

Doporučení k ransomware

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

10. února 2021, Brno
TLP: WHITE

Martin Knotek
Odbor Vládní CERT
Oddělení analytické

Úvod



- Ransomware je stále ransomware
- Změna v postupech útočníků
- Od rozsáhlých útoků skrz e-mailové přílohy
- Cílem uživatel a jeho stanice
- K ručním a cíleným postupům
- Cílí konkrétní uživatele nebo firmy
- Prolomení perimetru
 - RDP, přihlašovací údaje, zranitelnosti, ...
- Identifikace a ovládnutí hodnotných systémů
 - DC, webserver, zálohy, ...
- Smazání stop a zašifrování
 - V noci, o víkendu



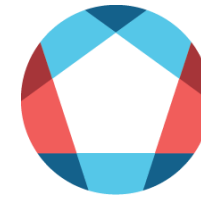
Aktuální stav ransomware

- Trendy ve světě
 - Extortion attack, RaaS, Cloudy
- Starý dobrý RDP
 - Používaný či zapomenutý
 - Oblíbený nejenom pro ransomware
- Další služby
 - Webové servery, VPN, ...
- Přihlašovací údaje
- Populární cíle – nemocnice
 - Přístup k datům, vytížení
- Vzorky
 - Buran, Dharma a další

Doporučení k ransomware



- Cílová skupina
 - Zejména ministerstva, úřady, ...
 - Lze uplatnit kdekoli
- Nejedná se o
 - Návodů k zařízením
 - Manuál nebo nastavení konkrétního řešení
- Preventivní opatření
 - Zálohování, segmentace, ...
- Reaktivní opatření
 - Izolace systémů, odpojení komunikace



NAKIT

Národní agentura pro
komunikační a informační
technologie, s. p.





Preventivní opatření

Zálohování

- Odděleno od produkční sítě
- Ideálně zálohující server přistupuje ke klientovi
- Oddělení účtů pro zálohy od administrátorských
- Aktualizace
- Testování záloh



Preventivní opatření

Segmentace

- Komplikuje šíření
- No-go „plochá“ síť
- Rozdělení na více částí
 - Zálohy, administrace, servery, ...
- Komunikační whitelist (allowlist)
 - Definují s čím může stanice komunikovat



Preventivní opatření

Aktualizace a služby

- Aktualizovat
 - Nejenom OS, ale i další SW
- Kontrolovat otevřené služby a porty
 - Zmenšíme riziko průniku útočníka
- Princip need-to-have
 - Vypneme co nepotřebujeme
 - Co potřebujeme skryjeme za VPN (+2FA)
- Často zneužívané služby
 - RDP, SMB, telnet, ssh+heslo
- PenTest CERT
 - Skenování sítě a zranitelností

Preventivní opatření



E-mailly

- Přílohy emailů
 - Velmi populární vektor útoku
- Maximální omezení maker
 - Úplný zákaz, příp. podepisování
- Omezení obsahu příloh
 - Spustitelné soubory, skripty

Uživatelé

- Běžná práce = běžná práva
 - Omezit použití admin práv
- Restrikce spouštěných souborů
 - SRP, Applocker
- Vzdělávání uživatelů
 - Otevírání emailů a příloh
 - Klikání na odkazy
- Hesla
 - Správce hesel, 2FA



Preventivní opatření

Logy

- Zásadní pro efektivní reakci
 - Skvělý zdroj informací
- V ideálním případě použít log management
 - Ukládat na jiný stroj
 - Útočník může mazat stopy
- Příklady:
 - Přihlášení, odhlášení
 - Přihlášení admina
 - Spuštěné procesy
 - ...

Reakce na útok



- Odpojit zálohy od sítě
- Omezit komunikaci mezi stroji
 - Panic mode na FW
 - V krajním případě odstavit od el. energie
- Odpojit komunikaci od veřejné sítě
- Pozastavit VM
- Zjistit rozsah napadení
 - Dokumentovat
- Neplatit výkupné
 - Nepodporujeme útočníky
- Kontaktovat Policii, poté NÚKIB

Co pro nás může NÚKIB udělat



- <https://www.nukib.cz/>
- Metodická pomoc
 - Doporučení
 - Pomoc s dotazy
- Sběr dat na místě a jejich analýza
- Konzultace obnovení infrastruktury
 - Pro regulované subjekty
- Analýza incidentu
 - Identifikace vektorů útoku
 - Zpětná vazba
 - Prevence dalšího incidentu



Martin Knotek

Referent bezpečnosti státu, Vládní CERT

Email: m.knotek@nukib.cz

Telefon: +420 607 013 729