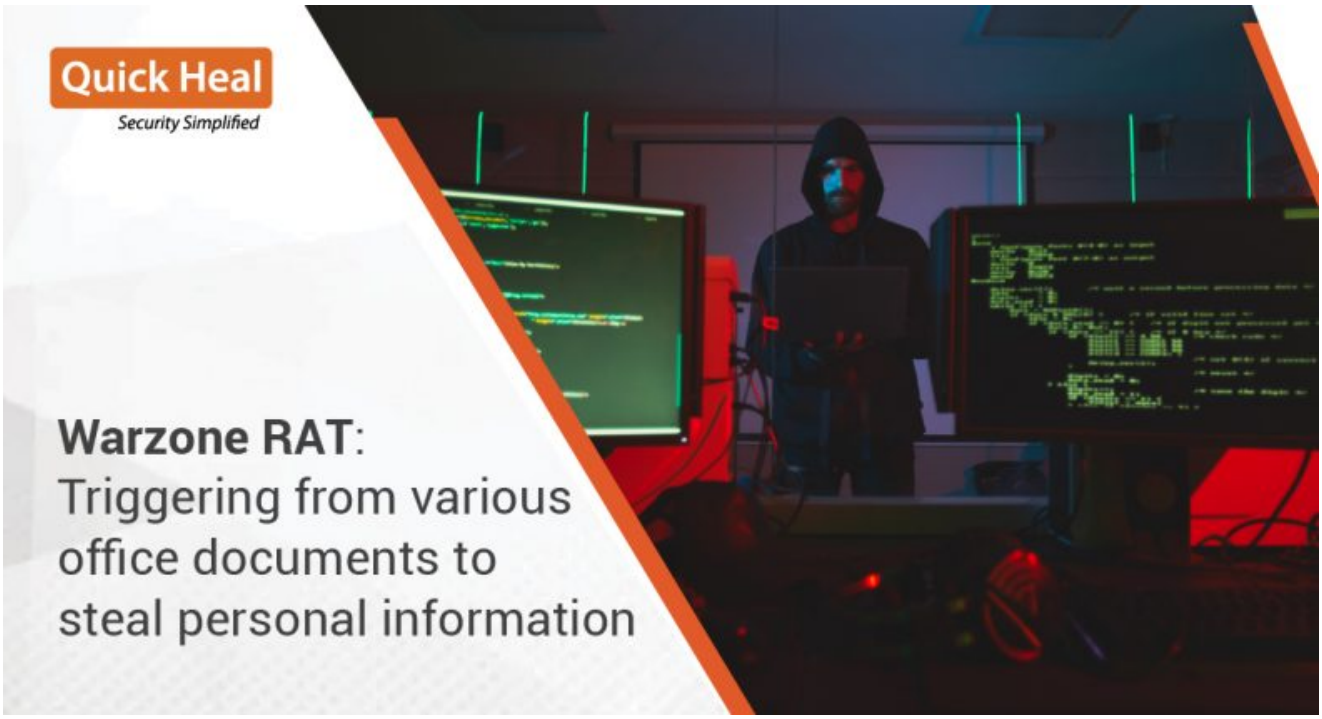
WARZONE RAT – Beware Of The Trojan Malware Stealing Data Triggering From Various Office Documents

blogs.quickheal.com/warzone-rat-beware-of-the-trojan-malware-stealing-data-triggering-from-various-office-documents/

July 1, 2021



Warzone RAT is part of an APT campaign named “Confucius.” Confucius APT is known to target government sectors of China and few other South Asian countries. This APT campaign was quite active around January 2021. Warzone RAT first emerged in 2018 as malware-as-a-service (MaaS) and is known for its aggressive use of “.docx” files as its initial infection vector. The initial payload is known as “Ave Maria Stealer,” which can steal credentials and log keystrokes on the victim’s machine. The advanced version of this malware is currently sold in the underground market for $22.95 per month and $49.95 for three months. The Warzone creators have an official website where it’s up for sale.

Figure 1: Warzone website showing selling price

These are the various features of the RAT mentioned on the website:

- Remote Desktop & Webcam
- Privilege Escalation – UAC Bypass
- Password Recovery
- Download & Execute.
- Live Keylogger
- Remote Shell
- Persistence
- Windows Defender Bypass

We came across a cracked version of Warzone RAT on GitHub. Here is the screenshot of that repository:

Figure 2: A cracked version of warzone on GitHub

Based on our research, we confirmed that the threat actor is trying to circumvent attacks with a decoy and manipulate users, delivering the next stage payload via template injection technique. In this blog, we are going to talk about ".docx" used as an initial attack vector and how it's delivering its final payload -Warzone RAT.

Technical Analysis:

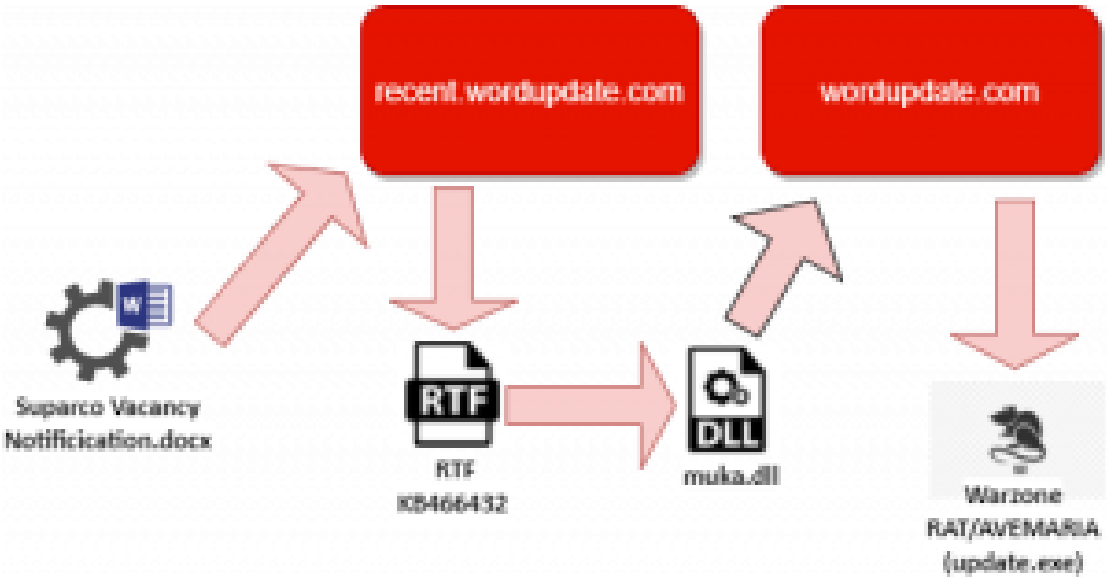


Figure 3: Attack Chain

The various phases of the attack are:

- The victim opens the word document.
- This document further downloads an RTF exploit (CVE-2017-11882).
- Exploit in RTF is triggered and muka.dll is dropped and executed.
- Muka.dll downloads Warzone RAT.

Phase 1:

Here the infection chain starts with a ".docx" file. We can see below the decoy document (Hash: *59ccfff73bdb8567e7673a57b73f86fc082b0e4eeaa3faf7e92875c35bf4f62c*). This decoy document was crafted by attackers to induce the victims.

پیک سکلز آرگنائزیشن کو اپنے اسلام آباد آفس کے لئے ذیل میں درج ذیل شعبہ میں باصلاحیت اور پروفیشنل افراد کی خدمات کنٹریکٹ کی بنیاد پر درخواستیں درکار ہیں۔

آسامی کا نام	تعلیمی قابلیت اور تجربہ کی تفصیل
ٹیلی کام آپریٹر -II	انٹرمیڈیٹ (فرسٹ ڈویژن) ہمراہ متعلقہ شعبہ 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 اترنے کی صورت میں شارٹ لسٹنگ کی خلاف ورزی نہیں ہوگی۔ اگر 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 کوئی ٹی اے/ڈی اے نہیں دیا جائے گا۔

درخواست دینے کا طریقہ

اپنے تحریر کردہ درخواست ہمراہ شناختی کارڈ کی مصدقہ نقل، ڈومیسائل کارڈ کی دو (02) عدد پاسپورٹ سائز تصاویر جن کی پشت پر امیدوار کا نام، پتہ اور تعلیمی و تجربہ کی اسناد کی تصدیق شدہ نقول منسلک کرکے 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)

Advt Reference (Ref No: 20-04)	Job Code :	Post applied for : Telecom Operator-II	Field : Admin	Location Interested

PERSONAL INFORMATION:

Name: _____ Father's Name: _____

Date of birth: dd/mm/yy | CNIC NO: | | | | | | | | | | | | | |

Religion: (Muslim, Hindu, Christian, Ahmadi or others): _____ Marital status: _____ (Single/e: _____

Postal Address: _____

Permanent Address: _____

Phone No: (with area code): _____ Mobile No: _____

E-mail Address: _____

Photograph

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

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

EXPERIENCE:

S.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 or Strategic nature

COURSES/TRAININGS:

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

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

Date of Application: _____ Signature of Candidate: _____

Figure 4: Screenshot from the "Suparco Vacancy Notification.docx"

While executing, it uses the template injection technique to download the next stage RTF exploit. This exploit delivers a dll embedded final payload that connects to the domain to connect to the CNC to download payload Warzone Rat. We can see from the below image.

Figure 5: Using Template Injection Technique

The RTF exploit is downloaded through “\word_rels\settings.xml.rels” file present in document structure using template injection technique as shown below.

Figure 6: settings.xml.rels containing a link to the template

Phase 2:

The downloaded RTF file (Hash: *686847b331ace1b93b48528ba50507cbf0f9b59aef5b5f539a7d6f2246135424*) contains code that exploits an old vulnerability “CVE-2017-11882”. The flaw resides within equation editor (EQNEDT32.exe), a component in Microsoft office that inserts or edits object linking and embedding (OLE) Objects. We found that muka.dll is embedded in an OLE object.

Figure 7: muka.dll embedded in an ole object

Phase 3:

The embedded muka.dll file (Hash: *1c41a03c65108e0d965b250dc9b3388a267909df9f36c3fefffbd26d512a2126*) contains export function zenu and this dll is used to provide functionalities to other programs. Here is an image showing this:

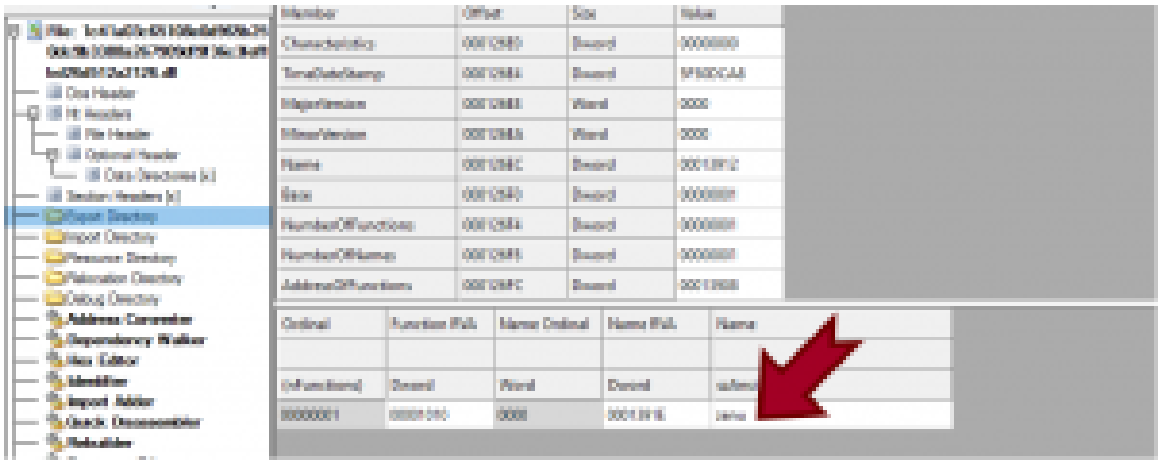


Figure 8: Export directory containing export function zenu

Phase 4:

Upon successful exploitation, the dll connects to a malicious domain (*wordupdate.com*) which is active nowadays also and downloads the final warzone payload.

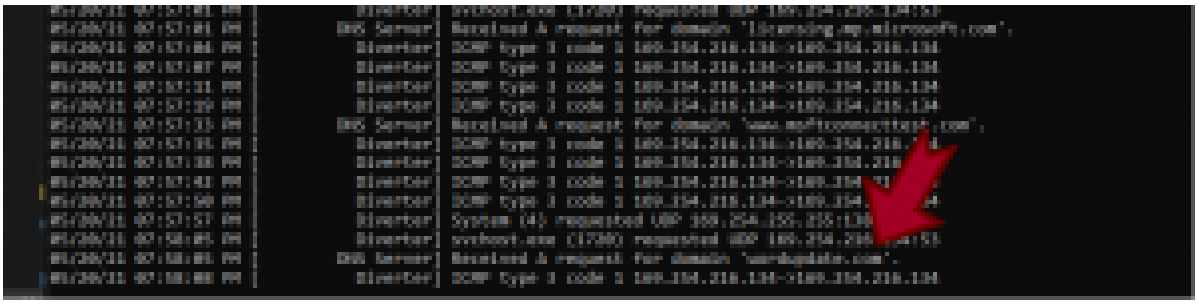


Figure 9: Requesting access to the malicious domain

The Warzone payload is saved as update.exe (Hash: *7dd1dba508f4b74d50a22f41f0efe3ff4bc30339e9eef45d390d32de2aa2ca2b*).

Conclusion:

Warzone RAT exploits a pretty old but popular vulnerability, “CVE-2017-11882,” in Microsoft’s equation editor component. This RAT works as an Info stealer malware. Attackers typically spread such malware through document files as email attachments. We recommend our customers not to access suspicious emails/attachments and keep their AV software up-to-date to protect their systems from such complex malware. We detect the initial infection vector as well as the final Warzone RAT as XML.Downloader.39387 and Trojan.GenericRI.S16988580 respectively.

IOCs:

- DOCX:*59ccfff73bdb8567e7673a57b73f86fc082b0e4eeaa3faf7e92875c35bf4f62c*
- RTF:*686847b331ace1b93b48528ba50507cbf0f9b59aef5b5f539a7d6f2246135424*
- DLL:*1c41a03c65108e0d965b250dc9b3388a267909df9f36c3fefffbd26d512a2126*
- EXE:*7dd1dba508f4b74d50a22f41f0efe3ff4bc30339e9eef45d390d32de2aa2ca2b*

Domains:

- *recent.wordupdate.com*
- *wordupdate.com*

Ayush Puri

Follow @