Fast Flux: A National Security Threat

Executive summary

Many networks have a gap in their defenses for detecting and blocking a malicious technique known as “fast flux.” This technique poses a significant threat to national security, enabling malicious cyber actors to consistently evade detection. Malicious cyber actors, including cybercriminals and nation-state actors, use fast flux to obfuscate the locations of malicious servers by rapidly changing Domain Name System (DNS) records. Additionally, they can create resilient, highly available command and control (C2) infrastructure, concealing their subsequent malicious operations. This resilient and fast changing infrastructure makes tracking and blocking malicious activities that use fast flux more difficult.

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), Canadian Centre for Cyber Security (CCCS), and New Zealand National Cyber Security Centre (NCSC-NZ) are releasing this joint cybersecurity advisory (CSA) to warn organizations, Internet service providers (ISPs), and cybersecurity service providers of the ongoing threat of fast flux enabled malicious activities as a defensive gap in many networks. This advisory is meant to encourage service providers, especially Protective DNS (PDNS) providers, to help mitigate this threat by taking proactive steps to develop accurate, reliable, and timely fast flux detection analytics and blocking capabilities for their customers. This CSA also provides guidance on detecting and mitigating elements of malicious fast flux by adopting a multi-layered approach that combines DNS analysis, network monitoring, and threat intelligence.

The authoring agencies recommend all stakeholders—government and providers—collaborate to develop and implement scalable solutions to close this ongoing gap in network defenses against malicious fast flux activity.

Technical details

When malicious cyber actors compromise devices and networks, the malware they use needs to "call home" to send status updates and receive further instructions. To decrease the risk of detection by network defenders, malicious cyber actors use dynamic resolution techniques, such as fast flux, so their communications are less likely to be detected as malicious and blocked.

Fast flux refers to a domain-based technique that is characterized by rapidly changing the DNS records (e.g., IP addresses) associated with a single domain [T1568.001].

Single and double flux

Malicious cyber actors use two common variants of fast flux to perform operations:

1. Single flux: A single domain name is linked to numerous IP addresses, which are frequently rotated in DNS responses. This setup ensures that if one IP address is blocked or taken down, the domain remains accessible through the other IP addresses. See Figure 1 as an example to illustrate this technique.

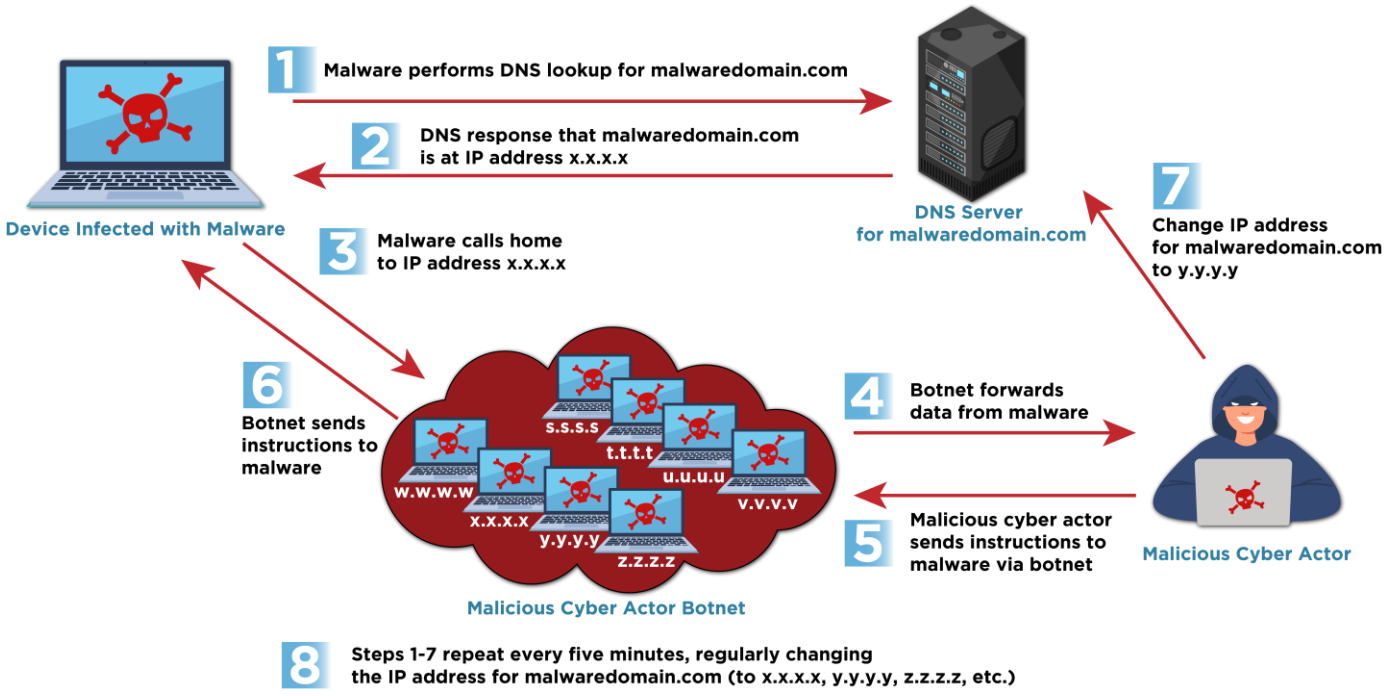

Figure 1: Single flux technique

Note: This behavior can also be used for legitimate purposes for performance reasons in dynamic hosting environments, such as in content delivery networks and load balancers.

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. This provides an additional layer of redundancy and anonymity for malicious domains. Double flux techniques have been observed using both Name Server (NS) and Canonical Name (CNAME) DNS records. See Figure 2 as an example to illustrate this technique.

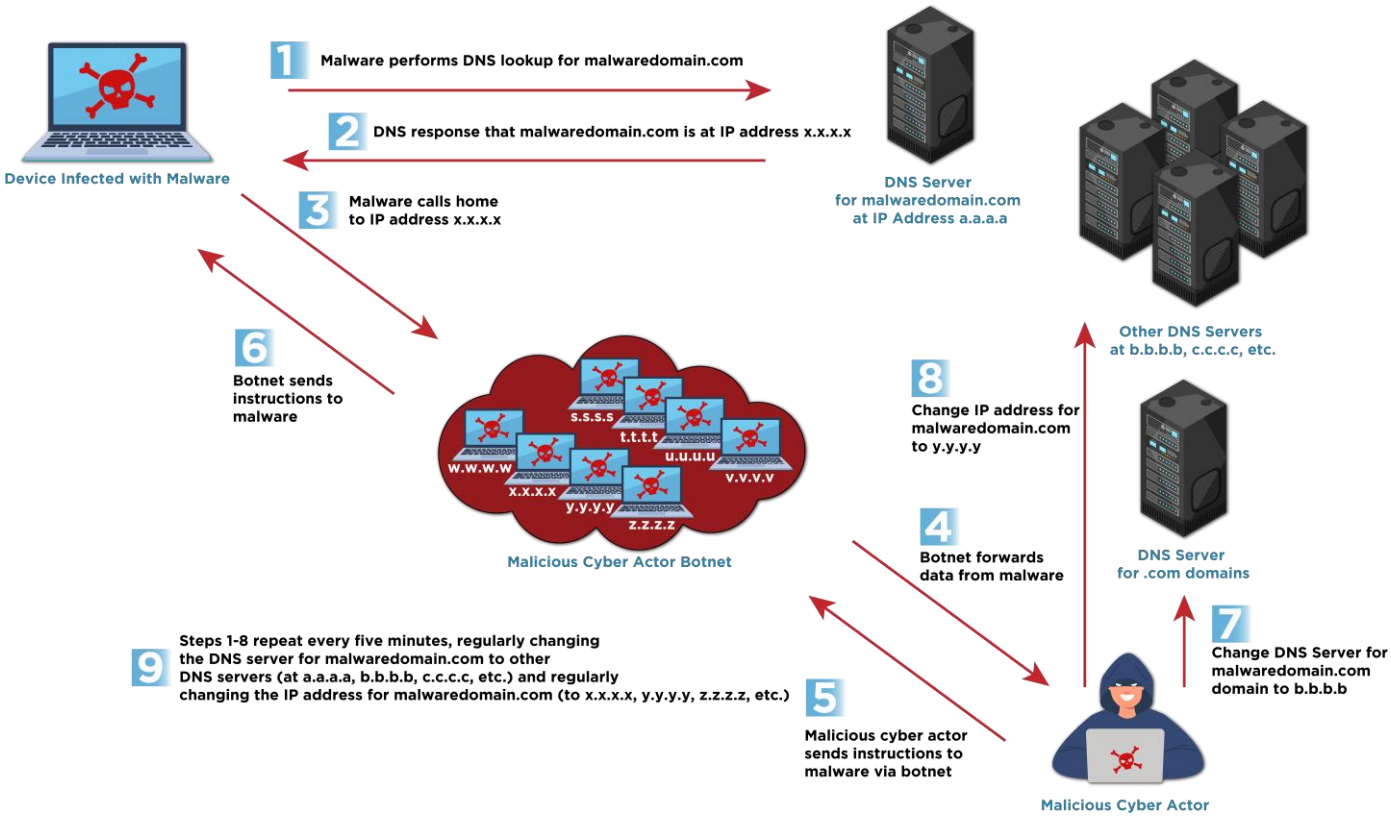

Figure 2: Double flux technique

Both techniques leverage a large number of compromised hosts, usually as a botnet from across the Internet that acts as proxies or relay points, making it difficult for network defenders to identify the malicious traffic and block or perform legal enforcement takedowns of the malicious infrastructure. Numerous malicious cyber actors have been reported using the fast flux technique to hide C2 channels and remain operational. Examples include:

- Bulletproof hosting (BPH) services offer Internet hosting that disregards or evades law enforcement requests and abuse notices. These providers host malicious content and activities while providing anonymity for malicious cyber actors. Some BPH companies also provide fast flux services, which help malicious cyber actors maintain connectivity and improve the reliability of their malicious infrastructure. [1]
    - Refer to ASD's ACSC's "Bulletproof" hosting providers: Cracks in the armour of cybercriminal infrastructure for more information on BPH providers. [2]
- Fast flux has been used in Hive and Nefilim ransomware attacks. [3], [4]
- Gamaredon uses fast flux to limit the effectiveness of IP blocking. [5], [6], [7]

The key advantages of fast flux networks for malicious cyber actors include:

- **Increased resilience.** As a fast flux network rapidly rotates through botnet devices, it is difficult for law enforcement or abuse notifications to process the changes quickly and disrupt their services.
- **Render IP blocking ineffective**. The rapid turnover of IP addresses renders IP blocking irrelevant since each IP address is no longer in use by the time it is blocked. This allows criminals to maintain resilient operations.
- **Anonymity**. Investigators face challenges in tracing malicious content back to the source through fast flux networks. This is because malicious cyber actors' C2 botnets are constantly changing the associated IP addresses throughout the investigation.

Additional malicious uses

Fast flux is not only used for maintaining C2 communications, it also can play a significant role in phishing campaigns to make social engineering websites harder to block or take down. Phishing is often the first step in a larger and more complex cyber compromise. Phishing is typically used to trick victims into revealing sensitive information (such as login passwords, credit card numbers, and personal data), but can also be used to distribute malware or exploit system vulnerabilities. Similarly, fast flux is

used for maintaining high availability for cybercriminal forums and marketplaces, making them resilient against law enforcement takedown efforts.

Some BPH providers promote fast flux as a service differentiator that increases the effectiveness of their clients' malicious activities. For example, one BPH provider posted on a dark web forum that it protects clients from being added to Spamhaus blocklists by easily enabling the fast flux capability through the service management panel (see Figure 3). A customer just needs to add a "dummy server interface," which redirects incoming queries to the host server automatically. By doing so, only the dummy server interfaces are reported for abuse and added to the Spamhaus blocklist, while the servers of the BPH customers remain "clean" and unblocked.

Figure 3: Example dark web fast flux advertisement

The BPH provider further explained that numerous malicious activities beyond C2, including botnet managers, fake shops, credential stealers, viruses, spam mailers, and others, could use fast flux to avoid identification and blocking.

As another example, a BPH provider that offers fast flux as a service advertised that it automatically updates name servers to prevent the blocking of customer domains. Additionally, this provider further promoted its use of separate pools of IP addresses for each customer, offering globally dispersed domain registrations for increased reliability.

Detection techniques

The authoring agencies recommend that ISPs and cybersecurity service providers, especially PDNS providers, implement a multi-layered approach, in coordination with customers, using the following techniques to aid in detecting fast flux activity [CISA CPG 3.A]. However, quickly detecting malicious fast flux activity and differentiating it from legitimate activity remains an ongoing challenge to developing accurate, reliable, and timely fast flux detection analytics.

1. Leverage threat intelligence feeds and reputation services to identify known fast flux domains and associated IP addresses, such as in boundary firewalls, DNS resolvers, and/or SIEM solutions.

2. Implement anomaly detection systems for DNS query logs to identify domains exhibiting high entropy or IP diversity in DNS responses and frequent IP address rotations. Fast flux domains will frequently cycle though tens or hundreds of IP addresses per day.
3. Analyze the time-to-live (TTL) values in DNS records. Fast flux domains often have unusually low TTL values. A typical fast flux domain may change its IP address every 3 to 5 minutes.
4. Review DNS resolution for inconsistent geolocation. Malicious domains associated with fast flux typically generate high volumes of traffic with inconsistent IP-geolocation information.
5. Use flow data to identify large-scale communications with numerous different IP addresses over short periods.
6. Develop fast flux detection algorithms to identify anomalous traffic patterns that deviate from usual network DNS behavior.
7. Monitor for signs of phishing activities, such as suspicious emails, websites, or links, and correlate these with fast flux activity. Fast flux may be used to rapidly spread phishing campaigns and to keep phishing websites online despite blocking attempts.
8. Implement customer transparency and share information about detected fast flux activity, ensuring to alert customers promptly after confirmed presence of malicious activity.

Mitigations

All organizations

To defend against fast flux, government and critical infrastructure organizations should coordinate with their Internet service providers, cybersecurity service providers, and/or their Protective DNS services to implement the following mitigations utilizing accurate, reliable, and timely fast flux detection analytics.

Note: Some legitimate activity, such as common content delivery network (CDN) behaviors, may look like malicious fast flux activity. Protective DNS services, service

providers, and network defenders should make reasonable efforts, such as allowlisting expected CDN services, to avoid blocking or impeding legitimate content.

1. DNS and IP blocking and sinkholing of malicious fast flux domains and IP addresses
    - 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.
2. Reputational filtering of fast flux enabled malicious activity
    - Block traffic to and from domains or IP addresses with poor reputations, especially ones identified as participating in malicious fast flux activity.
3. Enhanced monitoring and logging
    - Increase logging and monitoring of DNS traffic and network communications to identify new or ongoing fast flux activities.
    - Implement automated alerting mechanisms to respond swiftly to detected fast flux patterns.
    - Refer to ASD's ACSC joint publication, Best practices for event logging and threat detection, for further logging recommendations.
4. Collaborative defense and information sharing
    - Share detected fast flux indicators (e.g., domains, IP addresses) with trusted partners and threat intelligence communities to enhance collective defense efforts. Examples of indicator sharing initiatives include CISA's Automated Indicator Sharing or sector-based Information Sharing and Analysis Centers (ISACs) and ASD's Cyber Threat Intelligence Sharing Platform (CTIS) in Australia.

- Participate in public and private information-sharing programs to stay informed about emerging fast flux tactics, techniques, and procedures (TTPs). Regular collaboration is particularly important because most malicious activity by these domains occurs within just a few days of their initial use; therefore, early discovery and information sharing by the cybersecurity community is crucial to minimizing such malicious activity. [8]

5. Phishing awareness and training

    - Implement employee awareness and training programs to help personnel identify and respond appropriately to phishing attempts.
    - Develop policies and procedures to manage and contain phishing incidents, particularly those facilitated by fast flux networks.
    - For more information on mitigating phishing, see joint Phishing Guidance: Stopping the Attack Cycle at Phase One.

Network defenders

The authoring agencies encourage organizations to use cybersecurity and PDNS services that detect and block fast flux. By leveraging providers that detect fast flux and implement capabilities for DNS and IP blocking, sinkholing, reputational filtering, enhanced monitoring, logging, and collaborative defense of malicious fast flux domains and IP addresses, organizations can mitigate many risks associated with fast flux and maintain a more secure environment.

However, some PDNS providers may not detect and block malicious fast flux activities. Organizations should not assume that their PDNS providers block malicious fast flux activity automatically, and should contact their PDNS providers to validate coverage of this specific cyber threat.

For more information on PDNS services, see the 2021 joint cybersecurity information sheet from NSA and CISA about Selecting a Protective DNS Service. [9] In addition, NSA offers no-cost cybersecurity services to Defense Industrial Base (DIB) companies, including a PDNS service. For more information, see NSA's DIB Cybersecurity Services and factsheet. CISA also offers a Protective DNS service for federal civilian executive

branch (FCEB) agencies. See CISA's Protective Domain Name System Resolver page and factsheet for more information.

Conclusion

Fast flux represents a persistent threat to network security, leveraging rapidly changing infrastructure to obfuscate malicious activity. By implementing robust detection and mitigation strategies, organizations can significantly reduce their risk of compromise by fast flux-enabled threats.

The authoring agencies strongly recommend organizations engage their cybersecurity providers on developing a multi-layered approach to detect and mitigate malicious fast flux operations. Utilizing services that detect and block fast flux enabled malicious cyber activity can significantly bolster an organization's cyber defenses.

Works cited

[1] Intel471. Bulletproof Hosting: A Critical Cybercriminal Service. 2024. https://intel471.com/blog/bulletproof-hosting-a-critical-cybercriminal-service

[2] Australian Signals Directorate's Australian Cyber Security Centre. "Bulletproof" hosting providers: Cracks in the armour of cybercriminal infrastructure. 2025. https://www.cyber.gov.au/about-us/view-all-content/publications/bulletproof-hosting-providers

[3] Logpoint. A Comprehensive guide to Detect Ransomware. 2023. https://www.logpoint.com/wp-content/uploads/2023/04/logpoint-a-comprehensive-guide-to-detect-ransomware.pdf

[4] Trendmicro. Modern Ransomware's Double Extortion Tactic's and How to Protect Enterprises Against Them. 2021. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them

[5] Unit 42. Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine. 2022. https://unit42.paloaltonetworks.com/trident-ursa/

[6] Recorded Future. BlueAlpha Abuses Cloudflare Tunneling Service for GammaDrop Staging Infrastructure. 2024. https://www.recordedfuture.com/research/bluealpha-abuses-cloudflare-tunneling-service

[7] Silent Push. 'From Russia with a 71': Uncovering Gamaredon's fast flux infrastructure. New apex domains and ASN/IP diversity patterns discovered. 2023. https://www.silentpush.com/blog/from-russia-with-a-71/

[8] DNS Filter. Security Categories You Should be Blocking (But Probably Aren't). 2023. https://www.dnsfilter.com/blog/security-categories-you-should-be-blocking-but-probably-arent

[9] National Security Agency. Selecting a Protective DNS Service. 2021. https://media.defense.gov/2025/Mar/24/2003675043/-1/-1/0/CSI-SELECTING-A-PROTECTIVE-DNS-SERVICE-V1.3.PDF

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring cybersecurity agencies' missions, including their responsibilities to identify and disseminate threats, and develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

National Security Agency (NSA):

- Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
- Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
- Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov

Cybersecurity and Infrastructure Security Agency (CISA):
All organizations should report incidents and anomalous activity to CISA via the agency's Incident Reporting System, its 24/7 Operations Center at report@cisa.gov, or by calling 1-844-Say-CISA (1-844-729-2472). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment user for the activity; the name of the submitting company or organization; and a designated point of contact.

Federal Bureau of Investigation (FBI):
To report suspicious or criminal activity related to information found in this advisory, contact your local FBI field office or the FBI's Internet Crime Complaint Center (IC3). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC):
For inquiries, visit ASD's website at www.cyber.gov.au or call the Australian Cyber Security Hotline at 1300 CYBER1 (1300 292 371).

Canadian Centre for Cyber Security (CCCS):
CCCS supports Canadian organizations. Visit www.cyber.gc.ca for publications and guidance or contact CCCS via 1-833-CYBER-88 or email contact@cyber.gc.ca.

New Zealand National Cyber Security Centre (NCSC-NZ):
The NCSC-NZ assists New Zealand organizations. Visit www.ncsc.govt.nz for guidance and resources, or email NCSC-NZ at info@ncsc.govt.nz.