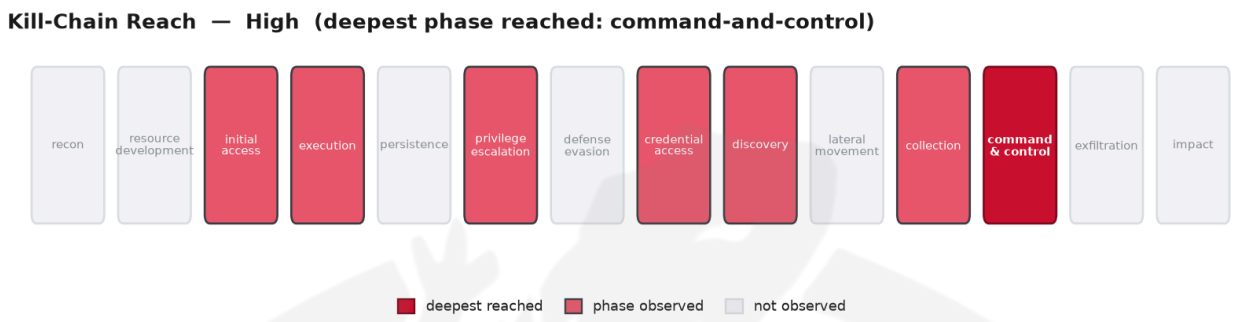
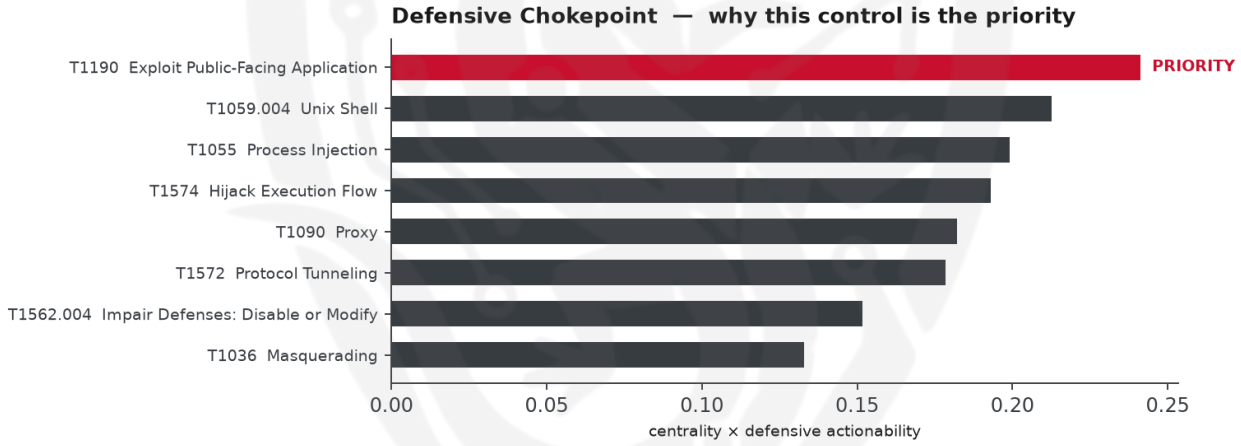
THREAT REPORT: UAT-7810

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The source attributes this activity to UAT-7810, a threat actor utilizing various malware families, including SHORTLEASH, LONGLEASH, DOGLEASH, JARLEASH, and LEASHTEST, to exploit vulnerabilities such as CVE-2020-22653. The targeted country and sectors are not specified due to insufficient data. Priority should be given to patching CVE-2020-22653 on all affected systems to mitigate the threat. The actor's use of these malware families and exploitation techniques poses a significant risk, requiring immediate attention to defensive measures.

Threat Overview

UAT-7810 is exploiting the CVE-2020-22653 vulnerability using malware families such as SHORTLEASH, LONGLEASH, DOGLEASH, JARLEASH, and LEASHTEST. The threat actor is targeting unspecified countries and sectors, leveraging techniques including system owner/user discovery, keylogging, and

system information discovery. The central vulnerability exploited is CVE-2020-22653, with other CVEs cited as well.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, starting with system owner/user discovery and progressing through keylogging, system information discovery, and exploitation of public-facing applications. The priority technique identified is T1190 Exploit Public-Facing Application, which serves as a critical chokepoint in the attack chain. To counter this, the priority action is to: Patch CVE-2020-22653 on all affected systems as the top priority, then: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Infrastructure and Corroboration

There is no available information on hosting providers or ASNs observed in relation to this threat. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1033 System Owner/User Discovery
- T1056.001 Keylogging
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1036 Masquerading
- T1055 Process Injection
- T1572 Protocol Tunneling
- T1562.004 Impair Defenses: Disable or Modify System Firewall
- T1090 Proxy
- T1083 File and Directory Discovery
- T1049 System Network Connections Discovery
- T1059.004 Unix Shell
- T1574 Hijack Execution Flow
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1095 Non-Application Layer Protocol
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.2413).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4212; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Velvet Ant	0.4212
Windigo	0.4029
Ke3chang	0.3761
Tropic Trooper	0.3704
FIN13	0.3693

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator
Hash	0352f3e338261d98895df4c7b7a76b296485b2290c72bce56603351d167d0601
Hash	03926e3da998f32ad898b640bd15cf145768f9e849e6f18d81350234254c424e
Hash	08701ed7975bf4f5688c2724d27ab497764200ad6f4dc53d3cc03b170378ced0
Hash	0a8555a71868749be8c905ed53296ce335af50a9262772b5e154ad3f9c35c2e4
Hash	0a8cae96e25e85c612b0736fe886f9b124ad70ec425bc2ec1a8a4135b25436ba
Hash	0af4c52a1d13e4132a1843ce7727abcf0ddd4d1ca6a4b17cdf599ec3f355c241

Type	Indicator
Hash	13acadb3541e75af50e02d5be56c2238b93d8f154ce5514be1558e6ee59a1432
Hash	1660536f448b8b9f086ce9ea3ce4e9deefc59a76711ea53ee6d8f08fc8c1bb99
Hash	16971f9706d70ac4925651c7c8719b9d77aff63e4c0a618129efc32c2c46b989
Hash	1b5649b479fd625de5c8120873644b5eb669cc89cd504582c18e0ae350fd8823
Hash	20fcba222f74dd68aaeb1f0ad30cdf702a828ee164a182b30d05d600c35b72d9
Hash	29686c933cec1e274467e2dae264625ae6f754824bb7f550bc9c3131f625562c
Hash	29c7fccc6ef8cbfe4da9a169c7c74bacaea1fb515a1fddef91ab1b1522f76e4c
Hash	2e0e43776e2e1a37d882a1b2ebb7d337ee88950177e43831dae645a367824feb
Hash	2ebc1b6cf543e2cb3f22d9a5b54b6676bb71dde98df7532f8791297734e44fdd
Hash	3169a6dbcce684e2c5a2f166996b58ffa673df6e58b8edf2bdf3e66271c8c69e
Hash	323c3a91be60ebc3e06e942bad04899a15911cea23269e43d07829164b2ce5d4
Hash	324d95024fc8da5c92b5a1f4825aed5a2a91c9ca8fb6aa52abb332a4c9cf4257
Hash	33c10b77e1da9f0679023d55fb3057879d15609db9c1d46ee5c3ff1240a3d052
Hash	3878dd5c8eba1e5b53ab2e07e7b5482e95a3fd3e98268bcd7861318bc9902376
Hash	3b89d183eb014e29d9d0d4e45fc2b784a7fcfcf31dd48fd3bde30f8d956383d1
Hash	3d296af7f29c0425655bd1cc0be48fe4aba52ee6760a89e805ca2589f4ef4d77
Hash	3fcaa3038e365b6ab0b121e2cd319c56b74e37381943a0da0e8dce407087cdb8
Hash	4130f49fa81a699a667cafdbd6d1f6e781edd686c947eb8ae27134f6dc2c43d7
Hash	425bf771c8c9f740b1ae9803dcb4fd45af4d6a6f171fcc72fc7d511095ca82ce
Hash	52b871429833e1dee348263844efb531f6a3fcd321f88dc8a876caaee912cedd
Hash	534a4a5bff2609a2d6e088cb87465c08c2d69c6aaa7d2ffcbcd491274b8505f1
Hash	53ac2b231c23d41234e55b1f7ed89f86234f785adbbe820959655d7b019d7df9
Hash	57bdab2ba4b05ec0338c06632599393d5b14227f31a43fe950ea8fdd47428715
Hash	5c3f190571645c4641dcff2c07a4c3ab9acad06aa9607350a385729d8d6139f1
Hash	5db2ce9acd50f96d566e8d139f6490abf2bbf7a9293b876eeb4598fd2c37c515

Type	Indicator
Hash	5dbfa033676b5caacfae902734ce462cd871181eefbe299250ca8ac7e139719e
Hash	5e225ea2648a8cba0fd94ec7fd8ce5315f5d0cc2922bafc9db3c8c41280e917c
Hash	5eab4c61baa67ae2838a36c2e6ff0476a8f2117b96a7027b830c8cb46ce78efc
Hash	5faea1650cac0f3ffd2dc1fb220182095a46e34158967d37c2a942e85e2ca97b
Hash	604b53f87d6c070bf387e80c70a6df8d272fa3fc143148d41f13e59d52ab1f13
Hash	62d4ec87ed21f0d15cb769b0b2a5577cab41fc2cdb1e7e796c5bdff09264dd9a
Hash	6366d59b573d50fd23ff650923c4a8c1c918518a02d0a56f12c23533c45f439d
Hash	65feba2c971c214e71303ad2e0fbf62b45ebcaa784cbf3d0dab62786cb4c0469
Hash	68445a37a9943a267a8b2100fba2678353d6ec88844505ccbba659e586c7a105

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** 32 of 170 documented groups that use Exploit Public-Facing Application also use Valid Accounts (conditional 0.73, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The adversary, UAT-7810, could pivot to using T1078 Valid Accounts if they have previously compromised or have access to credentials, which would likely allow them to maintain access and achieve their objectives despite the block on exploiting public-facing applications. They may attempt to use these valid accounts to move laterally within the network or access sensitive resources. To counter this, the mandated defensive control of Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons should be implemented.

Also plausible (same tactic): T1133 External Remote Services (n=17, lift 2.3), T1199 Trusted Relationship (n=9, lift 2.9)

Detection and hardening for the pivot (T1078 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry

- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)
  - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
  - Service or dormant accounts logging on interactively
  - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
  - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
  - Least-privilege review; separate admin from daily-driver accounts
  - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account