Targeted Attacks

8-Step Plan To Safeguard Your Organization

Plus 8 Case Studies

IMPERVA®

Share this eBook

Targeted Attacks

"U.S. companies lose about **$250 billion** per year through intellectual property theft, with another **$114 billion** lost due to cyber crime, a number that rises to **$338 billion** when the costs of down time due to crime are taken into account.[1]"

[1]Josh Rogin, NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history", http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history (Jul 2012).

Contents

Introduction

Everyone Is a Target

Cyber security experts suggest that it's likely your organization's data has already been breached. So rather than asking "what if?", it's time to ask "now what?". Research shows that 66% of breaches remains undetected for months or longer[2] and that enterprises typically become aware of a data breach only once external parties, such as law enforcement officials or outside service providers, alert them to it. Hackers are looking to steal confidential company information for economic and political gain. This is not exclusive to any one particular industry or corporate demographic—everyone is a target.

The target of choice for cyber attackers is often those individuals inside an organization, with access to the resources the attackers want. Over 75% of network intrusions take place because weak or stolen user credentials have been exploited[3]. Hackers use spear phishing and malware to target your trusted insiders, and then leverage stolen credentials to navigate the company network and gain access to the data center. Your data center is the ultimate goal for these attacks because it contains a concentration of sensitive data, as well as critical business applications. In the end, your organization is only as strong as its weakest link.

Dissecting Eight Targeted Attacks by Industry

This eBook features case studies of eight organizations across highly targeted industries. It explores how attackers infiltrated each organization's data center and details the resulting business implications. Each organization had two things in common: they possessed unique, sensitive data which was fundamental to their long-term business strategy; and they were breached by means of advanced targeted attacks. These events were devastating to the organizations' reputations and competitiveness. In some cases, the data breach cost billions of dollars, disrupted strategic initiatives, and destroyed years spent on research and development.

[2]Verizon, Data Breach Investigations Report 2013, http://www.verizonenterprise.com/DBIR/2013 (May 2013).
[3]Verizon, Data Breach Investigations Report 2013, http://www.verizonenterprise.com/DBIR/2013 (May 2013).

CASE STUDY

Retail

> **"The theft of deal-related information has become widespread even as it remains mostly secret, so much so that… if these attacks are left unchecked, they could have a devastating impact on the future earning potential of many major companies and the economic well-being of countries."**[4]

Perhaps one of the most significant, unacknowledged breaches in recent history was the theft of sensitive files related to a global beverage company's attempted purchase of a Chinese juice company in March of 2009. If successful, the $2.4 billion acquisition would have been the largest foreign acquisition of a Chinese company. The acquisition would have allowed the beverage company to respond to the slowing Chinese demand for soft drinks and expand its offering to support the fast-growing juice market.

Hackers first penetrated the beverage company's network by directly targeting the deputy president in charge of facilitating the deal. On February 16, 2009 the DP received an illegitimate email containing a link to a malware-infected file; the message appeared to have been sent from a company legal executive, with the subject line: "Save power is save money! (from CEO)". Upon clicking the link, a keystroke logger was installed on the machine to capture the DP's credentials, and the attackers ultimately gained full control of his machine via remote access. From here, the intruders were able to steal the account information of privileged users, enabling almost full access to the beverage company's network. Within two days, multiple malicious tools had been installed, which facilitated the theft of sensitive information.

Following the intrusion of the DP's device, hackers went on to compromise the devices of other employees. A public affairs executive in the Asia Pacific region, received a phishing email disguised as a media advisory originating from the World Bank office in Beijing, which contained malware exploiting an Adobe Reader vulnerability. The original compromised machine served as home base for the attackers, storing all sensitive data on the juice company deal taken from other devices. The malware used in this breach confined the intruders' extensive activity to a small footprint.

During approximately a one-month period, hackers rummaged through the beverage company's proprietary files, collecting sensitive deal information known to have originated from the DP. The Chinese Ministry of Commerce nullified the acquisition shorty following the breach, citing antitrust violations as the cause. The beverage company became aware of the breach after being notified by the FBI.

When news of the juice company acquisition was announced in September 2008, industry analysts were optimistic about the results the beverage company would gain. With Chinese consumers becoming more health conscious, the market for fruit juices was expanding, making it an opportune time to acquire the number one juice producer in China. The CEO of the beverage company stated that the deal would: "provide a unique opportunity to strengthen our business in China, especially since the juice market is so dynamic and fast growing..." The annulment of the deal, which presumably was tied to the attack, caused the beverage company to lose a unique opportunity, in a highly desirable market.

Organization: Beverage manufacturer

Stolen: Data for a planned acquisition deal

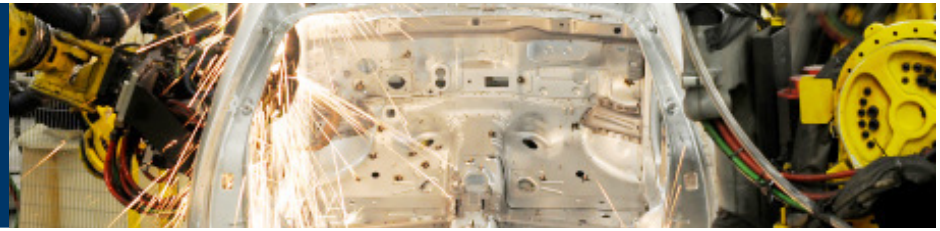
Target: Company executives involved in the acquisition

Presumed Impact: Lost critical window of opportunity to expand into a highly desirable market

[4]Ben Elgin, Bloomberg.com, (Nov 2012).

CASE STUDY

High-Tech Manufacturing



> **"While it may be easy to get caught up in toeing the compliance line and focusing solely on the protection of personally identifiable information (PII), at the end of the day security professionals need to remember that protecting business-critical intellectual property (IP) should be their No. 1 concern."**[5]

Given the priority that government bodies worldwide are placing on clean-tech, there are lucrative incentives to be among the first companies to market environmentally sustainable technologies. Industrial espionage is prevalent in these sectors, and in April 2012, it is suspected that an automobile manufacturer became a target for this reason.

The company issued a public statement on April 20, 2012, indicating that attackers succeeded in installing malware on the corporate information systems (IS) network at its Americas headquarters. The infiltration allowed them to exfiltrate employee user IDs and encrypted passwords. To investigate the incident, automobile manufacturer worked with their internal security teams and additionally hired an outside consultant. The teams determined that employee log-in information was sent to an outside server. It's likely that the stolen credentials enabled attackers to gain privileged access to the company network and forage through sensitive company files. Though no personally identifiable information (PII) is presumed to have been taken, the company believes that the hackers were after intellectual property relating to the company's proprietary electric vehicle (EV) drivetrain system.

According to the company's CEO, the future of the auto industry lies with the fuel-efficient vehicles they're developing. The company is passionate about zero-emission electric vehicles and believes that the market is headed in this direction. As part of their long term strategic vision, the company is dedicated to developing technology to make the offering affordable to the general consumer. With the race to develop the most fuel and cost efficient clean tech vehicles, the suspected cyber espionage activity could have devastating effects on their competitiveness and go-to-market strategy on an international level.

Organization: Automobile manufacturer

Stolen: Industrial designs

Target: Unknown

Presumed Impact:

- Designs stolen
- R&D lead eroded
- Experienced additional challenges competing internationally in the electric vehicle market

[5]Ericka Chickowski, Darkreading.com, (Apr 2012).

CASE STUDY

Energy

"Advanced attack groups are increasingly taking advantage of outsourcing relationships to gain access to the organizations they are targeting."[6]

In 2012, the energy sector experienced a vast majority of the recorded advanced targeted attacks. In roughly the same timeframe, foreign energy companies invested more than $17 billion in oil and gas deals in North America, providing a hint to what might be motivating some of these attacks.

One of the largest natural gas producers in the U.S. became a victim to cyber attackers who compromised one of their vendors to gain intelligence on the natural gas company. According to researchers, this approach is one of the fastest growing trends in cyber espionage.

When the data breach occurred, the natural gas company was working with a third-party investment banking firm to facilitate the sale of various stakes of land in the Ohio-based Utica shale deposit. Computer logs show that on September 22, 2011, hackers entered the system of an investment banker who managed the firm's energy deals. Attackers spent approximately three hours sifting through sensitive data on the investment banker's machine. The files they stole contained information very specific to natural gas leases for sale in the Utica shale deposit, as well as information on the foreign parties expressing interest in the land.

The natural gas company is the largest leaseholder in the U.S., holding drilling rights for over 15 million acres. Its leasing strategy is fundamental to its business model in which it derives profits by selling leases for land containing natural resources, versus producing the product itself. In a recent Securities and Exchange Commission (SEC) filing, the natural gas company identified advanced targeted attacks as a risk factor, stating: "We have been the subject of cyber attacks on our internal systems and through those of third parties…" While major foreign players are looking to pursue shale-produced gas; the breach of sensitive saleable lease information directly affects [our] business strategy, and its ability to sell land at a competitive price.

Organization: Natural gas producer

Stolen: Lease negotiation information

Target: Third-party investment banker

Presumed Impact:

- Lost ability to lease land or sell land leases at the most competitive prices

[6]Mandiant, Mandiant.com (Mar 2013).

CASE STUDY

Metals and Mining

"Digital intruders are increasingly targeting information about high-stakes business deals—from mergers and acquisitions to joint ventures to long-term supply agreements—and companies routinely conceal these breaches from the public."[7]

The competition for natural resources that is taking place among sovereign nations is brought to light by a targeted attack which may have jeopardized a multinational mining and petroleum company's $40 billion planned acquisition of a major Canadian potash producer. In September 2010, hackers penetrated several external parties involved in the deal, including seven Canadian law firms, the Canadian Finance Ministry, and the Canadian Treasury Board.

The investigation began after one of the affected law firms reported issues with network interruptions coupled with other indications of intrusion. The firm hired to research the incidents stated that most of the concurrent attacks were performed as a decoy, an attempt to conceal what the hackers were ultimately after: data pertaining to the acquisition of the potash producer. Their analysis confirms that phishing emails were used to distribute malware engineered explicitly to steal sensitive documents.

The attacks on the Canadian ministries leveraged similar tactics in which spoofed emails directed employees to a spyware-infected webpage that exploited vulnerabilities specific to internet browsers on the organizations' machines. The Canadian government subsequently issued a report stating that it was certain the breaches of the Finance Ministry and Treasury Board led to data theft.

At the time the attacks took place, multiple governments were on the search for new agrochemical suppliers. It's reported that a major state-owned Chinese chemical company began making competitive bids to disrupt the mining and petroleum company's deal and hired two major financial institutions to assist.

The targeted law firms and federal ministries held detailed information on the nature of the mining and petroleum company's negotiation, which likely included weak points of the deal. Any exposure to this sensitive data provided the attackers with significant leverage for deal-related discussions and put the company at a great disadvantage. Competitors were likely worried that a successful acquisition by the mining and petroleum company would have given them too much control over global potash resources. As a result of the breach, the company lost a major opportunity to gain access to a profitable natural resource which is in high demand worldwide.

Organization: Mining and petroleum producer

Stolen: Acquisition data

Target: Unknown

Presumed Impact:

- Lost opportunity to expand into a highly desirable market

[7]Ben Elgin, Bloomberg.com, (Nov 2012).

CASE STUDY

Aerospace and Defense

"The company is not only safeguarding a wealth of U.S. government military information from external sources, it's also protecting its own valuable projects—the F-16, F-22 and F-35 fighter aircraft; the Aegis naval combat system; and the THAAD missile defense."[8]

In 2011, the largest defense contractor for the U.S. government, responsible for sophisticated military equipment and the country's most sensitive defense projects suffered a breach. The advanced targeted attack that penetrated the organization had two stages: attackers gained entry to the network using information originally stolen in a separate attack on high-profile security vendor RSA, who supplied the company's two-factor security tokens.

RSA's SecurID tokens serve as a second layer of authentication between the company's corporate network and employees accessing the network via the corporate VPN. RSA describes in a detailed blog post that over a period of two days, two groups of employees received an email titled "2011 Recruitment Plan" containing an Excel spreadsheet attachment. Once opened, the document exploited an Adobe Flash vulnerability and injected malware containing a remote administration tool designed to be difficult to detect. RSA was able to remediate the attack relatively quickly, though it is believed that the hackers successfully stole critical intellectual property: a list of seed numbers that were key to producing SecurID-generated pseudorandom codes. A hacker with the seed numbers and the SecurID code generation algorithm (which was already somewhat public knowledge) would be able to circumvent the security offered by the SecurID tokens.

Security professionals believe that hackers installed key logger malware on at least one company computer used to access the company's VPN, then recorded username information, and used the stolen SecurID seeds to crack the second-layer security code. With this information, hackers gained entry to servers at the company's central data center.

An attack of this nature presents several implications. First, U.S. national security is at risk if confidential data regarding sophisticated defense equipment and military information is leaked externally. From the company's perspective, a main driver of their success is a result of extensive contracts with the U.S. government. To maintain this stature, the security of the data they house is crucial. Furthermore, the organization's ability to compete with other vendors is easily jeopardized upon a breach of proprietary trade secrets. This highly advanced attack against two major corporations showcases the persistence of cyber attacks in obtaining sensitive intellectual property.

Organization: Aerospace and defense contractor

Stolen: Trade secrets

Target: Company employee(s)

Presumed Impact:

- Breach of sensitive information impacted national security
- Stolen designs affected ability to compete

[8] Jason Mick, Dailytech.com, (May 2011).

CASE STUDY

Government

"The bill for the data breach now exceeds $14 million."[9]

Of all the security issues that organizations face, the theft of personally identifiable information, or PII, is one of the most crucial. Stolen PII often leads to identity theft, where the victims' information can be used to take out loans, open credit cards, or perform other forms of fraud. From August to October 2012, a U.S. State Government experienced a data breach in which 3.8 million tax returns containing social security numbers, and 3.3 million bank account numbers were stolen. The origin? An insider, compromised by malware.

In August 2012, a phishing email was sent to several employees at the U.S. State Government. At least one of the recipients clicked on a malicious link in the body of the message which installed malware and compromised the machine. User credentials were stolen and with these rights, the attacker gained access to the organization's internal systems and databases. Subsequently, other strains of malware were installed which enabled the hacker to steal account information across six department servers. Over a period of about ten days, other servers were accessed and reconnaissance activities were performed. After the attackers scoured through sensitive information, database backup files were discovered and the entire 75 GB database backup was stolen.

The advanced targeted attack in this example compromised 44 systems and involved 33 unique types of malware. The consequences of this data breach were extremely costly and jeopardized the identity of 80% of the individuals in the state. It was reported that over $14 million had been spent to mitigate the damage of the attack. Additionally, after it was determined that the agency could have employed greater diligence to protect its data, the U.S. State Government Director resigned.

Organization: U.S. State Government

Stolen: Personally identifiable information

Target: Company employee(s)

Presumed Impact:

- Jeopardized reputation
- Exposed substantial personal information
- Financial loss – spent over $14 million to mitigate attack

[9]Matthew J. Schwartz, Informationweek.com, (Nov 2012).

CASE STUDY

Payment Processing

> **"Whether it's a malicious insider, or an external attacker looking to exploit privileged accounts to gain access to sensitive information, these privileged access points accounts have emerged as the priority target for cyber-assaults. Attackers have used the privileged pathway to penetrate some of the most spectacular breaches over the past couple of years."**[10]

Financial institutions are one of the most targeted industries for data breaches and, as a result, constantly invest in security measures. In some cases, rather than directly attack financial organizations, attackers seeking personally identifiable information have exploited third-party payment processing systems. One of the most noted examples is where the credit card details of 1.5 million cards were exported from a global leader in payment processing services' network. The associated costs for remediation of the breach have reached $93.9 million.

It has been reported that the network was under attacker control for a period of 13 months, allowing the attackers to collect data on 24 million transactions. Security professionals believe that the breach occurred after an Oracle database administrator (DBA) was targeted and that the DBA's account, which was insufficiently protected, was taken over. In a KrebsonSecurity.com post, the well-respected Security blogger revealed a document, anonymously given to him after the breach, that the compromised administrator had created. Titled "Disaster Recovery Plan…Loss of the Atlanta Data Center", the document contained detailed information about the payment processing company's internal databases, and was likely used to navigate the infiltrated data center.

This breach was devastating to the company's brand, and will likely affect the future of the company. In violation of the Payment Card Industry Data Security Standard (PCI-DSS), a large percentage of the $93 million dollar price tag attached to the attack was appropriated to regain PCI compliance and meet the necessary data security requirements. Additionally, Visa and MasterCard removed the company from its list of compliant processors for over an eight month period, which poses an additional threat to business. The company stated, "Our failure or a delay in returning to the list could have a material adverse effect on our business, financial condition, results of operations and cash flows."

Organization: Payment processing services

Stolen: Personally identifiable information

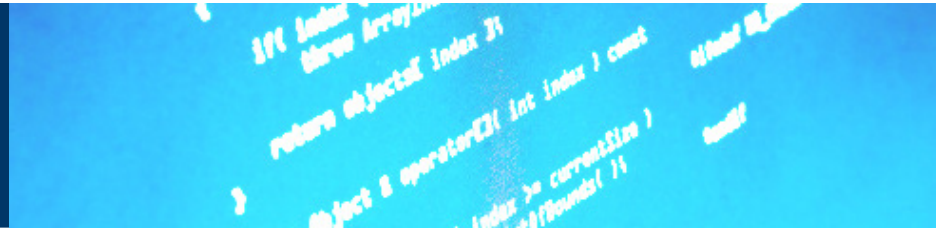
Target: Database Administrator

Presumed Impact:
- Jeopardized reputation
- Lost crucial contracts with Visa and MasterCard
- Violated PCI regulation
- Financial loss - $93 million spent to mitigate attack

[10]Cyber-Ark, Cyber-ark.com, (June 2012).

CASE STUDY

Computer Software



> **"…of the 33 companies that were hacked, the attacks were well targeted and 'unusually sophisticated' and aimed at grabbing source code from several hi-tech companies based in Silicon Valley as well as financial institutions and defense contractors."**[11]

For the major computer software companies of the world, their underlying source code is the key to their competitive advantage. Given the highly competitive nature of the industry, all computer software corporations are a target of cyber espionage and intellectual property theft.

In 2010, a small group of employees, who worked extensively with source code management systems for a multinational corporation specializing in Internet-related services and products, were targeted by an advanced targeted attack. The employees received an email containing a PDF document infected with malicious code. The malware exploited a vulnerability in the Adobe Reader application. Once the company learned that malicious software was present in its systems, they uncovered that the code was connected to an outside server put in place to store stolen sensitive information. Researchers confirmed that intellectual property was stolen from the company, and that source code was the target. This attack was part of a highly coordinated effort labeled "Operation Aurora" in which an unprecedented combination of strategies was used to penetrate the networks of at least 33 other companies.

An attack of this nature poses many risks. First, it provides hackers with an opportunity to inflict source code changes, potentially allowing for further reconnaissance on machines running the company's software products. Furthermore, the loss of intellectual property that sustains core business operations in turn, poses serious threats to a company's overall competitiveness and strategic advantage in the market.

Organization: Internet-related services and products

Stolen: Source code

Target: Software Developers

Presumed Impact:

- Stolen intellectual property affected ability to compete and/or reduced the impact of innovation efforts

[11]Kim Zetter, Wired.com, (Jan 2010).

Targeted Defense for Advanced Targeted Attacks

"…actions that evade signature detection require a more preventative approach to protecting assets… As history has shown, **focusing on finding specific vulnerabilities and blocking specific exploits is a losing battle**[12]."

[12]Verizon, Data Breach Investigations Report 2013, http://www.verizonenterprise.com/DBIR/2013 (May 2013).

8-Step Plan to Safeguard Your Organization

Rebalance Your Security Portfolio

To date, organizations continue to spend the vast majority of their cyber security budget on endpoint defenses, such as antivirus software, firewalls, next-generation firewalls (NGFW) and intrusion prevention systems (IPS). While these defenses are an important and key part of security strategy, even if they were 100% effective, additional layers would be needed to ensure that critical business data is protected. Each case study outlined in this eBook demonstrates how advanced targeted attacks, often using spear phishing and malware, consistently defy these technologies. The moment one attacker passes through traditional defenses, the data that drives your organization is theirs for the taking.

Hackers looking to steal sensitive data, such as intellectual property, deal data or PII, know exactly where to find it: in the databases, file servers, and applications that comprise an organization's data center. The reality is that cyber-attacks have become increasingly sophisticated, leveraging multiple tactics and tools, with the explicit purpose of circumventing conventional barriers. The breed of targeted attacks that exist in today's threat landscape requires organizations to rebalance their security portfolio so that it includes a layer of protection positioned closely around the data and applications in the data center.

Secure Your Data Center with Critical Layers of Technology

In order to uphold an effective security posture, it's important that organizations are prepared to manage the threat of an advanced targeted attack. The next section in this eBook introduces the eight steps required to safeguard your organization from advanced targeted attacks, and examines critical layers of technology that businesses can implement to ensure that their data center is protected.

Step 1: Reduce Risk

Identify sensitive data, build policies to protect that data, and audit access activity.

Recommended Solutions

Database Audit and Protection Solutions

A comprehensive database audit and protection (DAP) solution, such as SecureSphere Database Firewall, monitors all access to sensitive data and provides real-time alerting, and blocking, of unwanted or suspicious activity. Leading database audit and protection solutions, such as SecureSphere, include the ability to locate sensitive data within the database to help focus security efforts, and feature database assessments to identify unpatched vulnerabilities and poorly configured security settings which an attacker might use to breach these systems.

File Activity Monitoring Solutions

To protect intellectual property, deal data, and other sensitive data stored in files, file activity monitoring solutions, such as SecureSphere File Firewall, perform continuous monitoring of file access in real time to provide organizations with alerting on unwanted or suspicious activity and a complete audit trail of file data access.

Microsoft SharePoint Security Solutions

For sensitive files and applications hosted in SharePoint, a complete solution for securing SharePoint, such as SecureSphere for SharePoint, has the ability to address the unique security requirements of the platform's file, web, and database elements. SecureSphere security policies allow businesses to respond immediately when SharePoint data, or application access activity violates company policies.

Directory Services Monitoring Solutions

As a critical piece of IT and security infrastructure, directory services, such as Microsoft Active Directory, is a likely target for today's advanced attacks. Solutions for monitoring directory services, such as SecureSphere Directory Services Monitoring, provide real-time auditing and alerting on all changes in Microsoft Active Directory. SecureSphere helps to closely monitor changes within Active Directory, and then take action when undesirable behaviors are observed.

Step 2: Prevent Compromise

Train users how to identify spear phishing emails and deploy solutions that prevent unwanted software from reaching user devices.

Recommended Solutions

Secure Web Gateway

A secure web gateway solution filters malware from everyday Internet traffic, protecting users' machines and enforcing compliance with business and regulatory policies. This technology includes capabilities such as URL filtering, malware detection and filtering, and controls for web-based applications.[13]

[13]Gartner IT Glossary, Secure Web Gateway, http://www.gartner.com/it-glossary/secure-web-gateway (May 2013).

Step 3: Detect Compromise

Identify abnormal and suspicious user access activity and find malware-infected devices.

Recommended Solutions

Database Audit and Protection Solutions

A robust database audit and protection solution, such as SecureSphere Database Firewall, monitors database activity in real time and establishes a baseline of normal user access patterns. SecureSphere identifies material variances in behavior, such as those which occur during malware infiltration, and alerts or blocks suspicious database access activity.

File Activity Monitoring Solutions

In the event that an insider is compromised and malicious attempts are made to access sensitive business data, a sophisticated file activity monitoring solution, such as SecureSphere File Firewall, can detect and stop behavior that violates corporate policy. SecureSphere provides a flexible security policy framework that can be used to block unauthorized or suspicious activity to sensitive unstructured data.

Malware Detection Solutions

It's important for organizations to be able to identify insiders that have been compromised by malware. A malware detection solution, such as the FireEye Malware Protection System (MPS), includes a virtual execution system to protect against multifaceted-targeted attacks that combine web-based attacks, spear phishing, and zero-day exploits.

Step 4: Contain Compromised Devices

Block command and control (CnC) communications from compromised devices.

Recommended Solutions

Malware Detection Solutions

Malware detection solutions can stop outbound callback communications in order to prevent compromised systems from being controlled and exploited by botnet Command and Control servers.

Web Application Firewall Solutions

Protecting critical business applications used internally requires a web application firewall, such as SecureSphere Web Application Firewall. SecureSphere policies can block compromised insiders from accessing the critical applications and the sensitive data they contain.

Step 5: Insulate Critical Applications and Sensitive Data

Stop compromised users and devices from accessing sensitive applications and data.

Recommended Solutions

Database Audit and Protection Solutions

A database audit and protection solution, such as SecureSphere Database Firewall, prevents insiders, known to be compromised, from accessing sensitive database data.

File Activity Monitoring Solutions

File activity monitoring solutions, such as SecureSphere File Firewall, prevent malware-compromised insiders from accessing sensitive unstructured data.

Web Application Firewall Solutions

A web application firewall, such as SecureSphere Web Application Firewall, prevents malware-compromised devices from accessing critical applications.

Step 6: Remediate Compromised Passwords

Change user passwords.

Recommended Solutions

Directory Services

Functionality built into directory services, such as Microsoft Active Directory, provide centralized management and configuration of user settings, which allow IT organizations to facilitate a mandatory employee-wide password reset. This is important in the event that a targeted attack succeeds in compromising a user's credentials.

Step 7: Remediate Compromised Devices

Rebuild compromised devices.

Recommended Solutions

Change and Configuration Management Systems

Change and configuration management systems, such as Microsoft's System Center platform, enable organizations to issue new operating system software to employees, in the event of a large-scale malware infiltration.

Step 8: Post-incident Analysis

Leverage audit trail and forensics to improve the incident response process.

Recommended Solutions

Analytics and Reporting Solutions

Interactive audit analytics simplify forensic investigations and enable identification of trends and patterns that may indicate security risks. SecureSphere, for example, enables security teams to analyze, correlate, and view database and file activity. With both pre-defined and fully customizable reports, SecureSphere's rich graphical reporting capabilities enable organizations to easily understand security status.

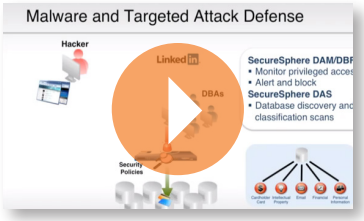
Additional Resources

View Infographic

7 Stages of a Targeted Attack

Download White Paper

How Malware and Targeted Attacks Infiltrate Your Data Center



View Video

Malware and Targeted Attack Defense Customer Story

About Imperva

Imperva is a pioneer and leader of a new category of business security solutions for critical applications and high-value data in the data center. Imperva's award-winning solutions protect against data theft, insider abuse, and fraud while streamlining regulatory compliance by monitoring and controlling data usage and business transactions across the data center, from storage in a database or on a file server to consumption through applications.

LEARN MORE

Find Us on the Web | Contact Us Direct | Read our Blog

Imperva Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com