



Digital Security
Progress. Protected.

Slnko, seno, ransomware?

...alebo aké facky lietajú na ransomware scéne

Ondrej Kubovič

Špecialista na digitálnu bezpečnosť

(eset):research



+15%

Publikovaných útokov

5,100



-35%

Objem platieb

\$813 miliónov



+43%

Počet operátorov

96



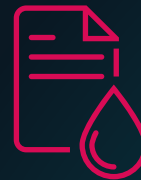
EDR killery

Prudký nárast



RMM nástroje

Zneužívanie



Krádež dát

...aj bez šifrovaniaa

Operácie proti ransomwaru

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in
with the FBI and the international law enforcement task force, 'Operation Claret'

We can confirm that Lockbit's
services have been disrupted as a
result of International Law
Enforcement action – this is an
ongoing and developing
operation.

Return here for more
information at:

11:30 GMT on Tuesday 20th
Feb.



THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law
enforcement action taken against ALPHV Blackcat Ransomware



This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property
Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program.
Information can be submitted through the following Tor-based tip line: <https://bit.ly/3xvz8d8> (Tor browser required).

Operácie proti ransomwaru



Operátor zľahčuje dopady

Strata dôvery u partnerov

Na hranici prežitia

Pokúša sa o návrat s verziou 4.0



Operátor zľahčuje dopady

Strata dôvery u partnerov

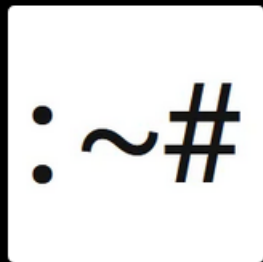
Vzdáva sa bez boja

Rebranding

Počet obetí podľa leak stránky


LOCKBIT 3.0



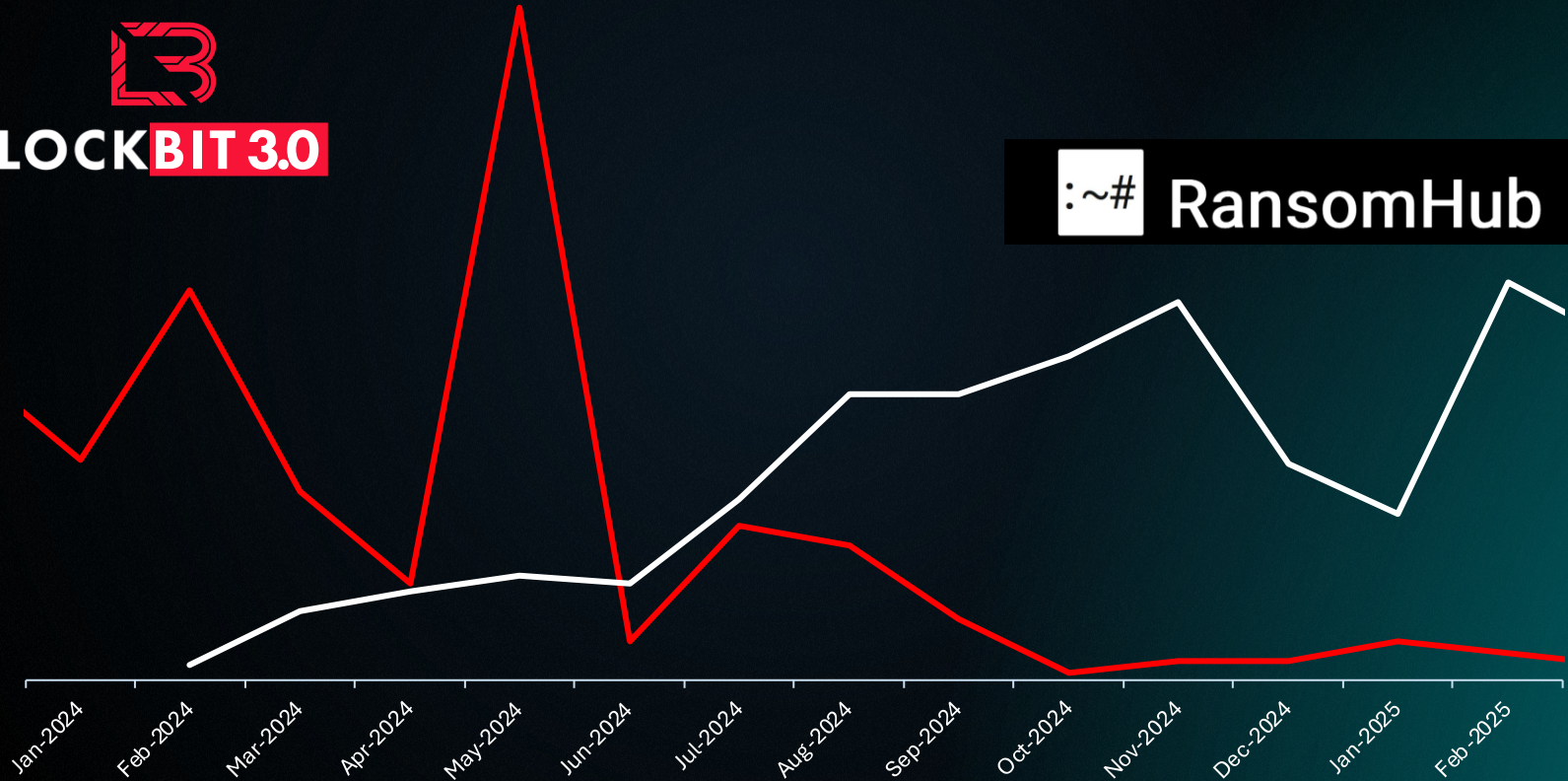


RansomHub

Počet obetí podľa leak stránky


LOCKBIT 3.0

 RansomHub





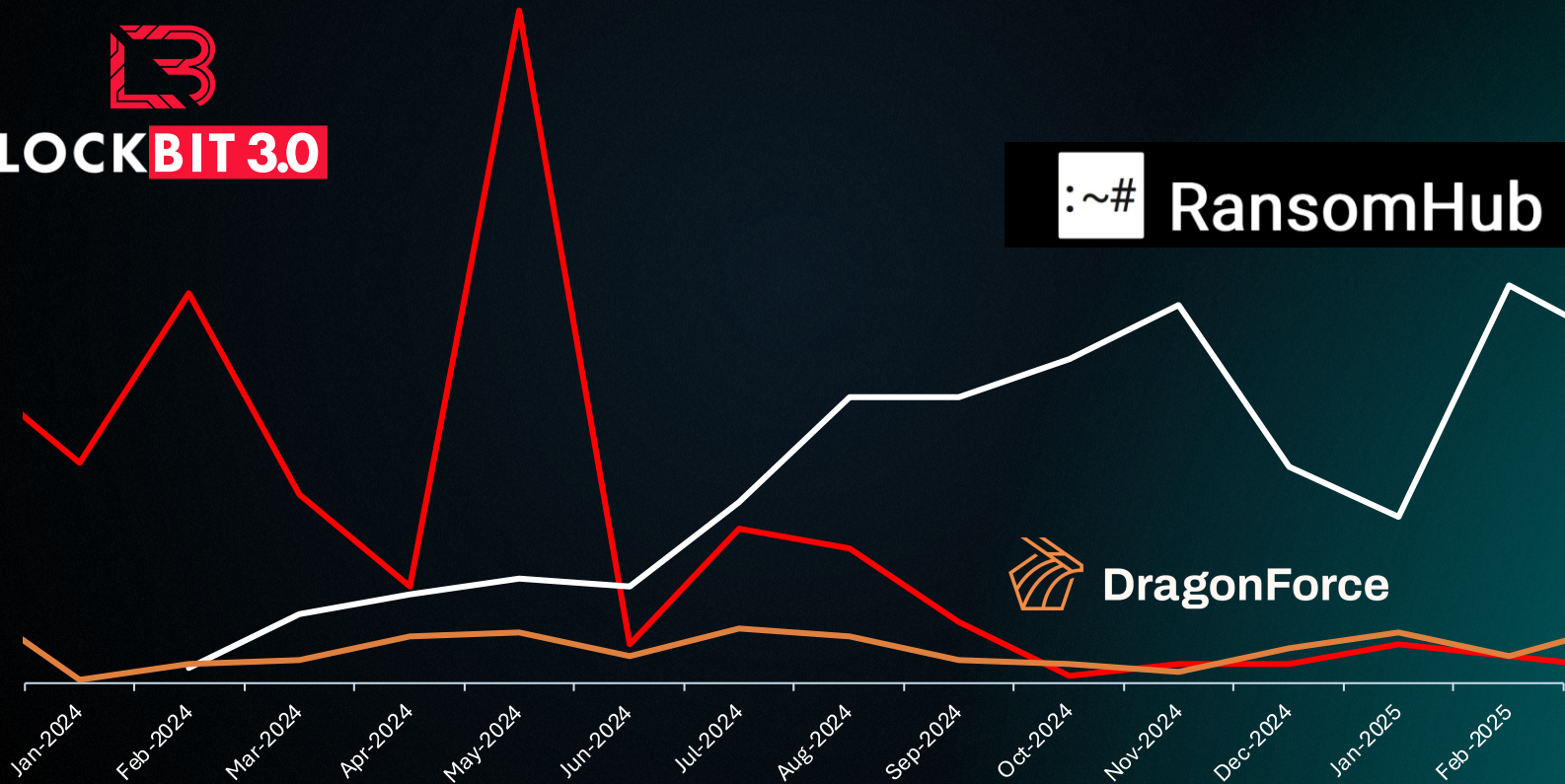
DragonForce

Počet obetí podľa leak stránky


LOCKBIT 3.0

 RansomHub

 DragonForce





DragonForce

DragonForce - work without paranoia

[z3wqggtxft7id3ibr7srivv5gjo5fwg76slwnzwwakjuf3nlhukdid.onion](#)

/etc/passwd

.env (0h-no...)

Chat dump

It is not good...

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
clevis:x:997:993:Clevis Decryption Framework unprivileged user:/
var/cache/clevis:/sbin/nologin
unbound:x:996:992:Unbound DNS resolver:/etc/unbound:/sbin/
nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/
run/lsm:/sbin/nologin
dnsmasq:x:990:990:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/
sbin/nologin
cockpit-ws:x:989:989:User for cockpit web service:/nonexisting:/
```



dragonforce

Feb 18, 2024

Messages 13

Reaction score 4

Points 3



DragonForce

&

RansomHub

Hi. Don't worry **RansomHub** will be up soon, they just decided to move to our infrastructure! We are reliable partners. A good example of how "**projects**" work, a new option from The **DragonForce** Ransomware Cartel!

- RansomHub / Blog: [REDACTED]
- RansomHub / Client: [REDACTED]

Spoiler: Settings,

P.S. RansomHub hope you are doing well, consider our offer! We are waiting for everyone in our ranks.

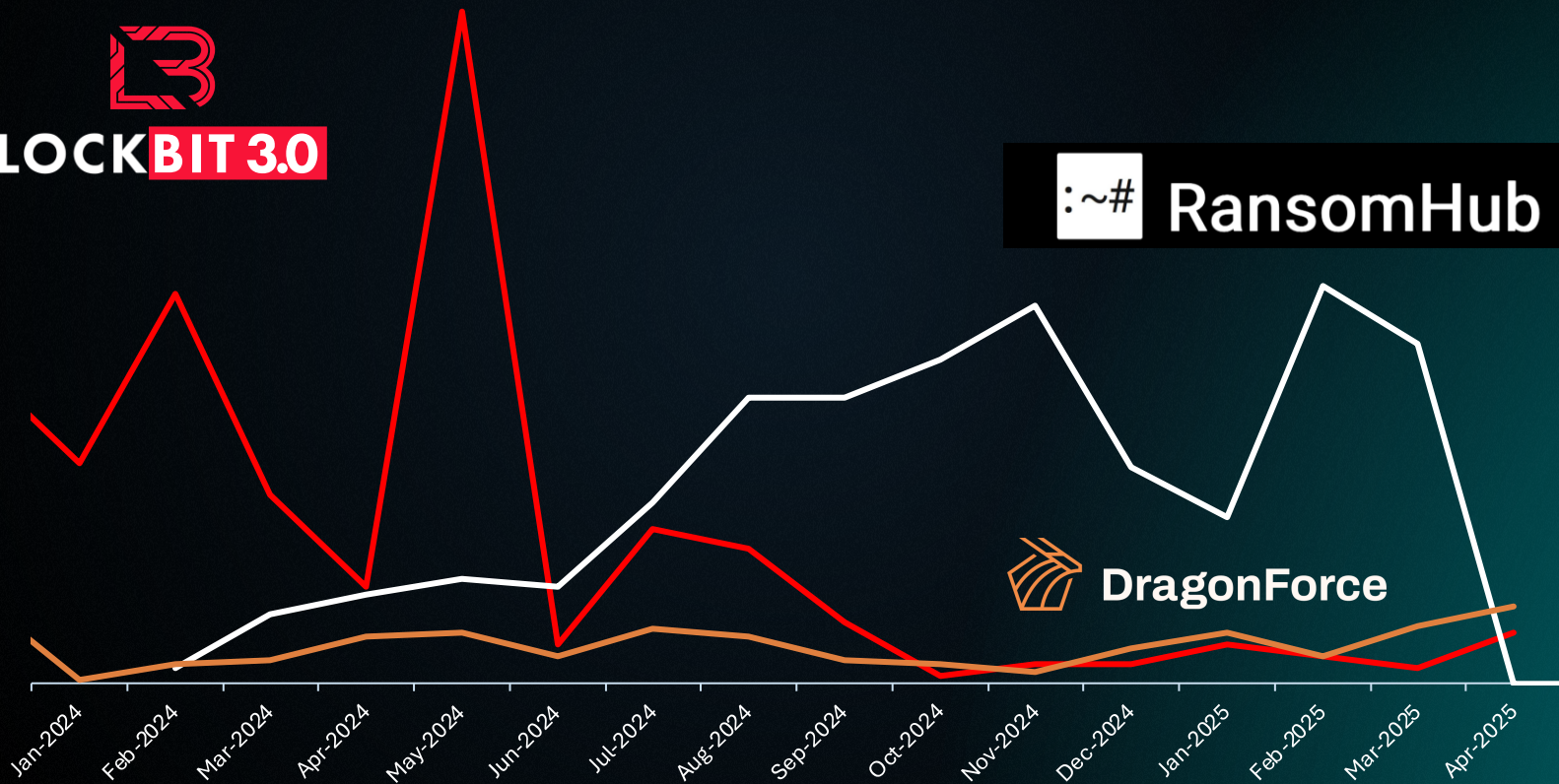
Zdroj: Sophos

Počet obetí podľa leak stránky


LOCKBIT 3.0

 RansomHub

 DragonForce



Čo si zapamätať?

1. Ransomware gangy útočia už aj na konkurenciu
2. Takedowny sú účinný spôsob boja a majú citeľný dopad
3. Ransomware neodchádza, naopak stáva sa nebezpečnejším
4. Dodržiavať pravidlá bezpečnosti:
 - Aktualizovať
 - Vzdelávať
 - Chrániť kvalitnými riešeniami (endpoint, aj EDR)

Ďakujem!

