Daggerfly: Espionage Group Makes Major Update to Toolset

By About the Author

Archived: 2026-04-02 11:13:46 UTC

The Daggerfly (aka Evasive Panda, Bronze Highland) espionage group has extensively updated its toolset, introducing several new versions of its malware, most likely in response to exposure of older variants. The new tooling was deployed in a number of recent attacks against organizations in Taiwan and a U.S. NGO based in China, which indicates the group also engages in internal espionage. In the attack on this organization, the attackers exploited a vulnerability in an Apache HTTP server to deliver their MgBot malware.

Among the new additions to Daggerfly's arsenal are a new malware family based on the group's MgBot modular malware framework and a new version of the Macma macOS backdoor. While Macma is a previously documented threat, it had hitherto been of unknown authorship. However, Symantec's Threat Hunter Team has now found evidence suggesting that it is developed by Daggerfly.

Active for at least a decade, Daggerfly is primarily known for its development and use of the MgBot framework. In 2023, Symantec reported a Daggerfly intrusion against a telecoms operator in Africa involving previously unseen plugins for MgBot.

Macma update

Macma is a macOS backdoor that was first documented by Google in 2021 but appears to have been used since at least 2019. At the time of discovery, it was being distributed in watering hole attacks involving compromised websites in Hong Kong. The watering holes contained exploits for iOS and macOS devices. Users of macOS devices were targeted with a privilege escalation vulnerability (CVE-2021-30869) which allowed the attackers to install Macma on vulnerable systems.

Macma is a modular backdoor. Functionality includes:

- Device fingerprinting
- Executing commands
- Screen capture
- Keylogging
- Audio capture
- Uploading and downloading files

Following its exposure, further details about the threat were published by Objective-See and SentinelOne.

Recent variants of Macma found by Symantec exhibit evidence of ongoing development. One version (SHA256: 003764fd74bf13cff9bf1ddd870cbf593b23e2b584ba4465114023870ea6fbef) contained a different main module (SHA256: 1f5e4d2f71478518fe76b0efbb75609d3fb6cab06d1b021d6aa30db424f84a5e) to previously documented versions. The main difference lies in strings that appear to function as configuration data (see Figure 1).

A second version of Macma (SHA256: dad13b0a9f5fde7bcdda3e5afa10e7d83af0ff39288b9f11a725850b1e6f6313) contained what appeared to be incremental updates to the existing functionality. Some of the identified updates included:

- Updated modules in its appended data
- Updated file directory paths and filenames (and related string quotes when constructing command-lines for processes to start)
- Additional debug logging

Its main module (SHA256: fce66c26deff6a5b7320842bc5fa8fe12db991efe6e3edc9c63ffaa3cc5b8ced) exhibited evidence of more extensive modification. This included:

- New logic to collect a file's system listing, with the new code based on Tree, a publicly available Linux/Unix utility.
- Modified code in the AudioRecorderHelper feature
- Additional parametrisation
- Additional debug logging
- Addition of a new file - param2.ini – that is related to settings around a feature named "autoScreenCaptureInfo"

In addition to this, it too had different strings containing configuration data (see Figure 1).

Another module from this variant (SHA256: eff1c078895bbb76502f1bbad12be6aa23914a4d208859d848d5f087da8e35e0) contained modified code to adjust the size of a created screen capture, which apparently related to the aspect ratio when resizing the capture.

Attribution to Daggerfly

Although Macma was widely believed to have been linked to advanced persistent threat (APT) activity, it has hitherto not been linked to a particular group. However, Symantec has found evidence to suggest that it is part of the Daggerfly toolkit. Two variants of the Macma backdoor connected to a command-and-control (C&C) server (103.243.212[.]98) that was also used by an MgBot dropper.

In addition to this shared infrastructure, Macma and other known Daggerfly malware including Mgbot all contain code from a single, shared library or framework. Elements of this library have been used to build Windows, macOS, Linux, and Android threats. Functionality provided by this library includes:

- Threading and synchronization primitives
- Event notifications and timers
- Data marshaling
- Platform-independent abstractions (e.g. time)

An example of this library code is seen when the magic string "inp" is sent over a SOCK_DGRAM socket:

```
sendto(*(_DWORD *)(v2 + 56), "inp", 3, 0, (const struct sockaddr *)(v2 + 60), 16);
```

While sendto() may be used to communicate with other hosts in general, here the communication is with a local machine (127.0.0), and could be even be threads in the same process. Another example involves the magic string "tim" being sent over a socket similar to the following:

```
sendto(*(_DWORD *)(v1 + 56), "tim", 3, 0, (const struct sockaddr *)(v1 + 60), 16);
```

Symantec has yet to find any matching code in public repositories. Shared code and shared infrastructure between Macma and other Daggerfly tools suggests that Macma is also part of the Daggerfly toolkit.

New backdoor

A new addition to Daggerfly's toolkit is a Windows backdoor (Trojan.Suzafk), which was first documented by ESET in March 2024 as Nightdoor (aka NetMM) when it was observed being used alongside Mgbot. Suzafk was developed using the same shared library used in Mgbot, Macma, and a number of other Daggerfly tools.

Suzafk is a multi-staged backdoor capable of using TCP or OneDrive for C&C. The malware contained the following configuration, indicating the functionality to connect to OneDrive is in development or present in other variants of the malware:

```
ReadMe=ConnONEDRIVE;Version=256;Tag=15ad490f332f3d9a;DownloadUrl=http://103.96.131.150:19876/30_1410402971.exe;token=
{"refresh_token":"REDACTED","client_id":"4aa6708f-f3c8-4511-8118-
5a7208be6a44","client_secret":"REDACTED"};DownloaderSavePath=C:\Programdata\Office\;HttpServerFolder=C:\Program
Files\Common Files\Cloudata\;
```

Another configuration to use a TCP connection for C&C purposes is also present in the backdoor:

```
ReadMe=ConnTCP;Version=256;Tag=15ad490f332f3d9a;DownloadUrl=http://103.96.131.150:19876/30_1292836936.exe;IP=103.96.131.150;Port=40020;D
Files\\Common Files\\Cloudata\\;
```

The loader (SHA256: 5687b32cdd5c4d1b3e928ee0792f6ec43817883721f9b86ec8066c5ec2791595) drops two files: Engine.dll and MeitUD.exe. MeituUD.exe is a legitimate application named DAEMON Tools Lite Helper. Engine.dll is a loader DLL that sets persistence via scheduled tasks and loads the final payload in memory.

The backdoor has embedded code from the al-khaser project, a public code repository aimed to detect virtual machines, sandboxes, and malware analysis environments. It also creates the folders C:\ProgramData\Office\EFir and C:\ProgramData\Office\Temps and stores additional network configuration data under the C:\ProgramData\Office\sysmgr file XOR encrypted with the key 0x7A.

The network configuration in plaintext has the following parameters and values:

```
[InfoRecord]
```

```
CMD_SEND_SN=0
```

```
LOCAL_CALENDAR
```

```
SEND_EMAIL_NUM=0
```

```
LOCAL_MAC_ADDR=[mac address]
```

```
PROXY_INFO
```

`[CtrlTermKey]`

`KEY`

`BSK=[sha256 value]`

`PRK=[sha256 value]`

`[CtrlTermKeyStatus]`

`STATUS=1`

`[CtrlTermKeyVer]`

`VER=1`

`[ManageTermKey]`

`[ManageTermKeyStatus]`

`[ManageTermKeyVer]`

`[ManageTermServerInfoOffset]`

`[ManageTermEmailTo]`

`[ManageTermUseCreateCloudDirAlgorithm]`

Next, the malware creates a cmd.exe shell to send and receive commands from the C&C server (103.96.131[.]150) via open pipes. Additionally, the following commands can be executed:

`ipconfig`
`systeminfo`
`tasklist`
`netstat`

Heavily Resourced

New findings provide a clearer picture of the capabilities and resources behind Daggerfly. The group can create versions of its tools targeting most major operating system platforms. In addition to the tools documented here, Symantec has seen evidence of the ability to Trojanize Android APKs, SMS interception tools, DNS request interception tools, and even malware families targeting Solaris OS. Daggerfly appears to be capable of responding to exposure by quickly updating its toolset to continue its espionage activities with minimal disruption.

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.
