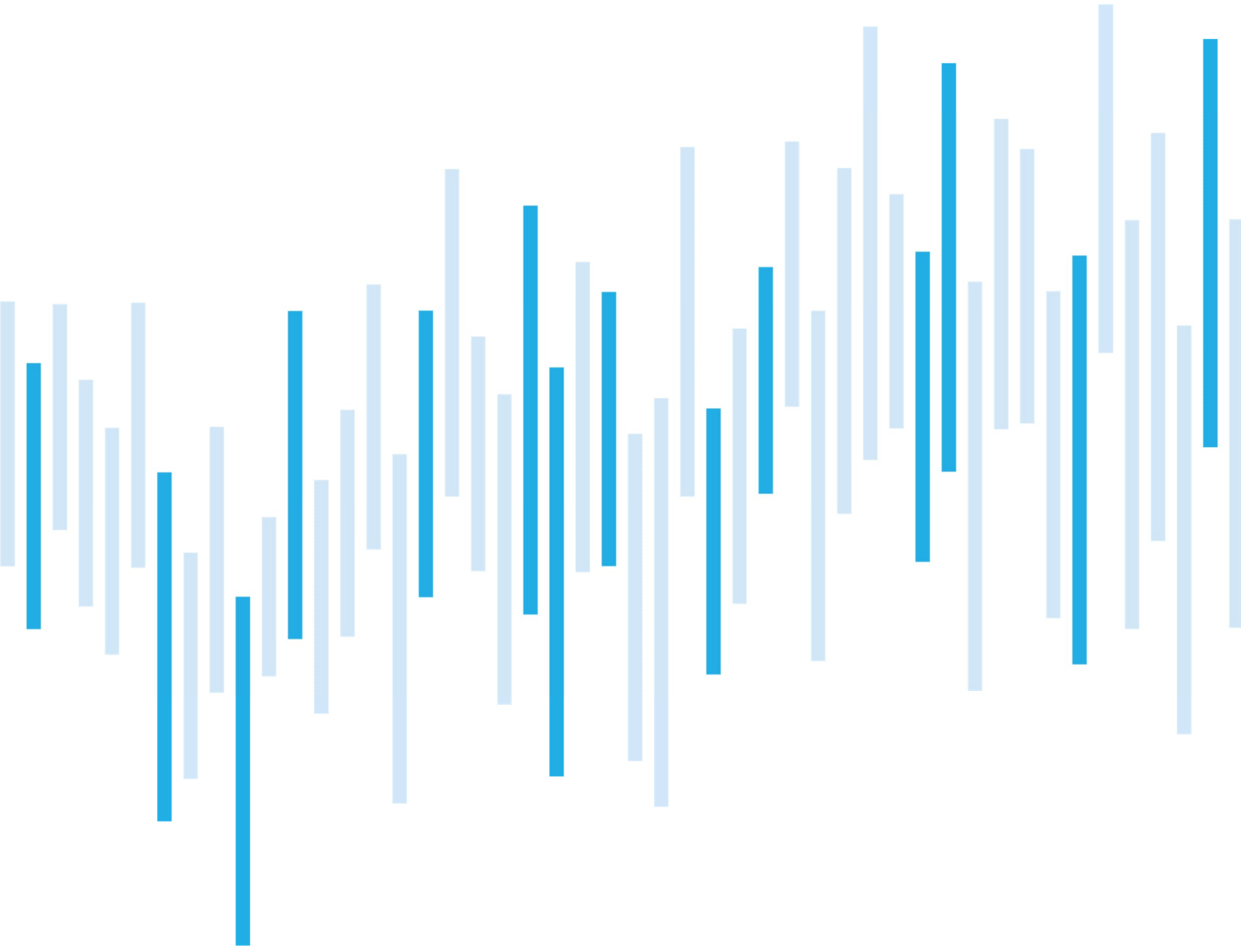
Kybernetické incidenty pohledem NÚKIB

ČERVENEC 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Po dvouměsíčním období nadprůměrných hodnot incidentů došlo v červenci k jejich výraznému poklesu, což bylo dáno zejména snížením počtu registrovaných DDoS útoků. Navzdory tomu i nadále převažovaly incidenty spadající do kategorie omezení dostupnosti. Většina incidentů tohoto typu však byla způsobena výpadky či špatnou konfigurací systémů.

V kapitole *Zaměřeno na hrozbu* se věnujeme tématu phishingových kampaní v ČR. Phishing dlouhodobě představuje jeden z nejčastěji užívaných vektorů kybernetických útoků, čemuž odpovídá i jeho pravidelný výskyt v rámci evidovaných incidentů NÚKIB. Tento vektor může být využíván jak pro jednotlivé útoky, tak i plošně v rámci phishingových kampaní.

V červenci NÚKIB zaznamenal další phishingovou kampaň vedenou vůči českým cílům, která využívá veřejně dostupného malwaru Vjw0rm. NÚKIB v současnosti nedisponuje informacemi o tom, jaký aktér za danou kampaní stojí.

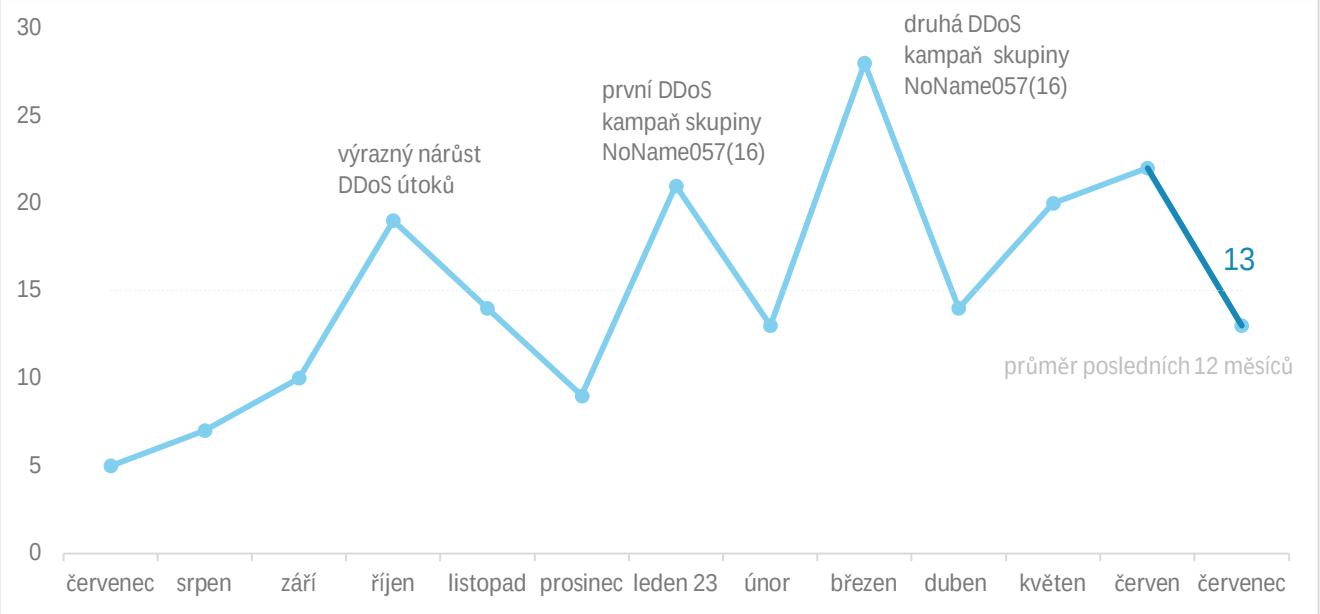
Obsah

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.

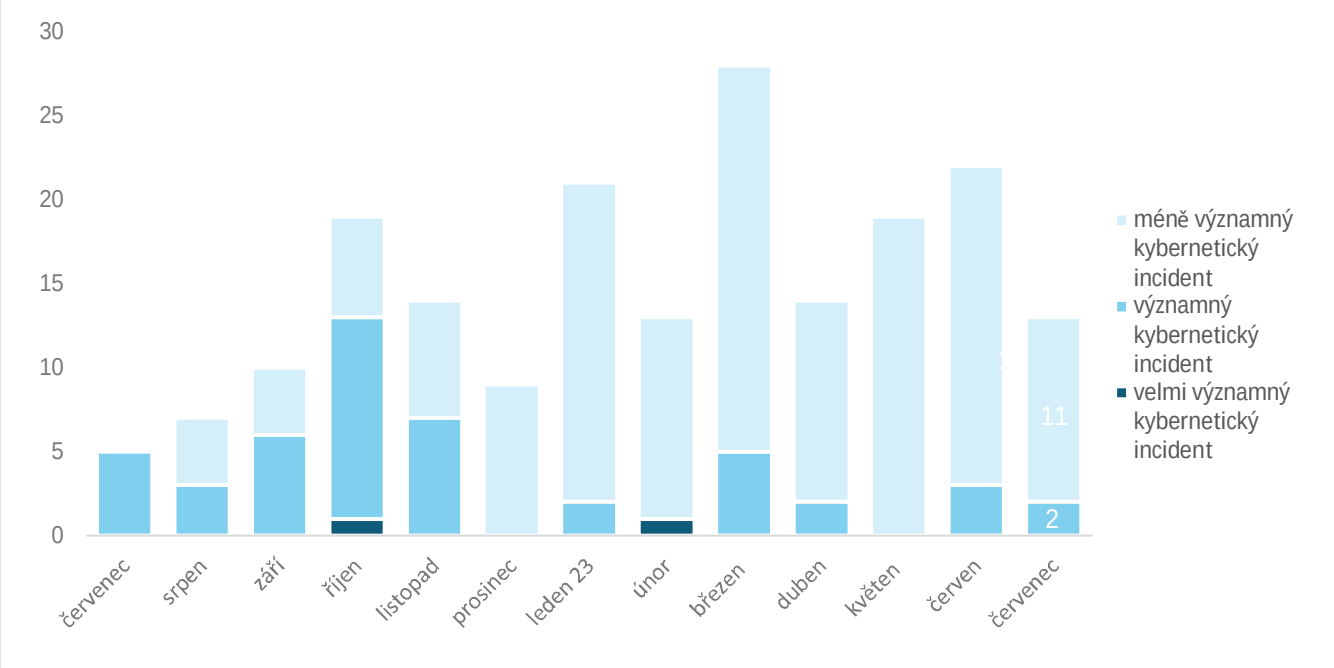
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Po dvouměsíčním období nadprůměrných hodnot incidentů došlo v červenci k jejich výraznému poklesu, což bylo dáno zejména nižším počtem registrovaných DDoS útoků.[1]



Závažnost řešených kybernetických incidentů[2]

Červenec se stal již čtvrtým měsícem v řadě, kdy nebyl zaregistrován žádný velmi významný kybernetický incident. Zaznamenány byly pouze významné a méně významné kybernetické incidenty, které v rámci evidence dlouhodobě převažují.



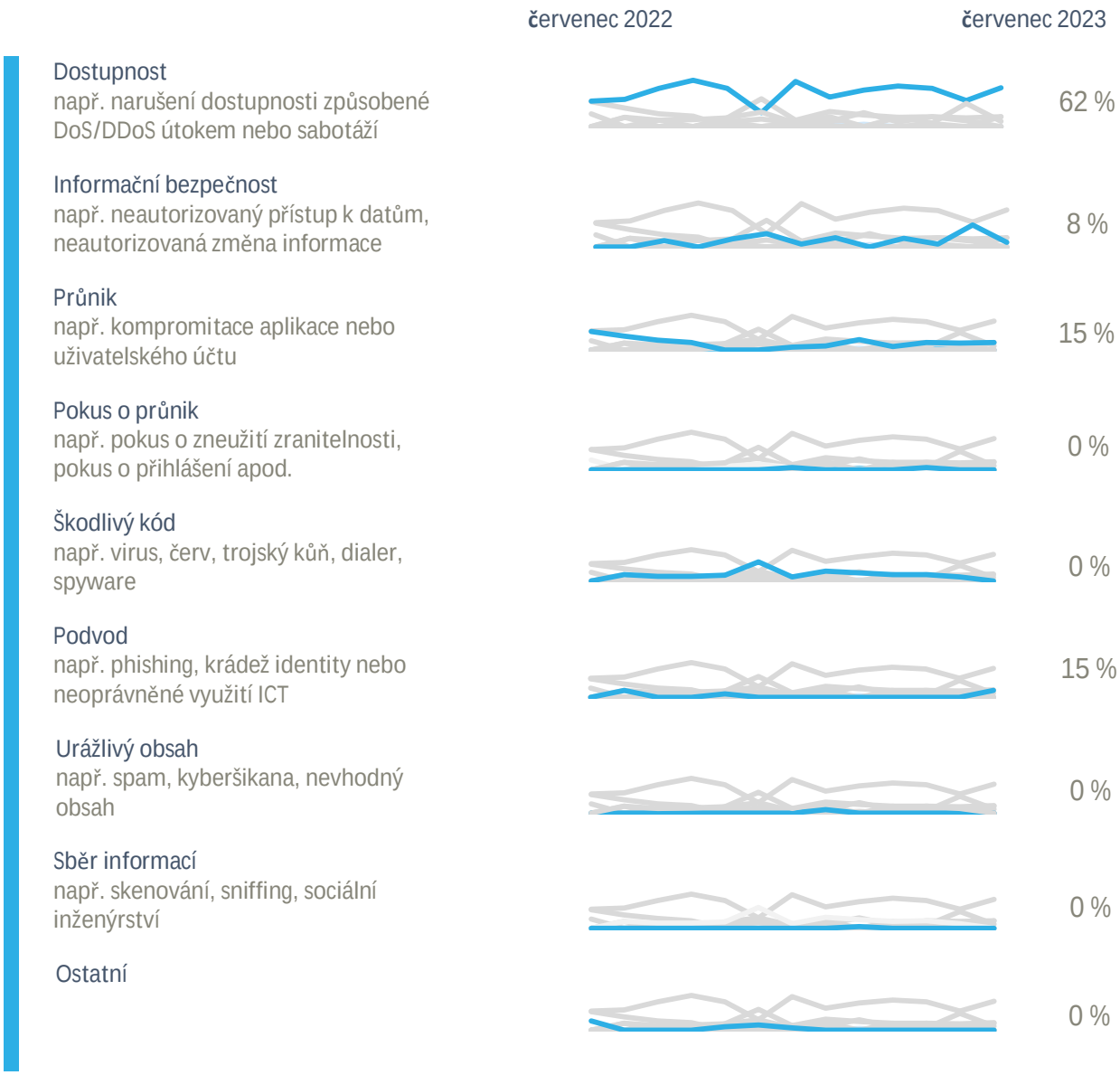
[1] NÚKIB evidoval 10 incidentů u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající 3 incidenty nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Také v červenci pokračoval trend, kdy v rámci evidence převažovaly incidenty spadající do kategorie omezení dostupnosti služeb. Tentokrát však byla většina incidentů spojených s dostupností způsobena výpadky či špatnou konfigurací systémů, nikoliv DDoS útoky.

Vedle toho NÚKIB řešil incidenty v těchto třech kategoriích:

- V červenci byly zaznamenány dva průniky, které však neměly výraznější dopady.
- Dva incidenty byly evidovány v kategorii podvod. Během těchto incidentů útočníci kompromitovali poštovní schránky obětí, ze kterých dále posílali spamy či phishingové e-maily.
- Jeden incident z kategorie Informační bezpečnost byl spojen s ransomwarem MedusaLocker, který vedl k zašifrování dat neregulovaného subjektu.



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

Trendy v kybernetické bezpečnosti za červenec pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

NÚKIB tento měsíc evidoval dva případy phishingu u regulovaných subjektů, v rámci kterých útočníci kompromitovali poštovní schránky obětí, z nichž dále posílali spamy či phishingové e-maily. V obou případech NÚKIB obdržel hlášení incidentu od příjemců phishingu, nikoliv od kompromitovaných subjektů.

Mimo to NÚKIB zaregistroval phishingovou kampaň, která je blíže popsána v kapitole *Zaměřeno na hrozbu*.

Malware

NÚKIB v červenci zaznamenal malware Vjw0rm užívaný v rámci phishingové kampaně vedené mj. proti českým cílům. Více informací o tomto malwaru i o samotné phishingové kampani nabízí kapitola níže.

Zranitelnosti

NÚKIB vydal upozornění na novou zranitelnost CVE-2023-30799, která se týká operačního systému MikroTik RouterOS. Podle nástroje Shodan bylo v Česku v době vydání upozornění zranitelných až 24 tisíc zařízení tohoto výrobce.

Ransomware

Po červnovém nárůstu ransomwarových útoků došlo v červenci k jejich výraznému poklesu. NÚKIB evidoval pouze jeden úspěšný ransomwarový útok. Neregulovaný subjekt byl zasažen ransomwarem MedusaLocker, který způsobil zašifrování značného množství interních dat.

Útoky na dostupnost

V červenci došlo k poklesu zaznamenaných DDoS útoků. Za všemi útoky tohoto typu stála proruská hacktivistická skupina NoName057(16), která se pravidelně zaměřuje na české cíle již od ledna tohoto roku.

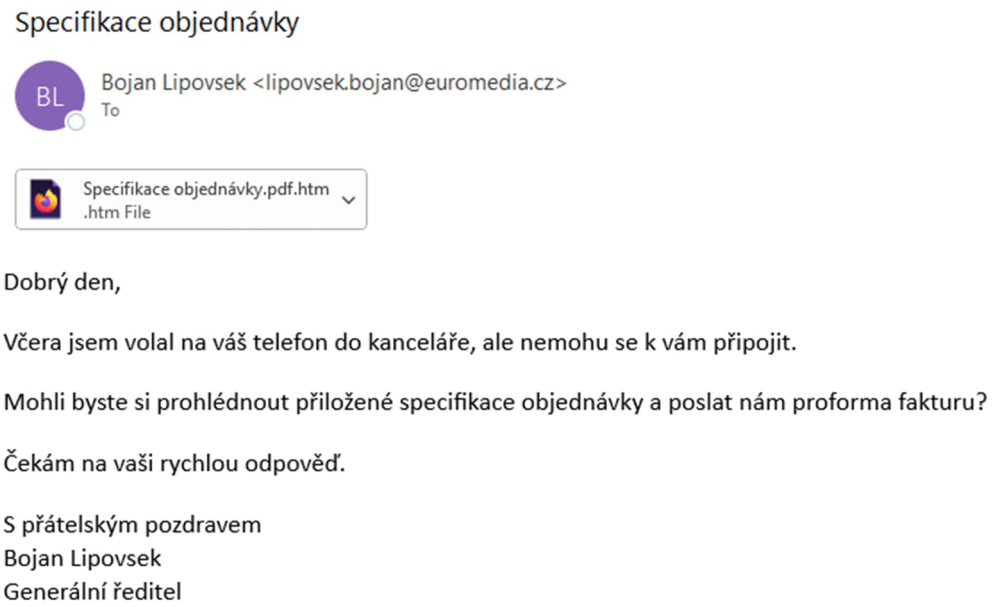
[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Zaměřeno na hrozbu: Phishingové kampaně v ČR

Phishing dlouhodobě představuje jeden z nejčastěji užívaných vektorů kybernetických útoků, čemuž odpovídá i jeho pravidelný výskyt v rámci evidovaných incidentů NÚKIB. Tento vektor může být využíván jak pro jednotlivé útoky, tak i plošně v rámci phishingových kampaní, které se zaměřují na větší množství cílů. V letošním roce NÚKIB zaznamenal těchto plošných phishingových kampaní několik. Zmínit lze například kyberšpionážní kampaně vedené vůči českým a evropským diplomatickým cílům, za kterými dle dostupných informací stáli státem sponzorovaní aktéři (více viz Kybernetické incidenty pohledem NÚKIB – únor a Kybernetické incidenty pohledem NÚKIB – duben).

V červenci NÚKIB zaznamenal další phishingovou kampaň zaměřenou vůči českým cílům, před kterou již varovala společnost Aricoma (dříve AEC). Ta má cílit na řadu subjektů nejen v České republice, ale také ve Francii, Španělsku či Rusku. V rámci této kampaně dochází k rozeslání podvodného e-mailu se škodlivou přílohou. Tato příloha obsahuje odkaz, skrze který dochází ke stažení souboru ZIP obsahující malware Vjw0rm.

Obr. 1: Ukázka phishingového e-mailu dané kampaně



Zdroj: aec.cz

Vjw0rm je veřejně dostupný malware, který se poprvé objevil již v listopadu 2016. Jde o tzv. Remote Access Trojan psaný v jazyce JavaScript, který útočníkovi umožňuje získat vzdálený přístup k zařízení oběti. V minulosti byl Vjw0rm využíván například kyberkriminálními skupinami TA558 či TA2541. NÚKIB v současnosti nedisponuje informacemi, jaký aktér za danou kampaní stojí, což je mimo jiné dáno také veřejnou dostupností malwaru, která ztěžuje následnou atribuci.

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