Ransom Cloud 0365

Discover how could be the new generation of Ransomware and protect yourself in time.

2016-06-16
Índice

Executive Summary ........................................................................................................................................... 3
1. Introduction: Spam Phishing & Spear Phishing Attacks ................................................................................................................. 3
2. Accounts Theft in IdPs .......................................................................................................................................................... 4
3. Spear Phishing: Attacks and countermeasures .................................................................................................................. 4
4. OAuth in a nutshell ................................................................................................................................................................. 6
   4.1. Access request ............................................................................................................................................................ 7
   4.2. Access Approval ........................................................................................................................................................ 8
   4.3. Access Achievement ................................................................................................................................................... 9
5. Construction of the O365 application Ramson Cloud ........................................................................................................... 10
6. Construction of the URL request Scopes .......................................................................................................................... 13
7. Attacking Office 365 Accounts .......................................................................................................................................... 16
   7.1. JWT (JSON Web Token) ............................................................................................................................................... 17
   7.2. Actions on the Office 365 account via OAuth token .................................................................................................. 19
   7.3. Office 365 email hijack ............................................................................................................................................... 21
   7.4. Decrypting the emails .................................................................................................................................................. 24
8. Attacking Windows Live Mail y OneDrive accounts ........................................................................................................... 25
9. App review inside the Identity Providers .......................................................................................................................... 27
10. Recommendations against Spear Apps attacks .................................................................................................................. 29
    10.1. New safety training for users ....................................................................................................................................... 29
    10.2. The use of the SOC’s Cloud ......................................................................................................................................... 30
    10.3. Solutions: Public Cloud Encryption ......................................................................................................................... 31
    10.4. Application of the 2nd Factor Authorization solutions ............................................................................................ 32
11. Final thoughts ........................................................................................................................................................................ 32
About ElevenPaths ......................................................................................................................................................... 33
More information ................................................................................................................................................................. 33
Executive Summary

Today, the world of ransomware has become a profitable business for the world of cybercrime, from which individuals and organizations are extorted in a simple but lucrative way: encrypting files by infecting the computers and then demanding money for the decryption keys. This scheme we have seen it exploited through spam campaigns, infections Exploit kits or the use of binary infected P2P networks. On the other hand, in the world of e-mail services, many organizations have begun to use public cloud schemes to offer service to this, based on popular platforms such as Microsoft Office 365 or Gmail. On these platforms, the ability to integrate related applications allows an attacker to gain access to email without obtaining the user name and password, and bypassing the 2nd Factor Authentication systems. Getting together spam attacks, with the creation of a malicious app created for Office 365 or Gmail platforms, you can build an effective ransomware specially designed for these services. In this article we explain the operation of O365 RansomCloud, a ransomware specially designed to attack Microsoft Office 365 platforms.

1. - Introduction: Spam Phishing & Spear Phishing Attacks

In recent years we have seen a lot of attacks on organizations that have put an end with information theft and damage to the company reputation. Some of the cases in which security has been compromised have gained sufficient visibility in the technical community dedicated to information security to justify the need to invest in security measures and try to get more resistant to cyberattacks systems. The problem arises when trying to advance this investment in preventive rather than reactive measures only. In these cases, the effectiveness of the measures is not the optimal one and it is impossible not to go behind the attackers, leaving some fundamental challenges unresolved.

If we look at the origins of many of the best known of our recent years attacks, we see that most of the attacks started with a simple Spear Phishing attack. The Spear Phishing is a scam via e-mail with the aim of obtaining unauthorized access to confidential data or access resources. Unlike Phishing attacks, which are massively released, the Spear Phishing focuses on a specific organization or group of people or interest. With this type of attack, the attacker gains access to an internal identity of the organization that had set up more security measure using a username and password, without a second authentication factor or a second factor authorization (2FA&2FA).

As we will see in this document, this may still be much more complex to protect when taking into account that the attacks are aimed at theft of access email accounts, in those scenarios where you must not compromise the username and password. In these scenarios, for example, theft OAuth tokens could allow an attacker to bypass 2FA knowing that by its design the access via API using OAuth is out of these protections.
Being able to automate this fraudulent acquisition of OAuth tokens could get to the possibility to get access privileges to critical resources of the victim and implement critical attacks on them. In the following sections we will try to illustrate the feasibility of this hypothesis.

2. Accounts Theft in IdPs

In this article, the IdP (Identity Providers) we selected is Microsoft, through its services Office 365 and Windows Live, but the work is analogous to other IdP as Twitter, Facebook, Google, and so on. The aim of stealing tokens techniques is to get access to resources via API, making the user instead of delivering a set of valid credentials to submit by himself an AuthCode OAuth which allows the access to his data.

If we think about the ways in which a Office365 account can be protected against an attack we can find various scenarios:

- **Just 1FA**: In this case, the Office 365 account is protected only with a single first factor authentication (username and password). In this scenario the attacker can steal credentials via Spear Phishing attacks.

- **2FA and Application Passwords**: In this case the account is protected by a 2FA and only those customers with application-specific password (Password application) will be exempt from passing through the 2FA. In this case, the attacker needs to deal both different scenarios: to steal the Password Application of where it is stored or compromise the second factor of authentication.

- **2FA without Application Passwords**: The account has a 2FA and no use of Application Passwords, so either the user, password and 2FA it is being obtained or a network attack to session hijacking has to be done.

- **2FA without a network or 2FA access**: Si la cuenta es remota, y no hay acceso ni a la red para hacer un ataque de man in the middle ni al 2FA, parece el entorno más complicado. If we have a remote account and there is no Access to the network so we can initiate a man in the middle or 2FA attack, then the environment seems to be more complicated to hijack.

In all these cases, if we focus the efforts on stealing OAuth tokens, all scenarios could be vulnerable because none of the protective measures used apply to the attack scenario we are about to explain.

3. Spear Phishing: Attacks and countermeasures

Phishing attacks are based on tricking the user to enter his own credentials to get inside a fake web. These sites are hosted on fraudulent domains that simulate the environment known to the victim. So if you want to steal an Office365 account, you could simulate the login Office 365. If an Apple ID is desired to be stolen then the Apple ID website should be simulated (see Picture 1). That easy!
In order to attract victims to these sites, there are two types of attacks that can be made. Mass Attack, known as SPAM Phishing, which is not personalized and is being sent to a lot of recipients hoping for success based on probabilities. Orientated Attack which is directed to a specific victim, called Spear Phishing. In the latter case, the email is personalized with details that could induce the victim think the truthfulness of the message (see Picture 2). It is in this latter type of messages where attackers put their efforts when we are in a stage of APT against an organization.
To avoid Phishing, SPAM Phishing & Spear Phishing attacks, different security measures are to be used. There are various types of security measures and each one has to be applied to the different levels of the organization:

- **Awareness:** It consists in educating the user to recognize one of these attacks (Phishing, SPAM and Phishing Spear Phishing). For this reason they need to be explained that they should not give their credentials to any website that sends them an email asking for it, also to pay attention to the domain of the servers that are connected, and so on. Unfortunately, neither these recommendations are entirely correct in all cases, nor organizations encourage them to comply, as the massive and careless use of business emails inside the organization goes against them.

It is quite common to see teams contracted agencies hired for events marketing, HR consulting or various advisers to send emails to the employees of an organization requesting them to register on a website. This awareness should always be accompanied by a series of actions coherent with good practices that are intended to inculcate and not creating a false sense of security or confusion among users.

- **AntiPhishing Technology:** Both in terms of email and at browser level too, measures are integrated to detect SPAM Phishing emails as well as Phishing sites. Tools such as AntiPhishing filters of Google Safe Browsing or Microsoft Smart Screen are integrated to detect sites that are doing the Phishing. However, when we talk about targeted attacks such Spear Phishing, the thing is much more difficult to detect, and in almost all cases it passes under the radar of these technologies.

- **Second Authentication Factor:** The last bastion to prevent theft of accounts is to protect digital identities. To do so, the ideal way is to protect the account with, at least, one extra factor of authentication. This extra factor could be something that may be known just for one person (password), or something that one can have into his power (phone or physical token) or something that identifies somebody as a person (biometrics).

Some organizations use smart cards protected by biometrics means or digital certificates stored on USB tokens that can only be opened with biometrics and passwords at the same time. The choice will depend on each system. In the case of Office 365 / Windows Live can put a 2FA to protect accounts. Typically, these additional factors have to be thought to use when authenticating a different channel, a channel which is has to be completely different to the first authentication factor. Thus the probability of the attack success is reduced, as if they were to succeed in breaking the first factor would be necessary to also succeed in surpassing the second attack identity.

Unfortunately, none of these three measures will be useful to protect users against attacks designed to steal the OAuth tokens, as we will see.

4. OAuth in a nutshell

OAuth is an authorization protocol usually implemented in version 2 (OAuth2) in most IdPs Internet (see Picture 3). It is based on a licensing system where the user indicates the IdP authorizing a third party to use resources on its behalf. Thus third-party applications may access data and perform actions on a user’s resources on the IdP. To summarize the process, there are three phases:
4.1. Access request

In this first part, an application registered in the IdP provides a link to the IdP address with a list of permissions, which can be called Scopes, the application identifier and the address where to return the AuthCode in case the user authorizes the use of its resources. In case you want to access Office365, an application in Microsoft and inside the link to be sent to the user victim, the different fields discussed above will appear. Picture 4 and 5 are presented below as an example of a Spear Phishing.
4.2. Access Approval

When the user clicks or is redirected to the URL access requested, a screen on the website of IdP (Microsoft, Google, etc.) will be shown, a screen where he will be informed of the accesses that are being requested to him and also whether to grant or deny such access. That is the last barrier before granting the requesting application all the data it is asking.

When the user is not logged in the IdP services, the web that appears will be similar to the login (see Picture 6). However, in the URL you can see that there is a list of permissions that are precisely those the URL from first point has generated. On the other hand, if the user has already logged previously, it will go directly to the part of granting or denying the access permissions, like on a website shown below (see Picture 7).
If the user clicks YES, then the IdP server will generate an AuthCode at this stage so that will allow the application to request the access token to the resources.

4.3. Access Achievement

If the user granted the Auth Code in the previous phase, it is now the task of the consuming application to request the access Token. To do this you must use your ApplicationID, your Secret, your AuthCode and request that the access Token to be sent to an EndPoint. It will be where the IdP will provide you, via API, the valid token that gives access to the requested resources in the Scopes list. The application will be registered in the list of apps of granted permissions. Picture 8 shows an approved malicious app in a Windows Live account.
From now on, the Access via API will be possible to each of the IdP resources that have been previously granted, as we are to see in the following sections of this article.

5. Construction of the O365 application Ramson Cloud

Entendiendo cómo funciona el sistema descrito, ya es posible trazar cómo sería un ataque de este tipo. El esquema que se debe seguir consistiría en los siguientes puntos. Understanding how the described system works, it is possible to trace how an attack of this kind could be. The scheme to be followed consist of the following points.

1) Build a malicious application for the IdP to attack
2) Build a URL with an adequate SCOPE application (permits)
3) Getting the Auth Code when the user accepts the app
4) Requesting the Access Token with the Auth Code
5) With the Access Token access all services via API
6) Possibility of using Cloud Ransom module O365 against email and data of the user victim

So far the attack vector Spear Phishing has been described, which is using Sappo platform to carry out the theft of OAuth tokens so to access resources. The Sappo platform provides different modules that allow the attacker to manage the possibilities on the victim in a simple and flexible manner. One of the features Sappo provides is the RansomCloud. The RansomCloud allows an attacker to encrypt, decrypt and could ask for email rescue of the victim.
Here is a complete example, meaning, first the theft accounts using Sappo is carried out and then, run the RansomCloud module. Firstly we need to create an application, which will be called RamsonCloud, in the Microsoft platform to help us extract data from the accounts that rely on it. For this purpose, using any Outlook account, we must go to the address apps.dev.microsoft.com and create a new application (see Picture 9). There we will receive an Application ID and a Secret, plus we have to specify a server with an end-point, also known as Redirect URI, where we will receive the AuthCode and accessToken. This server should be in our infrastructure and we have to install a program to listen all the calls.

![Sappo Registration](image)

**Picture 9: Creating a malicious application in Microsoft**

To control the application, which we have called Sappo, inside our data infrastructure we need to register the data of the app we have just created (see Picture 10). This will allow us to make use of the API Office365 and/or Windows Live through the access Token granted to the app by the user directly from our platform.
Once we have created the app, we can create the requests for permits where the user has to click YES and for this purpose the social engineering is a very important part in the way of achieving it. In the above example we have called the app Sappo, so to make clear that is this app the user must accept, but to achieve greater impact on social engineering one should look more attractive names (see Picture 11).

Picture 10: Registering the app on our platform to launch Ransom Cloud O365

Picture 11: A malicious App called MS AntiSpam PRO O365
For our presentation, we have chosen to create an app that simulates to be a free AntiSpam Pro, which does not call too much the attention when permissions to read and write e-mail is requested. Of course, the end-point domain and the logo will be essential to give the adequate effect in each case.

6. Construction of the URL request Scopes

To obtain the necessary permissions, the user must request the Microsoft server a URL with the following format:

GET

As you can see, you need to identify that the app is the one requesting permission, in this case Client_id, then you have to specify the list of permissions to be obtained in Scope_List (see Picture 12) and, finally, that what is expected to get is an AuthCode that must be delivered in Redirect_URI.

<table>
<thead>
<tr>
<th>Scope</th>
<th>Enables</th>
</tr>
</thead>
<tbody>
<tr>
<td>wL.basic</td>
<td>Read access to a user’s basic profile info. Also enables read access to a user’s list of contacts.</td>
</tr>
<tr>
<td>wL.offline_access</td>
<td>The ability of an app to read and update a user’s info at any time. Without this scope, an app can access the user’s info only while the user is signed in to Live Connect and is using your app.</td>
</tr>
<tr>
<td>wL.signin</td>
<td>Single sign-in behavior. With single sign-in, users who are already signed in to Live Connect are also signed in to your website.</td>
</tr>
</tbody>
</table>

Picture 12: Some Windows Live Scopes

The list of permissions that exist in Windows Live is a large one (see Picture 13), and although some of them specifies that allows reading and writing the email via API, the truth is that in many of the accounts is not allowed yet. Of course, y for example, to OneDrive documents, or contact list can be accessed as we will see in one of the demos.
In the case of Office 365, those APIs to access email are available and therefore reading, sending emails, or deleting messages from different folders in the mailbox of the victim can be done (see Picture 14).

<table>
<thead>
<tr>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail.Read</td>
<td>Read e-mail. Access to folders (Inbox, Drafts, Sent, ...)</td>
</tr>
<tr>
<td>Mail.Send</td>
<td>Send e-mails</td>
</tr>
<tr>
<td>Mail.ReadWrite</td>
<td>Read &amp; Send e-mails with Outlook API in Office365</td>
</tr>
<tr>
<td>Calendars.Read</td>
<td>Read Appointments</td>
</tr>
<tr>
<td>Calendars.ReadWrite</td>
<td>Read &amp; Write Appointments</td>
</tr>
<tr>
<td>Contacts.ReadWrite</td>
<td>Read &amp; Write Contacts information</td>
</tr>
<tr>
<td>Contacts.Read</td>
<td>Read Contacts information</td>
</tr>
</tbody>
</table>

Once sent, it generates the URL, thus the next step is to have it sent to the victim through an email that will mislead him to think it is true. In our case we have chosen a Microsoft Mail that personalizes the message and sends it as if it would be a AntiSpam Pro message. This customization we do it directly from the Sappo tool, through which you only choose a new victim to whom you send a Sappo app (see Picture 15).
The mail sent in this attack is generated as if it were a real message, so in this way the user who is not especially alert against these attacks, will encounter himself with the diatribe of whether to approve or not the permits to this “magnificent” app that will allow him to have less spam in his inbox (see Picture 16).
When the victim receives the email and clicks on the link, ends up with a screen where his approval is requested (see Picture 17).

![Picture 17: Acceptance screen permits for malicious app](image)

As you can see in Picture 17, it is not a Phishing website. There is no request for users and passwords. It is under the official domain of Microsoft, with HTTPS and a green certificate as all the measures for detecting phishing attacks are being recommended. Of course, the browser phishing filter has not went off and the victim is a 2FA account configured.

Of course, on this screen it is clear that to this application, a list of permissions are being granted, permissions that if it is a malicious app then it could be very dangerous to accept. Unfortunately, as happens with the permissions of apps in the world of Android operating systems, many users accept it without understanding the real consequences of it.

7. Attacking Office 365 Accounts

Getting to this point, where the user has to choose whether to grant or deny permits, it is when the latest security measure ends. If the user decides to grant them, from this moment - and until permits are revoked or expire without any process of renegotiating the access Token - the app can access all the resources listed in the Scopes list.

When the user clicks YES in the end-point marked on the Redirect-URI an AuthCode will be received, which will allow the application to request the Access Token. This is done this way because the Access Token request must indicate the Application ID and the Secret so to show that the app’s owner himself needs the permissions. The request to be made to the Access Token are as follows:
POST common/oauth2/token HTTP/1.1

Host: https://login.microsoftonline.com

Content-Type: application/x-www-form-urlencoded

grant_type=[authorization_code]&code=[authCode]
&client_id=[client_id]&client_secret=[secret]
&redirect_uri=[redirect_uri]

As you can see, you are asked to deliver the Access Token in Redirect_URI, and if the AuthCode delivered is correct, the answer that will get back to IdP server, in this case Microsoft, will be an access token.

7.1. JWT (JSON Web Token)

In the case of Microsoft, the token arrives in a JWT format that is no more than a string URL, Encoded in BASE64 with a three parts structure: Header, Payload and Signature. In the following screenshot you can see a token recovered in JWT format (see Picture 18).

If we change the string in BASE64, we can see that the payload is full of information about the entire access session. This provides the app information, the list of permissions and account data that has been granted permissions to (see Picture 19).

Picture 18: Complete 3 part JWT
This token, in a raw manner, will have to be sent in each access request to the resources in the IdP account, whenever a call to the API Office365 or Windows Live is made. Requests must be made in the format below:

```
GET https://login.microsoftonline.com/common/oauth2/authorize

HTTP/1.1

Host: login.microsoftonline.com

Authorization: Bearer [Access_Token]

Using Office 365 API to access resources
```

The entire process is automated on our platform, so when the user grants access to the Scopes of the petition, the items which will appear on the list of tokens will be all those valid that can be used to access the account data (see Picture 20).
7.2. Actions on the Office 365 account via OAuth token

In the case of Office 365, the access is entirely to emails, so we can list all the messages in the inbox or in any other folder of the account, or, as we shall see in the next section, do the encryption of all messages and execute a hijacking mailbox with O365 RansomCloud module. To make it easier we have integrated a user interface that allows you to browse your mailbox and launch actions.

Among these options, you are also have the one of deleting mail messages, the one of sending messages from the account and activate or deactivate the RansomCloud process in this specific mailbox (see Picture 21).
These types of techniques have been used to cheat victims and steal money when a manipulated message introduced inside a legitimate conversation is being introduced, for example, get a message that the payment of a work item to be realized in another bank account - controlled by the cybercriminal - instead of the victim’s account (see Picture 22).

Picture 22: Sending emails using Office 365 API and the Access Token

Contacts from demo@e-paths.com

<table>
<thead>
<tr>
<th>DisplayName</th>
<th>EmailAddress</th>
<th>MobilePhone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Braulio Karakol</td>
<td><a href="mailto:braulio001@hotmail.com">braulio001@hotmail.com</a></td>
<td></td>
</tr>
</tbody>
</table>

Picture 23: Account contact list
These tasks (see Picture 23) can be made while the access to the Office 365 application is not revoked. To achieve this, the user should go to Configuration part of Office 365, to the Permissions Application section, and remove the access to his data from any unwanted app.

![Picture 24: List of all emails. Can be displayed complete and with attachments](image)

### 7.3. Office 365 email hijack

Once you have access to all the folders and messages in a mailbox from Office 365, the process to hijack mail messages is fairly straightforward. First you have to access a message that is then downloaded to the attacker’s server. After that, the original message is deleted while the attacker’s server encryption itself is performed. Finally, the encrypted message is uploaded to the server so to be up there. The scheme would be as simple as described in Picture 25.

![Picture 25: Mailbox hijack process in Office 365](image)
To make this process more effective, the attacker could use a system based on first hijack the oldest messages, which will be less possible to be accessed by the victim and, therefore, the work of mailbox hijack will have a greater opportunity time window to encrypt the greatest possible number of messages.

To obtain the emails in a specific folder, having the appropriate permissions on the SCOPE, the attacker only needs to use the API that provides Office 365 for it. This would be the necessary request to access e-mail messages.

```
POST /api/v2.0/me/messages HTTP/1.1
Host: https://outlook.office.com
Authorization: Bearer + AccessToken
X-AnchorMailBox: yourEmail@domain.com
```

**AccessToken:** This token allow access to email

The hijacking process is based on deleting the original message and replace it with an encrypted copy of the same. To make it more difficult to decipher by a reverse engineering algorithm, the simplest way is to use algorithms to generate random values to create a Random Key and a random initialization vector (Random IV) for each hijacked email account.

```
cipher.key = aes_key = <Random Key for Email Account>
cipher.iv = aes.iv = <Random IV for Email Account>
encrypted = cipher.update(messageBody)
```

With this process, the emails from the mailbox hijacked by RansomCloud will be encrypted with AES and for the victim will be useless documents that cannot be used unless decrypted. This is an example (see Picture 26) of a message hijacked by RansomCloud.
El texto necesario para descifrar los mensajes se almacena en una base de datos que puede ser accedida desde la plataforma en cualquier momento (vea la Figura 27). Es tan fácil tener los mensajes cifrados, como descifrarlos y el sistema puede hacerlo de forma autónoma solo seleccionando la acción "Desactivar RansomCloud".

Figura 26: Mensaje secuestrado por RansomCloud

The values needed to decrypt the messages are stored in a database which can be accessed from the platform at any time (see Picture 27). As easy as you can have the messages encrypted, you can decrypt them and the system can do it autonomously only by selecting Disable RansomCloud action.

Picture 27: CipherIV and CipherKey list of the hijackedmailbokes

While e-mail is encrypted on the RansomCloud server, the original messages must be removed from the original mailbox. To do this, the platform will delete the API using Office 365 offers for these tasks and for which permissions were requested to the Scopes list granted to the malicious app when the victim accepted. The request would be like this:

```

```
DELETE /api/v2.0/me/messages/{message_id} HTTP/1.1
Host: https://outlook.office.com
Authorization: Bearer + AccessToken
AccessToken: This token allow access to email
Message_id: Message in the mailbox

Once removed the original message, Ransom Cloud uploads the encrypted message to the cloud using AES, and again this is done by a function that provides the API directly. The request to upload a particular e-mail - in this case an encrypted message by the malicious application - is as follows:

POST /api/v2.0/me/MailFolders/inbox/messages HTTP/1.1
Host: https://outlook.office.com
Content-Type: application/json;odata.metadata=minimal
Authorization: Bearer + AccessToken
X-AnchorMailBox: yourEmail@domain.com

Body: Subject => "subject", Message => "encrypted message"... toRcpt, from, etc... (All params of original email)

AccessToken: This token allow access to email

Finally, to complete the process of hijacking the Office 365 Mailbox from a victim, would be enough to give one last message, this time in clear text unencrypted, in which the victim is informed of what happened and how it should realize the payment so to regain the control of the messages in the mailbox.

7.4. Decrypting the emails

The platform, through another app accepted by the user could perform the reverse process. That is, at any time, the platform can automatically reverse the process using a model based on access messages algorithm, decrypt, delete the encrypted message mailbox and deposit the old messages unencrypted on the server (see Picture 28). The process allows the platform to manage the entire process with just one click.
8. Attacking Windows Live Mail y OneDrive accounts

We can do exactly the same attack we have seen in the previous case but now against a Windows Live account. So we could use the same malicious app that we initially created or create a different one, and also could use the same email with social engineering or a different one, but we have to change the SCOPE_LIST email request permission so to adapt it to those available in Windows Live, which are different from those that exist in Office 365.

Once the victim decides to accept permissions to the app by clicking YES, our platform receives an Access Token that would allow invoke the Windows Live API to access all the granted resources (see Picture 29). As you can see, in the existing deployment at present Windows Live does not allow to access e-mail, although the Scopes are already defined for it. They are currently in a migration process that have not yet been concluded and which will soon make available the access to all mailboxes.
From the platform it is possible, however, to use other APIs, such as access contacts or file storage OneDrive service. As part of the demo we have implemented the access to OneDrive in a graphical way, so that it would be enough with just one click on the OneDrive button to access the structure documents contained (see Picture 30).

This way you can download all the files, browse folders (see Picture 31) to look for documents and, even, launch search queries of words within documents, which would help find information in a much more targeted way.
Similarly to messages from Office 365, with RansomCloud you can access files, delete them from their original location, encrypt them as it has been done with messages of the email and deposit seized in the folder of the victim along with a file to explain what the process has to be followed for decrypting files.

9. App review inside the Identity Providers

The first recommendation service the Microsoft Office 365, Gmail or Windows Live cloud users must follow is to review what apps they have connected to their identity and what permissions they have been granted to each of them (see Picture 32).
Keep in mind that the Sappo platform and RansomCloud module can continue to operate and capturing the new arriving emails while the obtained OAuth token is still valid or the access to it hasn’t yet been revoked. It is therefore important to check what apps are no accepted and eliminate suspicious.

A curious thing is that new apps with permissions granted to the Microsoft Office 365 accounts takes a while to appear and when they appear, do not have to allow the access to the detailed information of the app (see Picture 33). Most often, the usual way is to request the permits information from the app and not being able to access them with Office365 if the app is malicious as the one created here.

![App permissions](image1.png)

**Picture 33: App with permits in the Office 365 user profile**

As in the case of Microsoft Office 365, with Windows Live you can see the permissions granted to the apps (see Picture 34). In this case, it is also possible to see in detail all the permissions that each of the associated apps has with the account. You have go to the Applications and Services area and there you will find the app. And if we click on the details you can see the detailed list of all the permissions that have been granted to this app.

![List of permits](image2.png)

**Picture 34: The list of the permits granted to this app**
Depending on what the Identity Provider is the functions that could be performed with this type of malicious Apps change, but the concept will always be the same. Getting an Access Token for a number of Scopes and implement access.

10. Recommendations against Spear Apps attacks

In this article we have been shown how you can use malicious apps connected to an IdP for a malicious purpose. The concept proof of this has been intended to explain how easy it can be to migrate a scheme from the world of cybercrime as it is the ransomware to the cloud. To prevent these attacks you must strengthen security measures to be taken against the Spear Apps attacks and these are some of the recommendations that can be followed, in addition to strengthening email systems to the maximum with second-factor authentication, antispam engines and antimalware powerful or protections against identity spoofing using SPF filters.

10.1. New safety training for users

As we have been telling throughout the article, in the end the most important problem is that we have been training users to detect a very specific type of phishing attack in which credentials, through a Web page hosted on a hacked server or a false one, where we cannot correctly identify the domain of the site, but all these recommendations fail when we talk about a Spear App attack (see Picture 35).

### Recognizing phishing

Fake emails often include a link to a fake web page that looks very real. These fake pages are used by criminals to collect personal information. If you visit a page and aren't sure whether it's really a web page from Adobe, especially if the page requests personal information from you, click off the site and visit the Adobe homepage at [www.adobe.com](http://www.adobe.com) to begin there. Also, updates to Adobe software are made available from Adobe only on our website — we do not make any updates to our software available through third parties. Even if the web address contains the word "Adobe," it might not be an Adobe site.

*Picture 35: Adobe recommendations to recognize phishing attacks*
In these attacks, when the user has to click on YES it does it in the original Web site of Microsoft. He is inside the Microsoft.com domain, under a HTTPs connection, with an Extended Validation Digital Certificate - Green – which is correct and belongs to Microsoft, and besides this it never requests any user or password. Everything learned so far won’t be of much use.

Besides all this, the AntiPhishing filter implemented in browsers cannot detect anything because the URL where you are is the right one of Microsoft, therefore will not block it. You have to train users to detect such Spear Apps attacks, besides training them to detect the Spear Phishing ones.

10.2. The use of the SOC’s Cloud

One of the important recommendations that can be done is to practice active monitoring (see Picture 36) of abnormal situations, through an analysis of the logs that Cloud providers are offering.

![Picture 36: Cloud Security Monitoring based on LogTrust technology](image)

In Microsoft Office 365 it is possible to access the activity logs of all accounts of a corporate domain so to proceed with its activity analysis. A Cloud Intrusion Detection System (Cloud IDS) which analyzes these logs to detect abnormal patterns or unusual behavior could detect the onset of a new app associated with a mailbox or the beginning of the activity of an app, RansomCloud type, acting on one of the mailboxes.
Technologies such as LogTrust, https://www.logtrust.com, which allows the analyze of all logs and create usage rules or solutions such as Elastica, https://www.bluecoat.com, from BlueCoat (see Picture 37) can support this type of jobs to be performed by the safety equipment of a company.

10.3. Solutions: Public Cloud Encryption

Finally, another possible option to prevent data theft by malicious apps could be the the use of encryption solutions of public cloud data. In this case, a solution like Vaultive, http://vaultive.com/, which encrypts Office 365 would figure, that if an app gets permission to access emails through an Access Token, this app cannot access the decrypted data account if it is not done through the corporate gateway that performs encryption and decryption of data (see Picture 38).
This solution does not protect against an attack from Ransom Cloud, but against espionage messages or an account files of one of the IdPs mentioned in this article. If the malicious app got the Access Token, but tries to access from outside the company network - without going through the gateway that encrypts and decrypts the public cloud - then would get all the data of email messages encrypted, as shown in the picture 39.

![Email encryption Office 365 with Vaultive](image)

A malicious application could continue destroying the mails or continue to accessing the list of senders, but could never read the emails from the mailbox as all of them are encrypted.

**10.4. Application of the 2nd Factor Authorization solutions**

Currently the main IdPs apply identity protection solutions in a single entry point, such as the login process. In this section, the user must provide the system’s credentials verification of a second authentication factor, such as a telephone terminal in which Google Authenticator is used or OTP codes are received through a SMS message.

However, if an attacker is able to steal a Token OAuth, protections like Second Factor Authentication won’t protect the account. It would therefore be necessary to add Second Factor Authorization solutions for which the user could not only protect the login but the actions he wants enabled or not on each of the accounts. We could have a protection type **Latch** (2FAutorización solution, https://latch.elevenpaths.com) to enable the owner to manage identity if you want to turn on or off certain account features so to prevent this type of solutions.

**11. Final thoughts**

These techniques are not new, and in the world of cybercrime have been occasionally used in many attack scenarios. In the past there have been SPAM Phishing attacks for Tokens OAuth, but it is important that those responsible for the identities in the organizations to be fully aware of the dangers that these attacks are greater than typical Spear Phishing attacks - already very dangerous to companies.

Of course, the companies responsible for the IdPs - Microsoft and Google – should take actions and detect malicious activity by connected apps with the sole purpose of removing them as soon as possible from their systems and revoke their access.
About ElevenPaths

At ElevenPaths we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We’re always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

More information

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com