


TA505 begins summer campaigns with a new pet malware downloader, AndroMut, in the UAE, South Korea, Singapore, and the United States

 proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south

July 2, 2019





[Blog](#)

[Threat Insight](#)

TA505 begins summer campaigns with a new pet malware downloader, AndroMut, in the UAE, South Korea, Singapore, and the United States



July 02, 2019 Matthew Mesa and Dennis Schwarz with the Proofpoint Threat Insight Team

Overview

Throughout 2018, Proofpoint researchers observed threat actors increasingly distributing downloaders, backdoors, information stealers, remote access trojans (RATs), and more as they abandoned ransomware as their primary payload. In November 2018, [TA505](#), a prolific actor that has been at the forefront of this trend, began distributing a new backdoor we named “[ServHelper](#)”. ServHelper has two variants: one focused on remote desktop functions and a second that primarily functioned as a downloader.

In June 2019, TA505 appears to have introduced yet another new downloader malware, AndroMut, which has some similarities in code and behavior to Andromeda, a long-established malware family. Proofpoint research has observed AndroMut download malware referred to as “FlawedAmmy.” FlawedAmmy is a full-featured RAT that was first observed in early 2016 and is based on the leaked source code of a legitimate shareware tool, Ammy.

- Also Read: [Leaked Ammy Admin Source Code Turned into Malware](#)
- Also Read: [Andromeda Under the Microscope \(Avast\)](#)

Campaign Analysis

Proofpoint researchers observed two distinct campaigns by TA505 that used AndroMut to download FlawedAmmy.

The first campaign used the following message details to target recipients in South Korea:

Sender Name:

백승기

Subject:

쌍용 인보이스 1234

URLs

See IOCs

Sender Name:

최성은

Subject:

송금증 \$123.12

Attachment Names:

- 20.06.2019 송금증 123.12.doc
- 20.06.2019 송금증 123.12.xls
- 20.06.2019 송금증 123.12.htm
- 20.06.2019 송금증 123.12.html

Sender Name:

"Kim, DongHoon (Dongtan_Con)"

Subject:

견적서

Attachment Names:

Cml-123456-1.xls

The HTM or HTML attachments contained links to the download of an Office file. Depending on the specific case, the delivered Word or Excel file used macros to execute a Msiexec command that would download and execute either the FlawedAmmy loader or AndroMut. In the cases that involved AndroMut, Proofpoint researchers observed it downloading FlawedAmmy.

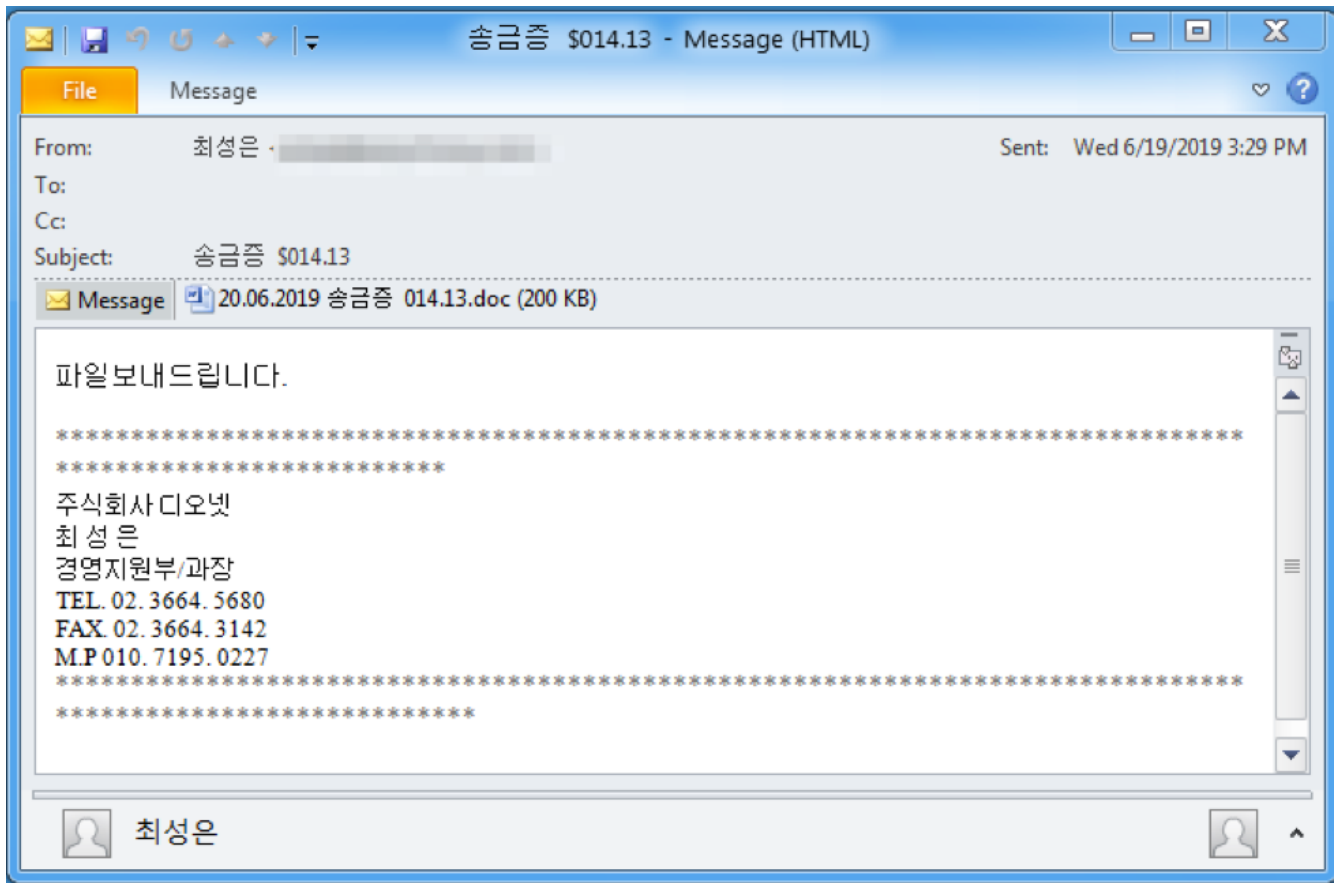


Figure 1: Example TA505 email used to deliver AndroMut

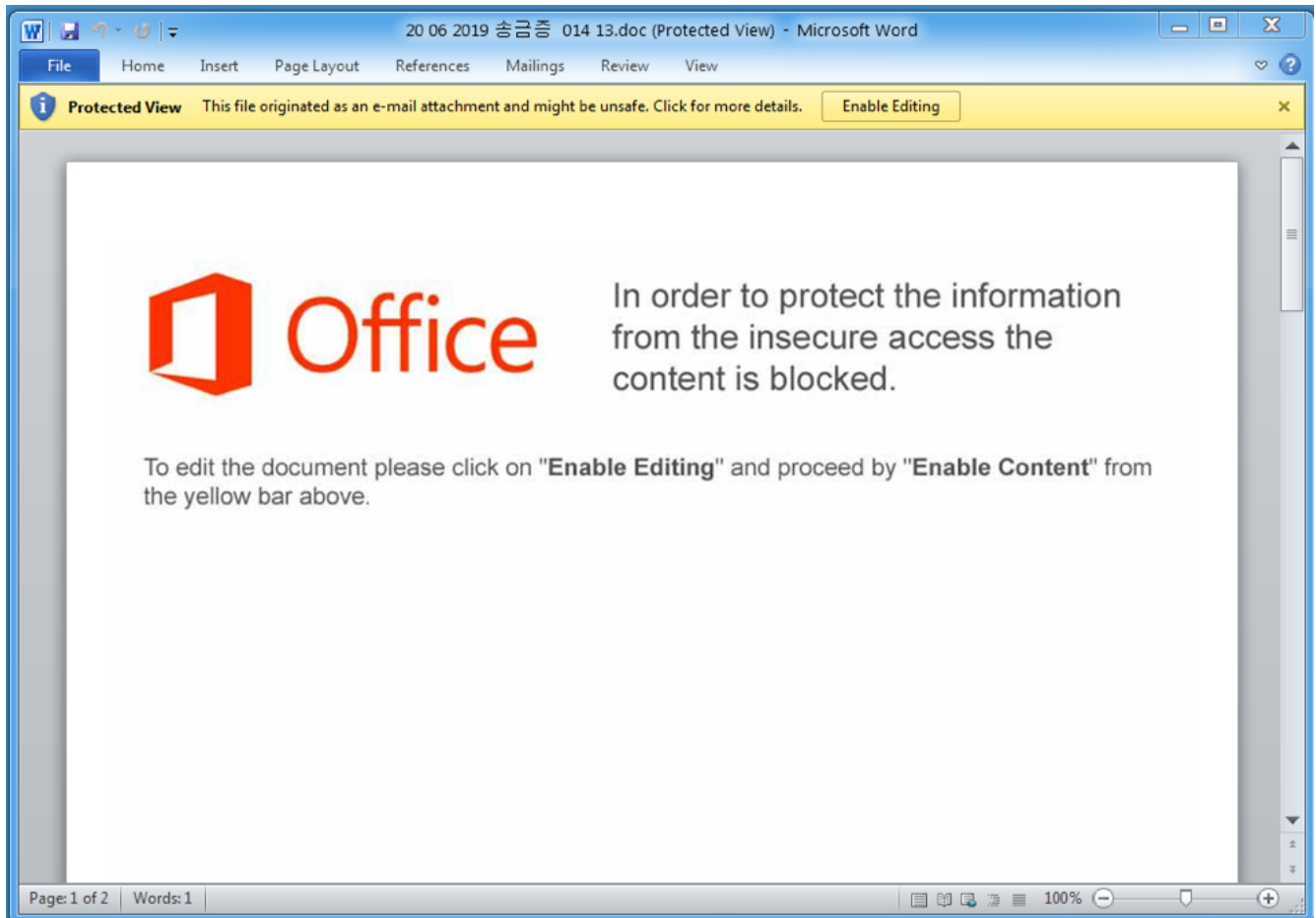


Figure 2: Example TA505 document used to deliver AndroMut

The second campaign targeted recipients at financial institutions in Singapore, UAE, and the USA. The message lures used the following details:

Sender:

Mir Imran Medhi

Subject:

Invoice & DOs

Attachments Names:

- invoice-5601.doc
- invoice.xls

Sender Name:

Ong Kai Chin

Subject:

Profoma Invoice_1234

Attachments Names:

invoice-1234.doc

Sender Name:

Rejeesh Aj

Subject:

request for holding cheque

Attachments Names:

- request.doc
- Rq20061901.doc

Again, depending on the specific case, the delivered Word or Excel file used macros to execute a Msiexec command that would download and execute either the FlawedAmmy loader or AndroMut. In the cases that involved AndroMut, we observed it downloading FlawedAmmy.

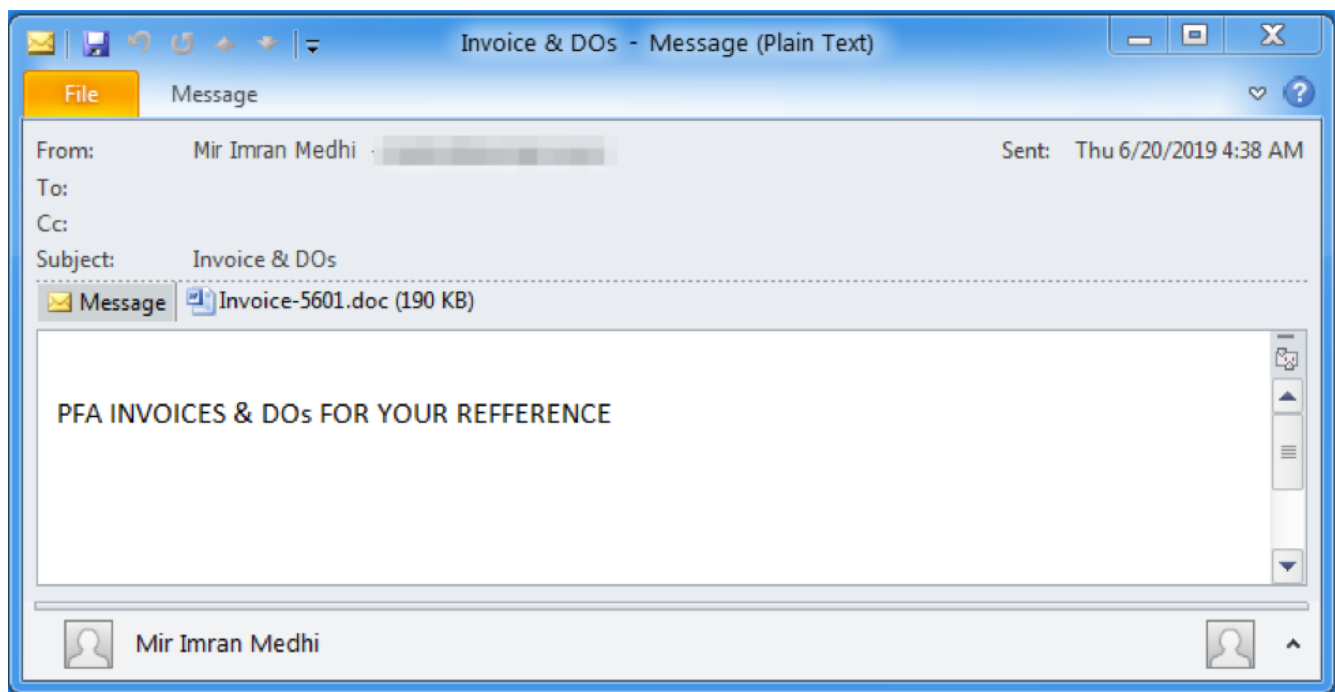


Figure 3: Example TA505 email with attachments used to deliver AndroMut

AndroMut Malware Analysis

AndroMut is a new downloader malware written in C++ that Proofpoint researchers began observing in the wild in June 2019. The “Andro” part of the name comes from some of the pieces which bear resemblance to another downloader malware known as Andromeda [1] and “Mut” is based off a mutex that the analyzed sample creates: “mutshellmy777”.

Windows API Calls

The malware resolves most of its Windows API calls at runtime by hash. The hashing algorithm is called “ror13AddHash32Dll” by FireEye [2] and it rotates right (ROR) each character of the DLL and API name by 13 then adds them together. Some example API hashes are:

- IstrcpyW - 0xE33D73B4
- CreateMutexW - 0x95898DFF
- socket - 0xED83E9BA

String Decryption

AndroMut decrypts strings in one of two ways:

The encrypted string is base64-decoded then decrypted with AES-256 in ECB mode. Each string has its own key and they look like 32-byte hex strings (Figure 4).

```
decrypt_str_type1("57735477746A4566636E517879496C70", "8YEK3BwtktvMeY55Db0NTg==", 1, &mutex_name, 0); // mutshellmy777
if ( init_and_anti_analysis(&mutex_name) == 1 )
{
    decrypt_str_type1("705467517264577865704F57796B4554", "cIDNE5NMsvmM/dEeyOK+FA==", 1, &up.config, 0); // up.config
    decrypt_str_type1(
        "795566766E70745149716B7454647473",
        "2tNrUo65siyatioiuUfOZdSoXNd/FiVwLtCx1FA6E/I=",
        1,
        &api.config,
        0); // C:\\Windows\\api.config
    decrypt_str_type1(
        "5562456E7579667A70756D5945736B57",
        "CUqyj0d22cw3pX3zxXIp9X6nlfj0I+vZpGshIzw0mJM=",
        1,
        &ComputerDefaults.exe,
        0); // ComputerDefaults.exe
    decrypt_str_type1("66456F7776734F756368774F746A6449", "p8L9Z2DGYnaK0zFCuZkoKg==", 1, &propsys.dll, 0); // propsys.dll
}
```

Figure 4: Example of Type 1 Encrypted Strings

The encrypted string is stored as a stack string. Each string decrypts by performing a unique math problem -- we were unable to observe any compelling patterns in the mathematics. Figure 5 shows an example of the string "cmd /C" being decrypted. An equivalent Python snippet of the code is available on Github [3].

```
enc_word = 0xE56E246F;
v203 = 0x83600269;
index = 0;
v204 = 0x2166A063;
v205 = 0x8F5C8E5D;
v206 = 0x8C5B;
do
{
    v64 = ~((~*(&enc_word + index) ^ 0x7942) + 1) - index - 36192;
    v65 = index + (((v64 << 15) | (v64 >> 1)) & 0xFFFF) + 54873;
    v66 = (index + (((v65 << 9) | (v65 >> 7)) & 0xFFFF)) << 7;
    *(&enc_word + index) = (16 * ((v66 | ((index + ((v65 << 9) | (v65 >> 7))) >> 9)) - 3641)) | (((v66 | ((index + ((v65 << 9) | (v65 >> 7))) >> 9)) - 3641) >> 12);
    ++index;
}
while ( index < 9 ); // "cmd /C"
```

Figure 5: Example of Type 2 Encrypted String

Anti-Analysis

In addition to Windows API hashing and string encryption, AndroMut uses the following anti-analysis techniques:

- Checks for sandboxing by looking for the following process names:
 - cmdvirth.exe (COMODO)
 - SbieSvc.exe (Sandboxie)
 - VMSvc.exe (Virtual PC)
 - xenservice.exe (Xen)
- Checks for mouse movement

- Checks for the Wine emulator by looking for the “HKEY_CURRENT_USER\SOFTWARE\Wine” subkey in the Registry
- Checks for debuggers by looking for debugging flags set in the NtGlobalFlag field of its Process Environment Block (PEB)
- Checks for debuggers by setting a “Puleg” mutex, setting the HANDLE_FLAG_PROTECT_FROM_CLOSE flag on the mutex handle, then trying to close the handle
- Explicitly zeroing memory after using important data

Persistence

Depending on user privileges the malware creates persistence by either scheduling a task that executes a created LNK file in the Recycle Bin or via the “Registry run” method.

Configuration

AndroMut contains five configuration pieces and stores them as type 1 encrypted strings:

- Command and control (C&C) host
- C&C port
- C&C URI
- Encryption key used in C&C
- JSON key used in C&C

Command and Control

The URL is constructed from the configuration and C&C communication is established using HTTP POST requests. An example response to such a request is depicted in Figure 6:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 12 Jun 2017 12:33:33 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Status: 200 OK

{"w": "B905D2A999F5152CDC26C2968815B71B74A89832E7CE844188C89935B0A97E0E05B1D4F8B8A218A159822B0FFC1FCE02"}
```

Figure 6: Example C&C response

Request and response data are both JSON objects that contain the configured JSON key (in the analyzed sample, the key was “w”). The key values can be decrypted by hex-decoding and decrypting with AES-256 in ECB using the configured C&C key (in the analyzed sample, the key was “736769476A5162373558736B71703962”).

An example plaintext request looks like:

```
{
  "data": {
```

```

    "arch": true,

    "cmd": 1,

    "os": "Win7",

    "rights": true,

    "tid": "<16 uppercase hex digits>"

}
}

```

It is a JSON object that contains a data key which contains the following keys:

- tid - Bot ID
- os - Windows version
- arch - "true" indicates x64
- rights - "true" indicates admin privileges
- cmd - Command response code

An example plaintext response looks like:

```

{
  "status": "200",

  "wmjf": "rtjlafogqsebkxuy"
}

```

The "status" key maps to different commands. The rest of the keys are command-specific arguments. AndroMut is able to execute the following commands:

- 100 - Remove self and exit
- 200 - Initial beacon response. Argument is not used and appears to be random padding
- 300 - Base64 decodes the "data" value, saves it the %TEMP% directory using the "name" value, then executes it with the CreateProcessW Windows API. See below for an example:

```

{
  "data": "TVqQAAMA...",

  "name": "okbrjzxp.tmp",

  "size": "797048",

  "status": "300",

  "type": "application/x-msdownload"
}

```

Other "status" codes include:

- 301 - Similar to “300” command, but executes the file using “cmd[.]exe [/]C”
- 302 - Similar to “300” command, but executes the file using the LoadLibraryEx Windows API
- 303 - Update self

Payloads

At the time of publication Proofpoint researchers have only seen AndroMut deliver the FlawedAmmy Remote Access Trojan (RAT) [4] in the above TA505 campaigns.

Similarity to Other Malware

While Proofpoint researchers believe that AndroMut is a new malware family, it is worth mentioning in passing that some of its analysis felt familiar. Proofpoint has observed some low-confidence overlaps between it and two other malware downloaders: Andromeda [1] and QtLoader [5] [6]. The research into the latter malware also noted some similarities to Andromeda.

Conclusion

TA505 has helped shape the threat landscape for years, largely because of the massive volumes associated with their campaigns through the end of 2017 and into 2018. Over the last two years, Proofpoint researchers have observed TA505 and a number of other actors focus on downloaders, RATs, information stealers, and banking Trojans. With this new June 2019 push, commercial banking verticals in the United States, UAE, and Singapore appear to be the primary targets as part of TA505’s usual “follow the money” behavioral pattern. The new AndroMut downloader, when combined with the FlawedAmmy RAT as its payload appears to be TA505’s new pet for the summer of 2019.

References

- [1] <https://malpedia.caad.fkie.fraunhofer.de/details/win.andromeda>
- [2] https://github.com/fireeye/flare-ida/tree/master/shellcode_hashes
- [3] <https://github.com/EmergingThreats/threatresearch/tree/master/andromut>
- [4] <https://www.proofpoint.com/us/threat-insight/post/leaked-ammy-admin-source-code-turned-malware>
- [5] <https://malpedia.caad.fkie.fraunhofer.de/details/win.qtbot>
- [6] <https://twitter.com/sysopfb/status/921396006431969280>

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
hxxp://greenthumbsup[.]jip/20.06.2019_746.38.doc	URL	TA505 Document

hxxp://fakers[.]co[.]jip/20.06.2019_130.22.doc	URL	TA505 Document
hxxp://nagomi-753[.]jip/20.06.2019_800.77.doc	URL	TA505 Document
hxxp://nanepashemet[.]com/20.06.2019_781.37.xls	URL	TA505 Excel File
52f0aaff3654110e82586d21b07c8a3de23dc9efb3f4001daf412286282315c0	SHA256	TA505 Document
d0aaf465a2569abbdcbafc049be1c1a643572f4ca185058833310435bfa53358	SHA256	TA505 Document
eb3792fc83cd65823bc466e7253caf12064826b058230666d2ed51542ac59275	SHA256	TA505 Excel File
f21039af47e7660bf8ef002dfcdb0c0f779210482ee1778ab7e7f51e8233e35c	SHA256	TA505 Document
3e3eb26211459eb2d8b52a2429a52e7e12d2145d7733823d7415663537a0b6ca	SHA256	TA505 HTML
8621fa54946096ed38aee5cbcc068c0620416a05c17328a527673e808847850d	SHA256	TA505 Excel File
c4963dcf6b32459740f6a3d3b4d06d9dc06f15087ca01775956df36206543301	SHA256	TA505 Document
a905838db6e6617edd9d25baaaee9c209381d456e809081977e27c3e0b15793	SHA256	TA505 Document
59af9102a921130fd1d120f6cee7fc7cdfc28292a7a4a8c24233126604aa9443	SHA256	TA505 Document
98b584b31457b21d0d48fcc78093439638e15dd1705e54182d9aa4ffad014c3a	SHA256	TA505 Excel File
bb5054f0ec4e6980f65fb9329a0b5acec1ed936053c3ef0938b5fa02a9daf7ee	SHA256	AndroMut
hxxp://kreewalk[.]com:80/viewforum.php	URL	C&C
5eddc55c0c445baf2752d56229fa384b7e3f1c7e76b22f43e389c6a711aa713a	SHA256	FlawedAmmyy

ET and ETPRO Suricata/Snort Signatures

2836975 ETPRO TROJAN AndroMut Checkin

[Subscribe to the Proofpoint Blog](#)