FULL REPORT • CREDENTIAL THEFT • MONOGRAPH 72 / 71 • 21 MIN READ

Microsoft Entra App-Role Abuse, AntiFox Overlaps, and OTP Autosecure Kits

Comparing enterprise Microsoft Entra app-only ROPC token minting and Host AF-01 overlaps against an 842-entry OTP and Playwright workbench

BY
Odin by Brandefense

PUBLISHED
19 November 2026

READING TIME
21 min read

EDITION
Version 1.1 · TLP:CLEAR

SCOPE
Prepared November 2026

1. Executive Summary

IN SHORT

Across evidence dated 13–27 November 2026, Odin by Brandefense matched 1 of 5 AntiFox/ARTEX IPv4s from a 20 November Entra report to Host AF-01. We also analyzed an unlinked 842-entry Autosecure server on TCP 8899. Retire Exchange full_access_as_app, require MFA to prevent ROPC, and enforce FIDO2 MFA.

Identity attacks split into two clear tracks based on what an attacker holds first. Monograph 60 covered seven-tool console growth and Storm-0940 or ZQAgent overlaps. By contrast, Monograph 72 examines Microsoft Entra application-only permission abuse alongside an 842-entry OTP and OAuth Autosecure workbench.

Across evidence dated 13–27 November 2026, Odin by Brandefense studied both tracks side by side. Zero IPv4s, TLS certs, or files link Host AF-01 to Workbench B; we compare them side by side to contrast workload-identity abuse with OTP session hijacking. We publish zero IPv4s, zero SHA-256 hashes, and zero captured user filenames.

1 **Broad Entra app roles allow five-minute ROPC token minting.**
On 20 November 2026, Abnormal Security reported an intrusion in a U.S. financial-services Microsoft Entra tenant. An operator abused an Entra app holding app-only user creation and Exchange Online `full_access_as_app`. The operator created short-lived users, requested internal API tokens via OAuth 2.0 ROPC, and disabled the users in roughly five minutes.

2 **One of five published AntiFox/ARTEX IPv4s matched a cloud ARTEX candidate.**
Sign-in and reset calls in the 20 November report came from five IPv4s (four labeled AntiFox and one ARTEX). Abnormal Security noted that the data does not show either tool ran the Entra calls directly. One IP matched Host AF-01 on Google Cloud `AS396982` (`TCP 80` on 19 November; `TCP 443` on 25-26 November), beside 6,343 ARTEX and 3,648 CyberStrikeAI candidate records.

3 **Workbench B exposes 842 staged entries for OTP bots and Playwright state.**
Recorded on 19-20 November 2026 on `TCP 8899` of a Germany VPS (first seen 13 November), Workbench B held 842 deduplicated entries. Six hundred fourteen sized files totaled 316,723,715 bytes, paired with 228 unsized items. Staged files hold a 298.9 MB Autosecure tar archive, 129 Discord OTP bot files, 36 OAuth script items, and 432 Playwright profile items.

4 **Both tracks defeat six-digit OTP checks through token or lure paths.**
In Microsoft Entra, app-only Graph roles and ROPC password grants mint user API tokens without prompting staff phones. On Workbench B, staged Discord modals and headless Chromium folders are built to collect live OTP codes and save login state on disk.

Three Decisions for Security Leaders

1. **Retire Exchange `full_access_as_app` and prevent OAuth 2.0 ROPC.** Audit all Entra apps holding `User.ReadWrite.All`, `RoleManagement.ReadWrite.Directory`, or `full_access_as_app`, and move mail apps to scoped Exchange RBAC. Block legacy authentication and require MFA for all users in Conditional Access so ROPC cannot complete, and lock workload tokens to trusted IPs and certs.
2. **Join cloud user creation, ROPC sign-ins, and fast disables in SIEM.** Alerts built only for permanent rogue users miss short-lived accounts disabled in five minutes. Run 10-minute joins

across Entra `AuditLogs` and `SigninLogs` to flag app-created users that sign in via ROPC and disable right away.

3. **Require `FIDO2` passkeys and block high-port server egress.** Replace SMS, email codes, and six-digit app codes on key portals with domain-bound FIDO2 passkeys or keys. Block server egress to high ports such as `TCP 8899` and alert on rogue Playwright folders.

The Study in Numbers

Number	What it is
5	AntiFox/ARTEX-linked IPv4s (4 AntiFox, 1 ARTEX) published by Abnormal Security on 20 November 2026 (1 matched Host AF-01; 4 unmatched).
6,343	Cumulative ARTEX candidate records through 26-27 November 2026 (up 1,800 from 4,543 on 15 November; 4 verified controllers).
3,648	Cumulative CyberStrikeAI candidate endpoint records observed through 26-27 November 2026.
842	Deduplicated entries on Workbench B (`TCP 8899` , Germany VPS, 19-20 November 2026): 614 sized (316,723,715 B) and 228 unsized.
432	Entries inside 16 headless Playwright Chromium folders (**27** items per folder, **1,265,772** bytes) on Workbench B.
129	Entries across 3 mirrored 43-entry Discord OTP bot trees (**239,408** B) beside 36 OAuth/OTC items (**122,132** B).
0	Published blocklist IPv4s, SHA-256 hashes, or Cluster 5 user filenames (**83** user items, **13,968,406** B withheld).

2. Microsoft Entra App-Role Abuse, ROPC Minting, and Host AF-01 Overlap

While Monograph 60 examined seven-tool console growth and Storm-0940 or ZQAgent cases, this section studies cloud workload-identity abuse (`[REF-04]`). When an app holds broad directory

rights and password grants stay open (`[REF-03]`), an operator can mint user API tokens without touching staff laptops.

On `20 November 2026` , Abnormal Security published its study of a breach in a U.S. financial-services Microsoft Entra tenant (`[REF-01]`). Teams can use cyber threat intelligence to link external console exposures with cloud sign-in spikes before revoking abused keys. Figure 1 compares that Entra track with the unlinked **842**-entry `Autosecure` server in Section 3.

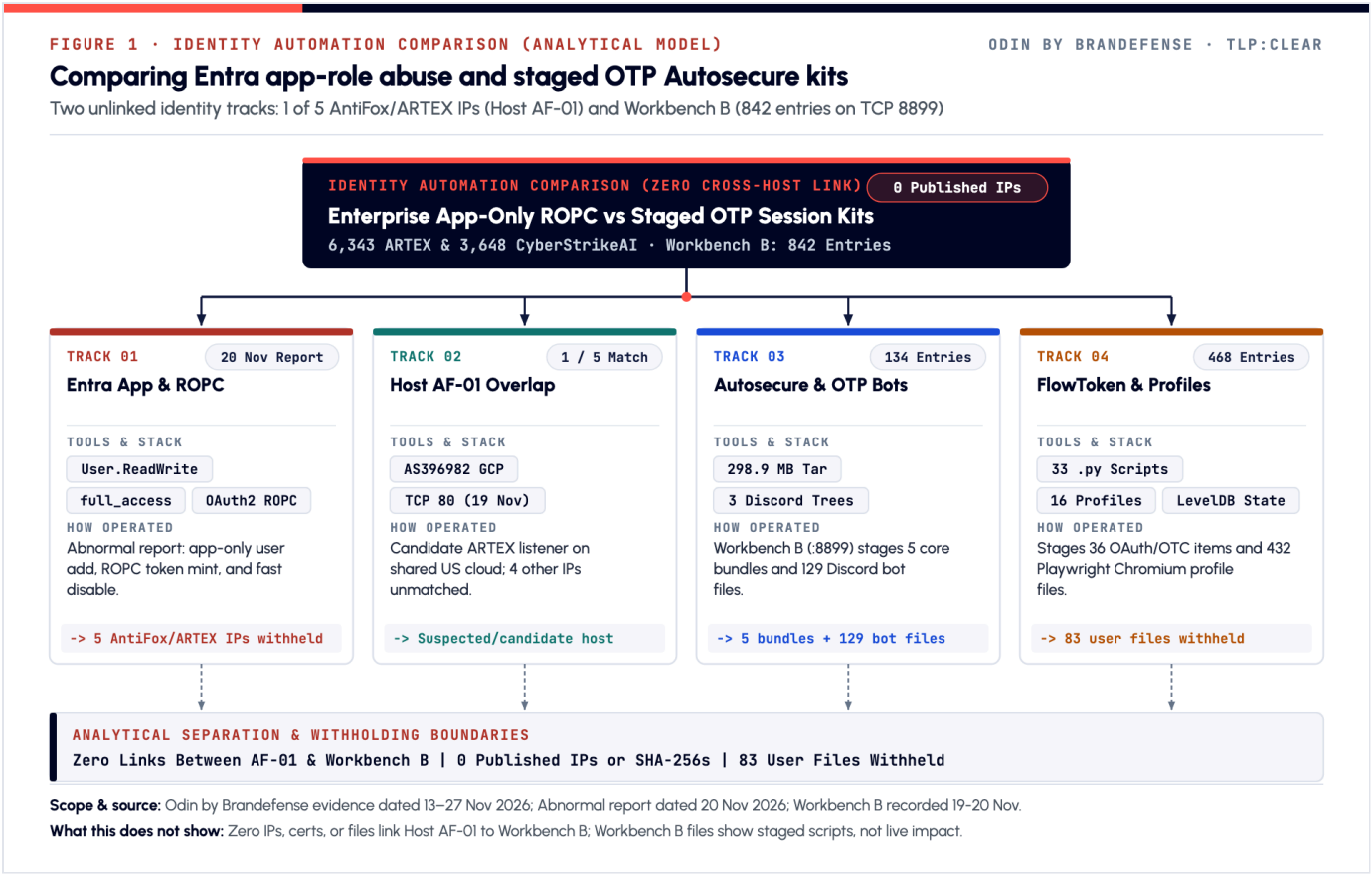

Figure 1: Comparing Entra app-role abuse and staged OTP Autosecure kits

How the Five-Minute Disposable ROPC Chain Worked (`[REF-01]`)

In the `20 November 2026` case (`[REF-01]`), an operator abused an over-privileged Microsoft Entra app inside a U.S. financial-services tenant. Instead of phishing a worker, the operator chained three built-in cloud features:

1. **Broad app-only roles.** The app held **application-only permissions** that run without a signed-in user. Those roles covered user creation (`User.ReadWrite.All` , `[REF-04]`) and Exchange Online `full_access_as_app` (`[REF-01]` , `[REF-02]`). Unless replaced by Exchange RBAC for Applications (`[REF-02]`), `full_access_as_app` opens every mailbox in the tenant.

2. **Short-lived users and ROPC login (`T1136.003` , `[REF-07]`).** App-only tokens often fail when internal APIs require user scopes. The operator created temporary cloud users (`[REF-07]`) and signed in via **OAuth 2.0 ROPC (`grant_type=password`)** at `/oauth2/v2.0/token` (`[REF-01]` , `[REF-03]`). ROPC sends raw passwords in a direct `POST` call and skips interactive MFA prompts (`[REF-03]`).
3. **Fast disablement (`[REF-01]`).** After getting internal business API tokens, the operator disabled each temporary user within roughly **five minutes**. The defender stopped the activity by removing `full_access_as_app` , deleting the app keys, and revoking live sessions (`[REF-01]`).

Checking the Five Published `AntiFox` / `ARTEX` IPv4s (`Host AF-01`)

Sign-in and reset calls in the `20 November 2026` report came from **5 `AntiFox` / `ARTEX` IPv4s** (**4** labeled `AntiFox` and **1** `ARTEX` , `[REF-01]`). Abnormal Security noted (`[REF-01]`) that traffic from `AntiFox` / `ARTEX` -linked hosts does **not** show either tool ran the Entra calls directly. Pairing dark web monitoring with cloud audit checks helps teams spot leaked client secrets early.

Metric or group	Count	Share / delta	Provenance & dates	IP status
Disclosed `AntiFox` / `ARTEX` IPv4s (`[REF-01]`)	5	100.0 %	Published by Abnormal Security on `20 November 2026` (4 `AntiFox` , 1 `ARTEX`).	Withheld (0 IPs)
Matched host (`Host AF-01`)	1	20.0 %	`Google Cloud` (`AS396982` , `US`): suspected `ARTEX` on `TCP 80` (`19 Nov`); candidate on `TCP 443` (`25-26 Nov`).	Withheld (0 IPs)
Unmatched disclosed IPs	4	80.0 %	No observed `ARTEX` or `CyberStrikeAI` panel across `13-27 Nov 2026` .	Withheld (0 IPs)

Metric or group	Count	Share / delta	Provenance & dates	IP status
`ARTEX` baseline (`15 Nov`)	4,543	Baseline	Cumulative `ARTEX` candidate count as of `15 November 2026`.	Withheld (0 IPs)
`ARTEX` total (`26-27 Nov`)	6,343	+1,800 (+39.6%)	Cumulative `ARTEX` candidate records (4 verified controllers).	Withheld (0 IPs)
`CyberStrikeAI` total	3,648	Peer count	Cumulative `CyberStrikeAI` candidate records through `26-27 Nov`.	Withheld (0 IPs)

Three points stand out in Table 1. First, Odin by Brandefense flagged `Host AF-01` (`Google Cloud AS396982`, United States) on `TCP 80` on `19 November 2026`. We then saw an open `ARTEX` candidate listener on `TCP 443` on `25-26 November 2026`. Because `Host AF-01` sits on shared cloud space without a C2 beacon capture, we treat it as a candidate host and withhold its IP.

Second, **4** of the **5** published IPs (**80.0%**) showed no web panel. Blocking console ports alone misses token calls sent from headless cloud VMs. Third, cumulative `ARTEX` candidate records rose from **4,543** on `15 November` to **6,343** on `26-27 November 2026` (**+1,800**, or **+39.6%**), beside **3,648** `CyberStrikeAI` records.

3. Inside Workbench B: 842 Staged Entries on TCP 8899

While `Host AF-01` provides enterprise API-role context, `Workbench B` shows how operators stage OTP lure bots, OAuth scripts, and browser state (`T1111`, `[REF-08]`). Zero IPv4s, TLS certs, or files link `Host AF-01` to `Workbench B`.

First seen on `13 November 2026` and recorded on `19-20 November 2026`, `Workbench B` ran on a Germany VPS (`DE`, IP withheld). It exposed an open HTTP index (`Directory listing for /`) on `TCP 8899`. Figure 4 maps all **842** entries on the host.



Figure 4: Workbench B exposes 842 entries (316.7 MB) across six artifact groups

Three Workspace Zones and Six File Kinds (842 Entries, 316,723,715 Bytes)

The HTTP index on `TCP 8899` listed **842 entries**, matching **614 sized files (316,723,715 bytes)** and **228 unsized items**. `Workbench B` stages `autosecure-app.tar.gz`, three Discord OTP bot trees, **33** OAuth/OTC scripts, **16** Playwright folders, and **83** user pages. We therefore treat `Workbench B` consistently as an **adversary staging workbench**, while withholding its IP and all **83** user filenames.

Workspace zone on `Workbench B` (`TCP 8899`)	Entries	Share (%)	Sized	Unsized	Sized bytes	Byte share (%)
Playwright Chromium Profiles (16 Profiles)	432	51.3%	254	178	1,265,772	0.4%
Root `Autosecure` Archives, Scripts & Logs	281	33.4%	239	42	315,218,535	99.5%
Discord OTP Bot Trees (3 Trees)	129	15.3%	121	8	239,408	0.1%

Workspace zone on `Workbench B (TCP 8899)`	Entries	Share (%)	Sized	Unsized	Sized bytes	Byte share (%)
Total	**842**	**100.0%**	**614**	**228**	**316,723,715**	**100.0%**

Sixteen Playwright folders (**27** items each = **432** entries) form **51.3%** of all entries yet only **0.4%** of bytes. By contrast, the **281** root entries hold **99.5%** of bytes because `autosecure-app.tar.gz` measures **298,924,100** bytes. Table 3 splits the **842** entries across six file kinds.

File kind	Entries	Share (%)	Sized	Unsized	Sized bytes	Top extensions (count)
`text`	355	42.2%	343	12	14,865,918	`none` (126), `.json` (66), `.log` (63), `.html` (53), `.txt` (35), `.md` (3), `.ts` (2), other (7).
`other`	275	32.7%	92	183	7,893	`none` (255), `.db-journal` (16), `.err` (2), `.out` (2).
`script`	138	16.4%	138	0	645,829	`.py` (76), `.sample` (42), `.js` (15), `.sh` (5).
`data`	34	4.0%	33	1	1,245,307	`none` (16), `.db` (16), `.bak` (1), `.sql` (1).
`image`	33	3.9%	1	32	296	`.png` (25), `.jpg` (7), `.bin` (1).
`archive`	7	0.8%	7	0	299,958,472	`.gz` (3), packaged archives (4).
Total	**842**	**100.0%**	**614**	**228**	**316,723,715**	**Exact sum across all 6 file kinds.**

Six Functional Staging Clusters on `Workbench B`

Table 4 and Figure 5 divide all **842** entries into six mutually exclusive clusters. Playwright folders (**432**), setup and ops logs (**157**), and Discord OTP bots (**129**) form **718 of the 842 entries (85.3%)**.

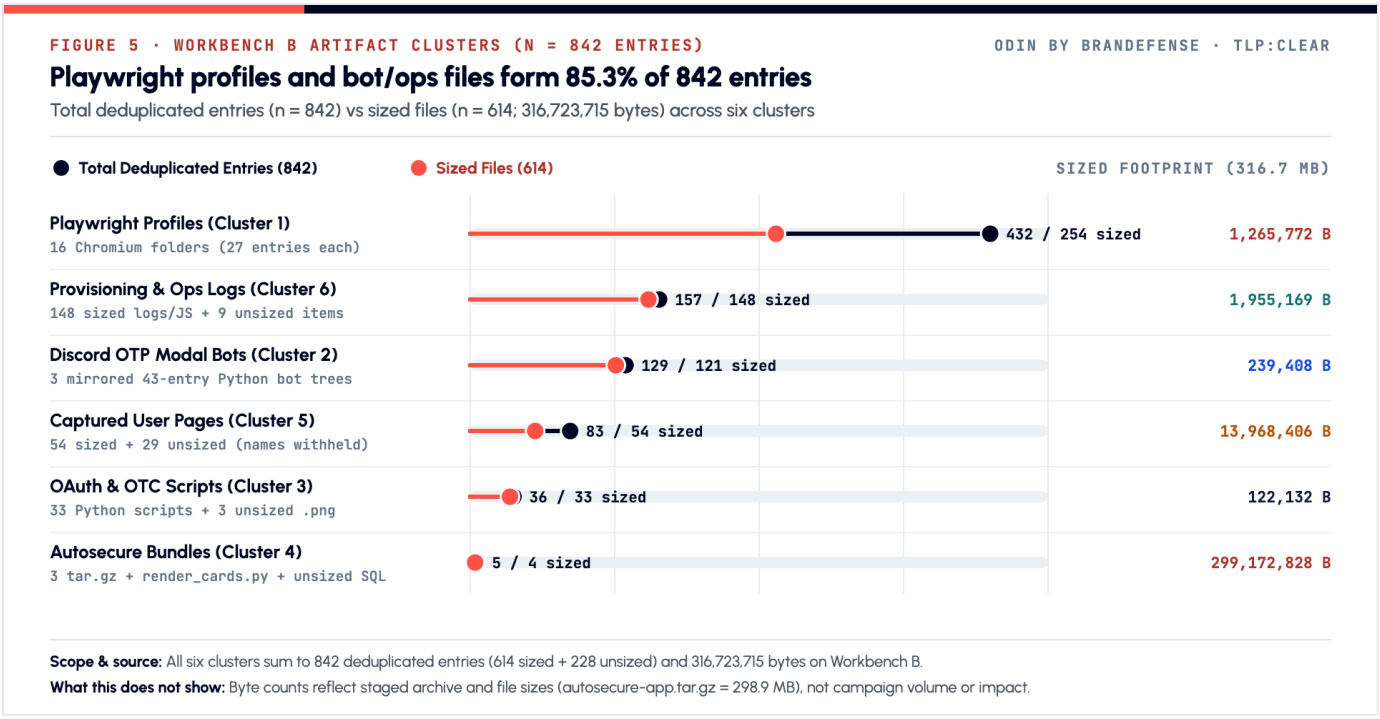

Figure 5: Playwright profiles and bot/ops files form 85.3% of 842 entries

Cluster on `Workbench B`	Entries	Share (%)	Sized	Unsized	Sized bytes	Staged examples (`Cluster 5` names withheld)
1. Playwright Profiles	432	51.3%	254	178	1,265,772	16 `playwright_chromiumdev_profile-*` folders (27 items each), `Shared Dictionary/db` (45,056 B).
6. Setup & Ops Logs	157	18.6%	148	9	1,955,169	`admin_check.js` (43,943 B), `provision.log` (26,735 B), `smoke.sh` (2,617 B). Handle JSON names withheld.

Cluster on `Workbench B`	Entries	Share (%)	Sized	Unsized	Sized bytes	Staged examples (`Cluster 5` names withheld)
2. Discord OTP Bots	129	15.3%	121	8	239,408	3 43-item trees (`Minecraft-Simple-Autosecure` , `template-otp` , `template_ref`), `views/otp.py` (15,571 B).
5. User Pages (Withheld)	83	9.9%	54	29	13,968,406	Filenames withheld (0 filenames or handles published).
3. OAuth & OTC Scripts	36	4.3%	33	3	122,132	27 `probe_*.py` files, `ms_probe.py` (2,831 B), 5 `test_*` / `e2e*` `.py` files, and 3 unsized `.png` items.
4. `Autosecure` Core	5	0.6%	4	1	299,172,828	`autosecure-app.tar.gz` (298,924,100 B), `autosecure-src.tar.gz` (242,567 B), `render_cards.py` (5,871 B).
Total	**842**	**100.0%**	**614**	**228**	**316,723,715**	**0 published IPs, 0 SHA-256s, and 0 Cluster 5 names.**

4. Staged Discord OTP Modals, OAuth FlowToken Scripts, and Playwright Profiles

In gaming and consumer fraud markets, `Autosecure` kits automate code interception (`T1111` , `[REF-08]`) and backup-email replacement. These kits push past basic credential stuffing by pairing Discord modal forms with saved browser sessions.

Figure 3 shows an analytical model comparing **Track A** (`20 November 2026` Entra ROPC report, `[REF-01]`) with **Track B** (staged files on `Workbench B`).

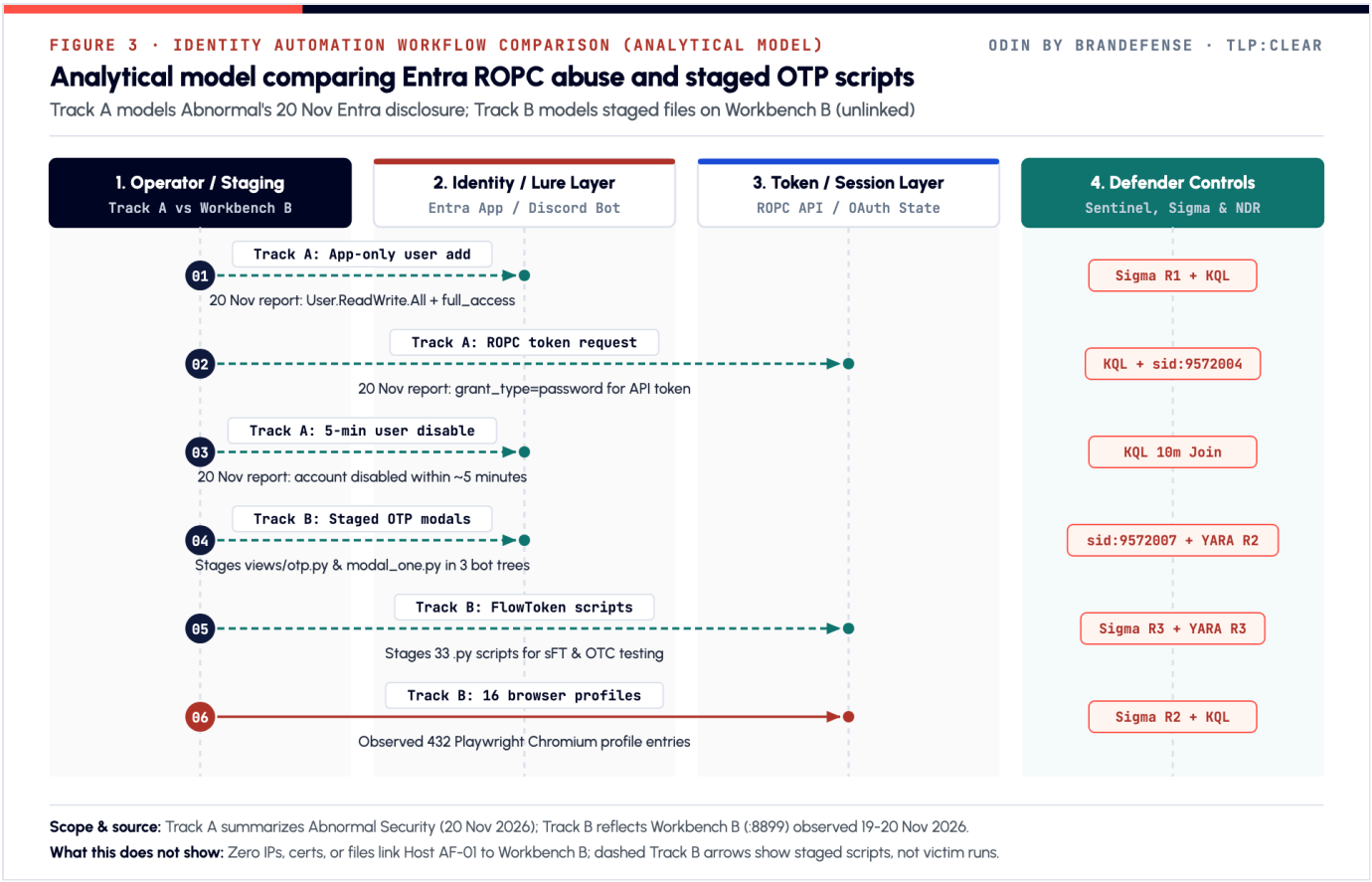

Figure 3: Analytical model comparing Entra ROPC abuse and staged OTP scripts

Four Staged Subsystems on `Workbench B`

Directory listings on `Workbench B` show operator staging rather than verified live victim runs:

- **Core `Autosecure` bundles (5 entries, 299,172,828 B).** `autosecure-app.tar.gz` (298,924,100 B) sits beside `autosecure-src.tar.gz` (242,567 B) and `autosecure-config.tar.gz` (290 B). The cluster also lists `render_cards.py` (5,871 B) and an unsized `autosecure-db.sql` file. Archive size reflects bundled app libraries, not victim count.
- **Discord OTP modal bots (129 entries, 239,408 B).** Three 43-entry Git trees (`Minecraft-Simple-Autosecure` , `template-otp` , `template_ref`) stage `views/otp.py` (15,571 B) and `views/modal_one.py` (12,384 B). Each tree also holds `views/modal_two.py` (4,717 B), `views/button_four.py` (4,278 B), `cogs/admin.py` (2,372 B), and `bot.py` (1,783 B). Those forms ask users for six-digit OTP codes that lack domain binding (`[REF-06]` , `[REF-08]`).

- **OAuth `flowToken` and OTC scripts (36 entries, 122,132 B).** Thirty-three `.py` files (**27** `probe_*.py` scripts, `ms_probe.py`, and **5** `test_*` / `e2e*` scripts) plus **3** `.png` items test `login[.]live[.]com` steps. Files include `probe_clean_signup.py` (**6,978** B), `probe_full_catch.py` (**6,976** B), `probe_flowtoken_cookie.py` (**6,835** B), and `probe_full_fingerprint.py` (**6,779** B). Other scripts include `probe_blocked_account.py` (**5,880** B), `probe_signup_otc.py` (**5,484** B), and `probe_otc_altemail.py` (**2,915** B).
- **Playwright Chromium folders (432 entries, 1,265,772 B).** Sixteen `playwright_chromiumdev_profile-*` folders (**27** entries each) store `Shared Dictionary/db` (**45,056** B), `Local Storage/leveldb`, and `shared_proto_db`. Setup files in `Cluster 6` add `inline.js` (**29,101** B), `auth.service.ts` (**7,810** B), `admin_ui.js` (**2,803** B), and `harden_live2.log` (**2,299** B). All **83** user files in `Cluster 5` (**13,968,406** B) stay withheld.

Figure 2 maps all five enterprise and consumer identity layers to the actions in Section 7 and the rules in Section 8.

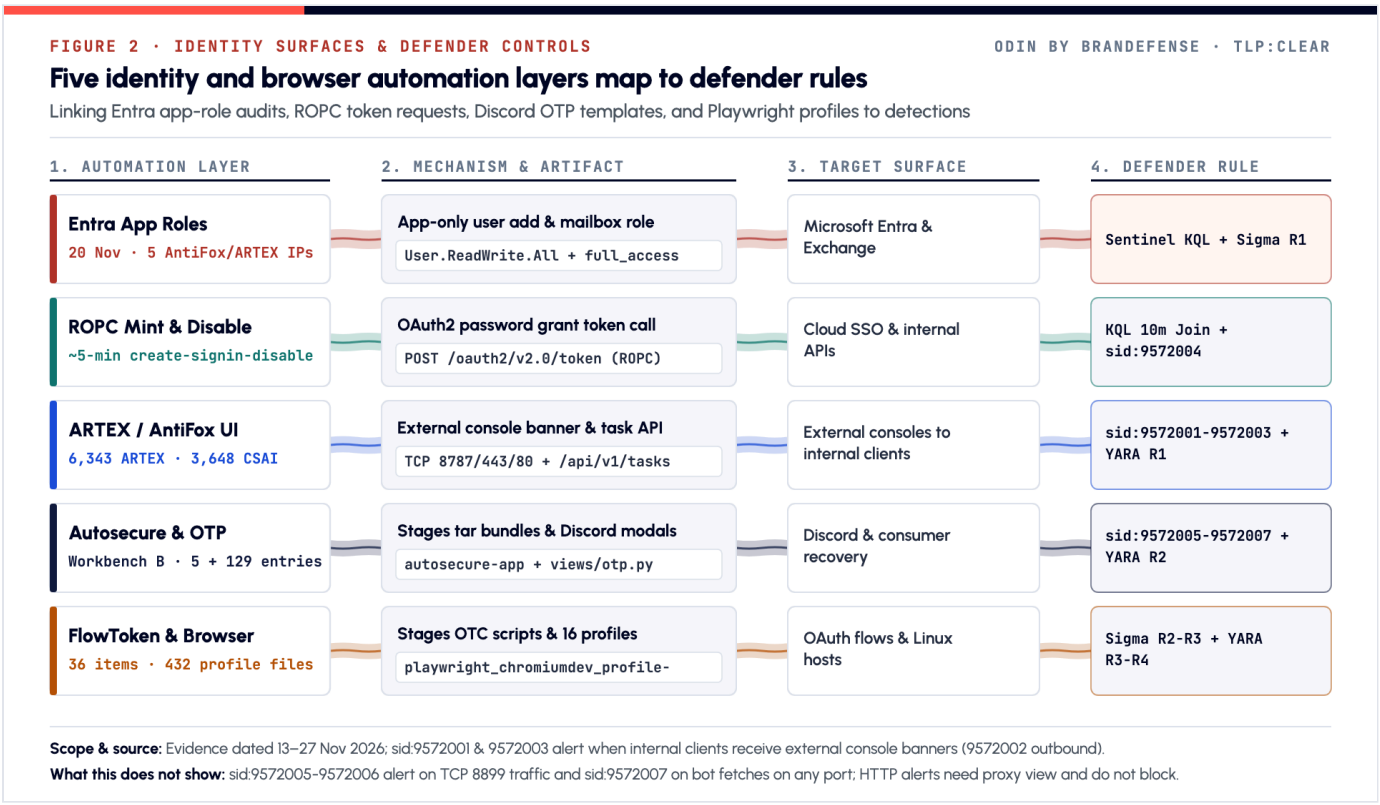

Figure 2: Five identity and browser automation layers map to defender rules

5. Enterprise Exposure and Control Verification

Teams should check five concrete controls across Microsoft Entra, Exchange Online, OAuth portals, and Linux hosts rather than assuming unverified root causes:

Exposure layer	Observed or reported evidence	Control to verify	Operational risk
Entra `full_access_as_app`	`20 Nov` report (`[REF-01]`): app held user add + `full_access_as_app` .	Verify whether apps use scoped Exchange RBAC (`[REF-02]` , `[REF-04]`).	Control of an app with this role could permit tenant-wide mailbox access; `[REF-01]` did not establish mailbox use or how the app was controlled.
OAuth 2.0 ROPC grants	`20 Nov` report (`[REF-01]`): short-lived users signed in via `ROPC` .	Verify whether Conditional Access blocks legacy auth, requires MFA for all users (including new accounts) so `ROPC` cannot complete, and gates app IPs (`[REF-03]` , `[REF-05]`).	Operators turn app roles into user API tokens (`[REF-07]`).
Open `ARTEX` panels	`Host AF-01` (1/5 match); 6,343 `ARTEX` & 3,648 `CyberStrikeAI` records.	Verify whether cloud VPCs gate 8787, 8444, 18666, 80, and 443 with mTLS.	Open panels leak LLM keys and cloud secrets.
Relayable OTP codes	`Workbench B` stages 3 Discord bot trees and 36 `flowToken` /OTC items.	Verify whether portals enforce `FIDO2` passkeys (`[REF-06]`) and reset holds.	Discord modals replay six-digit OTPs live (`[REF-08]`).
Port 8899 & Playwright	`Workbench B` serves 842 entries on :8899, including 16 browser folders.	Verify whether proxies block :8899 and EDR flags rogue Chromium profiles.	Hosts can pull staged tar kits or run browser bots.

6. Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
`Host AF-01` and `Workbench B` share one actor	Both touch Microsoft login or token flows in late November 2026.	Zero IPs, ASNs (`AS396982` US vs `DE` VPS), certs, ports, or files match.	**Rejected.** Treated strictly as two unlinked tracks.
`AntiFox` or `ARTEX` ran the Entra calls on its own	Sign-ins in `[REF-01]` used 5 `AntiFox` / `ARTEX` IPs (1 matching `Host AF-01`).	Abnormal Security noted (`[REF-01]`) that the data does not show direct tool runs; 4/5 IPs had no panel.	**Unproven.** Treat as host overlap, not proof of autonomous runs.
`Workbench B` (:8899) is a benign QA host	Holds 16 Playwright folders, `e2e_test.py` , and `smoke.sh` .	Stages `autosecure-app.tar.gz` , `Minecraft-Simple-Autosecure` OTP bots, `probe_flowtoken_cookie.py` , and 83 user pages.	**Contradicted.** Treated as an attacker workbench; IP and 83 user names stay withheld.
Six-digit OTP MFA stops both tracks	Numeric OTPs block basic password reuse when users ignore lures.	App roles + `ROPC` skip staff prompts (`[REF-01]`), while Discord modals relay live OTPs (`[REF-06]`).	**Refuted.** Pair Entra RBAC and universal MFA with `FIDO2` keys.

7. What Defenders Should Do

Security and identity teams can close both cloud app-role and OTP-relay gaps in five direct steps:

1. **Retire `full_access_as_app` and scope Entra roles (`0-48 Hours`).** Audit every service principal holding `full_access_as_app` , `User.ReadWrite.All` , or

`RoleManagement.ReadWrite.Directory` (`[REF-01]` , `[REF-04]`). Move mail apps to scoped Exchange RBAC (`[REF-02]`), replace secrets with certs (`[REF-04]`), and alert via Sigma Rule 1.

2. **Block OAuth 2.0 ROPC and gate workload tokens (`0-72 Hours`).** Block legacy authentication in Conditional Access. Require MFA for all users, including newly created accounts, on the relevant resources so ROPC cannot complete (`[REF-03]`). Restrict workload tokens to corporate IPs with Workload Identity Conditional Access (`[REF-05]`), and run the **10**-minute Sentinel KQL join (`[REF-07]`).
3. **Require `FIDO2` / `WebAuthn` passkeys (`Days 1-7`).** Replace SMS, email codes, and six-digit app codes with domain-bound **`FIDO2` keys or passkeys** (`[REF-06]` , `[REF-08]`). Require a step-up `FIDO2` check before any backup-email edit (`[REF-06]`).
4. **Gate cloud panels and block `TCP 8899` egress (`Days 7-14`).** Scan cloud ranges across **8787**, **8444**, **18666**, **80**, **443**, and **8080** for open `ARTEX` (`cd3ebd16437d6d3963592f7365dd3980`) and `CyberStrikeAI` panels, and put approved tools behind mTLS. Use `sid:9572001` and `sid:9572003` to alert when internal clients receive external console banners, and `sid:9572002` for outbound task calls. Block unauthorized `TCP 8899` egress in proxy policy; `sid:9572005` -**9572006** alert on that traffic, while `sid:9572007` alerts on bot-directory fetches on any port.
5. **Hunt rogue Playwright profiles on Linux hosts (`Days 14-21`).** Deploy Sigma Rules 2 and 3 plus YARA Rules 2 through 4 (`[REF-08]`). Flag `/chrome` or `/chromium` runs using `playwright_chromiumdev_profile-` outside QA hosts, and Python runs of `probe_flowtoken_cookie.py` or `views/otp.py` .

8. Detection Rules

The full rules are in the Detection rules tab and printed verbatim below. Because all **5** incident IPs, `Workbench B` 's IP, console IPs, and file SHA-256s stay withheld, each rule matches audit events, HTTP fields, CLI flags, or file strings.

Check scope (`Publication Rules §6`): all seven Suricata rules passed the Odin Suricata linter (**0** problems). YAML checks confirmed all three Sigma rules, and structural checks verified the Sentinel KQL and YARA files. Live engine binaries (`suricata -T` , `Kusto.Language` , `pySigma` , and `yara`) were not installed on the build host. Rules were not replayed on live traffic, so test and tune allowlists before rollout.

8.1 Suricata 7.x Ruleset (`sid:9572001` -9572007)

All seven `alert http` rules need cleartext HTTP or a TLS proxy view. If your proxy skips TLS inspection on `login.microsoftonline[.]com`, use Sentinel `SigninLogs` in Section 8.2 to catch `ROPC`. Because `alert` rules do not drop packets inline, enforce blocks in Conditional Access, WAF, or proxy policy.

Response-banner rules `sid:9572001` and `sid:9572003` alert when internal clients receive external `ARTEX` or `CyberStrikeAI` banners, while `sid:9572002` and `sid:9572004` alert on outbound task and `ROPC` calls. Rules `sid:9572005` and `sid:9572006` alert on `TCP 8899` directory listings and archive fetches, and `sid:9572007` alerts on outbound `/Minecraft-Simple-Autosecure/` fetches on any port.

SURICATA

```
# Odin by Brandefense - Monograph 72 Suricata 7.x Ruleset (sid:9572001-9572007)
# Checked with Odin Suricata linter (0 problems); needs HTTP or TLS proxy view.

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R72. Exposed ARTEX Banner"; f
low:established,to_client; http.response_body; content:"ARTEX - Autonomous Red-Team Ex
pert"; fast_pattern; classtype:trojan-activity; sid:9572001; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R72. ARTEX Task Call"; flow:e
stablished,to_server; http.method; content:"POST"; bsize:4; http.uri; content:"/api/v
1/tasks"; startswith; fast_pattern; classtype:trojan-activity; sid:9572002; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R72. CyberStrikeAI UI"; flow:
established,to_client; http.response_body; content:"CyberStrikeAI"; fast_pattern; clas
stype:trojan-activity; sid:9572003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R72. OAuth2. ROPC"; flow:esta
blished,to_server; http.uri; content:"/oauth2/v2.0/token"; endswith; http.request_bod
y; content:"grant_type=password"; nocase; fast_pattern; classtype:policy-violation; si
d:9572004; rev:1;)
alert http $EXTERNAL_NET 8899 -> $HOME_NET any (msg:"ODIN-R72. Dir Index 8899"; flow:e
stablished,to_client; http.response_body; content:"Directory listing for /"; conten
t:"autosecure-"; fast_pattern; classtype:bad-unknown; sid:9572005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET 8899 (msg:"ODIN-R72. Autosecure Tar"; flow:e
stablished,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/autosec
ure-"; startswith; fast_pattern; classtype:trojan-activity; sid:9572006; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R72. Discord OTP Bot"; flow:e
stablished,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/Minecra
ft-Simple-Autosecure/"; startswith; fast_pattern; classtype:trojan-activity; sid:95720
07; rev:1;)
```

8.2 Microsoft Sentinel KQL Hunt

This 7-day query joins app-created Entra users (`AuditLogs`) with `SigninLogs` (`AuthenticationProtocol =~ "ropc"`) and disable events within 10 minutes. It also flags `full_access_as_app` or `User.ReadWrite.All` grants and `playwright_chromiumdev_profile-` runs outside exact allowlists.

```kql
// Odin by Brandefense - Monograph 72
// Hunts Entra app-created disposable ROPC accounts, full_access_as_app grants, and Pl
aywright/Autosecure CLI activity.
let Lookback = 7d;
let ApprovedProvisioningAppIds = dynamic(["00000000-0000-0000-0000-000000000001"]);
let ApprovedAutomationHosts = dynamic(["qa-playwright-01.corp.example", "app-ci-01.cor
p.example"]);
let AppCreatedUsers =
    AuditLogs
    | where TimeGenerated >= ago(Lookback)
    | where OperationName in~ ("Add user", "Create user") and Result =~ "success"
    | extend InitiatingAppId = tostring(InitiatedBy.app.appId), InitiatingAppName = to
string(InitiatedBy.app.displayName)
    | where isnotempty(InitiatingAppId) and not(InitiatingAppId in~ (ApprovedProvision
ingAppIds))
    | extend TargetUPN = tolower(tostring(TargetResources[0].userPrincipalName))
    | where isnotempty(TargetUPN)
    | project CreateTime = TimeGenerated, TargetUPN, InitiatingAppId, InitiatingAppNam
e;
let RopcSignIns =
    SigninLogs
    | where TimeGenerated >= ago(Lookback)
    | where ResultType == 0 and AuthenticationProtocol =~ "ropc"
    | extend TargetUPN = tolower(UserPrincipalName)
    | project RopcTime = TimeGenerated, TargetUPN, SignInApp = AppDisplayName, Resourc
eDisplayName, IPAddress;
let DisabledUsers =
    AuditLogs
    | where TimeGenerated >= ago(Lookback)
    | where Result =~ "success"
    | where OperationName =~ "Disable account" or (OperationName =~ "Update user" and
tostring(TargetResources[0].modifiedProperties) contains "AccountEnabled" and tostring
(TargetResources[0].modifiedProperties) contains "false")
    | extend TargetUPN = tolower(tostring(TargetResources[0].userPrincipalName))
    | project DisableTime = TimeGenerated, TargetUPN;
let DisposableAccountRopcChain =
```

```
    AppCreatedUsers
    | join kind=inner (RopcSignIns) on TargetUPN
    | where RopcTime between (CreateTime .. (CreateTime + 10m))
    | join kind=inner (DisabledUsers) on TargetUPN
    | where DisableTime between (RopcTime .. (CreateTime + 10m))
    | project EventTime = DisableTime, Entity = TargetUPN, ActorOrHost = InitiatingApp
Id, SignalType = "EntraDisposableAccountRopc", Detail = strcat("App=", InitiatingAppNa
me, " ROPC->", ResourceDisplayName, " IP=", IPAddress);
let HighRiskEntraAppGrants =
    AuditLogs
    | where TimeGenerated >= ago(Lookback)
    | where Result =~ "success"
    | where OperationName in~ ("Add app role assignment to service principal", "Update
application - Certificates and secrets management")
    | extend InitiatingAppId = tostring(InitiatedBy.app.appId), ActorUPN = tostring(In
itiatedBy.user.userPrincipalName)
    | where not(InitiatingAppId in~ (ApprovedProvisioningAppIds))
    | extend TargetJson = tostring(TargetResources)
    | where OperationName =~ "Update application - Certificates and secrets managemen
t" or TargetJson has_any ("full_access_as_app", "User.ReadWrite.All", "RoleManagement.
ReadWrite.Directory")
    | project EventTime = TimeGenerated, Entity = tostring(TargetResources[0].displayN
ame), ActorOrHost = iff(isnotempty(InitiatingAppId), InitiatingAppId, ActorUPN), Signa
lType = "EntraHighRiskAppRoleOrSecret", Detail = OperationName;
let EndpointPlaywrightAutosecure =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAutomationHosts))
    | where ProcessCommandLine contains "playwright_chromiumdev_profile-" or ProcessCo
mmandLine has_any ("probe_flowtoken_cookie.py", "probe_signup_otc.py", "autosecure-ap
p.tar.gz")
    | project EventTime = Timestamp, Entity = AccountName, ActorOrHost = DeviceName, S
ignalType = "PlaywrightOrAutosecureCli", Detail = ProcessCommandLine;
union DisposableAccountRopcChain, HighRiskEntraAppGrants, EndpointPlaywrightAutosecure
| summarize FirstSeen = min(EventTime), LastSeen = max(EventTime), EventCount = count
(), Signals = make_set(SignalType, 5), SampleDetails = make_set(Detail, 5) by Entity,
ActorOrHost
| order by LastSeen desc
```

8.3 Portable Sigma Rules (3 Rules)

Rule 1 flags Azure `auditlogs` events granting `full_access_as_app`, `User.ReadWrite.All`, or `RoleManagement.ReadWrite.Directory`, or updating app keys. Rule 2 flags Linux Chromium runs

with `playwright_chromiumdev_profile-` outside QA hosts. Rule 3 flags Python runs of `Autosecure` OAuth or Discord scripts.

```yaml
title: Microsoft Entra High-Risk Application Role Grant or Credential Update
id: 72a8c341-5e19-4b84-9a22-72d40b91e701
status: experimental
description: Detects Microsoft Entra audit events granting Exchange full_access_as_app
or User.ReadWrite.All app roles or adding service-principal credentials outside approv
ed provisioning apps.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  product: azure
  service: auditlogs
detection:
  selection_role_op:
    properties.message: 'Add app role assignment to service principal'
    TargetResources|contains:
      - 'full_access_as_app'
      - 'User.ReadWrite.All'
      - 'RoleManagement.ReadWrite.Directory'
  selection_cred_op:
    properties.message: 'Update application - Certificates and secrets management'
  filter_approved_apps:
    InitiatedByAppId:
      - '00000000-0000-0000-0000-000000000001'
  condition: (selection_role_op or selection_cred_op) and not filter_approved_apps
falsepositives:
  - Planned secret rotations or Exchange RBAC updates performed by approved admins
level: high
tags:
  - attack.persistence
  - attack.privilege-escalation
---
title: Linux Headless Playwright Chromium Session Profile Automation
id: 72a8c341-5e19-4b84-9a22-72d40b91e702
status: experimental
description: Detects headless Chromium or Playwright browser launches referencing temp
orary playwright_chromiumdev_profile directories outside approved QA automation hosts.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
```

```
detection:
  selection_bin:
    Image|endswith:
      - '/chrome'
      - '/chromium'
      - '/headless_shell'
  selection_profile:
    CommandLine|contains: 'playwright_chromiumdev_profile-'
  filter_approved_hosts:
    ComputerName:
      - 'qa-playwright-01.corp.example'
      - 'app-ci-01.corp.example'
  condition: selection_bin and selection_profile and not filter_approved_hosts
falsepositives:
  - Authorized end-to-end web testing runners using Playwright temporary Chromium user
-data directories
level: medium
tags:
  - attack.credential-access
  - attack.t1111
---
title: Linux Python Execution of Autosecure OAuth FlowToken or Discord OTP Scripts
id: 72a8c341-5e19-4b84-9a22-72d40b91e703
status: experimental
description: Detects Python interpreter invocations running Autosecure OAuth flowToke
n, one-time-code submission, or Discord OTP lure modal scripts.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
detection:
  selection_py:
    Image|endswith:
      - '/python'
      - '/python3'
      - '/python3.12'
      - '/python3.13'
  selection_scripts:
    CommandLine|contains:
      - 'probe_flowtoken_cookie.py'
      - 'probe_signup_otc.py'
      - 'probe_otc_altemail.py'
      - 'ms_probe.py'
      - 'views/otp.py'
  filter_approved_hosts:
    ComputerName:
```

```
      - 'sec-lab-01.corp.example'
  condition: selection_py and selection_scripts and not filter_approved_hosts
falsepositives:
  - Isolated malware-analysis sandboxes inspecting captured Python phishing bot script
s
level: high
tags:
  - attack.credential-access
  - attack.t1111
```

8.4 Structural YARA Suite (4 `filesize`-Bounded Rules)

Four `filesize`-bounded rules match `ARTEX` or `AntiFox` bundles, Discord `discord.ui.Modal` bot files, Python `login[.]live[.]com` `sFT` scripts, and `Autosecure` configs.

```YARA
/*
   Odin by Brandefense - Monograph 72 YARA Suite
   4 filesize-bounded structural rules covering ARTEX/AntiFox console bundles,
   Discord OTP lure modal templates, OAuth flowToken/OTC probe scripts, and Autosecure
configs.
*/

rule ODIN_R72_ARTEX_AntiFox_Console_Bundle
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
        description = "Detects exposed ARTEX or AntiFox-fork console bundles and task
API routes"
        date = "2026-11-27"
    strings:
        $a1 = "ARTEX - Autonomous Red-Team Expert" ascii
        $a2 = "/api/v1/tasks" ascii
        $a3 = "AntiFox" ascii nocase
    condition:
        filesize < 5MB and ($a1 or $a3) and $a2
}

rule ODIN_R72_Discord_OTP_Modal_Phishing_Bot
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
```

```
        description = "Detects Python Discord interactive OTP lure modal templates sta
ged in Autosecure trees"
        date = "2026-11-27"
    strings:
        $d1 = "discord.ui.Modal" ascii
        $d2 = "views/otp.py" ascii
        $d3 = "modal_one" ascii
        $d4 = "Minecraft-Simple-Autosecure" ascii nocase
    condition:
        filesize < 256KB and $d1 and ($d2 or $d3 or $d4)
}

rule ODIN_R72_OAuth_FlowToken_and_OTC_Probe_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
        description = "Detects Python scripts automating OAuth flowToken extraction an
d one-time-code submission"
        date = "2026-11-27"
    strings:
        $p1 = "sFT" ascii
        $p2 = "flowToken" ascii nocase
        $p3 = "login.live.com" ascii nocase
        $p4 = "otc" ascii nocase
    condition:
        filesize < 128KB and ($p1 or $p2) and $p3 and $p4
}

rule ODIN_R72_Autosecure_Config_and_Card_Renderer
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
        description = "Detects Autosecure deployment manifests referencing SQL schema
s, card renderers, and Playwright profiles"
        date = "2026-11-27"
    strings:
        $c1 = "autosecure-app" ascii
        $c2 = "autosecure-db.sql" ascii
        $c3 = "render_cards" ascii
        $c4 = "playwright_chromiumdev_profile-" ascii
    condition:
        filesize < 1MB and 2 of ($c1, $c2, $c3, $c4)
}
```

9. Indicators

The Indicators tab holds **0** published blocklist IPv4 addresses and **0** file SHA-256 hashes. All **5** incident IPs (including `Host AF-01`), `Workbench B`'s IP, console IPs, and file SHA-256s stay withheld under Publication Rules §1. All **83** user filenames in `Cluster 5` (**13,968,406** B) stay withheld as well.

Indicator or marker group	Published in Indicators tab	Status in this report
Disclosed `AntiFox` / `ARTEX` IPv4s (5 total: 4 `AntiFox`, 1 `ARTEX`, including `Host AF-01`)	0	Withheld (`Publication Rules §1.2 & §1.3`).
`Workbench B` IP & candidate console IPs (6,343 `ARTEX`, 3,648 `CyberStrikeAI`)	0	Withheld (**83** user files in `Cluster 5` also withheld).
Staged file SHA-256 hashes (842 entries on `Workbench B`)	0	Withheld (**0** published SHA-256 hashes).
Behavioral, protocol, audit, and host hunt markers	0 (text-only table below)	**10** markers listed in the table below.

Behavioral, Protocol, and Audit Hunt Markers

Marker category	Pattern / artifact	Layer	Defensive hunt & control
ARTEX icon MD5	`cd3ebd16437d6d3963592f7365dd3980`	Web ports	Scan cloud subnets for `/favicon.ico` (15,406 B) on 8787, 443, 80, and 8080.
ARTEX HTML banner	`ARTEX - Autonomous Red-Team Expert`	Proxy / IDS	Alert when internal clients receive external console banners (`sid:9572001`, YARA R1; 6,343 records).
Task API route	`POST /api/v1/tasks`	TLS egress	Alert on outbound calls (`sid:9572002`) via TLS forward proxies.
Entra app roles	`full_access_as_app` + `User.ReadWrite.All`	`AuditLogs`	Move to Exchange RBAC (`[REF-02]`) and alert via Sentinel KQL and Sigma R1.

Marker category	Pattern / artifact	Layer	Defensive hunt & control
OAuth2 ROPC burst	`POST /oauth2/v2.0/token` (`grant_type=password`)	`SigninLogs`	Require MFA for all users so `ROPC` cannot complete (`[REF-03]`), and run the 10-minute KQL join + `sid:9572004`.
Autosecure bundle	`Directory listing for /` (`autosecure-app.tar.gz`)	`TCP 8899`	Block :8899 egress in proxy policy; alert on :8899 traffic via `sid:9572005`-9572006 and YARA R4.
Discord OTP bot	`/Minecraft-Simple-Autosecure/views/otp.py`	Proxy / EDR	Staged across 3 43-item trees (129 entries). Alert on bot-directory fetches on any port (`sid:9572007`) and YARA R2.
OAuth probe script	`probe_flowtoken_cookie.py` + `probe_signup_otc.py`	Linux EDR	Staged in 36-entry cluster. Hunt via Sentinel KQL, Sigma R3, and YARA R3.

Marker category	Pattern / artifact	Layer	Defensive hunt & control
Playwright folder	`playwright_chromiumdev_profile-`	Linux EDR	Sixteen folders (**432** entries) on `Workbench B`. Hunt via KQL and Sigma R2.
CyberStrikeAI UI	`CyberStrikeAI`	8444, 18666	Sweep cloud ranges and alert when internal clients receive external console banners (`sid:9572003` ; 3,648 records).

10. Scope and Limits

Odin by Brandefense ran this study on evidence dated `13-27 November 2026`. Monograph 60 covered seven-tool console growth and Storm-0940 or ZQAgent cases; Monograph 72 compares two unlinked identity tracks.

Track one checks Abnormal Security's `20 November 2026` Microsoft Entra report (`[REF-01]`). One of its **5** `AntiFox` / `ARTEX` IPv4s (**4** `AntiFox` , **1** `ARTEX`) matched candidate `Host AF-01` (`Google Cloud AS396982` , seen **19** and `25-26 November 2026`). Global records reached **6,343** `ARTEX` (**4,543** on `15 November`) and **3,648** `CyberStrikeAI` candidates.

Track two examines `Workbench B` , a Germany VPS on `TCP 8899` first seen `13 November` and recorded `19-20 November 2026` . It held **842** deduplicated entries: **614** sized files (**316,723,715** B) and **228** unsized items.

Zero IPv4s, TLS certs, or files link `Host AF-01` to `Workbench B`. Abnormal Security noted (`[REF-01]`) that `AntiFox` / `ARTEX` host overlap does not show direct tool command runs, and `Workbench B` files show staging rather than live victim runs. All **5** incident IPs, `Workbench B` 's IP, console IPs, file SHA-256s, and all **83** `Cluster 5` user filenames (**13,968,406** B) stay withheld.

11. Sources

1. `[REF-01]` Abnormal Security, *ARTEX in the Tenant: How an Agentic Offensive Framework Abused an Entra Application to Mint Disposable Accounts* (20 November 2026; verified on 27 November 2026).
2. `[REF-02]` Microsoft Learn, *Role-Based Access Control for Applications in Exchange Online (Replacing full_access_as_app)* (verified on 27 November 2026).
3. `[REF-03]` Microsoft Learn, *OAuth 2.0 Resource Owner Password Credentials (ROPC) Risks in Microsoft Identity Platform* (verified on 27 November 2026).
4. `[REF-04]` Microsoft Learn, *Securing Workload Identities and Service Principals in Microsoft Entra ID* (verified on 27 November 2026).
5. `[REF-05]` Microsoft Learn, *Conditional Access for Workload Identities* (verified on 27 November 2026).
6. `[REF-06]` CISA, *Implementing Phishing-Resistant MFA Fact Sheet* (verified on 27 November 2026).
7. `[REF-07]` MITRE ATT&CK, *Create Account: Cloud Account (T1136.003)* (verified on 27 November 2026).
8. `[REF-08]` MITRE ATT&CK, *Multi-Factor Authentication Interception (T1111)* (verified on 27 November 2026).

BRANDEFENSE CAPABILITIES RELATED TO THIS RESEARCH

Cyber Threat Intelligence

Track the actors, infrastructure and campaigns behind threats like these.

Dark Web Monitoring

Catch stolen credentials and sessions offered for sale.

Phishing and Domain Abuse

Find the lookalike login pages these kits serve.

DEFENDER KIT

Indicators of compromise

Verified adversary infrastructure and tool hashes from this study. Every value below is also discussed in the report.

No network or file indicators are published for this study

The hosts in this report are exposed or unattributed systems rather than confirmed adversary infrastructure, so they stay anonymous. Use the detection rules below to find the same exposure in your own estate.

10 records from this study are not published in this table: candidate, suspected and dual-use hosts, victim-related values, and hashes of exposed secrets or files.

DEFENDER KIT

Detection rules

The rule files exactly as printed in the report. Test them in your own engine before deployment.

Suricata `odin_entra_antifox_and_autosecure_hunt.rules` 11 lines

```
# Odin by Brandefense - Monograph 72 Suricata 7.x Ruleset (sid:9572001-9572007)
# Checked with Odin Suricata linter (0 problems); needs HTTP or TLS proxy view.

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R72. Exposed ARTEX Banner"; f
low:established,to_client; http.response_body; content:"ARTEX - Autonomous Red-Team Ex
pert"; fast_pattern; classtype:trojan-activity; sid:9572001; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R72. ARTEX Task Call"; flow:e
stablished,to_server; http.method; content:"POST"; bsize:4; http.uri; content:"/api/v
1/tasks"; startswith; fast_pattern; classtype:trojan-activity; sid:9572002; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R72. CyberStrikeAI UI"; flow:
established,to_client; http.response_body; content:"CyberStrikeAI"; fast_pattern; clas
stype:trojan-activity; sid:9572003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R72. OAuth2. ROPC"; flow:esta
blished,to_server; http.uri; content:"/oauth2/v2.0/token"; endswith; http.request_bod
y; content:"grant_type=password"; nocase; fast_pattern; classtype:policy-violation; si
d:9572004; rev:1;)
alert http $EXTERNAL_NET 8899 -> $HOME_NET any (msg:"ODIN-R72. Dir Index 8899"; flow:e
stablished,to_client; http.response_body; content:"Directory listing for /"; conten
t:"autosecure-"; fast_pattern; classtype:bad-unknown; sid:9572005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET 8899 (msg:"ODIN-R72. Autosecure Tar"; flow:e
stablished,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/autosec
ure-"; startswith; fast_pattern; classtype:trojan-activity; sid:9572006; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R72. Discord OTP Bot"; flow:e
stablished,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/Minecra
ft-Simple-Autosecure/"; startswith; fast_pattern; classtype:trojan-activity; sid:95720
07; rev:1;)
```

Show full rule

YARA `odin_entra_antifox_and_autosecure_kits.yar` 69 lines

```
/*
   Odin by Brandefense - Monograph 72 YARA Suite
   4 filesize-bounded structural rules covering ARTEX/AntiFox console bundles,
   Discord OTP lure modal templates, OAuth flowToken/OTC probe scripts, and Autosecure
configs.
*/
```

```
rule ODIN_R72_ARTEX_AntiFox_Console_Bundle
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
        description = "Detects exposed ARTEX or AntiFox-fork console bundles and task
API routes"
        date = "2026-11-27"
    strings:
        $a1 = "ARTEX - Autonomous Red-Team Expert" ascii
        $a2 = "/api/v1/tasks" ascii
        $a3 = "AntiFox" ascii nocase
    condition:
        filesize < 5MB and ($a1 or $a3) and $a2
}

rule ODIN_R72_Discord_OTP_Modal_Phishing_Bot
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
        description = "Detects Python Discord interactive OTP lure modal templates sta
ged in Autosecure trees"
        date = "2026-11-27"
    strings:
        $d1 = "discord.ui.Modal" ascii
        $d2 = "views/otp.py" ascii
        $d3 = "modal_one" ascii
        $d4 = "Minecraft-Simple-Autosecure" ascii nocase
    condition:
        filesize < 256KB and $d1 and ($d2 or $d3 or $d4)
}

rule ODIN_R72_OAuth_FlowToken_and_OTC_Probe_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
        description = "Detects Python scripts automating OAuth flowToken extraction an
d one-time-code submission"
        date = "2026-11-27"
    strings:
        $p1 = "sFT" ascii
        $p2 = "flowToken" ascii nocase
        $p3 = "login.live.com" ascii nocase
        $p4 = "otc" ascii nocase
```

```
    condition:
        filesize < 128KB and ($p1 or $p2) and $p3 and $p4
}

rule ODIN_R72_Autosecure_Config_and_Card_Renderer
{
    meta:
        author = "Odin by Brandefense"
        monograph = "72"
        description = "Detects Autosecure deployment manifests referencing SQL schema
s, card renderers, and Playwright profiles"
        date = "2026-11-27"
    strings:
        $c1 = "autosecure-app" ascii
        $c2 = "autosecure-db.sql" ascii
        $c3 = "render_cards" ascii
        $c4 = "playwright_chromiumdev_profile-" ascii
    condition:
        filesize < 1MB and 2 of ($c1, $c2, $c3, $c4)
}
```

Sentinel KQL **sentinel_entra_app_ropc_and_playwright_hunt.kql** 54 lines

```
// Odin by Brandefense - Monograph 72
// Hunts Entra app-created disposable ROPC accounts, full_access_as_app grants, and Pl
aywright/Autosecure CLI activity.
let Lookback = 7d;
let ApprovedProvisioningAppIds = dynamic(["00000000-0000-0000-0000-000000000001"]);
let ApprovedAutomationHosts = dynamic(["qa-playwright-01.corp.example", "app-ci-01.cor
p.example"]);
let AppCreatedUsers =
    AuditLogs
    | where TimeGenerated >= ago(Lookback)
    | where OperationName in~ ("Add user", "Create user") and Result =~ "success"
    | extend InitiatingAppId = tostring(InitiatedBy.app.appId), InitiatingAppName = to
string(InitiatedBy.app.displayName)
    | where isnotempty(InitiatingAppId) and not(InitiatingAppId in~ (ApprovedProvision
ingAppIds))
    | extend TargetUPN = tolower(tostring(TargetResources[0].userPrincipalName))
    | where isnotempty(TargetUPN)
    | project CreateTime = TimeGenerated, TargetUPN, InitiatingAppId, InitiatingAppNam
e;
let RopcSignIns =
    SigninLogs
    | where TimeGenerated >= ago(Lookback)
    | where ResultType == 0 and AuthenticationProtocol =~ "ropc"
```

```
    | extend TargetUPN = tolower(UserPrincipalName)
    | project RopcTime = TimeGenerated, TargetUPN, SignInApp = AppDisplayName, Resourc
eDisplayName, IPAddress;
let DisabledUsers =
    AuditLogs
    | where TimeGenerated >= ago(Lookback)
    | where Result =~ "success"
    | where OperationName =~ "Disable account" or (OperationName =~ "Update user" and
tostring(TargetResources[0].modifiedProperties) contains "AccountEnabled" and tostring
(TargetResources[0].modifiedProperties) contains "false")
    | extend TargetUPN = tolower(tostring(TargetResources[0].userPrincipalName))
    | project DisableTime = TimeGenerated, TargetUPN;
let DisposableAccountRopcChain =
    AppCreatedUsers
    | join kind=inner (RopcSignIns) on TargetUPN
    | where RopcTime between (CreateTime .. (CreateTime + 10m))
    | join kind=inner (DisabledUsers) on TargetUPN
    | where DisableTime between (RopcTime .. (CreateTime + 10m))
    | project EventTime = DisableTime, Entity = TargetUPN, ActorOrHost = InitiatingApp
Id, SignalType = "EntraDisposableAccountRopc", Detail = strcat("App=", InitiatingAppNa
me, " ROPC->", ResourceDisplayName, " IP=", IPAddress);
let HighRiskEntraAppGrants =
    AuditLogs
    | where TimeGenerated >= ago(Lookback)
    | where Result =~ "success"
    | where OperationName in~ ("Add app role assignment to service principal", "Update
application - Certificates and secrets management")
    | extend InitiatingAppId = tostring(InitiatedBy.app.appId), ActorUPN = tostring(In
itiatedBy.user.userPrincipalName)
    | where not(InitiatingAppId in~ (ApprovedProvisioningAppIds))
    | extend TargetJson = tostring(TargetResources)
    | where OperationName =~ "Update application - Certificates and secrets managemen
t" or TargetJson has_any ("full_access_as_app", "User.ReadWrite.All", "RoleManagement.
ReadWrite.Directory")
    | project EventTime = TimeGenerated, Entity = tostring(TargetResources[0].displayN
ame), ActorOrHost = iff(isnotempty(InitiatingAppId), InitiatingAppId, ActorUPN), Signa
lType = "EntraHighRiskAppRoleOrSecret", Detail = OperationName;
let EndpointPlaywrightAutosecure =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAutomationHosts))
    | where ProcessCommandLine contains "playwright_chromiumdev_profile-" or ProcessCo
mmandLine has_any ("probe_flowtoken_cookie.py", "probe_signup_otc.py", "autosecure-ap
p.tar.gz")
    | project EventTime = Timestamp, Entity = AccountName, ActorOrHost = DeviceName, S
ignalType = "PlaywrightOrAutosecureCli", Detail = ProcessCommandLine;
union DisposableAccountRopcChain, HighRiskEntraAppGrants, EndpointPlaywrightAutosecure
```

```
| summarize FirstSeen = min(EventTime), LastSeen = max(EventTime), EventCount = count
(), Signals = make_set(SignalType, 5), SampleDetails = make_set(Detail, 5) by Entity,
ActorOrHost
| order by LastSeen desc
```

Sigma `sigma_entra_app_abuse_and_autosecure_playwright.yml` 92 lines

```
title: Microsoft Entra High-Risk Application Role Grant or Credential Update
id: 72a8c341-5e19-4b84-9a22-72d40b91e701
status: experimental
description: Detects Microsoft Entra audit events granting Exchange full_access_as_app
or User.ReadWrite.All app roles or adding service-principal credentials outside approv
ed provisioning apps.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  product: azure
  service: auditlogs
detection:
  selection_role_op:
    properties.message: 'Add app role assignment to service principal'
    TargetResources|contains:
      - 'full_access_as_app'
      - 'User.ReadWrite.All'
      - 'RoleManagement.ReadWrite.Directory'
  selection_cred_op:
    properties.message: 'Update application - Certificates and secrets management'
  filter_approved_apps:
    InitiatedByAppId:
      - '00000000-0000-0000-0000-000000000001'
  condition: (selection_role_op or selection_cred_op) and not filter_approved_apps
falsepositives:
  - Planned secret rotations or Exchange RBAC updates performed by approved admins
level: high
tags:
  - attack.persistence
  - attack.privilege-escalation
---
title: Linux Headless Playwright Chromium Session Profile Automation
id: 72a8c341-5e19-4b84-9a22-72d40b91e702
status: experimental
description: Detects headless Chromium or Playwright browser launches referencing temp
orary playwright_chromiumdev_profile directories outside approved QA automation hosts.
author: Odin by Brandefense
date: 2026-11-27
logsource:
```

```
  category: process_creation
  product: linux
detection:
  selection_bin:
    Image|endswith:
      - '/chrome'
      - '/chromium'
      - '/headless_shell'
  selection_profile:
    CommandLine|contains: 'playwright_chromiumdev_profile-'
  filter_approved_hosts:
    ComputerName:
      - 'qa-playwright-01.corp.example'
      - 'app-ci-01.corp.example'
  condition: selection_bin and selection_profile and not filter_approved_hosts
falsepositives:
  - Authorized end-to-end web testing runners using Playwright temporary Chromium user
-data directories
level: medium
tags:
  - attack.credential-access
  - attack.t1111
---
title: Linux Python Execution of Autosecure OAuth FlowToken or Discord OTP Scripts
id: 72a8c341-5e19-4b84-9a22-72d40b91e703
status: experimental
description: Detects Python interpreter invocations running Autosecure OAuth flowToke
n, one-time-code submission, or Discord OTP lure modal scripts.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
detection:
  selection_py:
    Image|endswith:
      - '/python'
      - '/python3'
      - '/python3.12'
      - '/python3.13'
  selection_scripts:
    CommandLine|contains:
      - 'probe_flowtoken_cookie.py'
      - 'probe_signup_otc.py'
      - 'probe_otc_altemail.py'
      - 'ms_probe.py'
      - 'views/otp.py'
```

```
  filter_approved_hosts:
    ComputerName:
      - 'sec-lab-01.corp.example'
  condition: selection_py and selection_scripts and not filter_approved_hosts
falsepositives:
  - Isolated malware-analysis sandboxes inspecting captured Python phishing bot script
s
level: high
tags:
  - attack.credential-access
  - attack.t1111
```

