RANSOMWARE

Nedávne prípady a odporúčania ako postupovať v prípade incidentu

Ján Doboš
jan.dobos@nbu.gov.sk

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Cieľ prezentácie

- ransomware sa týka každého z nás
- rôznorodosť a najčastejšie vektory prieniku a spôsobov detekcie
- najčastejšie nedostatky zasiahnutých subjektov a ďalšie zaujímavosti z riešenia incidentov
- kľúčové komponenty incident handling-u v prípade ransomware

2021-2023 - Hlásené KBI - Kategorizácia podľa ZoKB

	2021	2022	2023
Dobrovoľné	878	1135	948
Kategória I	22	20	19
Kategória II	11	8	4
Kategória III	1	7	3
CELKOM	**912**	**1 170**	**974**

- V porovnaní so zahraničnými štatistikami relatívne malé čísla
- Viditeľné nedostatky v nesprávnej alebo chýbajúcej klasifikácii KBI
- Obraz “zrelosti” organizácií v oblasti KB

Nebojte sa incidenty hlásiť

Prehlbujte spoluprácu v oblasti výmeny informácií o incidentoch a IOC

2021-2023 - Hlásené KBI - Technický typ (TOP 5)

2021		2022		2023	
Získavanie informácií	431	Získavanie informácií	582	Získavanie informácií	611
Zraniteľnosť	104	Zraniteľnosť	169	Nedostupnosť	88
Nedostupnosť	86	Škodlivý kód	106	Prienik do systému	64
Prienik do systému	59	Prienik do systému	89	Škodlivý kód	49
Pokus o prienik	53	Nedostupnosť	72	Zraniteľnosť	46
Ostatné	179	Ostatné	152	Ostatné	116
CELKOM	**912**	**CELKOM**	**1 170**	**CELKOM**	**974**

Distribúcia typológie pokrýva najčastejšie vektory prieniku pri ransomware

P01 ISP

Spôsob detekcie: náhodné výpadky služieb, následné odhalenie súborov s podozrivými príponami

Rozsah a dopady: virtualizačná platforma, interné systémy, samoobslužné zákaznícke systémy

Zálohy: dostupné a nezasiahnuté

Spôsob riešenia

- **kto:** interne, externe
- **ako:** izolácia, kompletná reinštalácia, detailná analýza a nasadenie dodatočných bezpečnostných prvkov a procesov

P01 ISP

Právne úkony: podané trestné oznámenie

Vektor prieniku: zneužitie prihlasovacích údajov do VPN a MFA bombing

Zistenia, zaujímavosti

- šifrovanie v prvotnej fáze spôsobovalo výpadky služieb, ktoré boli riešené ako prevádzkový incident
- napriek existencii procesov pre riešenie ransomwaru vznikol chaos, lebo postupy neboli dostatočne nacvičené a infraštruktúra je komplexná
- v infraštruktúre pôsobila skupina útočníkov - experti aj menej zdatní
- ukážkovo zvládnutá mediálna komunikácia

P01 ISP

Zistenia, zaujímavosti

- zdroje sú limitované bez ohľadu na veľkosť subjektu
  - krízové riadenie v istom bode riešenia incidentu uprednostnilo obnovu systémov a služieb pred časovo náročným zaistením vzoriek malwaru
  - zákaznícka škoda minimálna, enormné náklady spojené s operatívnymi úkonmi počas riešenia incidentu a obnovou do pôvodného stavu
- incident cielený pôvodne na sesterskú spoločnosť a nasadené protiopatrenia spôsobili presmerovanie útočníka

P02 Ministerstvo

Spôsob detekcie: spomalenie pracovnej stanice a následné odhalenie súborov so zvláštnou príponou

Rozsah a dopady: 1 server a 9 desktopov

Zálohy: dostupné a nezasiahnuté

Spôsob riešenia

- **kto:** interne
- **ako:** izolácia, reinštalácia, dodatočné opatrenia, poučenie zamestnancov

P02 Ministerstvo

Externá komunikácia: sektorový a národný CSIRT

Vektor prieniku: nedodržanie interných pravidiel organizácie zamestnancom, stiahnutie škodlivého kódu

Zistenia, zaujímavosti

- prvotne infikované zariadenie bolo zapojené do domény, čo umožnilo šírenie
- analýza rodiny malwaru odhalila, že sa šíri prostredníctvom nelegálneho softvéru
- rôzne AV riešenie mali rôzne výsledky detekcie

P02 Ministerstvo

Zistenia, zaujímavosti

- nekontrolované pripojenie osobných zariadení do služobnej siete (USB, zdieľanie internetového pripojenia z mobilu)
- sťahovanie a inštalácia nelegálneho softwaru na služobné zariadenia
- prístup na webové stránky s pochybnou reputáciou
- vyvodenie disciplinárneho konania voči zamestnancovi

P03 Vzdelávacia inštitúcia

Spôsob detekcie: problému s dostupnosťou mailových služieb, až následne bol odhalený ransomnote

Rozsah a dopady: databázy, servery, koncové stanice

Zálohy: dostupné, ale zasiahnuté šifrovaním

Spôsob riešenia

- **kto:** interne, externí dodávatelia, súdny znalec
- **ako:** prebudovanie infraštruktúry

P03 Vzdelávacia inštitúcia

Externá komunikácia: zamestnanci, študenti, partneri, médiá

Právne úkony: podané trestné oznámenie

Leakpage, komunikácia s útočníkom: leakpage

Vektor prieniku: predmet znaleckého skúmania

Zistenia, zaujímavosti

- šifrovanie spustené mimo pracovných hodín (03:00)
- extrémne komplexné a heterogénne prostredie: rôzne platformy, študenti, dodávatelia, partnerské organizácie
- subjekt bol prekvapený, že vzorka ransomware nebola rozpoznaná AV riešením (signatúry, deaktivácia komponentov útočníkom)

P03 Vzdelávacia inštitúcia

Zistenia, zaujímavosti

- subjekt si bol vedomý viacerých nedostatkov infraštruktúry a až incident využil na ich odstránenie pri budovaní novej infraštruktúry
- subjekt si neuvedomoval aspekt, že v vo väčšine prípadov samotnému šifrovaniu predchádza aktivita útočníka
- subjekt sa priamo pustil do obnovy infraštruktúry, bez zistenia vektoru prieniku
- ransomvérová skupina aktívna na leakpage a aj sociálnych sieťach, videoanalýzy exfiltrovaných súborov - objednávky, osobné údaje, mailová komunikácia
- dodávateľ AV riešenia bol schopný dešifrovať časť zasiahnutých súborov

P04 Financie, účtovníctvo, audity a poradenstvo

Spôsob detekcie: nedostupnosť súborov, odhalenie README ransomnotu zamestnancami

Rozsah a dopady: sharepoint, filesharing, e-maily

Spôsob riešenia

- **kto:** externe
- **ako:** zamedzenie šírenia, obnova, dodatočné zabezpečenie

P04 Financie, účtovníctvo, audity a poradenstvo

Externá komunikácia: voči zákazníkom

Leakpage, komunikácia s útočníkom: útočník pri komunikácii poskytol zoznam exfiltrovaných súborov

Vektor prieniku: nezdieľané s odvolaním na prebiehajúce trestné konanie

Zistenia, zaujímavosti

- ransomnote tejto skupiny obsahoval zoznam infikovaných hostov a typológiu exfiltrovaných dát a prihlasovacie údaje do komunikačného portálu
- počas riešenia incidentu došlo k nahratiu vzoriek a ransomnote na VirusTotal
- zákazníci sa dopytovali CSIRT jednotiek ohľadom IOC

“Organizovaný chaos”

- chýbajúci asset management
- útočník je živý organizmus
- zraniteľnosti a nesprávna konfigurácia
- nedostatočné logovanie a absencia bezpečnostných prvkov
- ľudský faktor a OPSEC pri riešení incidentu
- komunikačná stratégia
- atď.

Komplexnosť ransomwarových incidentov a limitované zdroje organizácie priamo implikujú potrebu existencie procesov, metodík a best practice postupov pre obdobie PRED, POČAS a PO incidente.

Incident, incident handling

- Incident
  - akákoľvek udalosť s negatívnym vplyvom na kybernetickú bezpečnosť…
    - …porušenie triády CIA, bezpečnostnej politiky alebo záväznej metodiky
  - môže nastať bez ohľadu na preventívne kroky vykonané organizáciou
- Incident handling
  - proces ako incident vyriešiť a obnoviť pôvodný stav
    - prvotné zhodnotenie a kategorizácia, zastavenie prebiehajúceho útoku, obnova do pôvodného stavu, identifikácia vektora prieniku a útočníka, implementácia protiopatrení
  - komunikácia, eskalačné procesy

Buďte pripravení !!!

Analýza, plánovanie, realizácia

- krátke časové obdobie na prvotné zhodnotenie situácie, návrh a implementáciu postupov na zvládnutie incidentu
- konajte rozvážne a s kľudom (obzvlášť v prípadoch, ktoré nepokrývajú existujúce metodiky) a svoj postup dokumentujte
  - analýza
  - plánovanie
    - pomocné faktory: procesy, asset management, znalosť infraštruktúry, sieťovej topológie a bezpečnostných prvkov
  - realizácia
  - dokumentácia

Komunikácia

- nezanedbajte ani jeden zo smerov komunikácie
- mimoriadny význam má komunikácia s externými tímami CSIRT a národnou jednotkou CSIRT
  - praktické skúsenosti: procesné postupy, technické aspekty riešenia
  - off-site/on-site participácia (koordinácia/analýza/obnova)
  - neznalosť aktuálneho stavu incidentu, infraštruktúry a procesov organizácie
    - pomocné faktory: ransomnote, prípona a vzorky šifrovaných súborov, rozsah a dopady incidentu, základné informácie o infraštruktúre (technológie, verejne dostupné služby a komponenty) a vykonaných krokoch

Kľúčové komponenty IH v prípade ransomware

- kombinácia všeobecnej metodológie pre riešenie KBI s postupmi potrebnými pre zvládnutie špecifických problémov súvisiacich s ransomware

- **Zamedzenie šírenia** (Containment)
- **Zaistenie digitálnych stôp** (Digital evidence collection)
- **Bezpečná obnova** (Remediation and Recovery)
  - infraštruktúra, služby, aplikácie
  - dáta
  - zamedzenie opätovného výskytu incidentu a zvýšenie celkovej úrovne bezpečnosti

- **Analytické činnosti** (Analysis)
  - špecifické postavenie, prebiehajú súbežne s ostatnými fázami

Zamedzenie šírenia

- kritický krok z pohľadu minimalizácie škôd a limitovania aktivity útočníka v infikovanej infraštruktúre
- identifikácia a izolácia potenciálne zasiahnutých komponentov
  - špecifické kroky závislé od operatívneho stavu incidentu, pripravenosti infraštruktúry a existencie procesov, plánov a metodík
  - pamätajte, že platí Locardov princíp vzájomnej výmeny

Plán obnovy

- stanovené kroky môžu byť vykonávané súbežne
- najdôležitejšie kroky
  - zaisťovanie digitálnych stôp a forenzných artefaktov, zálohovanie obrazov diskov
  - bezpečná obnova infraštruktúry
    - nové zariadenia
    - zaručene neinfikované
    - riadená reinštalácia zariadení, na ktorých skončili predchádzajúce body
    - hardening a security best practices
  - analytické činnosti
    - na zozbieraných dôkazoch alebo zariadeniach, kde skončilo zaisťovanie stôp

Zaistenie digitálnych stôp

- kritické z pohľadu
  - dôkazového materiálu v prípadnom trestnom konaní
  - detailnej analýzy incidentu s cieľom identifikácie prvotného vektora prieniku, priebehu útoku a modusu operandi útočníka
  - možnosti obnovy dát
- súdny znalec, špecialista CSIRT, iná poverená osoba (podľa pokynov)
- musí byť systematické, presne zdokumentované a využitím bezpečnostnou komunitou uznávaných nástrojov
  - RAM, HDD zasiahnutých systémov
  - logy zo sieťových, bezpečnostných a iných monitorovacích prvkov
  - metadáta k zaisteným stopám

Bezpečná obnova

- vybudovanie novej infraštruktúry dodržaním postupov na elimináciu rizika prenosu a opakovanej infekcie
- základné zásady
  - oddelené sieťové segmenty
  - unikátne a silné heslá (pozor na recykláciu hesiel v infikovanom prostredí)
  - plná reinštalácia systémov a aplikácií z dôveryhodných zdrojov
  - aktualizácia a aplikovanie bezpečnostných záplat
  - hardening systému
  - kontrola a riadené obnovovanie dát aj z bezpečnej zálohy
  - špeciálnu kapitolu tvoria zásady interakcie s infikovanými zariadeniami a pre záchranu súborov v nich uložených
  - atď. (viď. časť “Pred incidentom”)

Špecializované analytické činnosti

- forenzná analýza, malwarová analýza, OSINT analýza, threat intelligence, obohacovanie a korelácia dát a mnoho ďalších činností
  - určenie vektora prieniku, časovej os incidentu, modusu operandi útočníka, použitých nástrojov, indikátorov kompromitácie (IOC), techník, taktík a procedúr útočníka (TTP)
  - analýza možností obnovy zasiahnutých dát (dešifrovanie, obnova zo zaistených stôp)
  - identifikácia typu a rozsahu potenciálne/reálne exfiltrovaných dát
- komunikácia s útočníkom
  - bližšia špecifikácia rozsahu exfiltrovaných údajov
  - získanie dodatočných IOC (kryptopeňaženky, e-maily a iné)
  - proces koordinovať s vedením, právnym oddelením, CSIRT a OČTK
  - dešifrovanie vybraných vzoriek
  - za špecifických podmienok kompletné dešifrovanie (nemocnice počas COVID pandémie)

Špecializované analytické činnosti

- návrh opatrení na minimalizáciu možností zneužitia exfiltrovaných dát
  - zmena hesiel a kryptografického materiálu
  - revokácia prístupov
  - zabezpečenie aktív, ku ktorým by mohol útočník získať prístup
  - komunikácia zistení podľa schválenej komunikačnej stratégie

Po incidente…

- Report
  - dokumentuje incident, jeho priebeh, riešenie a zistenia
- Kontinuálna potreba zlepšovať sa
  - Čo sme mohli vykonať lepšie a efektívnejšie?
  - Ako zabezpečiť, aby sa podobný incident nezopakoval?
  - Čo nemáme? Čo je potrebné zaobstarať a zabezpečiť?
  - Čo je potrebné zaviesť?
- Dodatočný monitoring leakpages, všeobecných informácií ohľadom ransomware a informácií ohľadom konkrétnej rodiny ransomwaru
  - zamedzenie rôznych foriem rizika
  - obnova časti zasiahnutých súborov
    - dekryptor
    - zverejnenie dát

ransomware.sk-cert.sk

Ján Doboš
jan.dobos@nbu.gov.sk

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI