

Winnti is Coming - Evolution after Prosecution@HITCON2021

Archived: 2026-04-06 01:14:32 UTC

Since APT41 was sued by the FBI last year, the group has not disappeared. Instead, they have used more innovative and less well noticed techniques to evade detection by security products, such as:

- Avoiding memory detection through dll hollowing technique
- Using DPAPI to encrypt the real payload to make forensics more difficult.
- Abusing the certificate to hide the payload in a signed PE file.
- Using domain fronting techniques to hide the real IP address.
- Using legitimate tools like InstallUtil to execute code and bypass application whitelisting.

In addition to malware that is known to be used by APT41 , we also found some newly developed malware. There are two new pieces of listening port malware. We also found a shellcode-based backdoor, Natwalk.

The group is also more careful in their usage of C2. They use DNS tunnelling extensively as well as Cloudflare Worker to hide their real C2 IP.

We have observed that APT41 targeted telecommunications companies, key medical institutions, governments, and major infrastructures in various countries in 2021.

The prosecution did not deter them, but instead prompted them to evolve their attack techniques, and make it harder for researchers to track and detect.

In this talk we will provide more details about the campaigns of APT41 , including its innovative TTPs, newly developed malware, lateral movement techniques, and the strategies they used for C2 after they were sued by the FBI.

We also research the relation of the subgroups under APT41, like fishmaster and GroupCC.



Transcript

1. [Winnti is Coming - Evolution after Prosecution TeamT5](#)
- 2.
- 3.
4. [Who is Winnti? 4 https://twitter.com/jfslowik/status/1420924040047337474](https://twitter.com/jfslowik/status/1420924040047337474)

5. [Winnti? APT41? 5 Ministry of State Security of the People's](#)

Republic of China(MSS) • Winnti = APT41 ? • APT41 = Chengdu404 ? • Under APT41, it can be divided into several groups via different techniques and targets • The targets are very wide. It is suspected that MSS has integrated the resources, attack techniques, and tools to make this group looks bigger. APT41 APT10 APT17 APT... Integration? Fishmaster /TAG-22 GroupCC Amoeba Unknown Group ...

6. [Target Country Talk in last section 6](#)

7.

8. [Compromise Winnti is Coming - Evolution after Prosecution](#)

9.

10. [Webshell Access 10](#)

11. [Probe plugin 11](#)

12. [Webshell Upload 12](#)

13. [Catalina Log 13](#)

14.

15.

16. [Post-Compromise Winnti is Coming - Evolution after Prosecution](#)

17.

18. [Timeline for disseminating the Cobalt Strike 2020.7 2020.11 2021.1 2021.3](#)

2021.4 Chacha20 shellcode or loader(Chatloader) appeared to extract Cobalt strike Beacon Use CDN service in Cobalt Strike, especially DNS beacon Use Cloudflare worker to hide real C2 IP Use certificate bypass and dll hollowing technique in Chatloader Use multiple .NET loaders and misuse InstallUtil to load Cobalt Strike 2021.6 Use funnyswitch to load Cobalt Strike and use early bird code injection technique 18

19.

20. [Chatloader ◆ Uses chacha20 algorithm to decrypt the payload ◆](#)

Most of the payload is Cobalt Strike, but we have also seen another backdoor ◆ ETW bypass ◆ Dll hollowing offset length data 0x0:0xB 0xC config nonce 0xC:0xF 0x4 config crc32 0x10:0x13 0x4 config_enc_length 0x14:0x14+config_enc_length config_enc_length ciphertext 0x100:0x120 0x20 config key 20

21. [length data 0x4 Header 0x4 Check User is SYSTEM 0x4](#)

Mutex trigger 0x4 Delete Loader trigger 0x4 Patch EtwEventWrite trigger 0x4 Process Hollowing trigger 0x4 Injected Process Name Length(x2) InjectedProcess Name Length(x2) InjectedProcess Name 0x4 Payload in Loader 0x4 Payload Name Length(x2) Payload Name Length(x2) Payload Name 0x4 Payload Size 0x4 Payload FilePointor 0x4 Payload crc32 0xC Payload Nonce length data 0x4 Header 0x4 Check User is SYSTEM 0x4 Mutex trigger 0x4 Delete Loader trigger 0x4 Patch EtwEventWrite trigger 0x4 Payload in Loader 0x4 Payload Name Length(x2) Payload Name Length(x2) Payload Name 0x4 Payload Size 0x4 Payload FilePointor 0x4 Payload crc32 0xC Payload Nonce Header:CB2F29AD Header:8BD6488B 21

22. [Chatloader config example ===== Decrypt Config ===== Config Nonce \(12](#)

bytes) = 0xb5 0x5e 0x14 0x8d 0x46 0xe1 0x2e 0x97 0x5d 0x3d 0x75 0xf1 Config Nonce (base64) = tV4UjUbhLpddPXXx Config CRC32 = 0xe 0xdc 0xac 0xad Config CRC32 (base64) = DtySrQ== Ciphertext length = 48 Config Key = 0xa2 0x42 0x99 0x5 0x5f 0x1f 0xc 0x14 0xcb 0xdd 0xb 0x1 0xdf 0xa6 0x4c 0x34 0xf5 0xfd 0x3 0x3c 0xa7 0xf1 0xaf 0x30 0xa0 0xc7 0x5c 0x57 0x35 0x9d 0x41 0xe0 Config Key (base64) = okKZBV8fDBTL3QsB36ZMNPX9Azyn8a8woMdcVzWdQeA= ===== Config ===== Head = 0xad 0x29 0x2f 0xcb Check User is SYSTEM = 0 Mutex trigger = 0 Delete Loader trigger = 0 Patch EtwEventWrite trigger = 1 Payload in Loader = 0 Payload Name Length = 14 Payload Name = Despxs.dll Payload Size = 3f800 Payload FilePointor = 0 Payload CRC32 = 0x40 0xf6 0x8f 0xa7 Payload Nonce (12 bytes) = 0x93 0x49 0x68 0x79 0x6a 0xda 0xb5 0xcf 0xf0 0xf1 0xb3 0x4f 22

23.

24. [DLL Hollowing \(cont.\) https://github.com/forrest-orr/phantom-dll-hollower-poc](https://github.com/forrest-orr/phantom-dll-hollower-poc) 24

25.

26. [.NET loader structure offset data offset 38\(h\) – 47 md5](#)

hash of offset 48 until end offset 48-53 Sha256 as AES key offset 54-67 MD5 as AES IV offset 68 - end Encrypted payload with AES(ECB) offset data offset 0-3 must be 1F A4 3A AC offset 4-7 the length of the payload offset 8 - end malware payload Version 2.63 offset Data offset 84(h) -93 md5 hash of offset 48 until end offset 94-9f Sha256 as AES key offset a0-ab MD5 as AES IV offset ac - end Encrypted payload with AES(ECB) offset data offset 0-3 must be 0C C0 73 95 offset 4-7 the length of the payload offset 8 - end malware payload Version 17.102 After decryption 26

27. [Funnyswitch loader ♦ Name from ptsecurity*, which will inject .NET](#)

backdoor funny.dll in memory ♦ We found new version loader(mcvsocfg.dll) which may target McAfee user ♦ E:\VS2019_Project\while_dll_ms\while\x64\Release\macoffe.pdb ♦ Another : E:\VS2019_Project\prewhiltedll\x64\Release\prewhiltedll.pdb ♦ We found the new loader inject Cobalt Strike and funny.dll *https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41- backdoors-old-and-new/ Cobaltstrike funnydll 27

28.

29. [Early bird code injection Loader ◆ Using open source Alaris](#)

loader* to use syscalls to run cobalt strike ◆ Load PNG resource as payload and decrypt with RC4 ◆ Using Detour to hook the Freelibary API of the launcher ◆ Using early bird code injection technique ◆ NtTestAlert ◆ KiUserApcDispatcher *<https://github.com/cribdragg3r/Alaris> 29

30.

31.

32. [loader used by GroupCC 32 Signed file Temp.tmp winprint.exe rundll32.exe](#)

2.Create rundll32.exe Process 1.Read File binary Stage_1.shellcode 4.Read File 5.decode cobaltstrike 3.Inject shellcode in rundll32 • winprint.exe first reads a piece of shellcode from the payload file and then opens rundll32.exe, calls RtlCreateUserThread to run the first stage shellcode in rundll32.exe • The first stage shellcode will read the payload file again, use VirtualAlloc to allocate memory in rundll32.exe, and inject the payload and decrypt it, finally, it will call EtwCreateEtwThread to move the thread to the starting point of the cobalt strike. GroupCC

33. [Backdoor Winnti is Coming - Evolution after Prosecution](#)

34.

35.

36.

37. [Shadowpad ◆ APT41 used the new builder of shadowpad in](#)

2021, which was mentioned in Ptsecurity's report* which used new obfuscation method and decryption method for configuration ◆ We think this builder was a shared Tool, because we have also seen Naikon Team use this builder ◆ Md5 of the loader:3520e591065d3174999cc254e6f3dbf5 37 def decrypt_string(src): key = struct.unpack("<H", bytearray(src[0:2]))[0] data_len = struct.unpack("<H", bytearray(src[2:4]))[0] data = src[4:4+data_len] result = "" i=0 while(i < data_len): tmp = key tmp += tmp key = key + ((tmp * 8) & 0xFFFFFFFF) + 0x107E666D result += chr(((HIBYTE(key) + BYTE2(key) + BYTE1(key) + LOBYTE(key)) ^ ord(data[i])) & 0xFF) i+=1 return result *<https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/> The method to decrypt the string of the configuration

38. [Shadowpad config example 38 id = 6/18/2021 11:26:19 AM Messenger](#)

= TEST Binary Path = %ALLUSERSPROFILE%\Microsoft\WinLSAM\ Binary Name = LSAM.exe Loader Name = log.dll Payload Name = log.dll.dat Service Name = SystemAssociationManager Service Display Name = System Association Manager Service Description = This service provides support for the device association software. If this service is disabled, devices may be configured with outdated software, and may not work correctly. Registry Key Install = SOFTWARE\Microsoft\Windows\CurrentVersion\Run Registry Value Name = LocalSystemAssociationManager Inject Target 1 = %windir%\system32\svchost.exe Inject Target 2 = %windir%\system32\wininit.exe Inject Target 3 = Inject

Target 4 = Supposed to have 4 server Server1 = TCP://1dfpi2d8kx.wikimedia.vip:443 Server2 = Server3 = Server4 = Socket 1 = SOCKS4 Socket 2 = SOCKS4 Socket 3 = SOCKS5 Socket 4 = SOCKS5 DNS 1 = 8.8.8.8 DNS 2 = 8.8.8.8 DNS 3 = 8.8.8.8 DNS 4 = 8.8.8.8 config offset:0x96

39. [Shadowpad Decryption Routine 39 Old Version](#)

40.

41. [Natwalk ♦ Dropped by chatloader ♦ First seen in the](#)

wild in 2021/3, and first seen on VT in 2020/9 ♦ Shellcode based backdoor ♦ It uses register + offset to call the Windows api (also used by crosswalk) ♦ The name is from the unique file path it will look up : “%AllUserProfile%\UTXP\nat” rbx = 7FEF1431534 41

42.

43.

44. [Natwalk\(cont.\) command description 0x64 Close sessions 0x5C Update the ChaCha20](#)

key for C2 communication 0x66 Change the current status 0x74 Terminate all threads 0x78 kill process 0x7c Run plug-in 0x82 Enumerate user info 0x8c Send config to C2 0x8E Load additional config 44 Software\Microsoft\Windows\CurrentVersion\Internet Settings ProxyServer explorer.exe %AllUsersProfile%\UTXP\nat\ %02X POST Mozilla/5.0 Chrome/72.0.3626.109 Safari/537.36 gtsid: gtuvid: https://msdn.microsoft.com https://www.google.com https://www.twitter.com https://www.facebook.com Unique string in the bottom of Natwalk

45.

46.

47. [HIGHNOON command ♦ Command is same as the HIGHNOON mentioned](#)

by Macnica* in 2018 command description 0 Bind Network Socket 1 Check IP address change and Receive Packet, Console Output 3 Console Output 4 Read //DEV//NULL and Console Output 5 Check IP address change and Receive Packet, Console Output *https://hitcon.org/2018/pacific/downloads/1214-R2/1330-1400.pdf 47

48.

49.

50.

51.

52. [Fastly \(GroupCC\) 52 BeaconType - HTTPS Port - 443 SleepTime](#)

- 1000 MaxGetSize - 1398119 Jitter - 10 MaxDNS - Not Found PublicKey_MD5 - 9ee3e0425ade426af0cb07094aa29ebc C2Server - pypi.python.org/latest/pip-check UserAgent - Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/84.0.4147.125 Safari/537.36 HttpPostUri - /latest/check ... PipeName - Not Found DNS_Idle - Not Found DNS_Sleep - Not Found SSH_Host - Not Found SSH_Port - Not Found SSH_Username - Not Found SSH_Password_Plaintext - Not Found SSH_Password_Pubkey - Not Found SSH_Banner - Host: pypi2-python.org ... Watermark - 426352781 ... ProcInject_AllocationMethod - VirtualAllocEx bUsesCookies - True HostHeader - Host: pypi2-python.org ... pypi2-python.org.global.prod.fastly.net pypi2-python.org Real C2 IP

53.

54. [Cobalt strike payload Same Xor key: 0x3A Funnyswitch dropper which](#)

injected cobalt strike ITW Url Fishmaster operation – TAG-22* Funnyswitch dropper which injected funnydll Connection of APT41 and fishmaster operation New builder of Shadowpad IR case Same PDB string * <https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/>

55.

56. [GroupCC Fishmaster BIOPASS RAT Python Script \(local online server\)](#)

57. [GroupCC Fishmaster BIOPASS RAT Python Script \(C1222 module\)](#)

58.

59. [GroupCC Used\(stolen\) certificate ◆ Quickteck.com ◆ Serial Number : 70](#)

D8 96 11 7E 15 30 2C 7E EF EC B2 89 B3 BF E0 ◆ 주식회사 엘리시온랩(ElySION Lab Co., Ltd.) ◆ Serial Number : 03 D4 33 FD C2 46 9E 9F D8 78 C8 0B C0 54 51 47 ◆ ARGOS LABS ◆ Serial Number : 00 F7 B7 5C 60 5B 00 83 95 73 8A AC 06 AB E3 B4 70 ◆ 1.A Connect GmbH ◆ Serial Number : 00 A7 E4 DE D4 BF 94 9D 15 AA 42 01 84 3F 1A B6 4D 59

60.

61. [Amoeba v.s Fishmaster v.s GroupCC 61 ◆ Amoeba v.s. Fishmaster](#)

◆ Two possibilities ◆ Shared C2 ◆ 163.138.137.235 ◆ 93.180.156.77 ◆ Shared customized CobaltStrike ◆ Xor key : 0x3A ◆ Fishmaster v.s. GroupCC ◆ Shared Tool : Biopass RAT ◆ Similar TTPs ◆ Uses some stolen or revoked certificate ◆ Uses Legitimate installer ◆ Use aliyun as payload sites Amoeba Fishmaster GroupCC

62.

63.

64. [HW operation\(護網行動\) ◆ To detect the security issues of key](#)

national infrastructure, and to test their event monitoring and ability to quickly coordinate with emergency incident ◆ The target involves many industries, including government, finance, electricity, and business key enterprises in China. ◆ From OSINT, the operation started from 4/8 in 2021 64

65. [南京木百文化传媒有限公司.exe](#)

66. [Maybe link to HW operation 66 Cobalt strike loader in](#)

IR case which use alaris loader with resource png payload Same loader 南京木百文化传媒有限公司.exe Funnyswitch Same unique shellcode in caculating api hash 调整中移在线服务有限公司 职工五险一金缴纳比例的通知.exe Cobalt strike loader in IR case which used early bird code injection VPN统一身份认证 ID.exe 运维安全管理与审计系统 单点登录插件.exe Same Cobalt strike payload header

67.

68. [IOC 68 ◆ Chatloader 7ee9b79f4b5e19547707cbd960d4292f F5158addf976243ffc19449e74c4bbad 1015fa861318acbbfd405e54620aa5e3 a1d972a6aa398d0230e577227b28e499 ◆ .NET](#)

loader bd2d24f0ffa3d38cb5415b0de2f58bb3 ◆ Funnyswitch loader e0a9d82b959222d9665c0b4e57594a75 07a61e3985b22ec859e09fa16fd28b85 d720ac7a6d054f87dbafb03e83bcb97c F85d1c2189e261d8d3f0199bbdda3849 5b2a9a12d0c5d44537637cf04d93bec5 ◆ Early bird code injection loader 4598c75007b3cd766216086415cc4335 Fd6ae1b8713746e3620386a5e6454a8d b028b4f8421361f2485948ca7018a2b0 ◆ Natwalk 1d36404f85d94bea6c976044cb342f24 7c6e75e70d29e77f78ea708e01e19c36 ◆ HIGHNOON loader 407b5200c061123c9bd32e7eea21a57b 5b99fa01c72ceb53a76cc72e9581189 ◆ Funnydll e0a9d82b959222d9665c0b4e57594a75 ◆ Spyder fba77006e8f8f3db6aac86211fa047fb ◆ Shadowpad af7cef9e0e6601cae068b73787e3ae81

69. [IOC 69 symantecupd.com microsoftonlineupdate.dynamic- dns.net www.sinnb.com pip.pythoncdn.com img.hmmvm.com reg.pythoncdn.com bbwebt.com](#)

ns1.tkti.me test.tkti.me ns1.microsofts.freeddns.com api.aws3.workers.dev ns1.hkserch.com godaddy1.txwl.pw godaddy2.txwl.pw ns.cdn06.tk update.facebookdocs.com ns1.dns-dropbox.com ns.cloud20.tk ns.cloud01.tk ns1.token.dns05.com sculpture.ns01.info work.cloud20.tk work.cloud01.tk help01.softether.net cloud.api-json.workers.dev update.microsoft-api.workers.dev up.linux-headers.com p.samkdd.com ns1.microsoftskype.ml ns1.hongk.cf ns1.163qq.cf 163qq.cf depth.ddns.info yjij4bpade.nslookup.club ooliviaa.ddns.info mootoorhead.ns01.info token.dns04.com ns1.watson.misecure.com vt.livehost.live sociomanagement.com ns1.hash-prime.com wntc.livehost.live smtp.bitl.ph perfeito.my cdn.cdnfree.workers.dev www.microsoftshelp.dns1.us ns1.mssetting.com www.corpsolution.net www.mircoupdate.https443.net publicca.twhinet.workers.dev microgoogle.ml www.google-dev.tk api.gov-tw.workers.dev 103.255.179.54 www.omgod.org 154.223.175.70 687eb876e047.kasprsky.info zk4c9u55.wikimedia.vip 193.38.54.110 api.aws3.workers.dev 4iiiiessb.wikimedia.vip 45.32.123.1 158.247.215.150 ntp.windows-time.com trulwkg5c.tg9f6zwxk.icu windowsupdate.microsoft.365filtering.com wustat.windows.365filtering.com ti0wddsnv.wikimedia.vip

70.

71. aragorn@51882@gmail.com **THANK YOU!**

Source: <https://speakerdeck.com/aragorntseng/winnti-is-coming-evolution-after-prosecution-at-hitcon2021>