

5 июня 2024 • Москва, LOFT HALL#2

БЕКОН^{'24}

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Мечтают ли антивирусы о docker-образах?

Капистка Владимир

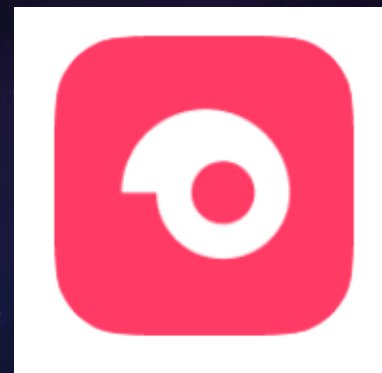
samokat.tech



tg: @kapistka



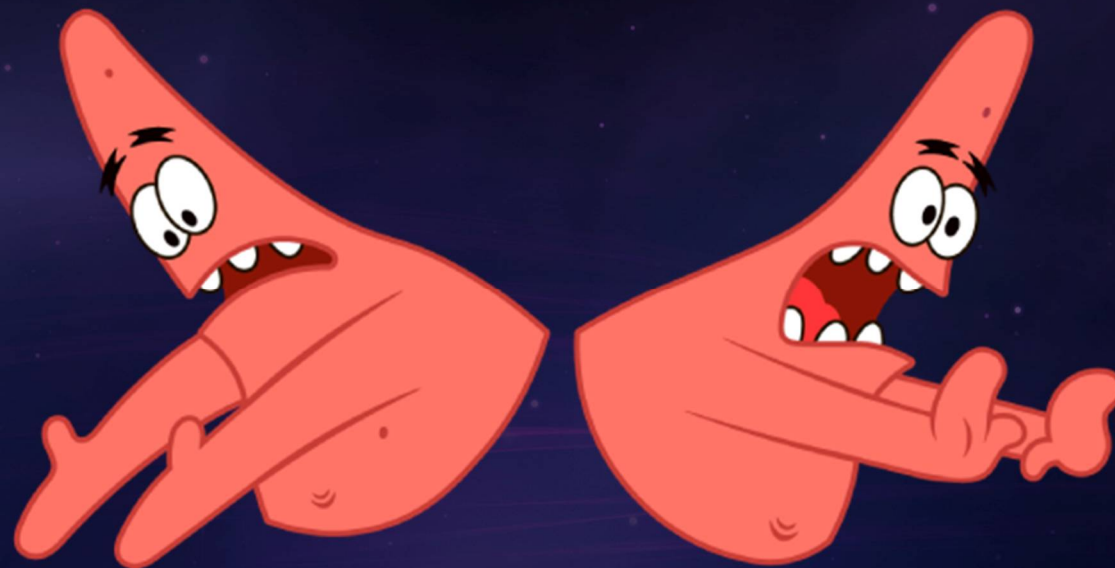
container security tech lead
samokat.tech



- git-ops вместо заявок
- что мы проверяем в публичных образах
- вредоносный код
- реализация анализа
- тестирование
- нюансы
- bypass
- результаты эксплуатации
- пользуйтесь

git-ops вместо заявок

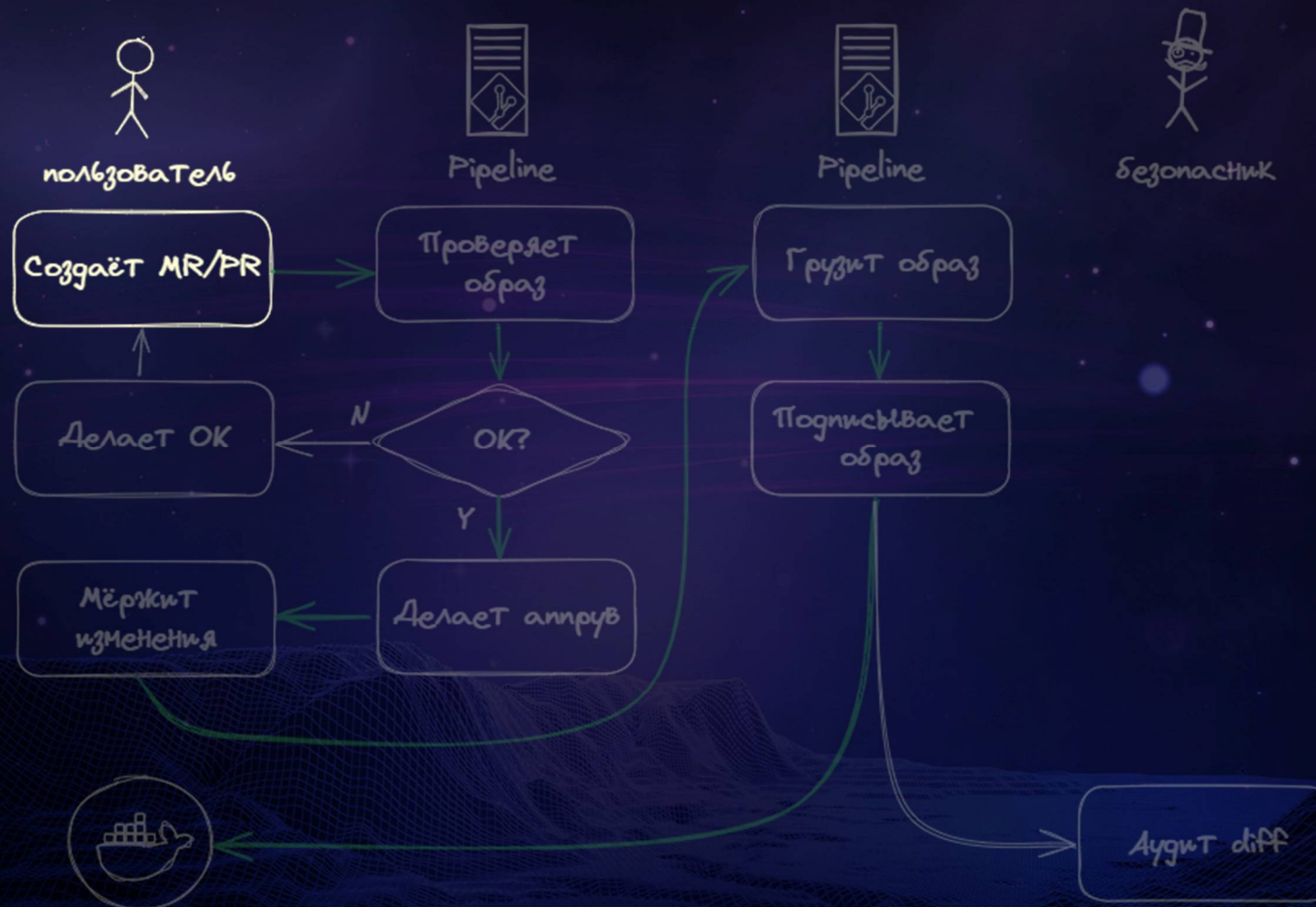


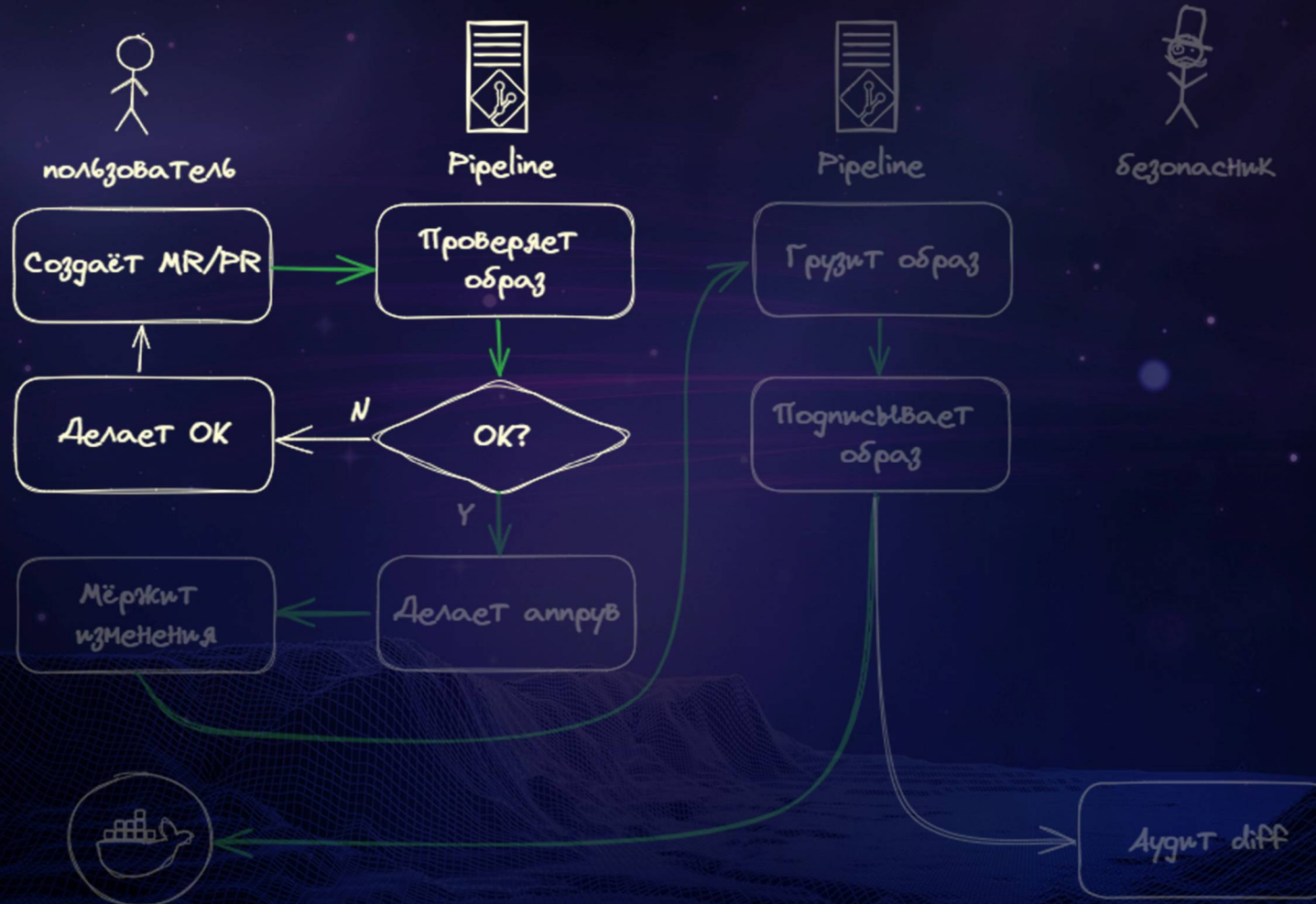


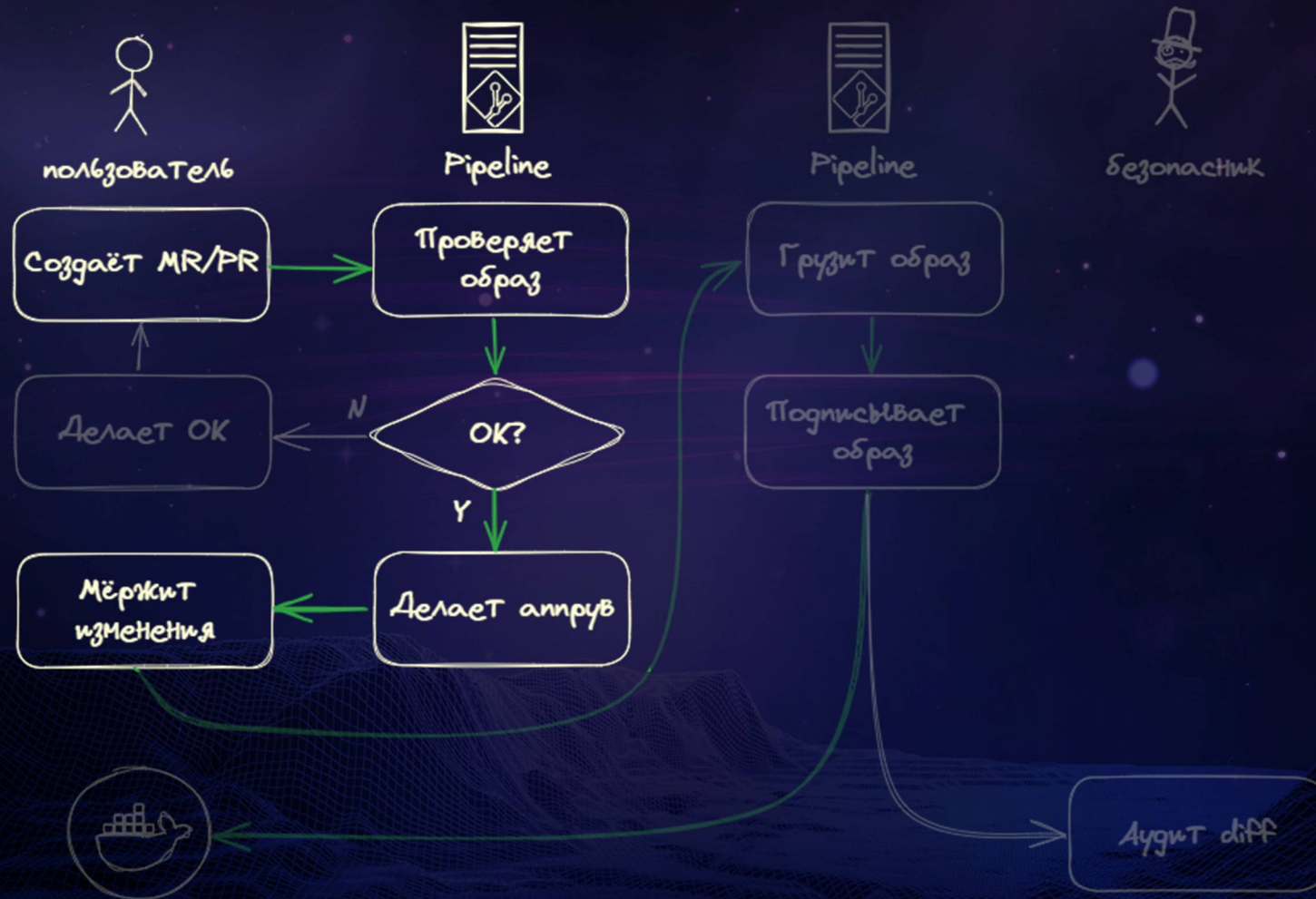
docker.io
gcr.io
ghcr.io

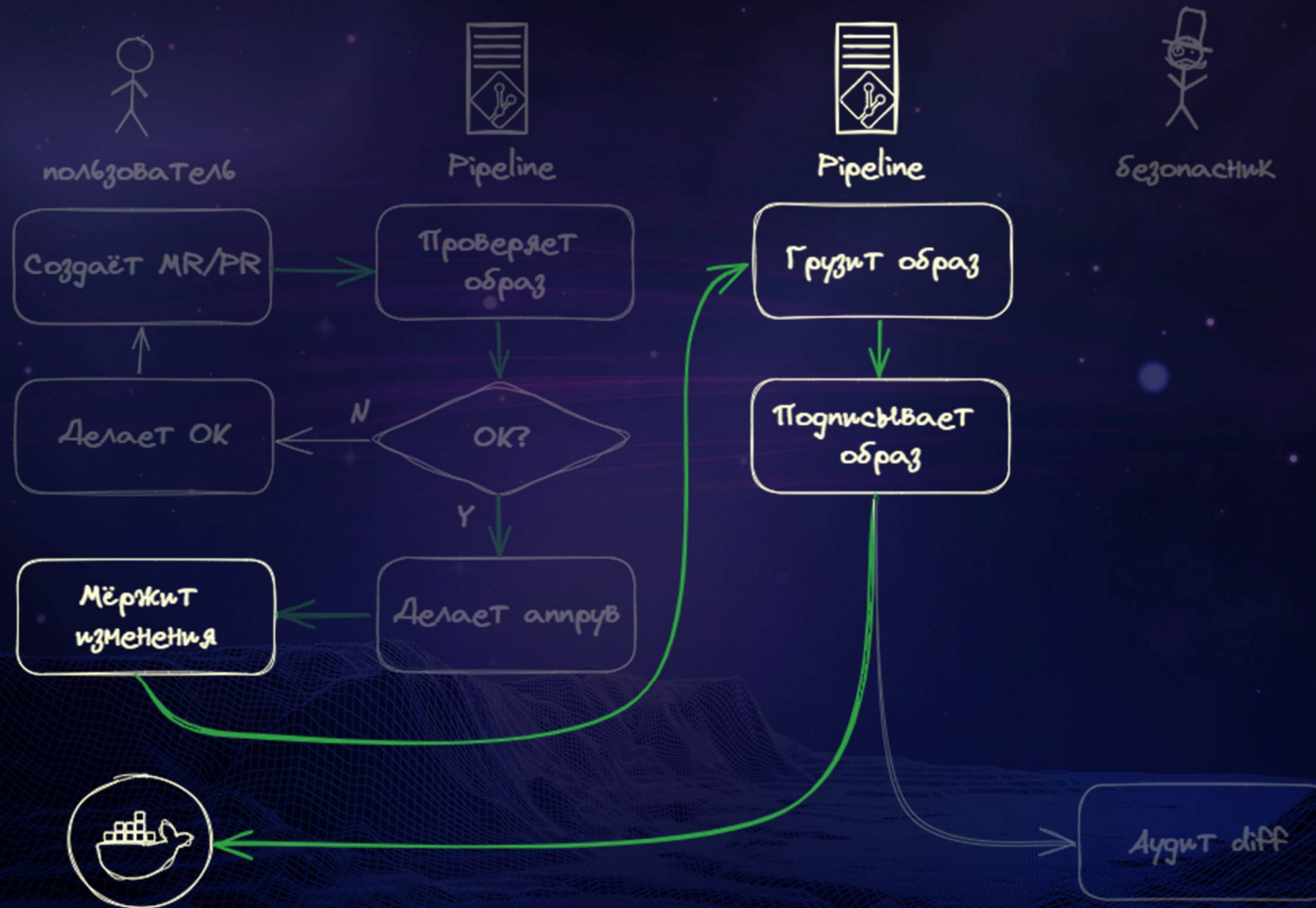


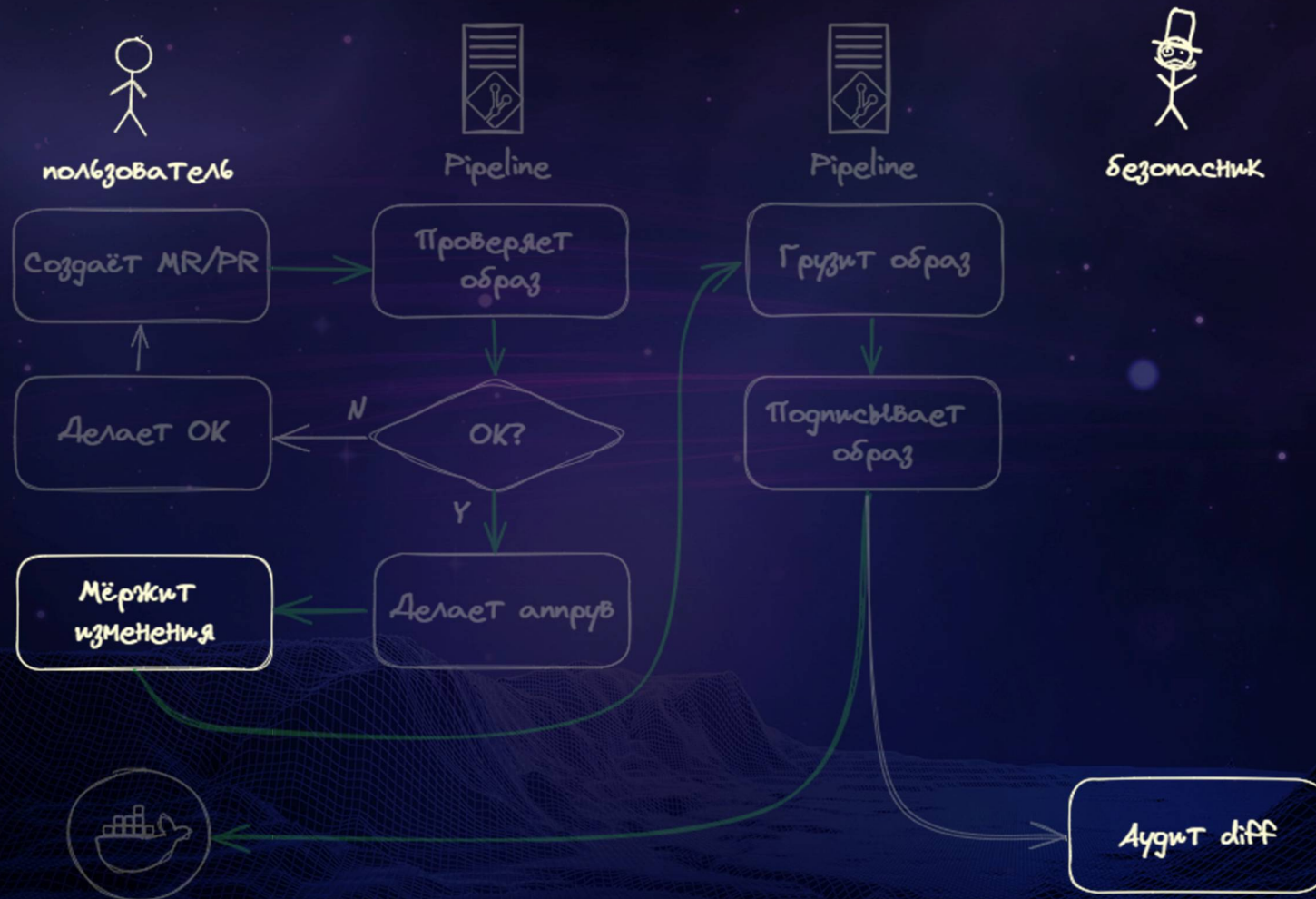
samokat.io

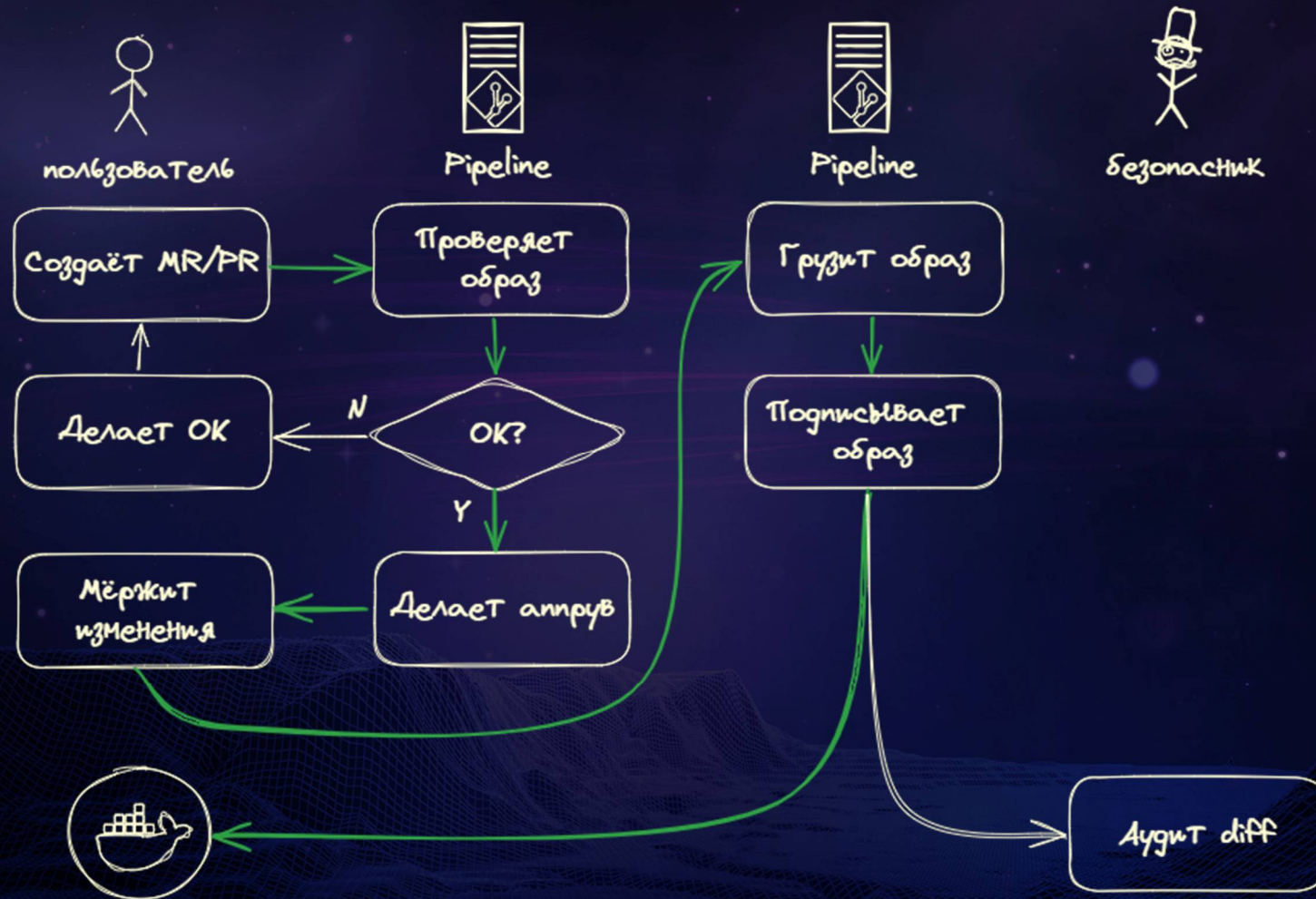


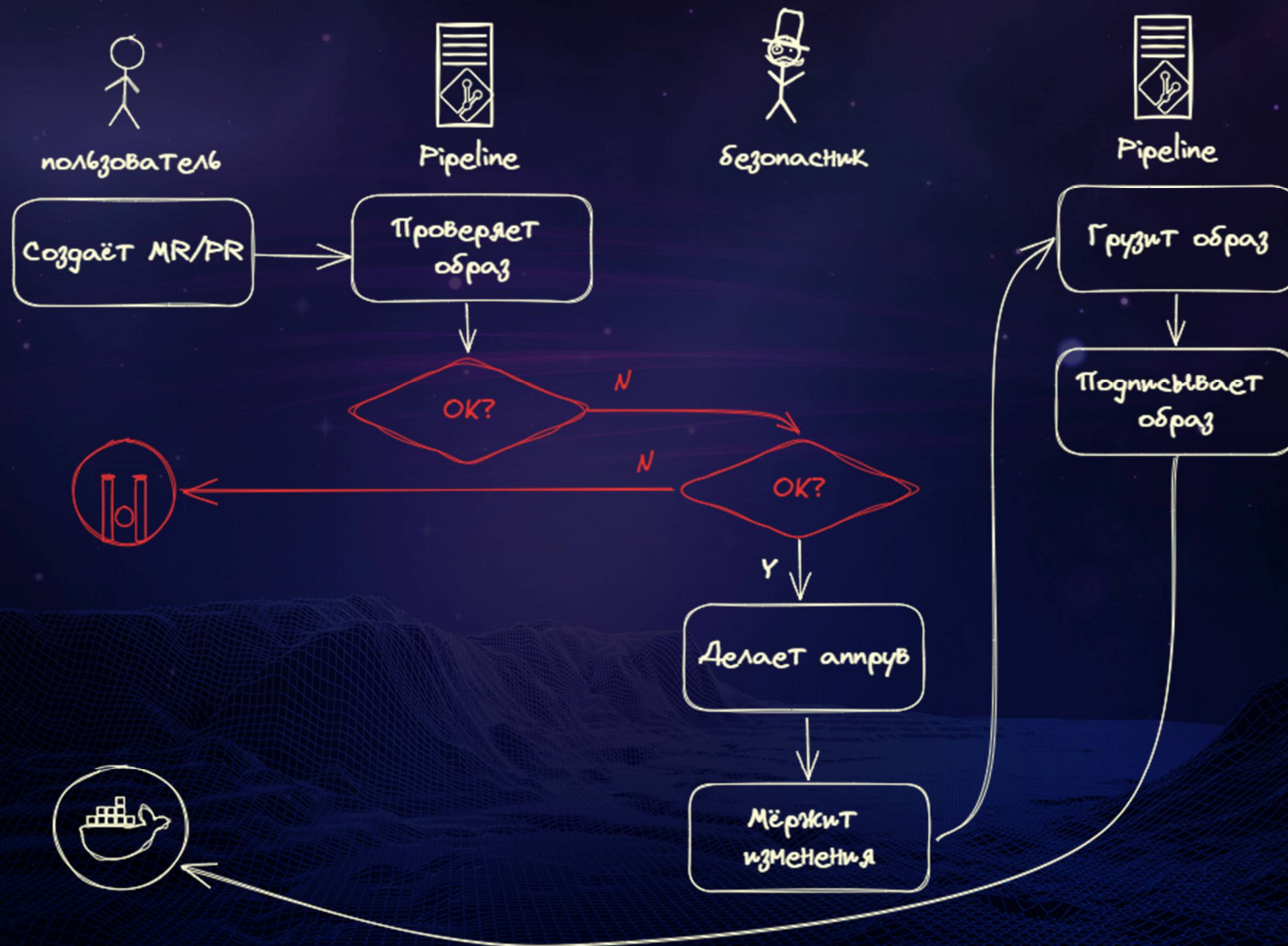












Что мы проверяем в публичных образах



Pipeline

Проверяет
образ

ЧТО МЫ ПРОВЕРЯЕМ В ПУБЛИЧНЫХ ОБРАЗАХ

БЕКОН

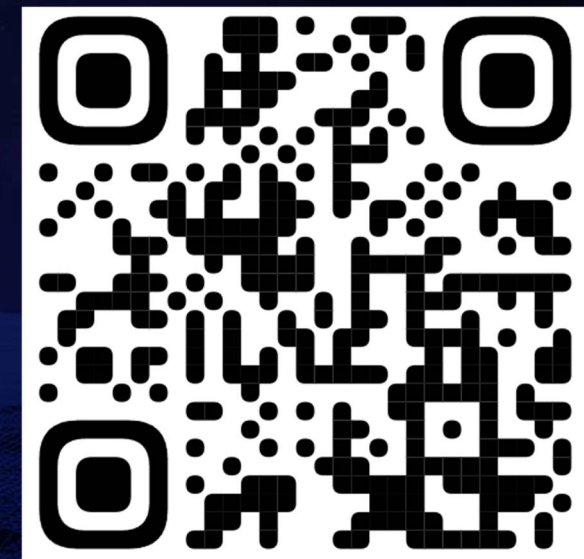
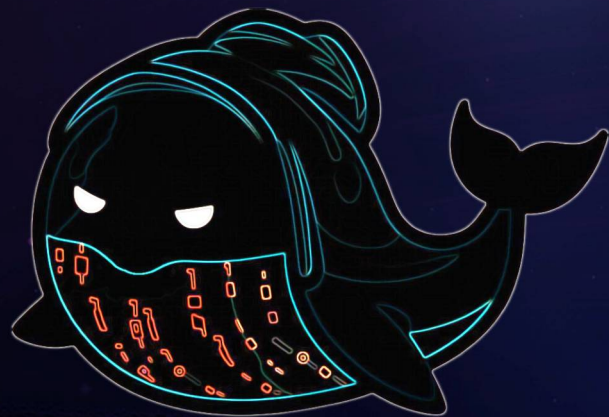
 Уязвимости

 Вредоносный код

 Мисконфигурация сборки

 Дата создания

 Тэг



<https://github.com/samokat-oss/pisc>

ЧТО МЫ ПРОВЕРЯЕМ В ПУБЛИЧНЫХ ОБРАЗАХ

БЕКОН

 Уязвимости – [CRITICAL | HIGH] + exploit

 Вредоносный код

 Мисконфигурация сборки

 Дата создания


 Тэг



ЧТО МЫ ПРОВЕРЯЕМ В ПУБЛИЧНЫХ ОБРАЗАХ

БЕКОН

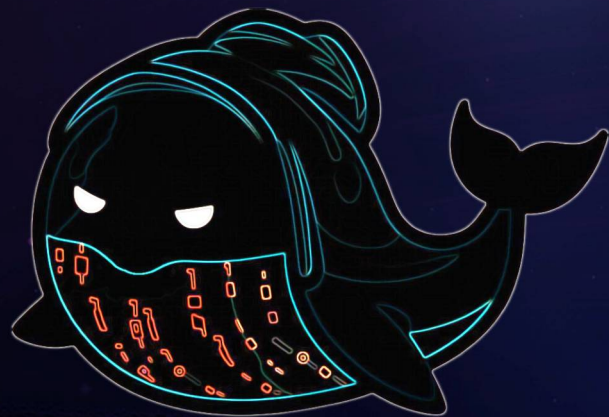
 Уязвимости

 Вредоносный код – о нём подробно

 Мисконфигурация сборки

 Дата создания

 Тэг



ЧТО МЫ ПРОВЕРЯЕМ В ПУБЛИЧНЫХ ОБРАЗАХ

БЕКОН

 Уязвимости

 Вредоносный код

 Мисконфигурация сборки – CVE-2024-21626

 Дата создания

 Тэг



ЧТО МЫ ПРОВЕРЯЕМ В ПУБЛИЧНЫХ ОБРАЗАХ

БЕКОН

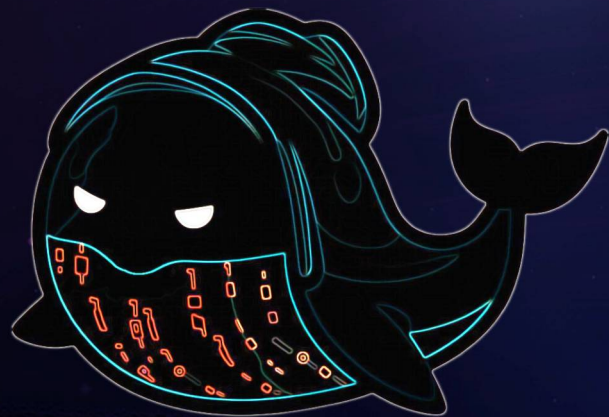
 Уязвимости

 Вредоносный код

 Мисконфигурация сборки

 Дата создания – 1 год

 Тэг



ЧТО МЫ ПРОВЕРЯЕМ В ПУБЛИЧНЫХ ОБРАЗАХ

БЕКОН



Уязвимости



Вредоносный код



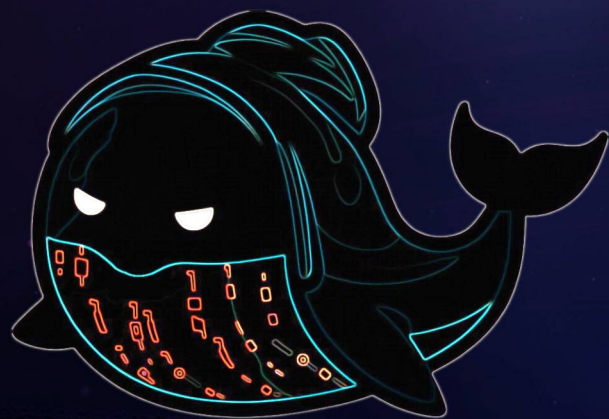
Мисконфигурация сборки



Дата создания



Тэг – latest и другие неверсионные




ЧТО МЫ ПРОВЕРЯЕМ В ПУБЛИЧНЫХ ОБРАЗАХ

БЕКОН

 Уязвимости

 Вредоносный код

 Мисконфигурация сборки

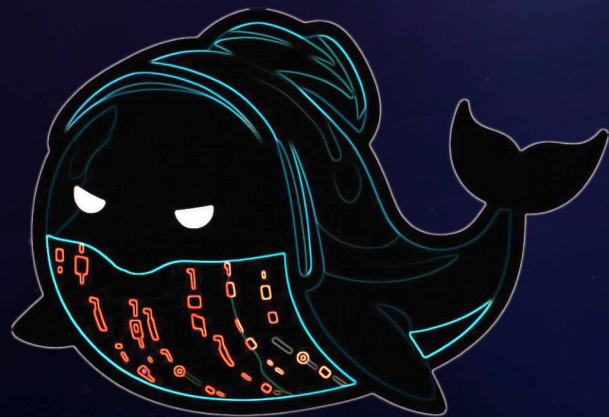
 Дата создания

 Тэг

Подпись вендора

Лицензионная политика

Секреты



Вредоносный код



Red-team tools



Crypto-miners



Backdoors



и их друзья...



Red-team tools

Crypto-miners

Backdoors

и их друзья...



30.05.2024



Red-team tools

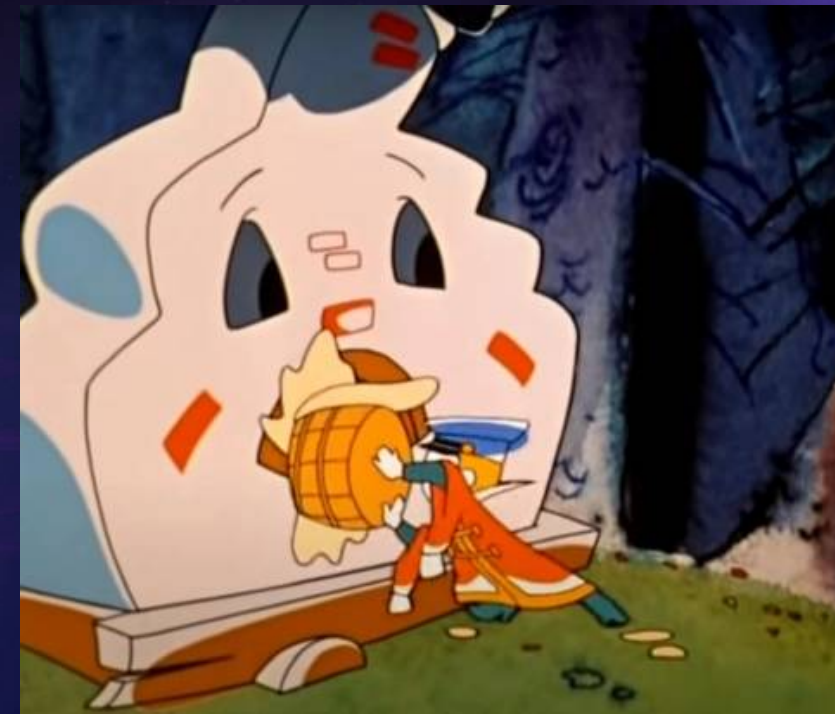
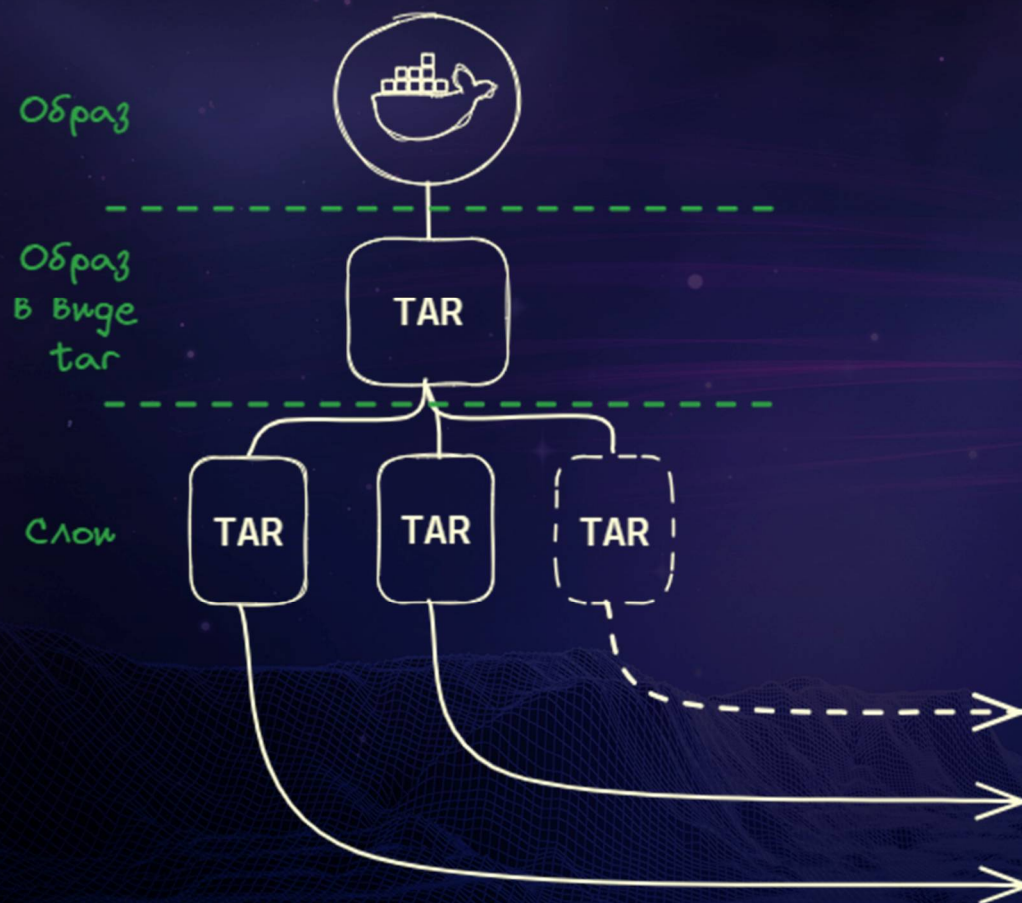
Crypto-miners

Backdoors

и их друзья...



Реализация





26ec0754f344acaa581e16a39a8794f9230f8842f40dab2fb96bdb57df212635

Имя tar-архива — это его хэш

26ec0754f344acaa581e16a39a8794f9230f8842f40dab2fb96bdb57df212635.tar

44eac47be777a3300076e9cddc9d8518799052446271a16c54c5359b92bc3371

VERSION

json

layer.tar -> ../5f70bf18a086007016e948b04aed3b82103a36bea41755b6cddfaf10ace3c6ef.tar

4b72a1836bb20caae1ca7eecd038582d145802a435cea0c707e906425136833.tar

4dd94982b60b34940233dba9ac9782fdf6bb340d74eaa9d2c7a24d39e1a971a1

VERSION

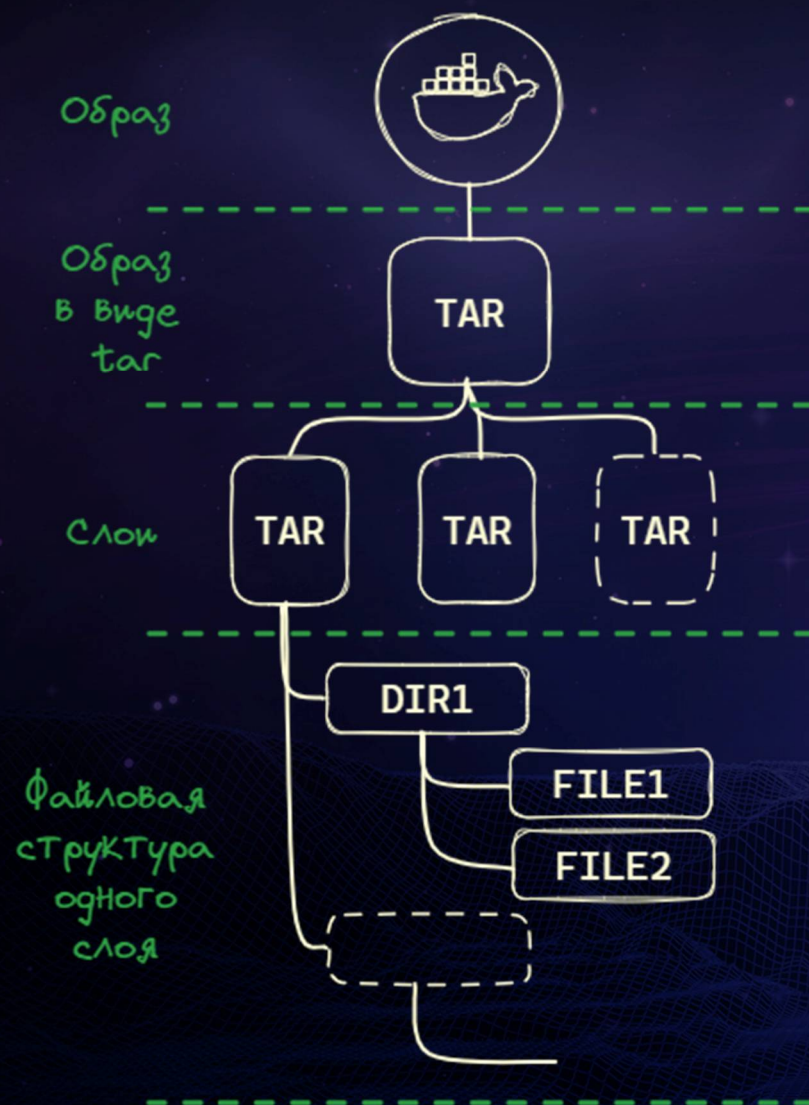
json

layer.tar -> ../e1b61a8823fa6238067134c15b11dd63eded5e3ba78cf13db850bbbb616b4120.tar

53df0e27263dd200f13e343e48b0c4ab2ae836f56af606c66ea4e93ca06a35cf

VERSION

json



`application/x-*` || `text/x-*`

```
usr/lib/x86_64-linux-gnu/security/pam_time.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_group.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_exec.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/libpamc.so.0.82.1: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_lastlog.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_succeed_if.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_stress.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_sepermit.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_filter.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_env.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/security/pam_access.so: application/x-sharedlib
usr/lib/x86_64-linux-gnu/libcom_err.so.2.1: application/x-sharedlib
usr/sbin/update-rc.d: text/x-perl
usr/sbin/dpkg-fsys-usrunmess: text/x-perl
usr/sbin/deluser: text/x-perl
usr/sbin/invoke-rc.d: text/x-shellscript
usr/lib/usrmerge/convert-usrmerge: text/x-perl
usr/lib/apt/apt.systemd.daily: text/x-shellscript
opt/bitnami/scripts/libos.sh: text/x-shellscript
usr/bin/libnetcfg: text/x-perl
usr/share/perl5/Debconf/ConfModule.pm: text/x-perl
opt/bitnami/scripts/libwebserver.sh: text/x-shellscript
usr/bin/corelist: text/x-perl
usr/bin/tzselect: text/x-shellscript
opt/bitnami/mongodb/bin/install_compass: text/x-script.python
usr/bin/migratepages: application/x-pie-executable
usr/bin/memhog: application/x-pie-executable
usr/bin/pod2man: text/x-perl
usr/bin/perl5.36-x86_64-linux-gnu: application/x-pie-executable
```


РЕАЛИЗАЦИЯ. БОЛЬШИЕ СЛОИ

БЕКОН

```
usr/lib/git-core/git-merge-resolve: text/x-shellscript
usr/lib/git-core/git-mergetool: text/x-shellscript
usr/lib/git-core/git-mergetool--lib: text/plain
usr/lib/git-core/git-quiltimport: text/x-shellscript
usr/lib/git-core/git-remote-http: application/x-pie-executable
usr/lib/git-core/git-request-pull: text/x-shellscript
usr/lib/git-core/git-sh-i18n: text/plain
usr/lib/git-core/git-sh-i18n--envsubst: application/x-pie-executable
usr/lib/git-core/git-sh-prompt: text/plain
usr/lib/git-core/git-sh-setup: text/plain
usr/lib/git-core/git-shell: application/x-pie-executable
usr/lib/git-core/git-submodule: text/x-shellscript
usr/lib/git-core/git-subtree: text/x-shellscript
usr/lib/git-core/git-web--browse: text/x-shellscript
usr/lib/git-core/mergetools/araxis: text/plain
```

берём
только
нужные
mime-Typle

Сортируем по размеру
и удаляем

175M	opt/bitnami/mongodb/bin/mongod
141M	opt/bitnami/mongodb/bin/mongosh
125M	opt/bitnami/mongodb/bin/mongos
16M	opt/bitnami/mongodb/bin/mongofiles
16M	opt/bitnami/mongodb/bin/mongorestore
16M	opt/bitnami/mongodb/bin/mongodump
16M	opt/bitnami/mongodb/bin/mongoimport
16M	opt/bitnami/mongodb/bin/mongoexport
16M	opt/bitnami/mongodb/bin/mongostat
15M	opt/bitnami/mongodb/bin/mongotop
14M	opt/bitnami/mongodb/bin/bsondump
9.4M	opt/bitnami/common/bin/yq
4.5M	usr/lib/x86_64-linux-gnu/libcrypto.so.3
3.7M	usr/lib/x86_64-linux-gnu/libperl.so.5.36.0
3.7M	usr/bin/perl5.36.0













Полтора спринта



Тестирование

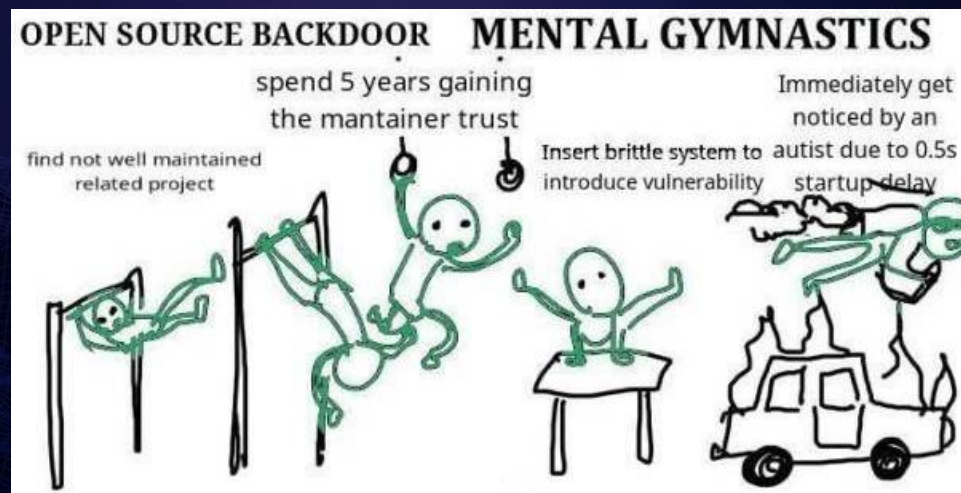
```
quay.io/petr_ruzicka/malware-cryptominer-container:2.0.2 >>> virustotal detected malicious file
layer:014773ab
https://www.virustotal.com/gui/file/014773ab466899811fdb762a477d6fff19cf233d1f2312bc8ca98b81f437f60b0
https://www.virustotal.com/gui/file/0b3e9e5e8f42eeab0832325ab0c850097609436940e61c1ccaae52b96fd4a9e7
usr/share/nginx/html/ILOVEYOU.vbs 48/61 🐛 worm.loveletter/scriptworm
usr/share/nginx/html/Invoke-ConPtyShell.ps1 22/62 🐛 hacktool.boxter/powershell
usr/share/nginx/html/L0Lz.bat 33/63 🐛 trojan.disabler/cdeject
usr/share/nginx/html/Linux.Trojan.Multiverze.elf.x86 42/61 🐛 trojan.gafgyt/mirai
usr/share/nginx/html/MadMan.exe 38/66 🐛 virus.madman
usr/share/nginx/html/Melissa.doc 56/62 🐛 virus.melissa/w97m
usr/share/nginx/html/Py.Trojan.NecroBot.py 33/64 🐛 trojan.python/necrobot
usr/share/nginx/html/TrojanSpy.MacOS.XCSSET.A 41/60 🐛 trojan.xcsset/xtesc
usr/share/nginx/html/Txt.Malware.Sustes.sh 35/58 💰 miner.zojfor/shell
usr/share/nginx/html/Unix.Downloader.Rocke.sh 36/58 💰 miner.zojfor/bash
usr/share/nginx/html/Unix.Malware.Kaiji.elf.arm 39/63 🐛 trojan.kaiji/ddos
usr/share/nginx/html/Unix.Trojan.Mirai.elf.m68k 40/58 🐛 trojan.mirai/bootnet
usr/share/nginx/html/Unix.Trojan.Mirai.elf.mips 44/60 🐛 trojan.mirai/gafgyt
usr/share/nginx/html/Unix.Trojan.Mirai.elf.ppc 45/60 🐛 trojan.gafgyt/mirai
usr/share/nginx/html/Unix.Trojan.Mirai.elf.sparc 40/58 🐛 trojan.mirai/gafgyt
usr/share/nginx/html/Unix.Trojan.Mirai.elf.x86_64 42/64 🐛 trojan.gafgyt/mirai
usr/share/nginx/html/Unix.Trojan.Spike.elf.arm 39/60 🐛 trojan.dofloo/rootkit
usr/share/nginx/html/Walker.com 42/63 🐛 virus.walker/abraxas
usr/share/nginx/html/WannaCry.exe 64/71 🐛 trojan.wannacryptor/wannacry
usr/share/nginx/html/Win.Trojan.Perl.perl 36/60 🐛 Malware.Generic-Script.Save.169b6505
usr/share/nginx/html/Zloader.xlsm 42/66 🐛 trojan.esls/w97m
usr/share/nginx/html/eicar/eicar.com.txt 66/71 🐛 virus.eicar/test
usr/share/nginx/html/eicar/eicarcom2.zip 57/69 🐛 virus.eicar/test
usr/share/nginx/html/xmrig/xmrig 43/65 💰 miner.qsqvz/r002c0pk322
usr/share/nginx/html/xmrig/xmrig-linux-static-x64.tar.gz 38/61 💰 miner.xmrig
```













```
 r0binak/mtkpi:v1.3 >>> detected dangerous misconfiguration
malicious-compliance - UPX detected
https://github.com/bgeesaman/malicious-compliance/blob/main/docker/Dockerfile-4-bin
 r0binak/mtkpi:v1.3 >>> virustotal detected malicious file
layer:26ec0754
https://www.virustotal.com/gui/file/26ec0754f344acaa581e16a39a8794f9230f8842f40dab2f
https://www.virustotal.com/gui/file/796c3bedb5c32e2330a96f34bc4f454ad8df48d202f3a2a1
cdk_linux_amd64 35/67  hacktool.multiverze/qkmmh
run/dnscat2/client/dnscat 35/67  trojan.dnscat/dnscat2
run/dnscat2/client/dnscat.o 7/63  dnscat/rioia
usr/local/bin/botb 35/67  trojan.brothbo/botb
usr/local/bin/cdk 35/67  hacktool.multiverze/qkmmh
usr/local/bin/ctrsploit 26/63  trojan.nvufh
usr/local/bin/ddexec.sh 4/64  trojan.expl/shellcode-loader
usr/local/bin/deepce.sh 4/63  hacktool.deepce/shell
usr/local/bin/kubesploit 25/63  trojan.kubesploit/malsource
usr/local/bin/linuxprivchecker.py 3/61  hacktool.empire/python
usr/local/bin/peirates 27/67  hacktool.pirat/ckyp1
usr/local/bin/traitor 37/67  hacktool.traitor/pgmep
```



```
r0binak/xzk8s:v1.1 >>> virustotal detected malicious file  
layer:0f28dfef  
https://www.virustotal.com/gui/file/0f28dfefbf3451ccfe3d5b11d17bc38cc8d1c4  
https://www.virustotal.com/gui/file/dc24581c3500b9640e03c7a4c14cd7c22f88c5  
layer:230cc513  
https://www.virustotal.com/gui/file/230cc513debf36c5294ba6dd2babd27934bb23  
https://www.virustotal.com/gui/file/935cfccfa8d31d0e03f2162e9b46b7f9df77d1  
root/liblzma.so.5.6.0.patch 33/67 🧑 trojan.xzbackdoor/cve20243094
```




```
ghcr.io/lpsm-dev/docker-crypto-miner:main >>> virustotal detected malicious file
layer:20340239
https://www.virustotal.com/gui/file/203402396117d40397806826aabab6c1c1ed3e4f9cc81
layer:34b05fc1
https://www.virustotal.com/gui/file/34b05fc1a9a96dfa0c3f90653247f79df2fdfaf9bb1f1
layer:95b9abf1
https://www.virustotal.com/gui/file/95b9abf16945cd3a63221324e2a9c0865c80c113a9fb1
https://www.virustotal.com/gui/file/6754d15910e1ea558316208c54342c0814c5e502730e1
bin/xmrig 37/67  miner.malxmr/smdsl64
```

```
awan/sugar-chain-crypto-miner:1.0.1 >>> virustotal detected malicious file
layer:6c36605e
https://www.virustotal.com/gui/file/6c36605e031cb51e92c0b3c16b63249361863b91e0966252fb40da4de46c6b0d
https://www.virustotal.com/gui/file/039f3c8d2882e9fc0a959e33fcb610f8261e5ea42c49b39cdefdbdb14557d8c0
layer:74557569
https://www.virustotal.com/gui/file/74557569755e49c02ef38d53856a01b02513c5e0ccb86f8ce038cb071ab6ace0
https://www.virustotal.com/gui/file/a7906e9b910221bb8d2d74c7c366aa1e4934c17595b640b16af78095d066df75
usr/local/bin/cpuminer 32/67  miner.camelot
layer:841ecab1
https://www.virustotal.com/gui/file/841ecab1fd6b2b45feca5a5254fd6a9bb47f8a059927debdb40e4a292a33ba5f
https://www.virustotal.com/gui/file/80bc0b7d71bfa0dd5986565de9527c4101d58c57c3a92e58c5aecacaa2bec8bc
cpuminer 32/67  miner.camelot
cpuminer-cpu-miner.o 9/65  miner.
cpuminer-lbry-gate.o 1/67  Tool.Linux.BtcMine.9999
cpuminer-opt-sugarchain/algo/blake/cpuminer-blake2b.o 1/65  Tool.Linux.BtcMine.9999
cpuminer-opt-sugarchain/algo/blake/cpuminer-decred-gate.o 1/66  Tool.Linux.BtcMine.9999
cpuminer-opt-sugarchain/algo/blake/cpuminer-sph_blake2b.o 1/67  Linux.Cryptominer.Camelot
cpuminer-opt-sugarchain/algo/hodl/cpuminer-hodl-gate.o 1/67  Tool.Linux.BtcMine.9999
cpuminer-sha2-x64.o 3/59  Malware.Generic-Script.Save.8
```



```

kasmweb/kali-rolling-desktop:1.13.1 >>> virustotal detected malicious file
layer:5c9c12eb
  https://www.virustotal.com/gui/file/5c9c12eb62adfc3ebb3357dc1988f68879f1a53d9fbf90a2c04152c0f9401ea3
layer:6080005d
  https://www.virustotal.com/gui/file/6080005d3a64dc16ee2e49222cd8f5e4a2fa18101160f0d4df3514236c4ee0bd
  https://www.virustotal.com/gui/file/cf8bd3f54b2b15d96373a46ca1c04acad8104c10d76458a7b3bf4134ef0074dd
layer:630fbc90
  https://www.virustotal.com/gui/file/630fbc90947eb3d8ee3594ba423c8cacefc0cc30e71af7e612a223a3f396e335
  https://www.virustotal.com/gui/file/d2fdc91d7b94ffd5562a99396b654d87f513068dfe154f2f60e8c8688761c99e
layer:89601e5e
  https://www.virustotal.com/gui/file/89601e5ec5a03b8b59968a7e713419620d8cccf6600cefa4e847a9c6cf676434
  ..asploit_payloads-mettle-1.0.20/build/aarch64-iphone-darwin/bin/sniffer 17/47 🦋 trojan.koiot/mettle
  ..etasploit_payloads-2.0.130/data/meterpreter/ext_server_sniffer.x64.dll 48/71 🦋 hacktool.meterpreter/hacktoolx
  ..etasploit_payloads-2.0.130/data/meterpreter/ext_server_sniffer.x86.dll 51/71 🦋 trojan.meterpreter/zenpak
  ..etasploit_payloads-mettle-1.0.20/build/x86_64-apple-darwin/bin/sniffer 30/65 🦋 trojan.koiot/mettle
  ..loit_payloads-2.0.130/data/meterpreter/ext_server_stdapi.x86.debug.dll 55/72 🦋 trojan.meterpreter/cerbu
  ..metasploit_payloads-2.0.130/data/meterpreter/ext_server_stdapi.x64.dll 54/74 🦋 trojan.meterpreter/beacon
  ..metasploit_payloads-2.0.130/data/meterpreter/ext_server_stdapi.x86.dll 56/71 🦋 trojan.meterpreter/beacon
  usr/share/metasploit-framework/data/post/bypassuac-x86.exe 56/73 🦋 trojan.uacskip/component
  usr/share/metasploit-framework/data/vncdll.x86.dll 61/74 🦋 trojan.diple/metasploit

```


Нюансы



Время анализа –
от 1 до 10 минут на слой



НЮАНСЫ. А ГДЕ ФАЙЛ?

БЕКОН

The screenshot shows the VirusTotal analysis page for a file. The file's SHA-256 hash is 0f28dfebbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3, and the filename is 0f28dfebbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3.tar. The file size is 120.70 MB, and it was last modified 1 month ago. The analysis shows that 19 out of 56 security vendors flagged the file as malicious. The file is categorized as a trojan, exploit, and cve-2024-3094. The file is also labeled as trojan.xzbackdoor, trojan, and xzbackdoor. The security vendors' analysis shows that AhnLab-V3, Arcabit, and Trojan.Linux.XZBackdoor.W have flagged the file as malicious.

19 / 56

19/56 security vendors and no sandboxes flagged this file as malicious

Reanalyze

0f28dfebbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3

0f28dfebbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3.tar

Size: 120.70 MB

Last Modified: 1 month ago

tar exploit cve-2024-3094

Community Score

DETECTION DETAILS COMMUNITY

RELATIONS нет

Popular threat label: trojan.xzbackdoor

Threat categories: trojan

Family labels: xzbackdoor

Security vendors' analysis

AhnLab-V3: Backdoor/Linux.Generic.247800

Arcabit

Trojan.Linux.XZBackdoor.W

Handwritten annotations: "это слой" (this is a layer) with an arrow pointing to the file hash, and "RELATIONS нет" (no relations) with an arrow pointing to the COMMUNITY tab.

НЮАНСЫ. А ГДЕ ФАЙЛ?

БЕКОН

The screenshot shows the VirusTotal analysis page for a file. At the top left, a circular progress indicator shows 19/56 vendors. A message states: "19/56 security vendors and no sandboxes flagged this file as malicious". The file hash is 0f28dfefbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3, and the filename is 0f28dfefbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3.tar. The file size is 120.70 MB, and it was last modified 1 month ago. The file is categorized as 'trojan' and 'cve-2024-3094'. The 'COMMUNITY' tab is selected, showing a 'Popular threat label' of 'trojan.xzbackdoor', 'Threat categories' of 'trojan', and 'Family labels' of 'xzbackdoor'. The 'Security vendors' analysis' section shows results from AhnLab-V3, Arcabit, and Trojan.Linux.XZBackdoor.W. Handwritten annotations include: "это слой" with an arrow pointing to the file hash; "RELATIONS нет" with an arrow pointing to the 'COMMUNITY' tab; and a large arrow pointing from the 'Trojan.Linux.XZBackdoor.W' entry to the right-hand text.

19/56 security vendors and no sandboxes flagged this file as malicious

0f28dfefbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3

0f28dfefbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3.tar

Size: 120.70 MB

Last Modified: 1 month ago

tar exploit cve-2024-3094

DETECTION DETAILS **COMMUNITY**

Popular threat label: trojan.xzbackdoor

Threat categories: trojan

Family labels: xzbackdoor

Security vendors' analysis

Vendor	Threat Name	Category
AhnLab-V3	Backdoor/Linux.Generic.247800	Arcabit
Trojan.Linux.XZBackdoor.W		

Оставляем
только
нужные mime-
типы,
отправляем
ещё раз

НЮАНСЫ. А ГДЕ ФАЙЛ?

БЕКОН

19 / 56

Community Score

19/56 security vendors and no sandboxes flagged this file as malicious

Reanalyze

0f28dfebbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3

0f28dfebbf3451ccfe3d5b11d17bc38cc8d1c4e721b842969466dc7989d835e3.tar

Size 120.70 MB

Last Modified 1 month ago

tar exploit cve-2024-3094

DETECTION

DETAILS

COMMUNITY

Popular threat label trojan.xzbackdoor

Threat categories trojan

Family labels xzbackdoor

Security vendors' analysis

Do you

AhnLab-V3

Backdoor/Linux.Generic.247800

Arcabit

Trojan.Linux.XZBackdoor.W

это слой

RELATIONS нет

Оставляем только нужные mime-типы, отправляем ещё раз

Если повезёт, увидим RELATIONS и путь к файлу

DETECTION	DETAILS	RELATIONS	COMMUNITY
Bundled Files (1)			
Scanned	Detections	File type	Name
2024-05-19	33 / 67	ELF	root/liblzma.so.5.6.0.patch
SHA-256	fbfddd1e77b684e9d2d18017ae658b24402727551447f41db0ab882d4a0cac81		
Date Bundled	2024-04-16 20:45:44		
File Size	241.99 KB		

Публичная почта

Access level

Usage

Request rate

Daily quota

Monthly quota

⚠ **Limited**, standard free public API

Must not be used in business workflows, commercial products or services.

1 lookups / min

1 lookups / day

31 lookups / month

Upgrade to premium



Корпоративная почта (x N)

Access level

Usage

Request rate

Daily quota

Monthly quota

⚠ **Limited**, standard free public API


Must not be used in business workflows, commercial products or services.

4 lookups / min

500 lookups / day

15.5 K lookups / month

Upgrade to premium





Bypass

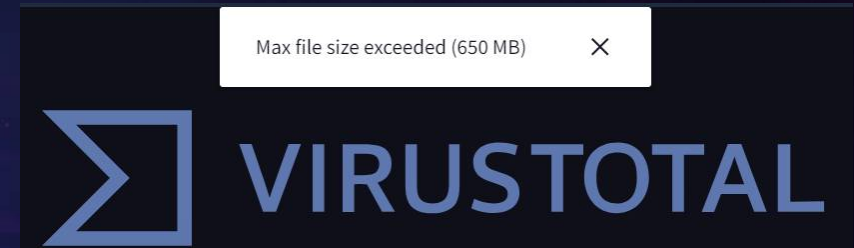


Файл/слой большого размера

Зашифрованный архив/модуль

Загрузка модулей в рантайм

Преднамеренная мисконфигурация приложений



Файл/слой большого размера

Зашифрованный архив/модуль

Загрузка модулей в рантайм

Преднамеренная мисконфигурация приложений



Fun with container images

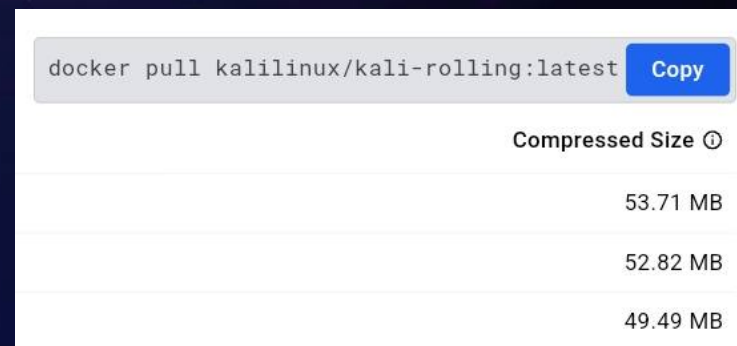


Файл/слой большого размера

Зашифрованный архив/модуль

Загрузка модулей в рантайм

Преднамеренная мисконфигурация приложений



```
docker pull kalilinux/kali-rolling:latest
```

Compressed Size ⓘ
53.71 MB
52.82 MB
49.49 MB

Файл/слой большого размера

Зашифрованный архив/модуль

Загрузка модулей в рантайм

Преднамеренная мисконфигурация приложений

```
FROM alpine:3.19.1
RUN apk add --no-cache openssh && ssh-keygen -A

ENV USERNAME="root"
ENV PASSWORD="root"

ENTRYPOINT ["sh", "-c"]
CMD ["echo ${USERNAME}:${PASSWORD} | chpasswd && /usr/sbin/sshd -D"]
```

Детектим поведение

~~Файл/слой большого размера~~

~~Зашифрованный архив/модуль~~

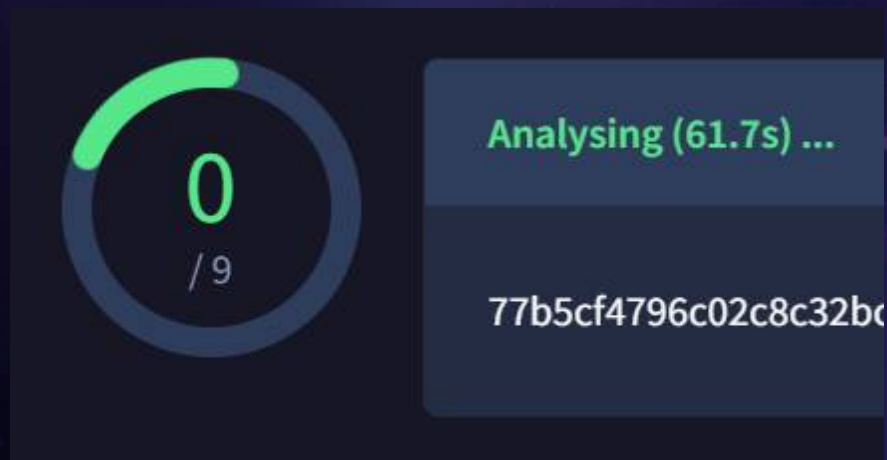
~~Загрузка модулей в рантайм~~

~~Преднамеренная мисконфигурация приложений~~



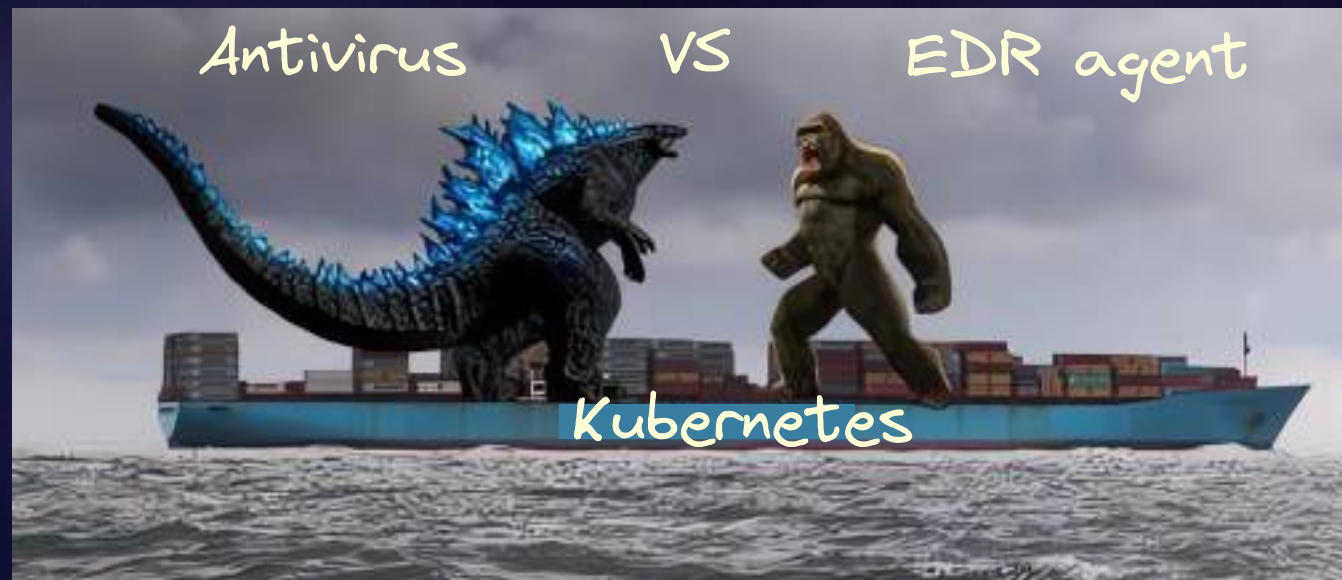
Результаты эксплуатации

В ожидании
malware в образе



В нашем случае:
true positive - 0
false positive ~ 10%





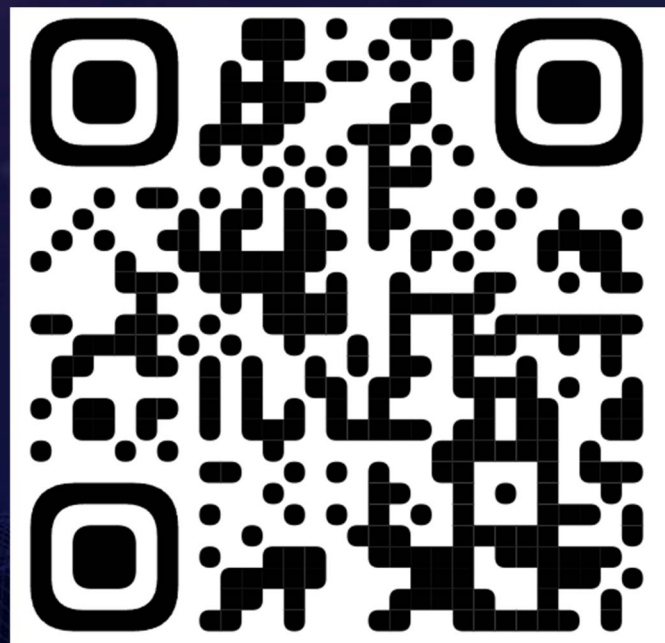
Есть вероятность false positive
Высокая утилизация ресурсов
Не cloud-native решение

- Антивирусную проверку образов лучше выносить наружу
- Можно взять историю as-is чтобы обогатить процессы
- virustotal «не любит» архивы, есть нюансы
- Не только virustotal, допиливайте под on-premise, если есть возможность
- Нулевая статистика (пока) в нашем случае - это только наш случай

ПОЛЬЗУЙТЕСЬ

БЕКОН

<https://github.com/samokat-oss/pisc>



tg: @kapistka