IoC digest 2026-11-26

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

618 indicators with a score of 70 or more, dated by their source in the 24 hours before 2026-11-26 07:00 Central. The most common labels are Mozi, mirai, SalatStealer. These families have been reported targeting education, energy, finance and other sectors.

Analysis

Today in numbers

Indicators scoring 70 or more, last 24 hours	618
Listed under Highlights	25
Labels resolved to malware in OpenCTI	3
Sectors those families are recorded targeting	10

Indicators by type



Top threat labels



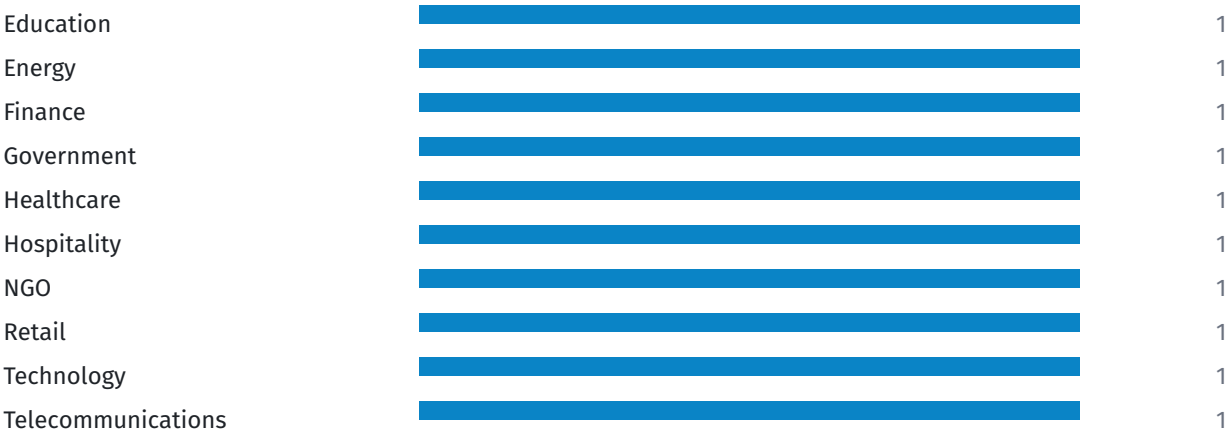


Labels the feeds put on today's indicators. They are the sources' tags, not verified malware identifications.

Who these families target

Targets OpenCTI holds for the families seen today (Mirai, elf.mozi, ValleyRAT), from earlier reporting. They show who these families go after, not who was hit today.

Sectors



Highlights

Indicator	Type	Label	Score	Source
hxxps://uc0be4bfd0b65731ccbdc736c791[.]dl[.]dropboxusercontent[.]com/zip_download_get/CwHC-dNXDC_n7zmL-vCi8QMe6369QYoTMPI_q2AHEC_CK9CBMb6WvBEOPXRvsp38rhFAiz8jT865OMPY-jG7zHx0bPM5JDVPbLKxh5WWZZPQ3g	Url	kitwatch	80	Abuse.ch
hxxps://ucbd1ef3d7be5e3d76ee90cfd8bf[.]dl[.]dropboxusercontent[.]com/cd/0/get/DMrt1tUEGJwbecL6uwurNf58NGTSfhzeBeCMrfAJt-8R4xTVtvrl1axUd8VkBrJCq3CSF7E0GnMKPq9hLJdGbFM09sCWNlldsL9Zh7hui6OAr8VLQDkHeZ1Bazw_Yf43_Dm0kfWFqOoZdivAb9pbR3ZS/file?dl=1	Url	kitwatch	80	Abuse.ch
hxxp://219[.]157[.]232[.]50:44060/bin[.]sh	Url	Mozi	80	Abuse.ch
hxxp://115[.]57[.]212[.]218:48527/bin[.]sh	Url		80	Abuse.ch
hxxp://115[.]50[.]151[.]228:49064/i	Url	Mozi	80	Abuse.ch
hxxp://39[.]89[.]45[.]59:54245/i	Url	Mozi	80	Abuse.ch
hxxp://200[.]81[.]161[.]26:49974/bin[.]sh	Url		80	Abuse.ch
hxxp://163[.]142[.]95[.]243:34472/bin[.]sh	Url		80	Abuse.ch

Indicator	Type	Label	Score	Source
hxxp://64[.]89[.]163[.]112/mips	Url	mirai	80	Abuse.ch
hxxp://31[.]56[.]53[.]117/gz067[.]arm5	Url	mirai	80	Abuse.ch
hxxps://i4-mi[.]cn/generated_pages/moban40/static/download/i4Tools[.]zip	Url	SilverFox	80	Abuse.ch
hxxps://bucketobs[.]oss-cn-hongkong[.]aliyuncs[.]com/i4Toolls_v9[.]12[.]012_Setuip_x64[.]zip	Url	Gh0st	80	Abuse.ch
hxxps://software-download-hk[.]oss-cn-hongkong[.]aliyuncs[.]com/aisizhushou-4[.]5[.]0[.]zip	Url	SilverFox	80	Abuse.ch
hxxps://001-ascjkasckj-acshkask-xnzjsknka[.]oss-ap-southeast-1[.]aliyuncs[.]com/i4Tools_Setup_x6420260921_222527[.]zip	Url	SilverFox	80	Abuse.ch
hxxps://hpp[.]duxlip[.]icu/Hyper[.]zip	Url	hype	80	Abuse.ch
hxxp://checkinidadd[.]com/token	Url	ClickFix	80	Abuse.ch
hxxps://runeliteplus[.]net/downloads/RuneLite[.]exe	Url	runelure	80	Abuse.ch
hxxp://123[.]233[.]80[.]134:46597/Mozi[.]m	Url	mirai	80	Abuse.ch
hxxps://pub-9f713b44098e49fc88246a955a24dd58[.]r2[.]dev/agent-linux-x86	Url	td-agent	80	Abuse.ch
hxxps://edge2[.]speedstest[.]org/files/msedgeupdate[.]dll	Url	malware rat c2	80	Abuse.ch
hxxps://pub-9f713b44098e49fc88246a955a24dd58[.]r2[.]dev/agent-linux-arm64	Url	td-agent	80	Abuse.ch
hxxps://123872[.]xyz/Q1fc8a9OCb7AsC6f/dl/50919e9a-9a60-4703-9059-6cb069788450?a=armv6	Url	td-agent	80	Abuse.ch
hxxps://123872[.]xyz/Q1fc8a9OCb7AsC6f/dl/50919e9a-9a60-4703-9059-6cb069788450?a=arm64	Url	xmr	80	Abuse.ch
hxxps://123872[.]xyz/Q1fc8a9OCb7AsC6f/dl/50919e9a-9a60-4703-9059-6cb069788450	Url	xmr	80	Abuse.ch
hxxps://gitlab[.]com/rackztyga/monotone-hwid-spoofer/-/raw/main/Monotone-HWID-Spoofer-master[.]zip	Url	LummaStealer	80	Abuse.ch

Many of these URLs sit on shared hosting such as GitHub, GitLab or Cloudflare. Block the exact URL, not the whole site.

Security headlines

- Multiple Vulnerabilities in Juniper Products Could Allow for Arbitrary Code Execution (Center for Internet Security, 2026-11-26)
- Kyungnam University Hacked, Personal Info of 1,202 Faculty and Students Leaked (unknown source, 2026-11-26)

Full list

OpenCTI: Observations, Indicators, filtered on valid from in the last day, score 70 or more and valid until after today; then Export, 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://64[.]89[.]163[.]112/mips	Url	80
hxxp://163[.]142[.]95[.]243:34472/bin[.]sh	Url	80
hxxp://200[.]81[.]161[.]26:49974/bin[.]sh	Url	80
hxxps://i4-mi[.]cn/generated_pages/moban40/static/download/i4Tools[.]zip	Url	80
hxxps://pub-9f713b44098e49fc88246a955a24dd58[.]r2[.]dev/agent-linux-x86	Url	80
hxxps://runeliteplus[.]net/downloads/RuneLite[.]exe	Url	80
hxxp://31[.]56[.]53[.]117/gz067[.]arm5	Url	80

Indicator	Type	Score
hxxp://39[.]89[.]45[.]59:54245/i	Url	80
hxxps://bucketobs[.]oss-cn-hongkong[.]aliyuncs[.]com/i4Toolls_v9[.]12[.]012_Setuip_x64[.]zip	Url	80
hxxp://115[.]57[.]212[.]218:48527/bin[.]sh	Url	80
hxxps://edge2[.]speedstest[.]org/files/msedgeupdate[.]dll	Url	80
hxxps://hpp[.]duxlip[.]icu/Hyper[.]zip	Url	80
hxxps://gitlab[.]com/rackztyga/monotone-hwid-spoofer/-/raw/main/Monotone-HWID-Spoofer-master[.]zip	Url	80
hxxps://123872[.]xyz/Q1fc8a9OCb7AsC6f/dl/50919e9a-9a60-4703-9059-6cb069788450?a=armv6	Url	80
hxxp://219[.]157[.]232[.]50:44060/bin[.]sh	Url	80
hxxps://123872[.]xyz/Q1fc8a9OCb7AsC6f/dl/50919e9a-9a60-4703-9059-6cb069788450?a=arm64	Url	80
hxxps://ucbd1ef3d7be5e3d76ee90cfd8bf[.]dl[.]dropboxusercontent[.]com/cd/0/get/DMrt1tUEGJwbecL6uwurNf58NGTSfhzeBeCMrfAJt-8R4xTVtvrl1axUd8VkBrJCq3CSF7E0GnMKPq9hLJdGbFM09sCWNlldsL9Zh7hui6OAr8VLQDkHeZ1Bazw_Yf43_Dm0kfWFqOoZdivAb9pbR3ZS/file?dl=1	Url	80
hxxps://001-ascjkasckj-acshkask-xnzjsknka[.]oss-ap-southeast-1[.]aliyuncs[.]com/i4Tools_Setup_x6420260921_222527[.]zip	Url	80
hxxps://123872[.]xyz/Q1fc8a9OCb7AsC6f/dl/50919e9a-9a60-4703-9059-6cb069788450	Url	80
hxxps://uc0be4bfd0b65731ccbdc736c791[.]dl[.]dropboxusercontent[.]com/zip_download_get/CwHC-dNXDC_n7zmL-vCi8QMe6369QYoTMPI_q2AHEC_CK9CBMb6WvBEOPXRvsp38rhFAiz8jT865OMPY-jG7zHx0bPM5JDVPbLKxh5WWZZPQ3g	Url	80
hxxps://pub-9f713b44098e49fc88246a955a24dd58[.]r2[.]dev/agent-linux-arm64	Url	80
hxxp://115[.]50[.]151[.]228:49064/i	Url	80
hxxps://software-download-hk[.]oss-cn-hongkong[.]aliyuncs[.]com/aisizhushou-4[.]5[.]0[.]zip	Url	80
hxxp://123[.]233[.]80[.]134:46597/Mozi[.]m	Url	80
hxxp://checkinidadd[.]com/token	Url	80

Malware 3

Name	Description
elf.mozi	Threat: elf.mozi Reporter: HoneyLabs
ValleyRAT	Threat: win.valley_rat Reporter: abuse_ch
elf.mirai	Threat: elf.mirai Reporter: Tuxxin

Created with OpenCTI.