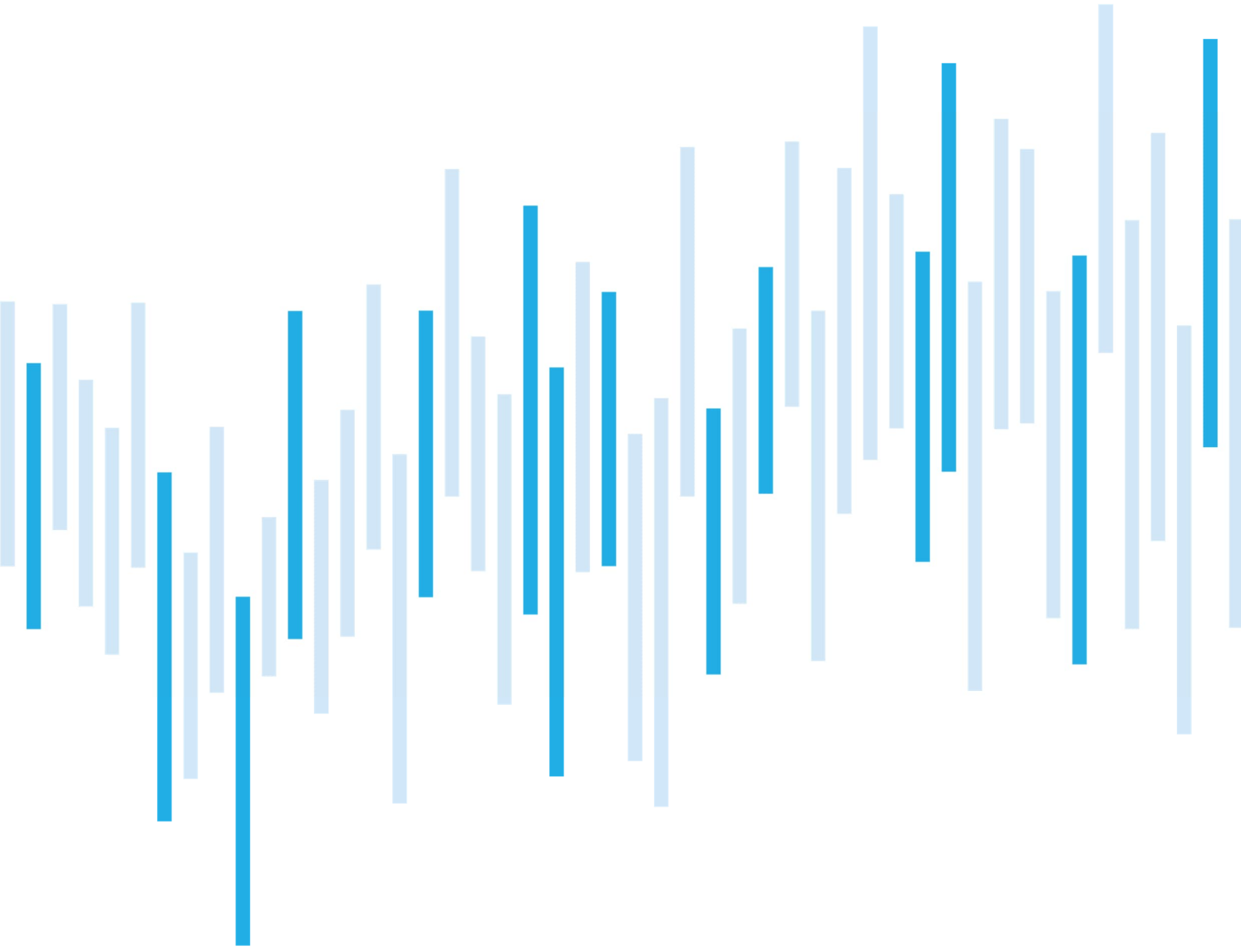
# Kybernetické incidenty pohledem NÚKIB

## ÚNOR 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

## Shrnutí měsíce

V únoru byl evidován totožný počet incidentů jako uplynulý měsíc. Jednalo se tak o čtvrtý měsíc v řadě s podprůměrnými hodnotami. Poprvé po třech měsících byl registrován významný kybernetický incident. Zbylých 17 incidentů pak spadalo do kategorie méně významných.

Dlouhodobý trend dominance incidentů spojených s dostupností přetrvával také v únoru. Evidovány byly také incidenty z kategorií Průnik a Informační bezpečnost.

V kapitole Zaměřeno na hrozbu se tentokrát věnujeme policejnímu zásahu vůči infrastruktuře ransomwarového gangu LockBit. Tento zásah lze považovat za jednu z největších akcí svého druhu. LockBit patřil mezi nejaktivnější kyberkriminální aktéry, přičemž od roku 2020 napadl více než 2000 obětí po celém světě. Bezpečnostní složky v rámci operace získaly kontrolu nad infrastrukturou, daty a dalšími informacemi ransomwarového gangu. V rámci operace byl získán také dekryptor k ransomwaru LockBit 3.0.

## Obsah

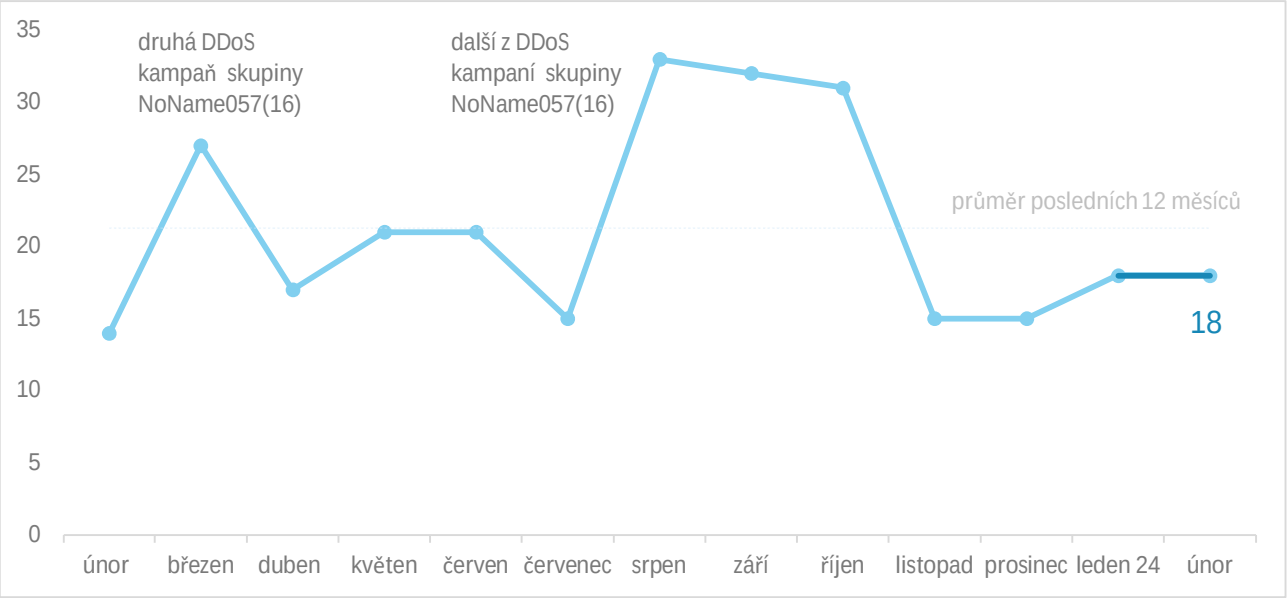


Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.cz.

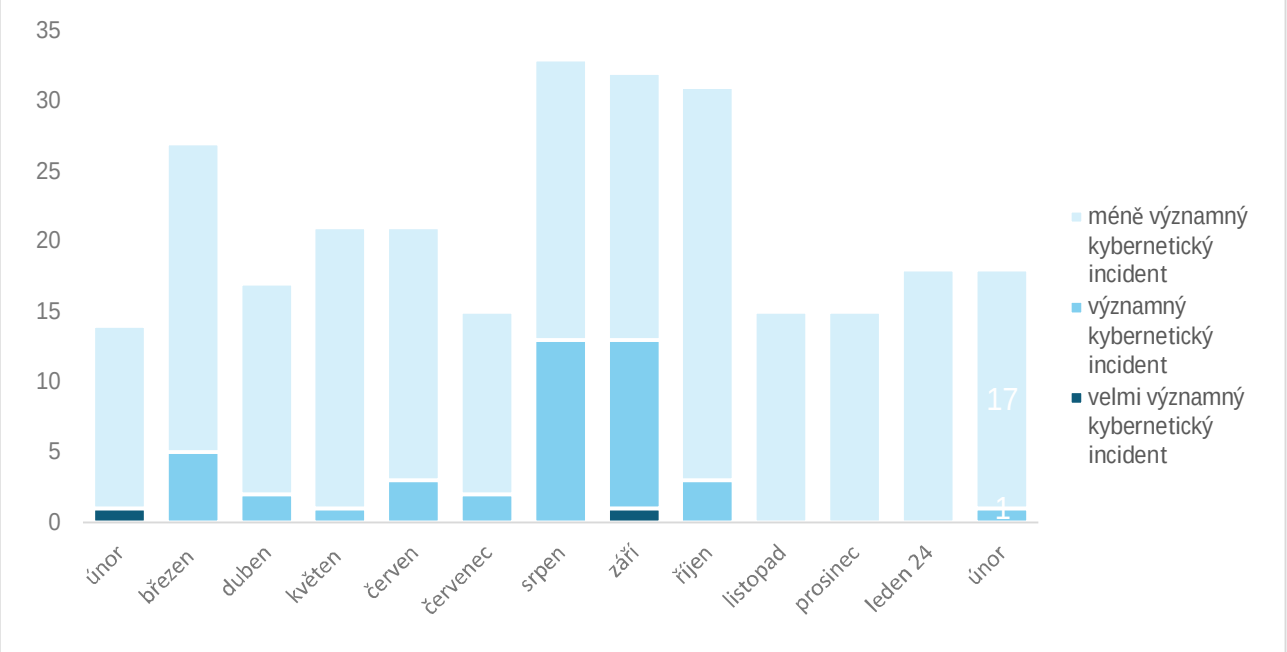
## Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB[1]

V únoru byl evidován totožný počet incidentů jako uplynulý měsíc. Jednalo se tak o čtvrtý měsíc v řadě s podprůměrnými hodnotami.




## Závažnost řešených kybernetických incidentů[2]

V průběhu února byl poprvé po třech měsících registrován významný kybernetický incident. Zbylých 17 incidentů pak spadalo do kategorie méně významných.



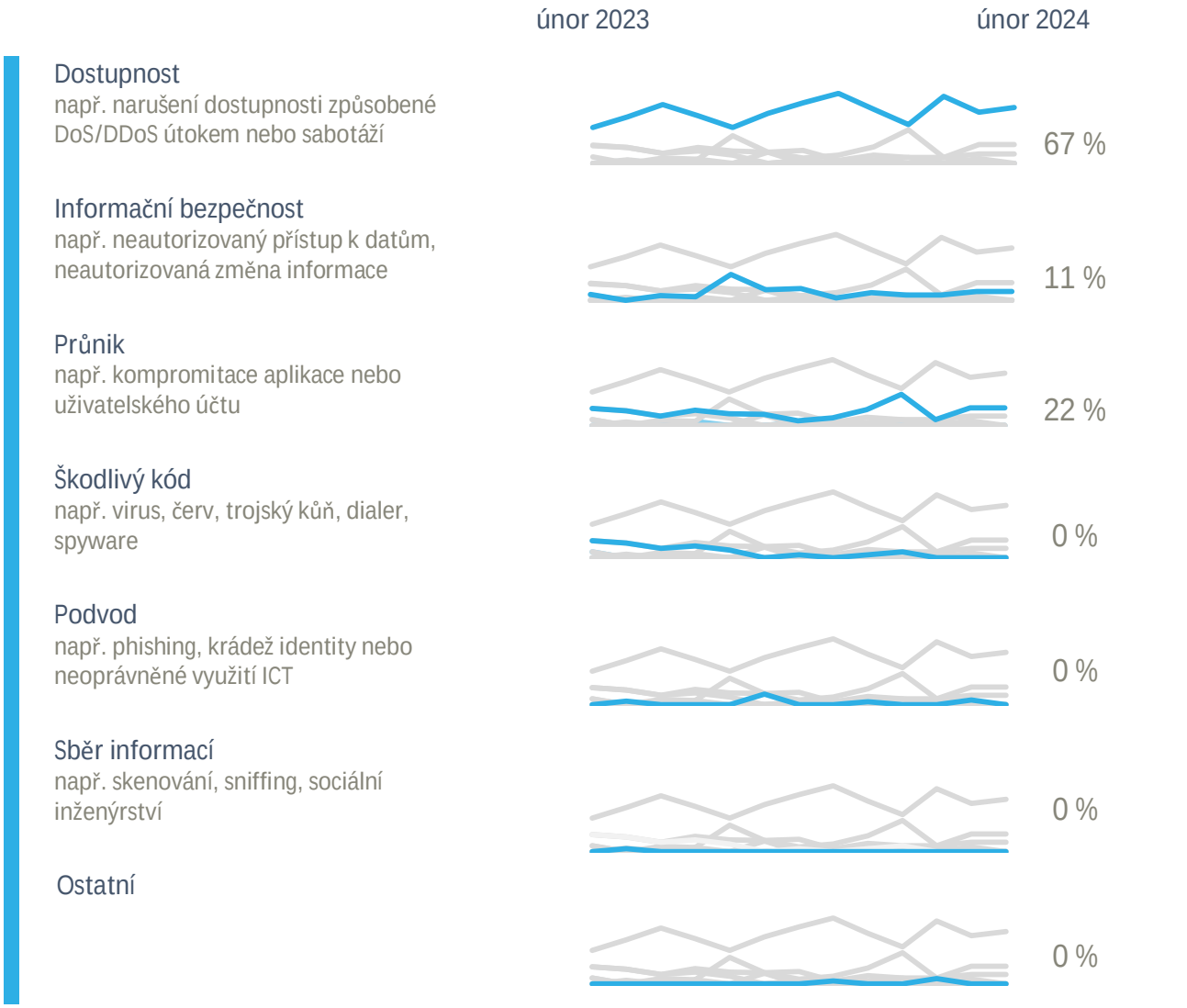

[1] NÚKIB evidoval 16 incidentů u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající 2 incidenty nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

## Klasifikace incidentů nahlášených NÚKIB[3]

Dlouhodobý trend dominance incidentů spojených s dostupností přetrvával také v únoru. Jako obvykle byla tato kategorie tvořena primárně DDoS útoky (viz následující kapitola) a provozními výpadky.

NÚKIB dále řešil incidenty ve dvou kategoriích:

- Během února byly zaregistrovány 4 různé případy průniku. Jeden incident v této kategorii byl spojen se zranitelnostmi produktů Ivanti, o kterých jsme informovali v minulém měsíčním přehledu. Tyto zranitelnosti se tak prozatím výrazněji nepropsaly do incidentů evidovaných NÚKIB, navzdory informacím z otevřených zdrojů o jejich rozsáhlém zneužívání.
- V rámci kategorie Informační bezpečnost evidoval NÚKIB jeden významný incident, během kterého došlo k úniku citlivých informací regulovaného subjektu. Dále pak do této kategorie spadal jeden incident spojený s ransomwarem, jež cílil na neregulovanou vzdělávací instituci.




[3] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu).

# Trendy v kybernetické bezpečnosti za únor pohledem NÚKIB[4]

## Phishing, spear-phishing a sociální inženýrství

NÚKIB v únoru zaregistroval pouze jeden incident, v rámci kterého byl prokazatelně využit phishing. Útočníkům se podařilo přimět oběť k vyplnění přihlašovacích údajů na podvodné stránce a poté zneužít tyto údaje pro přístup do dalších služeb.

## Malware

V únoru podobně jako v uplynulých měsících probíhaly kontinuální aktivity v oblasti malwarové analýzy v souvislosti s některými dříve evidovanými incidenty.

## Zranitelnosti

NÚKIB v průběhu února vydal jedno upozornění týkající se zranitelností. Jednalo se o dvě vzdáleně zneužitelné zranitelnosti v operačním systému FortiOS používaném ve firewallech FortiGate od společnosti Fortinet, Inc. NÚKIB doporučuje neprodleně provést aktualizaci všech zranitelných produktů od této společnosti. V případě, že firewally nenabízí provedení aktualizace, je nutné ji stáhnout přímo z webu výrobce.

## Ransomware

V únoru byl stejně jako v předešlých dvou měsících evidován pouze jeden incident spojený s ransomwarem. Jednalo se o RebornRansomware, prostřednictvím kterého útočníci zašifrovali virtuální servery neregulované vzdělávací instituce.

## Útoky na dostupnost

Během února NÚKIB evidoval celkem 7 DDoS útoků, které cílily převážně na státní instituce. Pouze za dvěma těmito útoky stály proruské hacktivistické skupiny.

[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

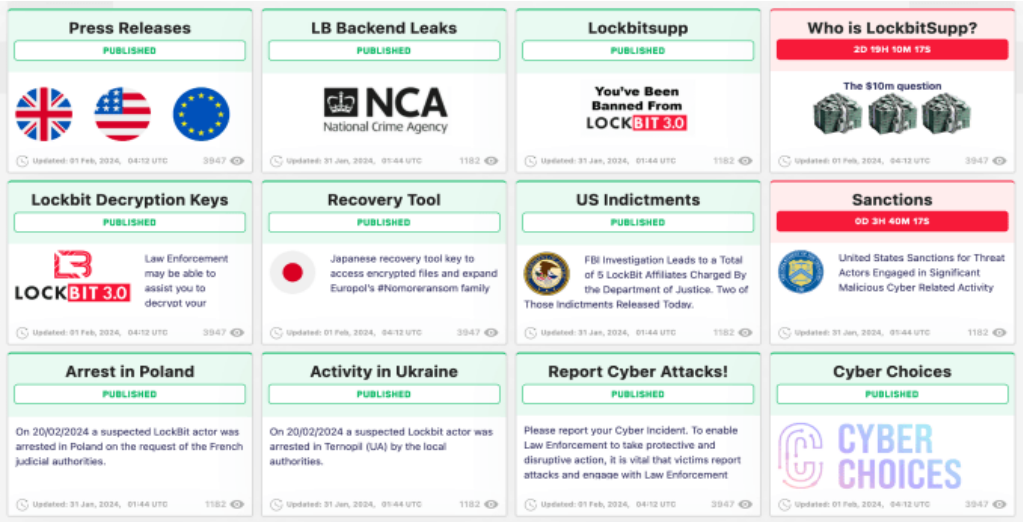
## Zaměřeno na hrozbu: Zásah vůči infrastruktuře ransomwarového gangu LockBit

Během pondělí 19. února byly zabaveny darkwebové stránky ransomwarového gangu LockBit v rámci mezinárodní operace bezpečnostních složek, do které se zapojil britský Národní kriminální úřad (National Crime Agency, NCA), FBI, Europol a několik mezinárodních policejních agentur. Bezpečnostní složky v rámci operace získaly kontrolu nad infrastrukturou, daty a dalšími informacemi ransomwarového gangu. Krátce poté začaly oznamovat celou řadu informací, a to prostřednictvím ovládnutých stránek LockBitu (viz Obrázek 1). Bezpečnostní složky také nedávno oznámily zajištění více než 14 tisíc účtů u služeb třetích stran, které patřily členům či partnerům gangu LockBit. Mezi další již zveřejněné informace patří například to, že LockBit si nechával data obětí i poté, co od nich získal výkupné.

Od doby oznámení operace již došlo k vydání prvních zatykačů ze strany USA a prvním zatknutím, konkrétně v Polsku a na Ukrajině. Množství zajištěného materiálu je však údajně enormní a jejich analýza bude trvat delší dobu. Velmi pravděpodobně (75–85 %) tak lze očekávat další zásahy vůči členům gangu a jeho partnerům či nové poznatky o jejich činnosti.

V rámci operace byl získán také dekryptor k ransomwaru LockBit 3.0.

Obr. 1: Screenshot tzv. leaksite ransomwarového gangu LockBit po jejím převzetí autoritami




Zdroj: techcrunch.com

Zásah policejních složek proti skupině LockBit lze považovat za jednu z největších akcí svého druhu. LockBit patřil mezi nejaktivnější kyberkriminální aktéry, který od roku 2020 napadl více než 2000 obětí po celém světě. Zásah vedl k narušení schopností, ale také poškození důvěryhodnosti skupiny, jejíž případné budoucí vztahy s kriminálními partnery budou provázeny obavami z kompromitace a infiltrace bezpečnostními složkami. Přesto však po pěti dnech skupina LockBit začala opět fungovat a vydala prohlášení, ve kterém se k zásahu policejních složek vyjadřuje. Skupina také v rámci své nové darkwebové stránky zveřejnila informace o nových obětech. Není však dosud jasné, zdali se jedná o reálné oběti, nebo jde pouze o snahu předstírat pokračování aktivit.

## Použité pravděpodobnostní výrazy

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

| Výraz | Pravděpodobnost |
|---|---|
| Téměř jistě | 90–100 % |
| Velmi pravděpodobně | 75–85 % |
| Pravděpodobně | 55–70 % |
| Nelze vyloučit/Reálná možnost | 25–50 % |
| Nepravděpodobně | 15–20 % |
| Velmi nepravděpodobně | 0–10 % |

## Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách nukib.gov.cz). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

| Barva | Podmínky použití |
|---|---|
| TLP:RED | Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace. |
| TLP:AMBER+STRICT | Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. |
| TLP:AMBER | Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. |
| TLP:GREEN | Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace. |
| TLP:CLEAR | Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena. |