April 20, 2023

TRIGONA RANSOMWARE | IOCs

IOC	Note
bef87e4d9fcaed0d8b53bce84ff5c5a70a8a30542100ca6d7822cbc8b76fef13	svhost.exe (Ransomware Binary)
853909af98031c125a351dad804317c323599233e9b14b79ae03f9de572b014e	Splashtop
24123421dd5b78b79abca07bf2dac683e574bf9463046a1d6f84d1177c55f5e5	Netscan
4724EE7274C31C8D418904EE7E600D92680A54FECDAC28606B1D73A28ECB0B1E	Netscan
e22008893c91cf5bfe9f0f41e5c9cdafae178c0558728e9dfabfc11c34769936	Netscan
8d069455c913b1b2047026ef290a664cef2a2e14cbf1c40dce6248bd31ab0067	Netscan
544a4621cba59f3cc2aeb3fe34c2ee4522593377232cd9f78addfe537e988ddc	start.bat
a15c7b264121a7c202c74184365ca13b561fb303fb8699299039a59ab376adc6	turnoff.bat
b7fba3abee8fd3bdac2d05c47ab75fdaa0796722451bed974fb72e442ab4fefd	newuser.bat
e5cf252041045b037b9a358f5412ae004423ad23eac17f3b03ebef7c8147a3bb	Mimikatz
5603d4035201a9e6d0e130c561bdb91f44d8f21192c8e2842def4649333757ab	Mimikatz
69f245dc5e505d2876e2f2eec87fa565c707e7c391845fa8989c14acabc2d3f6	Mimikatz
94979b61bba5685d038b4d66dd5e4e0ced1bba4c41ac253104a210dd517581b8	DC2.exe
9c8a4159166062333f2f74dd9d3489708c35b824986b73697d5c34869b2f7853	DC4.exe
c5d09435d428695ce41526b390c17557973ee9e7e1cf6ca451e5c0ae443470ca	DC6.exe
3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion	Trigona TOR negotiation portal
248e7d2463bbfee6e3141b7e55fa87d73eba50a7daa25bed40a03ee82e93d7db	File-based IOC
596cf4cc2bbe87d5f19cca11561a93785b6f0e8fa51989bf7db7619582f25864	File-based IOC
704f1655ce9127d7aab6d82660b48a127b5f00cadd7282acb03c440f21dae5e2	File-based IOC
859e62c87826a759dbff2594927ead2b5fd23031b37b53233062f68549222311	File-based IOC
8f8d01131ef7a66fd220dc91388e3c21988d975d54b6e69befd06ad7de9f6079	File-based IOC
97c79199c2f3f2edf2fdc8c59c8770e1cb8726e7e441da2c4162470a710b35f5	File-based IOC
a86ed15ca8d1da51ca14e55d12b4965fb352b80e75d064df9413954f4e1be0a7	File-based IOC
accd5bcf57e8f9ef803079396f525955d2cfffbf5fe8279f744ee17a7c7b9aac	File-based IOC
da32b322268455757a4ef22bdeb009c58eaca9717113f1597675c50e6a36960a	File-based IOC
e7c9ec3048d3ea5b16dce31ec01fd0f1a965f5ae1cbc1276d35e224831d307fc	File-based IOC
e97de28072dd10cde0e778604762aa26ebcb4cef505000d95b4fb95872ad741b	File-based IOC
f29b948905449f330d2e5070d767d0dac4837d0b566eee28282dc78749083684	File-based IOC

fa6f869798d289ee7b70d00a649145b01a93f425257c05394663ff48c7877b0d	File-based IOC
fbba6f4fd457dec3e85be2a628e31378dc8d395ae8a927b2dde40880701879f2	File-based IOC
fd25d5aca273485dec73260bdee67e5ff876eaa687b157250dfa792892f6a1b6	File-based IOC
c7a930f1ca5670978aa6d323d16c03a97d897c77f5cff68185c8393830a6083f	Dropper (svcservice.exe)
fb128dbd4e945574a2795c2089340467fcf61bb3232cc0886df98d86ff328d1b	Ransomware (svchost.exe)
19667eba21a1caefda0a23cb43bdcb09070944e7cf7e3c2c11de1ba036677f09	CLR Shell
09a5f38e6d534378583eb30ac6d893211983367cb0e01b58a11ef8933eb1f9a0	nt.exe
1e71a0bb69803a2ca902397e08269302	Batch Runner (svchost.bat)
45.227.253[.]99	IP address associated with Trigona activity
45.227.253[.]106	IP address currently hosting Trigona leak site
45.227.253[.]98	IP address associated with Trigona activity
45.227.253[.]107	IP address associated with Trigona activity
phandaledr@onionmail[.]org	Ransom note contact email
farusbig@tutanota[.]com	Ransom note contact email
how_to_decrypt.hta	Ransom note name

*** Please see the below-listed sources for context and a complete list of Indicators.**

Source(s):

[1] https://asec.ahnlab.com/en/51343/
[2] https://unit42.paloaltonetworks.com/trigona-ransomware-update/
[3] https://www.fortinet.com/blog/threat-research/ransomware-roundup-trigona-ransomware/
[4] https://www.extrahop.com/company/blog/2023/trigona-ransomware-uses-password-protected-malware/
[5] https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/