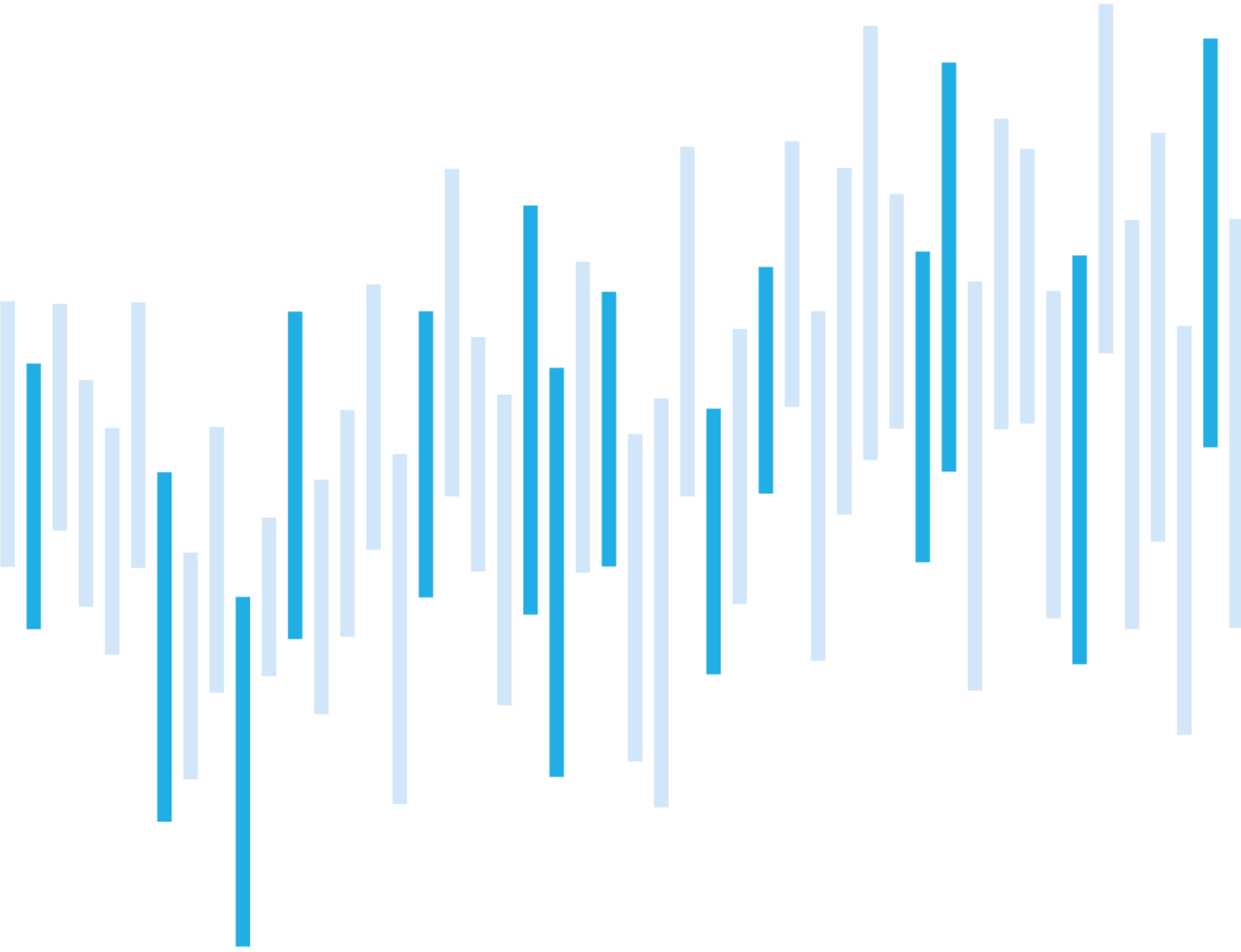
Kybernetické incidenty pohledem NÚKIB

LISTOPAD 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Listopad byl náročným měsícem jak z hlediska počtu incidentů (22), tak jejich závažnosti. Zapříčinilo to především zneužívání zranitelností MS Exchange Serveru a ransomwarové útoky.

Série zranitelností MS Exchange Serveru nazývaná ProxyShell se poprvé objevila už v srpnu tohoto roku, ale NÚKIB až nyní evidoval její aktivní zneužívání, když mu incident nahlásily čtyři organizace. Vzhledem k rozšířenosti MS Exchange Server je ale pravděpodobné (55–70 %), že počet českých kompromitovaných cílů je mnohem vyšší.

Listopad, kdy více jak čtvrtinu všech útoků tvořil ransomware, potvrdil rostoucí charakter této hrozby. Nelze vyloučit (25–50 %), že se do tohoto negativního trendu v následující měsících promítne i návrat malwaru Emotet. Provozovatelé Emotetu, kteří v listopadu začali svůj botnet znovu zprovozňovat, ho v minulosti často pronajímali ransomwarovým gangům, aby jim sloužil jako vstupní bod do sítí organizací, a Česká republika už tako-vou kampaň v minulosti zažila.

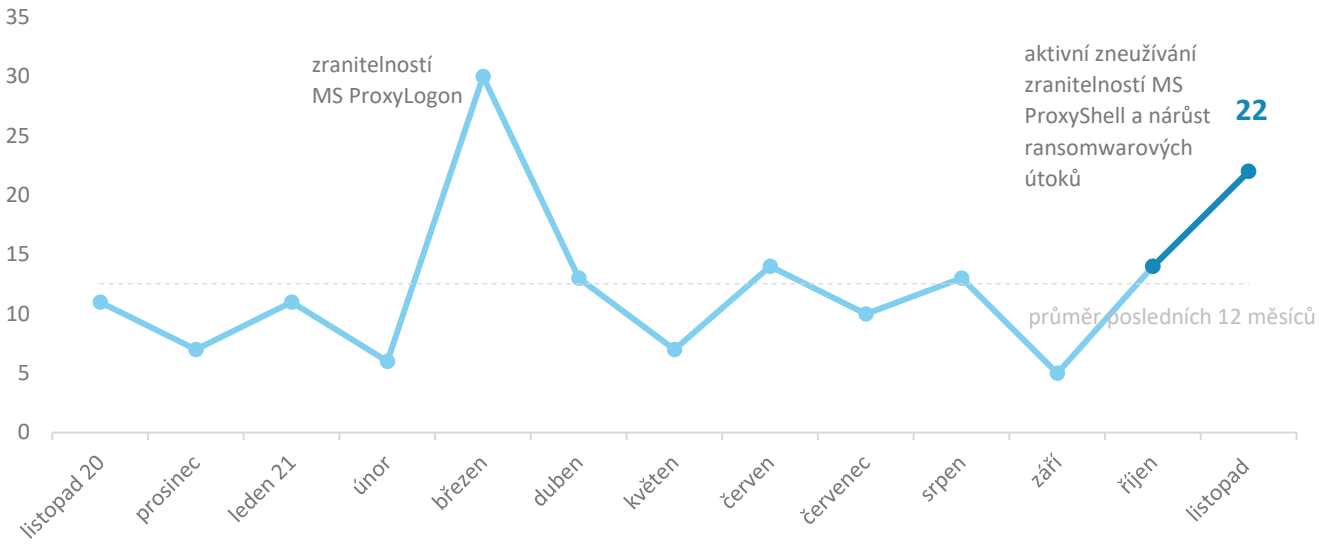
Obsah

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 uve-den původ těchto informací.

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

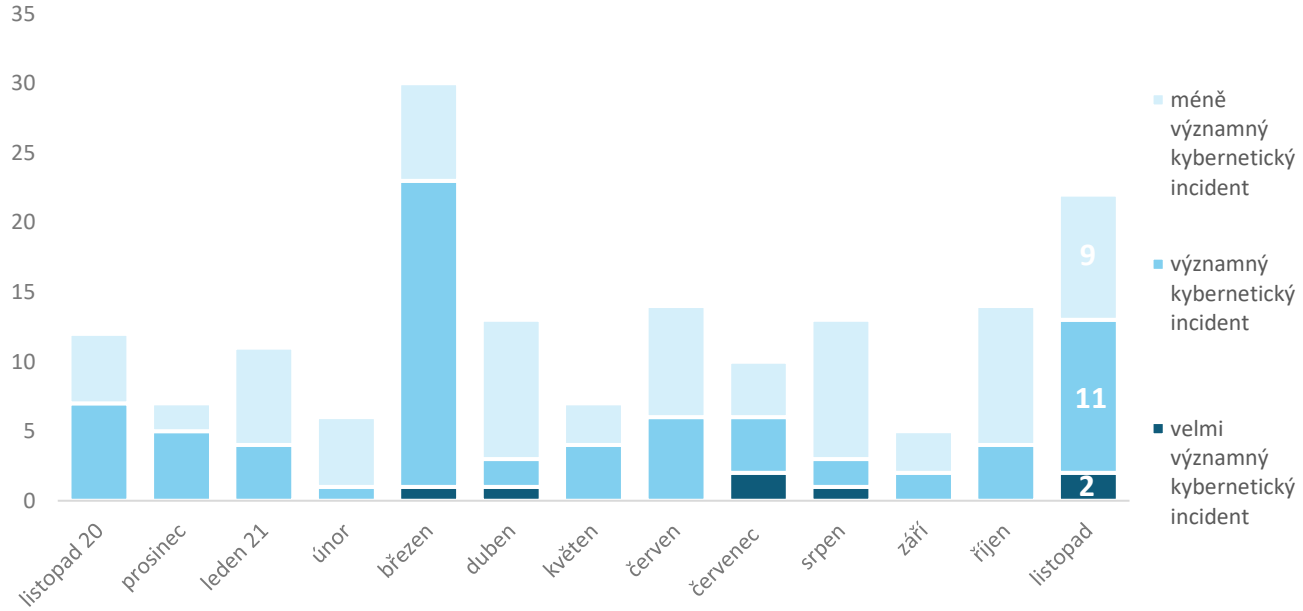
Počet kybernetických incidentů nahlášených NÚKIB

Počet incidentů, které NÚKIB řešil, se vyšplhal vysoko nad průměr posledního roku. Listopad s 22 incidenty tento průměr předčil téměř dvojnásobně.[1]



Závažnost řešených kybernetických incidentů[2]

Listopad byl pozoruhodný i z hlediska závažnosti řešených incidentů. Ve dvou případech se jednalo o velmi významný kybernetický incident, který znemožnil subjektům vykonávat svou hlavní funkci a v době řešení incidentu nebylo jasné, jak dlouho zabere obnova sítí, ve kterých se nacházely kritické prvky pro fungování dotčených společností.

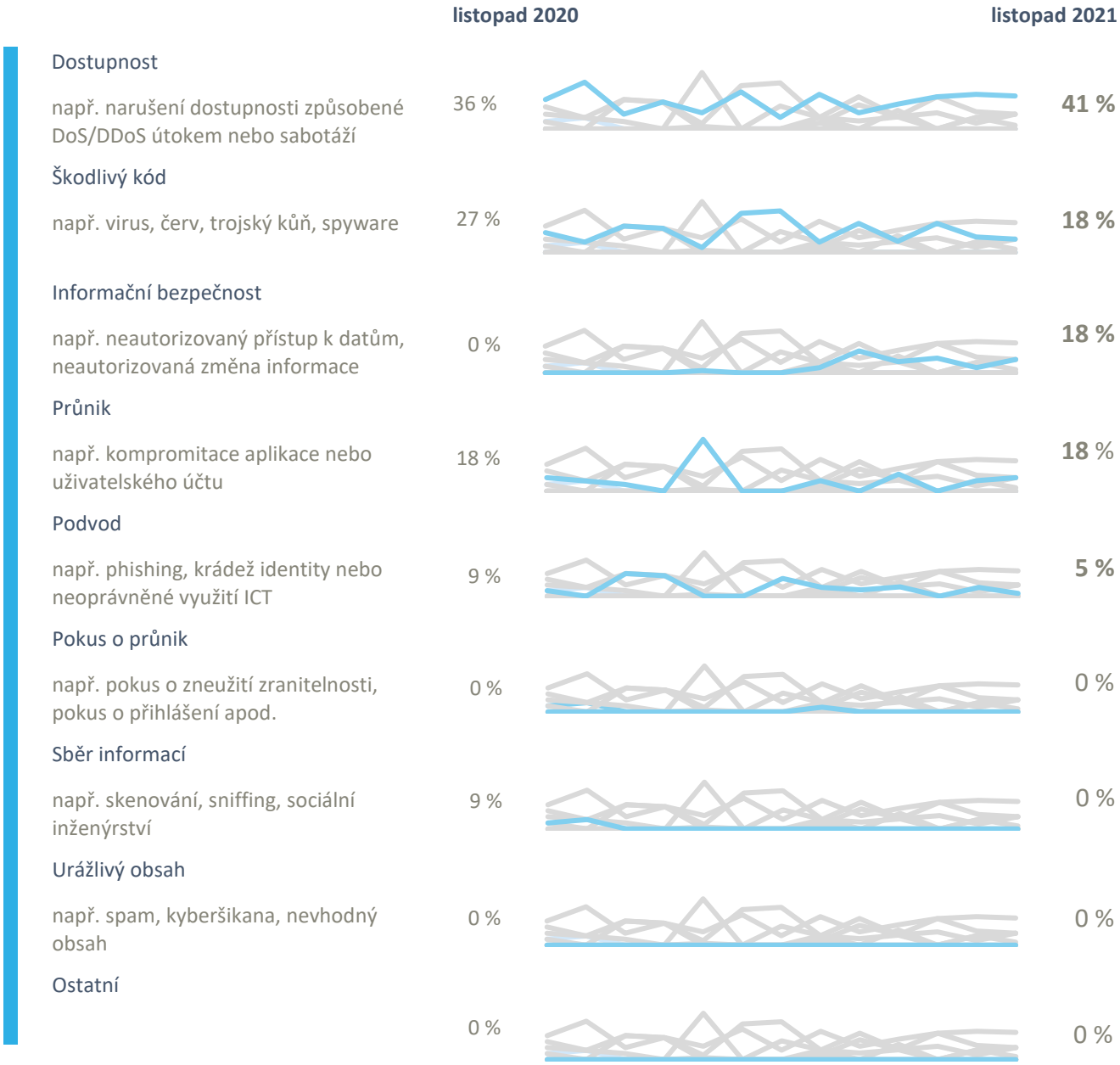


[1] Devět incidentů NÚKIB nahlásily povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých 13 incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů NÚKIB určuje na základě vyhlášky č. 82/2018 Sb a interní metodiky.

Klasifikace incidentů nahlášených NÚKIB[3]

Většina incidentů (9) vyústila v nedostupnost služeb. Ve čtyřech případech nedostupnost způsobily technické chyby na straně dotčených organizací, v dalších čtyřech zapříčinil částečný výpadek služeb ransomware, a za poslední nedostupností stál DDoS útok.

Vedle narušení dostupnosti NÚKIB řešil také škodlivé kódy, které čtyři organizace objevily ve svých sítích, čtyři případy průniků spojených se zneužitím série zranitelností MS Exchange Server známé jako ProxyShell, a čtyři případy, ve kterých došlo k narušení bezpečnosti informací. Ani v listopadu nechyběly phishingové kampaně, při kterých došlo ke kompromitaci uživatelských účtů a následnému rozesílání spamu z infikovaných schránek.



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

Trendy v kybernetické bezpečnosti za listopad pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Listopadová kampaň zneužívání zranitelností MS Exchange, které se říká ProxyShell, byla úzce spjata s phishingem. Ve všech případech, které NÚKIB řešil, si útočníci po získání kontroly nad mailovými servery stáhli obsah mailboxu a phishing navázali na předchozí legitimní korespondenci své oběti. Téměř jistě (90–100 %) to dělali v očekávání, že příjemce otevře škodlivý odkaz pravděpodobněji, pokud mu přijde jako odpověď na konverzaci, kterou vedl s člověkem, kterého zná.

Malware

Na kybernetickou scénu, včetně té české, se vrátil malware Emotet. Stalo se tak poprvé od ledna 2021, kdy se Europolu ve spolupráci s policejními složkami několika zemí podařilo zničit jeho infrastrukturu. Emotet nakazil jednu českou organizaci a její infrastrukturu použil jako své řídící servery. Návrat Emotetu je pro české cíle špatnou zprávou. V letech 2019 a 2020 čelily několika systematickým kampaním Emotetu a nelze tak vyloučit (25–50 %), že k nim v případě pokračujícího nárůstu aktivity malwaru přibude další.

Zranitelnosti

V listopadu čelila ČR aktivnímu zneužívání zranitelností Microsoft Exchange Server ProxyShell. ProxyShell se poprvé objevil už v srpnu tohoto roku, ale NÚKIB až nyní evidoval jeho zneužívání napříč republikou. Incident nahlásily čtyři organizace, a to jak povinné subjekty, tak neregulované organizace. Vzhledem k rozšířenosti MS Exchange Server je ale pravděpodobné (55–70 %), že počet českých kompromitovaných cílů je mnohem vyšší. Pravděpodobným důvodem aktivního zneužívání zranitelnosti budou připravené skripty pro útok, které byly od října k dispozici na darkwebu. Více informací k této kampani můžete najít ve veřejné analýze NÚKIB.

Ransomware

NÚKIB v listopadu evidoval šest případů ransomwaru. Ve čtyřech útočníci zašifrovali část infrastruktury a tím obětem znepřístupnili některá data a služby. V dalších dvou případech se jim podařilo i exfiltrovat data a napadeným organizacím hrozili tzv. dvojím vydíráním.

V listopadu na české cíle útočily LockBit, Avos Locker, Makop, Loki Locker a dvě organizace napadl Phobos. Phobos je ransomware, který v průběhu celého roku cílí především na malé a střední podniky. LockBit je v ČR také stálicí, poprvé se tento ransomware ve statistikách NÚKIB objevil na jaře minulého roku.

Útoky na dostupnost

V listopadových incidentech se objevil pouze jeden DDoS útok, který způsobil nedostupnost služeb napadené organizace na osm hodin.

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

Nejpoužívanější technika měsíce: Valid Accounts

NÚKIB kybernetické incidenty vyhodnocuje také na základě rámce MITRE ATT&CK, který slouží jako přehled známých technik a taktik používaných při kybernetických útocích. NÚKIB na jejím základě mimo jiné určuje četnost využívání technik/taktik.

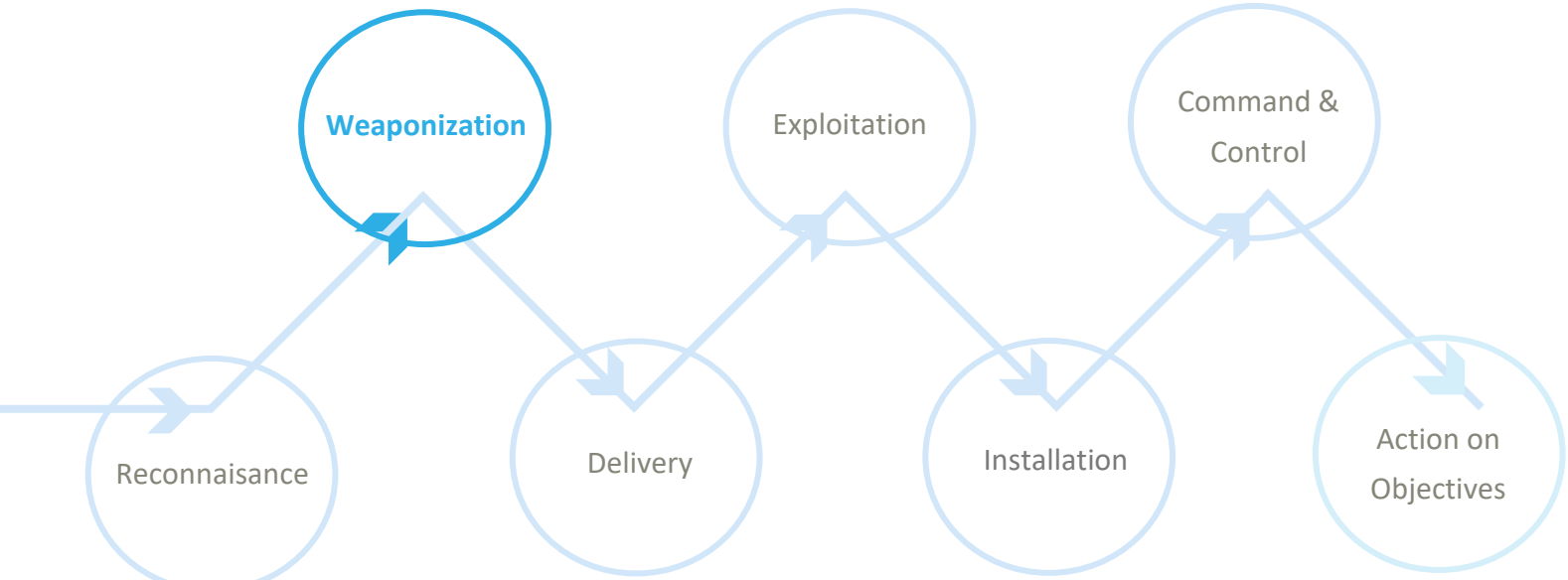
V říjnových incidentech se nejčastěji objevila technika, kterou MITRE nazývá „Valid Accounts“. Propsalo se do toho aktivní zneužívání zranitelností MS Exchange Serveru, kdy útočníci po kompromitaci serverů získali přístup k mailboxu oběti a z jejích legitimních účtů poté rozesílali phishingové zprávy.

Valid Accounts je technika, při níž útočníci získají přístup k účtům uživatelů, což jim umožní snadnější pohyb v infrastruktuře napadené organizace. Díky přístupu k legitimním účtům se jim jednodušeji podaří projít přes různé autorizační mechanismy v systému. Legitimní účty jim také zaručí větší odolnost, protože administrátor takový účet vnímá jako legitimní a nevěnuje mu potřebnou pozornost. Útočníci tím sníží pravděpodobnost odhalení, neboť jejich pohyb nezachytí firewall, antivirus ani další systémy monitorující škodlivé aktivity.

MITRE ID: T1078

Mitigace: V případě listopadových incidentů je mitigace spojená s doporučeními pro aktualizaci MS Exchange Serveru. Jelikož technika „Valid Accounts“ jde často ruku v ruce s kompromitací přístupových údajů, pojí se její mitigace také s bezpečností hesel. Organizace by tak měly vynucovat silná hesla, vyžadovat změnu po vytvoření nového účtu, zavést vícefaktorovou autentizaci nebo monitorovat účty mimo pracovní hodiny.

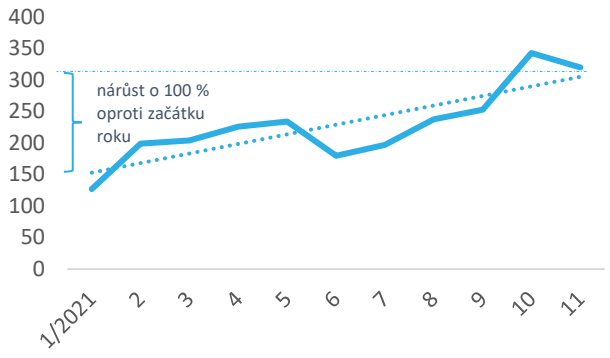
Znázornění „Valid Accounts“ v kill chainu, který ukazuje, ve které fázi útočníci techniku používají. V incidentech NÚKIB to odpovídalo Weaponization, ale obecně mohou útočníci tuto techniku zneužít ve většině fázích kill chainu.



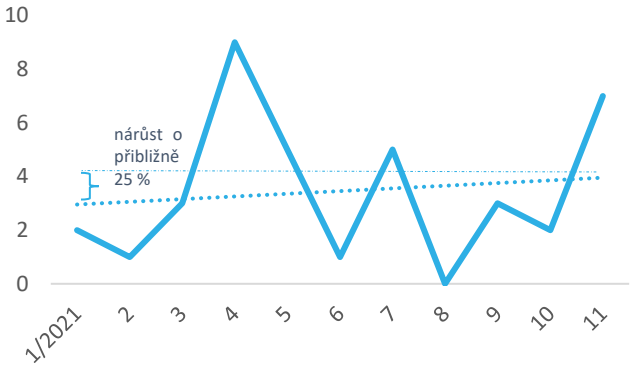
Zaměřeno na hrozbu: Ransomware jako služba

Počet ransomwarových útoků ve světě i České republice narůstá. Jen za poslední rok se počet ve světě přibližně zdvojnásobil, v ČR vzrostl cca o čtvrtinu (viz grafy níže). V listopadových incidentech byl ransomware zastoupen ve velkém, tvořil více než čtvrtinu všech kybernetických incidentů nahlášených NÚKIB.

Počet ransomwarových útoků ve světě od ledna 2021[5]

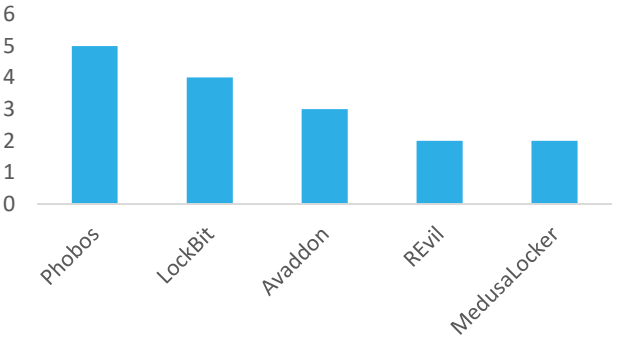


Počet ransomwarových útoků nahlášených NÚKIB od ledna 2021[6]



Ransomwary, které prozatím v ČR v průběhu roku 2021 nejvíce útočily (viz graf níže), jsou všechny pronajímány jako služba (ransomware-as-a-service, RaaS).[7] Kyberkriminální skupiny svůj kód za finanční obnos nabízí komukoliv, kdo chce provést ransomwarový útok. RaaS je proto neustále se měnící hrozba. Na rozdíl od APT skupin, jejichž operace mají trvalejší charakter, fungují některé kyberkriminální skupiny pouze krátkodobě. Často se stává, že po zániku jedné se rychle objeví nová, která používá podobné operační postupy.

Pět nejaktivnějších skupin v ČR od ledna 2021



Ransomwarové útoky na české cíle budou velmi pravděpodobně (75–85 %) v krátkodobém horizontu dále narůstat. Existuje reálná možnost (25–50 %), že se do tohoto rostoucího trendu promítne i návrat malwaru Emotet. Provozovatelé Emotetu, kteří v listopadu začali svůj botnet znovu zprovozňovat, v minulosti často poskytovali přístup do infrastruktury ransomwarovým gangům, aby jim sloužil jako vstupní bod do sítí organizací. Česká republika už takovou kampaň v minulosti zažila. Před Vánoci 2019 se ransomware Ryuk šířil napříč českými odvětvími a na jeho začátku stál vždy právě Emotet.

[5] Data v grafu vychází ze stránky DarkTracer, jejíž správci monitorují darkweb a na základě informací ze stránek ransomwarových skupin vytváří hromadné statistiky. Do statistik se tak nedostanou všechny ransomwarové útoky, ale pouze útoky těch skupin, které informace o svých útocích zveřejňují.

[6] Tento graf vychází incidentů hlášených NÚKIB. Na základě monitoringu darkwebu víme o dalších českých obětech ransomwarových skupin, ale jelikož nám útok nehlásily (jako neregulované subjekty ani neměly povinnost), do statistik jsme je z důvodu konsistence dat nedávali.

[7] dtto

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 www.nukib.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	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to--know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
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:WHITE	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.