# How Malware and Targeted Attacks Infiltrate Your Data Center

**"54% of breaches involve compromised servers"**

–Verizon 2013 Data Breach Investigations Report

Advanced targeted attacks are more focused and persistent than ever before, and they continue to increase in sophistication. These next generation threats are multi-phased and organized explicitly to bypass the security perimeter, most often targeting individuals as an entry point. It only takes one compromised user in order for attackers to successfully infiltrate your corporate network and gain full access to the data that drives your business. In the end, your organization is only as secure as your weakest link–the trusted employee.

Organizations understand that their most valuable data assets reside within the data center. Databases contain, for example, credit card data, personally identifiable information (PII), and personal health information (PHI), while file servers store intellectual property, deal data, competitive information, legal documents, and financial information.

While the data center contains the highest concentration of sensitive data and critical business applications, it tends to have the weakest security controls, leaving much of this highly sensitive and business-critical data vulnerable to cyber attack.

### The Impact of Data Breaches

Below are examples of organizations that experienced major data breaches as a result of malware infiltration.

**State of South Carolina**

Cyber attackers stole PII of approximately 4 million citizens, or 80% of the state's population. $14 million was spent to mitigate the attack.

**Chesapeake Energy Corporation**

A third-party financial firm was targeted and lease negotiation information stolen. The breach jeopardized Chesapeake's ability to sell land leases at the most competitive prices.

**Coca Cola**

Hackers targeted company executives and stole deal data relating to the $2.4 billion acquisition of a Chinese juice company. Coca Cola lost a critical window of opportunity to expand into a highly desirable market.

**Nissan**

Malware installed on the company information systems network allowed attackers to exfiltrate employee user IDs and passwords and forage through sensitive files. Designs related to electric vehicle drive train were stolen.

## Attack Motivation

Advanced targeted attacks are motivated by a number of reasons. Each attack operation has a specific purpose and is carried out against a defined target. These attacks are not limited to a certain industry or company demographic. Organizations both large and small are targeted and "taken down" by advanced targeted attacks.

A short list of threat actors and their presumed motivations includes:

### Governments

Government entities are performing advanced targeted attacks for economic or political gain. They typically operate under a low profile and maintain a presence in a network for as long as possible, slowly excavating through company data. An example is the theft of proprietary documents, like military product designs, to plan future wars or compete more successfully in the international market for these goods. Government entities seek a variety of sensitive data such as that which includes information about critical infrastructure, military capacity and technology, intellectual property, and even business data.

### Organized Criminals

Industrialized hacker groups attack organizations in order to pillage digitalized information. These groups are most often profit-driven and focus on data that can be converted into cash, such as credit card information, PII, and intellectual property. Data thefts of this nature are costly for companies, as they incur significant fees to remediate the breach as well as fees associated with failure to comply with regulations, such as Sarbanes-Oxley or HIPPA.

### Hacktivists

Hacktivists target organizations for political causes, ideology, and other personal agendas. Groups such as these have an interest in compromising corporate infrastructure, exposing intellectual property and sensitive data, and embarrassing the target organizations in support of their cause. Hacktivists often leverage online communities to discuss their tactics and actively recruit participants using social networks. These groups favor automated attacks and distributed denial of service (DDoS) attacks, but ultimately use many of the same techniques as the actors above.

**"40% of breaches incorporate malware"**

–Verizon 2013 Data Breach Investigations Report

## Anatomy of an Advanced Targeted Attack

Advanced targeted attacks leverage multiple tactics and tools, with the explicit purpose of circumventing conventional security barriers. Despite using a variety of tools, these attacks usually follow a familiar pattern:

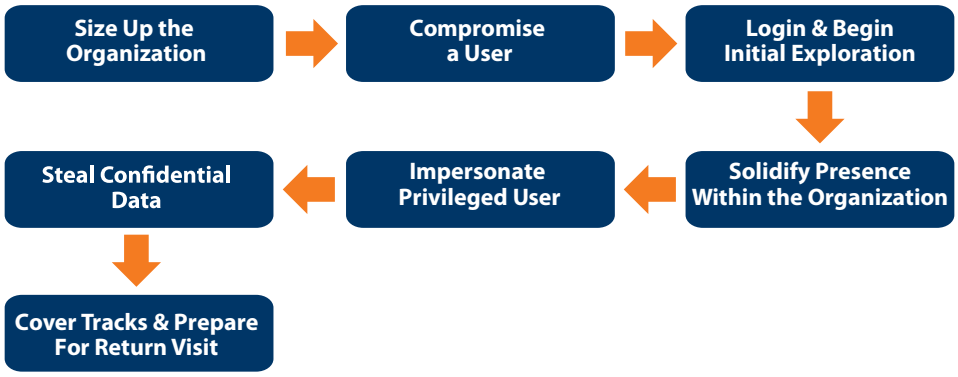
- Attackers begin an operation by searching social networks for specific individuals within the targeted organization.
- Malware is delivered to those individuals as a way to gain access to the corporate network, allowing the attackers to bypass perimeter defenses.
- The attackers then sift through company data stores to find the desired information.
- Before leaving, the attacker may create a reentry path that allows them to return in the future.

While each advanced attack is uniquely executed, they often have certain characteristics in common. The section below examines seven typical stages of an advanced targeted attack.

**"Executives and managers make sweet targets for criminals looking to gain access to sensitive information via spear phishing campaigns. Not only do they have a higher public profile than the average end user, they're also likely to have greater access to proprietary information."**

–Verizon 2013 Data Breach Investigations Report

## 7 Steps of a Targeted Attack




### Step 1: Size Up the Organization

Hackers begin by leveraging social engineering to find an individual or group at the targeted organization. In this stage, cyber criminals seek out insiders related to the particular data they are after, or individuals that have privileged access to the targeted organization's data center. For example, an attacker might search the online professional network LinkedIn for the database administrator (DBA) at a particular organization.

### Step 2: Compromise a User

Once the attackers have determined who within an organization is the desired target, they leverage a variety of hacking tools to install malware and take control of the user's machine. Examples of vehicles used to deliver malicious software include: crimeware, spear phishing, drive-by downloads, and cross-site scripting (XSS).

- **Crimeware** - A category of malware that is automated, scalable, and mass produced. The Blackhole exploit kit, for example, can be licensed from its authors with the intent to deliver a malicious payload to its victim.
- **Spear phishing** - Consists of highly targeted e-mails that are sent to a specific individual or group within an organization. These malicious e-mails appear to come from a trusted source with the goal of coaxing the receiver to perform an action such as clicking on a link or opening an attachment. Once the victim acts, a form of malicious programming, such as spyware, is installed on the device.
- **Drive-by downloads** - A malicious program is downloaded automatically onto a user's device without their consent or knowledge. Drive-by downloads can take place upon visiting a website, viewing an HTML e-mail, or they can be installed at the same time as a user-requested application.
- **Cross-site scripting** - A hacker places unauthorized code into a link that appears to be a trusted source. When the link is clicked, a program is sent as part of the web request and can be executed on the user's machine. This allows attackers to gain control over a device.

**"In many cases, an actor may gain initial entry using a malicious e-mail attachment, and then install additional malware on that and other systems throughout the environment."**

–Verizon 2013 Data Breach Investigations Report

### Step 3: Login and Begin Initial Exploration

Using credentials that were obtained by compromising an insider, cyber criminals log into the network and begin pillaging through company data. One advanced technique is to first seek out documents related to the architecture of the network, which enables attackers to quickly manipulate their way through corporate resources. Advanced targeted attacks attempt to leave the smallest footprint possible, in order for the attacker to remain undetected within the network for the maximum amount of time.

### Step 4: Solidify Presence Within the Organization

At this stage in a targeted attack, the perpetrators steal additional user names and passwords. Because each user has different data access permissions, hackers leverage these credentials to explore systems more swiftly and find the information they're seeking. Cyber criminals also strengthen their presence by installing back doors. This may include creating phantom user accounts for future access, or leaving behind loopholes to bypass security mechanisms and gain entry to the network at a later time.

**"Determined threat actors will leverage formidable skills and resources to entrench themselves in the victim's environment and remain hidden until their mission is accomplished."**

–Verizon 2013 Data Breach Investigations Report

### Step 5: Impersonate Privileged User

After employee credentials have been stolen, the attackers will likely attempt to escalate the privileges of users they have compromised, creating "power users". Since privileged user accounts are often closely monitored, increasing the permissions of other insiders is advantageous because they're less likely to be detected. The goal is to expand their reach into the corporate data center to access a variety of data types.

### Step 6: Steal Confidential Data

At this point in a targeted attack, the hackers now have an established presence in the organization's system and can steal the sensitive information that they covet.

### Step 7: Cover Tracks and Prepare for Return Visit

Once the sensitive data has been taken, the attackers will attempt to hide any evidence of the invasion. For instance, they may delete interim accounts that were created, delete the log records of their presence, or reset registry settings. The hackers will also return escalated permissions back to a normal state to reduce the chance that their presence is detected. It's common, however, to keep one or more accounts escalated, but inactive, in order to return and perform additional reconnaissance at a later time.

**"…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."**

–Verizon 2013 Data Breach Investigations Report

## Complementing Traditional Defenses with Data Center Protection

Looking back a decade or so, the perpetrators of cyber-attacks were essentially online vandals who lacked sophistication and organization. The destructive consequences of their actions were not the objective. The targets of their attacks were not clearly defined. For example, the Anna Kournikova worm of 2001 made headlines and landed the creator in court, but is estimated to have caused under $200,000 (USD) in damages. Many times, these attackers were "script kiddies" or digital "graffiti artists" out to do something simply, because they could. Today, the threat is not from vandals, but from professional groups: governments, organized criminals, and hacktivists.

While cyber threats have clearly evolved, security spending has not. New technologies have emerged to better protect organizations, but the solutions most businesses have in place–and continue to rely upon–are not addressing the core problem. Today, analyst firms estimate that the market spending on network firewalls, including next generation firewalls, is over $7 billion (USD). Intrusion prevention systems (IPS) account for $1.2 billion of security spending, and there is an additional $3 billion being spent on end-point protection solutions, such as anti-virus applications. If these solutions were truly effective at stopping advanced targeted attacks, far fewer data breaches would appear in the headlines.

### Why Traditional Defenses Are Not Sufficient Enough to Counter Modern Attacks

First and foremost, none of the traditional approaches focus on the data center assets, which are the ultimate target of these attacks. The vast majority of firewalls and IPS solutions are deployed at the network perimeter. Even those that are deployed in the data center lack the application and data focus required to protect the data center assets. For example, next generation firewalls, which have an application orientation, are focused in the wrong direction to secure the data center from abuse. They protect corporate users accessing applications outside the organization, but do not protect the organization's internal applications or data.

Compounding the problem is the technology approach these solutions use. Intrusion prevention systems and the IPS technology built into next generation firewalls are both signature based. Similarly, most end-point protection solutions also approach malware from a signature-based perspective. Signatures provide little-to-no protection against rapidly mutating malware or zero-day threats. While some next generation firewalls have added malware analysis engines, they still lack the application and data context to protect data center resources such as databases, file servers, and SharePoint sites from attack.

Organizations would do well to borrow the concept of "rebalancing" from the investment world and rebalance their security portfolios. That is, rather than continue to over-invest in traditional security approaches that do not address the real problem, organizations need to shift some of their investment to a new breed of solutions that can secure the data center assets so coveted by attackers.

Infographic

**8 Steps to Safeguard Your Organization from a Targeted Attack**

**View Infographic**

# How to Protect Your Sensitive Data and Critical Business Applications

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 your organization's data center. Securing your organization's structured and unstructured data is the first step toward an enhanced security posture for countering malware and targeted attacks.

This section introduces the critical functionality required to safeguard your organization from next generation threats and ensure that your data center is protected.

## Discover and Classify Sensitive Information

While it's ideal to have protection for all of your business data, at a minimum, you want to employ a solution with the ability to locate your sensitive data in order to help focus security efforts. You are likely to start by identifying regulated data like financial information, PHI, or PII that's subject to SOX, HIPPA, and other regulations. It's also important to classify sensitive file data such as legal documents, business plans, and sensitive intellectual property assets.

## Build Security Policies

Once the priority data has been identified, security policies should be put in place to enable your organization to respond immediately when data or application access activity violates company policies. In the event that an insider is compromised, and malicious attempts are made to access sensitive business data, it is important to have the ability to detect and stop that behavior.

Out-of-the-box policies that exist in automated solutions are a good way to initially address many well understood security risks. Once standard policies have been applied, it is important to invest in customizing a focused set of security policies for your specific business needs.

## Review and Rationalize Access Rights

Many organizations don't have a solid grasp of user access rights and find it challenging to understand how access was granted. Users typically receive access to information through multiple paths, commonly through membership in different groups, and through inherited permissions. A user rights management framework allows security teams to identify excessive user rights, as well as dormant user accounts that might be used by attackers.

## Audit and Analyze Access Activity

A data center security solution would be incomplete without the ability to monitor all data access activity. Analytics are then required to derive greater insight from the raw data resulting from the audit trail. If a security violation occurs, or suspicious activity requires investigation, it is essential to have rich filtering and drill-down capabilities that allow security teams to interactively sift through large volumes of data. The same analytics platform should have the ability to generate reports that provide greater transparency for business stakeholders.

Video [3:31]

### Malware and Targeted Attack Defense Customer Story

In this video, a hacker uses social engineering techniques to launch a targeted attack that compromises a Database Administrator with malware. The hacker then uses the DBA's credentials to steal credit card data. Imperva SecureSphere is deployed to monitor database activity and proves to be an effective countermeasure against future malware and targeted attacks.

**View Video**

#### Look for Unusual Behavior

With a comprehensive audit trail in place, organizations are able to establish a baseline of normal user access patterns and therefore identify material variances in behavior, such as those that occur during malware infiltration. From there, security policies can alert or block suspicious database or file access activities. The ability to compare monitored activity with the baseline of observed user behavior helps to identify fraudulent activities and attacks.

#### Identify Compromised Devices

It is important for organizations to be able to identify insiders that have been compromised by malware. A malware detection solution can help alert an organization to the presence of malware-compromised devices so that they can take appropriate actions to isolate and remediate these devices.

## Effective Malware Defense Solutions

#### The Imperva-FireEye Solution

Effective malware defense includes a layer of protection closely positioned around the data and the applications in the data center that can be triggered by a malware detection system. Imperva and FireEye enable a comprehensive security solution that automatically restricts applications and data from being accessed by a malware compromised system. The FireEye Malware Protection System identifies infected hosts and then passes that information along to Imperva SecureSphere. SecureSphere uses this actionable intelligence to prevent infected machines from accessing critical business applications and sensitive information in database and file servers.

With the FireEye-Imperva joint solution, organizations can pinpoint machines that have been compromised by malware, and then enforce access controls that prevent malware-compromised insiders from accessing critical applications and sensitive data.

# Imperva SecureSphere Business Security Suite

SecureSphere is the market leading solution for business security. SecureSphere provides comprehensive, integrated application security and data security to prevent data breaches, streamline regulatory compliance, and establish a repeatable process for data risk management.

## DATABASE SECURITY PRODUCTS

**Database Activity Monitoring**
Full auditing and visibility into database data usage

**Database Firewall**
Activity monitoring and real-time protection for critical databases

**Discovery and Assessment Server**
Vulnerability assessment, configuration management, and data classification for databases

**User Rights Management for Databases**
Review and manage user access rights to sensitive databases

**ADC Insights**
Pre-packaged reports and rules for SAP, Oracle EBS, and PeopleSoft compliance and security

## FILE SECURITY PRODUCTS

**File Activity Monitoring**
Full auditing and visibility into file data usage

**File Firewall**
Activity monitoring and protection for critical file data

**SecureSphere for SharePoint**
Visibility and analysis of SharePoint access rights and data usage, and protection against Web-based threats

**Directory Services Monitoring**
Audit, alert, and report on changes made in Microsoft Active Directory

**User Rights Management for Files**
Review and manage user access rights to sensitive files

## WEB APPLICATION SECURITY PRODUCTS

**Web Application Firewall**
Accurate, automated protection against online threats

**ThreatRadar Reputation Services**
Leverage reputation data to stop malicious users and automated attacks

**ThreatRadar Fraud Prevention**
Stop fraud malware and account takeover quickly and easily

## Share this White Paper with Your Network




WP-MTA-0613.1