Threat Actors Exploit Misconfigured Apache Hadoop YARN

By By: Alfredo Oliveira, David Fiser Jul 27, 2021 Read time: 5 min (1372 words)

Published: 2021-07-27 · Archived: 2026-04-05 13:13:05 UTC

To examine this risk, we experimented with exposing such services in the wild. We then learned that it didn't take too long for threat actors to find the exposed service and deploy various malicious payloads. In the following section, we will discuss the malware families targeting exposed YARN services.

Payloads deployed in the attacks: Kinsing and other cryptojacking malware

As cryptojackingnews- cybercrime-and-digital-threats malware is known to be one of the dominant and common payloads for Linux environmentsnews- cybercrime-and-digital-threats, it is no surprise that they were deployed in the YARN service as well. In this case, the payload belongs to a well-known malware family — Kinsing (detected as Trojan.Linux.KINSING.AB and Trojan.SH.KINSING.G).

At the onset of the attack, the threat actors send commands to the exposed service via an HTTP POST request. As an unintended response, the YARN then creates a launch script that incorporates the attackers' commands.

Once the Hadoop container script is executed, it downloads a remote script that deploys Kinsing malware.

It also deploys a Go-compiled binary with spreading capability. This binary communicates with the remote command-and-control (C&C) server, providing a backdoor to the infected system as well as deploying the known Kinsing cryptojacking process called kdevtmpfsi.

Notably, Kinsing is not the only cryptojacking malware found there. The cryptocurrency mining arena remains a battlefield for resources. We found a competitor cryptojacking malware in Hadoop YARN as well. This competing malware then proceeds to eradicate Kinsing from the system.

What are the tactics used in these attacks?

Threat actors aiming to exploit these misconfigured cloud services commonly employ several tactics.

First, threat actors disable the system's protection. As security solutions for cloud services become more popular in enterprises, threat actors adapt by searching for and attempting to uninstall protection software. This functionality is common in cryptojacking malware.

Threat actors also gather credentials. With the ever-increasing variety of platforms that require authentication for access, the need for access tokens and so-called secrets — sensitive information such as credentials used to access systems — also grow. It's not uncommon for users who have a hard time keeping track of them to save these on the machines where they are used. Sadly, this is done without any additional protection. Threat actors are aware of this, and those who successfully access the systems actively seek these unshielded credentials.

And of course, they don't stop with harvesting: they also use these credentials to gain entry into other systems — even non-cloud ones — to infect them. We have similarly observed this behavior in a previous research paper on TeamTNTservices. With this, it can be deduced that threat actors try to infiltrate as many systems as possible to maximize their gains.

It should be emphasized that if the private key that the threat actors used for accessing another system was protected by the owner with at least a passphrase encrypting for the key, the infection of the target system will be unsuccessful. This highlights the importance of employing such security precautions.

Finally, as we shared in our previous research on the Linux threat landscapenews- cybercrime-and-digital-threats, we found out that it is quite common for threats to spread from one infected device to another. To do this, threat actors are using port scanning tools such as masscan to identify exposed and vulnerable services. Once these services are identified, the threat actors try to deploy their payload.

Since the Hadoop YARN service can also run on Windows, threats that were crafted for this platform can also be found in the cluster.

Strengthening cloud service security

As reliance on online systems continues to grow, cloud services are becoming a vital part of enterprises. Cloud security should not be taken for granted. Here are some recommendations:

- **Deliberately configure cloud service.** Users can maximize the built-in security settings afforded by these platforms.
- **Employ the principle of least privilege.** Here, users will only be granted the minimum amount of access required for their task.
- **Adhere to the shared responsibility model.** Users, and not just cloud service providers, are responsible for keeping these platforms secure.
- **Don't store credentials in plaintext; consider using secret vaults.** These store secrets in encrypted form. They can also be used to alter secrets from one place and reflect that modification to multiple applications without the need for a code change.

Cloud security solutions, such as Trend Micro Cloud One™products, help enterprises secure cloud services. The platform includes:

- **Workload Securityproducts: runtime protection for workloads**
- **Container Securityproducts: automated container image and registry scanning**
- **File Storage Securityproducts: security for cloud file and object storage services**
- **Network Securityproducts: cloud network layer IPS security**
- **Application Securityproducts: security for serverless functions, APIs, and applications**
- **Conformityproducts: real-time protection for cloud infrastructure — secure, optimize, complyproducts**

Indicators of Compromise

Hashes

SHA-265	Trend Micro Pattern Detection
25d19152363063eb2b1976b416452e63ad21c205f727837d38d17001831f17f3	Trojan.Linux.KINSING.AB
ec5ed2498945a5b0b1c1f149e201d7395bf3cb1c50f471d820500028ffe19d53	Trojan.SH.KINSING.G
d17b00fd7687d2de31b0dd3b43d468f1de281002228361ef3125b92de0c08772	Trojan.SH.CVE20207961.SM
6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b	Coinminer.Linux.MALXMR.PUWEMA
11547e36146e0b0956758d48faeb19d4db5e737dc942bc7498ed86a8010bdc8b	Coinminer.Win32.MALXMR.TIAOODGJ
1caf7ed35dcb8eddb5bca9120294bc79e7d9a24d451bc0fbebb2195fa5826808	Coinminer.Win32.MALXMR.TIAOODGJ
7cd493e9a14eb33279a96fe025aae0ff37712a300e83dd334cff8ce138fd721a	Coinminer.Win32.MALXMR.TIAOODGJ
83c4ff76659aec8db03942b3b7094736e4377048166839d3ab476067fbc2f892	Coinminer.Win32.MALXMR.TIAOODGJ
559a8ff34cf807e508d32e3a28864c687263587fe4ffdcefe3f462a7072dcc74	Coinminer.Win32.MALXMR.TIAOODDS/16.845.00
a5604893608cf08b7cbfb92d1cac20868808218b3cc453ca86da0ababeadc0537	Coinminer.Win64.MALXMR.SMA/16.845.00

b5584e223d79a1bac7dd75e707f8a6f1be2edd1334d194f30a1c060c11ec130d	Coinminer.MSIL.MALXMR.TIAOODBF
e7446d595854b6bac01420378176d1193070ef776788af12300eb770a397bf7	Coinminer.Linux.MALXMR.UWEKM/16.845.00
fe0816092e006960f2261a3fa919b577aa392291bb0a11149805c651ac633909	Coinminer.SH.MALXMR.UWEKA
1b7e6877d9cc8f4a64e097dbccac1eef9c596fed743d495d5eb9658bb92e3010	Trojan.Win64.MALXMR.N
01b4ccc7be55485ff529ca1f92fd5dbefcce93e13720a8b4d5d3385e944fff8a	Trojan.SH.MALXMR.UWELB
bc79c734cb4378e1d13e429b6237fcee52a1261a396219add751462d0a1ae1b0	Trojan.Linux.MALXMR.UWELD
508ec039ca9885f1afc6f15bb70adfa9ed32f9c2d0bff511052edb39898951c7	Trojan.Python.MALXMR.I
653e638e6e38636b0f14ce233661947f624011ef36f7c7edbc8a7614248c3fce	Trojan.Python.MALXMR.I
599393e258d8ba7b8f8633e20c651868258827d3a43a4d0712125bc487eabf92	PUA.Win64.PhoenixMiner.E
f5d0572b2a5c76bfcf5986b6fbbc96d2cd44da36ae08d2633284fa4782fe68bf	Backdoor.Linux.MIRAI.SMMR1/16.845.00
fa212943d8c9a66e5087ffd73901a887fea6a5bc657db87575889d20f99a2a40	Backdoor.Linux.MIRAI.SMMR1/16.845.00

8a932e992dde32dfa422691ccf46681050bb675472a2877fdc7d69fb36817c8a	Backdoor.Linux.MIRAI.SMMR1/16.845.00
1ab11b57b2848c4ed513acb453cc08b2be65087485ae5fb05b8535fa99645d7b	Backdoor.Linux.MIRAI.SMNM4/16.845.00
6aa250a48dc8e50dd2d96e638eb223a72862441cf41972ecd8529d1c3fe02c8d	Backdoor.Linux.MIRAI.SMNM4/16.845.00
30a36bcc9c9939d7f1ce76965e17cbb0b4514c41ccfda0e8648f117a037c8567	Backdoor.Linux.MIRAI.USDSEFM21/16.845.00
807a6d1de933d35d2793d0932f6ea6a15ee4f76dd3ee91fff4c4f54c1bd0f2e1	Backdoor.Linux.MIRAI.USDSEFM21/16.845.00
44bd5e06802690ceef122c321bc9bc1b570c8738c9d23260ca32ee0e4eba5e0f	Backdoor.Linux.MIRAI.USDSEFM21/16.845.00
1a372a7e7da228278fbeeff1964066eef45f3cf0ae3293031728c69fb8d92b3e	Backdoor.Linux.MIRAI.USDSEFM21/16.845.00
09634a6fab8acacf01b60c0acba85d222d4ad40483259d193cd56c5311449d93	Backdoor.Linux.MIRAI.USDSEFM21/16.845.00
ac7525e69dc3c07ce43344a8b58dca1436088dd2c21878e2dae8b30a69e4d80f	Backdoor.Linux.MIRAI.USDSEFM21/16.845.00
3c250e10153ae0eea58ee17e04868f4fed568f4587774de27f31affb85a7fa19	Backdoor.Linux.MIRAI.USELVEO21/16.845.00
e55c980a3eddb47a26af86af1ce80ae7a251648923770d5feea7c74b1e7dfbf5	Backdoor.Linux.MIRAI.USELVEO21/16.845.00

fe176f4af1beabf9b85bb93f3f585d491209430a11e4376ea8106a2974761387	Backdoor.Linux.MIRAI.USELVEO21/16.845.00
aaaf9574ee271ad917dad99318084256062bbbc7fe90449021963061104a250e	Backdoor.Linux.MIRAI.USELVEO21/16.845.00
b2ab91b682b3b36a31836df30d8298f804697240eddbb5291001c1c588ed832d	Backdoor.Linux.MIRAI.USELVEO21/16.845.00
23656bbf8b94a039f062d24e40fbea51b9aadb29eaeaa7e9a834a43ff378bdab	Backdoor.Linux.MIRAI.USELVEO21/16.845.00
43cbd16376a32ad679aba66e276c644524f275851b991db760295c9160e753f4	Backdoor.Linux.MIRAI.SMMR1/16.845.00
8971773fb614498d64a5220e48da87a9d395faa326bfc66d775815908b18cdb5	Backdoor.Linux.MIRAI.SMMR1/16.845.00
e74d856b07ebcf4c3b21425918daed075f10b3b14f9f97aadf3a2ada96d8a892	Backdoor.Linux.MIRAI.SMMR1/16.845.00
2706f6fa6b0da69436513b0790a9194dcdd2463a5150b9d00699fa30708a9ff9	ELF_MIRAILOD.SM/16.845.00
76d42ec36a9157ba20ccc643d59d8a735ea31016ac1064dc92b4843a578c1520	Backdoor.Linux.GAFGYT.USELVEO21/16.845.00
9a4c8cf6336544d27c62355b85a882fd8137a336d4aaa893d1607ef1b4aa2743	Backdoor.Linux.GAFGYT.USELVEO21/16.845.00
9aa8a11a52b21035ef7badb3f709fa9aa7e757788ad6100b4086f1c6a18c8ab2	HackTool.Linux.PortScan.A/16.845.00

1225cc15a71886e5b11fca3dc3b4c4bcde39f4c7c9fbce6bad5e4d3ceee21b3a	HKTL_SSHBRUTE/16.845.00
558c12a703cac54a1a1206d80b12203d323b869e486a18c4340a09ff0a482570	TROJ_FRS.VSNW18E21/16.845.00
b6154d25b3aa3098f2cee790f5de5a727fc3549865a7aa2196579fe39a86de09	PUA.Win32.XMRig.KAZ

URL

URLs	**Category**
hxxp://update.aegis.aliyun.com/download/uninstall.sh	Disease Vector
hxxp://update.aegis.aliyun.com/download/quartz_uninstall.sh	Disease Vector
hxxp://h.epelcdn.com/dd210131/pm.sh	Disease Vector
hxxp://h.epelcdn.com/dd210131/phpupdate	Malware Accomplice
	Coin Miners
hxxp://176.123.7.127/id210131/phpupdate	Malware Accomplice
	Coin Miners
hxxp://176.123.7.127/id210131/newdat.sh	Malware Accomplice
hxxp://h.epelcdn.com/dd210131/newdat.sh	Malware Accomplice

hxxp://176.123.7.127/id210131/config.json	Disease Vector
hxxp://h.epelcdn.com/dd210131/config.json	Disease Vector
hxxp://176.123.7.127/id210131/networkmanager	Malware Accomplice
hxxp://h.epelcdn.com/dd210131/networkmanager	Malware Accomplice
hxxp://176.123.7.127/id210131/phpguard	Malware Accomplice
hxxp://h.epelcdn.com/dd210131/phpguard	Malware Accomplice
hxxp://h.epelcdn.com/dd210131/spre.sh	Disease Vector
hxxp://209.141.40.190/xms	Insecure IoT Connections
	Disease Vector
hxxp://209.141.40.190/hxx	Malware Accomplice
	Disease Vector
hxxp://209.141.40.190/pas	Disease Vector
	Coin Miners
hxxp://209.141.40.190/scan	Disease Vector
hxxp://bash.givemexyz.in/x86_64	Disease Vector

hxxp://h.epelcdn.com/dd210131/1.0.4.tar.gz	Disease Vector
hxxp://h.epelcdn.com/dd210131/scan.sh	Disease Vector
hxxp://bash.givemexyz.in/i686	Disease Vector
hxxp://bash.givemexyz.in/bashirc.i686	Malware Accomplice
	Disease Vector
hxxp://bash.givemexyz.in/x64b	Malware Accomplice
hxxp://bash.givemexyz.in/x32b	Malware Accomplice
hxxp://209.141.40.190/x86_64	Coin Miners
hxxp://209.141.40.190/bashirc.x86_64	Disease Vector
	Coin Miners
hxxp://209.141.40.190/i686	Disease Vector
	Coin Miners
hxxp://209.141.40.190/bashirc.i686	Disease Vector
	Coin Miners
hxxp://168.138.143.186/batata/Winbox.arm6	Malware Accomplice

hxxp://168.138.143.186/batata/Winbox.arm7	Malware Accomplice
hxxp://168.138.143.186/batata/Winbox.m68k	Malware Accomplice
hxxp://209.141.40.190/ps	Disease Vector
	Coin Miners
hxxp://168.138.143.186/batata/Winbox.mips	Malware Accomplice
hxxp://168.138.143.186/batata/Winbox.mpsl	Malware Accomplice
hxxp://168.138.143.186/batata/Winbox.ppc	Malware Accomplice
hxxp://168.138.143.186/batata/Winbox.sh4	Malware Accomplice
hxxp://168.138.143.186/batata/Winbox.spc	Malware Accomplice
hxxp://168.138.143.186/batata/Winbox.x86	Malware Accomplice

Source: https://www.trendmicro.com/en_us/research/21/g/threat-actors-exploit-misconfigured-apache-hadoop-yarn.html