Co-Authored by:

China-Linked Hacking Group QTFY Targets Military and Critical Infrastructure with Malicious Distributed Systems

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact the FBI's Internet Crime Complaint Center (IC3), and/or your local FBI field office. 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. For NSA-client requirements or cybersecurity inquiries, contact CybersecurityReports@nsa.gov.

This document is distributed as TLP:CLEAR. Recipients may only share this information without restriction. Information is subject to standard copyright rules.For more information on the Traffic Light Protocol, see Traffic Light Protocol (TLP) Definitions and Usage.

Publication: September 2, 2026

Federal Bureau of Investigation | National Security Agency | Cyber National Mission Force

Advisory at a Glance

Title	China-Linked Hacking Group QTFY Targets Military and Critical Infrastructure with Malicious Distributed Systems
Original Publication	August 26, 2026
Last Update	September 2, 2026
Executive Summary	The Federal Bureau of Investigation, National Security Agency, and Cyber National Mission Force are releasing this joint cybersecurity advisory to alert organizations concerning China-linked cyber threat actors, who use the acronyms QTFY, QT, and QTCYBER for themselves and their tools and have developed malicious distributed platforms to compromise the networks of US and foreign organizations. The cyber actors' products have enabled hackers to obfuscate their location and target systems in critical infrastructure sectors including defense industrial base (DIB), communications, government, and higher education. This advisory provides details on the actors' activities; tactics, techniques, and procedures (TTPs); infrastructure details; and indicators of compromise (IOCs). The information is derived from incident response and investigative techniques.
Key Actions	▪ **Apply the latest software and firmware updates** to your organization's devices. ▪ **Protect operational information from unintentional disclosure** via internet-facing applications. ▪ **Isolate critical systems from edge devices.**
Indicators of Compromise	For a downloadable copy of indicators of compromise, see: https://www.ic3.gov/CSA/2026/QTFY_IOC_Files.csv and https://www.ic3.gov/CSA/2026/QTFY_IOC_Infrastructure.csv
Intended Audience	**Organizations:** Government; Federal Civilian Executive Branch (FCEB); State, Local, Tribal, and Territorial (SLTT); Critical Infrastructure **Sectors:** Government Services and Facilities, Defense Industrial Base, Communications, Energy, Information Technology, Water and Wastewater Systems **Roles:** Defensive cybersecurity analysts, vulnerability analysts, and security systems managers

Table of Contents

Advisory at a Glance 2
Introduction 4
QTFY Background 4
Business Activity 4
Targeting Activity 6
Technical Details 8
Malicious Products Overview 8
QScan 8
QTRouter 9
Botnet Platforms 10
Reconnaissance 11
Initial Access 11
Persistence 11
Resource Development 11
Indicators of Compromise 12
MITRE ATT&CK Tactics and Techniques 33
Incident Response 34
Mitigations 34
Validate Security Controls 35
Contact Information 35
Disclaimer 36
Version History 36

Introduction

The Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cyber National Mission Force (CNMF), hereafter referred to as the authoring agencies, are urgently warning U.S. organizations of ongoing cyber activity by the China-linked hacking group QTFY.

Since its establishment in 2018, the China-linked hacking group QTFY has developed malicious tooling, traded malware and exploits within freelance hacking networks, established and maintained an obfuscation botnet, and ultimately targeted critical systems in the United States. Targeted entities include the defense industrial base (DIB), telecommunications, local government and higher education, among others.

For more information on China-linked obfuscation botnets, see the joint cybersecurity advisory on Defending against China-nexus covert networks of compromised devices. For more information on People's Republic of China (PRC) state-sponsored malicious cyber activity in general, see FBI's Cyber Threat Overview: China webpage.

The authoring agencies encourage organizations to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of QTFY incidents.

For a downloadable copy of IOCs, see:

- https://www.ic3.gov/CSA/2026/QTFY_IOC_Files.csv
- https://www.ic3.gov/CSA/2026/QTFY_IOC_Infrastructure.csv

QTFY Background

The China-linked hacking group QTFY is attributed to Nanjing Xinjiuwei Network Technology Co. (XJW) (南京鑫玖维网络科技有限公司), established in 2018. XJW is an enabling company for cyber operations linked to the People's Republic of China (PRC). XJW has business relationships with PRC Ministry of State Security (MSS) units and larger private China-based cyber enabling companies with expertise in critical infrastructure security to target victim organizations. QTFY actors include former People's Liberation Army (PLA) members and leverage their contacts for contracts and sub-contracts related to the targeting of critical infrastructure. Additionally, QTFY actors have participated in China-based freelance brokering networks, buying and selling cyber exploit items, including access to victim networks.

Business Activity

As of June 2026, XJW had business relationships with the following entities in the PRC enabler ecosystem:

Entity	Chinese Translation	Description
Unit 0718	N/A	An MSS unit that had a business relationship with Sichuan Zhixin Ruijie Network Technology, which is associated with Salt Typhoon. For additional information see JCSA Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System.
Unit 9086	N/A	An MSS unit located in Guangxi Province. In 2019, China-based cyber intrusion company i-Soon had two contracts with Unit 9086.
Hunan Province Ecological and Environmental Construction Management Office	**湖南省生**态环境建设管理办公室	
China Information Technology Testing and Evaluation Center (CNITSEC), Jilin Subcenter (JITSEC)	**中国信息安全**测评中心吉林测评中心	As of September 2021, CNITSEC provided vulnerabilities to the MSS 13th Bureau for review prior to public publication.
Bozhi Security Technology Co., Ltd, (a.k.a. Elextec Cybersecurity, Inc.)	博智安全科技股份有限公司	In June 2025, Bozhi submitted three bids to the National University of Defense Technology (NUDT) for power system vulnerability detection and information assurance awareness projects. Also in June, Bozhi participated in an energy sector cybersecurity conference and was invited to a conference on industrial control system security.

Changyang Technology (Cy-Tech) (Beijing) Co., Ltd.	长扬科技股份有限公司	As of May 2024, Cy-Tech described itself as "focused on industrial internet security, industrial network control, and industrial production safety."
Nanjing Lexbell Information Technology Co., Ltd.	**南京莱克**贝尔信息技术有限公司	In June 2025, Lexbell won a bid to develop a networked data mining and analysis tool to parse unstructured data for human analysis to support command and control system design.
Zhengzhou Hanjiang Electronic Technology Co., Ltd.	郑州汉江电子技术有限公司	
Fujian Ares Network Technology Co., Ltd.	**阿拉**赛斯（厦门）科技有限责任公司	Between May 2023 and October 2025, Ares was the finalist or winning bidder for at least six NUDT projects. The projects called for radio frequency hardware and software products.

Targeting Activity

QTFY actors have expertise in targeting critical infrastructure and other sensitive networks. For nearly a decade, their products and infrastructure have been observed targeting sensitive networks in the US and around the world. The following timeline is a sample of the observed activity:

Date	Target
May 2018	Conducted vulnerability scanning of US Department of Energy. Unsuccessful attempt to gain access to network.
July 2019	Conducted vulnerability scanning of a US election system. Unsuccessful attempt to gain access to network.
August 2019	Used exploit for Pulse Secure VPN vulnerability (CVE-2019-11510) against US Department of Justice, US Federal Reserve, and NASA

October 2019	Attempted to exploit Fortinet FortiOS SSL VPN vulnerability (CVE-2018-13379)
November 2019	Email account “qtfy100@gmail[.]com” received abuse complaint from a US entity classified as “National Security Objective Facility - class A”
January 2020	Used exploit for Citrix Application Delivery Controller (ADC) and Gateway vulnerability (CVE-2019-19781) against numerous US targets
March 2020	Conducted vulnerability scanning of a US Department of Health and Human Services. Unsuccessful attempt to gain access to network.
August 2020	Email account “qtfy100@gmail[.]com” received an abuse complaint regarding a Pulse SSL VPN attack against a healthcare entity. The victim reported “Attacking healthcare in a pandemic is just wrong.”
2021	Installed Remote Access Trojans (RAT) on Taiwan energy sector systems
March 2021	Used “ProxyLogon” exploit for Microsoft Exchange vulnerability (CVE-2021-26855)
June 2021	Conducted vulnerability scanning of a US children’s hospital. Unsuccessful attempt to gain access to network.
July-August 2021	Used exploit for F5 BIG-IP vulnerability (CVE-2020-5902) against a US state government and large US retailer
August 2021	Used exploit for Kentico CMS vulnerability (CVE-2019-10068) at a US telecommunications company
December 2021	Used exploit for “Log4J” / “Log4Shell” JNDI vulnerability (CVE-2021-44228)
October 2023	Used exploit for Atlassian Confluence vulnerability (CVE-2023-22515)
February 2024	Conducted vulnerability scanning of Ivanti management devices at a US semiconductor company. Unsuccessful attempt to gain access to network.
May 2024	Used QScan to scan US power and telecommunication companies, leveraging an exploit for a Check Point Quantum Gateway vulnerability (CVE-2024-24919). Exfiltrated data from over 300 organizations in the United States and around the world. Victims included US defense contractors, financial institutions and universities.

September 2024	Used zero-day exploits for Ivanti Cloud Services Appliance (CSA) vulnerabilities (CVE-2024-8190, CVE-2024-8963, CVE-2024-9380) at three US Department of Energy labs, the US National Institute of Health, the US Health Resources and Services Administration, and a US security device manufacturer
March 2025	Conducted vulnerability scanning of a US power company. Unsuccessful attempt to gain access to network.
April 2025	Exploited CrushFTP vulnerability (CVE-2025-31161) at a US biotechnology company
February 2026	Utilized QScan to exploit BeyondTrust Remote Support (RS) vulnerability (CVE-2026-1731) against a US state government. Also targeted a US water district.
March 2026	Conducted vulnerability scanning of the US Senate and a US hospital system. Unsuccessful attempt to gain access to networks.
June 2026	Used QScan to conduct vulnerability scanning of a US election system. Unsuccessful attempt to gain access to network.

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 19. See the MITRE ATT&CK Tactics and Techniques section of this advisory for tables of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

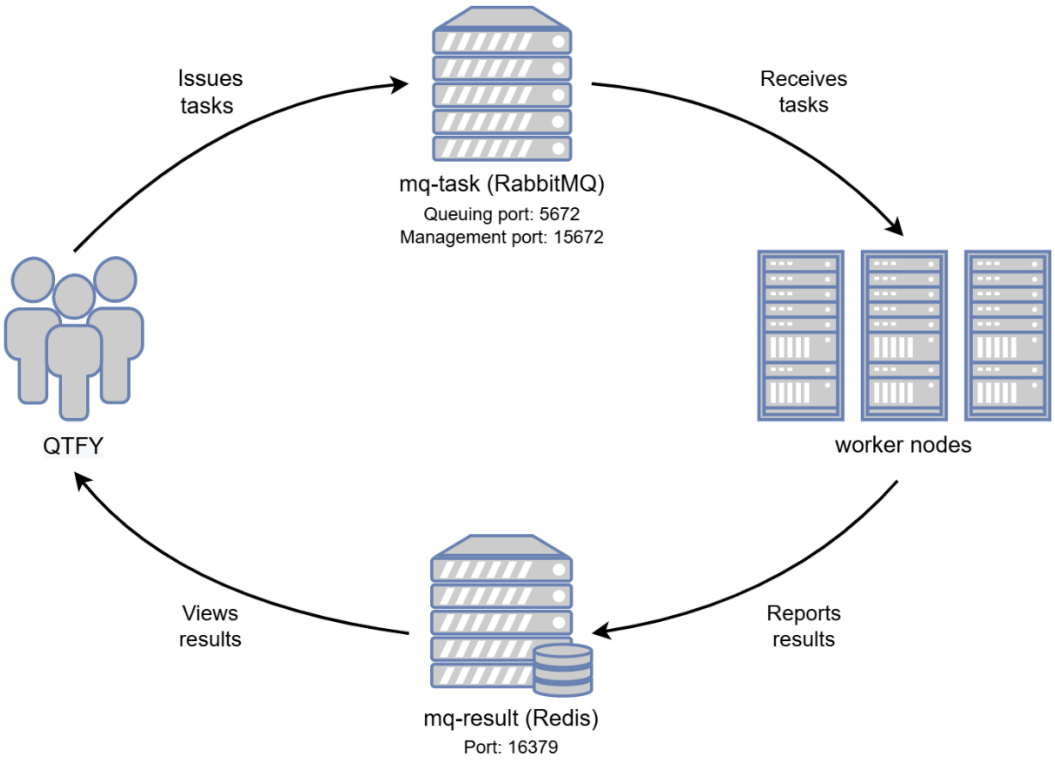
Malicious Products Overview

QTFY actors developed branded products, including a vulnerability scanning and exploitation platform named "QScan", an obfuscation network named "QTRouter", and botnets of compromised Internet of Things (IoT) devices. These products work in conjunction with each other. QScan is used to exploit vulnerable IoT devices and identify vulnerabilities in victim networks. QTFY uses botnet products to control the compromised IoT devices and include them as QTRouter proxy nodes. This enables QTFY-affiliated actors to blend in with legitimate users when targeting victim organizations.

QScan

QScan is a distributed system that processes a large volume of internet scanning tasks, including malicious penetration testing. As of December 2025, the domain qt-proxy[.]org had subdomains mq-task.qt-proxy[.]org and mq-result.qt-proxy[.]org. Prior to December 2025, the domains were mq-task.qt-team[.]com and mq-result.qt-team[.]com.

These domains resolved to servers at IP addresses which hosted respective components of the system. The “mq-task” server hosted RabbitMQ message queues, which provided scanning tasks to a pool of worker nodes primarily housed on leased servers located outside of China. The “mq-result” server received completed tasks with Redis.



QScan processed a variety of task queues, including webpage scraping, TLS certificate collection, subdomain enumeration, and penetration testing, among others. Included with web scraping was a task queue dedicated to detecting the presence of certain plugins installed with content management systems which may have weakened the security of a website. For penetration testing, the system included a database of over 200 proof-of-concept exploits written in Python and was designed for large scale employment. On a single day in 2024 for example, QScan processed over two million scanning and penetration testing tasks.

The QScan platform was used to target a variety of websites and web applications representing organizations worldwide. In the United States, QScan targets included cleared defense contractors, energy companies, telecommunications companies, financial institutions, universities, and local governments.

QTRouter

The QTRouter product is a network traffic obfuscation network running on devices that include routers with custom OpenWrt software. As of June 2026, QTRouter devices authenticate to administration servers named “Proxy Node Management System” (代理节点管理系统) at www.qtproxy[.]xyz and

securelink.qtproxy[.]xyz. QTRouter nodes include commercial proxy service IP addresses (including a proxy service called Fastlink), Alibaba Cloud IPs, and compromised IoT devices.

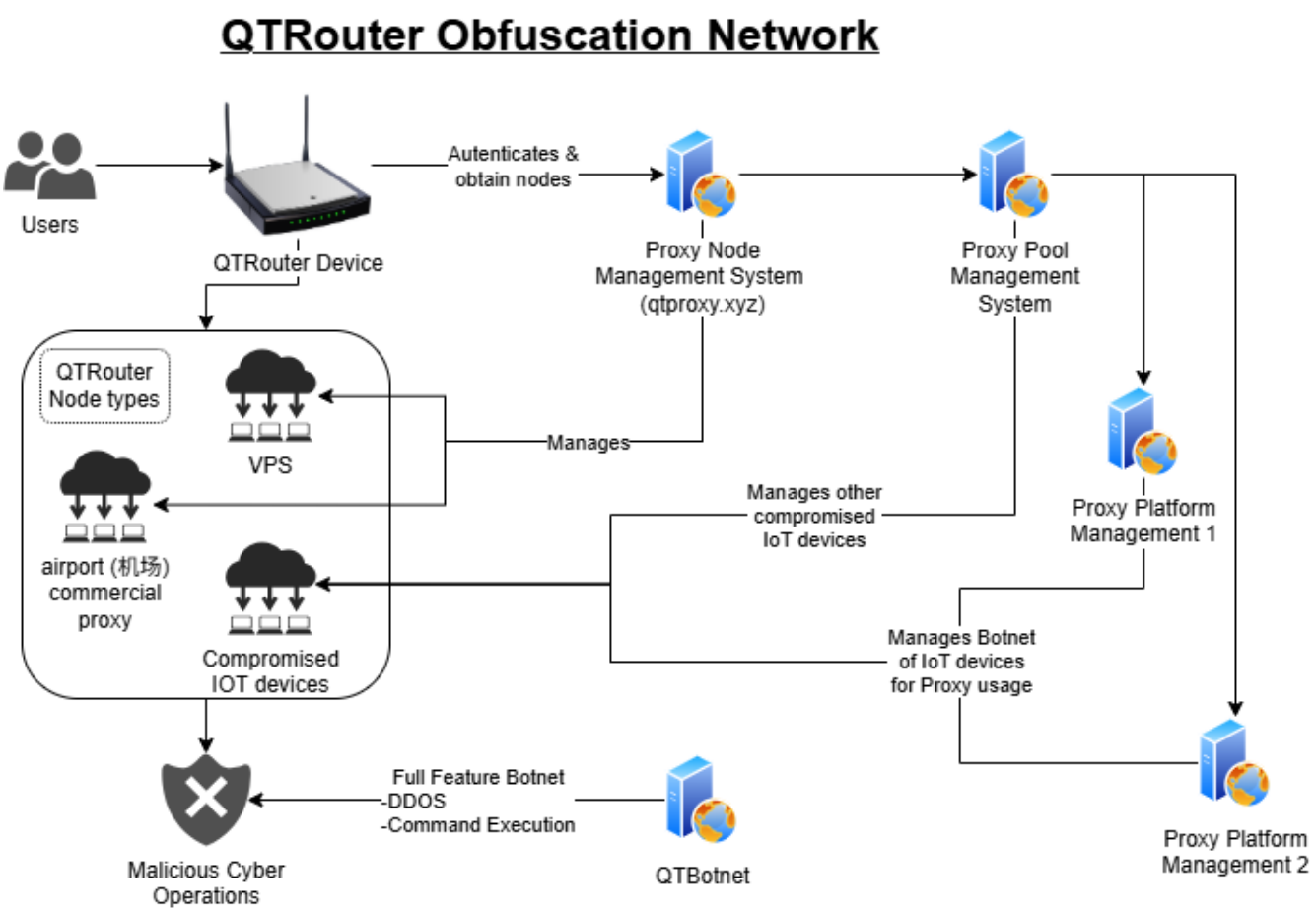
QTRouter uses Clash to establish proxy connections. Its functionality includes viewing available nodes and chaining nodes together to obfuscate the actor behind the malicious activity. Additionally, by mixing the malicious traffic with legitimate traffic on commercial proxy services and using compromised IoT devices to utilize the locations of legitimate users, QTRouter makes it difficult to identify and track the malicious activity.

As of December 2025, a jump server for QTFY's obfuscation network uses the domain jump.qt-proxy[.]org. Prior to December 2025, jump.qt-team[.]com was used. Unique user agent strings originating from IP addresses in China indicate QTRouter was used by QTFY personnel and PRC government personnel in Jiangsu, Qingdao, Jilin, and Sichuan, China.

Botnet Platforms

QTFY actors developed and maintained at least three major platforms that can manage botnets of compromised IoT devices and include them as obfuscation network nodes:

1. **"Proxy Platform Management" (代理平台管理)**: This platform manages a botnet of compromised devices, including IoT devices. Its primary function is to manage botnet nodes and to configure proxy software on those devices. Three components of the platform were identified and hosted on open web directories: a "client", an "agent", and a "server". The threat actor interacts with the server and the agent handles communication between the client and the server.
2. **"Proxy Pool Management System" (代理池管理系统)**: This platform was hosted at IP address 206.19.67[.]207. It is an aggregator of compromised IoT devices and hosted tools to compromise IoT devices. It hosts a database of exploits and a database of server fingerprints to quickly identify systems to target when a new exploit is discovered or when new proxy nodes are needed. It contains lists of multiple categories of compromised IoT devices along with access details (e.g., password). Categories include botnet SOCKSS5 proxies, MikroTik RouterOS devices, and PPTP devices.
3. **QTBotnet**: This platform is composed of a main controller server, secondary level control servers, and compromised devices. Such compromised botnet devices connect to the secondary level control servers. The secondary level control servers manage communication between the main control server and the compromised devices. The control server can launch DDOS attacks, view nodes, import nodes, run commands on compromised IoT devices, and manage the level 2 servers.



Reconnaissance

QTFY actors utilize their QScan platform to conduct reconnaissance against victim networks. They maintain a large database from nearly a decade of Internet scanning that they can leverage when targeting a specific victim, or to quickly identify targets of interest when a new vulnerability is identified.

Initial Access

QTFY actors exploit zero-day and N-day vulnerabilities to gain initial access to victim networks.

Persistence

QTFY actors utilize various remote access trojans (RAT), web shells, and obtain legitimate credentials from compromised systems to maintain persistence. They utilize their QTRouter obfuscation network to access victim networks from nearby compromised IoT, blending in with legitimate users.

Resource Development

QTFY actors are active in the exploit development community, freelance PRC hacker networks, and PRC malicious cyber contracting and subcontracting marketplaces. QTFY participates on the offensive end of

network attack and defense events (护网/HW/HVV) against Chinese critical infrastructure. Their use of Ivanti CSA zero-day exploits in September 2024 occurred directly after one of these events. Their involvement in these circles allows them to keep up with new hacking tactics and techniques. They have also been observed heavily researching and integrating AI into their processes over the last two years.

Indicators of Compromise

See **Table 1** through **Table 8** for indicators of compromise (IOCs) associated with QTFY infrastructure and related activity.

Disclaimer: Several of the following indicators are linked to historical QTFY activity as early as 2017, and many are affiliated with current QTFY infrastructure. The authoring agencies recommend these IP addresses be investigated or vetted by organizations prior to taking action, such as blocking.

Table 1. IPs & Domains Affiliated with QTRouter

IP Address	First Seen	Last Seen
1.32.216[.]171	2026-04-13	Active
8.148.149[.]147	2025-11-30	Active
45.202.210[.]27	2026-05-29	Active
jump.qt-proxy[.]org	2025-12-14	2026-12-14*
jump.qt-team[.]com	2022-02-25	2032-02-25*
securelink.qtproxy[.]xyz	2022-11-10	2027-11-10*
www.qtproxy[.]xyz	2022-11-10	2027-11-10*

Table 2. IPs & Domains Affiliated with Proxy Platform Management

IP Address	First Seen	Last Seen
23.95.220[.]192	2026-03-12	2026-05-12
103.201.131[.]121	2026-03-16	2026-05-16
109.236.48[.]121	2026-03-09	2026-03-11
install.anticonstitutionally[.]sbs	2026-03-03	2027-03-03*
mail.fastsecurey[.]info	2026-03-30	2027-03-31*

IP Address	First Seen	Last Seen
www.fastsecurey[.]info	2026-03-30	2027-03-31*

Table 3. IP Affiliated with Proxy Pool Management System

IP Address	First Seen	Last Seen
206.119.167[.]207	2026-01-23	Active

Table 4. IPs & Domains Affiliated with QScan

IP Address	First Seen	Last Seen
64.32.22[.]203	2024-05-14	2025-05-12
148.135.90[.]22	2023-12-07	2025-06-03
154.64.238[.]222	2025-06-03	Active
154.64.238[.]247	2025-05-12	Active
1.32.216[.]3	2026-06-05	2026-07-03
1.32.216[.]4	2026-06-05	2026-07-03
1.32.216[.]27	2025-09-03	2025-10-03
1.32.216[.]33	2026-06-28	2026-06-29
1.32.216[.]49	2026-02-27	2026-03-27
1.32.216[.]77	2025-09-03	2025-10-03
1.32.216[.]83	2026-01-26	2026-02-27
1.32.216[.]92	2026-04-07	2026-05-27
1.32.216[.]94	2026-01-26	2026-02-27
1.32.216[.]104	2025-11-25	2025-12-24
1.32.216[.]113	2025-09-23	2025-10-23
1.32.216[.]123	2025-09-23	2025-10-23

IP Address	First Seen	Last Seen
1.32.216[.]126	2026-05-08	2026-06-04
1.32.216[.]130	2025-12-24	2026-01-26
1.32.216[.]132	2025-08-20	2025-09-21
1.32.216[.]145	2025-11-25	2025-12-24
1.32.216[.]167	2025-09-03	2025-10-03
1.32.216[.]177	2025-12-24	2026-01-26
1.32.216[.]187	2025-08-20	2025-09-21
1.32.216[.]225	2025-08-20	2025-09-21
1.32.216[.]226	2026-05-08	2026-06-04
23.225.180[.]171	2023-05-07	2026-06-04
23.225.180[.]177	2023-05-07	2026-06-04
23.225.195[.]20	2023-05-07	2026-06-04
23.225.195[.]35	2023-05-07	2026-06-04
23.225.195[.]44	2023-05-01	2026-06-04
23.225.195[.]56	2023-05-01	2026-06-04
27.124.24[.]220	2026-08-04	Active
27.124.24[.]137	2026-08-04	Active
38.14.63[.]7	2026-04-28	2026-05-27
38.14.63[.]8	2026-04-28	2026-05-27
38.14.63[.]179	2026-05-08	2026-06-04
38.14.63[.]235	2026-05-08	2026-06-04
45.147.200[.]105	2022-04-25	2023-09-09

IP Address	First Seen	Last Seen
45.196.221[.]138	2026-08-04	Active
45.196.221[.]149	2026-07-03	2026-08-03
45.196.221[.]152	2026-07-03	2026-08-03
45.202.65[.]135	2025-10-24	2025-11-24
45.202.210[.]32	2026-06-05	2026-07-03
69.176.89[.]102	2023-05-07	2023-06-04
134.122.150[.]22	2026-08-04	Active
134.122.150[.]25	2026-08-04	Active
134.122.150[.]27	2026-07-03	2026-08-03
134.122.150[.]73	2026-05-08	2026-06-04
134.122.151[.]19	2026-05-08	2026-06-04
134.122.186[.]21	2025-10-24	2025-11-24
134.122.194[.]131	2026-01-26	2026-02-27
134.122.194[.]135	2026-06-05	2026-07-03
134.122.194[.]137	2026-06-05	2026-07-03
134.122.194[.]143	2025-10-24	2025-11-24
134.122.194[.]149	2026-04-07	2026-05-27
134.122.194[.]161	2026-01-26	2026-02-27
134.122.194[.]168	2025-12-24	2026-01-26
134.122.194[.]170	2026-02-27	2026-03-27
134.122.194[.]171	2026-04-07	2026-05-27
134.122.194[.]173	2025-11-25	2025-12-24

IP Address	First Seen	Last Seen
134.122.194[.]198	2025-09-03	2025-10-03
134.122.194[.]209	2025-12-24	2026-01-26
134.122.194[.]217	2025-11-25	2025-12-24
134.122.194[.]222	2025-09-03	2025-10-03
134.122.194[.]232	2025-10-24	2025-11-24
134.122.194[.]235	2026-02-27	2026-03-27
134.122.206[.]11	2022-12-18	2025-03-17
137.220.181[.]142	2024-11-07	2025-03-21
137.220.181[.]143	2024-11-07	2025-03-21
137.220.181[.]196	2024-05-31	2025-03-20
137.220.244[.]18	2024-05-31	2025-04-27
137.220.244[.]23	2024-05-31	2025-04-27
154.38.104[.]144	2024-12-18	2025-06-02
154.38.105[.]11	2024-05-31	2025-03-17
154.38.105[.]39	2024-05-31	2025-04-27
154.38.105[.]109	2024-05-31	2025-03-17
154.198.213[.]58	2024-05-31	2025-06-02
155.94.129[.]191	2021-12-13	2023-06-04
156.234.193[.]62	2023-05-07	2025-03-17
156.234.193[.]79	2023-05-07	2025-03-17
156.245.124[.]20	2026-02-27	2026-03-27
156.245.124[.]25	2025-09-03	2025-10-03

IP Address	First Seen	Last Seen
156.245.124[.]44	2025-10-24	2025-11-24
156.245.124[.]47	2025-11-25	2025-12-24
156.245.124[.]57	2025-12-24	2026-01-26
156.245.124[.]82	2026-04-07	2026-04-27
156.245.124[.]113	2025-10-24	2025-11-24
156.245.124[.]115	2026-02-27	2026-03-27
156.245.124[.]131	2025-12-24	2026-01-26
156.245.124[.]157	2026-04-07	2026-04-27
156.245.124[.]172	2026-01-26	2026-02-27
156.245.124[.]180	2025-09-03	2025-10-03
156.245.124[.]223	2025-11-25	2025-12-24
156.245.124[.]243	2025-11-26	2026-02-27
156.251.172[.]166	2025-03-21	2025-06-02
156.251.172[.]167	2025-03-21	2025-06-02
156.251.172[.]168	2025-03-21	2025-06-02
172.247.15[.]222	2023-05-01	2025-03-17
172.247.15[.]236	2024-05-31	2025-05-25
198.50.168[.]185	2024-05-31	2025-04-29
198.50.168[.]189	2024-05-31	2025-04-29
mq-task.qt-proxy[.]org	2025-12-14	2026-12-14*
mq-result.qt-proxy[.]org	2025-12-14	2026-12-14*
mq-task.qt-team[.]com	2022-02-25	2032-02-25*

IP Address	First Seen	Last Seen
mq-result.qt-team[.]com	2022-02-25	2032-02-25*

Table 5. Domains Affiliated with QTFY Infrastructure

Domain	First Seen	Last Seen
adaadada[.]top	2022-09-24	2023-09-25
anticonstitutionally[.]sbs	2026-03-03	2027-03-03*
apexrecord[.]top	2023-03-02	2024-03-03
bigchains[.]net	2019-03-17	2025-03-17
bigdataocean[.]net	2018-12-24	2021-12-24
cataclysmdda[.]xyz	2022-12-05	2024-12-05
categorystore[.]net	2020-11-20	2026-03-02
ccgv[.]me	2018-03-12	2027-03-12*
daumcab[.]net	2019-08-01	2024-08-01
dlview[.]net	2019-03-17	2024-03-17
docker-hub[.]qt-team[.]com	2022-02-25	2032-02-25*
fastsecurey[.]info	2026-03-30	2027-03-31*
helicopter-crash[.]online	2021-12-10	2022-12-10
huntger[.]store	2018-04-01	2020-04-01
instantmessagehub[.]tech	2023-11-03	2026-11-03*
jump[.]qt-proxy[.]org	2025-12-14	2026-12-14*
jump[.]qt-team[.]com	2022-02-25	2032-02-25*
miandfish[.]store	2018-06-14	2020-06-14
mirrorstorage[.]org	2020-10-15	2023-10-15

Domain	First Seen	Last Seen
mq-result[.]qt-proxy[.]org	2025-12-14	2026-12-14*
mq-result[.]qt-team[.]com	2022-02-25	2032-02-25*
mq-task[.]qt-proxy[.]org	2025-12-14	2026-12-14*
mq-task[.]qt-team[.]com	2022-02-25	2032-02-25*
newtourism[.]pw	2020-06-26	2024-06-26
onlion[.]shop	2024-06-22	2026-06-22*
oraclelabs[.]biz	2025-09-03	2026-09-03*
qtcyber[.]com	2021-09-02	2031-09-02*
qtproxy[.]com	2017-07-20	2020-07-20
qt-proxy[.]org	2025-12-14	2026-12-14*
qtproxy[.]tk	2018-10-10	2022-09-17
qtproxy[.]xyz	2022-11-10	2027-11-10*
qt-team[.]com	2022-02-25	2032-02-25*
securityforce[.]cf	2020-06-27	2022-06-27
serverbks[.]xyz	2023-11-30	2024-11-30
taskqueue[.]work	2021-06-06	2022-06-06
turandotarting[.]org	2017-11-07	2021-11-07
vigorlabs[.]info	2023-12-29	2025-12-29
vsky[.]tech	2018-11-08	2019-11-08
whtsapp[.]online	2018-04-01	2020-04-01
wintel[.]biz	2025-09-03	2026-09-02*
worldswar[.]online	2022-03-02	2027-03-02*

Domain	First Seen	Last Seen
xinjiuwei[.]net	2022-01-14	2024-01-14

**Future dates denote currently known registration expiration dates.*

Table 6. Other QTFY Actor-Controlled IPs

IP Address	First Seen	Last Seen
1.32.216[.]31	2025-09-11	2025-09-13
5.34.176[.]230	2020-02-18	2020-02-19
5.34.183[.]142	2020-10-21	2020-11-30
5.183.179[.]105	2019-07-26	
5.183.179[.]120	2020-07-02	
5.183.179[.]133	2021-09-11	2026-05-28
23.95.82[.]90	2018-03-04	
23.224.39[.]80	2023-04-04	2023-09-12
23.224.46[.]224	2021-08-03	2022-10-10
23.235.147[.]235	2018-11-08	2018-12-14
23.238.217[.]23	2020-09-20	2021-03-07
23.254.161[.]193	2019-07-24	2020-09-18
23.254.164[.]48	2019-05-21	2020-08-22
23.254.164[.]181	2019-05-21	2020-09-18
23.254.167[.]3	2019-05-21	2019-07-21
23.254.202[.]64	2019-06-30	2020-06-22
23.254.227[.]240	2020-02-19	2020-03-21
23.254.229[.]43	2019-05-21	2019-07-22

IP Address	First Seen	Last Seen
23.254.250[.]188	2020-02-19	2020-03-04
27.102.118[.]249	2019-11-25	2019-12-14
27.102.127[.]93	2020-04-29	2020-04-30
31.169.126[.]162	2025-06-23	2026-05-08
31.170.160[.]61	2018-11-07	2018-11-07
31.170.161[.]71	2018-03-31	2019-02-19
31.170.161[.]78	2018-05-23	Active
39.104.208[.]77	2024-02-28	2020-05-10
43.240.12[.]129	2017-12-31	2025-07-07
45.8.158[.]64	2025-06-06	2025-06-21
45.8.159[.]228	2025-01-22	2020-07-26
45.12.206[.]12		2020-07-18
45.12.206[.]26	2019-07-15	
45.12.206[.]72	2020-11-19	2021-11-19
45.12.206[.]76	2019-08-15	2020-10-15
45.12.206[.]87	2020-07-29	2022-02-04
45.12.206[.]234	2019-07-15	2020-07-16
45.32.23[.]254	2021-06-21	2021-06-26
45.32.32[.]50	2020-08-02	2020-08-03
45.82.167[.]22	2020-12-02	2021-10-23
45.82.167[.]112	2019-07-26	
45.82.167[.]115	2019-07-26	

IP Address	First Seen	Last Seen
45.82.167[.]121	2019-07-26	
45.82.167[.]222	2019-07-26	
45.90.57[.]148	2020-10-14	2020-10-24
45.95.2[.]119	2026-03-13	2026-04-13
45.117.102[.]170		2019-09-10
45.128.153[.]29	2023-03-21	2024-01-29
45.128.153[.]126	2020-11-19	
45.134.17[.]84	2022-01-09	
45.154.2[.]94	2021-03-06	2021-03-07
45.157.136[.]157	2020-03-17	2021-03-08
45.157.136[.]158	2020-03-17	
45.157.136[.]159	2020-03-17	
45.199.188[.]1	2019-04-02	
45.199.188[.]251	2018-10-23	2019-07-18
45.199.189[.]122	2019-07-05	2019-08-20
45.199.189[.]123	2019-07-05	
46.3.242[.]214	2023-12-06	2023-12-20
47.76.131[.]175	2024-02-28	2026-05-31
47.88.175[.]61	2017-12-19	2020-11-03
47.96.8[.]186	2025-03-22	2025-11-28
47.122.42[.]2	2024-05-05	2025-11-28
58.152.47[.]231	2020-12-18	2020-12-22

IP Address	First Seen	Last Seen
62.216.88[.]18	2020-06-23	2021-06-21
62.216.88[.]26	2020-06-23	2022-12-25
64.32.15[.]23	2018-03-13	2018-04-28
64.32.15[.]166	2018-04-03	
64.32.15[.]198	2018-03-16	2018-05-30
66.154.120[.]18	2018-07-19	2018-12-31
75.140.50[.]69	2018-09-03	2021-09-01
77.83.117[.]245	2020-03-14	
78.142.19[.]106	2019-04-30	2020-03-14
78.142.19[.]207	2019-07-26	2019-07-27
79.143.186[.]63	2018-03-07	2018-05-07
80.241.213[.]68	2018-03-06	2018-05-06
80.241.213[.]90	2018-03-06	2018-05-06
80.241.213[.]93	2018-03-06	2018-05-06
85.143.202[.]117	2019-05-31	
88.119.175[.]225	2020-01-07	2018-05-07
88.119.175[.]229	2021-08-04	2022-07-30
89.31.127[.]87	2020-07-18	2022-04-10
89.31.127[.]242	2020-06-26	2023-06-26
89.223.100[.]18	2019-04-29	2019-06-30
91.194.90[.]213	2018-03-26	2018-05-30
91.194.91[.]25	2018-03-06	2018-05-06

IP Address	First Seen	Last Seen
91.194.91[.]84	2018-03-26	2018-06-04
91.220.202[.]243	2020-06-23	2020-08-26
92.38.139[.]64	2019-12-07	2022-05-12
92.38.163[.]102	2020-03-09	2020-07-19
94.156.236[.]183	2025-07-10	2026-04-09
101.35.24[.]222	2022-04-01	2022-05-18
103.83.157[.]38	2020-12-13	2021-10-07
103.103.128[.]6	2020-01-14	
103.114.161[.]228	2018-06-18	2019-04-27
103.114.161[.]243	2018-06-22	2018-07-24
103.114.163[.]112	2019-04-01	
104.168.123[.]211	2021-03-08	
104.168.145[.]175	2019-02-01	
104.168.148[.]236	2019-02-01	2020-08-22
104.168.153[.]230	2019-04-01	2019-10-21
104.168.157[.]30	2018-11-28	2019-05-21
104.168.158[.]113	2018-11-28	2019-05-21
104.168.158[.]114	2018-11-28	2019-05-21
104.168.158[.]181	2019-01-02	2019-07-20
104.168.165[.]68	2018-11-29	
104.168.166[.]42	2019-05-21	2019-10-21
104.168.166[.]234	2019-05-21	2020-08-22

IP Address	First Seen	Last Seen
104.168.170[.]48	2018-11-28	2019-05-21
104.168.173[.]43	2019-05-21	2019-10-21
104.168.173[.]191	2020-02-19	
104.168.175[.]134	2019-01-01	2019-07-22
104.168.194[.]148	2019-05-21	2020-08-22
104.168.203[.]65	2019-11-03	2019-12-22
104.168.211[.]139	2019-02-17	2020-08-22
104.168.211[.]236	2019-02-18	2019-05-21
104.234.174[.]5	2026-02-06	
106.14.33[.]83	2025-03-22	2025-08-13
106.14.68[.]99	2025-05-12	2025-08-12
106.14.164[.]140	2025-03-22	2025-08-12
106.14.184[.]69	2024-01-25	2026-01-17
107.155.95[.]134	2021-02-04	2021-03-12
107.175.215[.]126	2020-12-15	2021-03-07
108.61.203[.]184	2017-12-31	2018-03-16
108.174.199[.]29	2019-06-28	2022-05-18
108.174.200[.]249	2019-05-19	2020-05-22
109.166.36[.]217	2020-08-18	2021-05-24
110.163.142[.]168	2019-03-27	
111.223.246[.]9	2019-09-02	2019-12-14
113.212.91[.]177		2020-12-29

IP Address	First Seen	Last Seen
118.31.35[.]233	2025-03-11	2025-09-11
119.84.120[.]157	2019-07-24	2021-12-13
119.237.159[.]189	2021-12-09	2021-12-13
120.27.150[.]114	2025-02-27	2025-11-28
122.112.169[.]163	2020-02-20	2024-03-15
141.164.39[.]12	2020-10-22	2021-01-21
142.11.211[.]86	2018-11-22	2020-09-24
142.11.211[.]250	2019-07-21	2022-08-04
142.11.212[.]111	2019-05-19	2020-05-22
142.11.213[.]132	2021-08-04	2022-07-29
142.11.213[.]254	2019-05-19	2020-09-22
142.11.215[.]132	2019-05-21	2019-07-22
142.11.219[.]75	2020-07-11	2021-09-10
142.11.227[.]204	2020-02-06	2020-08-22
142.11.227[.]246	2020-03-15	2020-03-19
142.11.236[.]143	2019-02-17	2020-02-22
142.11.237[.]112	2020-07-11	2022-06-29
154.85.14[.]250	2019-04-20	2019-12-25
154.85.32[.]39	2018-06-21	
154.85.32[.]43	2018-06-18	
154.198.212[.]233	2023-08-09	2023-08-23
154.210.13[.]78	2019-12-15	2019-12-19

IP Address	First Seen	Last Seen
154.211.2[.]78	2018-12-16	2019-06-10
156.23.19[.]18	2023-12-07	2024-11-29
156.67.220[.]50	2020-09-29	2020-10-15
156.234.193[.]18	2023-12-03	2024-12-27
156.234.193[.]182	2023-08-09	2023-08-30
167.160.86[.]103	2018-10-09	2019-04-18
167.160.86[.]168	2018-06-23	2020-07-26
173.231.242[.]82	2024-07-16	2024-07-21
173.247.227[.]62	2018-07-01	
173.247.232[.]36	2019-01-16	2019-03-15
173.247.232[.]38	2019-01-03	2021-05-11
185.2.103[.]236	2018-03-06	2018-05-06
185.14.31[.]21	2020-10-14	2020-10-24
185.62.189[.]42	2018-03-22	2018-12-30
185.82.216[.]142	2020-10-14	2020-12-21
185.82.218[.]133	2020-10-29	
185.126.116[.]236	2021-06-06	2022-06-09
185.141.24[.]3	2018-02-24	
185.160.24[.]70	2020-03-20	2020-07-26
185.162.128[.]136	2018-03-03	2018-06-04
185.167.116[.]125	2020-07-13	2024-01-28
185.172.65[.]80	2018-11-30	2019-03-24

IP Address	First Seen	Last Seen
185.173.235[.]54	2020-12-15	2021-03-06
185.173.235[.]172	2020-09-27	2021-03-06
185.194.216[.]13	2021-11-29	2022-03-22
185.198.56[.]14	2019-11-03	
185.198.58[.]131	2018-02-06	
185.198.58[.]240	2018-02-06	
185.198.58[.]241	2018-02-06	
185.201.9[.]198	2020-05-01	2020-10-22
185.234.218[.]240	2019-05-09	2019-06-23
185.239.69[.]163	2022-09-09	2023-04-24
188.209.49[.]95	2018-03-17	2018-10-12
192.119.73[.]100	2020-02-06	2020-04-29
192.119.73[.]107	2020-02-06	2021-08-23
192.119.73[.]108	2020-02-06	2021-08-23
192.119.77[.]232	2020-10-23	2021-08-23
192.236.147[.]72	2019-11-04	2019-12-22
192.236.162[.]232	2020-02-23	2020-09-20
192.236.163[.]117	2020-02-23	2020-08-22
192.236.163[.]119	2020-02-23	2020-09-19
192.236.178[.]206	2019-05-21	2019-07-16
192.236.178[.]207	2019-05-21	2020-08-18
192.236.179[.]163	2019-07-27	

IP Address	First Seen	Last Seen
192.236.179[.]164	2019-07-27	
192.236.179[.]166	2019-07-27	
192.236.179[.]167	2019-07-27	
192.236.179[.]173	2019-07-27	
192.236.179[.]216	2019-07-27	
192.236.179[.]254	2019-07-27	
192.236.192[.]3	2019-07-27	2020-08-22
192.236.192[.]4	2019-07-27	2020-02-22
192.236.192[.]5	2019-07-27	2020-09-21
192.236.192[.]6	2019-07-27	2020-08-22
192.236.192[.]119	2019-07-27	2020-08-22
193.34.144[.]131	2018-03-06	2018-05-06
193.38.51[.]46	2020-07-25	2020-07-26
193.160.32[.]138	2020-09-20	2021-03-07
193.160.32[.]141	2020-09-27	2021-03-07
193.160.65[.]116	2019-02-18	2019-10-03
193.160.96[.]154	2020-12-15	2021-03-06
193.200.241[.]157	2018-03-06	2018-05-06
194.104.10[.]58	2026-03-03	2026-06-01
194.124.33[.]93	2022-05-17	2023-02-05
194.124.35[.]104	2019-07-15	2020-07-19
194.126.173[.]71	2021-02-04	2021-04-27

IP Address	First Seen	Last Seen
194.126.173[.]154	2021-02-02	2021-04-27
194.156.120[.]205	2022-08-25	2024-01-12
195.123.213[.]218	2018-11-21	2018-12-28
195.123.237[.]33	2020-10-07	2021-05-07
195.123.240[.]47	2020-10-20	2020-11-20
198.13.37[.]185	2017-11-08	2018-03-16
198.44.14[.]72	2020-10-22	2021-08-23
198.44.15[.]200	2020-10-23	2021-08-05
198.46.233[.]13	2020-08-28	2021-03-07
198.50.168[.]176	2021-03-07	2022-05-29
198.50.168[.]182	2020-09-25	2022-05-29
198.74.112[.]85	2022-05-17	2023-11-21
198.84.122[.]140	2020-10-23	2021-08-23
208.51.62[.]181	2017-06-26	2018-08-12
213.136.66[.]213	2018-03-08	2018-05-29
213.183.56[.]96	2020-10-29	2021-02-28
213.252.244[.]38	2020-01-03	2020-01-07
213.252.244[.]51	2020-01-03	2020-01-07
218.66.59[.]169	2023-03-02	2024-03-03
221.226.197[.]238		2020-12-15
222.99.101[.]22	2019-04-04	

Table 7. Proxy Platform Management Binaries

Name	SHA-256
agent_linux_386	d810f1253ee4bee05ca96a70a9c293f2839fb00b2aa238861f7b89e3a66bd357
agent_linux_amd64	7a4c87677d7892b66c30c82ea72893bd29cfe793fade45222b4cf853b877d300
agent_linux_arm	c1381b35c21aec9e74e8d42b60c4733abd23fd012c75ab0e9101e37c9be62a7a
agent_linux_arm64	e939954618ec089485eff4de098f6c5ce4d672acfd03150f5f0b38bbecbba664
agent_linux_armhf	6decf77b1a3595374a15a014bbb9ac9774f67dca7df59ccf4b734a68d9e35224
agent_linux_mips	5329f26cc11cba660382f58f388d2dad50e10e2ba37d0d6002622c8061b211b2
agent_linux_mips64	69a20babb22ffb372733900cb2e6739598b316aecdbc0394ce8029717ee13089
agent_linux_mips64le	9759492bc73a1704d6d71c6f40ab5321a095f9ab2ae5ca069dd4f7b3a98235fa
agent_linux_mipsle	dd014653fce1fe5f19d1b0e1ad5f254118ca6d002e29c549ecb15029ed0a381e
agent_linux_powerpc	c7abdd66dae9f0e190361d7a39a73128e9d7dc3da338c02f3d93488786813eb3
agent_linux_riscv32	4a7a9354c5764a0977a004f3bf590db8c86ea747d170bf9a1541b8c7cfcf4009
agent_linux_riscv64	6547c0f20c7770bb228b9b0ac61a6d2e16e74afad37b62bcecc7e69b51354a87
agent_linux_s390x	12b1f2078fcdcf792e5482308acaea8cc617c58d51019edd4a381fef52329dec
c_client_arm	00b0045e9e28b89946e7e839ac910f1f2e6f3c28937839aff3b0b41008c80188
c_client_arm64	ea89a969d7a4e4b9c3da24577fe2d633f74c4f25fd1494905063b40b57aeca31
c_client_mips	7bba7912b7fc01795b3a0503d0e546087990124a2256b083c1c5a498a205a721
c_client_mips64	26c9b561e431d033aa16f94580bfa7ace390a1c9c6834a0ee1a6b0a9a306485c
c_client_mips64le	bb1428134f6f587d63a3092ef125a7a2ac50fda3ee71b830bf725f20956b0d3f
c_client_mipsle	ef1b84fa1f3087415ba1e798b018f35c675de1032723579e38d81f79dcc37878
c_client_ppc64le	ab745ad10ffcbf65acdf171cd47d20aed581ac07304570d96caffacc6ece2651
_client_riscv64	996b3aedb34426184ca4f8141daec29a0c5785b11e7eea47559f2e0ef1e6180a

Name	SHA-256
c_client_s390x	ce8832b4681e63118c159f379de82f8c97adc62a81c19cae903d1ba0e5629cf1
client_linux_386	08dc78ae82d9c480420f7cfa797334c8976077a02df5f6b4cee3072ed4a197f9
client_linux_amd64	ba20494fe5a12955a408f076c3677bf8ae600c890554b9906049b8cd07206cfb
client_linux_arc700	5c0708b7a7a7ca00188b40df6b80f4875b2e430b2b0c38b68dd9428bfcb98d09
client_linux_arm	0d48039b416a236f6e0e0fd702b5a824e8c7118af597c81271c64bd6b0adfec2
client_linux_arm64	ad2fae2894432da7b82fec0d5d3a75b5ffa1b84a50ad67477b6063a1769a3846
client_linux_armhf	dbcd1588caae92b7525aac096b7ec8c543b5ab8c4c95dfb33051d42c351e19b3
client_linux_mips	86881181d7244a8e9d45f5fe1e2b7f4c3e8bd6cd1e6383c92693ee956c4d87fb
client_linux_mips64	dc0624c316667b89aa88afa716933235584a27d14b2a08606e43a657a95db991
client_linux_mips64le	239b9f5677b66d3dc69e003028d041c09440330dd367763e68c0a56454afd91a
client_linux_mipsle	b3b32e592a73d46566c51ed18c07155ad3d980142f1a4c32c4e9728208c02fce
client_linux_powerpc	2d29f9f75e40e5b58cb4379d44ff7b511620e8dea584ffaf4db6a7597ee23562
client_linux_riscv32	5653a062a37d8a650c9a603cee0e7744af128bad28be8916c9de9ac16f1a82e5
client_linux_riscv64	ed24ea239799e470c66d160eb7b097ab1d7627fc6c51236d6169da920f5b3b5c
client_linux_s390x	92e9c9c36d469d56fbeba052d3062b77cd869c6df8f10faafd184717c557a245

Table 8. Proxy Platform Management scripts

Name	SHA-256
a	c73bd1c498a147e71e345a99f5f85e3442243c2a7b7cb65f0d00a72acc0a87e7
b	bea44e8cbf35c240c9cddc88284b6f8f94129e4e0a42a85e2603406980b83990
c	a617e06c27d3514c57fd83711c75846d798e3ecefd5a0246b5ac9a191392e98a
d	c337b92789987efe8ae0afcd56da948b38aa4b0e5859f2d51a61e2bc152c1feb
e	5fb500afd83fb64f64a2789abc66f0a158d915167e1def6ba56d9543dd9de3d7

Name	SHA-256
F	c46944343b7e33c0f88ca9583b8145a4735d6e9780f9df1777b4c59887b56a35
in.sh	0cf8ed7064d3d4827f841451c661d788d4cf7d067901e35a7a019f1c9d5ef656

MITRE ATT&CK Tactics and Techniques

See **Table 9** through **Table 12** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 9. Reconnaissance

Technique Title	ID	Use
Active Scanning: Vulnerability Scanning	T1595.002	Actors run software to check whether target systems match the configuration of a system that is expected to be vulnerable.

Table 10. Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Actors may run remote commands affecting the target system in a minor way to confirm a vulnerability exists. Then, other commands may be run to exploit a weakness in an application accessible via the public web.

Table 11. Persistence

Technique Title	ID	Use
Server Software Component: Web Shell	T1505.003	Actors may write or download a small script onto the target system which can be run to expose backdoor access to the system via the internet.

Table 12. Resource Development

Technique Title	ID	Use
Acquire Infrastructure: Virtual Private Server	T1583.003	Actors may purchase virtual private servers (VPSs) available via cloud computing providers. These systems are easily configurable in a rapid manner.

Technique Title	ID	Use
Develop Capabilities	T1587	Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in house.

Incident Response

If a potential compromise is detected, organizations should take the following actions:

1. **Determine which hosts were compromised and isolate them** by quarantining or taking them offline.
2. **Initiate threat hunting activities to scope the intrusion**—collect and review relevant artifacts, logs, and other data to identify threat actor TTPs, compromised devices and accounts, a timeline of activity, etc.
3. **Report the compromise to the FBI** and other agencies as appropriate (see Contact Information for details).
4. **Apply eviction countermeasures**, including those listed below, to contain the incident and eradicate the threat actor from the network (**Note:** Start applying countermeasures after collecting enough threat hunting data to inform effective countermeasure selection; this will likely overlap with threat hunting activities):

    a. Use CISA's Eviction Strategies Tool to assemble countermeasures for a systematic eviction plan—the tool comprises **Playbook-NG** (a web application) and **COUN7ER** (a database of post-compromise countermeasures mapped to adversary TTPs).

    b. Use Playbook-NG and COUN7ER together to assemble a systematic eviction plan, or playbook, that leverages distinct countermeasures to contain and evict cyber threat actors. The playbook features a list of recommended response actions based on threat actor TTPs and includes each action's intended outcome, preparatory steps, and associated risks. For more information, see CISA's Eviction Strategies Tool Fact Sheet.
5. **Harden the network to prevent additional malicious activity** (see **Mitigations** for guidance).

Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture based on QTFY's activity.

- **Apply the latest software and firmware updates to your organization's devices**: Enable automatic updates where possible. Audit your environment for end of support (EOS) devices and use lifecycle management procedures to plan for their replacement. For more information on mitigating risk from EOS devices, see Reducing the Attack Surface for End-of-Support Edge Devices.
    - Ensure web server software and plugins are up to date. Monitor for web shells. See Detect and Prevent Web Shell Malware for related guidance.

- **Protect operational information from unintentional disclosure via internet-facing applications**: Regularly audit your organization's web pages and applications for published secrets (API keys, tokens, or sensitive configuration details). As much as possible, configure these applications to provide only non-sensitive information to web crawlers and scanners.
- **Isolate critical systems from edge devices**: Implement zero trust (ZT) network segmentation principles to limit the scope of a potential breach. See CISA's Zero Trust best practice information (link: https://www.cisa.gov/topics/cybersecurity-best-practices/zero-trust) for additional guidance.
- **Hunt for the provided indicators of compromise (IOCs)** to detect suspicious activity in the network environment or network monitoring solution. Organizations can leverage machine learning techniques to build understandings of their network activity baselines.

Validate Security Controls

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 9** to **Table 12**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Contact Information

US organizations are encouraged to report suspicious or criminal activity related to information in this advisory to the FBI:

- Contact your local FBI field office. 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; and
- Name of the submitting company or organization, and a designated point of contact.

- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

Version History

September 2, 2026: Corrections to Business Activities table, Table 4, and Table 7.

August 26, 2026: Initial version.