TLP:CLEAR

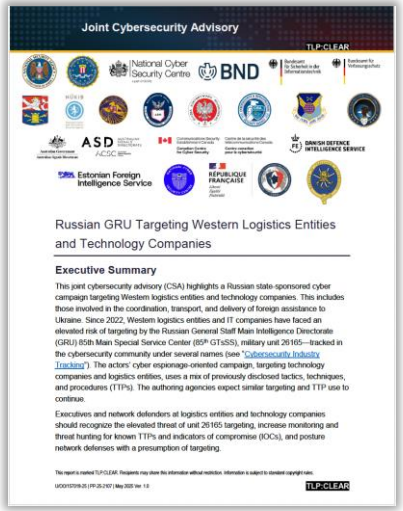
(veľmi živé)
skúsenosti z incidentov

Milan Pikula
National Cyber Security Center
National Security Authority, Slovakia

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Prípad 1 – aktivity GRU a kamery na hraniciach

- vyšiel dokument “Ruská GRU cieli na západnú logistiku”
  - “klasické” spear phishingové aktivity
  - kamery na hraniciach a logistických uzloch
- “klasické aktivity”
  - indikátory z reportu sme spárovali s množstvom našich incidentov,
    - viac než polovicu z nich sme už mali interne pripísaných tomuto aktérovi
    - zvyšné sme stotožnili
- kamery
  - cielené varovanie na zraniteľné sektory a subjekty
  - bolo treba kontaktovať partnerov so žiadosťou o detaily
    - využili sme podporu špeciálneho vyslanca NBÚ pre vo Washingtone pre KB


Joint Cybersecurity Advisory

TLP:CLEAR

Russian GRU Targeting Western Logistics Entities and Technology Companies

Executive Summary

This joint cybersecurity advisory (CSA) highlights a Russian state-sponsored cyber campaign targeting Western logistics entities and technology companies. This includes those involved in the coordination, transport, and delivery of foreign assistance to Ukraine. Since 2022, Western logistics entities and IT companies have faced an elevated risk of targeting by the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (85th GTsSS), military unit 26165—tracked in the cybersecurity community under several names (see "Cybersecurity Industry Tracking"). The actors' cyber espionage-oriented campaign, targeting technology companies and logistics entities, uses a mix of previously disclosed tactics, techniques, and procedures (TTPs). The authoring agencies expect similar targeting and TTP use to continue.

Executives and network defenders at logistics entities and technology companies should recognize the elevated threat of unit 26165 targeting, increase monitoring and threat hunting for known TTPs and indicators of compromise (IOCs), and posture network defenses with a presumption of targeting.

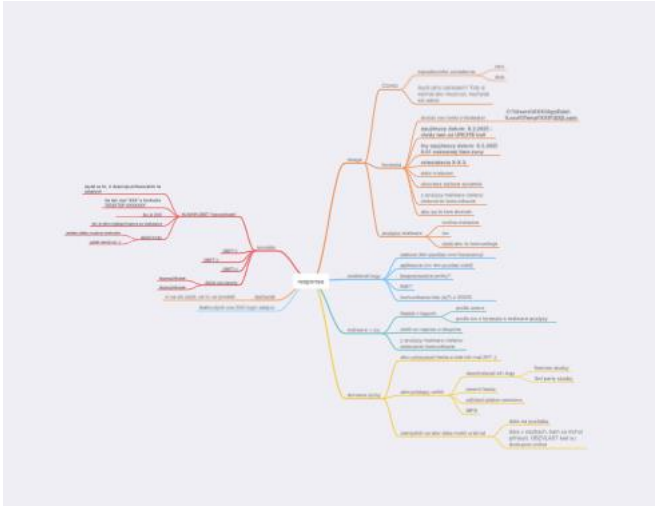
TLP:CLEAR

Prípad 2 – JISKB a väčší ransomvérový incident

- nahlásený aj koordinovaný cez JISKB
- prebieha forenzia a analýza malvéru
  - na základe ransomnote identifikovaná skupina
  - potvrdené analýzou
    - z počítača vytiahnutá vzorka malware
    - sedia TTP (správanie, nástroje, všetko)

- informácie neboli členené a vkladané tam, kam by mali patriť
  - incident handler musel skákať hore-dole aby spravil chronológiu
  - poznámky boli dokonca aj v timeline logu o incidente
- prosím, hláste incidenty ale venujte pozornosť aj vypĺňaniu

Prípad 3 – JISKB a infostealer



- únik prihlasovacích údajov do JISKB cez infostealer a predaj na dark webe
  - štyri rôzne e-mailové adresy, tri subjekty
  - JISKB je Jednotný systém kybernetickej bezpečnosti, prístup tam majú MKB a štatutári
- prvý pohľad
  - predaj od 02/2025
  - adresy súvisia, traja sú štatutári, jeden je MKB
  - podľa formátu dát predpokladáme Lumma Stealer
  - login MKB do JISKB z troch SK adries (jedna “domáca”), štatutári žiadny prístup
  - urobili sme “veľký plán”

Prípad 3 – JISKB a infostealer

- urobili sme “veľký plán”
- …a potom prišiel telefonát
  - ”o napadnutom zamestnancovi vieme, to je vyriešené”
    - ale boli ste to vy?!
  - “objavilo sa mi nečakane prihlasovacie okno, prihlásil som sa, počítač bol zrazu pomalší” – “heslo sme zmenili a preinštalovali sme počítač”
  - prečo ste nehlásili incident?
  - ”no… ani mi nenapadlo.”
  - leaknutých cca. 300 prihlasovacích údajov. Dúfam, že ich pomenil všetky… kopec vecí už sa nikdy nedozvieme.
- hláste incidenty, dobre vám radím

TLP:CLEAR

(veľmi živé)
skúsenosti z incidentov

Milan Pikula
National Cyber Security Center
National Security Authority, Slovakia

SK NBÚ CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI