Indicator	Type	Description
Spinstall0.aspx	File name	Web shell used by threat actors Actors have also modified the file name in a variety of ways – such as *spinstall.aspx* , *spinstall1.aspx* , *spinstall2.aspx*
IIS_Server_dll.dll	File name	Storm-2603 IIS Backdoor
SharpHostInfo.x64.exe	File Name	Pentest tool observed during attack that is used to collect host information using NetBIOS, SMB, and WMI
xd.exe	File Name	Fast reverse proxy tool used to connect to C2 IP 65.38.121[.]198
debug_dev.js	File name	File containing web config data, including MachineKey data
\1[5-6]\TEMPLATE\LAYOUTS\debug_dev.js	File path	File path for stolen web configs
92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514	SHA-256	Hash of *spinstall0.aspx*
24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf	SHA-256	Web shell that leverages http & curl to receive and execute commands from Storm-2603 C2 "*update[.]updatemicfosoft[.]com*"
b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0	SHA-256	Web shell that leverages sockets & DNS to receive and execute commands from Storm-2603 C2 *"update[.]updatemicfosoft[.]com"*
c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94	SHA-256	Web shell that leverages sockets & DNS to receive and execute commands from Storm-2603 C2 *"update[.]updatemicfosoft[.]com"*
1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192	SHA-256	Web shell that leverages sockets & DNS to receive and execute commands from Storm-2603 C2 *"update[.]updatemicfosoft[.]com"*
4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)

7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
6f6db63ece791c6dc1054f1e1231b5bbcf6c051a49bad0784569271753e24619	SHA-256	Observed hash for *IIS_Server_dll.dll* (Storm-2603 IIS Backdoor)
d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d	SHA-256	Hash for *SharpHostInfo.x64.exe*
62881359e75c9e8899c4bc9f452ef9743e68ce467f8b3e4398bebacde9550dea	SHA-256	Hash for *xd.exe*
4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030	SHA-256	.NET module - initial hash observed
b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70	SHA-256	.NET module
fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7	SHA-256	.NET module - targeting ViewState
390665bdd93a656f48c463bb6c11a4d45b7d5444bdd1d1f7a5879b0f6f9aac7e	SHA-256	.NET module
66af332ce5f93ce21d2fe408dffd49d4ae31e364d6802fff97d95ed593ff3082	SHA-256	.NET module
7baf220eb89f2a216fcb2d0e9aa021b2a10324f0641caf8b7a9088e4e45bec95	SHA-256	.NET module
c34718cbb4c6.ngrok-free[.]app/file.ps1	URL	Ngrok tunnel delivering PowerShell to C2

msupdate[.]updatemicfosoft[.]com	URL	C2 domain for Storm-2603
131.226.2[.]6	IP	Post exploitation C2
134.199.202[.]205	IP	IP address exploiting SharePoint vulnerabilities
104.238.159[.]149	IP	IP address exploiting SharePoint vulnerabilities
188.130.206[.]168	IP	IP address exploiting SharePoint vulnerabilities
65.38.121[.]198	IP	Post-exploitation C2 for Storm-2603
107.191.58[.]76	IP	Exploitation Source
96.9.125[.]147	IP	Exploitation Source
139.144.199[.]41	IP	Exploitation Source
89.46.223[.]88	IP	Exploitation Source
45.77.155[.]170	IP	Exploitation Source
95.179.158[.]42	IP	Exploitation Source
154.223.19[.]106	IP	Exploitation Source
185.197.248[.]131	IP	Exploitation Source
149.40.50[.]15	IP	Exploitation Source