DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

ALERT
16.02.2024

UNCLASSIFIED

Backmydata Ransomware Indicators of Compromise (IOCs) UPDATE

During the night of 11 to 12 February 2024 there was a ransomware cyber-attack on the Romanian Soft Company (RSC) www.rsc.ro, which develops, manages and markets the Hippocrates computer system (a.k.a. HIS). According to DNSC data, the attack disrupted the activity of 26 Romanian hospitals using the Hippocrates IT system.

The malware used in the attack is **Backmydata ransomware application** that is part of the **Phobos malware family**, known for propagating through **Remote Desktop Protocol (RDP)** connections. **Backmydata** is designed to encrypt target files using a complex algorithm. Encrypted files are renamed with **.backmydata** extension. After encryption, the malware provides two ransom notes (**info.hta** and **info.txt**), with details of the steps to be taken for contacting the attackers and how to pay the ransom.

The Directorate recommends to all healthcare entities, whether or not they have been affected by the Backmydata ransomware attack, to scan their IT &C infrastructure using the YARA scanning script.

IOCs validated with hospitals at 16.02.2024

DNSC is currently in the process of validating a new series of IOCs which will be published soon.

Hashes

396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6 **AntiRecuvaDB.exe**
70211a3f90376bbc61f49c22a63075d1d4ddd53f0aefa976216c46e6ba39a9f4 **kprocesshacker.sys**
6606d759667fbdfaa46241db7ffb4839d2c47b88a20120446f41e916cad77d0b **dControl.exe**
b4cc0280e2caa0335361172cb7d673f745defc78299ded808426ffbc2458e4d9 **DotNetTools.dll**
61e8cd8de80a5c0d7ced280fe04ad8387a846a7bf2ee51bcbba96b971c7c1795 **ExtendedNotifications.dll**
5ae7c0972fd4e4c4ae14c0103602ca854377fefcbccd86fa68cfc5a6d1f99f60 **ExtendedServices.dll**
f2805e0f81513641a440f1a21057a664961c22192cb33fca3870362c8f872d87 **ExtendedTools.dll**
acd49f2aa36d4efb9c4949e2d3cc2bd7aee384c2ced7aa9e66063da4150fcb00 **HardwareDevices.dll**
85aba198a0ba204e8549ea0c8980447249d30dece0d430e3f517315ad10f32ce **hydra.exe**
476aa6af14dd0b268786e32543b9a6917a298d4d90e1015dac6fb2b522cf5d2e **NetworkTools.dll**
7336d66588bbcfea63351a2eb7c8d83bbd49b5d959ba56a94b1fe2e905a5b5de **OnlineChecks.dll**
4259e53d48a3fed947f561ff04c7f94446bedd64c87f52400b2cb47a77666aaa **peview.exe**
bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4 **ProcessHacker.exe**
8bae7326cb8456ce4c9409045264ca965e30f6381ddcaa6c87ba3ac5e7683555 **pw-inspector.exe**
57c56f7b312dc1f759e6ad039aac3f36ce5130d259eb9faad77239083398308b **SbieSupport.dll**
5713d40dec146dbc819230daefe1b886fa6d6f6dbd619301bb8899562195cbab **ToolStatus.dll**
0c11cdc3765ffb53ba9707b6f99ec17ae4f7334578a935ba7bcbbc9c7bdeed2e **Updater.dll**
fc9d0d0482c63ab7f238bc157c3c0fed97951ccf2d2e45be45c06c426c72cb52 **UserNotes.dll**
282696487ea5dc781788d5d8477b977f72b7c70f201c2af0cfe7e1a9fd8d749a **WindowExplorer.dll**
e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b **BulletsPassView64.exe**
b19dfe440e515c39928b475a946656a12b1051e98e0df36c016586b34a766d5c **BulletsPassView.exe**
c4304f7bb6ef66c0676c6b94d25d3f15404883baa773e94f325d8126908e1677 **ChromePass.exe**
598555a7e053c7456ee8a06a892309386e69d473c73284de9bbc0ba73b17e70a **Dialupass.exe**
dbe98193aced7285a01c18b7da8e4540fb4e5b0625debcfbabcab7ea90f5685d **iepv.exe**
16c6af4ae2d8ca8e7a3f2051b913fa1cb7e1fbd0110b0736614a1e02bbbbceaf **mailpv.exe**
d032001eab6cad4fbef19aab418650ded00152143bd14507e17d62748297c23f **mimidrv_32.sys**
d43520128871c83b904f3136542ea46644ac81a62d51ae9d3c3a3f32405aad96 **mimidrv.sys**
66b4a0681cae02c302a9b6f1d611ac2df8c519d6024abdb506b4b166b93f636a **mimik_32.exe**

31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc **mimik.exe**
a6527183e3cbf81602de16f3448a8754f6cecd05dc3568fa2795de534b366da4 **mimilib_32.dll**
59756c8f4c760f1b29311a5732cb3fdd41d4b5bc9c88cd77c560e27b6e59780c **mimilib.dll**
b42725211240828ccc505d193d8ea5915e395c9f43e71496ff0ece4f72e3e4ab **mimilove_32.exe**
7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26 **mspass.exe**
6a87226ed5cca8e072507d6c24289c57757dd96177f329a00b00e40427a1d473 **netpass64.exe**
de374c1b9a05c2203e66917202c42d11eac4368f635ccaaadf02346035e82562 **netpass.exe**
91041b616969e1526ee6dce23f8d18afdd353786ac6afa0b6611903263ee6f63 **NetRouteView.exe**
8e4b218bdbd8e098fff749fe5e5bbf00275d21f398b34216a573224e192094b8 **OperaPassView.exe**
04cc60eba7041e0cef2deb1bec9a087432344737dd2e5141c9cda981506ca1a5 **pars.vbs**
7fee96ae0ed1972a80abbd4529dc81ec033083857455bbf3c803c4f47e1ac31c **PasswordFox64.exe**
e01b0e7feadd08a7ea87c1cde44e7b97daf9632eaee8311ef6967f33258d03c1 **PasswordFox.exe**
64788b6f74875aed53ca80669b06f407e132d7be49586925dbb3dcde56cbca9c **pspv.exe**
5e85446910e732111ca9ac90f9ed8b1dee13c3314d2c5117dcf672994ce73bd6 **PstPassword.exe**
205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964 **rdpv.exe**
ae474417854ac1b6190e15cc514728433a26cc815fdc6d12150ef55e92d643ea **RouterPassView.exe**
c92580318be4effdb37aa67145748826f6a9e285bc2426410dc280e61e3c7620 **SniffPass64.exe**
1e13fd79ad54fe98e08d9ffca2c287a470c50c2876608edce2fe38e07c245266 **SniffPass.exe**
816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019 **VNCPassView.exe**
b556d90b30f217d5ef20ebe3f15cce6382c4199e900b5ad2262a751909da1b34 **WebBrowserPassView.exe**
48b77c1efbc3197128391a35d0e1ed0b5cc3a05b96dd12c98ac73ffc6a886fc8 **WirelessKeyView64.exe**
12f13d129579c68ec3cc05bef69880b6a891296fa9fce69b979b1c04998f125c **WirelessKeyView.exe**

#YARA rules

1. A complex set of YARA rules have been published on DNSC website:

https://www.dnsc.ro/vezi/document/yara-scan-dnsc-v101

2. Instructions for using the YARA rules script:
    a. Download and save locally the "**YARA-Scan_DNSC-v101.zip**" archive from the link above
    b. Extract the archive in the desired folder
    c. Run the "**scanare-drive-C-backmydata.bat**" script with administrator rights to start the scan (NOTE: Right-click on the script and select “Run as administrator”)
    d. Optionally, if it is necessary and applicable, also run the script "**scanare-drive-D-backmydata.bat**"
    e. Check the generated messages in the terminal and the **.txt** file in the “Logs” directory
    f. In case of malware files detected, please send the **.txt** file to DNSC at alerts@dnsc.ro

OTHER RECOMMENDATIONS

The Directorate firmly recommends that no one pays the ransom or get in touch with the attackers!

alerts@dnsc.ro

Phone 1911

#DNSC #alert #cybersecurity #awareness