|  |  |  |
| --- | --- | --- |
| **ALERTĂ 14.02.2024**NECLASIFICAT/UNCLASSIFIED | **Backmydata Ransomware** **Indicators of Compromise (IOCs)** | Icon  Description automatically generated |

În cursul nopții de 11 spre 12 februarie 2024 a avut loc un atac cibernetic de tip ransomware asupra companiei Romanian Soft Company (RSC) [www.rsc.ro](http://www.rsc.ro) care dezvoltă, administrează și comercializează sistemul informatic **Hipocrate (alias HIS)**. Conform datelor DNSC, atacul a perturbat activitatea a **26 spitale din România** care utilizează sistemul informatic **Hipocrate**.

Malware-ul utilizat în cadrul atacului este **aplicația** **ransomware Backmydata** care face parte din **familia de malware Phobos**, cunoscută pentru propagarea prin conexiuni de tip **Remote Desktop Protocol (RDP).** **Backmydata** este conceput pentru a cripta fișierele țintei vizate utilizând un algoritm complex. Fișierele criptate sunt redenumite cu extensia **.backmydata**. După criptare, malware-ul furnizează **două note de răscumpărare** (**info.hta** și **info.txt**) cu detalii despre pașii de urmat pentru contactarea atacatorilor și stabilirea detaliilor pentru plata răscumpărării.

**IOCs validați cu spitalele la data de 14.02.2024**

La nivelul DNSC sunt în proces de validare o serie suplimentară de IOCs ce vor fi publicați curând.

**Hashes**

396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6 **AntiRecuvaDB.exe**

70211a3f90376bbc61f49c22a63075d1d4ddd53f0aefa976216c46e6ba39a9f4 **kprocesshacker.sys**

**#YARA rules**

rule Phobos\_CrypterBinary\_DNSC {

 meta:

 description = "Phobos Ransomware Crypter Binary"

 author = "Directoratul National de Securitate Cibernetica (DNSC)"

 date = "2024-02-12"

 hash1 = "396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6"

 strings:

 $s1 = "\\.#\* 0\_" fullword ascii

 $s2 = "9F:b:{:" fullword ascii

 $s3 = "D$(Y\_^[" fullword ascii

 $s4 = "tEWVVVV" fullword ascii

 $s5 = "YSVWj(j" fullword ascii

 $s6 = "^yMQb O8y" fullword ascii

 $s7 = "tjWWVhKE@" fullword ascii

 $s8 = "D$LPVVVWVVV" fullword ascii

 $s9 = "D$PPSj" fullword ascii

 $s10 = "YY9\\$0t" fullword ascii

 $s11 = "8$8/8|8" fullword ascii

 $s12 = "SVWj23" fullword ascii

 $s13 = "\\\\?\\X:" fullword wide

 $s14 = "\\\\?\\ :" fullword wide

 $s15 = "\\\\?\\UNC\\\\\\e-" fullword wide

 $s16 = "D$HY\_^[" fullword ascii

 $s17 = "L{gYm+" fullword ascii

 $s18 = "2\*262H2Q2^2j2" fullword ascii

 $s19 = "9\\$Pt." fullword ascii

 $s20 = "Y9\\$4t&9\\$Xt " fullword ascii

 $op0 = { 53 e8 34 7d 00 00 59 89 45 dc 8d 45 cc 50 68 06 }

 $op1 = { 39 5c 24 34 74 0a 39 5c 24 44 0f 84 af }

 $op2 = { 6a 18 c7 46 34 00 00 01 00 c7 46 30 00 00 10 00 }

 $ap0 = "MPR.dll" fullword ascii

 $ap1 = "WS2\_32.dll" fullword ascii

 $ap2 = "WINHTTP.dll" fullword ascii

 $ap3 = "KERNEL32.dll" fullword ascii

 $ap4 = "USER32.dll" fullword ascii

 $ap5 = "ADVAPI32.dll" fullword ascii

 $ap6 = "SHELL32.dll" fullword ascii

 $ap7 = "ole32.dll" fullword ascii

 $ap8 = "GetTickCount" fullword ascii

 $ap9 = "GetIpAddrTable" fullword ascii

 condition:

 uint16(0) == 0x5a4d and filesize < 200KB and

 ( 8 of them and all of ($op\*) and all of ($ap\*) )

}

rule kprocesshacker\_Phobos\_DNSC {

 meta:

 description = "Phobos kprocesshacker.sys"

 author = "Directoratul National de Securitate Cibernetica (DNSC)"

 date = "2024-02-14"

 hash1 = "70211a3f90376bbc61f49c22a63075d1d4ddd53f0aefa976216c46e6ba39a9f4"

 strings:

 $x1 = "d:\\projects\\processhacker2\\kprocesshacker\\bin\\amd64\\kprocesshacker.pdb" fullword ascii

 $x2 = "kprocesshacker.sys" fullword wide

 $s3 = ":http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl0O" fullword ascii

 $s4 = ":http://crl4.digicert.com/DigiCertHighAssuranceEVRootCA.crl0@" fullword ascii

 $s5 = "\\Device\\KProcessHacker3" fullword wide

 $s6 = "KProcessHacker" fullword wide

 $s7 = "www.digicert.com1503" fullword ascii

 $s8 = "http://ocsp.digicert.com0R" fullword ascii

 $s9 = "Fhttp://cacerts.digicert.com/DigiCertSHA2HighAssuranceCodeSigningCA.crt0" fullword ascii

 $s10 = "\*http://crl3.digicert.com/sha2-ha-cs-g1.crl00" fullword ascii

 $s11 = "\*http://crl4.digicert.com/sha2-ha-cs-g1.crl0L" fullword ascii

 $s12 = "DynamicConfiguration" fullword wide

 $s13 = "Sydney1" fullword ascii

 $s14 = "\\CDvQbX/0" fullword ascii

 $s15 = " Microsoft Code Verification Root0" fullword ascii

 $s16 = "SHA256" fullword wide /\* Goodware String - occured 507 times \*/

 $s17 = "New South Wales1" fullword ascii /\* Goodware String - occured 1 times \*/

 $s18 = "CIQh't%" fullword ascii

 $s19 = "DigiCert, Inc.1\*0(" fullword ascii

 $s20 = "Licensed under the GNU GPL, v3." fullword wide

 $op0 = { 8c 99 00 00 58 20 00 00 c0 90 }

 $ap0 = "PsGetCurrentProcessId" fullword ascii

 $ap1 = "SePrivilegeCheck" fullword ascii

 $ap2 = "PsInitialSystemProcess" fullword ascii

 $ap3 = "ZwQuerySystemInformation" fullword ascii

 condition:

 uint16(0) == 0x5a4d and filesize < 100KB and

 ( 1 of ($x\*) and 4 of them and all of ($op\*) and all of ($ap\*))

}

**RECOMANDĂRI**

Directoratul recomandă cu fermitate ca nimeni să nu plătească răscumpărarea către atacatori!

Folosirea indicatorilor de mai sus pentru scanarea infrastructurii IT&C de către toate entitățile din domeniul sănătății, indiferent dacă au fost sau nu afectate de atacul ransomware Backmydata.

**alerts@dnsc.ro**

**Telefon 1911**

#DNSC #alert #cybersecurity #awareness