Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

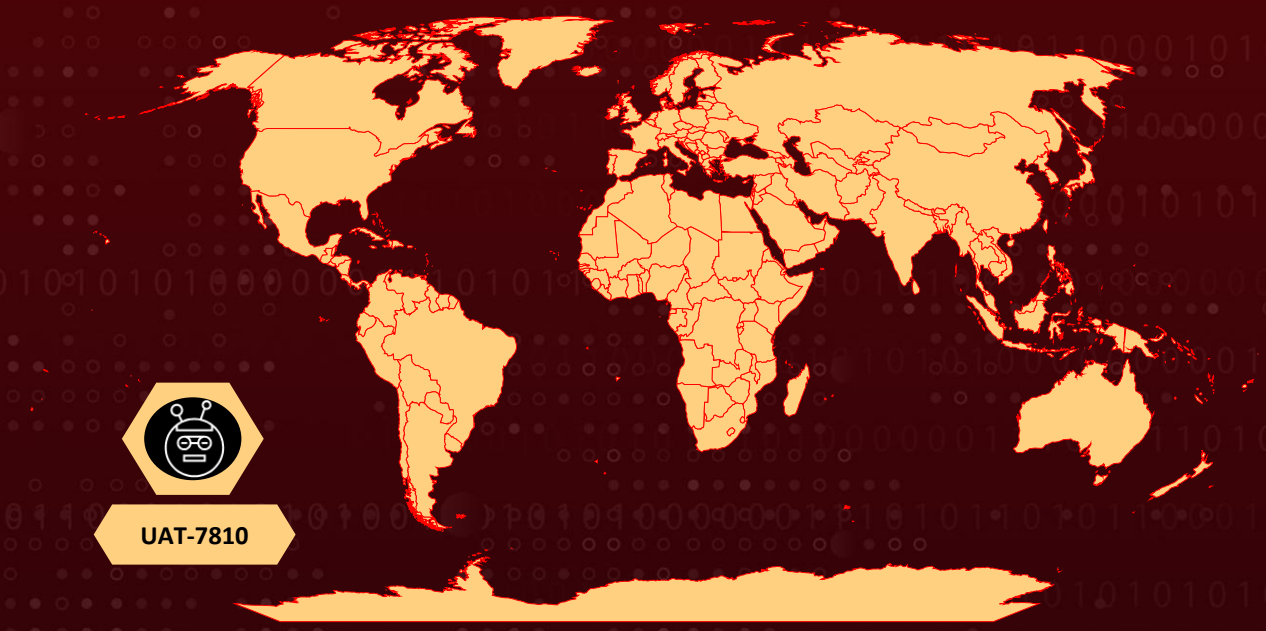
UAT-7810 Expands Its Arsenal with New LONGLEASH and DOGLEASH Malware

Date of Publication	Admiralty Code	TA Number
July 09, 2026	A1	TA2026191

Summary

First Seen: 2025
Targeted Regions: Worldwide
Targeted Platforms: Linux; embedded/IoT networking devices (MIPS, ARM, x64)
Targeted Products: Ruckus wireless routers
Threat Actor: UAT-7810
Malware: SHORTLEASH, LONGLEASH, DOGLEASH, LEASHTEST, JARLEASH
Attack: UAT-7810 is a China-nexus APT that builds and maintains an Operational Relay Box (ORB) network, which other China-aligned actors then use to hide the origin of their own attacks. The group breaks into internet-facing networking devices, mainly unpatched Ruckus routers, by exploiting known (n-day) vulnerabilities, then deploys custom Linux malware to turn each device into a relay node. Its newest tools include LONGLEASH (an upgraded SHORTLEASH backdoor), the DOGLEASH passive backdoor, and the LEASHTEST testing utility.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-22653	Ruckus Unauthorized Image Signature Injection Vulnerability	Ruckus Wireless Networking Devices	✗	✗	✓
CVE-2020-22658	Ruckus Unauthorized Image Boot Vulnerability	Ruckus Wireless Networking Devices	✗	✗	✓
CVE-2023-25717	Multiple Ruckus Wireless Products CSRF and RCE Vulnerability	Ruckus Wireless Admin	✗	✓	✓

Attack Details

#1

UAT-7810 gains its first foothold by targeting internet-facing networking hardware, primarily Ruckus wireless routers that have not been patched. Rather than relying on phishing or stolen credentials, the group weaponizes publicly known (n-day) vulnerabilities in these devices, including CVE-2020-22653, CVE-2020-22658, and CVE-2023-25717. The last of these allows unauthenticated remote code execution through a crafted HTTP GET request, giving the attacker direct command execution on the device without any login. Activity observed earlier this year also reached into ASUS AiCloud routers vulnerable to CVE-2025-2492, suggesting the group is looking to broaden the range of hardware it can recruit into its relay network.

#2

Once a device is compromised, UAT-7810 runs a shell script that downloads its DOGLEASH backdoor from attacker-controlled servers, adds firewall (iptables) rules so inbound traffic can reach a chosen port, and then launches the malware. DOGLEASH sits quietly listening on that local port, decrypts incoming requests using a hardcoded password, and acts on command codes to run shell commands, read or back up files, gather operating-system details, or execute code directly in memory. On more capable devices the group deploys LONGLEASH, an upgraded version of its older SHORTLEASH backdoor that shares the same codebase (internally named "ff-agent"). LONGLEASH is built for stealth and performance, disguises its traffic with a fake Windows Chrome browser identifier, and will wipe itself and its traces from the device if it detects tampering. A Java-based administrative tool, JARLEASH, is also used on some servers to manage files and provide easy remote access.

#3

UAT-7810's goal on each device is not to move deeper into a single victim network but to convert the device into a node in its wider ORB relay infrastructure. LONGLEASH can proxy and redirect traffic across HTTP, DNS, SOCKS, TCP, ICMP, and UDP, set up and manage network tunnels, and even act as an intermediate command-and-control server that relays instructions and data between the primary C2 and other infected nodes. By chaining compromised devices together this way, the group provides secondary China-nexus actors, such as UAT-5918, with regional infrastructure that makes their attacks appear to come from legitimate local systems and complicates attribution.

#4

Because the compromised devices function as relay and tunneling points, data movement is handled through LONGLEASH's encrypted channels rather than a single smash-and-grab exfiltration step. The implant uses TLS with public-key infrastructure and x509 certificates (built on the MbedTLS library) to secure its communications, and the operators stood up TLS services on non-standard ports using a distinctive certificate. DOGLEASH's file-read and backup commands and JARLEASH's FTP, SFTP, and web-based file management give the operators direct ways to stage and retrieve files from a compromised host. The LEASHTEST utility, meanwhile, is a non-malicious test binary the group uses to confirm that MIPS-based devices can support the functions LONGLEASH needs, indicating the toolset is still under active development.

Recommendations

Patch Vulnerable Ruckus Devices: Apply the vendor firmware updates for CVE-2020-22653, CVE-2020-22658, and CVE-2023-25717 immediately, prioritizing any internet-facing Ruckus wireless devices. Where a device is end-of-life and cannot be patched, disconnect it from the internet.

Retire and Replace End-of-Life Hardware: Inventory networking hardware for models that no longer receive security updates and replace them, since unpatchable devices are exactly the targets UAT-7810 recruits into its relay network.

Block Known Malicious Infrastructure: Block the attacker download and C2 IP addresses and URLs listed in the IoC section at the perimeter, and alert on any historical connections to them.

Hunt for the Malware Footprint: Search endpoints and networking devices for the file hashes provided, for unexpected listening TCP ports created by unfamiliar iptables rules, and for outbound TLS connections on non-standard ports such as 99 and 2222.

Deploy Vendor Detection Coverage: Enable the published network intrusion and antivirus/ClamAV signatures for this cluster so that DOGLEASH, LONGLEASH, and JARLEASH samples are detected on sight.

Inspect for Anomalous Proxy and Tunneling Traffic: Monitor for devices generating proxy or tunneled traffic across HTTP, DNS, SOCKS, ICMP, and UDP, especially where a networking appliance suddenly relays connections it never handled before, which is a hallmark of ORB relay behavior.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.003: Virtual Private Server
	T1587: Develop Capabilities	T1587.001: Malware
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004:Unix Shell
	T1620: Reflective Code Loading	
Defense Evasion	T1562: Impair Defenses	T1562.004: Disable or Modify System Firewall
	T1070: Indicator Removal	T1070.004: File Deletion
Discovery	T1082: System Information Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001.001: Web Protocols
	T1090: Proxy	T1090.003: Multi-hop Proxy
	T1572: Protocol Tunneling	
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
	T1105: Ingress Tool Transfer	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1b5649b479fd625de5c8120873644b5eb669cc89cd504582c18e0ae350fd8823, 755fcee1337a252203002ecfdf673a08cfadeda8d738bef2d518a08e0626aa4f, e799d72929d7ccc7f6b6109742b8cc482838303207efc989543b6e1ca6d16e9c, 3b89d183eb014e29d9d0d4e45fc2b784a7fcfcf31dd48fd3bde30f8d956383d1, 324d95024fc8da5c92b5a1f4825aed5a2a91c9ca8fb6aa52abb332a4c9cf4257, bafba443170e54ef7fd431ce7f1b5e202719f3fd022e4ef70788904f574d2cdf, c2ab9adaba93ff094b8f3fc37d906014d870582039d276b7bd03e6fd583d8a15, 604b53f87d6c070bf387e80c70a6df8d272fa3fc143148d41f13e59d52ab1f13, c92541f273eeb576d39235d0a5c6f18f2574b132a1022598edfa38065783ab98, 29c7fccc6ef8cbfe4da9a169c7c74bacaea1fb515a1fddef91ab1b1522f76e4c, 425bf771c8c9f740b1ae9803dcb4fd45af4d6a6f171fcc72fc7d511095ca82ce, ac8eae94d27122f4751bc96d9ea52d30000b7ca37569a2291b2710824ca3396f, dc4f25b2247cfdd6fc96848db30a178baa4419a4c854e86e315b465836102d14, 3878dd5c8eba1e5b53ab2e07e7b5482e95a3fd3e98268bcd7861318bc9902376, 9b9e0e5a1eb469b8d20dc23351e08ff5d5731e1cedce0ddee9bbd00a76217f13, 57bdab2ba4b05ec0338c06632599393d5b14227f31a43fe950ea8fdd47428715, b8d247fd1fb85d24a17afeec3815906dfbcdc5359647910b4a153900ec999a0f,

TYPE	VALUE
SHA256	5e225ea2648a8cba0fd94ec7fd8ce5315f5d0cc2922bafc9db3c8c41280e917c, d5cf7315186a78ab6a7475c338bdf101bc6461930aaa7a012a02cf93f347c207, dd0fc1a88180fde8367bec7086f99294f36b8332f12994293139ed532d2ebbac, 5c3f190571645c4641dcff2c07a4c3ab9acad06aa9607350a385729d8d6139f1, 323c3a91be60ebc3e06e942bad04899a15911cea23269e43d07829164b2ce5d4, 880425fee707e9f42e0b8d60119ed639b1ad506ea29877d126bdebce379cd229, e5d2de8ae98579bfb940290f60e59a502b3065345aaf765456387989c0488b20, 2e0e43776e2e1a37d882a1b2ebb7d337ee88950177e43831dae645a367824feb, b5969636eec376ad6c3ece2202b1722219955638e09b6f96d4cfc0598d3b1890, 1660536f448b8b9f086ce9ea3ce4e9deefc59a76711ea53ee6d8f08fc8c1bb99, 65feba2c971c214e71303ad2e0fbf62b45ebcaa784cbf3d0dab62786cb4c0469, 53ac2b231c23d41234e55b1f7ed89f86234f785adbbe820959655d7b019d7df9, 33c10b77e1da9f0679023d55fb3057879d15609db9c1d46ee5c3ff1240a3d052, 5faea1650cac0f3ffd2dc1fb220182095a46e34158967d37c2a942e85e2ca97b, 62d4ec87ed21f0d15cb769b0b2a5577cab41fc2cdb1e7e796c5bdff09264dd9a, 534a4a5bff2609a2d6e088cb87465c08c2d69c6aaa7d2ffcbcd491274b8505f1, 5eab4c61baa67ae2838a36c2e6ff0476a8f2117b96a7027b830c8cb46ce78efc, 0af4c52a1d13e4132a1843ce7727abcf0ddd4d1ca6a4b17cdf599ec3f355c241, d4861088161fc72b9922abf933b4ea664a807105ec1eab4a173253aa60bfe6d7,

TYPE	VALUE
SHA256	3d296af7f29c0425655bd1cc0be48fe4aba52ee6760a89e805ca2589f4ef4d77, f235d2e044c2f7814e6bbcd835b9fd9f10f227dacfb9396185ec2013e7df4db4, 4130f49fa81a699a667cafdbd6d1f6e781edd686c947eb8ae27134f6dc2c43d7, 0a8555a71868749be8c905ed53296ce335af50a9262772b5e154ad3f9c35c2e4, 5dbfa033676b5caacfae902734ce462cd871181eefbe299250ca8ac7e139719e, 20fcba222f74dd68aaeb1f0ad30cdf702a828ee164a182b30d05d600c35b72d9, 912adea5339c73cb4a777a3e9f98bf3cb08da6622c9dd3b4cc9b083cb03d10a2, 03926e3da998f32ad898b640bd15cf145768f9e849e6f18d81350234254c424e, 16971f9706d70ac4925651c7c8719b9d77aff63e4c0a618129efc32c2c46b989, 6917c0f9eafefe42e33e791b75a7e503ff8b081bc10a98449e4076787dfc6c16, c7c9bfa9ffcd8fb6a2afe656f510c406ddc58ebff48ce1d0fd3fad951b46a36e, b9fe48bda9a6c8787981a24f8bbc723a6f6aa80cab5fa53481937382f3c6ce85, f3fbf4481f30fd840f35568746f54be49eb92b2c9ac95597a7760abb171cb54b, 6366d59b573d50fd23ff650923c4a8c1c918518a02d0a56f12c23533c45f439d, 3fcaa3038e365b6ab0b121e2cd319c56b74e37381943a0da0e8dce407087cdb8, bf70c6f3a8e913f526ec57eeec50e1306f7b34b037915b7a1cf2968cc46acc58, 0352f3e338261d98895df4c7b7a76b296485b2290c72bce56603351d167d0601, 52b871429833e1dee348263844efb531f6a3fcd321f88dc8a876caaee912cedd, 5db2ce9acd50f96d566e8d139f6490abf2bbf7a9293b876eeb4598fd2c37c515,

TYPE	VALUE
SHA256	3169a6dbcce684e2c5a2f166996b58ffa673df6e58b8edf2bdf3e66271c8c69e, d871d76171504597bbda387689e12e7a5e354c360ff135f4df231cec68c761af, d1f963b88672f3676a7da1580262ba0d4f367cc57a94b551754c20f77a670c43, 76d9e2a2ff313f5b91cc67aab1127122baee1c3efbae1087e58a25bc5f1eb065, 8c104da0e66ef6384663309aaf8fb49f549f2785d835eec620b265f8aa11d9f0, c494c878e28284539419612616d964ab9224cbe27e57f42293d91d02d684e3db, 08701ed7975bf4f5688c2724d27ab497764200ad6f4dc53d3cc03b170378ced0, 0a8cae96e25e85c612b0736fe886f9b124ad70ec425bc2ec1a8a4135b25436ba, 8459ff264a2c81c68a34c4ee6bc109d141ad28b96037d34ff112322a4c853739, 68445a37a9943a267a8b2100fba2678353d6ec88844505ccbba659e586c7a105, 29686c933cec1e274467e2dae264625ae6f754824bb7f550bc9c3131f625562c, d973ad5a80c3d7468a9c392db4166857ed32b5d61cd6755766ba8922156dada3, f5a57dfae488d9dfe260b32460a1d947fb5af58ceaf2fb0139bc08b4bb79a966, 2ebc1b6cf543e2cb3f22d9a5b54b6676bb71dde98df7532f8791297734e44fdd, 6dbd507ca7cecea861f9cf704b3c5c37f5bd5392886a8c2562088892b7703fa5, 89f0a67bc595ab8bce02c2f95f9292ad06e1868207e809c76bd16f0cab800c06, d81201d0fc19977e51104438a5b9cba861f4da20cea3ae9183edf16ab11d98f8, 9d52cb4febf3342c34dcc8198dcaf453458be3699ab47dc08616aa7f18daa7fa, 9a927c37a31b80975c5c5467f112b61478c9493c0462810464435253358a5acb0,

TYPE	VALUE
SHA256	6cda1e81667f869940401f05a55c8dea94dbdf3ceffb93b5f320a6462cfea44d, 745538dea8ed9aec4466e67a9d0aecf9e7026ff16a792d1d6f306e8b67d3f34c, 13acadb3541e75af50e02d5be56c2238b93d8f154ce5514be1558e6ee59a1432
IPv4	194[.]233[.]92[.]26, 217[.]15[.]160[.]247, 217[.]15[.]164[.]147, 95[.]182[.]100[.]231
URLs	hxxp[:]//217[.]15[.]160[.]247[:]8088/, hxxp[:]//217[.]15[.]160[.]247[:]2222/, hxxp[:]//217[.]15[.]160[.]247[:]99/, hxxp[:]//194[.]233[.]92[.]26[:]8088/, hxxp[:]//194[.]233[.]92[.]26[:]2222/, hxxp[:]//217[.]15[.]164[.]147[:]99/, hxxp[:]//217[.]15[.]164[.]147[:]8088/, hxxp[:]//217[.]15[.]164[.]147[:]2222/, hxxp[:]//95[.]182[.]100[.]231[:]2222/

Patch Links

CVE-2020-22653: https://support.ruckuswireless.com/security_bulletins/302

CVE-2020-22658: https://support.ruckuswireless.com/security_bulletins/302

CVE-2023-25717: https://support.ruckuswireless.com/security_bulletins/315

References

https://blog.talosintelligence.com/uat-7810/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 09, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com