Repeated HTTP POST requests to "/usaherds/Logon.aspx" • fileupload.aspx within .\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET • Files\usaherds\c99cd219\8fb4a6b8 • App_Web_egdio02m.dll within .\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary • ASP.NET Files\usaherds\c99cd219\8fb4a6b8 • t.dll within .\Users\Public • ntuser.dll.zip within .\TEMP • cmqpxyxl within .\Windows\Temp • t.dll.zip within .\TEMP • cmxnot1n within .\Windows\Temp • 1pkub5lt within .\Windows\Temp • x.dll.zip within .\TEMP • versions.txt within \Sites\USAHerds\usaherds\versions.txt

- Change rights to process C:\windows\system32\spoolsv.exe

- W3WP.exe->ipconfig /all

- W3WP.exe->netstat -ano -p tcp

- Reg save hklm\sam C:\ProgramData\SAM

- Reg save hklm\system C:\ProgramData\SYSTEM

- Dropped files in C:\programdata including users.dat Domains • Time12[.]cf

- Afdentry.workstation.eu[.]org – KEYPLUG C2 IPs

- 192.155.81[.]36 – download malicious tools and exfiltrate files

- 104.18.6[.]251 – download malicious tools and exfiltrate files

- 139.59.248[.]56 – used to download malicious tools and exfiltration

- 104.18.7[.]251 – C2 destination10 • 34.139.13[.]46 – Exploit source • 104.16.0[.]0/13 – Remote subnet

Possible IPs associated with intrusion (possibly recon or secondary exploit sources):

- 172.104.46[.]213

- 138.124.180[.]203

- 34.117.254[.]173

- 34.120.57[.]236

- 34.120.243[.]77

- 34.98.122[.]108

- 34.120.85[.]253

• 104.149.134[.]38 – C2 destination

• 8.46.116[.]152 – Exploit source (Cloudflare) File Names • SymEFASI.dat (Keyplug – dropped in C:\programdata\symefasi\) • a.exe (Bat2Exe – creates a scheduled task for Keyplug and executes it) • b.exe (Bad Potato) • s.exe (SweetPotato) • h.exe (Potato)

• dwn.exe (unknown)

• ff.DAT (unknown)

• pa.DAT (unknown)

• s.dat (unknown)

• shark.dat (unknown)

• shark2.dat (unknown)

• x64.dll (unknown)

• USOShared.xlm (unknown) Hashes MD5 • c4bbab6d0b96a0ca7f8d520675bd273d • eeddaaa11fa7231a8f4016d43530bf77 10 At a point in time, the IP was involved with malicious activities and then recycled by the threat actor, thus no longer being used related to the malicious activity described. As has been reported in previous intelligence analysis, threat actors have been known to use cloud services in U.S. availability zones to minimize suspicion of threat actor network traffic.

• 143278845a3f5276a1dd5860e7488313 – BADPOTATO • 069a5b09fb66a4c6cf0f62dab4e76220 • Da89dcefcde116e4c9569f6d367e3c73 – Dropper • f8eefd05b03055d2beccdde299086328 • dbf0bf5264ce164cd02c2da7e0151ec6

• 139dbb1cb6a292abe2b162179d7e6c56 – Webshell

• 17851fbe051ba87664447e17e1e3ef61 – DEADEYE

• 1f18fef3235774187ab98acc7936d1c2 – DEADEYE

• 258fd54579185c08b3dd14ea3deec991 – DEADEYE

• 3f812f8f759c82bd8c313103ea02ea63 – LOWKEY

• 4d866a6d8aeb677a9592f0b40f3f328a – KEYPLUG

• 623edb0c7cb9b811544c38027b7e3e58 – MIMIKATZ

• 7f46277080e124b34f5887449db6a5f4 – KEYPLUG

• b5aa4107a1feec9707a1f6f26886fa6d – KEYPLUG

- e34f8c9044120d6149aca99658131d1d – DEADEYE

- ebcf7556224f4fe8a726d2eb85b589cf – KEYPLUG

- f35b410326f97ef995a865b464141d3e – Unknown

- c843b00b8e0ab346c558ce4894600183 – Unknown SHA1 • d5bedeb401a84070a460409a19929acaaeead892 • 57b2c1299d79892fe313fd62428226ccbf2fc376 • 6f6b51e6c88e5252a2a117ca1cfb57934930166b • 4edcec79780cde00df3fdac9b40a70106c3a8de5 • Df01f4aae885eb8126b91da7bdaa7d94696d0943

- 12aa9d56903f57df3802a9c79107ea9c s-1-5-18 – DEADEYE SHA256 • fbef9a5d1337c6ce979d31ca1411456ab5e5938a8a593436b6c91409a3c4436a • b6488338d74248096eef15ce58bde96a13a8bd805f3ff76da679b5ef9728e7a8 • a4647fcb35c79f26354c34452e4a03a1e4e338a80b2c29db97bba4088a208ad0 • 0b7b1988a07d1a7ea4b545cc97a360d1bd59c3c37a425fe30746de4278642b18 • d5b216bdd2782228c53fccc35ec661965b04c52bf6586571523f2c8781d20e94