# GIMMICK Malware Attacks macOS to Attack Organizations Across Asia

By Guru Baran

Published: 2022-03-24 · Archived: 2026-04-05 18:15:38 UTC


An espionage threat actor from China known for attacking target organizations across Asia has been linked to a new malware implant for macOS devices.

As Volexity's Network Security Monitoring service monitored an environment late in 2021, it detected an intrusion. Cybersecurity firm Volexity believes the group responsible for the attacks is called Storm Cloud while describing the malware as "GIMMICK."

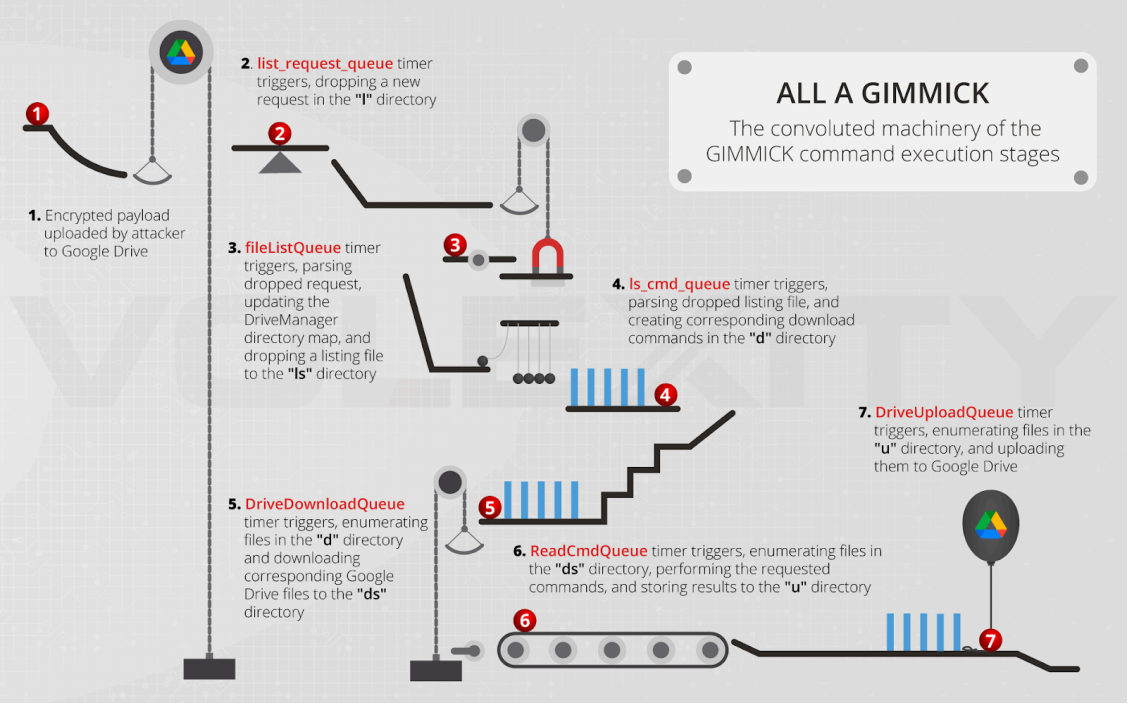
In an intrusion campaign, the data was recovered from a compromised MacBook Pro running macOS 11.6 (Big Sur) through memory analysis. Apart from this, several instances of the malware family have been encountered by Volexity.

For commands and controls (C2) GIMMICK uses Google Drive, a public cloud hosting service since GIMMICK is a multi-platform malware.

Windows versions are written in both .NET and Delphi, while the newly identified macOS variant, GIMMICK is written mostly in Objective C.

Volexity tracks the malware under the same name, regardless of the programming languages used and the operating systems targeted. However, this happened due to the following factors:-

- Shared C2 architecture.
- File paths.
- Behavioral patterns used by all variants.




Volexity researchers Damien Cash, Steven Adair, and Thomas Lancaster stated:-

“Storm Cloud is an advanced and versatile threat actor, adapting its toolset to match different operating systems used by its targets.”

In order to integrate with Target’s network traffic, GIMMICK communicates with its Google Drive-powered C2 server only during working hours and days. While as part of Volexity’s work with Apple, all users now have protection against GIMMICK malware.

### Startup & Initialization

After the implementation of GIMMICK malware on the infected system, GIMMICK can run either as an ‘application’ or as a ‘daemon’ and is designed to mimic the behavior of a program commonly used by the user-targeted.

The cybersecurity firm, Volexity has observed that in the Windows variant of GIMMICK malware there is no concept of setting its own persistence.

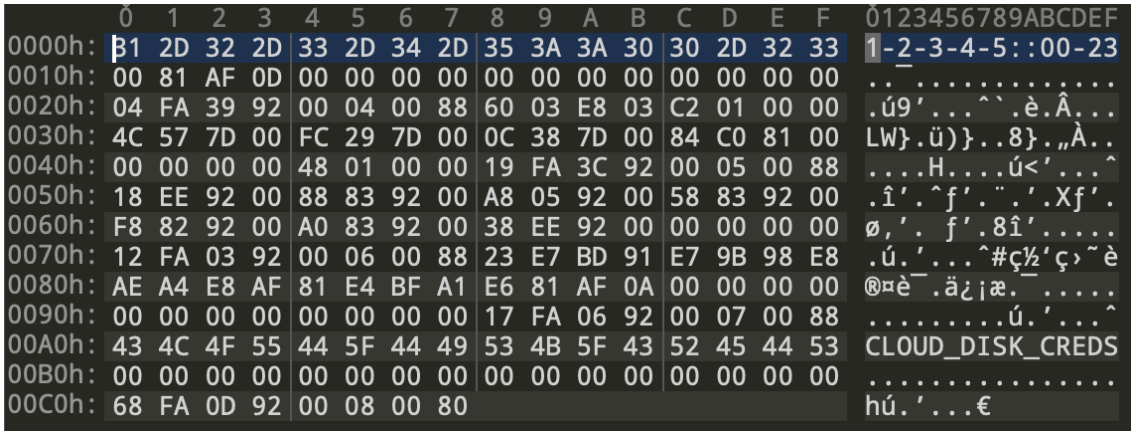
In order to blend in with the network traffic in the target environment, GIMMICK only communicates with its Google Drive C2 server on working days. A JSON object with OAuth2 credentials for accessing Google Drive is retrieved from the first decoding loop.

```
{
  "token": "ya29.a0ARrdaM_3h5LqnwTmt929m5mw4ul9pMVGICT-
  [snipped]
  OWLfpG2lwTVAovNlk2FOMJeMoxZdDVH_7gE48JMFtiAK1zuSOVOPTddm
  n1V",
  "expire": "2021-09-14 09:57:24",
  "clientid":
  "1092974474287-h18u696gfqp7998iab7v9i0ra2lmd38f.apps.
  googleusercontent.com",
  "refresh_token": "1//0e9-6utdQixCiCgYIARAA[snipped]
  -iM6KTYFwIxZ9otUvnbwyre3zkZKnPLSEfJBo6kS4KXg",
  "token_uri": "https://oauth2.googleapis.com/token",
  "scopes": ["https://www.googleapis.com/auth/drive"],
  "client_secret": "faOO[snipped]g89CXm7"
}
```

Second, the 32-byte string is decoded, which is then run through a third-party conversion stage. After decoding the 32-byte string, two characters are converted to numeric representations at a time, and the resulting byte is written to a buffer.

```
idxAesKeyConvert = -2LL;
pgAesKey = __g_szAesKey;
do
{
  szKeyNum[2] = 0;
  szKeyNum[0] = 0;
  szKeyNum[1] = 0;
  sprintf(
    szKeyNum,
    "%c%c",
    (unsigned int)bytesAESKey[idxAesKeyConvert + 2],
    (unsigned int)bytesAESKey[idxAesKeyConvert + 3]);
  *pgAesKey = strtol(szKeyNum, 0LL, 16);
  idxAesKeyConvert += 2LL;
  ++pgAesKey;
}
while ( idxAesKeyConvert < 30 );
```

As a result of the final decoding, the configuration data is a 200byte binary blob that only shows a few overlapping data boundaries.



| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000h: | 31 | 2D | 32 | 2D | 33 | 2D | 34 | 2D | 35 | 3A | 3A | 30 | 30 | 2D | 32 | 33 | 1-2-3-4-5::00-23 |
| 0010h: | 00 | 81 | AF | 0D | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .. ¯ ..... |
| 0020h: | 04 | FA | 39 | 92 | 00 | 04 | 00 | 88 | 60 | 03 | E8 | 03 | C2 | 01 | 00 | 00 | .ú9'...^`.è.Â... |
| 0030h: | 4C | 57 | 7D | 00 | FC | 29 | 7D | 00 | 0C | 38 | 7D | 00 | 84 | C0 | 81 | 00 | LW}.ü)}..8}.„À.. |
| 0040h: | 00 | 00 | 00 | 00 | 48 | 01 | 00 | 00 | 19 | FA | 3C | 92 | 00 | 05 | 00 | 88 | ....H....ú<'...^ |
| 0050h: | 18 | EE | 92 | 00 | 88 | 83 | 92 | 00 | A8 | 05 | 92 | 00 | 58 | 83 | 92 | 00 | .î'.^ƒ'.¨.'.Xƒ'. |
| 0060h: | F8 | 82 | 92 | 00 | A0 | 83 | 92 | 00 | 38 | EE | 92 | 00 | 00 | 00 | 00 | 00 | ø,'. ƒ'.8î'..... |
| 0070h: | 12 | FA | 03 | 92 | 00 | 06 | 00 | 88 | 23 | E7 | BD | 91 | E7 | 9B | 98 | E8 | .ú.'...^#ç½'ç›˜è |
| 0080h: | AE | A4 | E8 | AF | 81 | E4 | BF | A1 | E6 | 81 | AF | 0A | 00 | 00 | 00 | 00 | ®¤è¯.ä¿¡æ.¯..... |
| 0090h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 17 | FA | 06 | 92 | 00 | 07 | 00 | 88 | .........ú.'...^ |
| 00A0h: | 43 | 4C | 4F | 55 | 44 | 5F | 44 | 49 | 53 | 4B | 5F | 43 | 52 | 45 | 44 | 53 | CLOUD_DISK_CREDS |
| 00B0h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 00C0h: | 68 | FA | 0D | 92 | 00 | 08 | 00 | 80 | | | | | | | | | hú.'...€ |

In addition, the backdoor has its own uninstall feature that allows it to remove itself from the compromised machine, in addition to retrieving arbitrary files and executing commands from the C2 server.

**Custom ObjectiveC classes of GIMMICK**

There are three custom Objective-C classes of GIMMICK malware, and here below we have mentioned them all:-

- DriveManager
- FileManager
- GCDTimerManager

**Recommendations**

To prevent similar attacks Volexity has recommended the following mitigations:-

- Always audit and monitor the persistence locations.
- To keep track of anomalous proxy activity and internal scanning always monitor network traffic.
- On macOS, systems make sure to enable XProtect and MRT from Apple.
- Always use complex passwords.
- Make sure to enable a multi-factor security mechanism.

**You can follow us on Linkedin, Twitter, Facebook for daily Cybersecurity and hacking news updates**.



Source: https://cybersecuritynews.com/gimmick-malware-attacks/