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] 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.

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 –

a53399476a73154681fd
4d39614be6b7b41c20865eb
979434eb49fd69851a706

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 units.
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.” 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.

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 Ptynenko, 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** - ef05a612ebfc0954746e81b0b40f2a73e2a5d65c55373fa06cc32cf9fe92951b

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.
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
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 file 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.
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.
### MITRE ATT&CK™

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

### 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.
<table>
<thead>
<tr>
<th>SHA256</th>
<th>FirstSeen</th>
<th>FileName</th>
<th>Template URL</th>
<th>Template Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>481eee236eadf6c947857820d3a5f3a97cae8b4c45791f0bbd3da21f080786e75</td>
<td>2019-09-04 14:08:07</td>
<td>04.09.2019.docx</td>
<td><a href="http://libre-templates.ddns.net/internet.dot">http://libre-templates.ddns.net/internet.dot</a></td>
<td></td>
</tr>
<tr>
<td>9a13848680905f4630bc8615c5252a26405af08da1857fabc7297d66c69b5c1</td>
<td>2019-09-05 13:20:02</td>
<td>протокол.docx</td>
<td><a href="http://libre-templates.ddns.net/internet.dot">http://libre-templates.ddns.net/internet.dot</a></td>
<td></td>
</tr>
<tr>
<td>f071e1338464c6d05913cbe422956c8f6d683c66199e4b48cc5ca598f346a9f</td>
<td>2019-09-09 13:01:01</td>
<td>запит.docx</td>
<td><a href="http://office-constructor.ddns.net/net/zaput.dot">http://office-constructor.ddns.net/net/zaput.dot</a></td>
<td></td>
</tr>
<tr>
<td>e68001e37577a90980409dcdbdfd925a40e0f750475922195d2649f3d207821</td>
<td>2019-09-10 08:09:44</td>
<td>запит.docx</td>
<td><a href="http://office-constructor.ddns.net/net/zaput.dot">http://office-constructor.ddns.net/net/zaput.dot</a></td>
<td></td>
</tr>
<tr>
<td>bf55c8d6c1ba6232cf5648831ed8e8e9a7e7e07eacc1a92e91b74ae573ca9b2</td>
<td>2019-09-10 10:41:24</td>
<td>Planning.docx</td>
<td><a href="http://librebooton.ddns.net/net/booton.dot">http://librebooton.ddns.net/net/booton.dot</a></td>
<td></td>
</tr>
<tr>
<td>17d813f4f54ac7883f3dbf6da4d1c30d4df3f8eeedd1da2713ce2bb824c1697ba</td>
<td>2019-09-10 10:42:52</td>
<td>PARP.docx</td>
<td><a href="http://librebooton.ddns.net/net/booton.dot">http://librebooton.ddns.net/net/booton.dot</a></td>
<td></td>
</tr>
<tr>
<td>3b00f6802bfba4ba4b55dc82a26343bb599f833b530f1903c26ddcb3994094</td>
<td>2019-11-06 14:09:15</td>
<td>Документ Microsoft Office Word.docx</td>
<td><a href="http://inbox-office.ddns.net/inbox.dot">http://inbox-office.ddns.net/inbox.dot</a></td>
<td></td>
</tr>
<tr>
<td>b3b06267814370d32ea0ab8bd802bcaef127ad98ee41d9c805555efbd1ab8b187</td>
<td>2019-11-07 13:16:52</td>
<td>Інформаційна безпека України.docx</td>
<td><a href="http://office-crash.ddns.net/crash.dot">http://office-crash.ddns.net/crash.dot</a></td>
<td></td>
</tr>
<tr>
<td>da1291742f5bcb2e2d54c4aae4fcdd86b539fa686e79f0994bb681b391c8f3ce</td>
<td>2019-11-07 17:26:43</td>
<td>Запит.docx</td>
<td><a href="http://micro-set.ddns.net/net/micro.dot">http://micro-set.ddns.net/net/micro.dot</a></td>
<td></td>
</tr>
<tr>
<td>8d0c02d05b5a439fe2cfe1e7df45d5b2c784af89226dc640324256b708e31</td>
<td>2019-11-08 16:15:21</td>
<td>Запит.docx</td>
<td><a href="http://office-lite.ddns.net/net/lite.dot">http://office-lite.ddns.net/net/lite.dot</a></td>
<td></td>
</tr>
<tr>
<td>64c6a60f51761b22b94914a6974e8478aad05b7f91ba87dd8c1d1f0b79e4249</td>
<td>2019-11-11 10:47:13</td>
<td>довідка.docx</td>
<td><a href="http://word-gread.ddns.net/net/gread.dot">http://word-gread.ddns.net/net/gread.dot</a></td>
<td></td>
</tr>
<tr>
<td>76aab8e1861c1264b340cf37483c6c473b04d042cd6bdfa9ce51d086cb5a1a</td>
<td>2019-11-18 10:26:49</td>
<td>провадження.docx</td>
<td><a href="http://win-apu.ddns.net/apu.dot">http://win-apu.ddns.net/apu.dot</a></td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>Date</td>
<td>File Name</td>
<td>HTTP URL</td>
<td>HTTP URL</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
<td>-----------------------</td>
<td>----------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>ef05a612ebfc0954746e81b0b40f2a73e2a5d65c53573fa06cc32cf9fe92951b</td>
<td>2019-11-19 8:57:23</td>
<td>Матеріали.docx</td>
<td><a href="http://win-ss.ddns%5B.%5Dnet/ss.dot">http://win-ss.ddns[.]net/ss.dot</a></td>
<td><a href="http://get-icons.ddns%5B.%5Dnet/%5BComputerName+SerialNumber%5D/autoindex.php">http://get-icons.ddns[.]net/[ComputerName+SerialNumber]/autoindex.php</a></td>
</tr>
<tr>
<td>647dfdf939de6a8df97572c389910c8fe4b469676162e6f02e23ef79e3be4868</td>
<td>2019-11-21 14:46:46</td>
<td>ровид 343_9130.docx</td>
<td><a href="http://win-gu.ddns%5B.%5Dnet/win.dot">http://win-gu.ddns[.]net/win.dot</a></td>
<td></td>
</tr>
<tr>
<td>47723574d99719733f87e1859e80cfdb88c5482428344593d2d025bf2108368</td>
<td>2019-11-25 12:24:29</td>
<td>Запит_ГУР.docx</td>
<td><a href="http://yotaset.ddns%5B.%5Dnet/yota.dot">http://yotaset.ddns[.]net/yota.dot</a></td>
<td></td>
</tr>
<tr>
<td>730074e625245c3075aace0eb0d4fbb31717f0845651e990224c0ace3618e5a1b</td>
<td>2019-11-25 14:34:59</td>
<td>підозра.docx</td>
<td><a href="http://win-gu.ddns%5B.%5Dnet/gu.dot">http://win-gu.ddns[.]net/gu.dot</a></td>
<td></td>
</tr>
<tr>
<td>72dbd31ce620869c0f7238e93d7f6aa628773d0ff382487157bbf8b98f275a</td>
<td>2019-11-25 14:39:20</td>
<td>Запит_СЗР.docx</td>
<td><a href="http://yotaset.ddns%5B.%5Dnet/yota.dot">http://yotaset.ddns[.]net/yota.dot</a></td>
<td></td>
</tr>
<tr>
<td>f8c110022c7c8d03f60d5a53cbafbe9ea2b54cdc596e31b3f8e3ff203c2733bd</td>
<td>2019-11-26 15:29:39</td>
<td>розрахунок.docx</td>
<td><a href="http://zariks.ddns%5B.%5Dnet/word.dot">http://zariks.ddns[.]net/word.dot</a></td>
<td><a href="http://kavkazwork.ddns%5B.%5Dnet/%5BComputerName+SerialNumber%5D/rebootor.php">http://kavkazwork.ddns[.]net/[ComputerName+SerialNumber]/rebootor.php</a></td>
</tr>
<tr>
<td>1f185b6d28c8e87142d8fb0f8172caf56924ab1812c3dca218bb7da5e01d23b54</td>
<td>2019-11-28 10:35:58</td>
<td>Запит_СБУ.docx</td>
<td><a href="http://ironiya.ddns%5B.%5Dnet/is.dot">http://ironiya.ddns[.]net/is.dot</a></td>
<td><a href="http://korneliuswork.ddns%5B.%5Dnet/%5BComputerName+SerialNumber%5D/rebootor.php">http://korneliuswork.ddns[.]net/[ComputerName+SerialNumber]/rebootor.php</a></td>
</tr>
<tr>
<td>03d46971fdf32ef2d5f647a12bf272dd28fb58a777f025a717b6e017e64d5a3</td>
<td>2019-11-29 7:33:12</td>
<td>Запит_СБУ.docx</td>
<td><a href="http://ironiya.ddns%5B.%5Dnet/il.dot">http://ironiya.ddns[.]net/il.dot</a></td>
<td><a href="http://korneliuswork.ddns%5B.%5Dnet/%5BComputerName+SerialNumber%5D/rebootor.php">http://korneliuswork.ddns[.]net/[ComputerName+SerialNumber]/rebootor.php</a></td>
</tr>
</tbody>
</table>
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
- 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

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