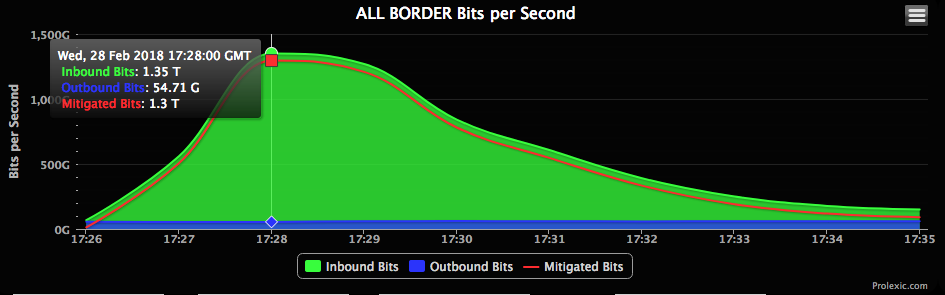
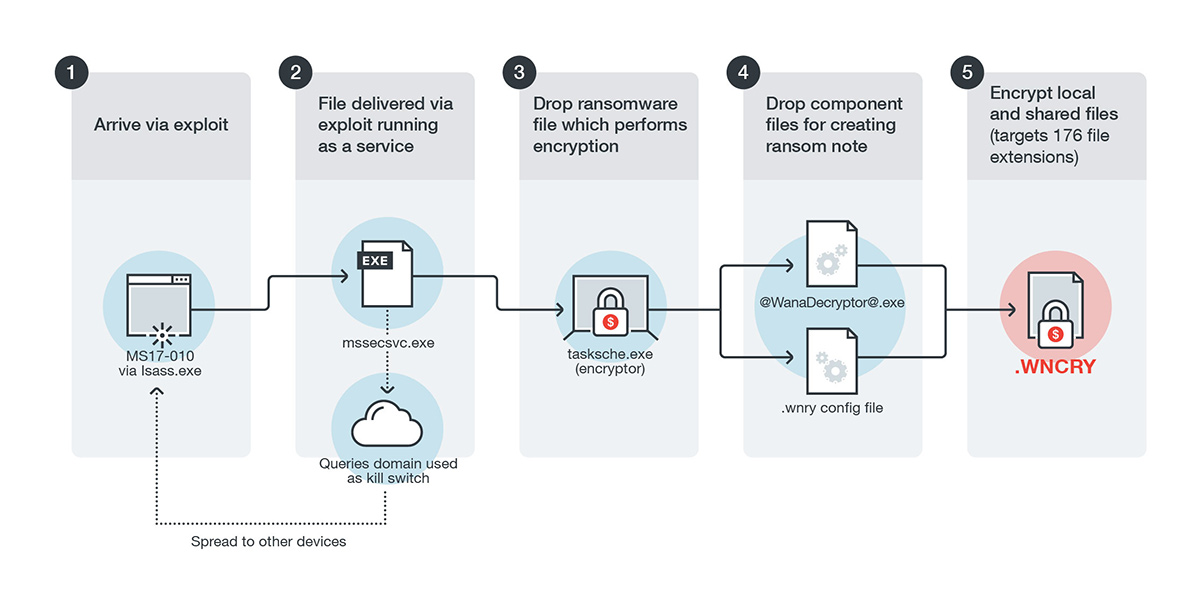
**1. Denial-of-Service (DoS) Attacks**

* **Definition:** A cyberattack that overwhelms a server, network, or system with traffic, rendering it unavailable to legitimate users.
* **Example:** In 2018, GitHub experienced a massive DoS attack with traffic peaking at 1.35 Tbps, temporarily disrupting its services.
* **Protection Measures:**
  + Use firewalls and intrusion detection systems.
  + Implement rate-limiting on network traffic.
  + Employ content delivery networks (CDNs) to absorb excess traffic.



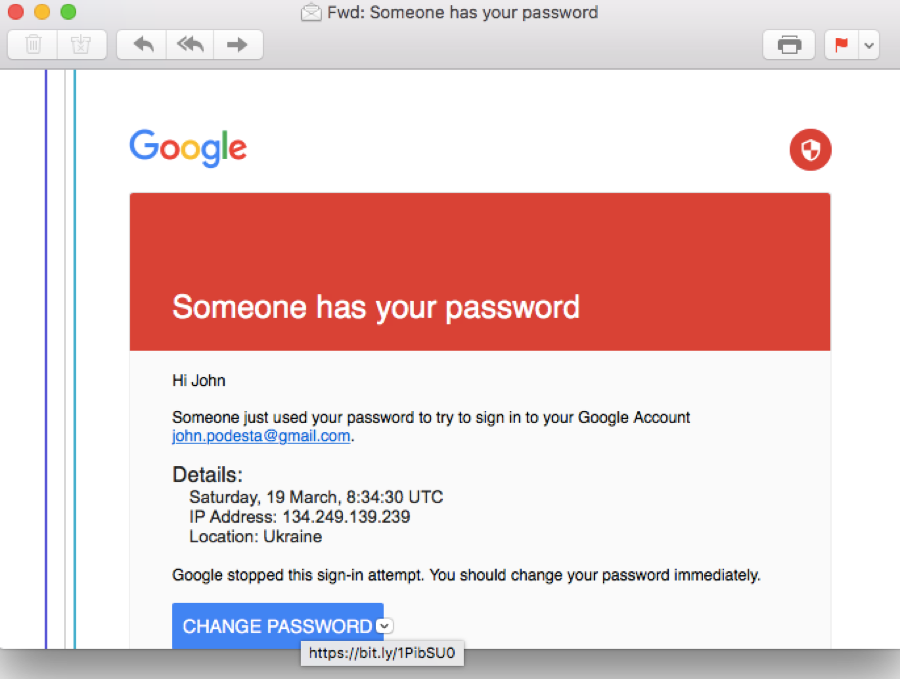
**2. Malware**

* **Definition:** Malicious software designed to harm, exploit, or otherwise compromise devices, networks, or data.
* **Example:** The WannaCry ransomware attack in 2017 affected over 200,000 systems globally, encrypting files and demanding ransom payments.
* **Protection Measures:**
  + Use up-to-date antivirus and antimalware tools.
  + Regularly update operating systems and software.
  + Train employees on recognizing and avoiding suspicious links or attachments.



**3. Phishing**

* **Definition:** A cyberattack where attackers trick users into providing sensitive information, such as passwords or credit card numbers, by pretending to be trustworthy entities.
* **Example:** In 2016, phishing emails targeted John Podesta, Hillary Clinton’s campaign chairman, leading to the compromise of his email account.
* **Protection Measures:**
  + Enable email filtering to detect phishing attempts.
  + Use multi-factor authentication (MFA) for accounts.
  + Educate users about recognizing phishing scams.



**4. Spoofing**

* **Definition:** A tactic where an attacker impersonates a trusted entity, such as a device, website, or person, to deceive victims and gain access to sensitive information.
* **Example:** In 2013, attackers spoofed the Associated Press's Twitter account, falsely reporting explosions at the White House, causing a temporary stock market drop.
* **Protection Measures:**
  + Verify the authenticity of communication sources.
  + Use email authentication protocols like SPF, DKIM, and DMARC.
  + Monitor network traffic for unusual activity.



**5. Identity-Based Attacks**

* **Definition:** Attacks where an attacker exploits stolen or fake identities to gain unauthorized access to systems or data.
* **Example:** In 2020, Twitter suffered an attack where hackers used compromised employee credentials to take over high-profile accounts, promoting a Bitcoin scam.
* **Protection Measures:**
  + Use MFA and strong password policies.
  + Regularly audit user access permissions.
  + Deploy behavior-based anomaly detection systems.

