ExLibris
Voyager

How to Prevent a Hack

ExLibris The bridge to knowledge

CONFIDENTIAL INFORMATION

The information herein is the property of Ex Libris Ltd. or its affiliates and any misuse or abuse will result in economic loss. DO NOT COPY UNLESS YOU HAVE BEEN GIVEN SPECIFIC WRITTEN AUTHORIZATION FROM EX LIBRIS LTD.

This document is provided for limited and restricted purposes in accordance with a binding contract with Ex Libris Ltd. or an affiliate. The information herein includes trade secrets and is confidential.

DISCLAIMER

The information in this document will be subject to periodic change and updating. Please confirm that you have the most current documentation. There are no warranties of any kind, express or implied, provided in this documentation, other than those expressly agreed upon in the applicable Ex Libris contract. This information is provided AS IS. Unless otherwise agreed, Ex Libris shall not be liable for any damages for use of this document, including, without limitation, consequential, punitive, indirect or direct damages.

Any references in this document to third-party material (including third-party Web sites) are provided for convenience only and do not in any manner serve as an endorsement of that third-party material or those Web sites. The third-party materials are not part of the materials for this Ex Libris product and Ex Libris has no liability for such materials.

TRADEMARKS

"Ex Libris," the Ex Libris bridge , Primo, Aleph, Alephino, Voyager, SFX, MetaLib, Verde, DigiTool, Preservation, URM, Voyager, ENCompass, Endeavor eZConnect, WebVoyage, Citation Server, LinkFinder and LinkFinder Plus, and other marks are trademarks or registered trademarks of Ex Libris Ltd. or its affiliates.

The absence of a name or logo in this list does not constitute a waiver of any and all intellectual property rights that Ex Libris Ltd. or its affiliates have established in any of its products, features, or service names or logos.

Trademarks of various third-party products, which may include the following, are referenced in this documentation. Ex Libris does not claim any rights in these trademarks. Use of these marks does not imply endorsement by Ex Libris of these third-party products, or endorsement by these third parties of Ex Libris products.

Oracle is a registered trademark of Oracle Corporation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

Microsoft, the Microsoft logo, MS, MS-DOS, Microsoft PowerPoint, Visual Basic, Visual C++, Win32,

Microsoft Windows, the Windows logo, Microsoft Notepad, Microsoft Windows Explorer, Microsoft Internet Explorer, and Windows NT are registered trademarks and ActiveX is a trademark of the Microsoft Corporation in the United States and/or other countries.

Unicode and the Unicode logo are registered trademarks of Unicode, Inc.

Google is a registered trademark of Google, Inc.

Document released: January 2010

Web address: http://www.exlibrisgroup.com

Table of Contents

1

How to Prevent a Hack

Site's Role

Each site is responsible for ensuring their server is on the most current security patch.

Solaris™ and AIX® sites need to install any available security patches, or request Customer Support do this for you on a one-time basis (new incident for each patch). Solaris™ and AIX® sites need to turn off any/all insecure processes that are running, or request Customer Support to do this. Solaris™ sites can use our Hardening Against Attack list. Windows® server sites should always verify with Customer Support before adding any patch.

Ex Libris' Role

For all known exploits that could jeopardize an Ex Libris server, we will send out a target email (see Target Email document) to all Primary and Secondary Technical contacts, as well as Primary Library contacts. We will also post notice of the exploit to SupportWeb. This will be an announcement stating the exploit, what vendor it is with, and what patch can be applied. We will also offer options to install this for the site, if the site requests it.

Ex Libris recommends that sites take security into consideration at all times. Even though hackers attempt to cause problems to the operating system (/m1 and /oracle are not their target), you still should try and prevent harm whenever possible.

The security patches, as well as the hardening list, will assist with this. Installing a firewall is one recommended form of security, while utilizing deny and allow for certain IPs, and closing off unneeded ports. Also, requiring encrypted connections to the server, like SSH and SCP (turning off telnet and ftp), is something to consider. Ex Libris offers setting up SSH through its Services division.

Making sure the server is physically secure is also important. Consider who has access to logging in, including if its location is secure. Ex Libris has offered a security class at the Annual Users Group Meeting in past years. Attending this class will make you very aware of threats and what to do about them. The first step to securing your server is to acknowledge it's at risk.

What To Do If You Are Hacked

If you or Ex Libris has identified (or agreed) that your Ex Libris server has been hacked, there are several things that must take place with your site and at Ex Libris.

Site's Role

1. Don't panic. Commonly a hacker has employed scripts to modify things in the root file system that causes problems, but are not vicious. /m1 and /oracle are not their target, and should be okay. Make sure your backups are always good with these!
2. Open an incident with Customer Support about your hacked server (https://support.exlibrisgroup.com).
3. Identify what was affected or exploited, and report it in your incident. (Customer Support can attempt to do this.)
4. Attempt to restore any harmed binaries in the operating system (Customer Support can do this), so that your server is functional.
5. Ensure successful back-ups are being done on the data volumes (/m1 and /oracle, and any additional crons, scripts, or third party software you may have installed).
6. Verify you have the current operating system cdrom for a reload.
7. Schedule a date for the re-install, either requesting that Customer Support be available to assist you or requesting Customer Support do this for you. (You need to be available to Customer Support on this day.) Customer Support will provide assistance or perform the re-install during regular business hours (9:00AM to 5:00PM Central Time), Monday-Thursday. This request should be made at least one (1) week in advance.
8. Obtain the re-install instructions from Customer Support.
9. Get the server re-installed.
10. Establish all scripts, crons, and third party software not installed by Ex Libris. (Sites are responsible for re-installing these themselves. If Ex Libris did not install it or agree to support it, this is the site's responsibility.)
11. Continue to apply all security patches available to your operating system.

Ex Libris' Role

1. We will work with the site to ensure the system is operational after the hack. This will allow the site time to prepare for the re-install and still be operational.
2. We will try to identify what was hacked, and if it was through a known exploit.
3. We will try to accommodate a requested re-install date. The re-install must be scheduled at least one (1) week in advance, during regular business hours, and on a Monday-Thursday.

We will re-install any and all needed files for Voyager® to run. Each site is responsible for re-installing any scripts, crons, or third-party software not installed by Ex Libris.

4 We will work with the site to do the re-install at no additional charge; however, if Ex Libris announced an exploit and your server was not patched to the latest security patch fixing that exploit, a $225.00 (USD)/hour fee may be applied.