Need to know details for Administrators

Active Directory was compromised, now what?

Author

Bob Bobel

Cayosoft | Need2Know

About the Author

As a Product Management Director, Bob is responsible for driving innovation and strategy for Security, Compliance and Identity products. Bobel combines his twenty+ years of IT management and enterprise software experience to provide strategic vision to high-performance teams through times of growth and change. Bobel previously held Product Management roles at enterprise software companies Netwrix Software and Quest Software Inc. (Acquired by Dell in 2012) While at Quest, Bobel's role included creating the first true Active Directory centric Identity Management platform – ActiveRoles Server®. A frequent traveler, Bob resides in Ohio with his wife and two children.

Email: bob@cayosoft.com
LinkedIn: linkedin.com/in/robertbobel
Twitter: @rbobel

Overview

Microsoft's Active Directory (AD) provides a secure and stable directory service on which many organizations depend to provide user authentication and authorization. Because AD represents the preverbal keys to the kingdom it typically receives the appropriate level of care and feeding required maintaining it. Despite proper upkeep, there is still a chance that an Advanced Persistent Threats (APT) may be successful and compromise your Active Directory. Because of the nature of APTs a wide range of attacks vectors may be tried that may or may not attempt to subjugate AD directly. The result is that a successful compromise may go undetected for some time until the attacker decides to exploit the compromise by stealing data or making critical systems unavailable.

Most administrators are now resigned to the fact that their network will be hacked. It's just a matter of time. It's no secret that there is a lot of activity around cyber security, and the most serious and damaging breach that could happen to any organization is a compromise of their Active Directory (AD) environment. AD is at the heart of many missile critical services, including desktop logins, file & print sharing, email & other communications and collaboration. And once the compromise happens, it can have far reaching effects. Plus, attackers are much more sophisticated, using various tactics to penetrate and then stay hidden within your environment.

Reducing the immediate threat – Domain Admins role

A quick way to reduce the threat to Active Directory is to reduce the number of privileged accounts that can make major changes to Active Directory. This is especially important for AD users who have the Domain Administrators privilege. Because of the Active Directory design, many organizations have dozens or many dozens of users who hold this role. There are several management solutions on the market today that will allow administrators to perform day-to-day tasks without requiring the Domain Administrator's role. Another critical way to reduce the threat to your production environment is to ensure your directory auditing and monitoring solutions are up to the task.

Why re-establishing AD after a critical compromise goes beyond normal recovery

Because a critical compromise may only be uncovered long after it was introduced the validity and security of backup data because changes made via. the compromise may be indistinguishable from day-to-day administrative changes. The sheer volume of changes made from the time of the compromise's introduction to the current state of the directory data make it virtually impossible to identify the changes intentional vs. non-intentional. The best option and certainly the fastest option is to remove the compromise and maintain your directory data is to migrate the data to a new sanitized directory on clean servers.

More on Advanced Persistent Threats

An Advanced Persistent Threat (APT) typically refers a conspiracy by a group of foreign government attempt or complete some a cyber-attack. What makes these threats particularly scary is after the group or foreign government perpetrating these attacks the compromise may not be exploited until such time as maximum damage can be achieved or when the highest value theft can be achieved.

Additional information:

For more information on Advanced Persistent Threats see:
http://en.wikipedia.org/wiki/Advanced_persistent_threat

*Windows Credential Editor - **If you don't think people can get past your complex AD password, check out http://www.ampliasecurity.com/research/wcefaq.html.***

Conclusion

It may be a simple matter of time before your directory gets hacked so you should develop a strategy to deal with the possibility. Because Active Directory is central to key infrastructure services, data and applications AD's mission critical nature must be fully understood. Remember this is a cyber-arms race, and the "bad guys" only have to win once to get in - you must win every day.

Cayo | Software™

To get additional practical whitepapers from Cayo | Software, please visit www.cayosoft.com.

WARRANTY

The information contained in this document is subject to change without notice. Cayo|Software makes no warranty of any kind with respect to this information.

Cayo | SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Cayo | Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

Cayo | and Cayo | Software are trademarks of Cayo | Software, LLC. in the United States of America and other countries. Other trademarks and registered trademarks used in this document are property of their respective owners.

Netwrix® is a registered trademark of Netwrix Software. Dell®, Quest Software® and ActiveRoles® are registered trademarks of Dell® Computer Corporation.

For additional information please see our web site at (www.cayosoft.com)

This page intentionally left blank