[N S S | > research]

TECHNICAL ANALYSIS / NSS-KD-01 TLP:CLEAR Deep Research



Expanded by NSS

188 names from NSS's own records, 161 of them on no list on 16 Nov 2026; the Fortnite checker campaign type was in public reporting first

Phishing aimed at children and their families: 188 look-alike names in six sets

Parents and carers: jump to what to do tonight.

Between 27 October and 16 November 2026 NSS recorded 188 new web names built to take children's and teenagers' game accounts, and through those accounts their families' money, devices and social accounts. The largest single piece is one server that answered for 40 names written for Russian speakers: Roblox sign-in and "Robux" names, a Brawl Stars gem store, Roblox script sites, look-alikes of the VK social network, a voting lure and a shopping look-alike, most of them each on a DNS account of its own. Beside it sit a Fortnite "locker worth" checker server whose newest 39 names were almost all unlisted, Roblox link names bought in four bursts, staged Mobile Legends "support" names and

Minecraft "creator" invitations. On 16 November 161 of the 188 were on no threat list NSS takes in. This paper gives every name, takes apart the anti-bot gate that keeps the Fortnite checker off blocklists, and sets out what parents, schools and platform teams can do.

PUBLISHED	LAST UPDATED	READING TIME	MARKING
16 Nov 2026	16 Nov 2026	32 min	TLP:CLEAR

188
new names aimed at young players' game and social accounts, recorded 27 October to 16 November 2026

161
of them on no threat list NSS takes in on 16 November

40
names written for Russian speakers answering from one server: Roblox, Brawl Stars, VK, voting and shopping look-alikes

12
Fortnite checker names on one server run the same anti-bot gate; NSS took the gate apart, captured the kit read-only and ships tested detection

What parents and carers can do tonight

You do not need to know anything about servers. These steps make the pages in this paper far less likely to work on your child's accounts.

1. Agree one family rule: nobody types a game password, or a code that arrives by text or email, into a page opened from a chat message, a video comment or a friend's link. Real games sign in inside the game (for Brawl Stars, the Supercell ID login inside the game), the official app, or the official website typed in by hand, never through a link someone sent.
2. Turn on two-step sign-in (a code on your phone as well as the password) for every game account, the email address

behind it, and your own email. A two-step code is never shared with anyone or typed into a page reached from a link.

3. Give each account its own password. If a child's game password is also your email or shopping password, change yours first.
4. Do not leave a payment card saved on a child's game account. Use a parent-approved purchase setting or a prepaid balance instead, and turn on purchase alerts from your bank.
5. Talk about the bait, not just the danger. Try: "If anyone offers 'free Robux', gems or a skin check, show me first. You will not be in trouble, even if you already clicked."
6. Keep cheats and executors (programs kids download to cheat in Roblox) off the family computer. If one was installed, change the passwords saved in that computer's browser from another device.
7. If an account is taken: use the game's official recovery page, change the password on the email behind the account, and tell the child's friends that messages from the account are not from them. If a card was charged, call your bank to dispute it and ask for a new card. If the purchase went through an app store, ask that store for a refund too.
8. Report the account to the game's support team, report the link inside the game or app, and report money lost to your country's fraud reporting service (in the US the FTC at reportfraud[.]ftc[.]gov, in the UK Action Fraud at actionfraud[.]police[.]uk).
9. Signs an account was taken: your child cannot sign in, items or currency are gone, friends got odd messages from them, or you see an email about a new sign-in or a password change you did not make.

Your child is not in trouble for clicking. These pages are built by adults to fool people of every age, and children who tell a parent quickly lose

the least.

Key findings

1. Children are the target and families pay. Every set in this paper imitates something young players use: Roblox and its currency, Robux; Fortnite skins; Brawl Stars gems; Mobile Legends accounts; Minecraft's biggest server, Hypixel; and the VK social network that Russian-speaking children use. A stolen game account is sold for its items and currency; a saved payment card on it can be spent; a reused password opens a parent's email; a stolen social account messages relatives; a fake cheat download runs on the family computer.

2. One server, 40 names, written for Russian speakers (set K1). NSS's own sensors recorded 40 names on 87.120.104[.]209 between 11 and 16 November 2026, and on 16 November 40 of the set's 45 names answered from it. They imitate Roblox sign-in and Robux (rbxsauth[.]top, robuxs[.]biz), Roblox script sites, a Supercell and Brawl Stars store (supercellstore[.]sbs, brawl-link[.]shop), VK (eight names such as vlkontakte-v[.]sbs), a voting lure (goloskerru[.]cfd, vote-quick[.]sbs), and a Russian marketplace, cinema and coupon sites. None of the 45 was on a threat list NSS takes in on 16 November; the address itself has been on a list since 2 September 2026.

3. Why "Russian-language" and no more. The K1 names are built from Russian words written in Latin letters ("golos", vote; "yashik", box; "kinoman", film fan; "kyponka", coupon) and imitate services that Russian speakers use (VK, a Russian marketplace). NSS's captures on 16 November met empty pages at the K1 names' front doors, so the language claim rests on the names. The server's network is registered in Hong Kong and the address sits in Bulgaria, and the names were bought at registrars in several countries; nothing in NSS's records points to a state or a named group, and NSS names none.

4. A Fortnite checker server whose newest names were unlisted (set F2). 75 names on 193.187.110[.]18 in NSS's record: 64 Fortnite "locker worth", skin-value and checker names (fortnitelockerworth[.]com, fortchecker[.]net, lockfort[.]app) and 11 crypto "check" names. On 16 November 64 still answered from the server and 43 of those were on no list NSS takes in. Of the 39 names NSS first recorded on 12 and 13 November, 2 were listed. Public reporting from July 2026 describes this campaign type: a page that values a player's skins asks for the game sign-in and its two-step code.

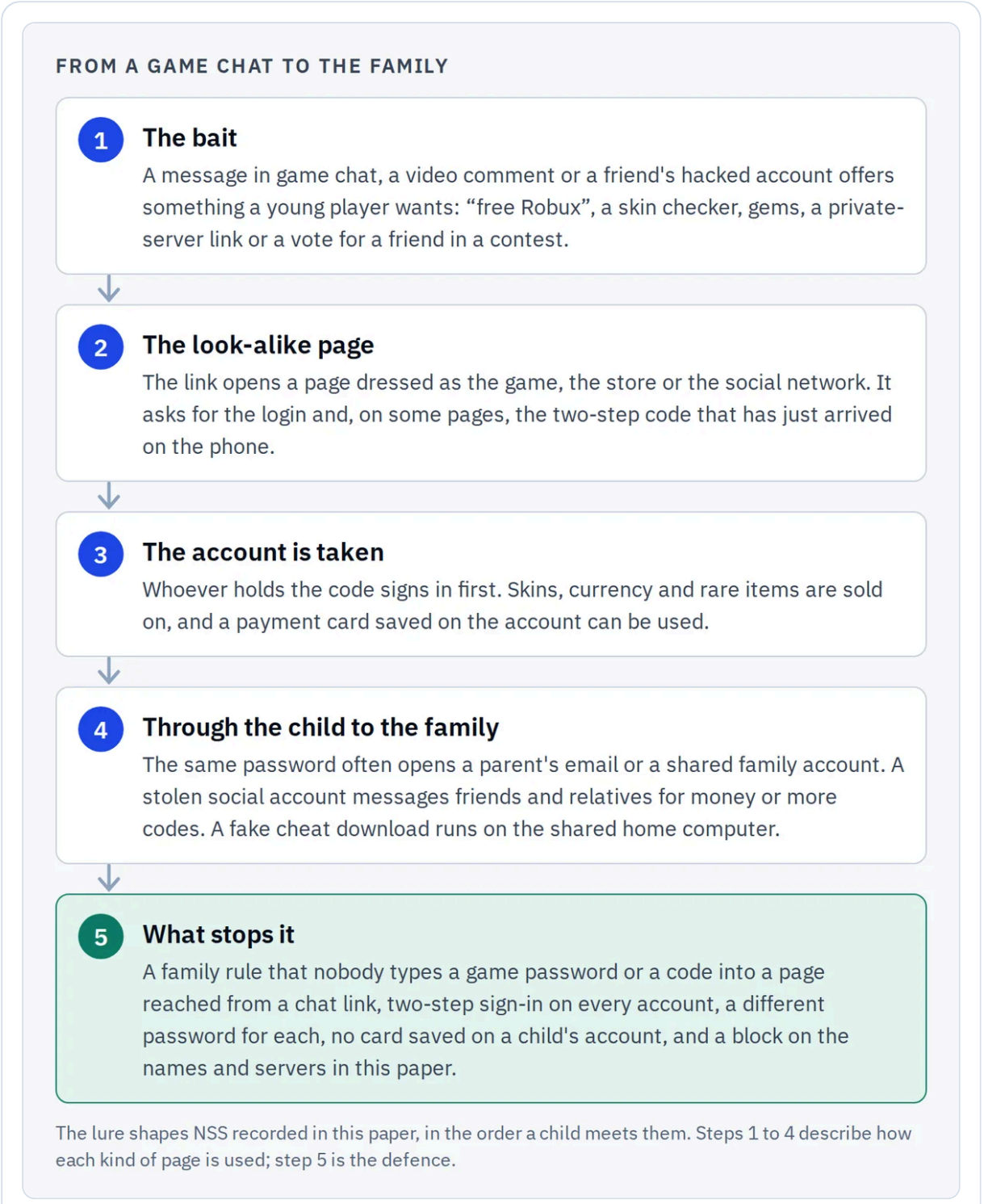
5. Roblox link names bought in four bursts (set R1). Fourteen .com names that read like a Roblox address with one or two letters added (at-roblox[.]com, roblox-id[.]com) were registered at one registrar in four bursts of three or four names, each burst inside two and a half minutes: 10 November at 02:05 UTC, 11 November at 21:21, 13 November at 03:42 and 15 November at 01:40. Names from different bursts later shared DNS accounts. None was listed on 16 November; 13 answered, all behind a delivery network.

6. Staged sets waiting for a message (M1, H1). 34 Mobile Legends "support team" names on .cloud, 1 to 16 November, at one registrar, 7 of them writing "rn" for "m" (rnoontonsupport[.]cloud, helprnoonton[.]cloud); they sit on the registrar's shared landing address with fresh certificates, which is what a hosting account being prepared looks like. 17 Minecraft and Hypixel names ("content creator", "YouTube rank", "account migration"), 2 of them answering. None of the 51 was listed.

7. Fake cheat downloads for Roblox (set X1). One DNS account took xeno-executor[.]info, wave-executor[.]live and solara-executor[.]top, named after the script tools children search for to cheat in Roblox. Public reporting from 2025 and 2026 describes information stealers shipped as game cheats; on a shared home computer that puts the parents' saved passwords at risk.

8. What NSS cannot say. Each set is tied together by its own evidence; the sets are not shown to be tied to each other, so this is several operators

or one, and NSS does not decide. On 16 November NSS read all 192 indicators (the 188 names, both servers and the two listed context names) on both Investigate and Scan, and the two surfaces gave the same band on every one: the two servers, the listed names on the F2 server and the Roblox link names read Suspicious or higher, and the other unlisted names read Clean, because NSS judges a name by the page it serves and none of these pages showed a lure form to NSS on 16 November; the infrastructure record, not the band, is the finding here.



The lure shapes NSS recorded in this paper, in the order a child meets them. Steps 1 to 4 describe how each kind of page is used; step 5 is the defence.

How the lure shapes in this paper reach a family. Steps 1 to 4 describe how each kind of page is used; step 5 is the defence.

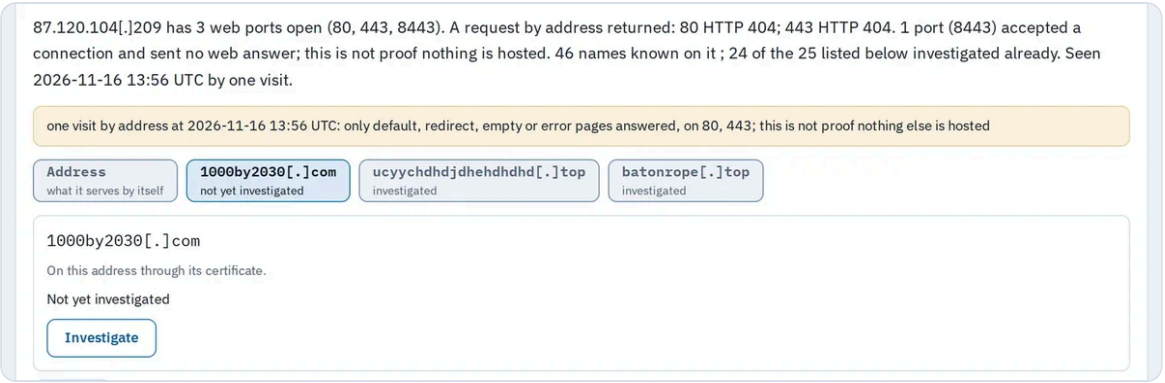


The six sets on 16 November 2026. Each set is tied together as its row says; the sets are not tied to each other.

How an analyst finds this with NSS

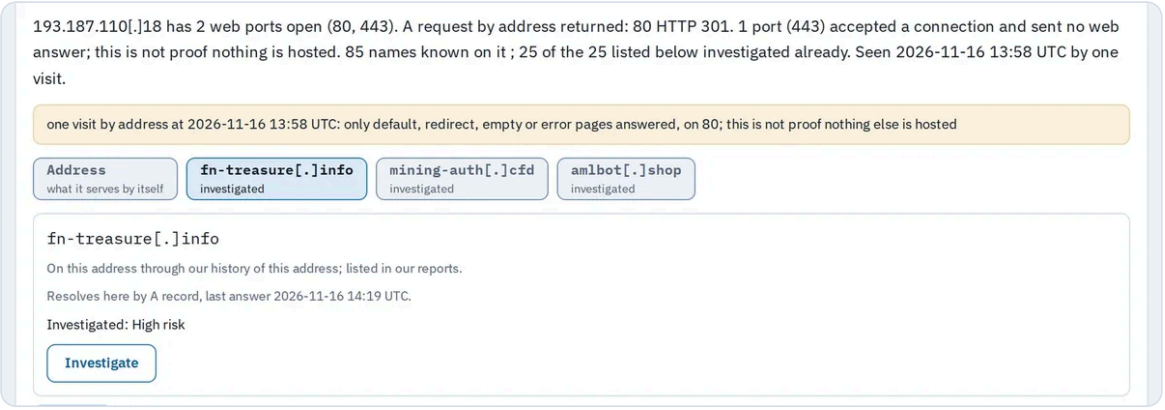
The same case, worked the way a defender works it in NSS: from each server to the names on it, and from one Fortnite name to every name beside it. Every picture is the real Station on 16 November 2026, cropped to the panel in use.

01 Start from the K1 server. Investigate rates 87.120.104[.]209 Suspicious and shows what it serves: by address it answers "not found", and 42 names are known on it, the set's names among them, one (1000by2030[.]com) known only from its certificate. Each name opens with one click.



Investigate, 16 November 2026, cropped to the panel in use.

02 Do the same for the Fortnite server. 193.187.110[.]18 also reads Suspicious, and its panel counts 75 names known on it.



Investigate, 16 November 2026.

03 From any one Fortnite checker name, run a two-step tool chain on its Scan page: the addresses NSS has on record for the name, then every name NSS has seen on those addresses. One name gives one address and every name on it, Fortnite and crypto alike: 85 by the afternoon of 16 November, ten more than the 75 this paper counts from the morning's read, so the set is still growing.



The chain run on 16 November 2026. The results continue below the crop in the same form.

04 Then act: watch the server so a new name on it raises an alert, share the casefile with a colleague, or download it as JSON or CSV for a filter or a block list (Full features).



The casefile's actions, 16 November 2026. Nothing was clicked for the picture but the More menu.

Steps 1 to 3 run in the Community tier; watching and downloads are Full features.

Automate it with the NSS API

Every NSS check is JSON: a risk band, the host class, how many names share the host, the public-listing state and the time of the answer. The public check needs no key and takes one domain name or one IP address, a few checks a day for each network. A Full account adds API keys, each with its own daily allowance and a limit per minute, made on the account's API keys page. A school or a platform team can run the paper's file every morning and see any name that changes.

One check from a shell

```
NAME=$(jq -r '.indicators[0].value' nss-kd-01.json)   # the first indicato
curl -s "https://nsshq.com/api/v1/check?value=$NAME"
```

The paper's indicator file, in JSON or CSV, is linked at the end of this page.

The answer for the K1 server on 16 November 2026


```
{
  "as_of": "2026-11-16T13:57:09Z",
  "band": "Suspicious",
  "band_is_host_class": false,
  "found": true,
  "host_class": { "class": "unknown", "label": "Host type unknown", (...)
  "known_good": false,
  "names": { "at_least": false, "listed": 0, "total": 40 },
  "public_listing": { "date": "2026-09-02", "line": "Listed publicly on 20
  "registration": null,
  "reports": 0,
  "type": "ipv4",
  "value": "87.120.104[.]209",
  "view": "public"
}
```


The real public answer for 87.120.104[.]209, read on 16 November 2026 at 14:02 UTC (the verdict itself dated 13:57 UTC). Here the value is defanged and two blocks shortened. It reads Suspicious, counts 40 names on the address with none of them listed, and shows that the address itself has been on a public list since 2 September 2026. When a network's public checks for the day are used up, the same request answers HTTP 429 with a body that says when they reset (00:00 UTC); a Full key has its own allowance.

Check the whole file every day and flag changes (Python 3, standard library only)

```
#!/usr/bin/env python3
"""Check every name and address in an NSS paper's indicator file and flag

  python3 nss_check_file.py nss-kd-01.json
Without a key it uses the public check (no key needed, a few checks a day
page, then set NSS_API_KEY to the key and NSS_API_URL to the request that
header, never in the address. Prints one JSON line per indicator; exits 2
"""
import json, os, sys, time, urllib.error, urllib.parse, urllib.request

URL = os.environ.get("NSS_API_URL", "https://nsshq.com/api/v1/check?value=
KEY = os.environ.get("NSS_API_KEY", "")
STATE = os.environ.get("NSS_STATE", "nss-verdicts.json")


def request_url(value):
    u = urllib.parse.urlsplit(URL)
    q = urllib.parse.parse_qsl(u.query)
    q = [(k, value if v == "example.org" else v) for k, v in q] if any(v =
    return urllib.parse.urlunsplit(u._replace(query=urllib.parse.urlencode


def check(value):
    req = urllib.request.Request(request_url(value), headers={"Accept": "a
    while True:
        try:
            with urllib.request.urlopen(req, timeout=120) as r:
                return json.load(r), r.headers.get("NSS-Quota-Remaining")
        except urllib.error.HTTPError as e:
            try:
                body = json.loads(e.read() or b"{}")
            except ValueError:                                    # an e
                body = {}
            if e.code == 429 and e.headers.get("Retry-After"):    # per-
                time.sleep(int(e.headers["Retry-After"]) + 1)
                continue
            if e.code == 429:                                     # the
                return {"stopped": body.get("resets_at") or "daily limit r
            return {"error": e.code, "detail": body.get("error")}, None
```

```
def verdict(answer):
    return answer.get("band") or answer.get("label") or answer.get("verdic


def main(path):
    items = json.load(open(path))["indicators"]
    old = json.load(open(STATE)) if os.path.exists(STATE) else {}
    new, changed = dict(old), False
    for it in items:
        if it["type"] not in ("domain", "ipv4"):                    # the
            continue
        answer, left = check(it["value"])
        if "stopped" in answer:
            print(json.dumps({"stopped": answer["stopped"]}), file=sys.std
            break
        v = verdict(answer)
        row = {"value": it["value"], "type": it["type"], "verdict": v, "as
        row["changed"] = bool(row["previous"]) and v != row["previous"]
        changed |= row["changed"]
        if v:
            new[it["value"]] = v
        print(json.dumps(row))
        if left == "0":
            break
        time.sleep(1.1)                                             # stay
    json.dump(new, open(STATE, "w"), indent=1)
    sys.exit(2 if changed else 0)


if __name__ == "__main__":
    main(sys.argv[1] if len(sys.argv) > 1 else "nss-kd-01.json")
```

One JSON line per indicator for a SIEM, a school filter's import or a log, and exit code 2 when a verdict changed since the last run. With a Full key, set NSS_API_KEY and NSS_API_URL (the request your API keys page shows); the key travels only in the Authorization header, and the script waits when told to slow down and stops when the day's allowance is spent. For the staged sets (M1, H1) the change to watch is a name that starts answering.

Every morning, with a mail when a verdict changes

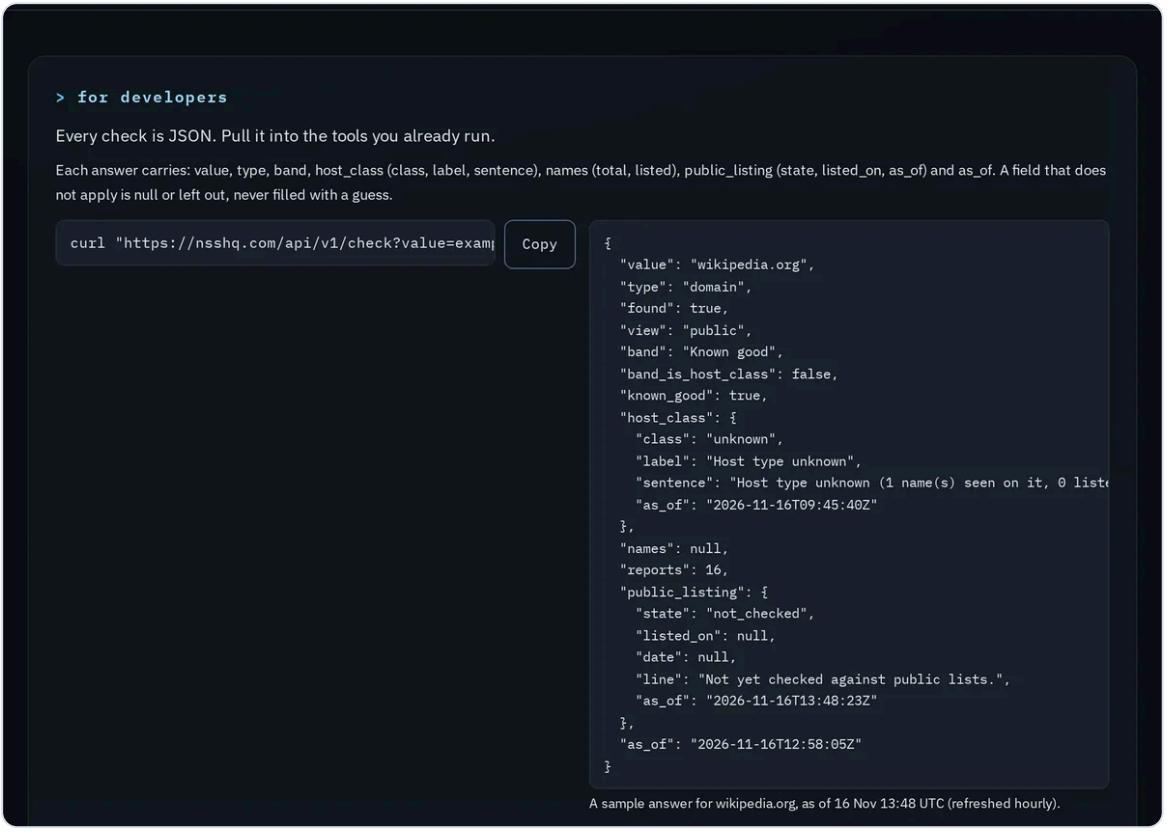
```
0 6 * * * cd /opt/nss && python3 nss_check_file.py nss-kd-01.json >> check
```

STIX 2.1 and threat-sharing event files

```
git clone https://github.com/nsshq/nssresearch
# each paper's folder holds stix2.1-bundle.json, misp-event.json and iocs.
```

This paper's folder is added when it is published. Staged names are typed anomalous-activity with a 30-day validity, so a platform can watch them without a permanent block.

At the DNS layer the cheapest control is the two servers: block 87.120.104[.]209 and 193.187.110[.]18, and any new name the operators point at them is covered. For the other sets the names and the shapes under What a defender can look for are the control.



The public Developers page on nsshq.com, 16 November 2026: the request, the fields every answer carries and a live answer.

Timeline

3 Apr 2025

The first Roblox look-alike of the "https-www" shape is listed. Public lists carry 52 of that family by 16 November 2026.

Jul 2026
Public reporting describes fake Fortnite "locker worth" checkers that ask for the game sign-in and its two-step code.

2 Sep 2026
87.120.104[.]209, later the K1 server, is on a public list, two months before any K1 name exists.

27 Oct
NSS records the first name on the F2 server, a crypto check name.

1 Nov
The first Mobile Legends support names (M1) enter DNS.

5 to 11 Nov
The first Fortnite checker names appear on the F2 server; with the crypto names, 35 names are on it by 11 November, 24 of them on a list by 16 November.

8 Nov, 20:45 UTC
rbxsauth[.]top, a Roblox sign-in look-alike, is registered.

10 Nov, 02:02 to 02:07 UTC
lhttps-www--roblox[.]com is registered at one registrar; two and a half minutes later the first R1 burst, four names, at another.

11 Nov, 04:20 UTC
NSS records the first names on 87.120.104[.]209: voting, VK, marketplace and cinema look-alikes.

11 Nov, 21:21 UTC
Second R1 burst, three names.

12 Nov
Seven Hypixel creator names enter DNS on one registrar's default name servers.

12 and 13 Nov
39 new names on the F2 server; 2 of them are on a list on 16 November.

13 Nov, 03:42 UTC
Third R1 burst, four names.

14 Nov
Certificates are issued for ten Mobile Legends support names, two of them minutes after registration.

15 Nov
Ten more M1 names enter DNS; fourth R1 burst at 01:40 UTC; supercellstore[.]sbs is registered at 12:46 UTC.

16 Nov
Five more M1 names; NSS reads the names and both servers back on Investigate and Scan, and 161 of the 188 are on no list NSS takes in.

Why this matters: children, and the families behind them

Most phishing is written for adults: a bank, a parcel, a tax refund. The six sets in this paper are written for children and teenagers. They offer what young players want (game currency, rare skins, a higher rank, a private server, a vote for a friend), they arrive where parents rarely look (game chat, community servers, video comments, a friend's account), and they push for speed. These pages are built to catch a player who has not yet learned that a game never asks for a password on an outside page.

The harm does not stop at the child:

- **The account itself.** Years of play, bought items and currency. Stolen game accounts are resold, and a child who loses one often hides it.
- **The family's money.** A payment card saved on a game account can be spent once the account is taken. A "store" page that sells gems or coins asks for card details directly.
- **The family's other accounts.** The email behind a child's game account is often a parent's, and children reuse passwords. One stolen password can open more than the game.

- **Friends and relatives.** A stolen social account keeps messaging the people who trust it. A voting lure ("vote for my child in a contest") is built to travel from relative to relative.
- **The home computer.** A fake cheat download runs with the child's rights on whatever computer the family shares, where parents' banking and email passwords are often saved.

None of this needs a sophisticated attacker. It needs a name that looks right, a page that looks right, and a moment of hurry.

The six sets

SET	IMITATES	NAMES	ON A LIST, 16 NOV	ANSWERING, NOV
K1	Roblox, Brawl Stars, VK, voting, a Russian marketplace	45	0	40 from the server, 3 elsewhere
F2	Fortnite locker checkers, crypto checks	75	27	64 from the server
M1	Mobile Legends support	34	0	all on a registrar's shared land address
H1	Minecraft, Hypixel	17	0	2

R1	Roblox addresses	14	0	13 behind a delivery network
X1	Roblox cheat downloads	3	0	3

Each row is tied together by its own evidence. Between rows NSS has no link: different servers, registrars, languages and audiences. Read them as six findings about one kind of target, not as one campaign.

K1: one server, children's games and family accounts

NSS's own sensors recorded 40 names on 87.120.104[.]209 between 11 November 2026 04:20 UTC and 16 November 07:05 UTC. Five more names of the same vocabulary answered from the address in the fresh look-up of 16 November, which makes the set 45; on that day 40 of the 45 answered from the server, three from other addresses and two not at all; all five had been recorded on the server between 11 and 13 November.

THEME	NAMES
Roblox sign-in and Robux	rbxsauth[.]top, robuxs[.]biz
Roblox scripts	topscriptik[.]shop, scriptosbestos[.]shop
Supercell and Brawl Stars	supercellstore[.]sbs, supercell-store[.]xyz, brawl-link[.]shop, brawlstarsfreeloveyashik23[.]club, maxbrawls[.]live, zoda[.]skin, gamerpro[.]top
VK look-alikes	vlkontakte-v[.]sbs, vlkontakte-vi[.]sbs, vlkontakte-vk[.]sbs, vlkontakte-ai[.]sbs, vlkontakte-il[.]sbs, vlkontalkte-l[.]sbs, vlkontalkte-ru[.]sbs, vikontakte-io[.]sbs
Voting	goloskerru[.]cfd, vote-quick[.]sbs

Shopping, cinema, coupons	ozon-fresh[.]sbs, kinoman[.]sbs, videohab[.]sbs, kyponka-prom[.]xyz, max-coupon24[.]club, maxhiru[.]club, maxeeru[.]club, referralsx[.]xyz, mowmod[.]one
Short random names	batonrope, cabinlake, covesolvent, kernelclip, liope, mooselithium, neonlounge, pencilvalley, rinseplug, tapecanyon and ucyychdhdjdhehdhdhd, all .top; so2[.]space, st2[.]fun, nakaiqun[.]club, mokront[.]com

The mix is the point. The same server carries children's lures (Robux, Brawl Stars gems, Roblox scripts) and lures for the adults around them (a marketplace, cinema and coupon sites, a voting page). VK is the social network where Russian-speaking children and their parents both have accounts, so a VK sign-in taken from a child is also a way into the family's circle.

The operator spread its accounts on purpose. 39 of the 45 names use a delivery network's DNS, and each of those 39 sits on its own name-server pair, which that provider hands out per account: one account per name. The other six use registrars' own DNS. The names came from several registrars and entered DNS between 6 and 16 November (rbxsauth[.]top was registered on 8 November at 20:45 UTC, supercellstore[.]sbs on 15 November at 12:46 UTC). Taking down one account or one registration removes one name; the server is the tie, and the block point.

None of the 45 names was on a threat list NSS takes in on 16 November. The address itself has been on a list since 2 September 2026, before any of these names existed, so a defender who blocks listed addresses already blocks this server; one who relies on listed names does not see the set.

Names of the same vocabulary on other servers are recorded and not counted: maxbrawl[.]club, brawls-stars[.]life, brawl-starsy[.]club, brawl-star[.]live, nullsbrawl[.]click, brawlpromsfree[.]club, vkontakte-ll[.]sbs and vkontakte[.]live. Same words, different hosting: possible relatives, no tie.

F2: Fortnite locker checker names, an unlisted wave of a reported campaign type

Public reporting from July 2026 describes the campaign type: a site offers to tell a Fortnite player what their "locker" (their skins and items) is worth, then asks them to sign in with the game account and enter the two-step code, and the account is taken. NSS reached the page behind these sites read-only and documents it in the Teardown below. NSS's record holds 75 names on one server, 193.187.110[.]18, first recorded between 27 October and 15 November 2026: 64 Fortnite names built from "fort", "fn", "epic", "locker", "worth", "value", "checker", "skin", "OG" and "treasure" (fortnitelockerworth[.]com, fortchecker[.]net, fort-locker[.]net, fnlocker[.]help, lockfort[.]app, skincalculator[.]net, myfortskin[.]com), and 11 crypto "check" names (amlbot[.]shop, coinbace-transaction[.]com, tx-auth[.]cfd).

FIRST RECORDED BY NSS (UTC)	NAMES	ON A LIST, 16 NOV
27 Oct to 11 Nov	35	24
12 and 13 Nov	39	2
15 Nov	1	1

On 16 November 64 of the 75 still answered from the server, and 43 of those 64 were on no list NSS takes in. The names were bought at several registrars, and 63 of the 66 with a DNS record use one DNS hosting service shared by many unrelated users, which ties nothing; the server does.

Every one of these sites hides behind a timed, human-only puzzle that screens out automated checkers, which is why the newest names stayed off blocklists; the Teardown section takes that gate apart. The crypto names on the same server could be the same operator or a second customer of the same host; NSS records them, ships them in the files, and does not decide.

R1: Roblox addresses bought in four bursts

Fourteen .com names read like a Roblox address with one or two letters added, the shape of a link pasted into game chat that looks right at a glance. All fourteen were registered at one registrar based in Vietnam, in four bursts:

BURST (REGISTRATION TIME, UTC)	NAMES
10 Nov, 02:05:20 to 02:07:33	av-roblox[.]com, roblox-vm[.]com, ur-roblox[.]com, uv-roblox[.]com
11 Nov, 21:21:22 to 21:22:50	at-roblox[.]com, ec-roblox[.]com, ma-roblox[.]com
13 Nov, 03:42:21 to 03:44:16	ae-roblox[.]com, ei-roblox[.]com, rn-roblox[.]com, robloxj[.]com
15 Nov, 01:40:23 to 01:41:34	roblox-at[.]com, roblox-id[.]com, roblox-is[.]com

The first three bursts are one buyer: names from the second burst share a DNS account with a name from the first (at-roblox[.]com with ur-roblox[.]com), and by 15 November six names from the second and third bursts sat on one DNS account. The fourth burst, on the registrar's default name servers, matches by registrar, shape and buying habit only. On 16 November 13 of the 14 answered, all behind a delivery network that hides the server; none was on a list.

There is a listed family next door. Public lists have carried 52 Roblox look-alikes of a different shape, where "https-www" or a "wvvw" misspelling is written into the name (https-wvww-roblox[.]com), since 3 April 2025. One of them, lhttps-www--roblox[.]com, was registered at another registrar at 02:02:47 UTC on 10 November, two and a half minutes before the first R1 burst, and listed on 14 November. The timing and the lure idea make a tie between the two families likely; NSS does not count it as confirmed. The two-letter shape of R1 was on no list.

M1 and H1: staged names waiting for a message

Mobile Legends (M1). 34 .cloud names from 1 to 16 November, new names on ten days, five on 16 November alone, all from one small vocabulary: mlbb, mobilelegends (and the misspelt mobilegends), moonton, with cs, team, help, support, global, play, games and notification. Seven write "rn" for "m", which reads as "m" in many fonts: rnoontonsupport[.]cloud, rnoontongames[.]cloud, helprnoonton[.]cloud, csrnoonton[.]cloud, notificationrnoonton[.]cloud, globalrnoonton[.]cloud and rnobilelegendssupport[.]cloud. All 34 are at one registrar; 33 sit on its shared landing address and one on a server of its own. A shared landing address usually means an idle name, but public certificate logs show certificates for eleven of these names issued on 13 and 14 November, two of them minutes after registration (playmlbb[.]cloud, registered at 10:11 UTC on 14 November, certificate at 10:21; rnoontonsupport[.]cloud, 11:10 and 11:12). That is consistent with a hosting account being prepared. Mobile Legends is played mostly by teenagers in South-East Asia, and fake "customer service" pages are the usual way their accounts are taken. The registrar and the address are shared by many users, so the vocabulary, the TLD and the daily rhythm are the tie: likely, not confirmed.

Minecraft and Hypixel (H1). Seven Hypixel "creator" names (hypixel-creators[.]net, hypixel-youtube[.]net, hypixel-content-creators[.]net and four more) entered DNS on the same day, 12 November, on one registrar's default name servers; two read through public registration records were registered on 6 and 8 November. Seven Minecraft "support" and "migration" names (.help and .click) entered DNS between 4 and 11 November on another registrar's default name servers. Three more Hypixel names: invite-hypixel[.]net, and hypixelclaim[.]shop and xn--hypxel-5va[.]shop (with an accented letter), which share one DNS account. Hypixel is the largest Minecraft server and its players are young; the lure shape is the invitation to apply for a "YouTube" or "content creator" rank, which ends at a fake Microsoft sign-in or a "verification" download. Only two of the 17 answered on 16 November. A creator-rank lure usually goes live when the messages are sent; these names are the ones to load into filters now.

X1: fake cheat downloads

Xeno, Wave and Solara are executors (programs kids download to cheat in Roblox). One DNS account took xeno-executor[.]info and wave-executor[.]live on 9 November and solara-executor[.]top on 11 November. Public reporting from October 2025 and November 2026 describes information stealers handed out as game cheats. A cheat runs with the child's rights on the computer the family shares, and an information stealer looks first for saved browser passwords, which on a family computer are often the parents'.

Teardown: how the operator's Fortnite checker gate works

This paper carries NSS's Deep Research label: a full teardown of the operator's kit, with the artifacts, their hashes and tested detection a defender can deploy. This is the technical section. It describes the operator's machine only: its gate, its endpoints, its fingerprinting and the detection you can build from them. It does not describe how NSS captured any of it. NSS documented the gate and read the page behind it read-only, without running anything. Confidence is marked per claim: **observed** (NSS saw it directly, with the HTML or a screenshot in hand), **assessed** (NSS's reading of the operator's own code), **possible** (consistent with the evidence and public reporting, not confirmed by NSS).

The gate ran on 12 names, all on one server, 193.187.110[.]18: amlapp[.]site, fortbow[.]com, fortchecker[.]net, fortch[.]sbs, fort-locker[.]net, fortloker[.]com, fortnitelockerworth[.]com, fortniteskins[.]shop, fortwint[.]top, fortyear[.]top, lockfort[.]app and stopapupahah[.]shop. No other server in NSS's records carries it (observed). Every visitor, NSS's automated captures included, met a timed, human-only puzzle before any content loaded, which is why these names read as an empty "Loading" page in automated checks and sat on almost no list.

The requests (the operator's endpoints)

STEP	METHOD AND PATH	SHAPE OR EFFECT	HOW WE KNOW
1	`GET /`	redirect to the challenge	observed
2	`GET /.rt/challenge?tier=captcha&return_to=%2F`	the puzzle page, title "Loading", `noindex,nofollow`	observed
3	`POST /.rt/ce`	sent repeatedly while the puzzle runs; behaviour or entropy telemetry	observed (the requests); assessed (the purpose)
4	`POST /.rt/verify`	fail returns `{"captcha_url":"/.rt/challenge?tier=captcha&return_to=%2F","success":false}` and the same puzzle is served again; pass returns `{"first_party_ticket":"<long opaque token>","return_url":"/","success":true}` and the puzzle is not re-served	observed (both bodies)
5	`GET /` (after a pass)	the checker landing loads	observed
6	checker lookup, then sign-in	a text field, placeholder "Enter your Epic display name", with a CHECK VALUE button; after the lookup the page reveals two "SIGN IN WITH EPIC" buttons (script-driven, no static link). No installer link on any page	observed (lookup field, sign-in button, no installer)

Other endpoints seen in the flow and named in the operator's own tracker: `POST /.rt/captcha/verify`, `POST /.rt/e`, `POST /___init` and `POST /___tra`

`p` (bot traps), and the string literals `/.rt/consent` and `/ws` (present in the tracker source; neither was observed firing). All are first-party on each site; the gate contacts only the site host, no third party (observed).

What the gate fingerprints

While the puzzle runs, a worker reports these browser signals back to the page (observed). Each is a detection signal: the kit keeps a visitor it reads as automated on the challenge, and only serves the lure to a profile it reads as a real person who also solves a timed physics puzzle.

SIGNAL	WHAT IT TELLS THE KIT
`navigator[.]webdriver`	true on an automated browser: treated as non-human
`navigator[.]userAgent`	device and browser class; feeds the human-or-automation judgement and a desktop-or-mobile branch in the gate's own logic
`navigator[.]platform`	operating-system class
`navigator[.]hardwareConcurrency`	CPU core count; headless and server browsers cluster at tell-tale values

The puzzle is a timed spring-physics canvas (the matching outline attracts the shape, the others repel; statuses include "Pull the shape by its thread", "Flying... you can catch it" and "Time is up - one more try"). That the lure sits behind a timed, human-only puzzle is itself a finding: automated page readers, and the block lists that depend on them, see only "Loading", which is why the newest names on this server sat on almost no list.

The kit fingerprint (identical across the 12 names)

- `body[data-tpl="standard"]`; header text `TETHER . PULL TO DOCK`; heading `Guide the shape home`.
- Canvas `#tthCv` (role application), status `#tthStatus`, live region `#tthLive`.

- A footer support code of the form `euwest1::<unix-seconds>-<32 hex>`.
- Document `<title>Loading`; `<meta name="robots" content="noindex,nofollow">`; an inline SVG wave-mark favicon.
- The puzzle scripts are built in the page and loaded from `blob:` URLs, so there is no external script URL to block; the captured blob bodies are a 117-byte loader (sha256 df01ff1b...) and a 148-byte script (sha256 00421c5b..., seen twice byte-identical).

Behind the gate: the lure

NSS read the page behind the gate, read-only, as far as the sign-in button.

Observed (HTML and a screenshot in hand): a "Fortnite Locker Value" checker that borrows real Epic skin art and the real fortnite[.]com V-Bucks link to look genuine, with a CHECK VALUE call to action, "FAST / SECURE / FREE TOKEN" badges, fake skin valuations, an FAQ that includes "Do I have to give you my Epic password?", and a scrolling banner reading "PIRATE SHOP TOKEN . OFFICIAL EPIC SIGN-IN . RESULTS IN SECONDS". A single lookup field, "Enter your Epic display name" (reconnaissance, to confirm the handle exists), then two "SIGN IN WITH EPIC" buttons under the line "You sign in on Epic's own page, we never see your password." The sign-in button is the furthest NSS reached; NSS entered nothing and did not open the sign-in.

Assessed (from the operator's own tracker, `/libs/sg-min[.]js`, read not executed): the flow after the sign-in button includes a password screen and a one-time-code screen. The tracker names its own funnel `page_view -> offer_view -> otp_view -> otp_submit` and carries a form classifier that labels fields as `password / otp / 2fa / mfa / pin` and redacts those values from its own beacons. NSS did not open the password or one-time-code screens; they are assessed from the tracker, not screenshotted.

Possible (public reporting, read for context): Public reporting from July 2026 describes this exact lure as relaying the stolen password and the live

one-time code to Epic in real time, so the account is taken despite two-factor, then resold. NSS did not observe the relay.

The artifacts

Every artifact was captured read-only on 16 November 2026, holds no real child data, handle or credential (a fake display name was the only text typed, at the lookup), and carries a SHA-256 computed from the file in hand. Full list, with sizes and funnel positions, in the paper's indicator repository.

ARTIFACT	BYTES	SHA-256 (FIRST 16)	FUNNEL POINT
gate challenge page (HTML)	122430	8102f8b48e92ca4d	pre-gate puzzle
behind-gate checker landing (HTML)	71913	d11aeccf9c48004f	post-gate
sign-in-entry page (HTML)	76673	48a2a52928606898	post-gate, the "SIGN IN WITH EPIC" step
operator tracker sg-min[.]js	75071	b4cbf20f55c1928e	post-gate instrumentation
behind-gate landing screenshot	1230218	a87a7e47a5c5e695	post-gate
sign-in-entry screenshot	1903810	2142a5120adcb0ad	post-gate (furthest reached)

Detection you can deploy

NSS ships signatures for the behaviour, not only the names, because names rotate and behaviour lasts. All are in the paper's repository, versioned and dated, each with a false-positive note.

- **YARA** (validated 16 November 2026, fired against the captured samples): `NSS_KD01_gate_challenge_page` matches the gate challenge

page on the `#tthCv` / `#tthStatus` / `#tthLive` ids plus a `/.rt/` endpoint or the `euwest1::` support code (not on the common title "Loading" alone); `NSS_KD01_fortnite_checker_lure` matches the behind-gate checker page. Both fired on the real samples and not on a benign Fortnite-fan test page.

- **Suricata** (conditions matched against the captured requests; replay through a live sensor pending a pcap): rules for `GET /.rt/challenge?tier=captcha`, `POST /.rt/ce`, `POST /.rt/verify`, the fail-path body, and a correlated challenge-then-verify flowbit. Written to the kit's URI shape, not one hostname, so they survive a name change.
- **Blocklist-ready**: the request-path regex `^/\.rt/(challenge|verify|ce)\b`, the markup selector set, the support-code pattern `euwest1::[0-9]{9,11}-[0-9a-f]{32}`, and the server address 193.187.110[.]18, each on its own so you can take only what fits your controls.

One operator's tooling, one server

Two independent classes of durable evidence agree. **Kit internals**: the `/.rt/` endpoint family, the `TETHER` / `#tthCv` markup and the `euwest1::` support-code format are identical across the 12 gated names. **Build artifacts**: two content-addressed build assets are byte-identical across fortchecker[.]net and lockfort[.]app, logo-header-DSTmN--R[.]svg (sha256 d668fe90…) and epic-shield-fh9_fbax.svg (sha256 6ed60cff…), which is the same build, not shared hosting. Together these tie the Fortnite checker sites to one operator's tooling on one server. NSS names no actor and makes no country-of-origin claim. The crypto name on the same gate (amlapp[.]site) is a lead that one operator runs both the Fortnite and the crypto sides, or that the kit was sold to two customers on one host; recorded, not decided. Shared hosting alone is never the tie.

What we cannot say

- NSS confirmed the checker landing and the "SIGN IN WITH EPIC" credential-entry step by its own read-only capture. NSS did not open the fake Epic password screen or the one-time-code screen, so those

are assessed from the operator's own tracker, not observed. The real-time relay of the password and the live code to Epic is from public reporting only; NSS did not see it.

- NSS executed nothing. There was no installer on any captured page, so there is no persistence or command-and-control to report; this is credential phishing, not malware.
- NSS did not capture the complete post-gate flow across every device profile the gate serves; what sits beyond the credential-entry step is assessed from the operator's own tracker and from public reporting, not observed. This is a known gap.
- NSS names no actor and makes no country-of-origin claim.

Who is behind it, and how far the evidence goes

What the records prove:

- **K1 is one server for one vocabulary.** 40 names on one address in six days, each on its own DNS account, and every name NSS recorded answering from the address belongs to the set (one more name appears only in the server's certificate). The names are built from Russian words and imitate Russian services: the lures are written for Russian speakers.
- **F2 is one server** with 75 names in NSS's record, and its newest wave was mostly unlisted on 16 November.
- **R1 is one buyer**: four purchase bursts at one registrar, the first three joined by shared DNS accounts.
- **X1 is one DNS account.** M1 and H1 are tied by registrar, naming and timing only, which is why they read "likely".

What they do not prove:

- **Who runs any set.** NSS names no actor. "Russian-language" describes the words of the K1 names and the services they imitate, nothing more. The server's network is registered in Hong Kong, its address sits in

Bulgaria, and the names were bought at registrars in several countries. Nothing in NSS's records points to a state or to any named group.

- **That the sets are one operation.** They do not share servers, registrars or DNS accounts, and they speak to different audiences: Russian-speaking children (K1), English-speaking Fortnite players (F2), South-East Asian teenagers (M1), Minecraft players (H1), Roblox players anywhere (R1, X1).
- **That a child was harmed by a given name.** NSS records infrastructure. It holds no victim data and sought none.

Responsible disclosure

NSS disclosed before publishing (the standing rule for a children-safety paper). On 16 November 2026, through its research outreach address, NSS notified the impersonated platform and the servers' abuse contacts, with each route verified the same day from the party's own security[.]txt or from the registry record:

- Epic Games (the brand the Fortnite checker impersonates), security route.
- The host of the Fortnite checker server 193.187.110[.]18, the single choke point for its 64 live

names, through its network abuse contact.

- The host of the K1 server 87.120.104[.]209, and the registrars of the named sets.
- Brand security routes for Supercell, Hypixel and Ozon.

A brand report for the Roblox look-alike names goes through Roblox's web report form (no email security route) and is in the outreach queue. This paper is held for a disclosure window and names no detail of how NSS reads a page. The notices were drafted before NSS reached the page behind

the gate; the Epic notice is updated to note that NSS has since confirmed the checker page read-only.

For platform trust and safety teams

1. **Put the names in your link checks today.** The files carry every name with its set and its state on 16 November. Staged names (M1, H1) are the ones worth loading before they are used: they go live when the messages go out.
2. **Block the two servers.** 87.120.104[.]209 (K1) and 193.187.110[.]18 (F2) answered for 40 and 64 of these names on 16 November. A new name the operator points at either address is covered by the same block.
3. **Match the shapes, not only the names.** The patterns below catch the next name of each set. Use them to hold a chat link for review, not to punish the sender: the sender is often a child whose account was taken.
4. **Normalise look-alike letters before brand matching.** Turn "rn" into "m", "vv" into "w", "l" and "1" into "i" where a brand name is expected, and decode accented letters (xn--) before comparing.
5. **Watch the sign-in that follows a relay page.** A sign-in from a new network that uses a two-step code minutes after it was sent, followed by a trade, a gift or a password change, is how a checker page cashes out. Slow down item trades and email changes on accounts that show it.
6. **Tell the child, not only the parent.** Recovery messages written for adults do not reach a twelve-year-old. A short in-game notice ("someone used your password; here is how to get your items back") does.

For schools

- Add the indicator file to the school web filter, and block newly registered names if the filter offers that category: every name in this paper was first recorded by NSS in the three weeks before 16 November.
- Teach the bait words in a lesson, not only the danger: "free Robux", locker checker, gem generator, "vote for my friend", private-server link, executor (a program kids download to cheat in Roblox).
- School devices should not run game cheats or executors. If one was installed on a shared device, change the passwords saved in its browser from another device. A pupil who reports a stolen account, a clicked link or an installed cheat should be helped, not sanctioned: quick reporting is what limits the harm.
- In the same period NSS found no look-alike of the main school sign-in platforms with a login page; this paper is about the games children play outside lessons, often on school-issued devices.

What a defender can look for

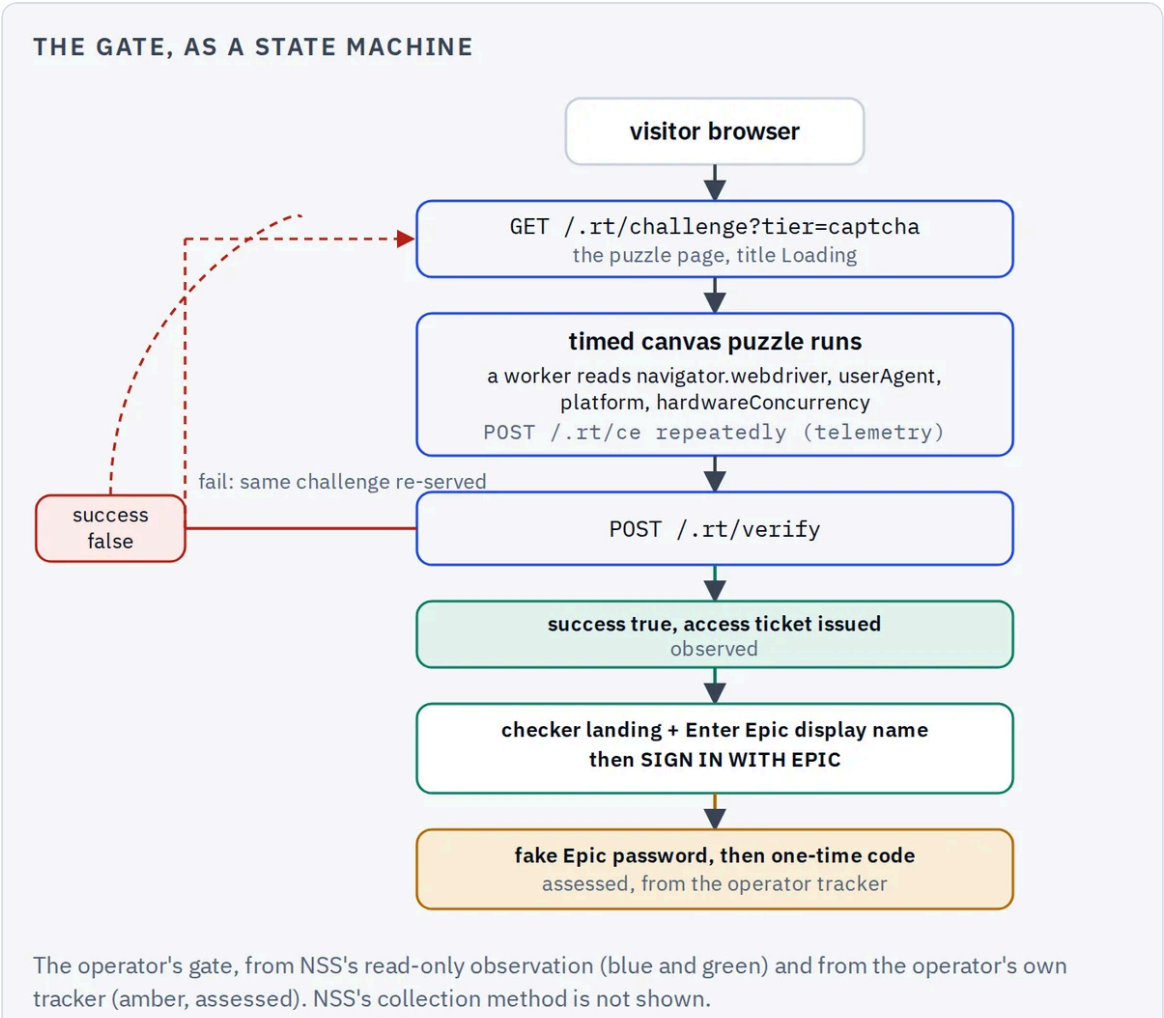
1. VK look-alikes of the K1 shape: `^v[il]kontal?kte-[a-z]{1,3}\.[a-z]+$` matches all eight in this paper and not the real service's names.
2. Roblox addresses of the R1 shape: `^(?:[a-z]{2}-roblox|roblox-[a-z]{2}|robloxj)\.com$` matches all fourteen. Alert, do not block: a short shape can match a brand's own defensive registration.
3. Mobile Legends support names: `(mlbb|moonton|rnoonton|mobilegend|mobilelegend|rnobilelegend|lbbgames)` on .cloud matches all 34.
4. Fortnite checker words at the start of a new name: `^(?:fort|fn|epic)[a-z0-9-]*(?:lo?c?k|loker|check|worth|val|skin|og|treasure|spin)|^(?:lock|check|worth|skin|og)[a-z0-9-]*(?:fort|fn)` matches the descriptive names (22 of the 64 Fortnite names, such as fortnitelockerworth[.]com, fort-locker[.]net and fnlocker[.]help); short invented names (fortvot[.]top, epicsan[.]top) are covered only by the server block. Alert only: it also matches ordinary names such as fortworth.

5. Hypixel and Minecraft "creator", "youtube", "event", "support" and "migration" names under three months old.
6. Any new name that answers from 87.120.104[.]209 or 193.187.110[.]18.

All indicators are in the list below, and each one opens as a casefile in NSS Investigate.

How it maps to ATT&CK

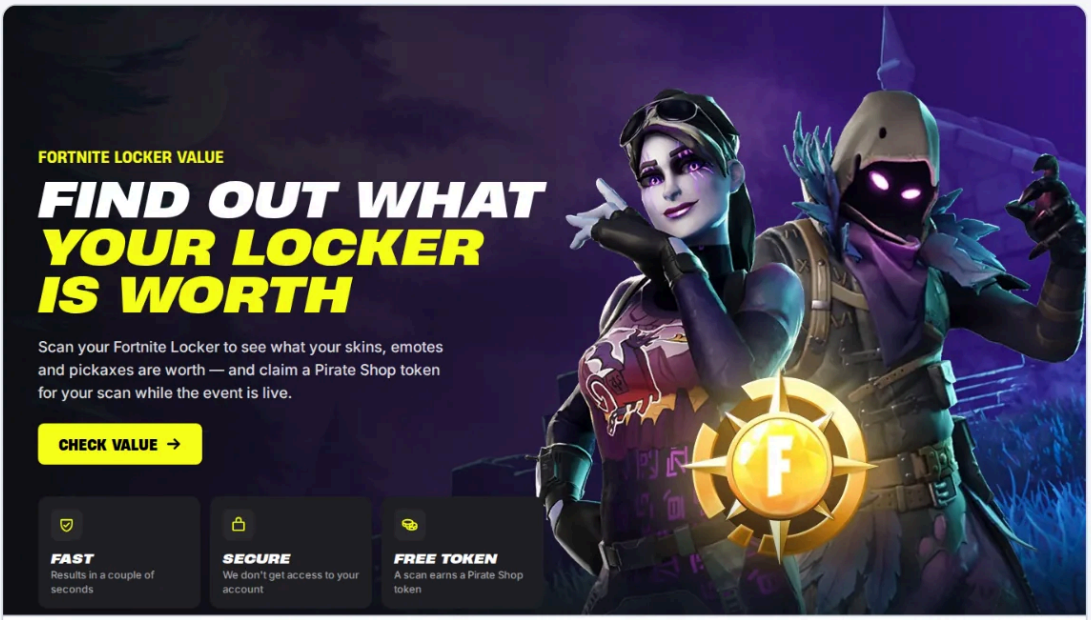
TECHNIQUE	WHAT NSS SAW
T1583.001 Acquire Infrastructure: Domains	188 names bought between late October and 16 November 2026, R1 in timed bursts
T1583.004 Acquire Infrastructure: Server	the K1 and F2 servers
T1566.003 Phishing: Spearphishing via Service	expected from the name shapes, not observed: lures shaped for game chat, community servers and social messages
T1656 Impersonation	Roblox, Epic Games, Supercell, Moonton, Hypixel and VK look-alikes



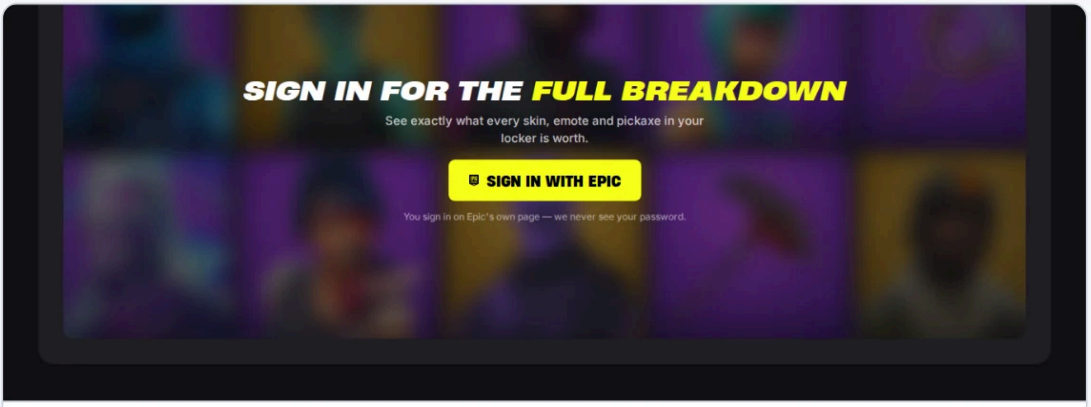
The operator's gate, from NSS's read-only observation (blue and green) and from the operator's own tracker (amber, assessed). NSS's collection method is not shown.

The operator's gate, from NSS's read-only observation (blue and green) and from the operator's own tracker (amber, assessed). NSS's collection method is not shown.

BEHIND THE GATE: THE FORTNITE CHECKER, 16 NOV 2026



fortchecker[.]net, behind the gate
Captured 16 Nov 2026. The checker landing a child reaches after the puzzle: real Epic skin art and a real V-Bucks link borrowed to look genuine, a CHECK VALUE button, and a promise of a reward token.



the same site, the credential step
Captured 16 Nov 2026 after a lookup with a fake display name. The page then asks the child to SIGN IN WITH EPIC. This is the furthest NSS went, read-only; NSS entered nothing and did not open the sign-in.

NSS's own captures, cropped to the page. Addresses are defanged. The page as served, shown as evidence; NSS is not affiliated with any brand the names imitate.

Behind the gate: the checker landing and the SIGN IN WITH EPIC step, captured read-only by NSS on 16 November 2026. The sign-in button is the furthest NSS reached; NSS entered nothing. The page is shown as evidence; NSS is not affiliated with any brand it imitates.

ROBLOX LINK NAMES, FOUR PURCHASE BURSTS

10 Nov, 02:02:47 UTC: lhttps-www--roblox[.]com, a listed look-alike of another shape, is bought at a different registrar, 2.5 minutes before burst 1.

Burst 1	10 Nov	02:05:20 to 02:07:33 UTC, one registrar `av-roblox[.]com` `roblox-vm[.]com` `ur-roblox[.]com` `uv-roblox[.]com`
Burst 2	11 Nov	21:21:22 to 21:22:50 UTC, one registrar `at-roblox[.]com` `ec-roblox[.]com` `ma-roblox[.]com`
Burst 3	13 Nov	03:42:21 to 03:44:16 UTC, one registrar `ae-roblox[.]com` `ei-roblox[.]com` `rn-roblox[.]com` `robloxj[.]com`
Burst 4	15 Nov	01:40:23 to 01:41:34 UTC, one registrar `roblox-at[.]com` `roblox-id[.]com` `roblox-is[.]com`

Registration times from public registration records, read 16 Nov 2026. Bursts 1 to 3 also share DNS accounts; burst 4 matches by registrar, shape and buying habit. None of the 14 was on a list on 16 Nov.

Set R1 from public registration records, read 16 November 2026.

The NSS tools used

> Discovery
Recorded the new names through NSS's own sensors and matched them to the games and services they imitate.

> Investigate
Read the casefile of every name and both servers: what each address serves and the names known on it.

> Scan
Read each indicator on 16 November on Scan as well as Investigate; every one read so far gave the same band on both.

> Tools
Chained two reads of NSS's own records over a Fortnite checker name: its addresses on record, then every name seen on those addresses.

Indicators

The first 25 of 192 indicators. Each is written defanged so it cannot be opened by accident. TLP:CLEAR. Use them in your own tools; no account needed.

INDICATOR	TYPE	NOTE
193[.]187[.]110[.]18	IP address	Server of set F2: 75 names recorded on it, 64 still answering from it on 16 Nov 2026 (43 of those on no threat list NSS takes in); Fortnite locker-worth and skin-checker names, plus crypto check names
across[.]cash	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; in DNS from 11 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
amlapp[.]site	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; in DNS from 9 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
amlbot[.]shop	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; in DNS from 29 Oct 2026; 16 Nov 2026: no address (registered, not answering); on a threat list NSS takes in, list date 30 Oct 2026
amlmonitor[.]cfd	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; in DNS from 9 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 9 Nov 2026
amltransactions[.]icu	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; in DNS from 8 Nov 2026; 16 Nov 2026:

		193[.]187[.]110[.]18; on a threat list NSS takes in, list date 9 Nov 2026
bookingusdt2cash[.]com	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 27 Oct 2026
coinbace-transaction[.]com	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 9 Nov 2026
collab-verify-land[.]com	Domain	F2 server (193[.]187[.]110[.]18), crypto check name; may be a second customer of the same host; in DNS from 12 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
epicfn[.]skin	Domain	F2 Fortnite locker checker server; in DNS from 7 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
epicgamers[.]top	Domain	F2 Fortnite locker checker server; in DNS from 11 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
epicmoon[.]top	Domain	F2 Fortnite locker checker server; in DNS from 11 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
epicsan[.]top	Domain	F2 Fortnite locker checker server; in DNS from 11 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)

fn-treasure[.]info	Domain	F2 Fortnite locker checker server; in DNS from 6 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 7 Nov 2026
fnawards[.]top	Domain	F2 Fortnite locker checker server; in DNS from 11 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
fnlocker[.]help	Domain	F2 Fortnite locker checker server; in DNS from 12 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
fnlocker[.]vip	Domain	F2 Fortnite locker checker server; in DNS from 5 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 6 Nov 2026
fnlockr[.]cc	Domain	F2 Fortnite locker checker server; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 9 Nov 2026
fnmkt[.]cc	Domain	F2 Fortnite locker checker server; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 9 Nov 2026
fnog[.]info	Domain	F2 Fortnite locker checker server; in DNS from 12 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
fntoken[.]surf	Domain	F2 Fortnite locker checker server; in DNS from 8 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
fntracker[.]skin	Domain	F2 Fortnite locker checker server; in DNS from 10 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on a

		threat list NSS takes in, list date 11 Nov 2026
fnvals[.]com	Domain	F2 Fortnite locker checker server; in DNS from 12 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
fnvalue[.]live	Domain	F2 Fortnite locker checker server; in DNS from 7 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on no threat list NSS takes in (16 Nov 2026)
fnzone[.]live	Domain	F2 Fortnite locker checker server; in DNS from 12 Nov 2026; 16 Nov 2026: 193[.]187[.]110[.]18; on a threat list NSS takes in, list date 12 Nov 2026

ALL 192 INDICATORS: CSV JSON also on GitHub No sign-up.

Check an indicator from this paper

How we know

What this rests on

- Responsible disclosure: NSS notified the impersonated platform (Epic Games) and the hosting and registrar abuse contacts on 16 November 2026, before publication, with each route verified from the party's security[.]txt or the registry record. This paper is held for a disclosure window.
- Which name answered from which address, and on which days, is NSS's own record, read on 16 November 2026 from NSS's records, plus a fresh DNS look-up of all 188 names on 16 November. Times are UTC.
- The listing state was checked on 16 November 2026 against every list NSS takes in. A listing of the name counts. A listing date is the date the list gives, not the day NSS took the listing in.

- Registration times and registrars are public registration records read by NSS on 16 November 2026. The day a name entered DNS is the first day NSS saw it in DNS.
- Certificate times are from public certificate logs.
- Every verdict in this paper was read on Investigate and then on Scan on 16 November 2026; all 192 indicators (the 188 names, both servers and the two listed context names) were read on both Investigate and Scan, and the two agree on every one; the files carry all 188 names and both servers, without bands.
- What the pages showed is from NSS's own captures of 16 November 2026 between 14:38 and 14:56 UTC. The Fortnite checkers showed a human check, the K1 names an empty page, and one Roblox link name a timeout; no capture showed a login, payment or code form.

What we cannot say

- "On no threat list NSS takes in" is not "on no threat list anywhere". Most names in this paper were under two weeks old at the check.
- A name that answers is not proof of a live lure: many of these pages show nothing at their front door, and a lure may open only at the full address in a message. Staged names (M1, H1) may never be used.
- The six sets are tied inside themselves and not to each other. M1 and H1 rest on registrar, naming and timing, which can be shared by unrelated buyers; they read "likely".
- "Russian-language" describes the words of the K1 names and the services they imitate. It says nothing about where the operator lives or who they are. NSS names no actor and sees no sign of any state.
- The crypto names on the F2 server may belong to another customer of the same host.
- NSS records infrastructure. It holds no victim data, sought none, and cannot say how many children met these pages.
- NSS's own bands lag this evidence. Most unlisted names read Clean on Investigate and Scan (the two agree) because NSS judges a name by

what it serves and the pages showed no lure form to NSS; the servers, most listed names and most Roblox link names read on both were Suspicious or higher. The files therefore do not carry bands.

Use and citation

This paper is marked TLP:CLEAR: it may be shared without restriction. Cite as:

```
Nexus Sentinel Station (NSS), "Phishing aimed at children and their
families: 188 look-alike names in six sets", NSS-KD-01, 16 Nov 2026.
https://nsshq.com/research/game-account-phishing-children
```

See something wrong? corrections@nsshq.com

More from NSS Research

NSS-RH-01: Lottery redirect names on a shared delivery network: technical analysis

NSS-OC-01: Linked hosting clusters and the purchase batches behind them: technical analysis

NSS-WA-01: WhatsApp lookalike kit: technical analysis

NSS is not affiliated with Roblox, Epic Games, Supercell, Moonton, Mojang, Microsoft, Hypixel, VK, Ozon or any registrar, hosting company, DNS service or network behind the names in this paper. They are named because the names and the public records name them; nothing here says they knew of or took part in the activity. No child's data was sought, opened or kept for this paper.