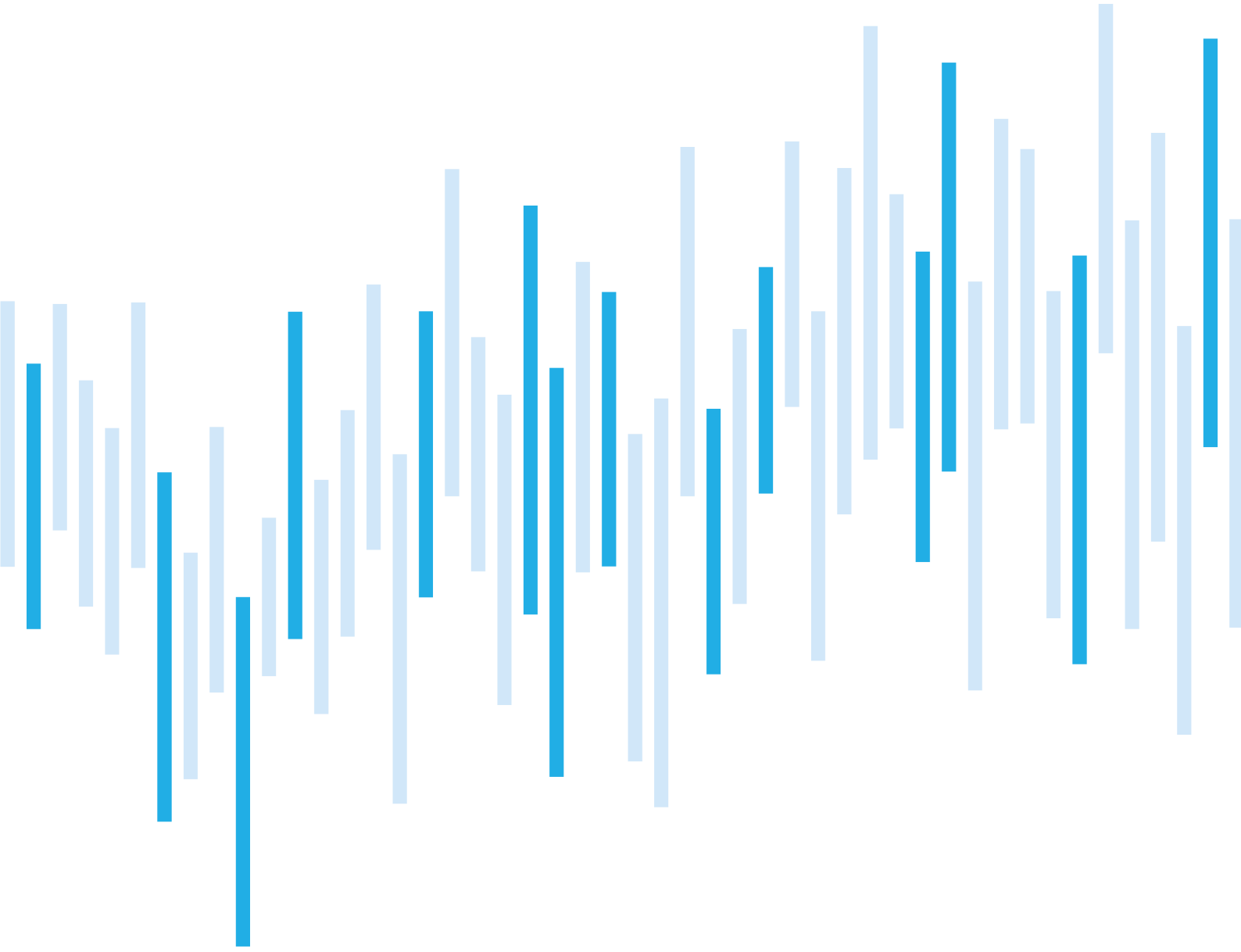
Kybernetické incidenty pohledem NÚKIB

PROSINEC 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet evidovaných kybernetických incidentů v prosinci oproti předešlému měsíci klesl a pohyboval se na podprůměrných hodnotách. Klesla také závažnost evidovaných incidentů. Prosinec se stal jediným měsícem roku 2022, kdy nebyl evidován významný ani velmi významný kybernetický incident.

V prosinci opět převažovaly incidenty, které hlásily povinné osoby dle ZKB. Oběťmi se staly subjekty ze sektorů veřejné správy, zdravotnictví, digitálních služeb a energetiky. Nejpočetnějším typem incidentu se poprvé za rok 2022 stala kategorie škodlivý kód.

Vzhledem k relativně častému zneužívání vzdáleného přístupu útočníky jako vstupního vektoru v rámci kybernetických útoků se v tomto reportu zaměřujeme na techniku T1133: External Remote Services.

V kapitole věnující se trendům jsme se tentokrát zaměřili na kyberkriminalitu jako službu (tzv. cybercrime-as-a-service). Jedná se o model, v rámci kterého kyberkriminální aktéři nabízejí za úplatu nástroje a služby určené pro provádění kybernetických útoků.

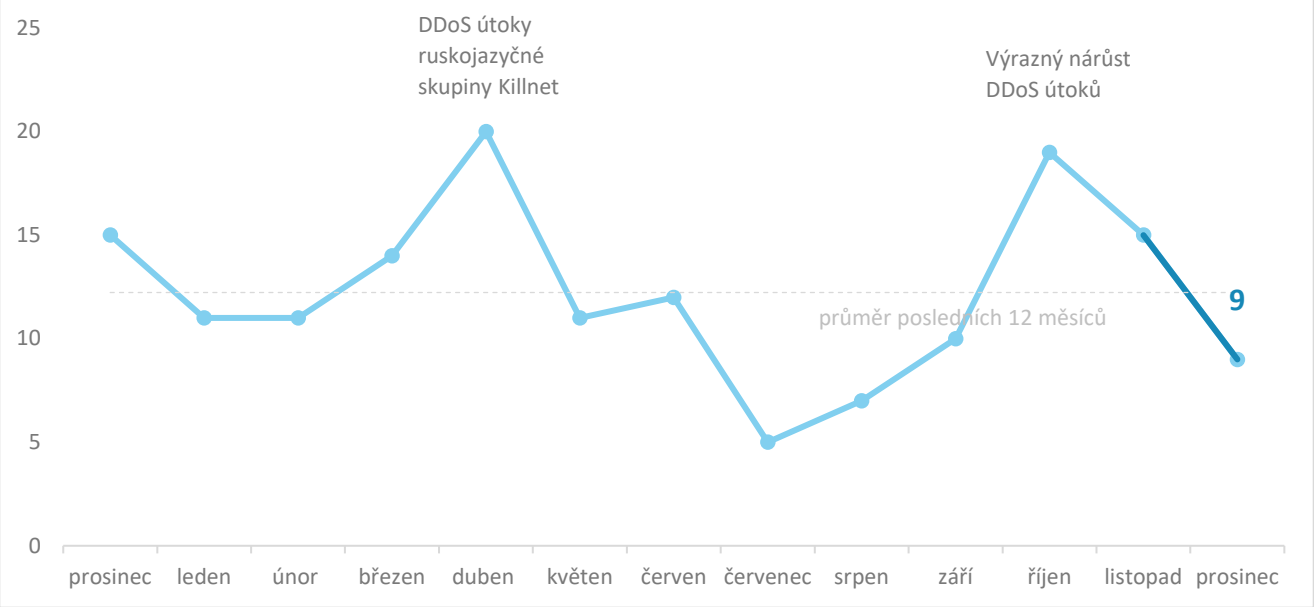
Obsah

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

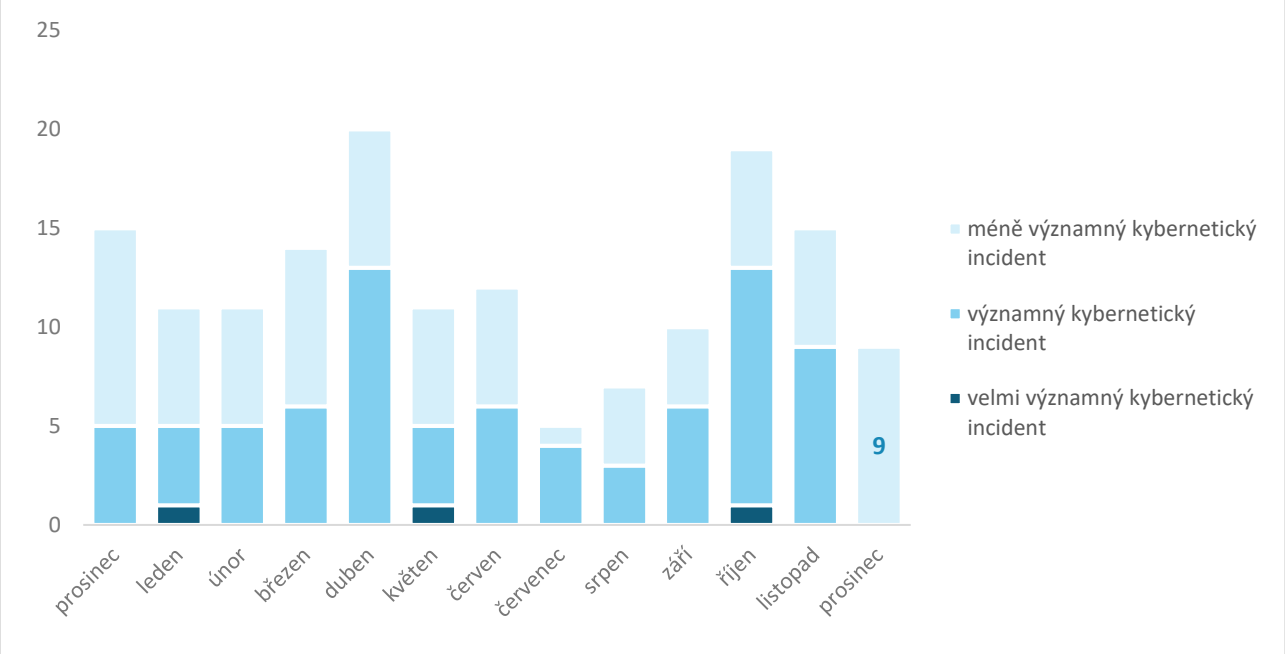
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Prosinec se podobně jako listopad vyznačoval poklesem kybernetických bezpečnostních incidentů. V závěru roku se tak počet incidentů dostal na podprůměrné hodnoty, přičemž prosinec se dokonce stal měsícem s třetím nejnižším počtem incidentů za rok 2022. [1]



Závažnost řešených kybernetických incidentů[2]

Konec roku se vyznačoval poklesem závažnosti kybernetických incidentů. Prosinec se stal jediným měsícem roku 2022, kdy nebyl evidován významný ani velmi významný kybernetický incident.

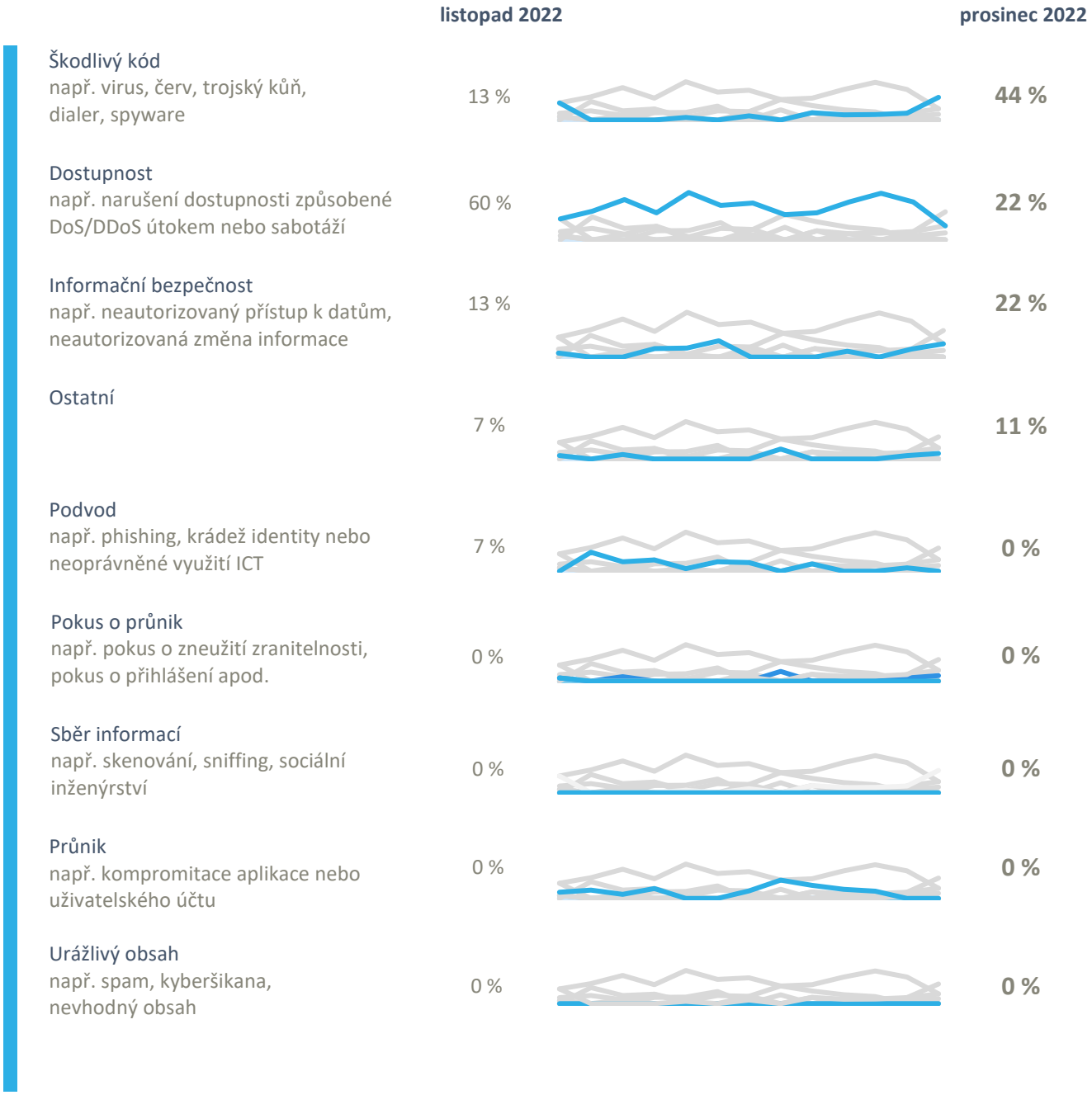


[1] Celkem šest incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbývajících třech NÚKIB informovaly zákonem neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Prosincové kybernetické incidenty NÚKIB zařadil do čtyř kategorií:

- Nejpočetnějším typem incidentu se stal škodlivý kód, který se po většinu roku držel na poměrně nízkých hodnotách. Prosincové incidenty zahrnovaly ransomware i jiné typy malwaru.
- V prosinci byly zaznamenány celkem dva útoky na dostupnost, z nichž pouze jeden zahrnoval DDoS útok. Ve srovnání s dvěma předešlými měsíci tak jde o výrazný pokles tohoto typu útoku.
- Stejně jako v listopadu došlo také v prosinci ke dvěma incidentům týkajících se informační bezpečnosti. Zatímco jeden z nich byl způsobem chybou systému, příčinou vzniku druhého incidentu bylo selhání lidského faktoru.
- NÚKIB v prosinci evidoval také jeden incident z kategorie ostatní.



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

Trendy v kybernetické bezpečnosti za prosinec pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishing a další techniky sociálního inženýrství jsou stálým trendem. V prosinci byl phishing využit k šíření škodlivého odkazu přinejmenším v jednom evidovaném případě.

Malware

Po několikaměsíční pauze NÚKIB evidoval dva případy incidentů zahrnujících využití malwaru. Jedním z nich byl malware Redline Stealer určený primárně ke sběru dat, který je nabízen jako služba (tzv. Malware-as-a-service).

Zranitelnosti

Stejně jako v listopadu, i v prosinci vydal NÚKIB jedno upozornění na zranitelnost. Tentokrát se jednalo o kritickou zranitelnost FortiOS CVE-2022-42475, jejíž zneužití umožňuje neautentizovaným uživatelům vzdálené vypnutí stroje a spuštění libovolného kódu.

Ransomware

NÚKIB v prosinci řešil celkem dva ransomwarové útoky, v obou případech u neregulovaných subjektů. Jednalo se o ransomwary PLAY a FAUST. Druhý jmenovaný patří do rodiny Phobos, která se v rámci evidovaných incidentů objevila v roce 2022 už poněkolikáté.

Útoky na dostupnost

V kontrastu s předchozími měsíci, kdy byly registrovány DDoS kampaně vedené vůči českým subjektům, došlo v rámci kategorie útoků na dostupnost k výraznému poklesu. V prosinci byl totiž evidován pouze jediný DDoS útok. Ačkoli byl tento útok úspěšný, vedl pouze ke krátkodobému výpadku webového portálu subjektu.

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

Technika měsíce: External Remote Services

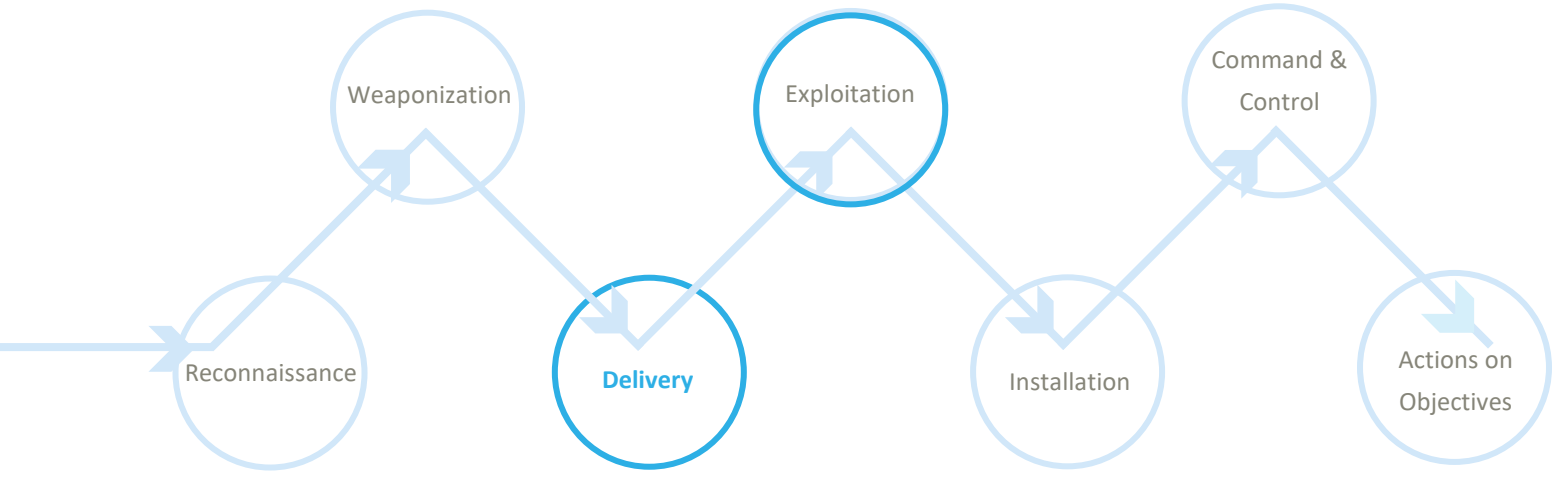
NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, jenž slouží jako přehled známých technik a taktik používaných při kybernetických útocích. Útočníci často využívají vzdáleného přístupu jako vstupního vektoru útoku. Proto jsme se nyní zaměřili na techniku T1133: External Remote Services.

MITRE ID: T1133

Technika External Remote services v rámci MITRE ATT&CK spadá do dvou fází, protože může být využita jak pro získání prvotního přístupu do sítě oběti, tak pro následné získání persistence. Útočníci za tímto účelem mohou zneužít vzdálené služby s externím přístupem (např. VPN, Citrix), které uživatelům umožňují připojit se k interním zdrojům podnikové sítě z externích míst. K připojení je většinou vyžadováno zadání přihlašovacích údajů, které mohou útočníci získat skrze řadu jiných technik. V některých specifických případech lze získat přístup také skrze služby, které nevyžadují autentizaci.

Mitigace: Jedním ze základních mitigačních opatření je zákaz nebo zablokování vzdáleně dostupných služeb, které nejsou nezbytně potřebné. Dále je vhodné také omezení přístupu ke vzdáleným službám skrze centrálně spravované koncentrátory, jako jsou sítě VPN a jiné spravované systémy vzdáleného přístupu. V obecnější rovině je pak vhodným mitigačním opatřením používání vícefaktorového ověření a síťová segmentace.

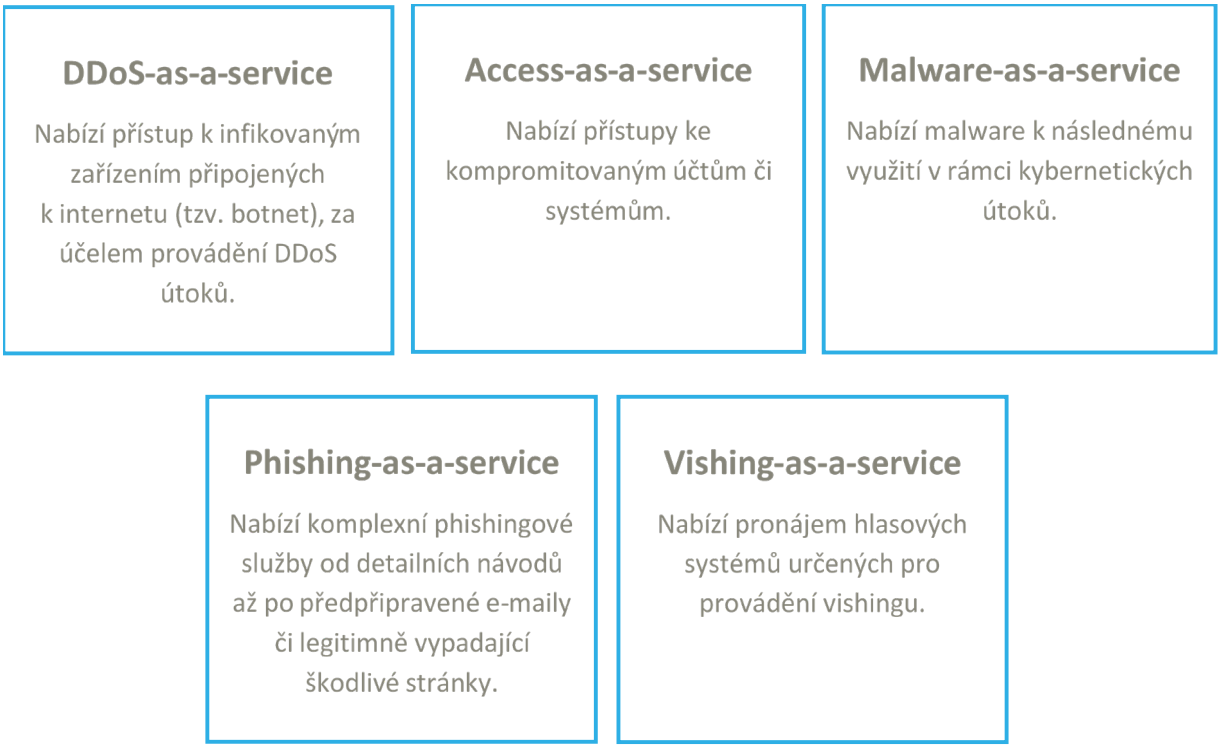
Znázornění techniky T1133 v kill chainu ukazujícím, kdy útočníci techniku používají:



Zaměřeno na trend: Kyberkriminalita jako služba

NÚKIB v prosinci evidoval incident, při němž byl využit malware, který je poskytován jako služba (tzv. malware-as-a-service). Tento incident tak odpovídá trendu, kdy různí kyberkriminální aktéři nabízejí za úplatu nástroje a služby v rámci tzv. cybercrime-as-a-service modelu. Ačkoli v současnosti bývá hojně diskutován především v kontextu ransomwaru, jedná se o model, v rámci kterého je možné zakoupení celé řady nástrojů i služeb. Ty mohou zahrnovat nejen ransomware, ale také jiné druhy malwaru, přístupy do již kompromitovaných systémů, komplexní služby pro phishingové kampaně či služby pro provádění vishingu (viz Obr. 1).

Obr 1: Příklady nabízených kyberkriminálních služeb a nástrojů



Cybercrime-as-a-service je tedy obchodním modelem, který umožňuje prakticky komukoliv s dostatečnými finančními prostředky využívání nástrojů či služeb k provádění kybernetických útoků. Škodlivá kybernetická činnost se tak stává stále dostupnější, a to i pro relativně nezkušené útočníky. Vzhledem k narůstající popularitě tohoto modelu, která s sebou přináší velké zisky, roste také konkurence, což zpětně vede k širší nabídce produktů, ale i ke snižování ceny. To pak následně činí poskytované služby a nástroje dostupnější širšímu okruhu potenciálních zájemců.

V řadě případů prospívá tento model také zkušenějším škodlivým aktérům, kteří mohou nabízený malware, ransomware či jiné nástroje zakomponovávat do svých toolsetů a využívat jej v rámci sofistikovanějších útoků či celých kampaní.

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.
TLP: AMBER+STRICT	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
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.