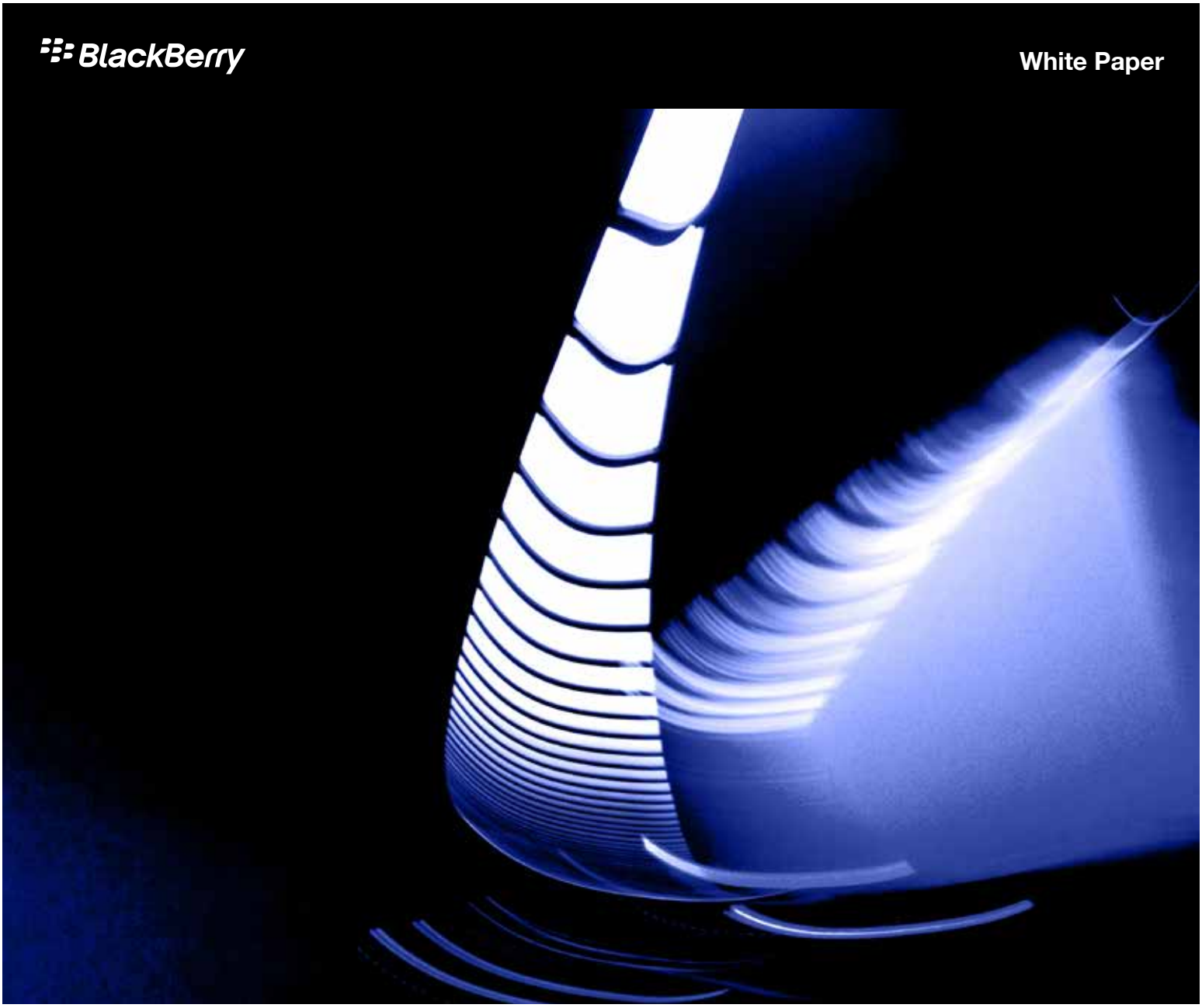
BlackBerry

White Paper



Raiders of the Lost File Shares

Defending Enterprise Data Against Destructive Malware

Introduction to Destructive Malware

With destructive malware ravaging the networks of governments, Aramco, Sands Corporation, and Sony Pictures, enterprise IT and security pros need to adjust their tactics. This paper takes a deeper look at these recent attacks and potential countermeasures to thwart them. Specifically, it covers:

- **What the recent wave of destructive malware does, and how it works**
- **Measures you can take now to mitigate the risk of such an attack**
- **Key considerations for protecting data on file shares, endpoints, and collaboration systems**

A Brief History of Destructive Malware

Destructive malware has a surprisingly long and varied history, dating back to at least the Morris worm in 1988. In the early days, not all malware authors set out to cause harm. For example, Robert Morris made a coding error that caused his worm to spiral out of control and take down a large portion of what was then the Internet.

The author of the AIDS Trojan, Dr. Joseph Popp, claimed that his encrypting ransomware was designed to raise money to fights AIDS. The malware hid all the directories and encrypted the file names on the C drive, demanding $189 be sent to a PO Box in Panama to fix the issue. He was arrested, but declared mentally unfit to stand trial.

However, recent incidents have changed the paradigm significantly. Attacks have targeted both workstations and file shares, and are intended to both exfiltrate data and destroy the systems on which the information was stored.

1988 The Morris worm mostly disables the internet (unintentionally)

1989 The first destructive ransomware emerges, highlighted by “AIDS” trojan

1995 “Concept” is the first virus to spread through Microsoft Word

2000 ILOVEYOU is a malicious worm that attacks tens of millions of Windows- based PCs

2004 Botnets embed themselves in large groups of web-enabled PCs — users are unaware that their machines are forwarding viruses and spam

2010 The Stuxnet worm embeds itself inside Iranian nuclear reactors; cyber warfare ensues

2012 The Shamoon attack at Aramco steals files, deletes them locally, and bricks hard drives on 30,000+ workstations

2012 The Wiper attack destroys computers in Iran

2013 Darkseoul attack takes down multiple South Korean TV stations and banks

2014 Wiper reemerges in a destructive attack against the Las Vegas Sands Corporation, linked to its CEO’s support of Israel

2014 #GoP attack against Sony Pictures, attributed to North Korea, attacks file shares and workstations

What Does the New Malware Look Like?

The newly destructive malware types used in the Shamoon, Wiper, and #GoP attacks are all quite similar. This paper will take a closer look at the latest of the breed, known as BKDR_WIPALL. This is not intended to be an exhaustive code-level analysis, many of which are publicly available from the major antivirus vendors.

The malware begins by appearing like most contemporary versions, with a "dropper" called diskpartmg16.exe. The target network is already thoroughly compromised, typically via spearphishing attacks against users with administrative credentials, which are then used to find credentials for other servers. The malware has an overlay with encrypted username and password combinations to log into a list of hostnames in a .dat file, most of which are believed to be file shares. Once logged in, the malware attempts to grant full access to everyone that will be accessing the system root, and drops another executable, called igfxtray.exe.

The next steps are where BKDR_WIPALL shows its true colors as destructive malware. The second executable does a variety of nasty things:

- Deletes the contents of all mapped (network) and fixed drives
- Deletes all the user's local files
- Stops the Microsoft Exchange Information Store service
- Creates a driver file, installs it as a USB host controller, and wipes the master boot record, rendering the disk unusable

Finally, the malware drops some ugly skeleton wallpaper, shown below:

Once the initial steps in the process were completed, the BKDR_ WIPALL malware delivered a warning message via this wallpaper.

The Three Major Challenges of File Share Attacks (And What to Do About Them)

Problem 1: The Files are Stolen

As in many other advanced attacks, it has been the massive volume of stolen and leaked data that has grabbed the headlines.

There are few ways to reliably protect enterprise data against an attack that leverages compromised user credentials, but embedding protection in files — also known as digital rights management (DRM) or information rights management (IRM) — can be effective.

Rights management controls travel with files, and can be used to revoke access from compromised user credentials even after the files have been exfiltrated. In addition, rights managed files provide an audit trail so IT teams can better understand the extent of data that has been accessed by malicious.

For existing repositories, like the file shares targeted by this kind of malware, rights management controls can be applied to content in place on the file shares, or, as files leave the system. Integration with a content-aware data loss prevention (DLP) system can help you determine which files in which repositories are most in need of this level of protection.

Problem 2: The Endpoint Gets Destroyed

This type of attack also highlights a less glamorous challenge: ensuring that users' files are backed up in case of compromise.

Modern solutions for file synchronization and backup can treat the endpoint as basically untrusted, establishing an encrypted container on any device, which can be restored on a new device in case of a destructive malware attack.

Restoring applications is often easier, but enterprises need to be conscious of the immense business disruption caused by the files that are destroyed in this type of attack. When PCs are destroyed, users fall back on personal smartphones and tablets, personal email accounts, and even move processes to paper. The disruption to productivity is difficult to contemplate, but must be factored into enterprise business continuity and disaster recovery planning. This is critical for systems most frequently targeted by malware (such as Windows® and Android™).

Modern enterprise file synchronization and sharing (EFSS) and backup solutions, whether run as cloud solutions or as on-premises virtual appliances, tend to be far more hardened against attack than endpoints are.

Problem 3: The File Shares Get Destroyed

For many IT professionals, perhaps the most worrisome action taken by destructive malware is the total deletion of file shares via mapped drives and local disk formatting.

Many enterprises have been dependent on CIFS (Common Internet File System) shares or similar file shares for decades, and migrating away from them to other forms of file storage proves to be challenging in practice.

For sensitive file shares, IT departments should consider restricting unsecured direct write access to file shares. Many tools can serve as proxies to provide access to the file shares (often via a slightly different interface) with greater resistance to advanced malware.

In fact, many EFSS services are evolving to serve this purpose, and can even apply controls like rights management to content in place on file shares.

An Innovative Solution

Enterprises need tools to be able to manage, monitor and secure which services and repositories employees use to store and share their files. In light of the destructive capabilities of new forms of malware, solving this challenge has never been more critical. Enterprises need to look for solutions that can protect and restore their files even when their endpoints have been compromised, and likewise need to invest in protecting the file repositories they depend on.

Key technologies like rights management, proxy-style file share connectors, and secure EFSS can help organizations to substantially mitigate the risk of information loss as well as business disruption posed by new forms of malware.

Security That Stays With Your Files

With BlackBerry® Workspaces, users can safely access, share, sync, and collaborate on even the most sensitive files, using any device — desktop (Windows, Mac®) or mobile (iOS®, Android, BlackBerry® 10).

Work on files in the way that's most convenient at any given time. Workspaces provides a suite of integrated collaboration tools that allow you to view, search for, annotate, edit and share Office, PDF and image files using your mobile device — or do it all using the native apps on your desktop. File locking allows teams to prevent duplication of effort by temporally limiting access to a document while it's being edited.

BlackBerry Workspaces embeds digital rights management (DRM) protection in your files so your content stays secure everywhere it goes, and you can control users' ability to view, edit, copy, print, download or forward files, even after those files are downloaded or shared with third parties.

Workspaces is the only EFSS solution that provides file-level security combined with a user experience that's as easy and intuitive as any consumer solution. It's also the only solution that encrypts files not just at rest or in transit, but while they're in use.

Deploy Workspaces in the way that best suits your IT environment: cloud, on-premise or a hybrid. Comprehensive tracking of all document activities provides critical information for audit, compliance and business intelligence.

And to ensure that secure data exchange doesn't make more work for IT, Workspaces provides default, self-provisioning authentication solutions and a unique feature known as mixed-mode authentication, which allows different types of users to authenticate in different ways.

Workspaces was positioned #1 for "High Security" in Gartner's 2015 Critical Capabilities Report on EFSS.

Workspaces also placed second in the "Mobile Workforce" and "Extranet" categories.

Mobilize Your Business Simply and Securely

With the BlackBerry Enterprise Mobility Suite, enterprises can say "yes" to their users' and business leaders' demands for anytime, anywhere productivity through secure mobile apps.

The BlackBerry Enterprise Mobility Suite provides consistent multi-platform endpoint and app management policies and controls across iOS, Android, Android™ for Work, Samsung Knox™, Windows®10, macOS and BlackBerry operating systems, no matter the device ownership model or the user groups being mobilized.

The BlackBerry Enterprise Mobility Suite provides a turnkey solution for rolling out collaboration apps, line of business apps, custom apps and/or leveraging your existing Microsoft® apps, all while protecting your business and your employees' privacy. BlackBerry-secured apps have consistent containerization and security policies across operating systems and devices to keep work and personal content separate.

When an employee leaves the organization, only the BlackBerry-secured apps and business data are wiped from the device. All personal data remains personal and the rest of the device is left intact. Enterprises, including organizations with the highest security requirements, that are concerned about the security of their content as it moves beyond their firewall and is shared with third-parties and external partners, trust BlackBerry Workspaces, the leading secure Enterprise File Sync and Share (EFSS) solution, to increase the security and trackability of their business data.

Workspaces is available on its own, or bundled with the BlackBerry Enterprise Mobility Suite — Content Edition. For details visit www.blackberry.com/suite

Security That Stays With Your Files

BlackBerry delivers proven security, trusted by thousands of companies around the world, to protect your most important assets — your privacy and your business data.

Why choose BlackBerry for secure Enterprise File Synchronization and Sharing (EFSS)?

- Leading the industry with over 70 certifications to meet your security and compliance needs*
- BlackBerry® 10 approved by NATO for classified communications up to "Restricted" level (BES®10 and BlackBerry 10 smartphones were the first to receive this approval)*
- 16 of the G20 governments trust BlackBerry*
- The top 10 largest law firms trust BlackBerry*
- 5 out of 5 of the largest oil and gas businesses rely on BlackBerry*

About Workspaces

BlackBerry Workspaces

BlackBerry Workspaces makes your content secure wherever it travels. With Workspaces, all stakeholders can safely access, share and collaborate on even the most sensitive files, using any device — desktop (Windows®, Mac®) or mobile (iOS, Android, BlackBerry). By combining a user experience that's as easy and intuitive as any consumer solution with a unique data-centric architecture (which embeds protection right in your files), BlackBerry Workspaces is designed to meet the needs of your organization, IT team, and users. To learn more, visit www.blackberry.com/workspaces.

* Current as of 10/14/2015