BRIEF FOCUS · QTFY · CHINA-LINKED THREAT ACTOR

QTFY: Industrializing Cyber Exploitation Against Critical Infrastructure

A joint FBI, NSA and CNMF advisory details how a China-linked actor turned vulnerability discovery into an industrial pipeline with two million scanning tasks in a single day, and data exfiltrated from more than 300 organizations in one campaign.

THREAT ACTOR	ATTRIBUTED TO	PLATFORMS	ADVISORY
QTFY **QT, QTCYBER**	**Nanjing Xinjiuwei Network Technology**	**QScan** **QTRouter**	**FBI · NSA · CNMF** **August 26, 2026**

SECTORS AT RISK

Government · Defense · Communications · Energy · Information Technology · Water

THE ACTOR

Who Is QTFY?

On August 26, 2026, the FBI, National Security Agency (NSA), and Cyber National Mission Force (CNMF) issued a joint Cybersecurity Advisory urgently warning U.S. organizations about ongoing activity by the China-linked hacking group QTFY.

Also known as QT and QTCYBER, the group has developed a sophisticated ecosystem of malicious distributed platforms used to target U.S. and foreign organizations, including critical infrastructure.

QTFY is attributed to Nanjing Xinjiuwei Network Technology Co. (XJW), a China-based company established in 2018. According to the advisory, XJW is an enabling company for cyber operations linked to the People's Republic of China, maintains business relationships with Ministry of State Security units, and includes former People's Liberation Army members among its actors.

For nearly a decade, QTFY infrastructure has been observed targeting sensitive networks worldwide.

THE PLATFORM: QSCAN

Exploitation At Industrial Scale

QScan transforms vulnerability discovery and exploitation into a highly scalable operation. Developed by QTFY, the distributed platform supports webpage scraping, subdomain enumeration, TLS certificate collection, vulnerability scanning, and malicious penetration testing.

Its database contains more than 200 proof-of-concept exploits, primarily written in Python.

This infrastructure enables QTFY to rapidly identify exposed systems across large numbers of potential targets and exploit vulnerable internet-facing infrastructure – activity that has involved vulnerabilities affecting technologies from a long list of widely deployed edge vendors.

THREAT SNAPSHOT

200+

Proof-of-concept exploits held in the QScan database

2M+

Scanning and penetration-testing tasks in a single day, 2024

300+

Organizations that had data exfiltrated in the May 2024 campaign

THE KILL CHAIN

From Initial Access To Data Theft

QTFY's activity demonstrates that large-scale scanning is only the beginning of the threat.

In May 2024, QTFY used QScan against U.S. power and telecommunications companies, leveraging CVE-2024-24919, a vulnerability affecting Check Point Quantum Gateway appliances. According to the joint advisory, the campaign resulted in data being exfiltrated from more than 300 organizations in the United States and around the world, including U.S. defense contractors, financial institutions, and universities.

Following successful compromise, QTFY actors have also used remote access trojans, web shells, and legitimate credentials to maintain persistence within victim environments.

This combination of automated reconnaissance, vulnerability exploitation, persistence, and data theft creates a significant risk for organizations operating sensitive and critical infrastructure.

TECHNOLOGIES TARGETED IN OBSERVED QTFY ACTIVITY

Pulse Secure **Fortinet** **Citrix** **Microsoft** **F5** **Atlassian** **Check Point** **Ivanti** **CrushFTP** **BeyondTrust**

OBFUSCATION: QTROUTER

Hiding In Plain Sight

QTFY also developed QTRouter, a network traffic obfuscation system designed to conceal the true origin of malicious activity.

QTRouter combines commercial proxy infrastructure with compromised Internet of Things (IoT) devices. QTFY can route malicious traffic through compromised devices located geographically close to targeted organizations, making connections appear to originate from legitimate local users rather than the threat actor's underlying infrastructure.

Combined with QScan and QTFY's botnet infrastructure, this provides an integrated ecosystem for identifying vulnerable systems, exploiting them, and obscuring subsequent malicious activity.

This approach can make traditional indicators such as source IP address and geographic location less reliable for defenders attempting to identify an intrusion.

RECOMMENDED ACTIONS

What Organizations Should Do

The joint advisory urges organizations to prioritize measures that reduce QTFY's ability to exploit internet-facing infrastructure.

Patch the edge
Apply the latest software and firmware updates to internet-facing systems.

Reduce exposure
Protect operational information from unintentional disclosure through internet-facing applications.

Isolate critical systems
Separate critical systems from edge devices so a compromised appliance is not a route inward.

Hunt historical activity
Use the indicators of compromise published by the FBI, NSA and CNMF to assess past activity.

THEN PLAN FOR WHAT COMES NEXT

QTFY's documented activity shows why organizations must also plan for what happens after an attacker bypasses perimeter defenses. The May 2024 campaign resulted not only in compromise, but in data being removed from hundreds of victim organizations.

> "A prevention-first strategy therefore needs to consider both sides of the attack: preventing attackers from getting in wherever possible and preventing sensitive data from getting out when other defenses fail."

THE BLACKFOG PERSPECTIVE

Protecting Data After Initial Compromise

No single security control can address every stage of an intrusion as sophisticated as QTFY.

BlackFog does not replace vulnerability management, patching, network segmentation, or controls designed to secure internet-facing infrastructure. These remain critical defenses against QTFY and are central to the recommendations contained in the joint advisory.

BlackFog provides an additional layer of protection at the point where compromised access can become a data breach.

BlackFog's anti data exfiltration (ADX) technology is designed to prevent unauthorized outbound data transfers from endpoints. When an attacker successfully establishes access and attempts to remove sensitive information, preventing that data from leaving the organization can limit the ultimate impact of the compromise.

QTFY provides a clear example of why this matters. In its May 2024 campaign, exploitation of vulnerable infrastructure ultimately resulted in data exfiltration from more than 300 organizations.

WHERE ADX FITS

Both Sides Of The Attack

KEEPING ATTACKERS OUT

Patching, segmentation and edge hardening remain the front line against QScan-driven exploitation.

KEEPING DATA IN

ADX blocks unauthorized outbound transfers on the endpoint, where persistence turns into exfiltration.

LIMITING IMPACT

When perimeter defenses fail, stopping the data leaving is what separates an incident from a breach.

ABOUT BLACKFOG

Real-Time, On-Device, Data Exfiltration Prevention

BlackFog helps organizations reduce modern cyber risk by stopping data exfiltration, the common factor behind ransomware, insider threats, zero day attacks, and Shadow AI exposure. Our anti data exfiltration (ADX) platform delivers real-time, on-device prevention. It stops sensitive data from leaving endpoints and networks without authorization and blocks ransomware communication, data theft, and AI driven leakage before damage occurs. By focusing on prevention instead of just detection, BlackFog helps organizations strengthen compliance, protect privacy, and improve operational resilience.