Daggerfly APT Group Updates Toolset

Threat actors using MACMA macOS backdoor variant and a new version of the MgBot malware.

Actor:

Daggerfly

Target Sectors:

Government and Education

Actor Aliases:

Evasive Panda, Bronze Highland

Attack Motivation:

Espionage

Target Geographies:

Taiwan

Overview

Symantec's Threat Hunter Team recently observed the Daggerfly advanced persistent threat (APT) group using an updated toolset.

Symantec uncovered a new previously undocumented version of the MACMA macOS backdoor malware being used by the group.

In addition, Daggerfly was also observed using the PlugX remote access Trojan (RAT) and a new version of MgBot, a modular malware framework previously used by the group. The updating of MgBot may be in response to recent reports on Daggerfly and its use of the malware published by Symantec and other vendors.

Components and malware modules recently used by the attackers allow them to target a diverse range of operating systems, such as Windows, Linux, macOS, Android, iOS, Solaris, etc.

This threat alert contains indicators of compromise associated with recent Daggerfly activity.

Tools Used:

- MgBot
- MACMA
- PlugX

Indicators of Compromise

SOC analysts should review this alert and hunt on their network for associated indicators of compromise (IOCs). Their presence may indicate a ransomware attack in preparation. If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file. If you discover any other unknown or unavailable files while hunting, you can submit them to Symantec for analysis .

Symantec products will detect and alert against the behaviors and techniques detailed in this alert. For guidance on how to use Symantec Endpoint Security Complete for Threat Hunting, please review this document.

SHA256 file hash: 017c957ba1cd9cd6fa890324cfa54300d57fae289cd3a66e0c596b04d1ae3a40
Description: MgBot dropper
Last seen: 2023-08-19

SHA256 file hash: 03ba06a3401c8153fda92f85c9bfba8f64a63630541caaf41cec3c0636ca74d3
Description: MgBot dropper
Last seen: 2023-08-21

SHA256 file hash: 07455b7f026c1f7be258cbd3266169931fb4bfbbff15a4c6327f88166bb8bb75
Description: MgBot DLL
File name(s): djcu.dll
Last seen: 2023-08-19

SHA256 file hash: 0919a72d8193261df75a0191197aff9b44eabb71aa440ff515c6c688027a0ac2
Description: MgBot dropper
Last seen: 2023-09-20

SHA256 file hash: 104ae53aa54c9e22a562ea26c1daab5eb2133ffd7616dc6017f7956048a96fe8
Description: MgBot dropper
Last seen: 2023-08-18

SHA256 file hash: 11d526a54b96bfe87b7a9a72f8e7b505a4de1b4a1bfdab5b5cbf0e286e9e7c98
Description: MgBot DLL
File name(s): util.dll
Last seen: 2023-12-19

SHA256 file hash: 2b79b19e52b25e8ab4c47b38c7ff5caa460746603c0e58a903d8a5a74b0c339a
Description: MgBot plugin
File name(s): kstrcs.dll
Last seen: 2023-11-21

SHA256 file hash: 34eaf21da6a45c9d148e46492cf3c118d62eedac7521039cd777b3c820b68ffd
Description: MgBot dropper
Last seen: 2023-07-31

SHA256 file hash: 3dfb3215b95b9f7b340c2ddb90e37480d3a268b5f5c8b3962a8f260efdca3aeb
Description: MgBot
File name(s): aasrvd.dll
Last seen: 2024-01-04

SHA256 file hash: 7c2cff362c46b186674758151b8b182b8b1b558e98bc55fc887212bb05acc8ca
Description: MgBot dropper
Last seen: 2023-08-22

SHA256 file hash: a68ea798f8238cdee85d9831a4fe7879d7d1e0ad8ae9c871511851c4b2d57059
Description: MgBot plugin
File name(s): gmck.dll
Last seen: 2023-11-21

SHA256 file hash: a8c355a715eac65dc646efde9c1c77201b45e12b2212bf54f3bceda637b05171
Description: MgBot dropper
Last seen: 2023-09-06

SHA256 file hash: b7fec9e2ded0b264a090036aabfad2d53d2accc0e932f9d815503752dbfea01a
Description: Possible PlugX DLL
File name(s): hex.dll
Last seen: 2023-07-25

SHA256 file hash: d0a6ea08739fb68aa0869d4a32ecd96b1eb75a882ab4f0af5f18fa2a34c16d2b
Description: MgBot dropper
Last seen: 2023-08-19

SHA256 file hash: e37e59042fc291e44e7e60853bbeaa6a74b48033ce0f0530b4a9bae67fd2fd2a
Description: MgBot dropper
Last seen: 2023-08-19

SHA256 file hash: e3d6b7fdd4b43f8ffab5507f55499db5c2c66aece32a0bab9b2e2e30e300a4f3
Description: MgBot dropper
Last seen: 2023-09-27

SHA256 file hash: cf5edcff4053e29cb236d3ed1fe06ca93ae6f64f26e25117d68ee130b9bc60c8
Description: OSX.MACMA

SHA256 file hash: d599d7814adbab0f1442f5a10074e00f3a776ce183ea924abcd6154f0d068bb4
Description: OSX.MACMA
File name(s): UserAgent

SHA256 file hash: 1f5e4d2f71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e
Description: OSX.MACMA
File name(s): UserAgent

SHA256 file hash: 003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef
Description: OSX.MACMA

SHA256 file hash: fce66c26deff6a5b7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8ced
Description: OSX.MACMA
File name(s): USAgent

SHA256 file hash: dad13b0a9f5fde7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313
Description: OSX.MACMA

SHA256 file hash: eff1c078895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0
Description: OSX.MACMA
File name(s): arch

SHA256 file hash: 955cee70c82bb225ca2b108f987fbb245c48eefe9dc53e804bbd9d55578ea3a4
Description: OSX.MACMA
File name(s): com.USAgent.mv.plist

SHA256 file hash(es):

017c957ba1cd9cd6fa890324cfa54300d57fae289cd3a66e0c596b04d1ae3a40
03ba06a3401c8153fda92f85c9bfba8f64a63630541caaf41cec3c0636ca74d3
07455b7f026c1f7be258cbd3266169931fb4bfbbff15a4c6327f88166bb8bb75
0919a72d8193261df75a0191197aff9b44eabb71aa440ff515c6c688027a0ac2
104ae53aa54c9e22a562ea26c1daab5eb2133ffd7616dc6017f7956048a96fe8
11d526a54b96bfe87b7a9a72f8e7b505a4de1b4a1bfdab5b5cbf0e286e9e7c98
2b79b19e52b25e8ab4c47b38c7ff5caa460746603c0e58a903d8a5a74b0c339a
34eaf21da6a45c9d148e46492cf3c118d62eedac7521039cd777b3c820b68ffd
3dfb3215b95b9f7b340c2ddb90e37480d3a268b5f5c8b3962a8f260efdca3aeb
7c2cff362c46b186674758151b8b182b8b1b558e98bc55fc887212bb05acc8ca
a68ea798f8238cdee85d9831a4fe7879d7d1e0ad8ae9c871511851c4b2d57059
a8c355a715eac65dc646efde9c1c77201b45e12b2212bf54f3bceda637b05171
b7fec9e2ded0b264a090036aabfad2d53d2accc0e932f9d815503752dbfea01a
d0a6ea08739fb68aa0869d4a32ecd96b1eb75a882ab4f0af5f18fa2a34c16d2b
e37e59042fc291e44e7e60853bbeaa6a74b48033ce0f0530b4a9bae67fd2fd2a
e3d6b7fdd4b43f8ffab5507f55499db5c2c66aece32a0bab9b2e2e30e300a4f3
cf5edcff4053e29cb236d3ed1fe06ca93ae6f64f26e25117d68ee130b9bc60c8
d599d7814adbab0f1442f5a10074e00f3a776ce183ea924abcd6154f0d068bb4
1f5e4d2f71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e
003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef
fce66c26deff6a5b7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8ced
dad13b0a9f5fde7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313
eff1c078895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0
955cee70c82bb225ca2b108f987fbb245c48eefe9dc53e804bbd9d55578ea3a4

File name(s):

aasrvd.dll
djcu.dll
gmck.dll
hex.dll
kstrcs.dll
util.dll
zydgzww.dll

Network indicator(s):

103.243.212[.]98
123.1.170[.]152
103.96.128[.]44
92.118.234[.]34