FULL REPORT • OPERATIONS • MONOGRAPH 55 / 55 • 16 MIN READ

Operation CampusKey: LMS Supply-Chain SSO Forgery, Campus Tunnels, and Cloud Pivots

Inside an operator's 6,203-file workbench pairing an ARTEX console with .NET LMS reverse engineering, RSA/JWT SSO forgery, live campus tunnels, and Entra ID pivots

BY
Odin by Brandefense

PUBLISHED
19 November 2026

READING TIME
16 min read

EDITION
Version 1.1 · TLP:CLEAR

SCOPE
Prepared November 2026

1. Executive Summary

IN SHORT

Operation CampusKey pairs an ARTEX console with manual reverse engineering of a shared learning management system. South Korean universities use that LMS. Odin by Brandefense analyzed 500 sampled entries from the 6,203-file workbench recorded on 16–20 November 2026. The sample holds SSO token-forgery scripts and three shared LMS database dumps. It also holds a live 16 November campus tunnel log, two LSASS dumps, and Entra ID scripts. Rotate LMS signing keys, require MFA so Entra ROPC fails, isolate campus portals, and alert on WebSocket tunnels.

Higher-education networks connect open student portals with campus databases and research servers. Those networks also connect to Active Directory domains and cloud tenants. When universities license the same regional e-learning software, a shared authentication weakness can create a cross-campus supply-chain attack path. Operation CampusKey combines shared LMS research with one logged campus tunnel and staged cloud identity scripts.

Between 16 and 20 November 2026, Odin by Brandefense analyzed an exposed workbench on a commercial virtual private server. On 20 November 2026, an open directory on that server

reported 6,203 total files.

From 16 to 19 November, the same host ran an ARTEX testing console on TCP port 8787. Counts in this report come from a 500-entry sample. That sample totals 70.89 megabytes across 388 sized files and 356 unique digests.

The server holds university database dumps, memory dumps, and institutional TLS private keys. Odin by Brandefense publishes no VPS addresses or workbench-file SHA-256 digests. The shared ARTEX favicon MD5 remains a console indicator. Both server addresses, all folder names, the LMS vendor name, academic subnets, and university names are withheld.

1 **Shared LMS research and database dumps support product reuse across targets.**

Across 45 numbered target folders (379 sampled entries) and 8 capability folders (55 entries), the operator collected 12 .NET libraries. The operator disassembled those libraries from a regional e-learning product.

The workspace also held 29 single sign-on and JSON Web Token scripts, RSA keys, and test outputs. Those files target the product's authentication bridge.

Database dumps sharing that identical LMS table schema sit inside three separate target folders. Those dumps support reuse of the same LMS product across targets. Directory listings alone do not show whether 45 folders map to 45 distinct universities. Some folders may map to several sub-systems per campus.

2 **A live reverse tunnel on 16 November forwarded six internal campus service types.**

A reverse-tunnel server log dated 16 November 2026 records active WebSocket sessions from a South Korean academic network. Those sessions forwarded six internal service types into the workbench.

The forwarded services cover Microsoft SQL Server, SMB, Remote Desktop, Windows Remote Management, FTP, and SQL Server Analysis Services. Across target folders, the workbench also held local privilege-escalation tools. It held 11 TLS certificate files and two LSASS memory dumps.

3 **Staged cloud scripts target Microsoft Entra ID and AWS environments.** Thirty-four sampled items target cloud identity and storage services. Twenty-three scripts and logs target Microsoft 365 and Entra ID. They use single-factor password-grant requests, Microsoft Graph role queries, and password resets. Eleven more scripts query Amazon Web Services STS, S3, and Transcribe APIs.

4 **Activity continued one month after South Korean police arrests involving ARTEX.** On 26 October 2026, South Korean police announced the 15 October arrest of a suspected ringleader. Police accused the group of using ARTEX across roughly 90 organizations. Six more suspects stayed under investigation. The 16 November campus tunnel and 16 to 20 November workbench activity ran one month later. Any link to that group remains an open question.

Three Decisions for University Leaders

1. **Eliminate shared or static SSO handoff keys across campus portals.** Require unique per-campus asymmetric keys. Enforce strict algorithm, issuer, and audience checks on JWT handoff endpoints. Audit third-party .NET modules.
2. **Isolate e-learning web servers from campus Active Directory and database subnets.** Place LMS servers in demilitarized zones with outbound proxy rules. Block WebSocket reverse tunnels from reaching internal SQL Server, SMB, RDP, or WinRM ports.
3. **Block legacy authentication, require MFA so ROPC fails, and protect LSASS.** Require MFA for relevant Entra users and apps so ROPC requests fail. Block legacy authentication separately and migrate approved ROPC clients. Alert on scripted Microsoft Graph calls and enable Windows Credential Guard.

2. Workbench Architecture, 500-Entry Sample, and Regional Context

Operation CampusKey ran from a commercial virtual private server (`LIGHT NODE` , address withheld). That host ran an **ARTEX console on TCP 8787** from `16 to 19 November 2026` . On `20 November 2026` , an open directory on the same server reported **6,203 total files**.

Monograph 53 (`Operation LedgerSwarm`) examined an operator running ARTEX worker waves across fintech and Web3 targets. That operator followed web discovery with cloud-bucket scripting. Operation CampusKey follows a different workflow. Web discovery on `TCP 8787` sits

alongside a manual `.NET` reverse-engineering, Windows Active Directory, and cloud identity workspace. Figure 1 maps the four workbench tracks.

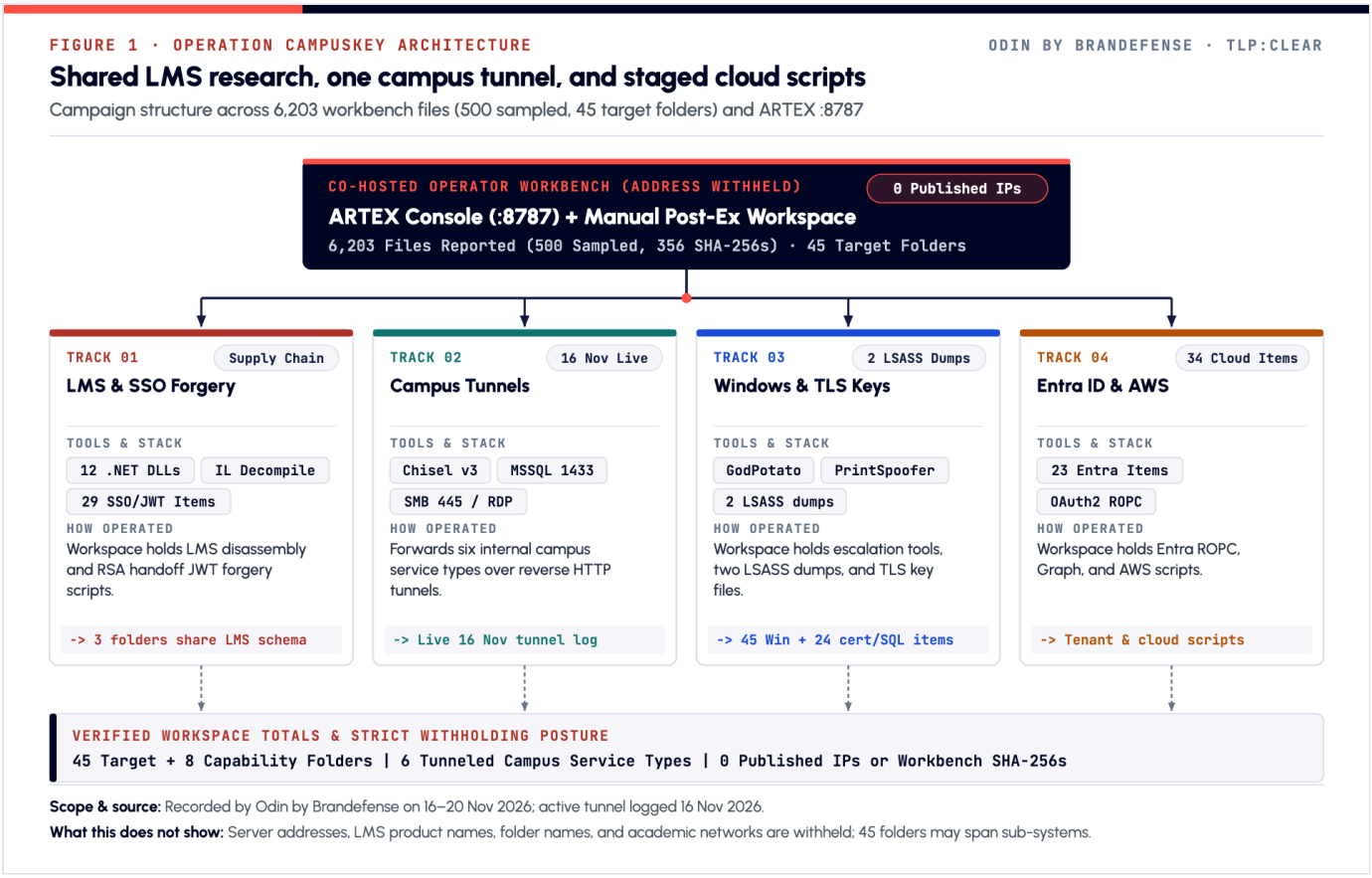


Figure 1: Shared LMS research, one campus tunnel, and staged cloud scripts

Workspace Zone Partition and File-Type Breakdown (`n = 500`)

Counts in this study come from the **500-entry sample** captured from the primary workbench. Within those **500** entries, **388** files report byte sizes totaling **70,892,250 bytes (70.89 MB)**. The remaining **112** entries omit byte size in listings. The sample spans **356 unique SHA-256 digests**, all withheld.

Workspace zone	Folder count	Sampled entries	Share (%)	Sized files	Unsized entries	Sized bytes	Unique SHA-256 (withheld)	Operational role
Numbered Target Folders	45	379	75.8%	282	97	30,963,020	256	Per-target folders holding **3** shared-schema LMS SQL dumps, `16 Nov` `chisel` logs, **2** LSASS memory dumps, and mail tests.
Functional Capability Folders	8	55	11.0%	42	13	3,197,973	41	Dedicated folders for `.NET` LMS disassembly, SSO scripts, Entra Graph scripts, AWS scripts, and TLS key stores.
Root Operator Workspace	1 (root)	66	13.2%	64	2	36,731,257	64	Top-level RSA/JWT forgery scripts, compiled binaries, and session logs.
Combined primary sample	**53 dirs + root**	**500**	**100.0%**	**388**	**112**	**70,892,250**	**356** (cross-zone)	**Sample from 6,203 directory-reported total files (`20 Nov 2026`).**

One analytical limit governs the **45 numbered target folders**. Folder names use internal numeric codes, which are withheld. Directory listings alone cannot show whether **45** folders equal **45** distinct institutions. Universities often run separate sub-domains for main portals, e-learning, libraries, and departments. Defenders can use external attack surface management to inventory them.

Artifact class	Sampled entries	Share (%)	Sized files	Unsized entries	Sized bytes	Representative extensions & contents
Scripts (`script`)	227	45.4%	199	28	858,990	147 `.py`, 25 `.ps1`, 17 `.php`, 16 `.js`, and shell wrappers.
Text & logs (`text`)	150	30.0%	140	10	1,380,922	46 `.log`, 18 `.out`, 15 `.txt`, and disassembled `.NET` IL files.
Binaries & libraries (`exe`)	74	14.8%	16	58	23,625,412	12 `.NET` `.dll` assemblies and tools including `chisel`, `GodPotato`, and `PrintSpoofer`; extension counts require recounting.
Data & memory dumps (`data`)	14	2.8%	8	6	28,793,918	7 `.sql` database dumps (3 sharing one LMS schema) and 2 LSASS memory dumps.
Archives (`archive`)	13	2.6%	7	6	15,745,642	12 `.zip` archives and 1 compressed package.
Secrets & keys (`secret`)	12	2.4%	12	0	272,366	RSA handoff PEM keys, signed JWTs, and harvested TLS/PFX files.
Other (`other`)	8	1.6%	4	4	135,640	Raw HTTP session state and binary fragments.
Documents (`doc`)	2	0.4%	2	0	79,360	Target architecture and reference notes.

Artifact class	Sampled entries	Share (%)	Sized files	Unsized entries	Sized bytes	Representative extensions & contents
Total	500	100.0%	388	112	70,892,250	Exact byte-level parity (70.89 MB).

Figure 5 divides the **500** sampled entries into six mutually exclusive kill-chain clusters (`311 + 63 + 45 + 34 + 24 + 23 = 500`). LMS forgery, campus tunnelling, Windows escalation, TLS and SQL collection, and cloud identity files make up **37.8%** (**189** entries).

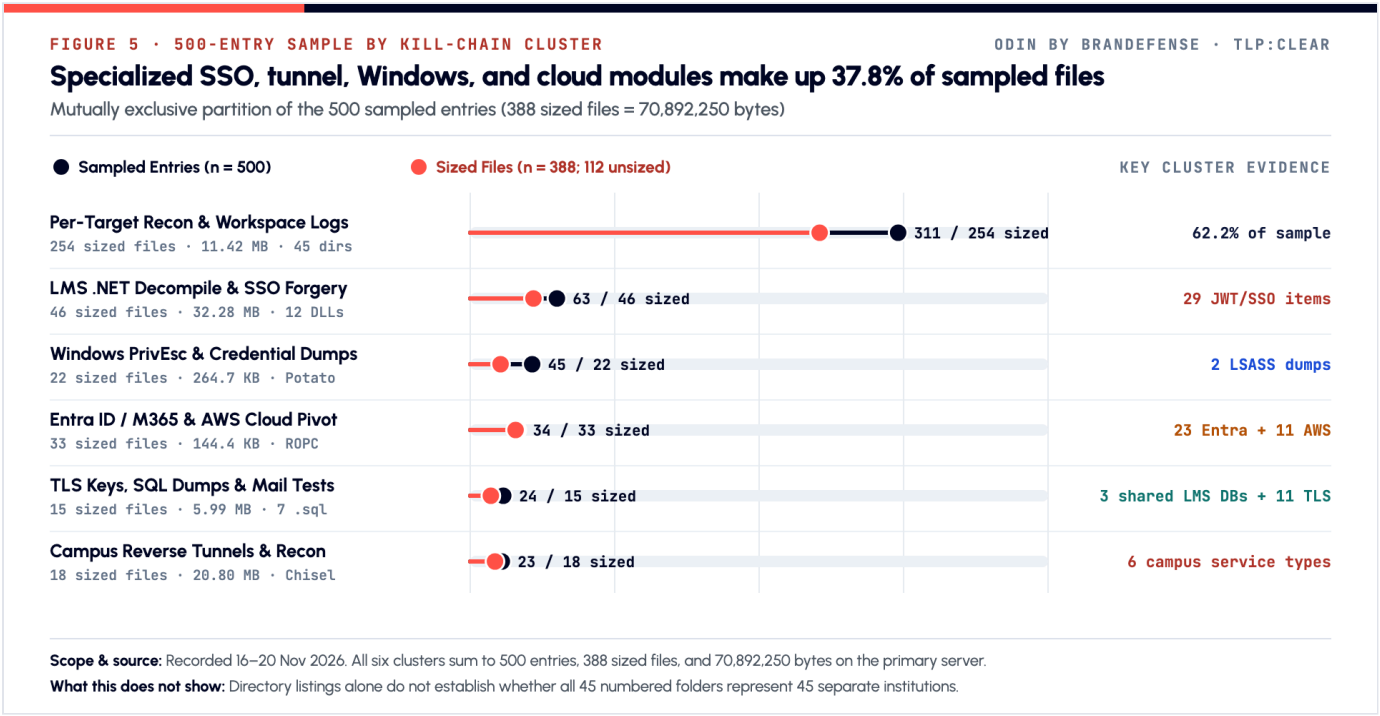


Figure 5: Specialized SSO, tunnel, Windows, and cloud modules make up 37.8% of sampled files

Post-Arrest Regional ARTEX Context and `/24` Neighbour Comparison

Two external and hosting facts place Operation CampusKey in clear context:

- **Activity one month after South Korean ARTEX arrests (`[REF-01]` , `[REF-02]`).** On `26 October 2026` , Seoul police announced the `15 October` arrest of a former penetration tester (`[REF-01]`). Police stated that the group used ARTEX (`[REF-03]` , `[REF-04]`). The group

targeted roughly **90** organizations, including universities. Police reported `8.2 million` stolen records. Six suspects stayed under investigation. The CampusKey ARTEX console (`16-19 November`), tunnel log (`16 November`), and open directory (`20 November`) ran **one month after** that arrest. Artifacts alone cannot show whether this host belongs to remaining suspects, copycats, or an unrelated operator.

- **Unconfirmed `/24` neighbour.** On `16 November 2026` , a second open directory sat in the same `/24` `LIGHT NODE` subnet (address withheld). That directory held **41** entries, **79,922** bytes, and **36** SHA-256s. It staged Linux privilege-escalation code for `CVE-2021-3156` (`sudo` before `1.9.5p2` ; fixed in `1.9.5p2` , `[REF-09]`) and `CVE-2021-4034` (`polkit` `pkexec` before **121**; fixed upstream in **121**, `[REF-10]`). Comparing all **356** primary digests with all **36** neighbour digests yields **0 shared hashes**. We therefore treat the second server strictly as an unconfirmed neighbour.

3. Shared LMS Reverse Engineering, SSO Forgery, and Live Campus Tunnels

Regional universities often adopt the same `.NET` e-learning packages. They link those portals to campus single sign-on with signed JSON Web Token (JWT) redirects. Figure 3 maps a possible sequence that cyber threat intelligence can help defenders investigate across campus networks.

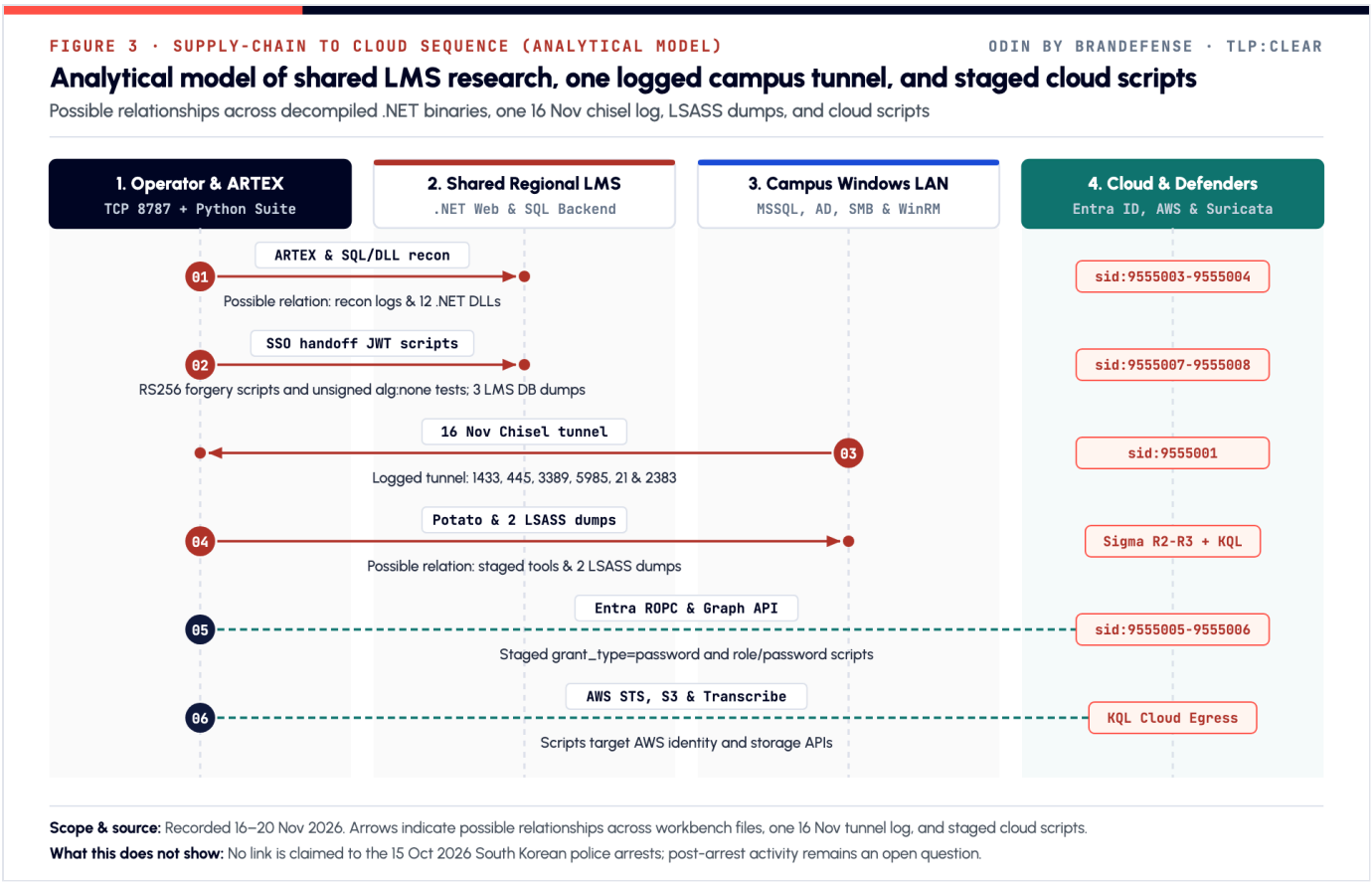


Figure 3: Analytical model of shared LMS research, one logged campus tunnel, and staged cloud scripts

`.NET` Disassembly and RSA / JWT SSO Token Forgery (63 Entries)

Within the LMS capability folder and root workspace (**63** entries, **32,278,804** sized bytes), the operator collected **12 compiled `.NET` `.dll` assemblies**. Those binaries belong to a South Korean e-learning product, with the vendor and filenames withheld.

The operator ran custom Python Intermediate Language (IL) disassembly scripts on those files. The scripts extracted class structures, token checks, and signing parameters.

From that disassembled code, the operator built **29 SSO and JWT token-forgery scripts, PEM keys, and test outputs**. Two artifact groups stand out in this cluster:

- **Handoff token forgery (`RS256` and `alg:none` checks).** Campus main portals authenticate users and redirect them to the LMS with a signed handoff JWT. The staged scripts use extracted RSA private keys (`.pem`) and unsigned `alg:none` validation tests. They build administrative SSO tokens designed to bypass interactive MFA prompts.

- **Shared LMS database dumps.** The TLS and SQL cluster holds **24** entries (**5,990,594** sized bytes), including **11** `.pem`, `.pfx`, `.key`, and `.crt` files and **7** `.sql` dumps. Three separate numbered target folders hold database dumps of the identical LMS schema. That overlap supports reuse of the same LMS product across targets.

Live `16 November 2026` Campus Reverse Tunnels (23 Entries) and Windows Post-Exploitation (45 Entries)

Campus firewalls normally block direct internet access to internal SQL and Active Directory servers. The tunnel cluster holds **23** entries (**20,798,257** sized bytes). In that cluster, the operator used `chisel` (`[REF-08]`) to wrap TCP port-forwards inside outbound HTTP WebSocket and SSH sessions.

Inside one numbered target folder, a `chisel` server log dated `16 November 2026` **(21:36)** records live reverse tunnels from a South Korean academic network (subnet withheld). Those sessions forwarded **six internal campus service types**:

1. **Microsoft SQL Server (`TCP 1433`).** Direct access to internal campus relational databases.
2. **SMB (`TCP 445`).** Windows file shares, RPC named pipes, and NTLM authentication surfaces.
3. **Remote Desktop Protocol (`TCP 3389`).** Interactive desktop sessions to internal Windows hosts.
4. **Windows Remote Management (`TCP 5985` and 5986).** PowerShell Remoting and WinRM management ports.
5. **FTP (`TCP 21`).** Legacy campus file and web-publishing servers.
6. **SQL Server Analysis Services (`TCP 2383`).** Campus analytics cubes (`SSAS`) holding student and administrative data.

The Windows post-exploitation cluster holds **45** entries (**264,679** sized bytes) alongside internal scanner logs (`fscan`). It includes two host-level privilege and credential artifact groups:

- **Named-pipe privilege escalation tools.** IIS and `.NET` application pools hold `SeImpersonatePrivilege`. The workbench staged `GodPotato` and `PrintSpoofer` binaries designed to elevate web service accounts to `SYSTEM`.
- **Two LSASS memory dumps.** Two separate numbered target folders hold captured LSASS memory dumps. Those folders also hold RPC and NTLM scripts and offline password-cracking

logs.

4. Federated Cloud Identity Pivots: Microsoft Entra ID and AWS

Universities sync Active Directory accounts with **Microsoft 365 / Entra ID** for mail and administration. Many also link lecture-captioning workloads to **AWS**. Figure 4 shows the co-hosted workbench layout. Separately from the on-campus dumps, the cloud cluster (**34** entries, **144,360** sized bytes) holds staged Entra ID and AWS scripts.

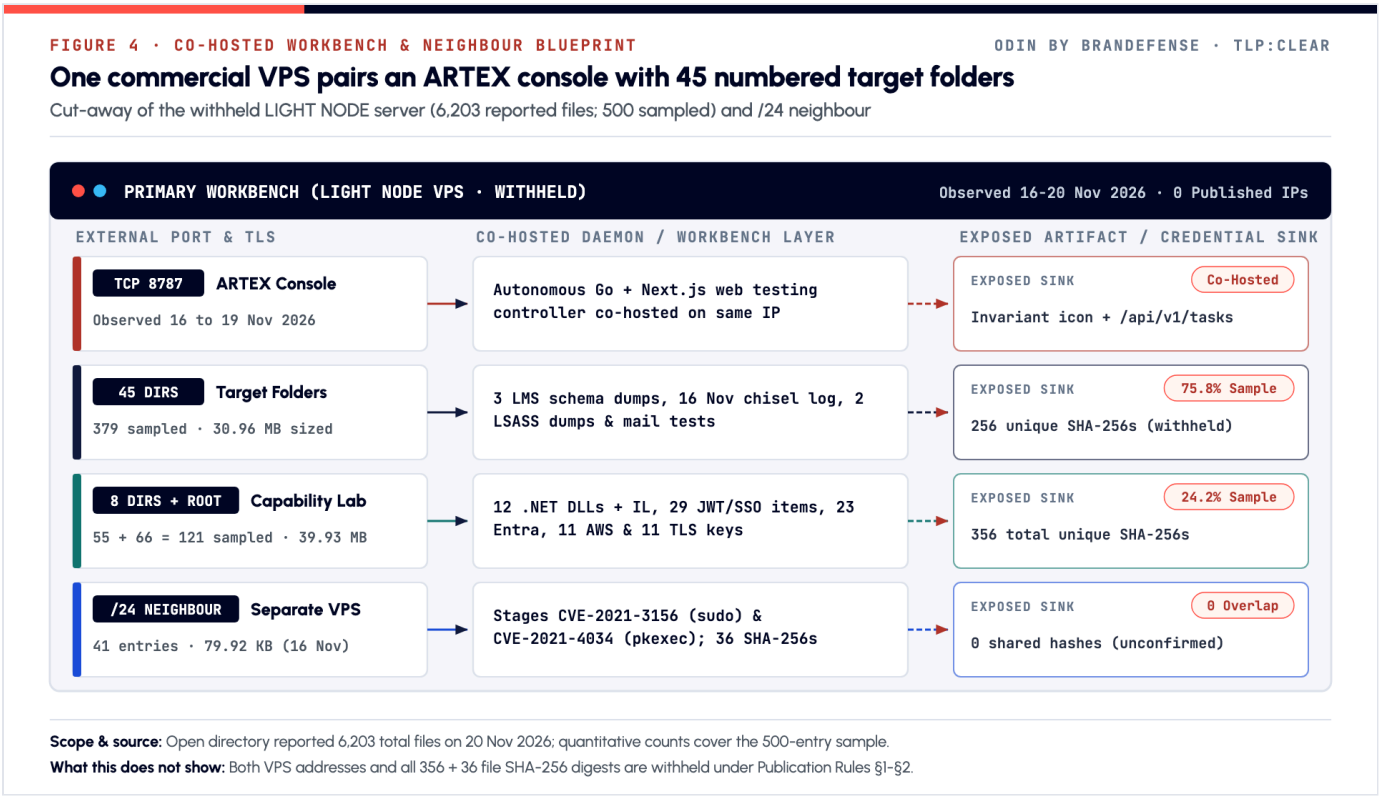


Figure 4: One commercial VPS pairs an ARTEX console with 45 numbered target folders

OAuth 2.0 `ROPC`, Microsoft Graph (23 Items), and AWS (11 Items)

The cloud folder holds **23 Microsoft 365 and Entra ID scripts, token files, and outputs**. This staged tooling targets sign-in and directory APIs in three ways.

- **Legacy `ROPC` single-factor token requests (`[REF-05]`).** Staged Python scripts prepare `POST` requests to `login.microsoftonline[.]com/<tenant>/oauth2/v2.0/token` with `grant_type=password`. Resource Owner Password Credentials (`ROPC`) requests cannot carry MFA challenges (`[REF-05]`). Some tenants do not require MFA for the user and app in

Conditional Access. In those cases, valid passwords can return Graph bearer tokens (`[REF-05]` , `[REF-06]`).

- **Microsoft Graph role queries and password-reset scripts.** Companion scripts query `graph.microsoft[.]com/v1.0/users` and `graph.microsoft[.]com/v1.0/directoryRoles` . They list privileged roles and issue `passwordProfile` reset calls.
- **AWS scripts and mail tests.** Eleven scripts query `sts.amazonaws[.]com` caller identity, `S3` buckets, and `Amazon Transcribe` captioning jobs tied to lecture portals. A separate target folder holds SMTP and typo-domain sender-spoofing test scripts.

Figure 2 maps the five workbench artifact groups to the Suricata, Sentinel KQL, Sigma, and YARA rules in Chapter 7.

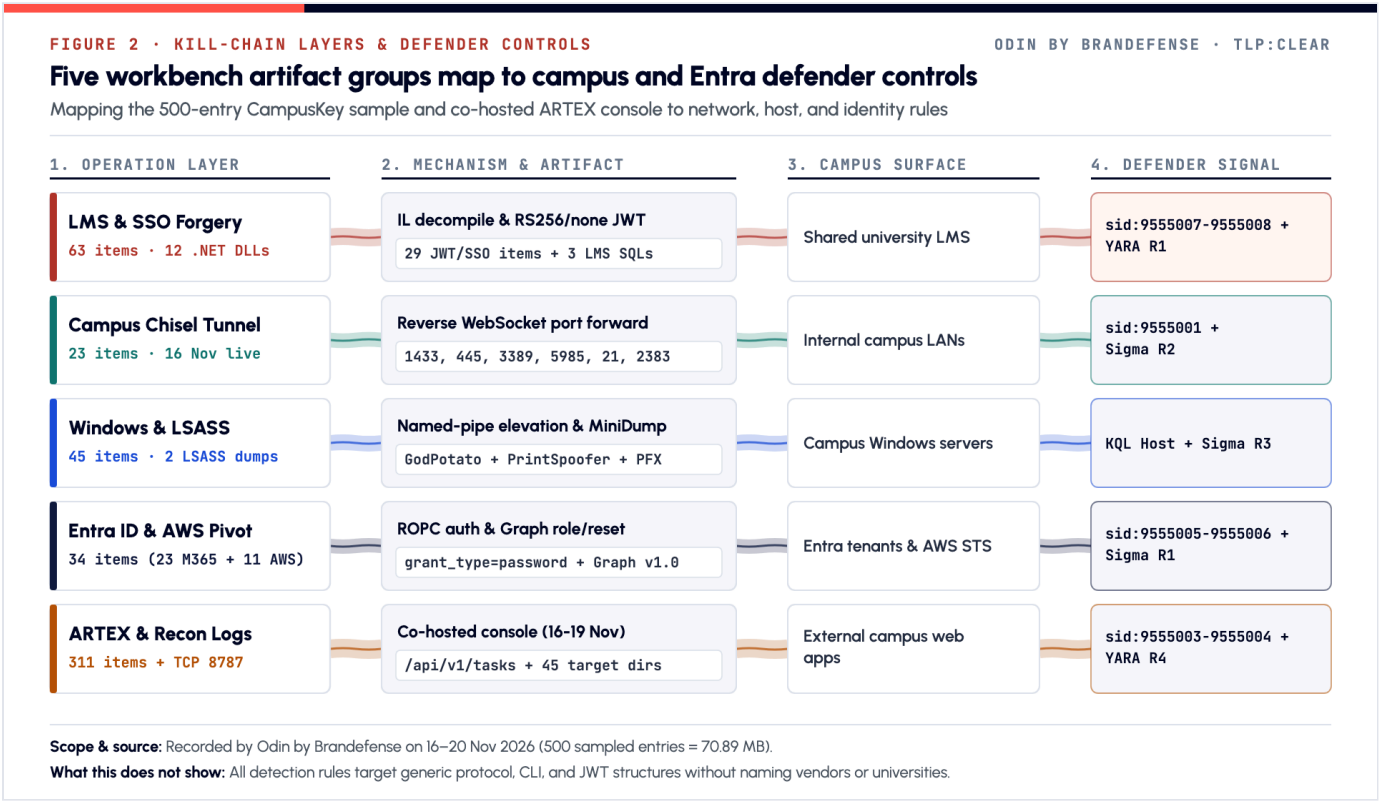


Figure 2: Five workbench artifact groups map to campus and Entra defender controls

5. Higher-Education Supply-Chain Exposure Analysis

The workbench shows four artifact groups. Campus teams should verify the related controls before treating any configuration as a root cause:

Exposure layer	Observed CampusKey evidence	Control to verify	Operational risk
Shared `.NET` LMS & SSO bridges	12 `.dll` files, 29 JWT/SSO items, 3 shared LMS SQL dumps.	Verify whether campuses share LMS modules or signing keys; the evidence establishes a shared database schema.	Cross-campus reuse of the forgery scripts remains unverified.
Campus network segmentation	`16 Nov` `chisel` tunnel to 1433, 445, 3389, 5985/5986, 21, 2383.	Verify the tunnel's origin host and its access to internal services; the log does not establish LMS server routing.	If a web host can reach these services, a foothold could expose internal administration ports.
LSASS protection & TLS key handling	`GodPotato`, `PrintSpoofer`, 2 LSASS memory dumps, 11 TLS/PFX files.	Verify IIS privileges, Credential Guard status, and TLS key export settings.	`SYSTEM` elevation, domain credential theft, and TLS key theft.
Entra `ROPC` & AWS key handling	23 Entra (`ROPC` + Graph) items and 11 AWS (`STS`, `S3`, `Transcribe`) items.	Verify whether ROPC grants can succeed without MFA and whether LMS hosts retain static AWS keys.	Single-factor cloud token minting, role checks, and bucket access.

6. Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
Splinter or continuation of arrested Korean ARTEX ring (`[REF-01]`)	Co-hosts ARTEX (:8787), targets Korean campuses, and ran one month after the `15 Oct` arrest while six suspects remained under investigation.	ARTEX is open-source; Censys counted 1,465 exposed consoles on 4 November 2026. Police forensic indicators are non-public.	**Open question.** Cite the October arrest strictly as context, not attribution.

Hypothesis	Evidence for	Evidence against	Assessment
45 **numbered folders equal** 45 **breached institutions**	45 distinct numbered directories hold 379 sampled entries (75.8%).	Universities run multiple sub-portals per campus, and several folders hold recon or mail tests only.	**Unsupported as an exact victim count.** State verified dump counts (3 shared LMS SQLs; 2 LSASS dumps).
Authorized red-team engagement	Uses numbered folders, `ARTEX`, and standard tunnel utilities.	Stores 3 LMS SQL dumps, 2 LSASS dumps, TLS private keys, and typo-domain mail tests on an open foreign VPS.	**Contradicted.** Multi-victim data retention and open exposure violate authorized testing rules.
Linked `/24` **VPS neighbour (41 entries)**	Same `/24` `LIGHT NODE` subnet observed on `16 November 2026`.	Comparing 356 primary hashes with 36 neighbour hashes shows 0 **shared digests**, and toolsets differ.	**Unconfirmed neighbour.** Shared VPS `/24` tenancy is routine; both IPs are withheld.

7. Validated Detection Rules

All VPS addresses and workbench-file SHA-256 digests are withheld. Defenders should deploy **protocol, CLI, and identity rules** that catch this tradecraft across any host. Every rule was tested before release. Checks passed on Suricata `7.0.12` (`suricata -T` and linter, 0 problems), Microsoft `Kusto.Language` (0 errors), `pySigma` (3 rules), and `YARA-X` (4 `filesize`-bounded rules).

7.1 Suricata 7.x Network Signatures (`sid:9555001`, `sid:9555003`-9555008)

These seven `alert` signatures detect `chisel-v3` WebSocket reverse tunnels and exposed or queried ARTEX consoles on TCP **8787**. They also match OAuth 2.0 `grant_type=password` (`ROPC`) requests, scripted Graph `passwordProfile` resets, and inbound `alg:none` JWT headers (`eyJhbGciOiJub25lIg`).

All seven HTTP rules need cleartext traffic or a sensor behind a TLS-inspecting proxy or reverse proxy. Defenders should enforce inline blocks in the firewall or proxy.

```
SURICATA

# Odin by Brandefense - Monograph 55 (Operation CampusKey) Suricata 7.x Ruleset
# Validated against Suricata 7.0.12 (-T) and Odin Suricata linter (0 warnings).

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R55 CampusKey Outbound Chisel
v3 WebSocket Reverse Tunnel Handshake"; flow:established,to_server; http.header; conte
nt:"Sec-WebSocket-Protocol: chisel-v3"; nocase; fast_pattern; classtype:command-and-co
ntrol; sid:9555001; rev:1;)
alert http $EXTERNAL_NET 8787 -> $HOME_NET any (msg:"ODIN-R55 CampusKey Exposed ARTEX
Console Response Banner on TCP 8787"; flow:established,to_client; http.response_body;
content:"ARTEX - Autonomous Red-Team Expert"; fast_pattern; classtype:trojan-activity;
sid:9555003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET 8787 (msg:"ODIN-R55 CampusKey Outbound ARTEX
Task Dispatch API Call"; flow:established,to_server; http.method; content:"POST"; bsiz
e:4; http.uri; content:"/api/v1/tasks"; startswith; fast_pattern; classtype:trojan-act
ivity; sid:9555004; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R55 CampusKey Legacy OAuth2 R
OPC Password Grant Token Request"; flow:established,to_server; http.method; content:"P
OST"; bsize:4; http.request_body; content:"grant_type=password"; fast_pattern; conten
t:"scope="; classtype:policy-violation; sid:9555005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R55 CampusKey Scripted Graph
API Password Reset Payload"; flow:established,to_server; http.request_body; content:"p
asswordProfile"; fast_pattern; content:"forceChangePasswordNextSignIn"; classtype:atte
mpted-admin; sid:9555006; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R55 CampusKey Inbound Unauthe
nticated alg-none JWT Header"; flow:established,to_server; http.header; content:"eyJhb
GciOiJub25lIg"; fast_pattern; classtype:web-application-attack; sid:9555007; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R55 CampusKey Inbound Unauthe
nticated alg-none JWT Handoff Query"; flow:established,to_server; http.uri; content:"e
yJhbGciOiJub25lIg"; fast_pattern; classtype:web-application-attack; sid:9555008; rev:
1;)
```

7.2 Microsoft Sentinel KQL Hunt

Replace the two placeholder FQDNs in `ApprovedAutomationHosts` with your campus IAM sync host allowlist before scheduling.

```kql
// Odin by Brandefense - Monograph 55 (Operation CampusKey)
// Hunts campus Chisel reverse tunnels, LSASS/Potato escalation, and non-browser Pytho
n/PowerShell calls to Entra ID and AWS STS.
let Lookback = 7d;
let ApprovedAutomationHosts = dynamic(["iam-sync-01.campus.example", "cloud-backup-01.
campus.example"]);
let CampusTunnelPorts = dynamic([":1433", ":445", ":3389", ":5985", ":5986", ":21", ":
2383"]);
let HostTunnelAndPostEx =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAutomationHosts))
    | where (
        (ProcessCommandLine has "chisel" and ProcessCommandLine has "client" and Proce
ssCommandLine matches regex @"(^|[^0-9]):(1433|445|3389|5985|5986|21|2383)([^0-9]|$)")
        or (ProcessCommandLine has_any ("GodPotato", "PrintSpoofer") or (ProcessComman
dLine has_any ("comsvcs.dll", "lsass") and ProcessCommandLine has "MiniDump"))
        or (ProcessCommandLine has "grant_type=password" and ProcessCommandLine has_an
y ("microsoftonline.com", "graph.microsoft.com"))
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "CampusPostExOrTunnel",
Detail = ProcessCommandLine;
let ScriptedCloudIdentityCalls =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAutomationHosts))
    | where InitiatingProcessFileName in~ ("python.exe", "python3", "python", "powersh
ell.exe", "pwsh.exe", "pwsh")
    | where RemoteUrl has_any ("login.microsoftonline.com", "graph.microsoft.com", "st
s.amazonaws.com", "transcribe.")
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, Signa
lType = "ScriptedCloudIdentityEgress", Detail = strcat(InitiatingProcessFileName, " ->
", RemoteUrl, " (", RemoteIP, ":", tostring(RemotePort), ")");
union HostTunnelAndPostEx, ScriptedCloudIdentityCalls
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count
(), Signals = make_set(SignalType, 6), SampleDetails = make_set(Detail, 5) by DeviceNa
me, AccountName
| order by LastSeen desc
```

7.3 Portable Sigma and YARA Rules

- **Sigma (`sigma_campuskey_entra_ropc_chisel_and_lsass.yml`).** Rule 1 detects CLI scripts passing `grant_type=password`, `/v1.0/directoryRoles`, or `passwordProfile`. Rule 2 catches `chisel` reverse tunnels (`R:`) across :**1433**, :**445**, :**3389**, :**5985**, :**5986**, :**21**, or :**2383**. Rule 3 detects Windows process command lines mentioning `GodPotato`, `PrintSpoofer`, or `comsvcs.dll` `MiniDump`.
- **YARA (`odin_campuskey_jwt_forger_and_postex_artifacts.yar`).** Four `filesize`-bounded generic rules detect RS256 JWT token-forgery scripts and `chisel` multi-service tunnel logs. They also match Entra `ROPC` and Graph reset scripts and exposed ARTEX console bundles.

8. Behavioral and Protocol Hunt Markers (0 Published IPs or Workbench SHA-256s)

No VPS IPv4 addresses or workbench-file SHA-256 digests appear in the indicator feeds. The server holds campus database dumps, LSASS dumps, and TLS private keys. Defenders should hunt using the 10 protocol, API, and host markers below.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
WebSocket tunnel header	`Sec-WebSocket-Protocol: chisel-v3`	HTTP / TLS egress	Alert on visible `chisel` WebSocket upgrades with `sid:9555001`. Enforce outbound blocks in the proxy or firewall.
Inner Chisel SSH string	`SSH-2.0-chisel`	WebSocket stream / host	Match in decapsulated WebSocket streams or host binaries. Client WebSocket frames mask this banner on raw TCP.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
ARTEX console icon MD5	`cd3ebd16437d6d3963592f7365dd3980`	TCP 8787	Use the favicon MD5 in external asset sweeps. Rule `sid:9555003` alerts on a visible ARTEX response-body banner.
ARTEX dispatch route	`POST /api/v1/tasks`	TCP 8787	Hunt proxy logs for outbound ARTEX task calls (`sid:9555004`).
Entra legacy OAuth flow	`grant_type=password` (`login.microsoftonline[.]com`)	HTTPS (443)	Hunt Entra sign-in logs. Rule `sid:9555005` alerts on visible HTTP at a TLS-inspecting proxy.
Microsoft Graph admin API	`/v1.0/directoryRoles` & `passwordProfile`	HTTPS (443)	Alert on scripted Graph calls in Entra logs or decrypted proxy HTTP (`sid:9555006`).
Forged JWT header (`none`)	`eyJhbGciOiJub25lIg` (`{"alg":"none"`)	HTTP / TLS ingress	Reject `alg:none` JWTs in the LMS. Rules `sid:9555007` - 9555008 alert on visible HTTP.
SSO handoff JWT (`RS256`)	`eyJhbGciOiJSUzI1NiIs` (`RS256` SSO handoff)	HTTPS (443)	Enforce unique per-campus RSA keys, strict `iss` / `aud` checks, and `<=60s` lifetimes.
Credential dump artifact	`comsvcs.dll MiniDump` / LSASS access	Windows EDR	Enable LSA Protection (`RunAsPPL`) and Credential Guard, and alert on LSASS memory reads.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
Token impersonation family	`GodPotato` / `PrintSpoofer`	Windows EDR	Alert on Windows process command lines mentioning `GodPotato`, `PrintSpoofer`, or `comsvcs.dll MiniDump` (Sigma Rule 3).

9. Hardening Priorities for Universities and EdTech Vendors

Campus security teams should close third-party portal and cloud identity gaps together:

1. **Re-key third-party LMS SSO handoff bridges (`0-48 Hours`).** Replace shared or vendor-default signing keys with unique per-campus RSA or ECDSA keys (`[REF-07]`). Store those keys outside the web root. Allowlist `RS256` or `ES256` only and reject `alg:none`. Check `iss` and `aud`, and cap handoff token lifetimes at **60** seconds.
2. **Block legacy authentication, require MFA against `ROPC`, and remove static cloud keys (`0-72 Hours`):** Require MFA for relevant Entra users and apps so `ROPC` password grants fail. Block legacy authentication separately. Migrate approved `ROPC` clients (`[REF-05]`, `[REF-06]`). Require phishing-resistant MFA for directory admins. Replace static AWS keys on lecture-caption servers with IAM roles.
3. **Isolate LMS servers (`Days 1-7`).** Place e-learning hosts in DMZ VLANs. Block them from initiating internal **1433**, **445**, **3389**, **5985**, **21**, or **2383** connections (`[REF-08]`). Enforce outbound proxy allowlists to block `chisel` tunnels.
4. **Protect LSASS and TLS keys (`Days 7-14`).** Enable `RunAsPPL` and Windows Defender Credential Guard on campus Windows servers. Mark institutional TLS private keys as **non-exportable** in the Windows Certificate Store.
5. **Enforce DMARC and review binaries (`Days 14-30`).** Publish SPF, DKIM, and DMARC (`p=reject`) records on `.ac.kr` and university mail domains. Require EdTech vendors to audit compiled `.NET` modules for hardcoded keys before deployment.

10. Scope, Limits, and External References

Odin by Brandefense analyzed workbench artifacts recorded between `16 and 20 November 2026`. File counts cover the **500**-entry sample (**70.89 MB** across **388** sized files). That sample came from an open directory reporting **6,203** total files on `20 November 2026`.

Directory listings alone do not show how many distinct institutions map to the **45** numbered target folders. Staged cloud scripts likewise do not show how many tenants experienced account changes. Both VPS addresses, all **356 + 36** workbench-file SHA-256 digests, LMS vendor names, folder names, and academic identifiers are withheld.

1. `[REF-01]` BleepingComputer, *Former pentester used ARTEX AI to steal 8.2 million data records* (26 October 2026; verified on 22 November 2026).
2. `[REF-02]` FBI Cyber Division, *FLASH-20261113-001: Malicious Use of Autonomous Penetration Testing Tool ARTEX* (13 November 2026)
3. `[REF-03]` Help Net Security, *ARTEX Goes from Pentesting Tool to Attacker Staple in Three Months* (9 November 2026)
4. `[REF-04]` Infosecurity Magazine, *FBI Warns of Growing Abuse of AI Pentesting Frameworks* (November 2026)
5. `[REF-05]` Microsoft Learn, *Microsoft Identity Platform and OAuth 2.0 Resource Owner Password Credentials (ROPC)*
6. `[REF-06]` Microsoft Learn, *Token Protection in Microsoft Entra Conditional Access*
7. `[REF-07]` IETF, *JSON Web Token Best Current Practices (RFC 8725)* (verified on 22 November 2026)
8. `[REF-08]` MITRE ATT&CK, *Protocol Tunneling (T1572)*
9. `[REF-09]` NIST NVD, *CVE-2021-3156 - Sudo Heap-Based Buffer Overflow*
10. `[REF-10]` NIST NVD, *CVE-2021-4034 - Polkit pkexec Local Privilege Escalation*

BRANDEFENSE CAPABILITIES RELATED TO THIS RESEARCH

Cyber Threat Intelligence

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

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_campuskey_chisel_artex_and_ropc_hunt.rules` 11 lines

```
# Odin by Brandefense - Monograph 55 (Operation CampusKey) Suricata 7.x Ruleset
# Validated against Suricata 7.0.12 (-T) and Odin Suricata linter (0 warnings).

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R55 CampusKey Outbound Chisel
v3 WebSocket Reverse Tunnel Handshake"; flow:established,to_server; http.header; conte
nt:"Sec-WebSocket-Protocol: chisel-v3"; nocase; fast_pattern; classtype:command-and-co
ntrol; sid:9555001; rev:1;)
alert http $EXTERNAL_NET 8787 -> $HOME_NET any (msg:"ODIN-R55 CampusKey Exposed ARTEX
Console Response Banner on TCP 8787"; flow:established,to_client; http.response_body;
content:"ARTEX - Autonomous Red-Team Expert"; fast_pattern; classtype:trojan-activity;
sid:9555003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET 8787 (msg:"ODIN-R55 CampusKey Outbound ARTEX
Task Dispatch API Call"; flow:established,to_server; http.method; content:"POST"; bsiz
e:4; http.uri; content:"/api/v1/tasks"; startswith; fast_pattern; classtype:trojan-act
ivity; sid:9555004; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R55 CampusKey Legacy OAuth2 R
OPC Password Grant Token Request"; flow:established,to_server; http.method; content:"P
OST"; bsize:4; http.request_body; content:"grant_type=password"; fast_pattern; conten
t:"scope="; classtype:policy-violation; sid:9555005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R55 CampusKey Scripted Graph
API Password Reset Payload"; flow:established,to_server; http.request_body; content:"p
asswordProfile"; fast_pattern; content:"forceChangePasswordNextSignIn"; classtype:atte
mpted-admin; sid:9555006; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R55 CampusKey Inbound Unauthe
nticated alg-none JWT Header"; flow:established,to_server; http.header; content:"eyJhb
GciOiJub25lIg"; fast_pattern; classtype:web-application-attack; sid:9555007; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R55 CampusKey Inbound Unauthe
nticated alg-none JWT Handoff Query"; flow:established,to_server; http.uri; content:"e
yJhbGciOiJub25lIg"; fast_pattern; classtype:web-application-attack; sid:9555008; rev:
1;)
```

Show full rule

YARA `odin_campuskey_jwt_forger_and_postex_artifacts.yar` 74 lines

```
/*
   Odin by Brandefense - Monograph 55 (Operation CampusKey) YARA Suite
```

```
   4 filesize-bounded structural rules covering RSA/JWT SSO token forgers, Chisel camp
us tunnel logs,
   Entra ID ROPC/Graph scripts, and co-hosted ARTEX consoles (zero victim or vendor id
entifiers).
*/

rule ODIN_CampusKey_RSA_JWT_SSO_Token_Forger
{
    meta:
        author = "Odin by Brandefense"
        monograph = "55"
        description = "Detects custom Python scripts forging RS256-signed SSO handoff
JWTs using extracted PEM private keys"
        date = "2026-11-22"
    strings:
        $j1 = "jwt.encode" ascii
        $j2 = "RS256" ascii
        $k1 = "BEGIN RSA PRIVATE KEY" ascii
        $k2 = "BEGIN PRIVATE KEY" ascii
        $k3 = "load_pem_private_key" ascii
    condition:
        filesize < 128KB and $j1 and $j2 and ($k1 or $k2 or $k3)
}

rule ODIN_CampusKey_Chisel_Campus_Service_Tunnel_Log
{
    meta:
        author = "Odin by Brandefense"
        monograph = "55"
        description = "Detects Chisel reverse-tunnel logs forwarding multiple internal
Windows and database service ports"
        date = "2026-11-22"
    strings:
        $c1 = "server: session#" ascii nocase
        $c2 = "tun:" ascii nocase
        $p1 = ":1433" ascii
        $p2 = ":445" ascii
        $p3 = ":3389" ascii
        $p4 = ":5985" ascii
        $p5 = ":2383" ascii
    condition:
        filesize < 2MB and ($c1 or $c2) and 3 of ($p*)
}

rule ODIN_CampusKey_Entra_ROPC_and_Graph_Reset_Script
{
    meta:
```

```
        author = "Odin by Brandefense"
        monograph = "55"
        description = "Detects scripts combining Entra ID OAuth2 ROPC password grants
with Microsoft Graph role or password operations"
        date = "2026-11-22"
    strings:
        $r1 = "login.microsoftonline.com" ascii nocase
        $r2 = "grant_type" ascii
        $r3 = "graph.microsoft.com/v1.0/" ascii nocase
        $g1 = "directoryRoles" ascii
        $g2 = "passwordProfile" ascii
    condition:
        filesize < 256KB and $r1 and $r2 and $r3 and ($g1 or $g2)
}

rule ODIN_CampusKey_ARTEX_Console_and_Task_API
{
    meta:
        author = "Odin by Brandefense"
        monograph = "55"
        description = "Detects exposed ARTEX autonomous testing console bundles and ta
sk API definitions"
        date = "2026-11-22"
    strings:
        $a1 = "ARTEX - Autonomous Red-Team Expert" ascii
        $a2 = "/api/v1/tasks" ascii
        $a3 = "artex-swarm-root" ascii
    condition:
        filesize < 5MB and $a1 and ($a2 or $a3)
}
```

Sentinel KQL **sentinel_campuskey_ropc_graph_and_campus_tunnel_hunt.kql**

26 lines

```
// Odin by Brandefense - Monograph 55 (Operation CampusKey)
// Hunts campus Chisel reverse tunnels, LSASS/Potato escalation, and non-browser Pytho
n/PowerShell calls to Entra ID and AWS STS.
let Lookback = 7d;
let ApprovedAutomationHosts = dynamic(["iam-sync-01.campus.example", "cloud-backup-01.
campus.example"]);
let CampusTunnelPorts = dynamic([":1433", ":445", ":3389", ":5985", ":5986", ":21", ":
2383"]);
let HostTunnelAndPostEx =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
```

```
    | where not(DeviceName in~ (ApprovedAutomationHosts))
    | where (
        (ProcessCommandLine has "chisel" and ProcessCommandLine has "client" and Proce
ssCommandLine matches regex @"(^|[^0-9]):(1433|445|3389|5985|5986|21|2383)([^0-9]|$)")
        or (ProcessCommandLine has_any ("GodPotato", "PrintSpoofer") or (ProcessComman
dLine has_any ("comsvcs.dll", "lsass") and ProcessCommandLine has "MiniDump"))
        or (ProcessCommandLine has "grant_type=password" and ProcessCommandLine has_an
y ("microsoftonline.com", "graph.microsoft.com"))
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "CampusPostExOrTunnel",
Detail = ProcessCommandLine;
let ScriptedCloudIdentityCalls =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAutomationHosts))
    | where InitiatingProcessFileName in~ ("python.exe", "python3", "python", "powersh
ell.exe", "pwsh.exe", "pwsh")
    | where RemoteUrl has_any ("login.microsoftonline.com", "graph.microsoft.com", "st
s.amazonaws.com", "transcribe.")
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, Signa
lType = "ScriptedCloudIdentityEgress", Detail = strcat(InitiatingProcessFileName, " ->
", RemoteUrl, " (", RemoteIP, ":", tostring(RemotePort), ")");
union HostTunnelAndPostEx, ScriptedCloudIdentityCalls
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count
(), Signals = make_set(SignalType, 6), SampleDetails = make_set(Detail, 5) by DeviceNa
me, AccountName
| order by LastSeen desc
```

Sigma `sigma_campuskey_entra_ropc_chisel_and_lsass.yml` 90 lines

```
title: CampusKey Scripted Entra ID ROPC and Graph Role Enumeration
id: 7f39b8d4-2a19-4c63-8e12-55b20f84d201
status: experimental
description: Detects command-line Python or shell scripts invoking Microsoft Entra ID
legacy ROPC password grants or querying Microsoft Graph directoryRoles and passwordPro
file endpoints.
author: Odin by Brandefense
date: 2026-11-22
logsource:
  category: process_creation
  product: linux
detection:
  selection_ropc:
    CommandLine|contains:
      - 'grant_type=password'
      - '/v1.0/directoryRoles'
```

```
      - 'passwordProfile'
  selection_ms:
    CommandLine|contains:
      - 'login.microsoftonline.com'
      - 'graph.microsoft.com'
  filter_iam_hosts:
    ComputerName:
      - 'iam-sync-01.campus.example'
  condition: selection_ropc and selection_ms and not filter_iam_hosts
falsepositives:
  - Legacy identity synchronization scripts running on designated IAM automation serve
rs
level: high
tags:
  - attack.credential-access
  - attack.privilege-escalation
  - attack.t1078.004
---
title: CampusKey Chisel Reverse Port-Forwarding Tunnel to Campus Services
id: 7f39b8d4-2a19-4c63-8e12-55b20f84d202
status: experimental
description: Detects Chisel client command lines establishing reverse port-forwarding
tunnels exposing internal MSSQL, SMB, RDP, WinRM, FTP, or SSAS ports to an external se
rver.
author: Odin by Brandefense
date: 2026-11-22
logsource:
  category: process_creation
  product: windows
detection:
  selection_client:
    CommandLine|contains: ' R:'
  selection_ports:
    CommandLine|contains:
      - ':1433'
      - ':445'
      - ':3389'
      - ':5985'
      - ':5986'
      - ':2383'
      - ':21'
  filter_redteam_hosts:
    ComputerName:
      - 'pentest-jump-01.campus.example'
  condition: selection_client and selection_ports and not filter_redteam_hosts
falsepositives:
  - Authorized red-team exercises operating from approved jump hosts
```

```
level: high
tags:
  - attack.command-and-control
  - attack.t1572
---
title: CampusKey Web-Tier Potato Privilege Escalation and LSASS Memory Dump
id: 7f39b8d4-2a19-4c63-8e12-55b20f84d203
status: experimental
description: Detects Windows process command lines mentioning GodPotato, PrintSpoofer,
or comsvcs.dll MiniDump.
author: Odin by Brandefense
date: 2026-11-22
logsource:
  category: process_creation
  product: windows
detection:
  selection_tools:
    CommandLine|contains:
      - 'GodPotato'
      - 'PrintSpoofer'
      - 'comsvcs.dll, MiniDump'
  filter_edr_lab:
    ComputerName:
      - 'sec-lab-01.campus.example'
  condition: selection_tools and not filter_edr_lab
falsepositives:
  - Controlled EDR validation labs testing credential-dumping detections
level: critical
tags:
  - attack.credential-access
  - attack.privilege-escalation
  - attack.t1003.001
```

