Daggerfly: APT Actor Targets Telecoms Company in Africa

MgBot modular malware framework

MgBot is a well-designed modular framework that is actively maintained. The components of the framework are the following:

- MgBot EXE dropper
- MgBot DLL Loader
- MgBot Plugins

The MgBot plugins that were deployed in this activity have numerous capabilities that can provide the attackers with a significant amount of information about compromised machines. Among the unique plugins that were deployed during this activity were:

- Network scanner – innocence.dll
    - Capabilities include: arp scan, http scan, determining the type of server (e.g. SQL, WebLogic, Redis, etc.) it is running on.
- A Chrome and Firefox infostealer that can gather information such as bookmarks and browsing history – bkmk.dll
- Logging module – famdowm.dll
    - Based on the open-source easylogging++, which can carry out basic logging, track performance and more.
- QQ messages infostealer – qmsdp.dll

    - Based on this blog, which details how a chat tool message database was cracked by hackers.
- Active Directory enumeration – ceeeb.dll
    - Collects the following information from Active directory:
        - Members info
        - Computers
        - Local Admins
        - Remote Desktop Users
        - Dcom Users
- Password dumper – cpfwplgx.dll
    - Drops a file to call the MiniDumpWriteDump API to dump a process memory.
- QQ Keylogger – kstrcs.dll
    - Keylogger that targets QQEdit.exe and QQ.exe processes.
- Screen and clipboard grabber – cbmrpa.dll
    - Captures clipboard and drag and drop data and saves it to a file.
- Outlook and Foxmail credentials stealer – maillfpassword.dll
- Audio capture – prsm.dll
    - Captures audio from the infected system.
    - Uses COM objects IMMDeviceEnumerator, IAudioCaptureClient.
- Process Watchdog – ansecprocesskeep.dll
    - Registered as service AnsecProcessKeep.
    - Confirmed to be a watchdog that keeps a process running.
    - The process name is found in an .ini file.

All of these capabilities would have allowed the attackers to collect a significant amount of information from victim machines. The capabilities of these plugins also show that the main goal of the attackers during this campaign was information-gathering.

Daggerfly's development of these previously unseen plugins demonstrates that the attack group is continuing to actively develop its malware and the tools it can use to target victim networks.

Continuation of a Trend

Telecoms companies will always be a key target in intelligence gathering campaigns due to the access they can potentially provide to the communications of end-users.

Symantec's Threat Hunter team also spotted some other recent activity targeting telecoms companies that was linked with moderate confidence to the threat actor Othorene (aka Gallium), in what appeared to be a continuation of an intelligence-gathering campaign first reported on by SentinelOne under the name Operation Tainted Love in March. SentinelOne reported that in that campaign Othorene was targeting telecoms companies in the Middle East.

Othorene has been active since around 2014, and it is believed to be a relatively small group that has a strong focus on the surveillance of individuals. There are some indications that Othorene may have links with the APT41 (aka Blackfly, Grayfly) APT group also. Overlap of both personnel and tactics,

techniques, and procedures (TTPs) among Chinese APT groups is not uncommon, and can mean that attributing activity to one group with high confidence is difficult.

In the activity Symantec saw, we found three additional victims of the same campaign that SentinelOne detailed, located in Asia and Africa. Two of the three were subsidiaries of the same Middle Eastern telecoms firm. The attackers had been active on victim networks since November 2022. Symantec saw attackers dumping credentials and scanning the network using NbtScan.

The main malware (pc.exe dubbed mim221) in this campaign was used to dump credentials, and it had the same password as the malware used in the activity documented by SentinelOne. The attackers also moved laterally across victims' networks, used Scheduled Task for persistence, and dumped SAM and System hives from the registry. There were indications that the attackers may have exported the Active Directory database on victim machines, and they were also able to gain access to domain controllers, giving them deep access to victim networks.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

File Indicators – Daggerfly

MgBot Dropper

c89316e87c5761e0fc50db1214beb32a08c73d2cad9df8c678c8e44ed66c1dab

90e15eaf6385b41fcbf021ecbd8d86b8c31ba48c2c5c3d1edb8851896f4f72fe

MgBot – aasrvd.dll, pmsrvd.dll

706c9030c2fa5eb758fa2113df3a7e79257808b3e79e46869d1bf279ed488c36

017187a1b6d58c69d90d81055db031f1a7569a3b95743679b21e44ea82cfb6c7

MgBot Plugins

cb8aede4ad660adc1c78a513e7d5724cac8073bea9d6a77cf3b04b019395979a

2dcf9e556332da2a17a44dfceda5e2421c88168aafea73e2811d65e9521c715c

a6ed16244a5b965f0e0b84b21dcc6f51ad1e413dc2ad243a6f5853cd9ac8da0b

ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024

585db6ab2f7b452091ddb29de519485027665335afcdb34957ff1425ecc3ec4b

29df6c3f7d13b259b3bc5d56f2cdd14782021fc5f9597a3ccece51ffac2010a0
ea2be3d0217a2efeb06c93e32f489a457bdea154fb4a900f26bef83e2053f4fd

54198678b98c2094e74159d7456dd74d12ab4244e1d9376d8f4d864f6237cd79

d9eec27bf827669cf13bfdb7be3fdb0fdf05a26d5b74adecaf2f0a48105ae934

cb7d9feda7d8ebfba93ec428d5a8a4382bf58e5a70e4b51eb1938d2691d5d4a5

2c0cfe2f4f1e7539b4700e1205411ec084cbc574f9e4710ecd4733fbf0f8a7dc

a16a70b0a1ac0718149a31c780edb126379a0d375d9f6007a6def3141bec6810

0bcdcc0515d30c28017fd7931b8a787feebe9ee3819aa2b758ce915b8ba40f99

PlugX Loader – proccom.dll, djcu.dll

c31b409b1fe9b6387b03f7aedeafd3721b4ec6d6011da671df49e241394da154

db489e9760da2ed362476c4e0e9ddd6e275a84391542a6966dbcda0261b3f30a

632cd9067fb32ac8fbbe93eb134e58bd99601c8690f97ca53e8e17dda5d44e0e

DumpCredStore – dumpcredstore.ps1, a.ps1

c1e91a5f9cc23f3626326dab2dcdf4904e6f8a332e2bce8b9a0854b371c2b350

5a0976fef89e32ddcf62c790f9bb4c174a79004e627c3521604f46bf5cc7bea2

AnyDesk – anydesk.exe

7bcff667ab676c8f4f434d14cfc7949e596ca42613c757752330e07c5ea2a453

File Indicators – Othorene

3f75818e2e43a744980254bfdc1225e7743689b378081c560e824a36e0e0a195 – pc.exe, rpc.exe (Main malware)

1b8500e27edc87464b8e5786dc8c2beed9a8c6e58b82e50280cebb7f233bcde4 – get.exe (used to print Syskey and Samkey)

03bc62bd9a681bdcb85db33a08b6f2b41f853de84aa237ae7216432a6f8f817e – pc.dll

ae39ced76c78e7c2043b813718e3cd610e1a8adac1f9ad5e69cf06bd6e38a5bd – pc.dll

f6f6152db941a03e1f45d52ab55a2e3d774015ccb8828533654e3f3161cfcd21 – pc.exe

2f4a97dc70f06e0235796fec6393579999c224e144adcff908e0c681c123a8a2 – pc.dll

22069984cba22be84fe33a886d989b683de6eb09f001670dbd8c1b605460d454 – pc.dll

7b945fb1bdeb27a35fab7c2e0f5f45e0e64df7821dd1417a77922c9b08acfdc3 – rpc.dll

e8be3e40f79981a1c29c15992da116ea969ab5a15dc514479871a50b20b10158 – pc.dl

b5c46c2604e29e24c6eb373a7287d919da5c18c04572021f20b8e1966b86d585 – rpc.dll

53d2506723f4d69afca33e90142833b132ed11dd0766192a087cb206840f3692 – test.exe

26d129aaa4f0f830a7a20fe6317ee4a254b9caac52730b6fed6c482be4a5c79d – g.dll

b45355c8b84b57ae015ad0aebfa8707be3f33e12731f7f8c282c8ee51f962292 – g.dll

17dce65529069529bcb5ced04721d641bf6d7a7ac61d43aaf1bca2f6e08ead56 – getHashFlsa64.dll

98b6992749819d0a34a196768c6c0d43b100ef754194308eae6aaa90352e2c13 – getHashFlsa64.dll

6d5be3e6939a7c86280044eebe71c566b48981a3341193aa3aff634a3a5d1bbd – getHashFlsa64.dll

1cf04c3e8349171d907b911bc2a23bdb544d88e2f9b8fcc516d8bcf68168aede – getHashFlsa64.dll