Hack of Polish Stock Exchange and Financial System

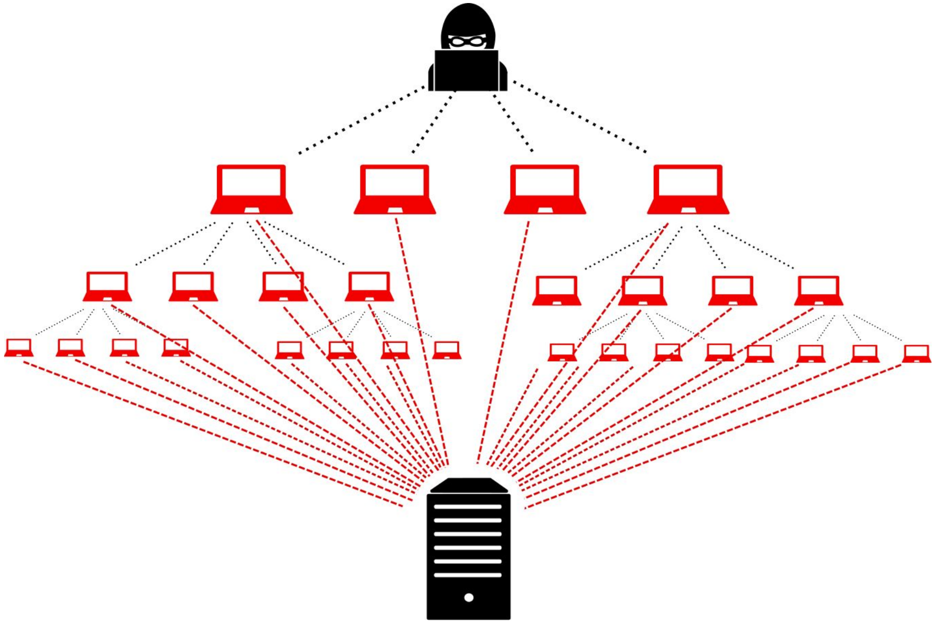
Tony Ashy and Saurabh Sharma

What happened?

- On August 28, 2023 Polish government officials claim a pro-Russian hacking group attacked their website.
- NoName claim responsibility on their Telegram channel.
- The attack was a response to an article written by a Polish columnist
- Quote from NoName, “To express our support to all adequate citizens of Poland who oppose the authorities of their country drowning in Russophobia, our DDoS rocket launchers today are aimed at Polish targets.”

History of DDoS

- 1996: the first known DDoS raid
- 2000: DDoS goes pro, hacktivism kicks in
- 2007: DDoS becomes a threat to nation-states
- 2016: DDoS via IoT botnets makes its debut
- 2018: ransom DDoS comes into existence and perseveres
- The present-day: multi-pronged attacks



Geopolitical Motives

- What is the Central/Eastern Bloc?
    - Also referred to as the Communist Bloc, Socialist Bloc and Soviet Bloc, it is a coalition of communist states of Central and Eastern Europe, East Asia, Southeast Asia, Africa, and Latin America that were friends of the Soviet Union

- The Ukraine/Russia war is described by the west as a war of democracy versus communism. A way of dividing support for the war between democratic/western countries versus all other forms of government.

How?

- The hackers use a DDoS attack to bombard the site of “Trusted Profile,” a verification services that allows the user to confirm their identity and receive a digital signature to work on government sites.
- NoName will recruit hackers on the dark web to help participate in targeted campaigns, and then compensate the hackers with cryptocurrency for their work depending on quantity of attacks and quality (The more successful the attack, the higher the payout)
- NoName has attacked the financial institutions of Ukraine, Italy, France and Switzerland.

How can this be prevented/deterred?

- Own Verification App/Traffic Thresholds - Software Solution
  - These sites are secure sites, accessed by only those with accounts or higher clearance. By implementing their own verification application and quantifying the number of users, the institutions can begin to set traffic limits as a way of defense.
- IP blocking - Software Solution
  - Somewhat common. Blocking IP’s of non-verified IP addresses would mitigate bot DDoS traffic from unverified/unauthorized IP’s
- Hardware solutions on servers utilizing advanced traffic filtering
  - Implement: geo-blocking, rate limiting, IP reputation and signature identification.

Questions?