مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

U.S. Department of Defense warns of Fast Flux Attacks, flags them as National Security Threat

Tracking #:432317040

Date:04-04-2025

Table of Contents

1 EXECUTIVE SUMMARY

In April, the U.S. Department of Defense released a Cybersecurity Advisory warning of the risks associated with Fast Flux attacks, which enable threat actors to consistently evade detection[i]. The advisory characterizes Fast Flux attacks as a threat to national security, noting that both cybercriminals and nation-state actors have been observed using this tactic to obscure the location of malicious servers by rapidly changing Domain Name System (DNS) records. This approach enhances the resilience of their operations by allowing them to create highly available command and control (C2) infrastructure, thereby concealing their subsequent malicious activities.

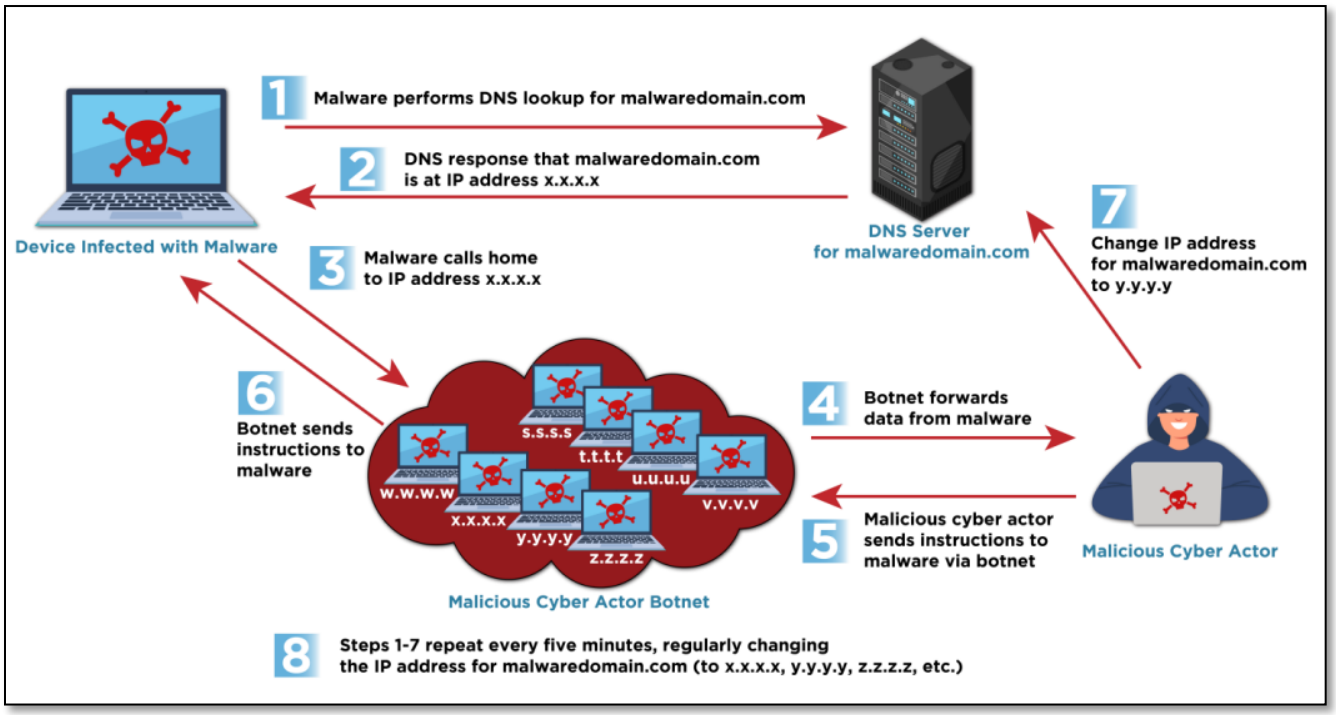
2 TECHNICAL ANALYSIS

DNS Fast Flux is a technique that rapidly swaps out the IP addresses associated with a domain, making it more difficult for cyber defenders to block malicious domains used for phishing attacks and other criminal activities such as botnet managers, fake shops, credential stealers, viruses, spam mailers etc.

The advisory highlights two main variants of fast flux to perform attacks:

1. Single flux: A single domain name is linked to numerous IP addresses, which are frequently rotated in DNS responses
2. Double flux: In addition to rapidly changing the IP addresses as in single flux, the DNS name servers responsible for resolving the domain also change frequently.

Figure 1: Single Flux Technique



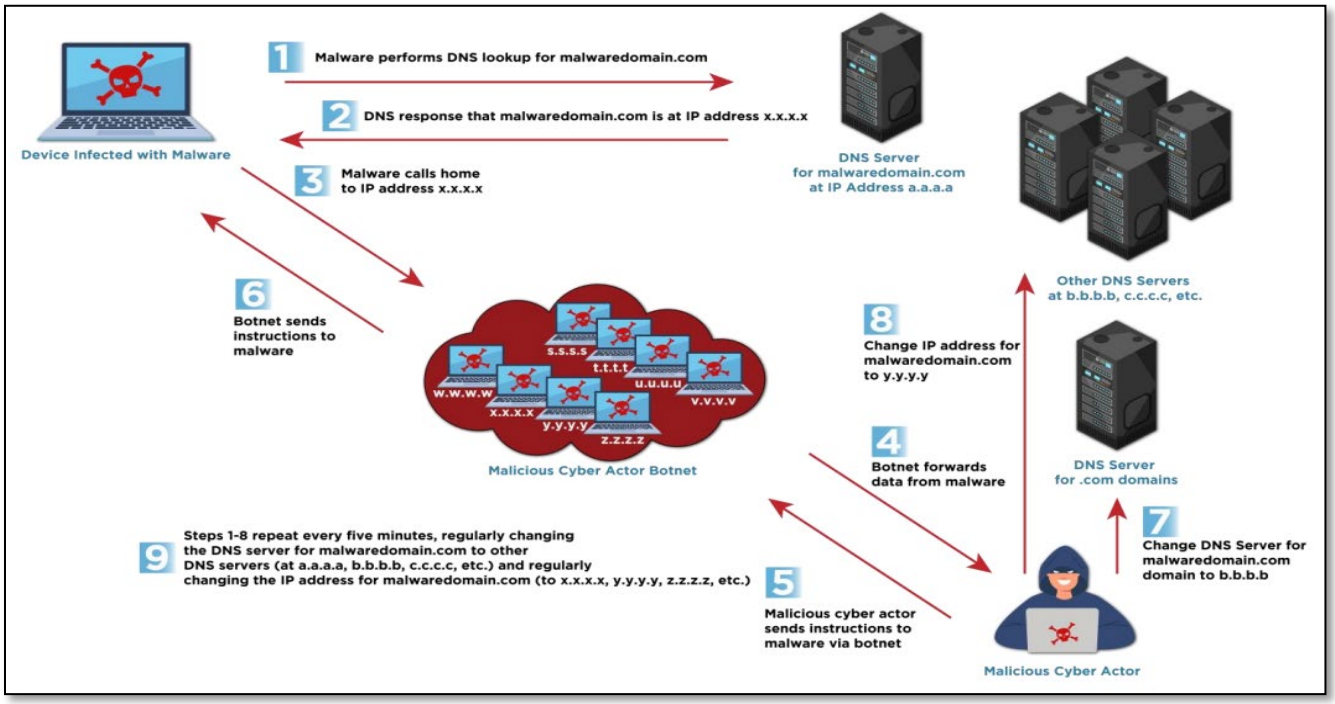


Figure 2: Double Flux Technique

Both techniques rely on wide network of compromised hosts, typically as a botnet, acting as proxies or relay points. This makes it hard for network defenders to identify and block malicious traffic or take down the malicious infrastructure. Many cyber actors use the fast flux technique to hide command and control (C2) channels and stay operational.

3. INDICATORS OF COMPROMISE

There are no related IoC's available at time of writing.

4. RECOMMENDED ACTIONS

- Block access to domains identified as using fast flux through non-routable DNS responses or firewall rules.
- Consider sinkholing the malicious domains, redirecting traffic from those domains to a controlled server to capture and analyze the traffic, helping to identify compromised hosts within the network.
- Block IP addresses known to be associated with malicious fast flux networks.
- Block traffic to and from domains or IP addresses with poor reputations, especially ones identified as participating in malicious fast flux activity.
- Increase logging and monitoring of DNS traffic and network communications to identify new or ongoing fast flux activities.
- Develop policies and procedures to manage and contain phishing incidents, particularly those facilitated by fast flux networks.

5. REFERENCES

[i] CSA-FAST-FLUX.PDF (defense.gov)