New Spear Phishing Campaign using Army Welfare Education Society's Scholarship form

seqrite.com/blog/new-spear-phishing-campaign-using-army-welfare-education-societys-scholarship-form/

Chaitanya Haritash March 22, 2021

22 March 2021
Written by Chaitanya Haritash

Cybersecurity

Estimated reading time: 5 minutes

Introduction:

Researchers at Quick Heal Security Labs have uncovered a potential Spear Phishing campaign targeted against Indian Army personnel. In this attack, the attackers are using "Army Welfare Education Society" Scholarship form as lure.

About AWES:

Army Welfare Education Society (AWES) manages and ensures proper education facilities to children of Indian Army personnel through Local Military Authorities. Established in 1983, the society has its office at Shankar Vihar, Delhi Cantonment and over the years has opened over 137 Army Public Schools and 249 Army Pre-Primary Schools across India.

Details about the recent attack:

Document Analysis:

"ESSA-Scholarships.docx"

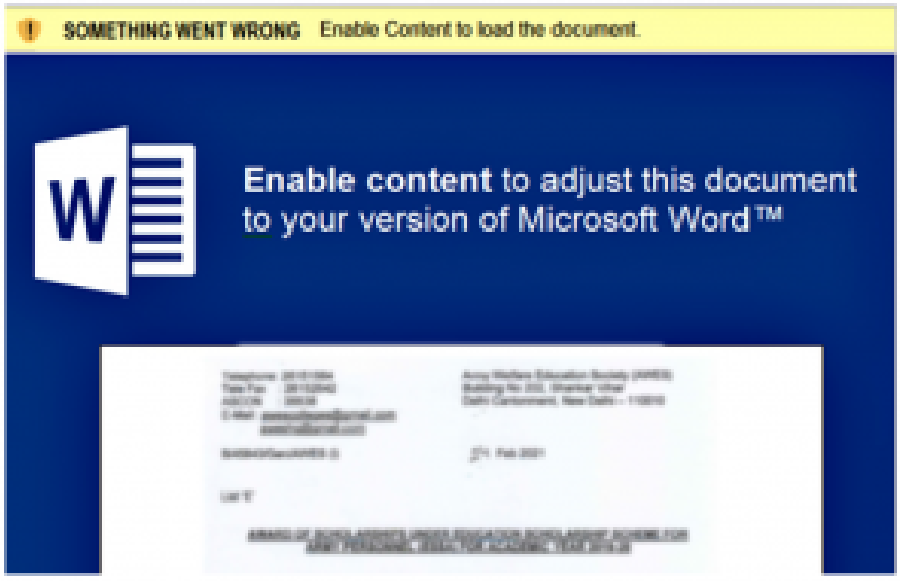


Fig.1 Template

Fig.2 ESSA-Scholarships.docx

The “ESSA-Scholarships.docx” triggers CVE-2017-0199 vulnerability which later launches the stage of “.dotm” file from landing page embedded inside “settings.xml.rels”.

This technique is popularly known as “Template Injection” as well and is popular among threat actors since the detection is trivial.

“essa.dotm”

As soon as the user disables “Protected View”, the previous stage downloads and executes “essa.dotm” which further executes the macros.

```
Sub Tournament(ByVal str As String)


Dim count As Integer
Dim myname As String
Dim buttercake As Object
count = 386
If count < 431 Then
myname = "Robertjunior"
Set buttercake = CreateObject("Excel.Sheet")
Dim petabytes As Object
Set petabytes = CreateObject("WScript.Shell")

vegetables = Array("tomato", "lady", "finger")
Dim vegetablenames As Variant
Dim iterate As String

For Each Item In vegetables
    vegetablenames = vegetablenames & Item & Chr(10)
    iterate = Item & Chr(10)
    If iterate = "lady" Then myname = "uejamc"

Next
For i = 1 To 10
    Call ReturnMeFavor("Bigger nd Better")
    If i = 5 Then petabytes.Run (GiveMe(2)), 0, False
Next i



End If

End Sub
```

Fig.3 Extracting Data

All the data of staged payloads are stored inside “UserForum.TextBox”. The macro has four text boxes as object, containing all the data to be dropped on disc as files and initiate further stages.

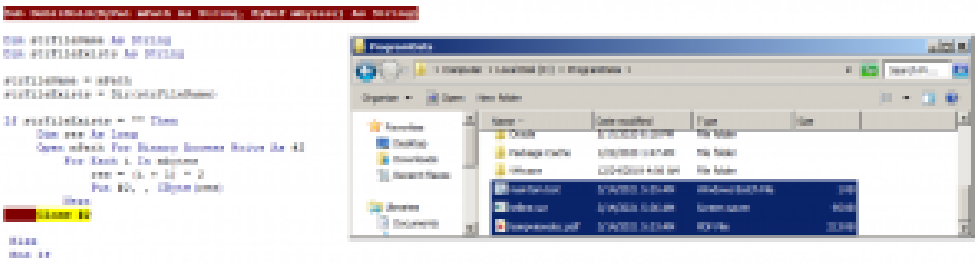


Fig.4 Routine for Saving all the files

Executable Payload Analysis:

“fixit.exe”: This tends to behave as loader unless command is not issued from command and control. The payload is completely new, written in .NET and does not perform too many actions.

Fig.5 Information collection

The payload comes with .scr extension and once executed, it collects the following information about infected host using WMI Queries:

1; Processer ID.
2; User Name.
3; General Details (Architecture, Caption, Version).
4; Check for Device Type (Laptop/Desktop).
5; Device Model.

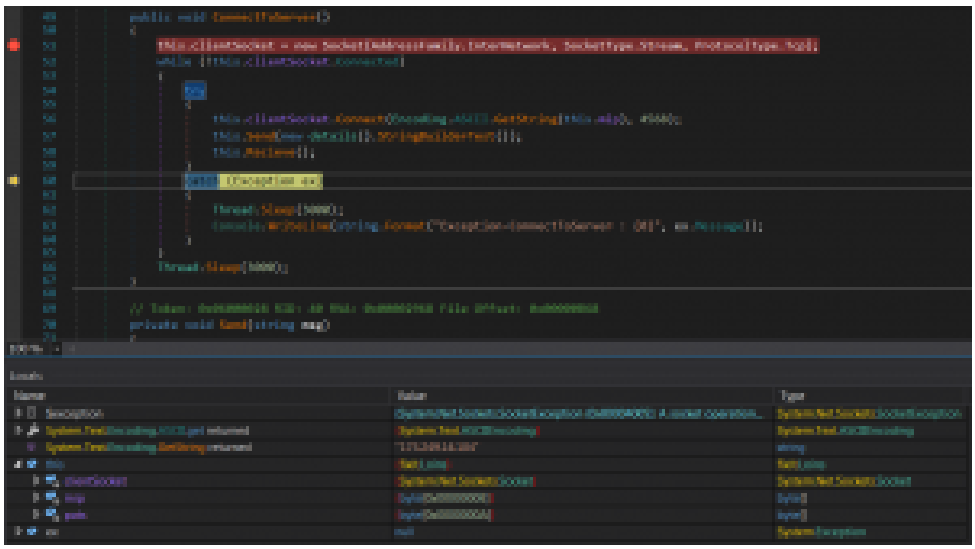


Fig.6 Initial knock being sent to C2

Once information is collected about the host, the payload sends it to C&C and performs following actions according to command issued from C&C:

1; Get Process List.

Fig.7 Sending Running Process List

If command “q7&F%2 ” is issued from C2, payload sends list of running processes by using “Process.GetProcesses()” and creates an array of list.

2; Write and Execute Files:

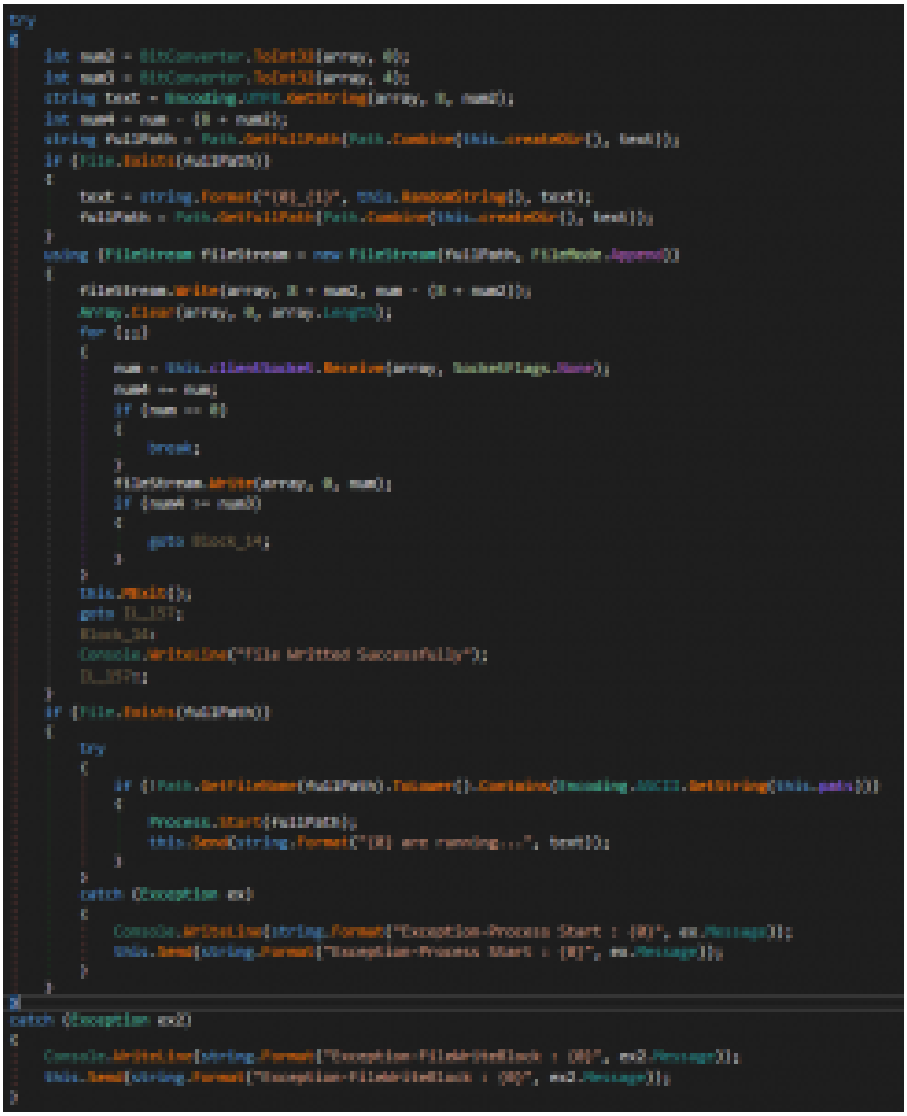


Fig.8 Write and Execute Routine

Once C2 responds back with command, the payload receives files and execute on current folder.

Persistence:

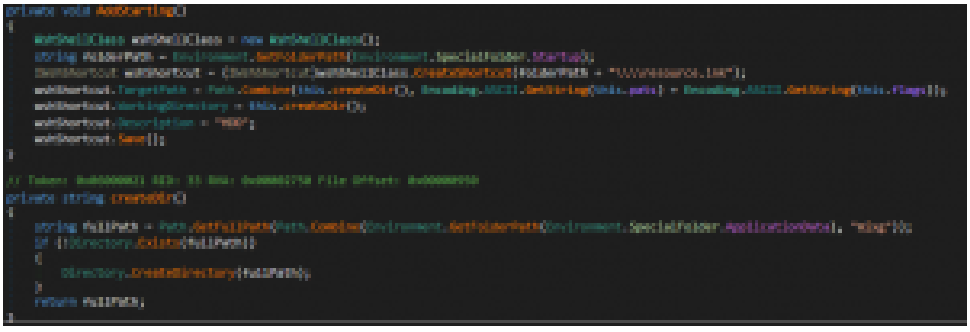
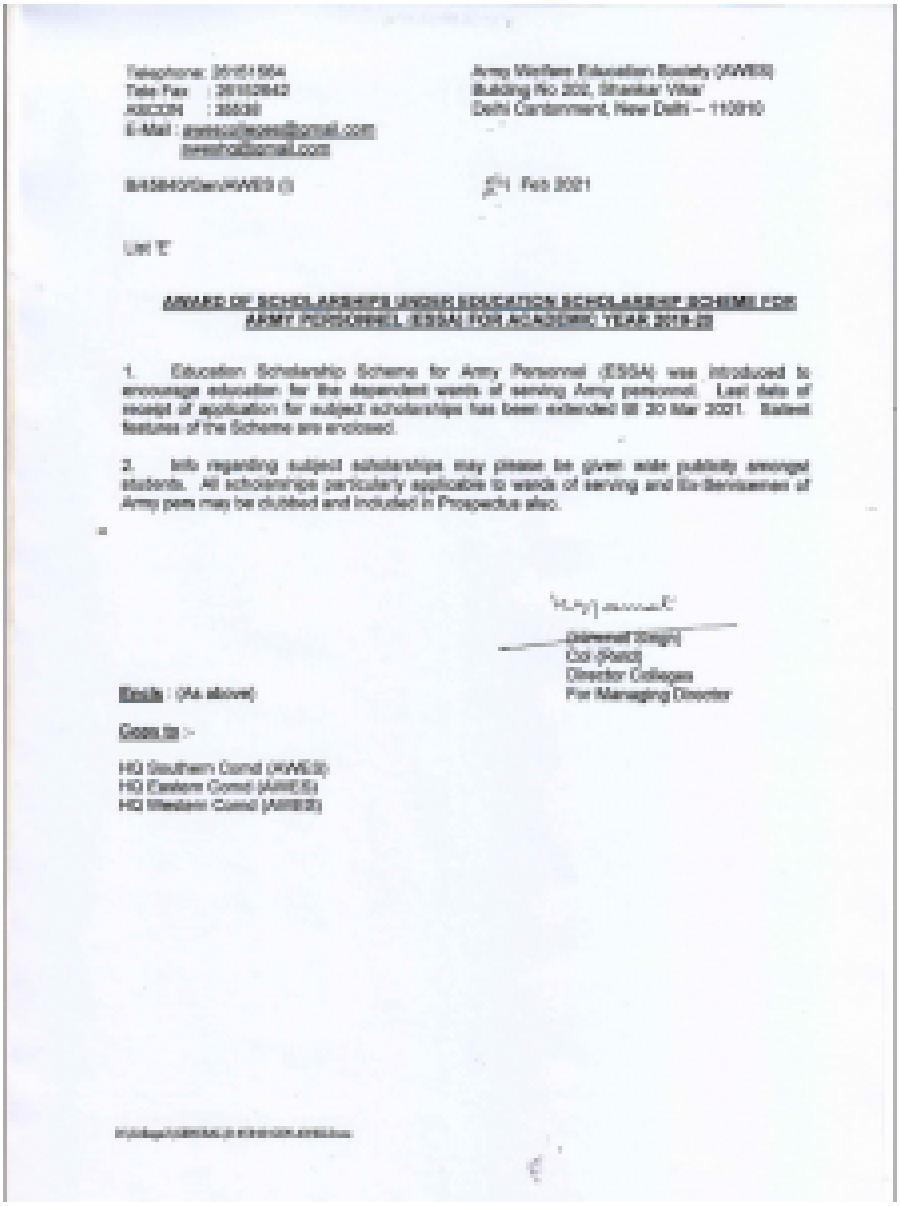


Fig.9 Creating Persistence

Payload gains persistence on infected host by writing LNK file to “Startup Folder”. It’s a well-known technique used by other threat actors. Payload loads an assembly which is publicly available called “IWshRuntimeLibrary.dll” and tries to create a LNK file in target folder giving reference to running payload’s working directory.



Telephone: [illegible]
Tele Fax : [illegible]
AGCDN : [illegible]
E-Mail : [illegible]

Army Welfare Education Society (AWES)
Building No 202, Shankar Vihar
Delhi Cantonment, New Delhi – 110010

[illegible]/Gen/AWES (i)

01 Feb 2021

List 'E'

AWARD OF SCHOLARSHIPS UNDER EDUCATION SCHOLARSHIP SCHEME FOR ARMY PERSONNEL (ESSA) FOR ACADEMIC YEAR 2019-20

1. Education Scholarship Scheme for Army Personnel (ESSA) was introduced to encourage education for the dependent wards of serving Army personnel. Last date of receipt of application for subject scholarships has been extended till 30 Mar 2021. Salient features of the Scheme are enclosed.

2. Info regarding subject scholarships may please be given wide publicity amongst students. All scholarships particularly applicable to wards of serving and Ex-Servicemen of Army pers may be clubbed and included in Prospectus also.

[illegible]
[illegible]
Col (Retd)
Director Colleges
For Managing Director

Encls : (As above)

Copy to :-

HQ Southern Comd (AWES)
HQ Eastern Comd (AWES)
HQ Western Comd (AWES)

[illegible]

Taken from – https://www.aitpune.com/Notices/Scholarship/ESSA-Circular.pdf

Once whole chain executed successfully, the macro opens PDF file dropped in ProgramData directory, which is publicly available.

Conclusion:

If the attack is successful, attackers they may be able to exfiltrate sensitive data from the victim machine. Our further analysis and observation is still on to identify which group is behind this attack. Till then, we advise AWES to exercise caution and inform all their members about this attack.

MITRE ATT&CK TTPs:

Spear Phishing with Attachment	T1566.001
Template Injection	T1221
User Execution: Malicious .docx and xls	T1204.002
Write Files to disc	T1006

Connects to Command And Control	TA0011
Persistence: Write LNK file to Startup Folder	T1547.001

How Quick Heal protects its users:

We have the following detections for the malicious samples:

VBA.Trojan.41523

O97M.Downloader.41522

Trojan.Perseus.S19235058

Trojan.Perseus.S19221636

Trojan.MSIL

Also, the domains and IPs used are classified as malicious by Quick Heal URLCAT.

IOCs:

Documents: CVE-2017-0199	
74e41223ec6359a9bd05bbce36b452fd046aaad64617f459ba262a5210925942	ESSA-Scholarships.docx
d035e96f54abe59dcdbc2156e55cd0135ec420f8e97aca7f109ee8d062baa755	irlaforyou.docx
d4b36731cb37ad05b0b9678b568c10a56f2e84967b393b626afb19d2df41c9b9	SARS_Eligible_Clubs___Resorts.xls

Templates :	
fc3dd043b795a1cedb8b7e1e5471f15c0b5c17c237f634c60c4e0a92d980914b	essa.dotm
108a5035ab40b13b489f8a1fb8fd8bdb5880368c9c18e1d244df23b8d5a26d67	temp.dotm
9fc84eadba969bd12cda144750cef361bcdff224026eb3921d8d46a5a424da5b	temp.dotm

Executables:	
d0a5ffa3b9c40eb1e4277e7c41a100b0836c9424b36fb9bbe281711c0b116883	fixit.exe
4c21c88399d95a3602aaacf85a83c8aaac5ae7b6bf192c4c25cef4f9224b6f7b	pixelworks.exe
2491caddf4445d9297404493c7707b54591c989b94fd4634a7afdf54c0d22e9c	sapesvx.exe
979f7952dd2225c149f1766b4bca020b680364a77ddb6006cfa462543e0a6440	winsuffix.exe
c7dbca435039a6148dc25208f04b734465e8b7c92010ede1401d88f5f8003f2d	foxpackage.exe
871cab3256acdbc3c27650adde878658568a85b87e85d3e3c137bdeb4592fb2c	amdSfx.exe
1eb0d373cea19124687ed4bffb0da3f80f98a18b9e0bebd3c12443f0a3d81689	modempx.exe
814ed2b9ae0770d727a8cd83581b4865b2abe16f8190240c5c1e821e22a280ab	foxpackage.exe
dd47cf8ec70658af85e0cd23922462ac788305034fe78ed725bb90c1a3fa04cc	scriptpbox.exe

Domains:

templatesmanagersync.info
10feeds.com

Landing Pages:
hxxp://templatesmanagersync.info/essa.dotm
hxxp://10feeds.com/temp.dotm

IP :
173.249.14.104

Subject matter Experts:

Chaitanya Haritash

Shayak Tarafdar

Chaitanya Haritash works as Security Researcher in Security Labs at QuickHeal. His main focus is on hunting unique threats and writing detection. Chaitanya is...

Articles by Chaitanya Haritash »

No Comments

Leave a Reply.Your email address will not be published.