incident occurs.
- **Create a disaster recovery plan.** A disaster recovery plan can ensure successful and efficient communication, mitigation, and recovery in the event of a DDoS attack. If you suspect that you have been the victim of a DDoS attack, it is important to contact your network administrator or provider for assistance.

To sign up to receive BusinesSafe directly to your email, visit our website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1