Handling BECs in an Office 365 environment

Presentation by Joey Rentenaar and Curtis Hanson
September 2019
Who is speaking today...

Curtis Hanson  
Threat Intelligence Specialist  
curtis.hanson@pwc.com

Joey Rentenaar  
Incident Response Specialist  
joey.rentenaar@pwc.com
Agenda

1. No love for BEC
2. What are the challenges?
3. A complete & reliable solution
4. Processing & analysing data
5. Resources
Not as sexy, but making money

$12.5B

- Industry tends to focus on APTs
- BEC attacks are simple
- But highly effective

Lazarus - Bangladesh Heist ($81M)
Carbanak/Cobalt ($1.2B)
BEC Attacks ($12.5B)
Maybe it’s OneDrive, Office 365, or just Microsoft as a whole. Whatever the case, fraudsters overwhelmingly impersonate some unit of this major brand when launching email-based attacks.

Agari
Email Fraud & Identity Deception Trends Q4 2018
What are the challenges?
Limited solutions for acquisition of the Office 365 Unified Audit Log (UAL) and it is a critical piece of evidence in a BEC investigation.
Log Acquisition

- Sheer amount of logs
- Export limits
- Be aware of license (E3 v. E5)
Log Analysis

- What is worth your time?
3

Complete & reliable solution
Solutions, but not complete or reliable

1. **Security Compliance Center**
   - Maximum of 50,000 records
   - Limit search/filter options
   - Unclear amount of events available

2. **Office 365 Management API**
   - Limited history of events
   - Most tools out there are based on the Management API

3. **Search-UnifiedAuditLog cmdlet**
   - Every session allows a maximum
     - 5,000 sorted records
     - 50,000 unsorted records
Office 365 Extractor

Script created by Joey Rentenaar & Konstiaan Stam @ PwC Incident Response Netherlands
Visit our Github github.com/PwC-IR/Office-365-Extractor for the full readme

Following actions are supported by this script:
1. Show available log sources and amount of logging
2. Extract all audit logging
3. Extract group audit logging
4. Extract specific audit logging (advanced mode)
5. ReadMe
6. Quit

Select an action:

Office 365 Extractor directly improves on the traditional acquisition methods by efficiently acquiring the complete Unified Audit Log.
Office 365 Extractor, a complete and reliable solution

Capture the complete UAL
Microsoft lists about 34 different record types but we identified 55:
- ExchangeAdmin
- ExchangeItem
- SharePointFileOperation

Improves on other methods
- Automatically creates a new session every time the 5,000 sorted record limit is reached.
- Regardless of the time interval chosen, the script adapts and guarantees all logs are extracted.

Gives acquisition options
1. All Logs
2. Group Audit Logs
   - Azure
   - Exchange
   - SharePoint
   - OneDrive
   - Skype
3. Specific Audit Logs
The Office 365 Extractor

1. Main Menu

2. Available log sources & amount
Extracting the UAL logging

1. Select action and date range

2. Auto adjusts time interval
4 Processing & analysing data
Processing the output file(s) is relatively easy...

- Output is a CSV
- Accomplished using any log management solution
- Be aware of license (E3 v. E5)
Analysing activity, this is where we begin

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Rules</td>
<td>Permission Changes</td>
<td>Suspicious Logins</td>
</tr>
<tr>
<td>• Active rules</td>
<td>• Grant access to another mailbox</td>
<td>• Brute force attacks</td>
</tr>
<tr>
<td>• Modified rules</td>
<td>• Escalation of privileges</td>
<td>• Disabling MFA</td>
</tr>
<tr>
<td>• New rules</td>
<td>• Folder Permission</td>
<td>• Logins at unexpected hours or locations</td>
</tr>
</tbody>
</table>
Forwarding Rules, a closer look

### 1. Detect active rules
- DeliverToMailboxAndForward
- ForwardingSMTPAddress...

### 2. Detect rules being modified
- Set-InboxRule
- Set-TransportRule...

### 3. Detect new rules
- New-InboxRule
- New-TransportRule...

#### Number of forwarding rules in this dataset

<table>
<thead>
<tr>
<th>CreateTime</th>
<th>Operation</th>
<th>MailboxID</th>
<th>RuleName</th>
<th>SourceAccount</th>
<th>SourceIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-01-05T11:15:29</td>
<td>New-InboxRule</td>
<td>F21874cb-3b50-4c64-8161-180e026d4a87</td>
<td>forwardingmails</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>99.195.28.1</td>
</tr>
<tr>
<td>2019-01-05T11:15:29</td>
<td>New-InboxRule</td>
<td>c019d3b3-8b91-456a-9581-2a6f086e5eef</td>
<td>delinoremails</td>
<td><a href="mailto:dave@domain.com">dave@domain.com</a></td>
<td>99.195.28.1</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>48f432df-3d30-4f51-9e69-666f706d616e</td>
<td>Forward_email</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>189.165.399.34</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>7b77199f-b765-4be8-9a08-090f8060603d</td>
<td>...</td>
<td><a href="mailto:dave@domain.com">dave@domain.com</a></td>
<td>189.165.399.34</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>a97a3dcb-994f-439c-9344-c5486040b30d</td>
<td>...</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>199.165.399.34</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>639174ce-4b77-447e-8565-65f5f6717c0d</td>
<td>...</td>
<td><a href="mailto:dave@domain.com">dave@domain.com</a></td>
<td>199.165.399.34</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>5264a2ce-48f7-4e7e-8388-9f213d026a8</td>
<td>...</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>46.144.22.5</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>5413b3b0-3e4d-4a2f-933a-569b6350a7e4</td>
<td>...</td>
<td><a href="mailto:dave@domain.com">dave@domain.com</a></td>
<td>46.144.22.5</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>6b4d6a11-6e6b-4d36-9f80-1f9a1e63a525</td>
<td>Forward_email</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>59.155.28.1</td>
</tr>
<tr>
<td>2019-01-05T11:25:47</td>
<td>Set-TransportRule</td>
<td>e0870554-9e6d-4a06-9377-39092a5f0235</td>
<td>DeleteMails</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>46.144.22.5</td>
</tr>
<tr>
<td>2019-01-05T11:25:41</td>
<td>Set-TransportRule</td>
<td>3e6b395d-9a37-40d9-990d-049b5d447f9b</td>
<td>ForwardAll</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>46.144.22.5</td>
</tr>
<tr>
<td>2019-01-05T11:25:41</td>
<td>Set-TransportRule</td>
<td>2c21b454-3632-4a08-9d30-699a096e7f3b</td>
<td>ForwardAll</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>46.144.22.5</td>
</tr>
<tr>
<td>2019-01-05T11:25:41</td>
<td>Set-TransportRule</td>
<td>61186e7e-4c8f-7e4b-8d86-7f7d9c237e</td>
<td>ForwardAll</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>46.144.22.5</td>
</tr>
<tr>
<td>2019-01-05T11:25:41</td>
<td>Set-TransportRule</td>
<td>23239c08-150d-4047-751c-404bc906827</td>
<td>...</td>
<td><a href="mailto:davidm@mail.com">davidm@mail.com</a></td>
<td>99.155.28.1</td>
</tr>
</tbody>
</table>
Permission Changes, a closer look

1. Detect permission changes
   - Add-MailboxPermission
   - Add-RecipientPermission...

2. Group and Role changes
   - Add member to role
   - Add member to group...

[Image of permission change detection tool]
Suspicious Logins, a closer look

1. Login activity
   - UserLoginFailed
   - UserLoggedIn...

2. MFA errors
   - UserStrongAuthClientAuthNRequired
   - UserStrongAuthClientAuthNRequiredInterrupt...

3. Brute forcing
   - IdsLocked
   - UserKey="Not Available"...
I need it!
No, I want it!
I need it!
# Resources

https://github.com/PwC-IR

- Office 365 Extractor
- Splunk Application
- Cheat Sheet

## Office 365 Extractor

### Cheat Sheet

<table>
<thead>
<tr>
<th>Forwarding Rules</th>
<th>Permission changes</th>
<th>Login Activity</th>
<th>Detect suspicious logins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect new rules</td>
<td>Detect mailbox permission changes</td>
<td>Detect brute forcing attacks</td>
<td>MailBoxLogin</td>
</tr>
<tr>
<td>New-InboxRule</td>
<td>Add-MailboxPermission</td>
<td>UserLocked</td>
<td>UserLoginFailed</td>
</tr>
<tr>
<td>New-TransportRule</td>
<td>Add-RecipientPermission</td>
<td>UserKey = &quot;Not Available&quot;</td>
<td></td>
</tr>
</tbody>
</table>

### Detect rules being modified
- Set-Mailbox
- Set-InboxRule
- Set-TransportRule

### Detect active rules
- DeliverToMailboxAndForward
- ForwardingSMTPAddress
- ForwardingAddress
- SentTo
- BlindCopyTo
- ForwardTo

### Detect folder permission changes
- Add-MailboxFolderPermission
- Set-MailboxFolderPermission

### Detect group or role changes
- Add member to role
- Add member to group

---

## Contact Us

- nl_incidentresponse@pwc.com
- joey.rentenaar@pwc.com
- curtis.hanson@pwc.com
Office 365 Extractor
Cheat Sheet

**Forwarding Rules**

*Detect new rules*
- New-InboxRule
- New-TransportRule

*Detect rules being modified*
- Set-Mailbox
- Set-InboxRule
- Set-TransportRule

*Detect active rules*
- DeliverToMailboxAndForward
- ForwardingSMTPAddress
- ForwardingAddress
- SentTo
- BlindCopyTo
- ForwardTo

**Permission changes**

*Detect mailbox permission changes*
- Add-MailboxPermission
- Add-RecipientPermission

*Detect folder permission changes*
- Add-MailboxFolderPermission
- Set-MailboxFolderPermission

*Detect group or role changes*
- Add member to role
- Add member to group

**Login Activity**

*Detect brute forcing attacks*
- IdsLocked
- UserKey=“Not Available”

*Detect MFA errors*
- UserStrongAuthClientAuthNRequired
- UserStrongAuthClientAuthNRequiredInterrupt

*Detect suspicious logins*
- MailboxLogin
- UserLoggedIn
- UserLoginFailed

Contact Us
nl_incidentresponse@pwc.com

GitHub
www.github.com/PwC-IR/Office-365-Extractor
Thank you