GrayBird/Colony - Pastebin.com

Archived: 2026-04-05 22:22:01 UTC

1. Downloader – Onlineinstaller.exe
2. MD5 bfd15475fdc15373622a7ad6c8736c1d
3. SHA1 cc3ba347b80b2bf849a75dd1256e57fe32139f1d
4. SHA256 bd43289d2e616c78c9d5807b6c2f57028cd3d23aebc4111d7d689493b8c8c87a
5.
6. services (name->path): amdfx -> C:\Windows\system32\drivers\amdfx.sys
7. services (name->path): mrxsmb22 -> C:\Windows\system32\drivers\mrxsmb22.sys
8. registry (key->data): HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\mrxsmb22\ImagePath -> system32\drivers\mrxsmb22.sys
9.
10. \Registry\Machine\System\CurrentControlSet\Services\amdfx
11. \Registry\Machine\System\CurrentControlSet\Services\mrxsmb22
12.
13. Check-in URL: http://iostream.system.band/dump/io/time.php
14. Download URL 1: http://ozkngbvcs.bkt.gdipper.com/xp/aXXXX
15. Download URL 2: http://ozkngbvcs.bkt.gdipper.com/xp/mXXXX
16.
17. Driver – mrxsmb22.sys
18. MD5 eb5591fc8979bfe67a19643a07397882
19. SHA1 08b067821535eaa99dd4f53866245784ffd3ed62
20. SHA256 5589a6960e76c4ccab41a834d41ee85180366f80968a92316148a734ceff9cc4
21.
22. Driver - amdfx.sys

23. MD5 e6b26e97a9186835ffbc7f1a2f433bbc
24. SHA-1 a4ef575f40a7e9634dbbb8dde7860e22145a2a9e
25. SHA-256 079daa5aa34c717308dd5792b88f604b904355f32f9e2b738855ad725d9deb45
26.
27.
28. Decrypt downloader check-in
29.
30. MD5(first 8 bytes of packet + hard-coded 8 byte string), AES-128-CBC. In every case I've seen so far, the hard-coded string is '1Q2a3k79'. The following is sufficient:
31.
32. 00000000: 4136 3946 4339 3344 4558 2b37 6262 4247 A69FC93DEX+7bbBG
33. 00000010: 5064 7339 524c 3474 344f 7362 4367 4867 Pds9RL4t4OsbCgHg
34. 00000020: 6834 484e 7877 6865 5947 732f 4272 436f h4HNxwheYGs/BrCo
35. 00000030: 3254 2b47 4977 4342 706f 4957 6544 416d 2T+GIwCBpoIWeDAm
36. 00000040: 7a67 4132 5363 7068 3758 3872 6d47 6f66 zgA2Scph7X8rmGof
37. 00000050: 6668 4c55 774a 624b 512b 7545 7634 766b fhLUwJbKQ+uEv4vk
38. 00000060: 5263 434b 3061 4e2b 6d65 6d71 3374 4845 RcCK0aN+memq3tHE
39. 00000070: 6454 4b6f 516a 7949 4c4f 4c6d 7533 6c62 dTKoQjyILOLmu3lb
40. 00000080: 6758 6c78 5061 4474 gXlxPaDt
41.
42. echo -n "A69FC93D1Q2a3k79" | md5sum
43. cat enc-traffic-1.bin | base64 -d | openssl enc -d -aes-128-cbc -K 'd3b56154ff02575f7d7502445878ccf4' -iv 0
44.
45. 00000000: 7561 3d35 322d 3534 2d30 302d 3441 2d41 ua=52-54-00-4A-A
46. 00000010: 442d 3231 2667 6574 3d42 5326 6c61 6e67 D-21&get=BS&lang
47. 00000020: 3d55 2e53 2672 6567 696f 6e3d 3130 2672 =U.S&region=10&r

48. 00000030: 6566 6572 7265 723d 756e 6b6e 6f77 266f eferrer=unknow&o
49. 00000040: 733d 5769 6e64 6f77 7337 2037 3630 3126 s=Windows7 7601&
50. 00000050: 6272 6f77 7365 723d 4368 726f 6d65 browser=Chrome
51.
52.
53. Seems it first appeared around December 2017 - also seems to be some slight confusion. Both of the drivers use Netfilter SDK which is a networking framework that consists of both kernel mode and user mode components, their files are already picked up as AdWare/PUA/PUP and as far as I could tell, had been detected as such for a long time before this appeared.
54. https://forums.malwarebytes.com/topic/217148-30tab-adware-mrxsmb22-need-fixlist-help/
55. https://forums.malwarebytes.com/topic/217215-adwarenetfilter-30tabcom-adware/
