TREND MICRO™

A TrendLabs Cloud Security Primer

Monitoring Vulnerabilities

ARE YOUR SERVERS EXPLOIT-PROOF?

Security Versus Uptime: A Critical Balancing Act

In an ideal world, security patches are applied to all endpoints and servers the moment vendors release them. But IT teams are also in charge of supporting the day-to-day operations of businesses. To install permanent patches, quality tests need to be run and sometimes mission-critical servers need to go offline for a reboot.

Keeping servers adequately secure often competes with the everyday reality of providing support to business operations for the following reasons:

- **Your IT man-hours are a limited resource.**
  - IT teams often have to make decisions about resource allocation that can be bad for security. Patches, in particular, can take up to 30 days for an average organization to do research on, test, and deploy.[1] Other IT projects or initiatives can force patch management activities to take a backseat.
  - IT administrators must do research on a security update before applying it to make sure it does not cause unintended effects. Actual deployment on hundreds or thousands of servers takes time as well.
  - Unforeseen or emergency and out-of-band updates or updates that are released out of the regular patch cycle established by software vendors can take significant IT resources away from daily operations. This can negatively affect overall productivity.
- **Your IT is either a cost center or a key cost savings enabler.** It can sometimes prove challenging for IT teams to implement or even recommend the timely upgrade or replacement of legacy systems or rebuild outdated in-house-developed applications, especially if these can still function as needed.
- **Your uptime trumps all.** The constant demand to maintain application uptime and avoid server downtime to meet SLAs and ensure business continuity can further force IT departments to deprioritize patch deployment.

Enterprise groups in charge of security face the challenge of ensuring that a business runs smoothly while minimizing risks to servers that support operations.

> The first level of complexity comes from the size and breadth of an enterprise environment. The more devices and applications an organization has, the more difficult it is to keep track of which patches have been installed, which are being installed, and which still need to be installed."
>
> – Using Virtual Patching to Optimize Security Management and Reduce Costs, IDC, June 2012

Managing Vulnerable Servers: Touching Base on Security Risks

Because IT teams help reduce operation costs and fulfill compliance mandates, their perception of and the decisions they make in terms of security can lean toward business and operational concerns. This can introduce a range of security risks such as:

- **Zero-day exploit:** An exploit that takes advantage of a publicly disclosed or undisclosed vulnerability prior to vendor acknowledgment or patch release.

1 http://www.trendmicro.co.uk/media/wp/ogren-group-virtual-patching-whitepaper-en.pdf

"Given how quickly exploits can reach the hands of attackers via automated exploit toolkits, organizations need to respond in kind."

– Using Virtual Patching to Optimize Security Management and Reduce Costs, IDC, June 2012

On April 18, 2012, a proof-of-concept (PoC) exploit leveraging the years-old Oracle Database TNS Listener Poison Attack Vulnerability[2] was found. This exploit affected a widely used database software and could be used without authentication to hijack prior connections to listen in. It can compromise and steal confidential information from affected servers.

The "Apache Killer," reported last August 20, 2011, targeted all versions of Apache software.[3] When used, it could prevent users from accessing target web servers or cause a denial of service (DoS), resulting in lost sales opportunities and disrupted business communication. Active use of this tool was seen.

- **"Buggy" or incomplete vendor patch:** A defective or flawed patch that a vendor releases to address a vulnerability.

  When an issue in the way PHP-CGI handled queries without an equal (=) sign was exploited in Nullcon Hackim 2012, PHP worked on a release to address the vulnerability.[4] If exploited, the vulnerability allows source code disclosure. The patch did not effectively solve the problem though. Another patch was later released to address the problem and the problematic fix.

- **In-the-wild exploit:** Cybercriminals routinely use exploits as part of their malware or cybercrime delivery mechanism. But despite the availability of patches, servers remain at risk if patches are not applied.

  On December 28, 2011, Microsoft released an emergency patch to address vulnerabilities in Microsoft® .NET Framework that also affected several other web applications.[5] These vulnerabilities can take down a server via DoS and expose a network to information disclosure risks, which can either damage an organization's brand image or cause it to incur costs. Because the patch was released at an inconvenient time, several servers remained vulnerable over the yearend holidays in 2011.

  The patch for the MySQL Authentication Bypass vulnerability was released on May 7, 2012.[6] But in June 2012, an exploit using this vulnerability was reported. This exploit allowed a remote attacker to access and log in to a MySQL database with any password, compromising a target database. While the exposure surface is not that large, the problem it causes for affected systems is serious. Incidentally, this vulnerability will not be patched for older builds of affected software.

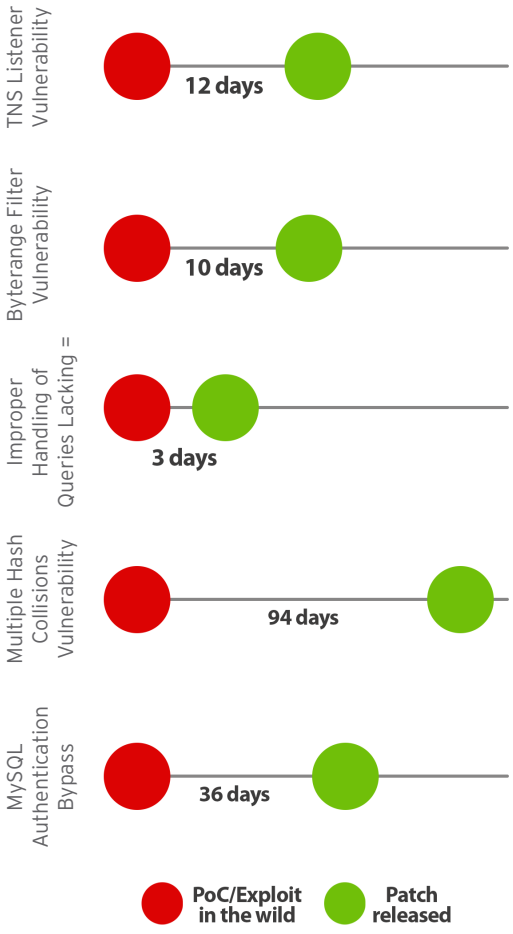

Figure 1. Window of exposure

The desire to avoid business disruption and to follow compliance mandates prevail over security. As such, organizations inevitably introduce windows of exposure despite efforts to patch systems and servers. Systems remain vulnerable to exploits and attacks, opening up networks to security issues like data breaches and DoS attacks that can lead to undesirable business consequences.

2 http://www.kb.cert.org/vuls/id/359816
3 http://blog.trendmicro.com/trendlabs-security-intelligence/solutions-now-available-for-apache-killer/
4 http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
5 http://blog.trendmicro.com/trendlabs-security-intelligence/microsoft-releases-out-of-band-update-before-year-ends/
6 http://blog.trendmicro.com/trendlabs-security-intelligence/mysql-password-verification-bypass-cve-2012-2122/

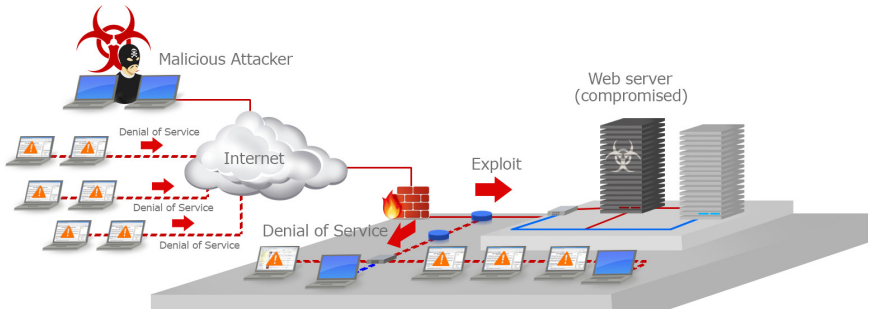

Figure 2. How the Apache Killer works

Virtual Patching: Protection Without the Downtime

IT administrators are seeing the value of virtual patching. As a strategy, virtual patching ensures that business operational goals are met without compromising security. Various studies support this finding.[7]

Virtual patching works on the premise that exploits take a definable path to and from an application in order to use a software flaw. It is therefore possible to create rules at the network layer that can control communication with a target software. By scanning traffic for protocols used, you can, to a certain extent, prevent exploits from doing what they set out to do.

- **Automatic protection.** Virtual patching empowers IT administrators to effectively manage the deployment of permanent patches in a way that will not readily impact operations. The amount of time spent doing research on, monitoring, and testing patches can be more efficiently scheduled. Emergency patches can be immediately dealt with. Unpatched vulnerabilities can be shielded from exploits without disrupting affected servers. Actual permanent patching can also be scheduled along with regular patch maintenance.

- **Protection for legacy software.** Virtual patching allows IT administrators to keep using legacy applications and systems as needed.

- **Protection without downtime.** Most importantly, virtual patching enables IT teams to meet demanding uptime requirements without risking crucial servers.

Trend Micro™ Deep Security can provide protection even before security updates are announced.[8] Deep Security can protect servers against exploits in a noninvasive manner and without requiring systems to go offline.

7 http://www.trendmicro.co.uk/media/wp/ogren-group-virtual-patching-whitepaper-en.pdf and http://poweringthecloud.com/download/347

8 http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/index.html

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO™

Securing Your Journey to the Cloud

TRENDLABS℠

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

TrendLabs
Global Technical Support & R&D Center of TREND MICRO