KPMG

Are your files sharing too much?

Cyber insights for the federal government

Today's reality:

- File shares are a ubiquitous part of organizations and are used by multiple employees within and across agencies.
- Many government agencies invest in protecting their network perimeter but haven't considered the security of their internal file shares. Security is often considered after the development and production of an information system.
- File share configurations and/or access may not be reviewed consistently, leaving data exposed to ex-employees.
- Government agencies cycle through multiple third-party contractors who are allowed to perform work on their company's computers which could lead to leakage of government data if out-processing procedures are not properly enforced by the responsible agency.

Determining whether your file shares are configured to protect or harm your agency.

Many organizations depend on file shares to allow efficient sharing between employees, to save files in a central repository for future use or to archive files on an agency server. File shares can be configured for entire organizations, specific functional groups or small teams of only a few people. Often established and accessed behind firewalls and VPNs, file shares are generally viewed as secure and a safe place to store data. Unfortunately, government agencies aren't the only ones who know this.

Increasingly, access to file shares and knowledge of content on shares is becoming a primary concern for organizations. Simultaneously, threat actors are also becoming wise to file shares and are including these as top-priority items when navigating a compromised network. Threat actors have discovered several vulnerabilities that may allow for unauthorized, and even undetected, access to file shares and the sensitive data within. By gaining access to a file share, threat actors can browse, steal or delete important data without much resistance.

The following sections examine two important considerations for government agencies as they review the protection of their file shares. Access controls focus on ensuring that the organization is protecting its data by managing access to it. Malicious attacks, on the other hand, focus on attacks or malware that may pose risk to an organization via its file shares.

Access controls

Access to file shares may be granted to employees in a myriad of ways, assigned by user or the department in which they work. User access may be assigned to a share based on employees' geography, specific role or for a unique project they are working on. In a large organization with hundreds of concurrent projects, ensuring that access controls are enabled or disabled in a timely manner can be a significant feat itself. However, without the correct access controls in place, organizations are leaving file shares open for years, allowing sensitive data to be leaked to unauthorized users.

An employee may assist with various programs throughout the course of a year. As he or she works with various departments, teams, and other agencies, file share permissions are granted to allow team members to work collaboratively. However, as employees move on to other projects, their access is not revoked. Soon, some team members may accumulate many more file shares than they continue to actively need. If a threat actor were to compromise one of these individual's machines, access to a large number of file shares could be easily gained as well.

Malicious attacks

Regardless of how well your access controls are maintained, threat actors or nefarious-minded individuals may still be able to exploit your file shares. One key advantage that file shares offer attackers is target surface: file shares, by nature, are typically made available to multiple people within an organization, if not the entire organization. File shares offer threat actors a way to quickly move laterally within an agency, stealing data and infecting other users simultaneously.

The following address some of the more recent file share-based malicious attacks.

File Sharing Redirection

An older but still effective attack, file share redirection leverages the fact that if Windows is pointed to a file:// link, it will automatically seek to initiate a server message block (SMB) request with the host. Using malicious web pages or advertisements, attackers could automatically redirect users to external file shares. Once the user has connected to the file share, a number of files could be opened, such as malicious Office documents or malware executables.

BadSamba

In January 2015, security researchers released a proof of concept titled "BadSamba," a play on words using Samba, the shared file and print service. BadSamba demonstrates how Windows Group Policy can be used to execute startup scripts from a file share. An attacker may gain control of a file share, placing malicious scripts to infect other hosts. By tweaking Windows group policies, an attacker may be able to force users to open the malicious script. By default, startup scripts are executed under the Local System account, which offers elevated privileges and access to the system.

Vendor-specific vulnerabilities

In addition to attacks that target file shares in general, an organization could also be at risk based on the manufacturer of its storage technology. In mid-2014, a botnet (a group of computers connected in a coordinated fashion for malicious purposes[1]) specifically compiled for use on network-attached storage devices made by Synology was discovered. The Linux-based operating system that powers Synology devices was found to have multiple vulnerabilities that would allow a threat actor to easily gain access to the operating system's files. While the botnet was being used to illegally generate cryptocurrency, the threat actors had full access to the files and could have caused significantly more harm to the organization(s).

Ransomware

Ransomware, not a new name to the world of malware, may also wreak havoc on file shares. When infecting a host, Ransomware routinely scans through each hard drive letter, looking for documents, pictures, videos, etc. to encrypt. If a user has an active connection to a file share, Ransomware may be able to successfully enumerate and encrypt files on that share. Ransomware thus could go from affecting one employee to hundreds very quickly.

1 http://www.techopedia.com/definition/384/botnet

How to protect your agency

- Frequently audit permissions and users with access to file shares; ensure that employees who have left the organization have all access to the environment removed. This should include third-party contractors and vendors as well. Furthermore, users with access to sensitive data should be audited to ensure their machines are not putting the data at risk.
- Be sure to patch file shares as patches become available. Often times, threat actors can quickly detect if you are behind on security patching and use this to their advantage.
- Enhance enterprise monitoring tools to identify and alert about suspicious file share traffic, such as traffic related to known exploits. File share activity typically happens on ports 139 and 445.
- Constantly examine your file shares for "old" data that you may not be required to store any longer - referred to as "defensible deletion."
- Increase logging capabilities on your file shares. Windows operating systems, for example, may require log tuning to capture important access events.
- File share activity typically happens within an organization; monitoring for file share traffic externally may detect unauthorized access or connections to suspicious file shares.
- Many endpoint security vendors will have signatures for well-known file share exploits; make sure you are monitoring your logs or alerts for suspicious activities.

Contact us

For further information, please visit us online at **kpmg.com/us/cyber**, call our 24x7 hotline at **855-444-0087** or contact:

Ron Plesco
Principal, Cyber Services – Cyber Investigations Lead
T: 717-260-4602
E: rplesco@kpmg.com

Tony Hubbard
Principal, Federal Advisory
T: 703-286-8320
E: thubbard@kpmg.com

Ken Adams
Director, Federal Advisory
T: 703-343-1221
E: kennethadams@kpmg.com

kpmg.com/socialmedia

This document is a revision of Are Your File Shares Sharing Too Much?. Authored by Edward Goings, Ronald Plesco, and David Nides of KPMG LLP.