Health-ISAC™
Collaborating for Resilience in Healthcare

# THREAT BULLETINS

## Joint Cybersecurity Advisory: Identification and Disruption of QakBot Infrastructure

○○○ TLP:WHITE

Aug 30, 2023

On August 30, 2023, the United States Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA) to disseminate QakBot infrastructure indicators of compromise (IOCs) identified in FBI investigations as of August 2023.

On August 25, the FBI, in coordination with international partners, executed a coordinated operation to disrupt QakBot infrastructure worldwide. Disruption operations targeting QakBot infrastructure resulted in the botnet takeover, which severed the connection between victim computers and QakBot command and control (C2) servers. The FBI is working closely with industry partners to share information about the malware to maximize detection, remediation, and prevention measures for network defenders.

All members are encouraged to review AA23-242A Identification and Disruption of Qakbot Infrastructure. CISA and FBI encourage organizations to implement the recommendations in the Mitigations section to reduce the likelihood of QakBot-related activity and promote the identification of QakBotfacilitated ransomware and malware infections. Additionally, if a potential compromise is detected, administrators should apply the incident response recommendations and report key findings to a local FBI Field Office or CISA.

The indicators of compromise contained within the CSA have been entered into the H-ISAC WHITE feed of Health-ISAC's automated sharing platform for those members ingesting automated threat indicators.

QakBot—also known as Qbot, Quackbot, Pinkslipbot, and TA570—is responsible for thousands of malware infections globally. QakBot has been the precursor to a significant amount of computer intrusions, to include ransomware and the compromise of user accounts within the Financial Sector. In existence since at least 2008, QakBot feeds into the global cybercriminal supply chain and has deep-rooted connections to the criminal ecosystem. QakBot was originally used as a banking trojan to steal banking credentials for account compromise; in most cases, it was delivered via phishing campaigns containing malicious attachments or links to download the malware, which would reside in memory once on the victim network.

Since its initial inception as a banking trojan, QakBot has evolved into a multi-purpose botnet and malware variant that provides threat actors with a wide range of capabilities, to include performing reconnaissance, engaging in lateral movement, gathering and exfiltrating data, and delivering other malicious payloads, including ransomware, on affected devices. QakBot has maintained persistence in the digital environment because of its modular nature. Access to QakBot-affected (victim) devices via compromised credentials are often sold to further the goals of the threat actor who delivered QakBot.QakBot and affiliated variants have targeted the United States and other global infrastructures, including the Financial Services, Emergency Services, and Commercial Facilities Sectors, and the Election Infrastructure Subsector. FBI and CISA encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood of QakBot-related infections and promote identification of QakBot-induced ransomware and malware infections. Disruption of the QakBot botnet does not mitigate other previously installed malware or ransomware on victim computers. If a potential compromise is detected, administrators should apply the incident response recommendations included in this CSA and report key findings to CISA and FBI.

### QakBot Infrastructure

QakBot’s modular structure allows for various malicious features, including process and web injection, victim network enumeration and credential stealing, and the delivery of follow-on payloads such as Cobalt Strike, Brute Ratel, and other malware. QakBot infections are particularly known to precede the deployment of human-operated ransomware, including Conti, ProLock, Egregor, REvil, MegaCortex, Black Basta, Royal, and PwndLocker.

Historically, QakBot's C2 infrastructure relied heavily on using hosting providers for its own infrastructure and malicious activity. These providers lease servers to malicious threat actors, ignore abuse complaints, and do not cooperate with law enforcement. At any given time, thousands of victim computers running Microsoft Windows were infected with QakBot—the botnet was controlled through three tiers of C2 servers.

The first tier of C2 servers includes a subset of thousands of bots selected by QakBot administrators, which are promoted to Tier 1 "supernodes" by downloading an additional software module. These supernodes communicate with the victim computers to relay commands and communications between the upstream C2 servers and the infected computers. As of mid-June 2023, 853 supernodes have been identified in 63 countries, which were active that same month. Supernodes have been observed frequently changing, which assists QakBot in evading detection by network defenders. Each bot has been observed communicating with a set of Tier 1 supernodes to relay communications to the Tier 2 C2 servers, serving as proxies to conceal the main C2 server. The Tier 3 server controls all of the bots.

## Indicators of Compromise

FBI has observed the following threat actor tactics, techniques, and procedures (TTPs) in association with OakBot infections:

- QakBot sets up persistence via the Registry Run Key as needed. It will delete this key when running and set it back up before computer restart: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<random_string>
- QakBot will also write its binary back to disk to maintain persistence in the following folder: C:\Users\<user>\AppData\Roaming\Microsoft\<random_string>\
- QakBot will write an encrypted registry configuration detailing information about the bot to the following registry key: HKEY_CURRENT_USER\Software\Microsoft\<random_string>

The IP addresses in this report were assessed to have obtained access to victim computers. Organizations are encouraged to review any connections with these IP addresses, which could potentially indicate a QakBot and/or follow-on malware infection.

The IP addresses are assessed to be inactive as of August 29, 2023. Several of these observed IP addresses were first observed as early as 2020, although most date from 2022 or 2023, and have been historically linked to QakBot. FBI and CISA recommend these IP addresses be investigated or vetted by organizations prior to taking action, such as blocking.

## MITRE ATT&CK TECHNIQUES

For detailed associated software descriptions, tactics used, and groups that have been observed using this software, see MITRE ATT&CK's page on QakBot, available here.

## Mitigations

For situational awareness, the following SHA-256 hash is associated with FBI's QakBot uninstaller:
7cdee5a583eacf24b1f142413aabb4e556ccf4ef3a4764ad084c1526cc90e117

### *Best Practice Mitigation Recommendations*

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- Require all accounts with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with NIST's standards when developing and managing password policies. This includes:
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length;
    - Store passwords in hashed format using industry-recognized password managers;
    - Add password user "salts" to shared login credentials;
    - Avoid reusing passwords;
    - Implement multiple failed login attempt account lockouts;
    - Disable password "hints";
    - Refrain from requiring password changes more frequently than once per year.
    - Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
    - Require administrator credentials to install software.
- Use phishing-resistant multi-factor authentication (MFA) (e.g., security tokens) for remote access and access to any sensitive data repositories. Implement phishing-resistant MFA for as many services as possible—particularly for webmail and VPNs—for accounts that access critical systems and privileged accounts that manage backups. MFA should also be used for remote logins.

For additional guidance on secure MFA configurations, visit cisa.gov/MFA and CISA's Implementing Phishing-Resistant MFA Factsheet.

- Keep all operating systems, software, and firmware up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities of internet-facing systems. CISA offers a range of services at no cost, including scanning and testing to help organizations reduce exposure to threats via mitigating attack vectors. Specifically, Cyber Hygiene services can help provide a second-set of eyes on organizations' internet-accessible assets. Organizations can email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services" to get started.
- Segment networks to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks to restrict adversary lateral movement.
- Identify, detect, and investigate abnormal activity and potential traversal of the indicated malware with a networking monitoring tool. To aid in detecting the malware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- Install, regularly update, and enable real time detection for antivirus software on all hosts.
- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.
- Audit user accounts with administrative privileges and configure access controls according to the principle of least privilege.
- Disable unused ports
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Implement time-based access for accounts set at the admin level and higher. For example, the Just-in-Time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- Disable command-line and scripting activities and permissions. Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- Perform regular secure system backups and create known good copies of all device configurations for repairs and/or restoration. Store copies off-network in physically secure locations and test regularly.

- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization’s data infrastructure.

| | |
|---|---|
| **Reference(s)** | CISA |
| **Report Source(s)** | CISA, FBI |

**Threat Indicator(s)**

IP(s):

89[.]163[.]212[.]111
46[.]151[.]30[.]109
188[.]127[.]242[.]178
193[.]29[.]187[.]41
94[.]198[.]51[.]202
95[.]211[.]172[.]7
95[.]211[.]172[.]86
94[.]198[.]50[.]147
94[.]198[.]50[.]210
188[.]127[.]243[.]147
62[.]141[.]42[.]36
95[.]211[.]172[.]109
94[.]103[.]85[.]86
188[.]127[.]243[.]130
188[.]127[.]243[.]133
95[.]211[.]250[.]98
95[.]211[.]250[.]117
51[.]195[.]49[.]228
51[.]38[.]62[.]182
188[.]127[.]243[.]145
188[.]127[.]243[.]148
94[.]198[.]53[.]17
193[.]29[.]187[.]57
95[.]211[.]95[.]14
185[.]4[.]67[.]6

188[.]127[.]242[.]119
95[.]211[.]198[.]177
193[.]201[.]9[.]93
95[.]211[.]250[.]97
87[.]117[.]247[.]41
51[.]161[.]202[.]232
95[.]211[.]172[.]108
45[.]84[.]224[.]23
85[.]14[.]243[.]111
185[.]81[.]114[.]188
51[.]38[.]62[.]181
95[.]211[.]172[.]6
188[.]241[.]58[.]140
23[.]236[.]181[.]102
188[.]127[.]243[.]193
190[.]2[.]143[.]38

**Alert ID** f685613e

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

**View Alert**

**Tags** QakBot

**TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**