Nelze zvážit, ale vyplatí se nebrat na lehkou váhu!

31.7.2025 - Tomáš Frolík | Policie ČR

Obezřetnost v kyberprostoru je víc než na místě!

Stejně jako je tomu na celém území České republiky, tak také v Ústeckém kraji došlo ke zhodnocení vývoje bezpečnostní situace v oblasti kybernetické kriminality a ostatní kriminality páchané v kyberprostoru. Oproti roku 2024 došlo k nárůstu této kriminality o 11%. Potvrzuje se trend posledních let a kontinuální nárůst kybernetické kriminality, která tvoří za první pololetí roku 2025 11,5% z celkové kriminality. Pachatelé této trestné činnosti používají důmyslné techniky sociálního inženýrství, phishingu, využívají anonymitu internetového prostoru, důvěřivost a naivnost poškozených. Nejčastější trestní jednání jsou majetkového charakteru. V mnoha případech se jedná o sériové trestné činy, kde pachatelé cílí na celou společnost a útoky automatizují pomocí software. Dokumentace, prověřování a objasňování tohoto druhu kriminality je časově náročná a vyžaduje specifickou kvalifikaci a vybavení policistů. Vyšetřování má mezinárodní přesah, narůstá analytická činnost a forenzní zkoumání nosičů dat. Nejúčinnější zbraní se stále jeví prevence, respektive masové a opakované vzdělávání a informování veřejnosti o tom, jak si počínat bezpečně v prostředí internetu. Vzhledem k dosavadnímu trendu predikujeme, že trestná činnost v oblasti kybernetické kriminality a ostatní kriminality páchané v kyberprostoru, bude v následujících období mírně stoupat a bude se zvyšovat její podíl v celkové kriminalitě.

Něco málo ze statistických údajů. V prvním pololetí roku 2025 byl zaznamenán další nárůst podvodných online útoků o 12%. Pokud jde o útoky na online platební prostředky, došlo k mírnému poklesu, a to o 19,2%. Pokles je zaznamenán také v problematice neoprávněných přístupů do počítačových systémů a útoků na ně, konkrétně o 8,1%. Mravnostní kriminalita naopak výrazně vzrostla o 47,3%. Dále je nutno poukázat na rostoucí počet legalizací výnosů z trestné činnosti o 48,3%. Jde o případy, kdy lidé stále více propůjčují za úplatu své identity a bankovní účty. Řada těchto případů navíc zůstává nepotrestaná, neboť orgány činné v trestním řízení nejsou schopny takovým osobám prokázat úmysl účastnit se na zdrojovém trestném činu, nebo se jakkoliv, byť z nedbalosti, podílet na legalizaci. Dále došlo k výraznému nárůstu násilné kriminality v prostředí internetu, konkrétně u vydírání o 89%, nebezpečné vyhrožování o 58%.

Novými trendy jsou phishingové útoky na platební prostředky a dále metody sociální inženýrství a manipulace osob k vylákání finančních prostředků na základě různých legend. Úspěšnost útoků je založena na důvěřivosti, nepozornosti a lehkomyslnosti poškozených. Současně detekujeme rostoucí agresi v rámci online komunikace a v prostředí sociálních sítí. Alarmující je rovněž rostoucí objem mravnostní kriminality a zneužívání dětí v sexuální oblasti.

Útoky pomocí aplikace Whatsapp - podvodné soutěže a hlasování

V poslední době jsme zaznamenali desítky útoky využívající komunikační aplikaci whatsapp. Modus operandi je založen na tom, že pachatel zašle oběti žádost o hlasování ve fiktivní soutěži, např. krasobruslařské. Součásti zprávy je phishingový odkaz na hlasování, kde si pachatel pod legendou autorizace hlasujícího vynutí zaslání kódu potřebného k převzetí WhatsApp účtu oběti. Tento účet následně převezme a využívá k distribuci podvodných žádostí o krátkodobé půjčky, které pod identitou oběti rozesílá vybraným kontaktům na účtu Whatsapp.

Sociální inženýrství – lákání finančních prostředků pod legendou tísně

Dále detekujeme případy, kdy pachatel rozesílá náhodně zprávy s tím, že se vydává za dceru nebo syna oběti a pod legendou ztráty nebo krádeže telefonu žádá o finanční prostředky na nutné výdaje – úhrada cesty, léčebné výdaje, splatnost pokuty.

Podvodný prodej na online bazarech

Rovněž roste počet případů, kdy si lidé objednají zboží od anonymních nebo nijak neověřených prodejců, dopředu jej uhradí a posléze obdrží balíček s jiným obsahem, nebo neodpovídající kvalitou. Jedná se převážně o přestupkové škody.

Nejčastější odvětví, se kterými se prakticky denně v online prostoru setkáváme:

a) Kybernetická kriminalita
Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230)

Ransomware

Neznámý pachatel prostřednictvím škodlivého software cíleně zašifruje data uložená v interních počítačových sítích různých obchodních korporací, subjektů veřejné správy, či kritické infrastruktury, čímž znemožní činnost takového subjektu, kdy za obnovu dat požaduje výkupné v kryptoměně Bitcoin, případně Monero. Tyto případy jsou spíše latentní a policii nejsou oznamovány. V rámci sledovaného období byl evidován pouze jeden případ.

b) Ostatní kriminalita páchaná v kyberprostoru
Podvody § 209

Evidujeme další nárůst podvodných jednání. V roce 2024 jsme evidovali 443 skutků nyní 496. Tento trend potvrzuje, že pachatelé cílí dominantně na finanční prostředky a majetkový zisk. Útoky na integritu nebo dostupnost dat jsou zanedbatelné.

V rámci nápadu podvodné trestné činnosti nadále evidujeme níže uvedené opakující se modusi operandi.

Podvodný investiční makléř

Pachatel vyvěsí na internet inzerát (reklamu) s nabídkou lákavé investice do kryptoměny, akcií, nebo jiných komodit, spolu s registračním formulářem. Jakmile se poškozený na portál zaregistruje, kontaktuje jej telefonicky falešný investiční makléř, přiměje poškozeného, aby investoval do fiktivní komodity a tím, se obohatí, případně své trestní jednání dále rozvíjí tak, že přiměje poškozeného, aby si do svého mobilu, či počítače instaloval software pro vzdálený přístup. Následně prostřednictvím vzdáleného přístupu vytvoří poškozenému fiktivní investiční účet a přiměje ho, aby „investoval“, nebo přiměje poškozeného, aby se zalogoval do internetbanking s tím, že investici nastaví za něj. Poté převezme kontrolu nad bankovním účtem a zcizí poškozenému dostupné finanční prostředky. Výnosy z trestné činnosti ukrývají do kryptoměn, nebo je legalizují prostřednictvím třetích osob, které jim pod různými legendami poskytnou své bankovní účty. Tyto jsou následně prověřovány pro legalizaci výnosů z trestné činnosti.

Falešný bankéř

Neznámý pachatel telefonicky kontaktuje poškozeného a představí se jako pracovník banky s tím, že banka detekuje pokus o napadení bankovního účtu poškozeného a je nutno co nejdříve všechny peníze z účtu vybrat a uložit na jiný „bezpečný účet“. Dále poškozeného instruuje, aby ihned došel do banky a vybral všechny finanční prostředky. S poškozeným komunikuje z tel. čísla, které odpovídá

číslu banky. Jde však o podvržené číslo (metoda spoofing). Obdobně poškozeného kontaktuje i falešný policista, či falešný bezpečnostní pracovník banky, kteří vše potvrdí, a také volají z podvržených čísel, které odpovídají skutečné bance, či Policie ČR. Jakmile poškozený prostředky vybere, zašle mu pachatel na jeho telefon (obvykle prostřednictvím aplikace WhatsApp) QR kódy, které obsahují adresy anonymních bitcoinových peněženek a poškozeného navede k bitcoinmatu a přesvědčí jej, aby všechny své peníze do bitcoinmatu vložil za pomoci zaslaných QR kódů s tím, že jde o zabezpečený záložní účet. Tím však poškozený přijde o všechny prostředky. Dále jsme u těchto případů zaznamenali nový trend, kdy pachatel nepožaduje vložení prostředků do vkladomatu kryptoměn, nýbrž osobní předání hotovosti „pracovníkovi banky“. Prostředky přebírá osoba, kterou si k tomu účelu pod různou legendou pachatel sjedná. Často jde o osoby cizí státní příslušnosti. Jejich jednání je pak posuzováno jako legalizace výnosu z trestné činnosti, účast na podvodném jednání, nebo je na ně nahlíženo jako na „živý nástroj“ bez trestní odpovědnosti. Dalším trendem je požadavek pachatele k převodu prostředků na „zabezpečený bankovní účet“, který pachateli pod různou legendou zpřístupní třetí osoba. Tyto osoby jsou rovněž posuzovány co do podezření z legalizace výnosu z trestné činnosti.

Podvodný dopravce

Pachatel reaguje na inzerát poškozeného umístěného na portálech „Bazoš, Vinted, apod. s tím, že chce koupit jeho nabízené zboží. Navrhne, že zaplatí přepravní službou PPL, DPD (a jiné), kdy poškozenému zašle prostřednictvím WhatsApp komunikace (či emailu) podvodný odkaz na internetové stránky, které vypadají jako stránky skutečného dopravce, či banky. Zde poškozený v dobré víře vyplní údaje ke své platební kartě, nebo přihlašovací údaje ke svému internetbanking a očekává příchozí platbu, čímž však pachatel získá přístup k jeho platební kartě nebo účtu a prostředky odcizí.

Podvodná nabídka brigády v prostředí internetu

Pachatel v rámci sítě internet nabídne přivýdělek. Nabídka práce spočívá v tom, že zájemce má prohlížet a tzv. lajkovat různé weby, aby zvýšil jejich rating a tím cenu umístěné reklamy. Pachatel takto slibuje přivýdělek v řádech stokorun. V průběhu „spolupráce“ nabídne vyšší odměnu, pokud se zájemce zaregistruje do tzv. „VIP programu“, kdy takto postupně od poškozeného vyláká „registrační poplatky“ v řádech tisíců, slíbený přivýdělek nedodá, tedy poškozeného uvede omyl a sebe tak obohatí.

Podvodné seznámení

Pachatel kontaktuje poškozenou stranu prostřednictvím některé sociální sítě nebo komunikační online platformy, vydává se za „amerického vojáka, lékaře, zaměstnance ropné plošiny, námořní lodi“, apod. Naváže citový vztah, slibuje společnou budoucnost, přičemž pod různými legendami vyláká z oběti finanční prostředky na zahraniční bankovní účty, např. k uhrazení poplatků za převod majetku do ČR, vyřízení dědictví, vyvázání se služby, podplacení úředníků za účelem vycestování do ČR, opravy lodi, operace, apod.

V rámci pohybu v kyberprostoru je dobré řídit se těmito základními preventivními pravidly:
Používejte kvalitně zabezpečený počítač, notebook, telefon!
Nedůvěřujte všem informacím, které naleznete na internetu, nejedná se vždy o pravdivé informace!
Vždy si chraňte soukromí a nikdy nesdělujte žádné PIN kódy, bezpečnostní kódy, ověřovací kódy!
Nikdy neodesílejte fotografie své platební karty či osobních dokladů. Nikomu! Ani nikomu, kdo tvrdí, že je z Vaší banky!

Bankovní instituce takové informace po svých klientech NIKDY nepožadují!
Nenechte se oklamat sliby virtuálních útočníků (dárky, peníze, vztah, láska apod.)!
Nikdy nevybírejte veškeré své úspory z účtu a nevkládejte je na neznámý účet!
Telefonické hrozby informující o napadení vašeho účtu a nutící vás k nelogickým finančním transakcím jsou vždy podvodem!
Ověřujte žádosti o peníze! Pokud vám někdo z blízkých napíše žádost o peníze, vždy si tuto žádost ověřte jiným způsobem, ideálně telefonickým hovorem nebo osobním setkáním!
Buďte obezřetní při neobvyklých požadavcích! Pokud zpráva přichází v nestandardní češtině, v noci, nebo obsahuje neobvyklou výzvu k poslání peněz, zbystřete!
Chraňte své účty, používejte dvoufázové ověření na všech sociálních sítích a komunikačních aplikacích, které tuto funkci umožňují!
Nesdílejte ověřovací kódy! Nikdy nesdílejte ověřovací SMS kódy, které vám přijdou na telefon!
Nebojte se nevhodnou komunikaci ukončit a říci jasné NE!

A nezapomínejte na to, že prevence byla, je a bude klíčem k Vašemu bezpečí!!!

31. 7. 2025
kpt. Mgr. Tomáš Frolík
Oddělení tisku a prevence
KŘP Ústeckého kraje

https://policie.gov.cz/clanek/nelze-zvazit-ale-vyplati-se-nebrat-na-lehkou-vahu.aspx