Raport consolidat eveniment cibernetic

Lynx Ransomware

Lynx Ransomware reprezintă o amenințare cibernetică avansată care compromite confidențialitatea, integritatea și disponibilitatea datelor printr-un atac structurat ce implică exfiltrarea și criptarea informațiilor sensibile ale victimelor. Utilizând tehnici precum phishing, exploatarea RDP și atacuri asupra lanțului de aprovizionare, ransomware-ul afectează în principal platformele Windows, vizând organizații din multiple sectoare. În lipsa măsurilor adecvate de securitate, atacatorii reușesc să paralizeze operațiunile organizațiilor, cerând plăți de răscumpărare și amenințând cu publicarea datelor exfiltrate.

Informații suplimentare

TIP	Lynx funcționează ca un Ransomware-as-a-Service (RaaS), permițând afiliaților să-l distribuie prin diverse metode, cum ar fi e-mailuri de phishing și descărcări malițioase.
Impact	Lynx utilizează o strategie de dublă extorcare, exfiltrând date sensibile înainte de a le cripta, amenințând cu publicarea acestora dacă nu se plătește răscumpărarea.
Vectori de atac	❖ **Phishing:** Lynx Ransomware utilizează phishing-ul ca metodă principală de livrare. E-mailurile conțin atașamente malițioase în formate precum *.zip, .exe* sau documente *Microsoft Office* cu macro-uri malițioase. Linkurile direcționează victimele către site-uri de tip watering-hole sau kituri de exploatare. ❖ **Exploatarea RDP (Remote Desktop Protocol):** Sistemele expuse cu credențiale slabe pentru RDP sunt o altă țintă comună, ransomware-ul utilizând *brute force* pentru acces. ❖ **Actualizări compromise:** În cazuri mai rare, Lynx a fost distribuit prin compromiterea lanțului de aprovizionare (supply chain), în special în software utilizat pe scară largă.

Mecanisme de persistență	Lynx implementează diverse tehnici pentru a rămâne persistent în sistem: • **Modificarea Registry:** Creează chei în HKCU\Software\Microsoft\Windows\CurrentVersion\Run pentru a executa ransomware-ul la pornirea sistemului. • **Task Scheduler:** Programează o sarcină Windows care execută ransomware-ul în mod periodic. • **Injectarea în procese legitime:** Injectează cod malițios în procese legitime pentru a evita detectarea de către soluțiile antivirus.
Reguli YARA	c02b014d88da4319e9c9f9d1da23a743a61ea88be1a389fd6477044a53813c72 1.exe hXXp://lynxblog.net/ **#YARA rules** rule ransomware_LYNX_1 { meta: description = "Detecteaza LYNX ransomware" author = "DNSC" date = "2024-12-10" hash1 = "c02b014d88da4319e9c9f9d1da23a743a61ea88be1a389fd6477044a53813c72" strings: $s1 = "[+] Successfully decoded readme!" fullword ascii $s2 = "[-] Failed to get service information for %s: %s" fullword wide $s3 = "--file C:\\temp.txt,D:\\temp2.txt" fullword ascii $s4 = "--file C:\\temp.txt" fullword ascii $s5 = "AppPolicyGetProcessTerminationMethod" fullword ascii $s6 = "[-] Failed to open service manager for %s: %s" fullword wide $s7 = "[-] Failed to open service handle for %s: %s" fullword wide $s8 = "[-] Failed to enum dependent services for %s: %s" fullword wide $s9 = "[-] Failed to kill dependent services for %s: %s" fullword wide $s10 = "[%s] Try to stop processes via RestartManager" fullword wide $s11 = "[%s] Kill processes and services" fullword wide $s12 = "Load hidden drives (will corrupt boot loader)" fullword ascii $s13 = "README.txt" fullword wide $s14 = "[-] Failed to mount %s: %s" fullword wide

```
      $s15 = "[-] Failed to decode readme: %s" fullword ascii
      $s16 = "Try to stop processes via RestartManager" fullword ascii
      $s17 = "Kill processes/services" fullword ascii
      $s18 = "--stop-processes " fullword ascii
      $s19 = "--stop-processes" fullword wide
      $s20 = "[%s] Encrypt network shares" fullword wide
      $op0 = { e8 22 c8 01 00 01 46 30 6a 00 11 56 34 6a 13 ff }
      $op1 = { 23 d1 89 55 d0 8b 55 e4 81 f2 ff ff ff 03 f7 d2 }
      $op2 = { 23 d1 89 55 d4 8b d7 81 f2 ff ff ff 01 f7 d2 8b }

   condition:

      uint16(0) == 0x5a4d and filesize < 500KB and
      ( 8 of them and all of ($op*) )
}
rule ransomware_LYNX_2 {
   meta:
      description = "Detecteaza LYNX ransomware"
      score = 80
            md5 = "2E8607221B4AB0EB80DE460136700226"
   strings:
      $s1 = "tarting full encryption in" wide
      $s2 = "oad hidden drives" wide
      $s3 = "ending note to printers" ascii
      $s4 = "uccessfully delete shadow copies from %c:/" wide
      $op1 = { 33 C9 03 C6 83 C0 02 0F 92 C1 F7 D9 0B C8 51 E8 }
      $op2 = { 8B 44 24 [1-4] 6A 00 50 FF 35 ?? ?? ?? ?? 50 FF 15}
      $op3 = { 57 50 8D 45 ?? C7 45 ?? 00 00 00 00 50 6A 00 6A 00 6A 02 6A 00 6A 02 C7 45 ?? 00 00 00 00 FF D6 FF 75 ?? E8 ??
?? ?? ?? 83 C4 04 8B F8 8D 45 ?? 50 8D 45 ?? 50 FF 75 ?? 57 6A 02 6A 00 6A 02 FF D6 }
      $op4 = { 6A FF 8D 4? ?? 5? 8D 4? ?? 5? 8D 4? ?? 5? 5? FF 15 ?? ?? ?? ?? 85 C0 }
      $op5 = { 56 6A 00 68 01 00 10 00 FF 15 ?? ?? ?? ?? 8B F0 83 FE FF 74 ?? 6A 00 56 FF 15 ?? ?? ?? ?? 68 88 13 00 00 56 FF 15
?? ?? ?? ?? 56 FF 15}
   condition:
      uint16(0) == 0x5A4D and
      (
         3 of ($s*)
```

	or 3 of ($op*) or (2 of ($s*) and 2 of ($op*))) }
Metode avansate de detecție	✓ **Instrumente de detecție dinamică:** Utilizați platforme EDR (Endpoint Detection and Response) capabile să observe comportamentele anormale, cum ar fi: • Crearea excesivă de fișiere .tmp. • Ștergerea copiilor shadow (comanda: *vssadmin delete shadows*). ✓ **Analiza hash-urilor și semnăturilor:** Actualizați bazele de date antivirus cu hash-uri cunoscute asociate Lynx. ✓ **Honeypot-uri:** Configurați honeypot-uri pe servere pentru a detecta mișcările laterale și încercările de criptare.
Analiză comportamentală la criptare	• **Criptare secvențială:** Lynx scanează structura directorului și criptează fișierele într-o ordine logică, prioritizând fișierele de dimensiuni mari și cele utilizate frecvent. • **Evitarea fișierelor critice:** În unele cazuri, ransomware-ul evită fișierele sistemului de operare pentru a permite dispozitivului să rămână funcțional și să afiseze nota de răscumpărare. • **Note de răscumpărare:** Lynx plasează un fișier text denumit tipic README_TO_DECRYPT.txt, care conține detalii despre plată și adresele Bitcoin.
Posibilități de decriptare	✓ **Informații pentru decriptare:** În absența unei soluții de decriptare disponibile public, este recomandat să monitorizați: • **NoMoreRansom Project:** (nomoreransom.org) - pentru soluții viitoare. • Forumurile de securitate, cum ar fi BleepingComputer, pentru anunțuri privind eventualele instrumente de decriptare. ✓ **Analiză propriu-zisă a cheilor:** Dacă ransomware-ul utilizează algoritmi simetrici (AES), capturați cheia din memorie în timpul criptării utilizând instrumente precum Volatility sau Process Hacker.
Măsuri avansate de remediere	• **Segmentarea rețelei:** Limitați propagarea ransomware-ului segmentând rețelele interne. Utilizați VLAN-uri pentru a separa serverele critice de sistemele mai vulnerabile. • **Liste albe pentru aplicații:** Permiteți rularea doar a aplicațiilor autorizate pentru a bloca executabilele ransomware. • **Audituri de securitate:** Implementați politici stricte de audit pentru a detecta accesul neautorizat sau încercările de exfiltrare a datelor.

	• **Analiza traficului rețelei:** Utilizați un SIEM (Security Information and Event Management) pentru a monitoriza și alerta pe activități neobișnuite, cum ar fi fluxuri mari de date către adrese externe.

Resurse externe

- https://www.nextron-systems.com/2024/10/11/in-depth-analysis-of-lynx-ransomware/
- https://blogs.blackberry.com/en/2024/10/lynx-ransomware
- https://dnsc.ro/citeste/alerta-lynx-ransomware-indicators-of-compromise-iocs
- https://unit42.paloaltonetworks.com/inc-ransomware-rebrand-to-lynx/