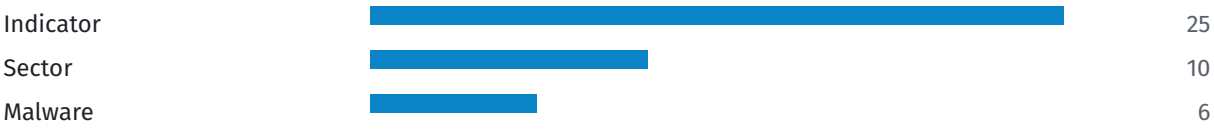
IoC digest 2026-11-29

TLP:CLEAR
Nov 29 2026
Prepared by Damian Villarreal

At a glance

Past targets: Education, Energy, Finance, Government, Healthcare, Hospitality, NGO, Retail, Technology, Telecommunications
Locations: none recorded

OpenCTI records attached to this report.



Summary

Sources reported 1750 URLs that scored 70 or higher in the 24 hours ending at 7:00 a.m. Central on Nov. 29. botnetdomain, Heyiwei and mirai were the most common feed tags.
The Highlights section lists 25 URLs for review.

Analysis

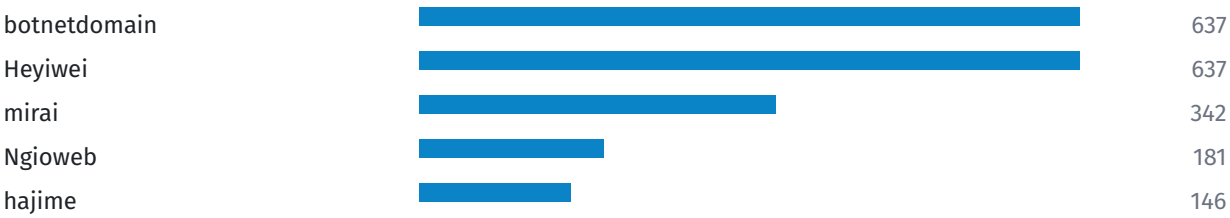
Today in numbers

Indicators scoring 70 or more, last 24 hours	1750
Of those, counted below (highest-scoring per type)	1000
URLs in Highlights	25
Malware families matched in OpenCTI	6
Sectors linked to those families in prior reports	10

Indicators by type



Top feed tags





The feeds supply these tags. Verify malware attribution before citing a family name.

Prior targeting

OpenCTI links elf.mozi, win.salatstealer, elf.mirai, elf.hajime, win.smartloader and Gafgyt to the sectors below based on earlier reporting.

Sectors

Education
Energy
Finance
Government
Healthcare
Hospitality
NGO
Retail
Technology
Telecommunications

Highlights

Indicator	Type	Label	Score	Source
hxxp://27[.]207[.]228[.]234:38888/bin[.]sh	Url	Mozi	80	Abuse.ch
hxxp://115[.]50[.]105[.]167:52743/i	Url	Mozi	80	Abuse.ch
hxxp://115[.]62[.]78[.]56:48831/i	Url	mirai	80	Abuse.ch
hxxp://42[.]227[.]153[.]116:54687/i	Url	mirai	80	Abuse.ch
hxxp://221[.]13[.]235[.]194:56583/i	Url	Mozi	80	Abuse.ch
hxxp://119[.]91[.]141[.]214:1234/Video[.]scr	Url	luckyware	80	Abuse.ch
hxxp://185[.]71[.]69[.]198:34190/Mozi[.]m	Url	hajime	80	Abuse.ch
hxxp://212[.]107[.]229[.]23:52295/Mozi[.]m	Url	hajime	80	Abuse.ch
hxxp://181[.]117[.]210[.]108:5315/bin[.]sh	Url	hajime	80	Abuse.ch
hxxp://115[.]63[.]201[.]225:48242/bin[.]sh	Url	dakkatoni	80	Abuse.ch
hxxp://125[.]43[.]25[.]118:42790/bin[.]sh	Url	dakkatoni	80	Abuse.ch
hxxp://182[.]123[.]253[.]9:33050/bin[.]sh	Url	dakkatoni	80	Abuse.ch
hxxp://182[.]117[.]202[.]117:40501/bin[.]sh	Url	mirai	80	Abuse.ch
hxxps://github[.]com/Eastzurfortress/powershell/releases/download/RELEASE/release[.]zip	Url	cheat	80	Abuse.ch

Indicator	Type	Label	Score	Source
hxxps://raw[.]githubusercontent[.]com/abrshewube/aau-connectivity/refs/heads/main/public/fonts/fa-solid-500[.]woff2	Url	DEVPOPPER	80	Abuse.ch
hxxp://103[.]75[.]190[.]47:49152/?h=103[.]75[.]190[.]47&p=49152&t=ws&a=w64&stage=true	Url	vshell	80	Abuse.ch
hxxps://studiogioeli[.]it/trichloroflouromethane/Order[.]js	Url	AgentTesla	80	Abuse.ch
hxxp://85[.]234[.]100[.]110/yrjrs/thth[.]bba	Url		80	Abuse.ch
hxxps://gateway[.]pinata[.]cloud/ipfs/bafybeiacdac2rwdp43tlq3neytltsizxwboutsyyodyolmtwd6kq26knji/probe-x86	Url		80	Abuse.ch
hxxps://gateway[.]pinata[.]cloud/ipfs/bafybeih6rbfbcghgoddnveyr2gbm7ulbrnbhlqgwm6st3wmcgdklxpdx3y/probe-x86	Url		80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/Tahir77ba/spare/refs/heads/main/[.]github/workflows/dear-nikki_v3[.]5[.]zip	Url	SmartLoader	80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/spammhedi/NIKA_desktop/refs/heads/main/oversparingly/v1[.]9[.]zip	Url	SmartLoader	80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/S-Hariharan-06/reelbird/refs/heads/main/haberdash/Website-AP-v2[.]5[.]zip	Url	SmartLoader	80	Abuse.ch
hxxps://github[.]com/elitebaiter2-cpu/payme/releases/download/yofr/Client-built[.]exe	Url	QuasarRAT	80	Abuse.ch
hxxps://github[.]com/mudherbalistanimate/Telegram-Zapret/releases/download/Telegram-Zapret/TgWsProxy_windows_7_32bit[.]exe	Url	SalatStealer	80	Abuse.ch

For indicators on shared services like GitHub and Dropbox, scope any block to the exact URL.

Security headlines

- SAT Provider College Board Hacked, Exposing User Data and Triggering Password Resets (unknown source, 2026-11-29)
- COLLEGE BOARD PROBES SAT DATA BREACH (unknown source, 2026-11-29)
- College Board Cyberattack: CSS Profile Down After AI Breach (unknown source, 2026-11-29)
- SAT administrator College Board hit by suspected AI-assisted cyberattack, new accounts and CSS Profile suspended: Check details (unknown source, 2026-11-29)
- Cyberattack exposes personal data of some US college exam users (unknown source, 2026-11-29)
- College Board breach puts CSS Profile on pause as aid deadlines loom (unknown source, 2026-11-29)
- College Board Confirms Cyberattack Suspected Of Involving AI Tools; Basic Account Data Accessed (unknown source, 2026-11-29)
- US student data exposed in cyberattack? SAT maker College Board hit after Air Force breach (unknown source, 2026-11-29)

Full list

In OpenCTI, open Indicators under Observations. Set Valid from to the last 24 hours, Score to 70 or higher and Valid until to after today. Select Export and choose CSV.

Entities

Sector 10

Name	Description
Energy	Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Finance	Public and private entities involved in the allocation of assets and liabilities over space and time.
Education	Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.
Telecommunications	Private and public entities involved in the production, transport and dissemination of information and communication signals.
Hospitality	Private entities offering to customers' leisure activities and experiences.
Retail	Distribution and sale of goods directly to the consumer.
Technology	Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
NGO	A legally constituted non-commercial organization created by natural or legal persons with no participation or representation of any government.
Healthcare	Public and private entities involved in research, services and manufacturing activities related to public health.
Government	Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator 25

Indicator	Type	Score
hxxp://185[.]71[.]69[.]198:34190/Mozi[.]m	Url	80
hxxps://github[.]com/elitebaiter2-cpu/payme/releases/download/yofr/Client-built[.]exe	Url	80
hxxp://103[.]75[.]190[.]47:49152/?h=103[.]75[.]190[.]47&p=49152&t=ws&a=w64&stage=true	Url	80
hxxps://raw[.]githubusercontent[.]com/S-Hariharan-06/reelbird/refs/heads/main/haberdash/Website-AP-v2[.]5[.]zip	Url	80
hxxps://github[.]com/mudherbalistanimate/Telegram-Zapret/releases/download/Telegram-Zapret/TgWsProxy_windows_7_32bit[.]exe	Url	80
hxxp://181[.]117[.]210[.]108:5315/bin[.]sh	Url	80

Indicator	Type	Score
hxxp://182[.]123[.]253[.]9:33050/bin[.]sh	Url	80
hxxps://gateway[.]pinata[.]cloud/ipfs/bafybeiacdac2rwdp43tlq3neytltsizxwboutsyyodyolmtwd6kq26knji/probe-x86	Url	80
hxxp://42[.]227[.]153[.]116:54687/i	Url	80
hxxp://27[.]207[.]228[.]234:38888/bin[.]sh	Url	80
hxxps://raw[.]githubusercontent[.]com/Tahir77ba/spare/refs/heads/main/[.]github/workflows/dear-nikki_v3[.]5[.]zip	Url	80
hxxps://gateway[.]pinata[.]cloud/ipfs/bafybeih6rbfbcghgoddnveyr2gbm7ulbrnbhlqgwm6st3wmcgdklxpdx3y/probe-x86	Url	80
hxxp://119[.]91[.]141[.]214:1234/Video[.]scr	Url	80
hxxp://85[.]234[.]100[.]110/yrjrs/thth[.]bba	Url	80
hxxp://221[.]13[.]235[.]194:56583/i	Url	80
hxxps://raw[.]githubusercontent[.]com/spammhedi/NIKA_desktop/refs/heads/main/oversparingly/v1[.]9[.]zip	Url	80
hxxp://115[.]63[.]201[.]225:48242/bin[.]sh	Url	80
hxxps://studiogioeli[.]it/trichloroflouromethane/Order[.]js	Url	80
hxxps://raw[.]githubusercontent[.]com/abrshewube/aau-connectivity/refs/heads/main/public/fonts/fa-solid-500[.]woff2	Url	80
hxxp://212[.]107[.]229[.]23:52295/Mozi[.]m	Url	80
hxxp://125[.]43[.]25[.]118:42790/bin[.]sh	Url	80
hxxp://115[.]50[.]105[.]167:52743/i	Url	80
hxxp://115[.]62[.]78[.]56:48831/i	Url	80
hxxps://github[.]com/Eastzurfortress/powershell/releases/download/RELEASE/release[.]zip	Url	80
hxxp://182[.]117[.]202[.]117:40501/bin[.]sh	Url	80

Malware 6

Name	Description
elf.mozi	Threat: elf.mozi Reporter: HoneyLabs
win.salatstealer	Threat: win.salatstealer Reporter: anonymous
elf.mirai	Threat: elf.mirai Reporter: Tuxxin
elf.hajime	Threat: elf.hajime Reporter: Tuxxin
win.smartloader	Threat: win.smartloader Reporter: PierrunoYT
Gafgyt	Threat: elf.bashlite Reporter: Tuxxin

Created with OpenCTI.