Severity

High

Analysis Summary

APT-17 group aka BITTER APT group has been recently active and targeting sectors in South Asia for information theft and espionage. This group has a history of targeting Energy, Engineering, Government in South Asia. Spear phishing emails have been the main strike force to target their victims and they've been doing it for years now. Many BITTER victims have been exploited through relatively popular Microsoft Office exploit, in order to download and execute a RAT binary from a website. Although the attack vector of this sample remains unknown of yet, this is an indication of their presence again in the South Asian region

As part of an ongoing effort that began in August 2021, this threat actor group known for targeting China, Pakistan, and Saudi Arabia has expanded to set its sights on Bangladeshi government agencies. With a spear-phishing email, this campaign targets an elite unit of Bangladesh's government. Emails may contain a malicious RTF document or a Microsoft Excel spreadsheet that is used to exploit known vulnerabilities. The Equation Editor application is automatically launched once the victim opens the maldoc to run the embedded objects containing the shellcode to exploit known vulnerabilities described by CVE-2017-11882, CVE-2018-0798, and CVE-2018-0802 in Microsoft Office, and then downloads and runs the trojan from the hosting server on the victim's machine. The trojan runs itself in this campaign, but the actor has more RATs and downloaders in their arsenal.

Impact

- Information Theft and Espionage

Indicators of Compromise

Domain Name

- olmajhnservice[.]com
- levarisnetqlsvc[.]net
- urocakpmpanel[.]com
- tomcruefrshsvc[.]com
- autodefragapp[.]com
- helpdesk[.]autodefragapp[.]com

MD5

- bdbbd70229591fb1102365f4bb22196b
- 5e5201514800509b2e75a3fcffad7405
- 72a7130e98119ecd70c4e0f6ce9c0030
- 527dc131149644af439e0e8f96a2c4eb
- bf51119c8b0673a9cfee1c384d1e236a
- 2a340b72e16fb1ece13d7f553ec3c266
- b9025eca96614a473e204e9e8a873e1d
- 59b043a913014a1f03258c695b9333af
- 2c8ed4045b76a1eca8c8d0161a4b65ec
- 2454a5b5f7793d372c96fd572c1de2cc

SHA-256

- b0b687977eee41ee7c3ed0d9d179e8c00181f0c0db64eebc0005a5c6325e8a82
- f7ed5eec6d1869498f2fca8f989125326b2d8cee8dcacf3bc9315ae7566963db
- 490e9582b00e2622e56447f76de4c038ae0b658a022e6bc44f9eb0ddf0720de6
- b7765ff16309baacff3b19d1a1a5dd7850a1640392f64f19353e8a608b5a28c5
- ce922a20a73182c18101dae7e5acfc240deb43c1007709c20ea74c1dd35d2b12

- e4545764e0c54ed1e1321a038fa2c1921b5b70a591c95b24127f1b9de7212af8
- fa0ed2faa3da831976fee90860ac39d50484b20bee692ce7f0ec35a15670fa92
- 3fdf291e39e93305ebc9df19ba480ebd60845053b0b606a620bf482d0f09f4d3
- 69b397400043ec7036e23c225d8d562fdcd3be887f0d076b93f6fcaae8f3dd61
- 90fd32f8f7b494331ab1429712b1735c3d864c8c8a2461a5ab67b05023821787

SHA-1

- b12e459dd3857f5379ac99e48def4ad2b8a3aa16
- 33f7efb563052da4d25405dd7f0366bb3bff5b26
- d297031f13599df567b3b8c1ed1cb7cd32bf758d
- 3ba50221785aa8d1f2dea2894fc9a9449e826724
- 3d540373b74ed12df6b21e1ea21566907fba04a1
- 7a94a3dcd68792877a4ca8747e23ec084b12da16
- 2360e4cff14fbfb2af6c80dbd7028d682fe2634e
- 2af2dcd9482a281228d987723640203e08ff93c9
- b17f0381fc7e4c4c6bb15dfcc0c37d2945266c6e
- bcd7a2191af9ddb1bd627e36a55fc55680e36f51

URL

- http[:]//autodefragapp[.]com/
- http[:]//olmajhnservice[.]com/updateReqServ10893x[.]php?x=035347
- http[:]//olmajhnservice[.]com/
- https[:]//olmajhnservice[.]com/nt[.]php/?dt=%25computername%25-BKP&ct=BKP
- http[:]//olmajhnservice[.]com/nxl/nx
- http[:]//olmajhnservice[.]com/nxl/nx/
- http[:]//olmajhnservice[.]com/nt[.]php/?dt=
- https[:]//olmajhnservice[.]com/nt[.]php/?dt=%25computername%25-EX-2&ct=2
- https[:]//olmajhnservice[.]com/nt[.]php/?dt=%25computername%25-EX-1
- http[:]//olmajhnservice[.]com/nt[.]php?dt=%25computername%25-ex-1&
- http[:]//olmajhnservice[.]com/nt[.]php
- http[:]//olmajhnservice[.]com/nt[.]php/
- http[:]//olmajhnservice[.]com/nt[.]php/?dt=%25username%25-EX-3ct=1
- https[:]//olmajhnservice[.]com/nt[.]php/?dt=%25computername%25-EX-1&ct=1
- https[:]//olmajhnservice[.]com/nt[.]php/?dt=%25computername%25-EX-3&ct=3
- http[:]//levarisnetqlsvc[.]net/drw/drw
- http[:]//levarisnetqlsvc[.]net/lt[.]php
- http[:]//levarisnetqlsvc[.]net/
- http[:]//levarisnetqlsvc[.]net/jig/gij
- https[:]//levarisnetqlsvc[.]net/lt[.]php/?dt=%25computername%25-LT-2&ct=LT
- http[:]//urocakpmpanel[.]com/axl/ax
- http[:]//urocakpmpanel[.]com/nt[.]php?dt=%25computername%25-****
- https[:]//urocakpmpanel[.]com/
- http[:]//urocakpmpanel[.]com[:]33324/
- https[:]//urocakpmpanel[.]com/nt[.]php

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.