Akamai

[state of the internet] / security

Attack Superhighway

A Deep Dive on Malicious DNS Traffic

Threats against enterprises

10%-16%

of organizations encounter command and control (C2) traffic in their network in any given quarter

36%

of affected devices exhibited traffic leading to threats targeting backups and internal data stored in network-attached storage devices

26%

of affected devices exhibited traffic associated with initial access brokers, which often play a role in facilitating ransomware attacks

Types of attack methodology found in organizations

Organizations see many types of threats to their networks, and not all are created equal. We're able to identify different attacker groups through the indicators of compromise associated with those groups. This gives us an understanding of the methodologies and goals associated with the malicious traffic.

Initial access brokers
IABs focus mainly on providing an initial entry point for other cybercriminals, including ransomware groups, to gain a foothold in organizations' networks.

Botnets
Attackers can use botnets for myriad purposes — from cryptomining and DDoS attacks to data exfiltration, malware deployment, and lateral movement.

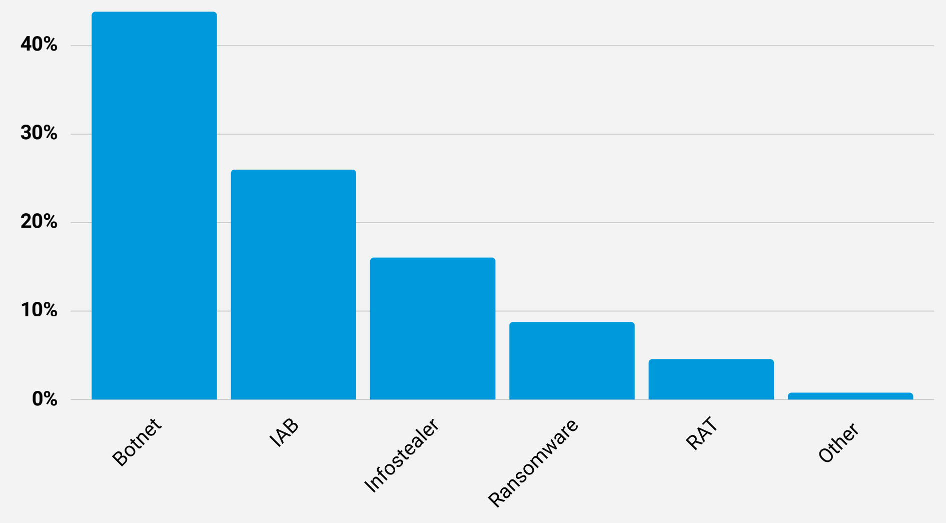
Ransomware as a service groups
These are groups that allow other attackers (even those without technical expertise) to become an affiliate and use their ransomware software for a fee.

Information stealers
Infostealers gather various types of data like usernames, passwords, system information, banking credentials, cookies, and so forth.

Remote access tools
RATs provide many use cases for cybercriminals, including reconnaissance, privilege escalation, lateral movement through the network, establishing persistence, remote payload execution after intrusion, and data exfiltration.

Percentage of Devices Per Threat Category

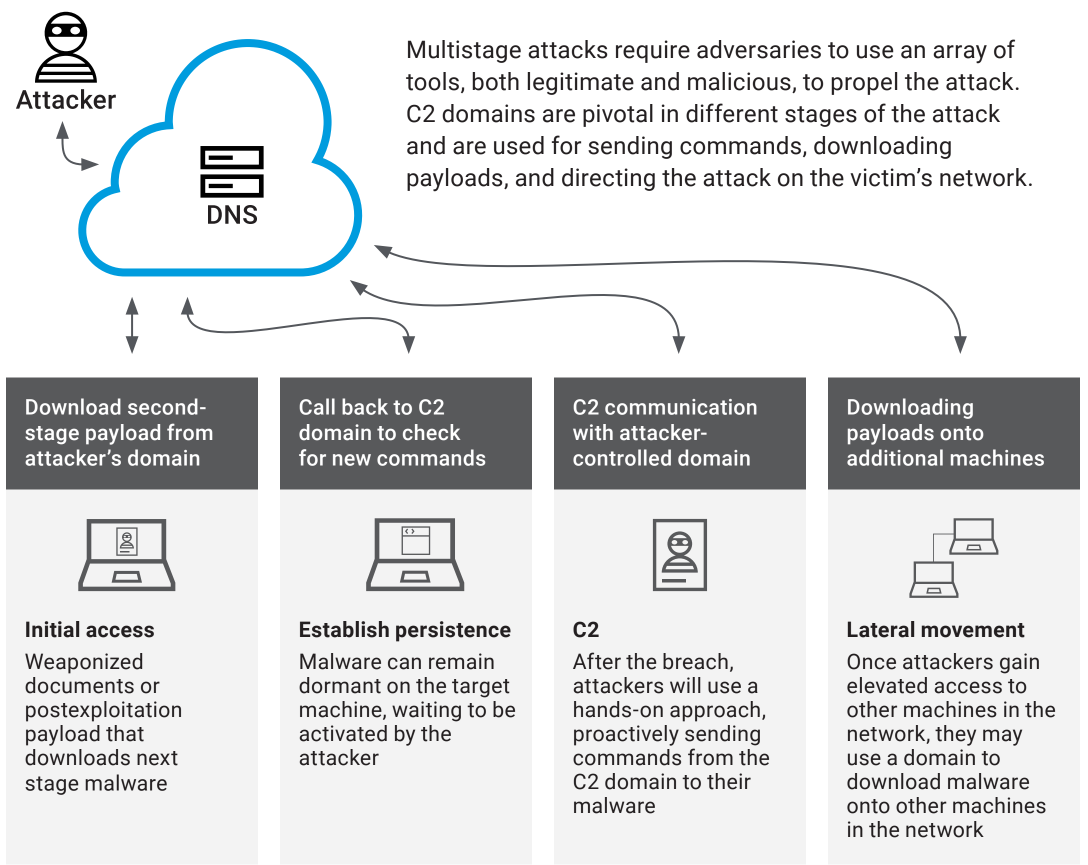
January 1, 2022 – December 31, 2022



Enterprises are predominantly targeted by botnets, IABs, and infostealers.
Each threat represents a risk to an organization's security and confidential data.

The role of DNS in a multistage attack

Multistage attacks require adversaries to use an array of tools, both legitimate and malicious, to propel the attack. C2 domains are pivotal in different stages of the attack and are used for sending commands, downloading payloads, and directing the attack on the victim's network.



Download second-stage payload from attacker's domain

Initial access
Weaponized documents or postexploitation payload that downloads next stage malware

Call back to C2 domain to check for new commands

Establish persistence
Malware can remain dormant on the target machine, waiting to be activated by the attacker

C2 communication with attacker-controlled domain

C2
After the breach, attackers will use a hands-on approach, proactively sending commands from the C2 domain to their malware

Downloading payloads onto additional machines

Lateral movement
Once attackers gain elevated access to other machines in the network, they may use a domain to download malware onto other machines in the network

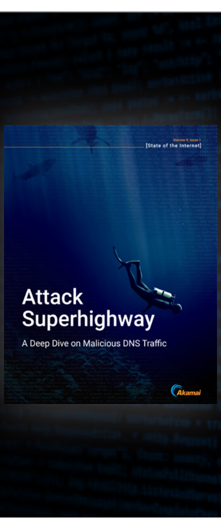
Attacks against home users

216M malicious queries related to Android malware FluBot. It spreads via SMS, enticing users to click a malicious link; this threat is capable of stealing banking credentials.

156M malicious queries related to Mirai, an IoT botnet; infected user devices are used to launch wide-scale disruption against high-profile targets

367M malicious queries related to Pykspa, a malware that spreads via Skype messenger

80M malicious queries related to Necurs, a botnet that deploys other malware like ransomware



To learn more about malicious DNS traffic of both enterprise and home users and more, download the report

Download the full report

| Support | Published 03/23