QakBot, Software S0650 | MITRE ATT&CK®

Archived: 2026-04-05 13:17:46 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

QakBot has the ability to use HTTP and HTTPS in communication with C2 servers.[5][6][3]

Enterprise T1010 Application Window Discovery

QakBot has the ability to enumerate windows on a compromised host.[4]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

QakBot can maintain persistence by creating an auto-run Registry key.[5][6][1][7]

Enterprise T1185 Browser Session Hijacking

QakBot can use advanced web injects to steal web banking credentials.[8][3]

Enterprise T1110 Brute Force

QakBot can conduct brute force attacks to capture credentials.[9][6][3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

QakBot can use PowerShell to download and execute payloads.[7]

.003 Command and Scripting Interpreter: Windows Command Shell

QakBot can use cmd.exe to launch itself and to execute multiple C2 commands.[6][4][3][10]

.005 Command and Scripting Interpreter: Visual Basic

QakBot can use VBS to download and execute malicious files.[5]
[9][6][1][8][7][10]

.007 Command and Scripting Interpreter: JavaScript

The QakBot web inject module can inject Java Script into web banking pages visited by the victim.[3][10]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

QakBot can remotely create a temporary service on a target host.[11]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

QakBot has collected usernames and passwords from Firefox and Chrome.[3]

Enterprise T1132 .001 Data Encoding: Standard Encoding

QakBot can Base64 encode system information sent to C2.[6][3]

Enterprise T1005 Data from Local System

QakBot can use a variety of commands, including esentutl.exe to steal sensitive data from Internet Explorer and Microsoft Edge, to acquire information that is subsequently exfiltrated.[2][3]

Enterprise T1074 .001 Data Staged: Local Data Staging

QakBot has stored stolen emails and other data into new folders prior to exfiltration.[9]

Enterprise T1140 Deobfuscate/Decode Files or Information

QakBot can deobfuscate and re-assemble code strings for execution.[8][4][3]

Enterprise T1482 Domain Trust Discovery

QakBot can run `nltest /domain_trusts /all_trusts` for domain trust discovery.[3]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

QakBot can use domain generation algorithms in C2 communication.[5]

Enterprise T1114 .001 Email Collection: Local Email Collection

QakBot can target and steal locally stored emails to support thread hijacking phishing campaigns.[9][1][3]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

QakBot can RC4 encrypt strings in C2 communication.[3]

Enterprise T1041 Exfiltration Over C2 Channel

QakBot can send stolen information to C2 nodes including passwords, accounts, and emails.[3]

Enterprise T1210 Exploitation of Remote Services

QakBot can move laterally using worm-like functionality through exploitation of SMB.[6]

Enterprise T1083 File and Directory Discovery

QakBot can identify whether it has been run previously on a host by checking for a specified folder.[4]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

QakBot has placed its payload in hidden subdirectories.[10]

Enterprise T1574 .001 Hijack Execution Flow: DLL

QakBot has the ability to use DLL side-loading for execution.[12]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

QakBot has the ability to modify the Registry to add its binaries to the Windows Defender exclusion list.[7]

Enterprise T1070 .004 Indicator Removal: File Deletion

QakBot can delete folders and files including overwriting its executable with legitimate programs.[9][6][4][7]

Enterprise T1105 Ingress Tool Transfer

QakBot has the ability to download additional components and malware.[5][6][1][8][3][7]

Enterprise T1056 .001 Input Capture: Keylogging

QakBot can capture keystrokes on a compromised host.[9][1][3]

Enterprise T1036 .008 Masquerading: Masquerade File Type

The QakBot payload has been disguised as a PNG file and hidden within LNK files using a Microsoft File Explorer icon.[7][10]

Enterprise T1112 Modify Registry

QakBot can modify the Registry to store its configuration information in a randomly named subkey under `HKCU\Software\Microsoft`.[2][7]

Enterprise T1106 Native API

QakBot can use `GetProcAddress` to help delete malicious strings from memory.[4]

Enterprise T1135 Network Share Discovery

QakBot can use `net share` to identify network shares for use in lateral movement.[5][3]

Enterprise T1095 Non-Application Layer Protocol

QakBot has the ability use TCP to send or receive C2 packets.[3]

Enterprise T1027 Obfuscated Files or Information

QakBot has hidden code within Excel spreadsheets by turning the font color to white and splitting it across multiple cells.[8]

.001 Binary Padding

QakBot can use large file sizes to evade detection.[5][7]

.002 Software Packing

QakBot can encrypt and pack malicious payloads.[8]

.005 Indicator Removal from Tools

QakBot can make small changes to itself in order to change its checksum and hash value.[6][8]

.006 HTML Smuggling

QakBot has been delivered in ZIP files via HTML smuggling.[10][12]

.010 Command Obfuscation

QakBot can use obfuscated and encoded scripts.[8][10]

.011 Fileless Storage

QakBot can store its configuration information in a randomly named subkey under `HKCU\Software\Microsoft`.[2][7]

Enterprise T1120 Peripheral Device Discovery

QakBot can identify peripheral devices on targeted systems.[5]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

QakBot can use `net localgroup` to enable discovery of local groups.[3][10]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

QakBot has spread through emails with malicious attachments.[5][9][1][8][4][3][7][12][13]

.002 Phishing: Spearphishing Link

QakBot has spread through emails with malicious links.[5][9][1][4][3][7][10]

Enterprise T1057 Process Discovery

QakBot has the ability to check running processes.[4]

Enterprise T1055 Process Injection

QakBot can inject itself into processes including explore.exe, Iexplore.exe, Mobsync.exe., and wermgr.exe.[5][9][1][3][10]

.012 Process Hollowing

QakBot can use process hollowing to execute its main payload.[4]

Enterprise T1572 Protocol Tunneling

The QakBot proxy module can encapsulate SOCKS5 protocol within its own proxy protocol.[3]

Enterprise T1090 .002 Proxy: External Proxy

QakBot has a module that can proxy C2 communications.[3]

Enterprise T1018 Remote System Discovery

QakBot can identify remote systems through the `net view` command.[6][3][10]

Enterprise T1091 Replication Through Removable Media

QakBot has the ability to use removable drives to spread through compromised networks.[5]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

QakBot has the ability to create scheduled tasks for persistence.[5][9][6][1][2][8][3][7]

Enterprise T1518 Software Discovery

QakBot can enumerate a list of installed programs.[7]

.001 Security Software Discovery

QakBot can identify the installed antivirus product on a targeted system.[6][4][4][3]

Enterprise T1539 Steal Web Session Cookie

QakBot has the ability to capture web session cookies.[9][3]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

QakBot can use signed loaders to evade detection.[4][12]

.005 Subvert Trust Controls: Mark-of-the-Web Bypass

QakBot has been packaged in ISO files in order to bypass Mark of the Web (MOTW) security measures.[10]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

QakBot can use MSIExec to spawn multiple cmd.exe processes.[6]

.010 System Binary Proxy Execution: Regsvr32

QakBot can use Regsvr32 to execute malicious DLLs.[2][8][4][10][11][12]

.011 System Binary Proxy Execution: Rundll32

QakBot has used Rundll32.exe to drop malicious DLLs including Brute Ratel C4 and to enable C2 communication.[6][2][8][4][10]

Enterprise T1082 System Information Discovery

QakBot can collect system information including the OS version and domain on a compromised host.[6][4][7][13]

Enterprise T1016 System Network Configuration Discovery

QakBot can use `net config workstation`, `arp -a`, `nslookup`, and `ipconfig /all` to gather network configuration information.[6][3][7][10][13]

.001 Internet Connection Discovery

QakBot can measure the download speed on a targeted host.[3]

Enterprise T1049 System Network Connections Discovery

QakBot can use `netstat` to enumerate current network connections.[3][10]

Enterprise T1033 System Owner/User Discovery

QakBot can identify the user name on a compromised system.[3][10]

Enterprise T1124 System Time Discovery

QakBot can identify the system time on a targeted host.[3]

Enterprise T1204 .001 User Execution: Malicious Link

QakBot has gained execution through users opening malicious links.[5][9][1][4][3][7][10]

.002 User Execution: Malicious File

QakBot has gained execution through users opening malicious attachments.[5][9][6][1][8][4][3][7][12][13]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

QakBot can check the compromised host for the presence of multiple executables associated with analysis tools and halt execution if any are found.[5][4]

.003 Virtualization/Sandbox Evasion: Time Based Checks

The QakBot dropper can delay dropping the payload to evade detection.[8][3]

Enterprise T1047 Windows Management Instrumentation

QakBot can execute WMI queries to gather information.[3]

Source: https://attack.mitre.org/software/S0650