IoC digest 2026-11-28

TLP:CLEAR
Nov 28 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 767 URLs that scored 70 or higher in the 24 hours ending at 7:00 a.m. Central on Nov. 28. SmartLoader, SalatStealer 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	767
URLs in Highlights	25
Malware families matched in OpenCTI	3
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, elf.mirai and win.smartloader 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://114[.]217[.]251[.]140:40365/bin[.]sh	Url	mirai	80	Abuse.ch
hxxp://182[.]123[.]188[.]210:42726/bin[.]sh	Url	Mozi	80	Abuse.ch
hxxp://37[.]48[.]187[.]103:46851/i	Url	Mozi	80	Abuse.ch
hxxp://101[.]29[.]21[.]174:43554/[.]i	Url	mirai	80	Abuse.ch
hxxp://115[.]53[.]218[.]98:42479/[.]i	Url	mirai	80	Abuse.ch
hxxp://115[.]50[.]46[.]120:57440/i	Url	dakkatoni	80	Abuse.ch
hxxp://37[.]48[.]187[.]103:46851/bin[.]sh	Url	Mozi	80	Abuse.ch
hxxp://113[.]238[.]163[.]94:56564/bin[.]sh	Url		80	Abuse.ch
hxxp://125[.]47[.]84[.]126:33138/i	Url		80	Abuse.ch
hxxp://218[.]13[.]149[.]41:49180/i	Url		80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/Nnoyrs/nnoyrs[.]github[.]io/refs/heads/main/ephectic/2[.]9-alpha[.]1[.]zip	Url	SmartLoader	80	Abuse.ch
hxxps://static[.]filecr[.]com/filecr-assistant_1[.]3[.]7[.]crx	Url	chrome-extension	80	Abuse.ch
hxxp://204[.]141[.]236[.]157:8092/csky/v_01000000[.]bin	Url	csky	80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/Yosef781227/kidus-aklog/refs/heads/main/public/fonts/fa-solid-500[.]woff2	Url	DEVPOPPER	80	Abuse.ch

Indicator	Type	Label	Score	Source
hxxps://ro-shade[.]lol/download/RoShade[.]zip?v=3	Url	roblox	80	Abuse.ch
hxxp://203[.]193[.]167[.]117:8080/jx/q000	Url	docker	80	Abuse.ch
hxxps://github[.]com/featherclient-mc/Feather-Client/releases/download/v0[.]2[.]0[.]338/Feather-Client[.]zip	Url	cheat	80	Abuse.ch
hxxps://github[.]com/QuarkSoundAdapter/47afe4ec/releases/download/8479c7d4/latest_release_x64[.]rar	Url	cheat	80	Abuse.ch
hxxp://108[.]165[.]95[.]35/x86_64	Url	docker	80	Abuse.ch
hxxps://render-96[.]com/f/qus5n9iecneukfdd5bqagg/8d5wkyb6	Url	Amos	80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/phonkakada/e_parking_barrier_controller/refs/heads/main/public/fonts/fa-solid-400[.]woff2	Url	DEVBOX	80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/carvanino/monty_t/refs/heads/main/public/fonts/fa-solid-400[.]woff2	Url	DEVPOPPER	80	Abuse.ch
hxxps://raw[.]githubusercontent[.]com/Ehtesham-Zahid/Ehtesham-Zahid/refs/heads/main/public/fonts/fa-brand-400[.]orc	Url	DEVPOPPER	80	Abuse.ch
hxxps://runelite[.]ch/scrilla/client[.]jar	Url	runelure	80	Abuse.ch
hxxp://204[.]141[.]236[.]157:8089/csky/Heyiwei-csky-abiv1	Url	Heyiwei	80	Abuse.ch

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

Security headlines

- Drupal sites are being hijacked, and a follow-up flaw is already under attack (Malwarebytes, 2026-11-27)

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.

Name	Description
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://204[.]141[.]236[.]157:8089/csky/Heyiwei-csky-abiv1	Url	80
hxxp://37[.]48[.]187[.]103:46851/bin[.]sh	Url	80
hxxp://125[.]47[.]84[.]126:33138/i	Url	80
hxxp://114[.]217[.]251[.]140:40365/bin[.]sh	Url	80
hxxp://37[.]48[.]187[.]103:46851/i	Url	80
hxxp://218[.]13[.]149[.]41:49180/i	Url	80
hxxps://raw[.]githubusercontent[.]com/carvanino/monty_t/refs/heads/main/public/fonts/fa-solid-400[.]woff2	Url	80
hxxps://ro-shade[.]lol/download/RoShade[.]zip?v=3	Url	80
hxxp://203[.]193[.]167[.]117:8080/jx/q000	Url	80
hxxps://raw[.]githubusercontent[.]com/phonkakada/e_parking_barrier_controller/refs/heads/main/public/fonts/fa-solid-400[.]woff2	Url	80
hxxps://raw[.]githubusercontent[.]com/Nnoyrs/nnoyrs[.]github[.]io/refs/heads/main/ephectic/2[.]9-alpha[.]1[.]zip	Url	80
hxxps://raw[.]githubusercontent[.]com/Ehtesham-Zahid/Ehtesham-Zahid/refs/heads/main/public/fonts/fa-brand-400[.]orc	Url	80
hxxp://113[.]238[.]163[.]94:56564/bin[.]sh	Url	80
hxxps://raw[.]githubusercontent[.]com/Yosef781227/kidus-aklog/refs/heads/main/public/fonts/fa-solid-500[.]woff2	Url	80
hxxp://101[.]29[.]21[.]174:43554/[.]i	Url	80

Indicator	Type	Score
hxxp://182[.]123[.]188[.]210:42726/bin[.]sh	Url	80
hxxps://static[.]filecr[.]com/filecr-assistant_1[.]3[.]7[.]crx	Url	80
hxxp://204[.]141[.]236[.]157:8092/csky/v_01000000[.]bin	Url	80
hxxps://render-96[.]com/f/qus5n9iecneukfdd5bqagg/8d5wkyb6	Url	80
hxxps://github[.]com/featherclient-mc/Feather-Client/releases/download/v0[.]2[.]0[.]338/Feather-Client[.]zip	Url	80
hxxps://runelite[.]ch/scrilla/client[.]jar	Url	80
hxxp://115[.]53[.]218[.]98:42479/[.]i	Url	80
hxxps://github[.]com/QuarkSoundAdapter/47afe4ec/releases/download/8479c7d4/latest_release_x64[.]rar	Url	80
hxxp://115[.]50[.]46[.]120:57440/i	Url	80
hxxp://108[.]165[.]95[.]35/x86_64	Url	80

Malware 3

Name	Description
elf.mozi	Threat: elf.mozi Reporter: HoneyLabs
elf.mirai	Threat: elf.mirai Reporter: Tuxxin
win.smartloader	Threat: win.smartloader Reporter: PierrunoYT

Created with OpenCTI.