Incident cases

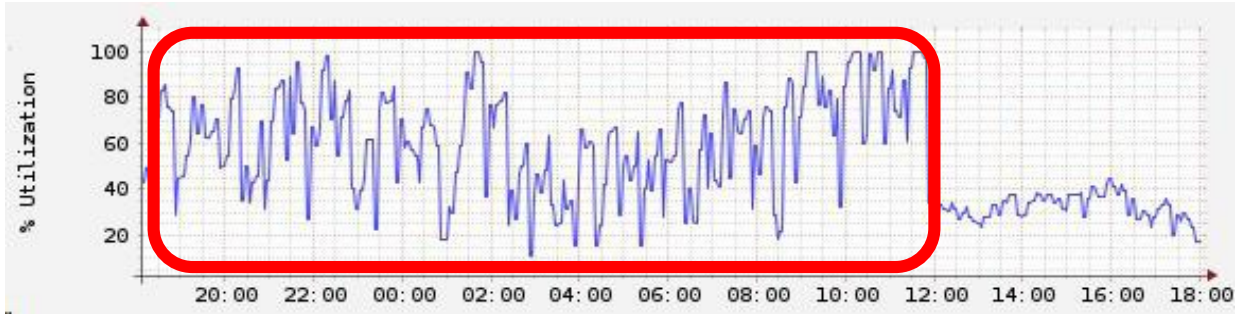
Kitisak Jirawannakool

Electronic Government Agency (EGA)

Kitisak.Jirawannakool@ega.or.th

Scenario #1

- One day, we monitor our systems and found something strange on dashboard. (we use Cacti)
  - Cacti is open-source tool for monitoring performance of servers
- Users can’t resolve domain because DNS doesn’t work properly
- Percentage of CPU utilization is high and swing quickly
- Number of concurrent sessions are normal



Investigate more

- Too many DNS requests from many sources
  - Monitor at the firewall
  - Next gen. firewall said this is “DNS ANY Queries brute force attack”
- Can’t track real attackers because of IPs were spoofed
  - Need to learn the pattern of attackers (group of IPs or country)
- Fortunately, all source IPs came from only one country (in my case)
  - Use WHOIS database
- Consumed all resources of DNS server
- DDoS attack

DNS ANY Queries brute force attack - explain

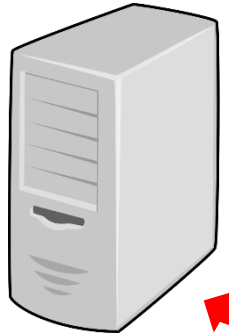
Attacker spoofed IP and sent many request with every types

www.abc.go.th, c-name, MX,A

www.abc.go.th, c-name, MX,A

www.abc.go.th, c-name, MX,A

www.abc.go.th, c-name, MX,A



DNS

No record found

www.abc.go.th

Root DNS

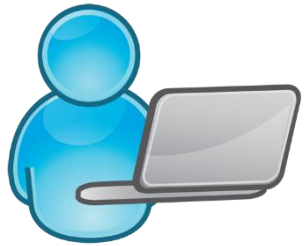
How to respond?

- Filtering based on different criteria (ex. Groups of IPs or country)
- Add Whitelist to allow only our clients be able to solve domain name (consideration about organization policy)
- In some cases, attackers send requests by using non-existent domain, we have to reject this kind of requests too

Scenario #2

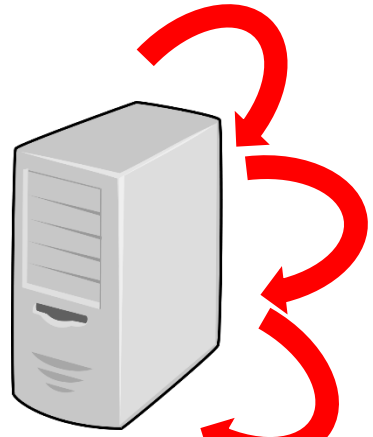
- There are several query requests from clients to outside
  - Firewall reported
- Signature of firewall said “Morto DNS request traffic”
- This action is blocked already
- More information
  - Morto is a type of internet worm and botnet
  - Send command through query requests
  - Looks like normal DNS query behavior
  - Next gen. firewall will analyze more on request contents

Morto DNS request traffic



Users got infected by Morto worm

Send command through DNS Record



C&C server (DNS)

Monitor at the Firewall

How to respond?

- If you find requests from outside
  - Possibly DNS servers are hacked and use it as C&C
  - Need to patch and improve security of DNS servers
- If you find requests to outside
  - Possibly clients got infected by malware
  - Use Anti-malware to clean
- Create the internal policy
- Work with other CERTs and find the best solutions to fight against the malware