DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

ALERTĂ
25.02.2022

UNCLASSIFIED / NECLASIFICAT

HermeticWiper malware

Un nou malware destructiv numit **HermeticWiper (alias KillDisk.NCV)** este folosit activ în contextul escaladării conflictului militar din **Ucraina** pentru atacuri cibernetice care au ca țintă organizații guvernamentale și private, afectând factori de decizie, personal tehnic dar și utilizatori obișnuiți.

HermeticWiper este un executabil mic, de aproximativ 115KB, semnat digital cu un certificat emis către "Hermetica Digital Ltd" și valabil în perioada aprilie 2021 - aprilie 2022.

Malware-ul se folosește de un driver legitim (asociat cu software-ul EaseUS Partition Master) pentru a corupe datele de pe harddisk-uri, inclusiv zona MBR (Master Boot Record). Pasul final al atacului cu **HermeticWiper** este inactivarea computer-ului victimă prin repornirea acestuia.

Atacurile cu **HermeticWiper** au fost cel mai probabil pregătite cu câteva luni în avans, atacatorii obținând acces la rețelele / infrastructura victimelor încă din noiembrie 2021, exploatând inițial vulnerabilități cunoscute ale serverelor **Microsoft Exchange** sau **Apache Tomcat**.

Accesul inițial a fost, de obicei, urmat de furt de credențiale de acces, mișcare laterală și web shells. **HermeticWiper** se propagă la nivel de **Active Directory** prin intermediul **Group Policy Objects (GPO).** Aceasta este o indicație a faptului că atacul este inițiat când atacatorii au preluat deja controlul parțial sau complet asupra rețelei / infrastructurii informatice.

Până în acest moment, Directoratul nu a înregistrat la nivelul României atacuri **HermeticWiper**.

RECOMANDĂRI

- Creați, actualizați, întrețineți și exersați periodic capacitățile de răspuns la incidente cibernetice, precum și planurile de continuitate și reziliență în cazul pierderii accesului sau controlului rețelei / infrastructurii informatice.
- Revizuiți strategia de back-up implementată la nivel de organizație, având în vedere că datele afectate / șterse de **HermeticWiper** nu pot fi recuperate.
- Aplicați imediat update-urile de securitate necesare pentru software-ul utilizat, în special pentru serverele **Microsoft Exchange** sau **Apache Tomcat**.
- Urmăriți indicatorii de compromis (IOC) **HermeticWiper** pe care Directoratul i-a inclus în această alertă sau cei comunicați de furnizorii de soluții de securitate cibernetică.
- Urmăriți, în paralel cu indicatorii de compromis **HermeticWiper**, și indicatorii de compromitere de rețea (de tip IP sau domenii) pentru care recomandăm includerea acestora în listele de tip threat intelligence ale echipamentelor de securitate din cadrul organizației dumneavoastră.
- Folosiți un scanner de IOC-uri (cum ar fi „LOKI Open-Source IOC Scanner”) pentru a automatiza monitorizarea indicatorilor de compromis în cadrul infrastructurii IT.

- Monitorizați atent fluxurile de date și componentele interconectate direct cu parteneri ucraineni și/sau situate în rețelele ucrainene, dar și celelalte conexiuni către exterior.
- Aplicați principiul celui mai mic privilegiu pentru toate sistemele cheie cu posibilitate de acces la distanță pe care le gestionați.
- Contactați imediat Directoratul, în cazul în care ați fost afectați de un atac cu **HermaticWiper**.

Indicatori de compromis (IOC)

- **SHA256 malware:**
  1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
  0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
  a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e
  3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
  2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf

- **SHA256 drivere EaseUS:**
  b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
  b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
  e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
  fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
  8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
  23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
  96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
  2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d

- **Certificat digital:**
  Nume: Hermetica Digital Ltd
  Thumbprint: 1AE7556DFACD47D9EFBE79BE974661A5A6D6D923
  Serial Number: 0C 48 73 28 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC

alerts@dnsc.ro

Telefon 1911

#DNSC #alert #cybersecurity #HermeticWiper