Partnering With Vendors to Limit Compromised User Accounts

Indianapolis, IN

Richard Guajardo, University of Houston
Don Hamparian, OCLC
Peter Katz, Elsevier
Topics

- UH Experience
- Excessive Use vs. Systematic Downloading
- Triggers of Excessive Use
- Addressing the Issue
  - Proxy Logs
  - Vendor Communication
  - Broader Security Implications
Dear Librarian,

This is to notify you that IP address XXX.X.XXX.XXX associated with your organization, UNIV OF HOUSTON MAIN, has been blocked from accessing content on the ACS Publications website due to an excessive downloads violation. The unauthorized activity that resulted in this IP block occurred at Wednesday, June 29, 2016 4:36:28 AM UTC. To restore access to the IP address, please investigate the situation, and inform us of your findings.

Unfortunately, valid users from your institution might also be blocked if they use the same IP address, or if the account is set up using a proxy IP address.

Please investigate and contact ACS directly at ipblock@acs.org to request restoration. This IP address will remain blocked until ACS Publications is contacted and the situation is satisfactorily resolved.

We apologize for the inconvenience. Thank you again for your support of the ACS Publications program.

Sincerely,
The Sales Operations Support Team
Excessive Use vs. Systematic Downloading

Systematic downloading is excessive use, but not all cases of excessive use are systematic downloading.
Excessive Use is . . .

- Not always intentional
- Can be legitimate research
- Usually determined by the vendor
  - Each vendor establishes their own threshold for excessive use
  - Usually defined by number of downloads within a specific time frame
  - Vendors, understandably, do not share what their established threshold
Systematic Downloading

• Is intentional
• Is often scripted
• Can affect multiple platforms simultaneously
• Typically not our patrons
• Usually caused by compromised accounts
Excessive Use: Triggers

- Users sharing account information
- Phishing
- Compromised workstation
- On-campus Wi-Fi access
- Citation Tools (Endnote, Zotero, etc.)
Addressing the Issue

- **Proactively Check Server Status – Sessions Active over 24 hours**
  - Note Session ID
  - Terminate session
  - Search Logs to Determine if Account Could be Compromised

- **Reacting to Vendor Notification**
  - Request additional information (Date, Time, Log Activity)
  - Use information to Query Proxy Logs
  - Identifying the User

- **If Account is Compromised**
  - Block User in Proxy Server
  - Notify Library and Campus IT
  - Campus IT Contacts User
  - Unblock User After Notification from Campus IT
Proxy Log Files

-0600] "GET http://ezproxy.lib.uh.edu:80/connect?session=sAJ0z5Xov7DFpJDS&url=menu
HTTP/1.1" 302 0 "--"

-0600] "GET http://ezproxy.lib.uh.edu:80/menu HTTP/1.1" 200 141 "--"

-0600] "GET http://ezproxy.lib.uh.edu:80/public/uhl.css HTTP/1.1" 304 0
"http://ezproxy.lib.uh.edu/menu"

-0600] "GET http://ezproxy.lib.uh.edu:80/public/uhl-logo.gif HTTP/1.1" 304 0
"http://ezproxy.lib.uh.edu/public/uhl.css"

webofknowledge.com HTTP/1.1" 302 0
"http://www.91lib.com/e/action/ShowInfo.php?classid=219&id=902"
Vendor Communication

- Notification from Vendor
- Request for Additional Information from Vendor
- Follow-up with Vendor
- Restoration of Access
Internal Communicating: High Impact Incidents

- Communication with Subject Liaisons
- Checking in with Library Administration
- Key Library Staff
- Other users (Faculty, Staff Students)
Partnering with Campus IT

- Meeting with Campus IT Security Office
- Compromised faculty/staff accounts
- Campus IT being proactive
  - Following Know Hacker Sites
  - Keeping the Library in the Loop
Meeting with Campus IT Security

• Provide log files and timeline of event
• Campus will query other campus systems accessed during the same time frame by the same user account
• Admissions, Registration, Academic Grading System
• Time-sensitive response
Memo to Campus IT

We believe the Cougarnet accounts listed below may have been compromised.

UH Libraries contracts with various vendors to provide access to electronic articles and electronic books. In early July we were contacted by one of our vendors about excessive use or mass downloading of content, which is considered a breach of contract. Based on the information provided by the vendor and a review of our logs (attached), we were able to determine that four accounts were being used. A separate email will be sent containing the log files and username of the remaining two accounts.

The user accounts are:

xxxxxxxx
xxxxxxx

We have restricted access to library resources for this account, and would appreciate notification when it has been cleared so that we can restore access. If you need additional information, please let me know.
Memo to Campus IT

It looks as if the following student account may have been compromised. It was discovered while doing some follow up on an earlier incident reported by a vendor. It follows the same pattern of other accounts that were compromised—the presence of multiple IPs for a single session, most of which originate outside the country (see attached log files).

The user account is: xxxxxxxx

We have restricted access to library resources for this account, and would appreciate notification when it has been cleared so that we can restore access. If you need additional information, please let me know.
Memo to Campus IT

We believe the following student account may have been compromised:

xxxxxxx

Based on the frequency of these occurrences lately, we are monitoring our logs more closely so that we can catch unusual activity before it reaches the vendor. It seems that as soon as one user account is addressed, another account is discovered. We have restricted access to library resources for this account. Please let us know when this account has been cleared so that we can restore access.
Response From Campus IT

We spoke with this user and gave her phishing awareness training. Her password has been reset. You can restore her access to Library resources.

Thanks
Q&A:

Partnering With Vendors to Limit Compromised User Accounts

Richard Guajardo (guajardo@uh.edu), University of Houston
Don Hamparian (hamparid@oclc.org), OCLC
Peter Katz (p.katz@elsevier.com), Elsevier

Thank You for Attending.