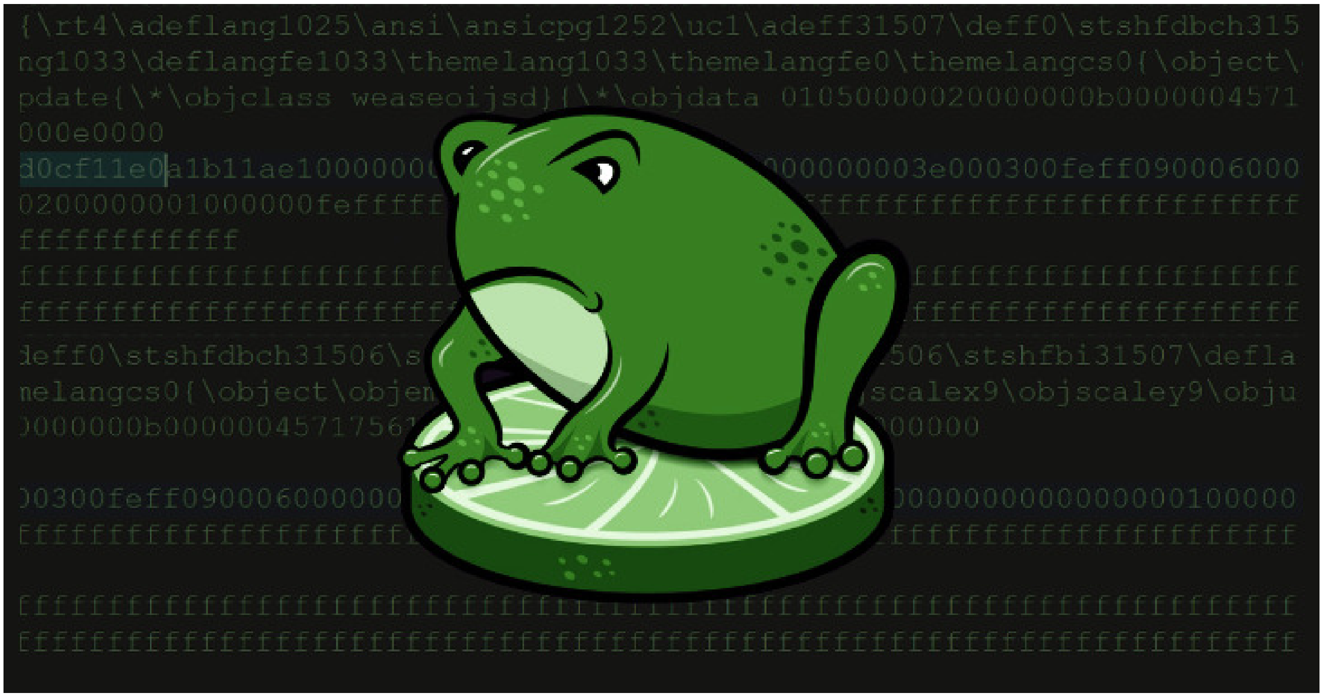
Bitter APT Hackers Add Bangladesh to Their List of Targets in South Asia

thehackernews.com/2022/05/bitter-apt-hackers-add-bangladesh-to.html

May 11, 2022


{\rt4\adeflang1025\ansi\ansicpg1252\uc1\adeff31507\deff0\stshfdbch315
ng1033\deflangfe1033\themelang1033\themelangfe0\themelangcs0{\object\
pdate{*\objclass weaseoijsd}{*\objdata 01050000020000000b0000004571
000e0000
d0cf11e0a1b11ae1000000
00000003e000300feff090006000
0200000001000000feffff
ffffffffffffffffffffffffff
ffffffffffff
deff0\stshfdbch31506\s
506\stshfbi31507\defla
nelangcs0{\object\objen
scalex9\objscaley9\obju
0000000b000000457175
00000
00300feff090006000000
000000000000000100000

An espionage-focused threat actor known for targeting China, Pakistan, and Saudi Arabia has expanded to set its sights on Bangladeshi government organizations as part of an ongoing campaign that commenced in August 2021.

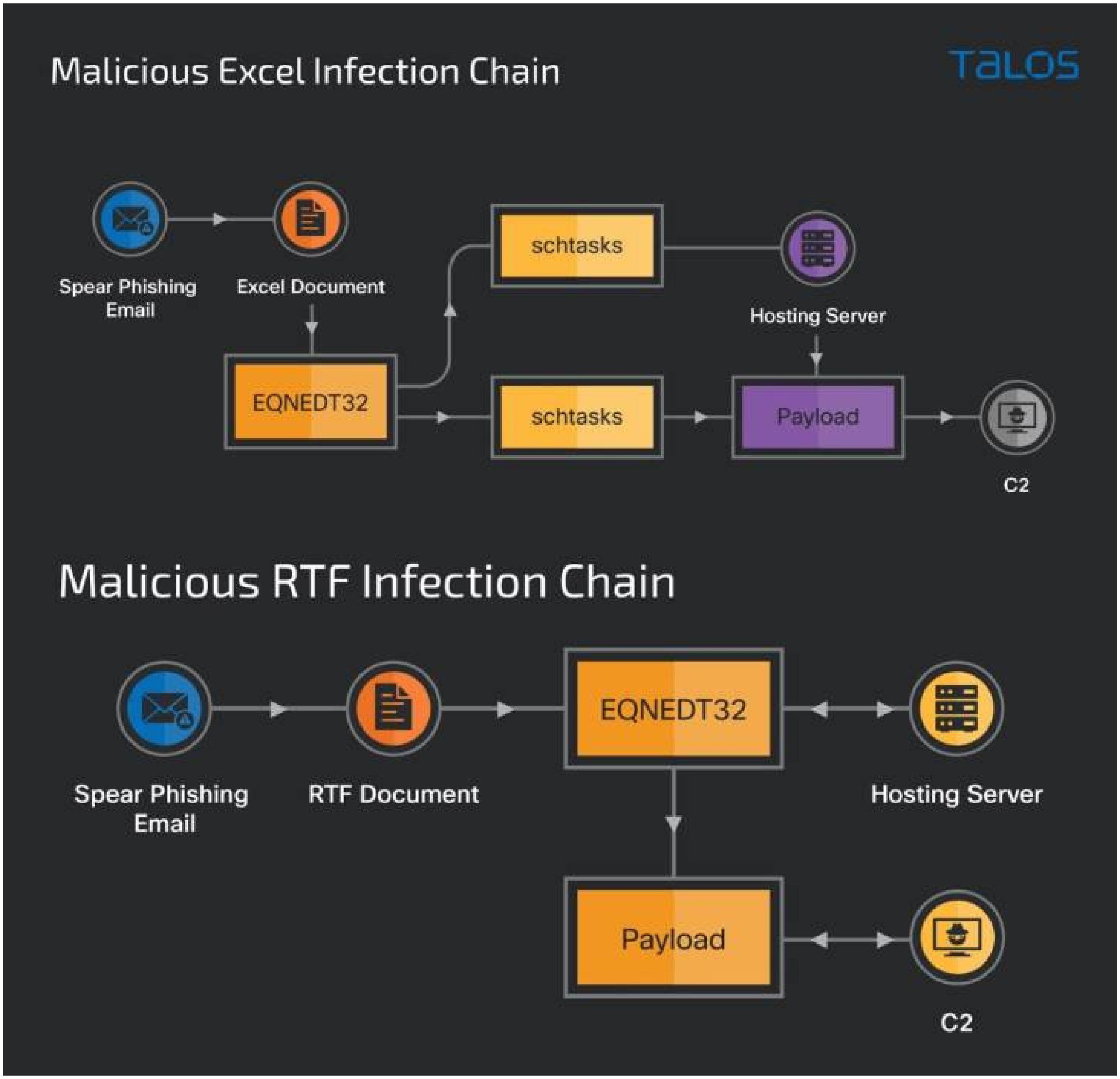
Cybersecurity firm Cisco Talos attributed the activity with moderate confidence to a hacking group dubbed the Bitter APT based on overlaps in the command-and-control (C2) infrastructure with that of prior campaigns mounted by the same actor.

"Bangladesh fits the profile we have defined for this threat actor, previously targeting Southeast Asian countries including China, Pakistan, and Saudi Arabia," Vitor Ventura, lead security researcher at Cisco Talos for EMEA and Asia, told The Hacker News.

"And now, in this latest campaign, they have widened their reach to Bangladesh. Any new country in southeast Asia being targeted by Bitter APT shouldn't be of surprise."

Bitter (aka APT-C-08 or T-APT-17) is suspected to be a South Asian hacking group motivated primarily by intelligence gathering, an operation that's facilitated by means of malware such as BitterRAT, ArtraDownloader, and AndroRAT. Prominent targets include the energy, engineering, and government sectors.

The earliest attacks distributing the mobile version of BitterRAT date back to September 2014, with the actor having a history of leveraging zero-day flaws — CVE-2021-1732 and CVE-2021-28310 — to its advantage and accomplishing its adversarial objectives.



The latest campaign, targeting an elite entity of the Bangladesh government, involves sending spear-phishing emails to high-ranking officers of the Rapid Action Battalion Unit of the Bangladesh police (RAB).

As is typically observed in other social engineering attacks of this kind, the missives are designed to lure the recipients into opening a weaponized RTF document or a Microsoft Excel spreadsheet that exploits previously known flaws in the software to deploy a new trojan dubbed "ZxxZ."

ZxxZ, named so after a separator used by the malware when sending information back to the C2 server, is a 32-bit Windows executable compiled in Visual C++.

"The trojan masquerades as a Windows Security update service and allows the malicious actor to perform remote code execution, allowing the attacker to perform any other activities by installing other tools," the researchers explained.

While the malicious RTF document exploits a memory corruption vulnerability in Microsoft Office's Equation Editor (CVE-2017-11882), the Excel file abuses two remote code execution flaws, CVE-2018-0798 and CVE-2018-0802, to activate the infection sequence.

"Actors often change their tools to avoid detection or attribution, this is part of the lifecycle of a threat actor showing its capability and determination," Ventura said.

SHARE □ □ □ □
SHARE □
cybersecurity, hacking news