



Detecting Non-Owner Mailbox Access with Exchange Mailbox Auditing

❑ Made possible by: **LOGbinder EX**

© 2013 Monterey Technology Group Inc.



❑ Brought to you by:

LOGbinder EX

www.logbinder.com


Special Guest:
Ratish Nair | Microsoft MVP Exchange
MSExchangeGuru.com

Preview of Key Points

- ❑ What can you audit?
- ❑ How to configure Exchange mailbox auditing
- ❑ Where mailbox audit logs are stored
- ❑ How to get mailbox audit reports from Exchange
- ❑ The gap between mailbox auditing and your SIEM


What can you audit?


- ❑ Access to mailboxes by
 - Owner
 - Not recommended
 - Delegate
 - By normal users who've been given access to this mailbox
 - Most actions by administrators
 - Admin
 - Some actions when performed a certain way
 - In-Place eDiscovery search a mailbox
 - New-MailboxExportRequest to export a mailbox
 - Microsoft Exchange Server MAPI Editor


What can you audit?

Action	Description	Admin	Delegate	Owner
Copy	Item copied to another folder.	•	•	n/a
Create	Item created in the mailbox. (For example, a message is sent or received.) Folder creation isn't audited	•	•	•
FolderBind	A mailbox folder is accessed. Note: MS says "Entries for folder bind actions performed by delegates are consolidated. One log entry is generated for individual folder access within a time span of three hours. "	•	•	•
HardDelete	Item deleted permanently from the Recoverable Items folder	•	•	•
MessageBind	Item accessed in the reading pane or opened	•	n/a	n/a
Move	Item moved to another folder	•	•	•
MoveToDeletedItems	Item moved to the Deleted Items folder	•	•	•
SendAs	Message sent using Send As permissions	•	•	n/a
SendOnBehalf	Message sent using Send on Behalf permissions	•	•	n/a
SoftDelete	Item deleted from the Deleted Items folder	•	•	•
Update	Item's properties are updated	•	•	

© 2013 Monterey Technology Group Inc.


- 
How to configure
- ❑ **Auditing controlled on each mailbox individually**
 - Creates a management issue needing a solution
 - ❑ **Set-Mailbox**
 - Identity "John Smith"
 - AuditDelegate SendAs,SendOnBehalf,FolderBind
 - AuditEnabled \$true
 - AuditLogAgeLimit 90
 - ❑ **Prevent auditing of mailbox scanners, etc**
 - Set-MailboxAuditBypassAssociation
- © 2013 Monterey Technology Group Inc.



Recommended mailbox audit policy

- Owner**
 - None
- Delegate**
 - Delegate, Copy, Create, FolderBind, HardDelete, Move, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update
- Admin**
 - Delegate, Copy, Create, FolderBind, HardDelete, MessageBind, Move, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update

© 2013 Monterey Technology Group Inc.



Reporting

- GUI**
 - Non-owner mailbox audit reports from the web based "Exchange Control Panel"
- PowerShell**
 - Search-MailboxAuditLog cmdlet
 - Synchronous
 - But one mailbox at a time
 - New-MailboxAuditLogSearch
 - Multiple mailboxes
 - But asynchronous (Exchange emails you the log as an attachment)

© 2013 Monterey Technology Group Inc.

ULTIMATE
WINDOWS
SECURITY
IObinder EX

Storage, Purging, Archival

- ❑ **Where stored?**
 - Hidden folder in each mailbox
 - Not written to any external text file or Windows event log
 - Inaccessible through any normal log-collection means
 - Creates another issue needing a solution

© 2013 Monterey Technology Group Inc.

ULTIMATE
WINDOWS
SECURITY
IObinder EX

Storage, Purging, Archival

- ❑ **Purging**
 - Automatically purges entries based on -AuditLogAgeLimit specied on each mailbox
 - mailbox on In-Place Hold or litigation hold, audit logs are retained until the hold is removed
- ❑ **Archival**
 - No automated, enterprise method for archiving mailbox audit logs
 - Can manually export audit logs via PowerShell as an XML file
 - Search-MailboxAuditLog
 - One mailbox at a time
 - Need to get audit logs out of application where generated and in to your audit log repository

© 2013 Monterey Technology Group Inc.

ULTIMATE
WINDOWS
SECURITY
IObinder EX

Performance

- ❑ **Work done by servers with Mailbox DB server role**
 - Auditing itself
 - Searches
- ❑ **Searches might impact CPU**

© 2013 Monterey Technology Group Inc.

ULTIMATE
WINDOWS
SECURITY
IObinder EX

Bottom Line

- ❑ **Comprehensive, efficient auditing of non-owner access**
- ❑ **Good ability to search on short term activity within Exchange Control Panel**
- ❑ **Gaps**
 - Alerting
 - Long term archival
 - Vulnerable to tampering by same privileged users intended to control
 - Integration with SIEM/log management
 - Audit policy management as mailboxes are provisioned

© 2011 Monterey Technology Group Inc.

Bottom Line

LOGbinder EX

- ❑ Comprehensive, official Windows Security Center access
- ❑ Good ability to monitor on short term activity within Windows Control Panel
- ❑ **Gaps**
 - Alerting
 - Long term archival
 - Vulnerable to tampering by same privileged users intended to control
 - Integration with SIEM/log management
 - Audit policy management as mailboxes are provisioned

Solved

LOGbinder EX

© 2013 Monterey Technology Group Inc.

LOGbinder EX

LOGbinder EX

```

    graph TD
      subgraph Exchange_Logs [Exchange Logs]
        Mailbox_Audit_Logs[Mailbox Audit Logs]
        Admin_Audit_Log[Admin Audit Log]
      end
      Mailbox_Audit_Logs --> LOGbinder_EX[LOGbinder EX]
      Admin_Audit_Log --> LOGbinder_EX
      LOGbinder_EX --> SIEM[SIEM]
  
```

- ❑ **Gaps Solved**
 - Alerting
 - Long term archival
 - Vulnerable to tampering by same privileged users intended to control
 - Integration with SIEM/log management
 - Audit policy management as mailboxes are provisioned

© 2013 Monterey Technology Group Inc.



Additional resources

- ❑ **New Exchange Section at UWS**
 - www.ultimatewindowssecurity.com/exchange
 - Both admin and mailbox auditing explained
- ❑ **LOGbinder EX**
 - www.logbinder.com/products/LOGbinderEX
 - Download a copy and connect Exchange to your SIEM
 - Whitepaper: [Whitepaper: Comparing Exchange Server's 3 Audit Logs for Security and SIEM Integration](#)

© 2013 Monterey Technology Group Inc.



❑ **Brought to you by:**

LOGbinder EX
www.logbinder.com