TREND MICRO

A TrendLabs Security Primer

MONITORING MALICIOUS EMAILS

ARE YOU CAPTURING ALL THREATS?

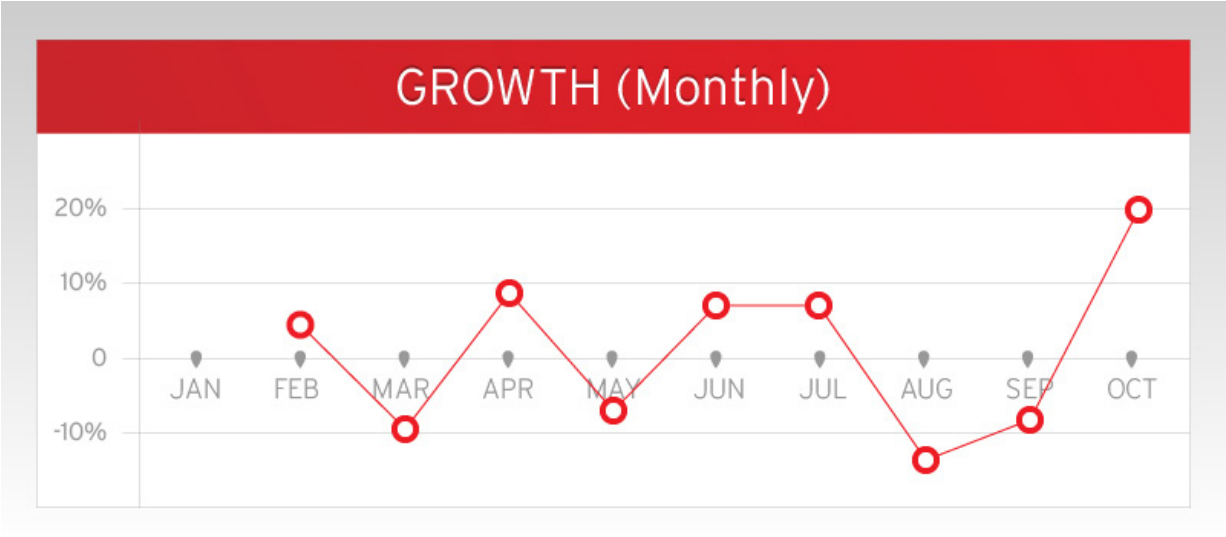
Malicious Emails in the Enterprise

Cybercriminals and other threat actors have seen the benefits of using email to get into target networks. Its ubiquity in offices, whether physical or virtual, has proven to be an efficient way to launch attacks.

Organizations receive at least 20 billion malicious emails each quarter.

Trend Micro internal monitoring conducted from the first to the third quarter of 2012 revealed that the overall volume of malicious emails that businesses received showed no signs of decreasing.[1] Our data indicates that organizations got at least 20 billion malicious emails each quarter. Furthermore, in the same internal monitoring, approximately 450 billion malicious links were blocked within the same period. A month-to-month comparison (see Figure 2) showed alternating ups and downs in the volume of malicious emails, with growth rates ranging from -13% to 20%.

Figure 1: Month-to-month comparison of malicious corporate email volume

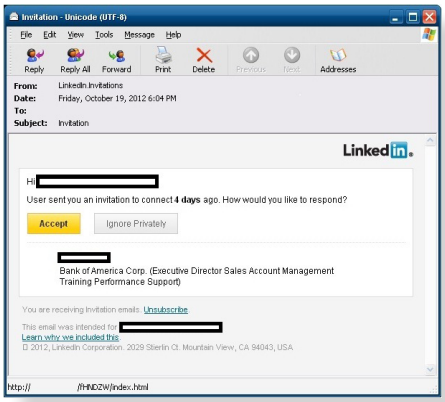


1 Internal monitoring of Trend Micro™ Smart Protection Network™ feedback from January to October 2012.

Attacks Initiated Through URLs Embedded in Emails

Emails can help malware enter a network or initiate an attack in two ways—via attachments or URLs. Successful attacks can range from malware downloads to phishing incidents to targeted attacks, which result in data breaches, compliance concern issues, and financial loss.

Figure 2: Sample email supposedly from LinkedIn



Exploit attacks using the Blackhole Exploit Kit

- The use of this exploit kit has changed how phishing is done.[2] In the past, phishing attacks required users to key in additional personal information; today, they simply prompt users to open an email and click an embedded link.
- Cybercriminals take legitimate emails from organizations like LinkedIn, Citibank, AT&T, or Verizon, and replace the links in the stolen emails with malicious ones.[3] As a result, the emails' content remains legitimate-looking apart from the link.
- This exploit kit has the capability to constantly change the link embedded in each email spammed to users, making detection and the takedown of related pages and/or sites difficult for conventional spam filters.[4]
- Aside from attempting to exploit software vulnerabilities in a user's computer, this kit also detects his/her browser and/or OS version and/or geographic location.[5]

Targeted Attacks

- Emails associated with targeted threats often come with a PDF, a Microsoft Word document, a Microsoft Excel spreadsheet, or a Microsoft PowerPoint presentation as attachments, however, this is not always the case.
- Trend Micro study revealed that 91% of targeted attacks involved spear-phishing emails. While most spear-phishing attacks used document exploits, embedded URLs were seen in 6% of the samples.[6]
- These attacks often targeted nongovernmental organizations and noncorporate entities that frequently have remote or mobile workers.

2 http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-exploit-kit-transforms-phishing/
3 http://blog.trendmicro.com/trendlabs-security-intelligence/same-operation-diversification-of-targets-being-spoofed-current-black-hole-exploit-kit-spam-runs/
4 http://blog.trendmicro.com/trendlabs-security-intelligence/protecting-customers-from-black-hole-exploit-kit-spam-runs/
5 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf
6 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Top reasons why executives think employees must use their own devices:

- Improved mobility (43.1%)
- Avoidance of carrying and/or maintaining multiple devices (13.6%)
- Perception of BYOD as an employee benefit (10.5%)

SOURCE:

Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey, 2012

It is natural for corporate security groups to anticipate threats that may exploit email, more specifically, organizations that adopt trends like BYOD or support users like remote workers. The BYOD trend and the influx of information workers who either remotely work or telecommute have extended the workplace beyond the walls of the office. These virtual offices make email access necessary and inevitable. In a Trend Micro-commissioned study by Decisive Analytics LLC, only a few of the companies that suffered from a data breach actually shut down their BYOD programs.[7] From an enterprise perspective, the benefits of BYOD outweigh the risks it brings. What risks stem from existing corporate practices?

Working via a Mobile Device

- Accessing email accounts outside the organization's network perimeter can bypass security layers like the mail gateway
- Reading office email using mobile devices that have outdated security software or using devices that only get security updates when connected to and inside the office network
- Sending hyperlinks instead of actual file attachments via email, abandoning opportunities to do basic attachment scans

Adopting a BYOD Policy

- Allowing the use of personal mobile devices or handhelds puts security in the hands of users, limiting the organization's control over protection

Employing Traditional Antispam Methods

- Using basic security solutions that either only block unsolicited bulk email or only scan attachments can leave an organization's network vulnerable to other emerging threats
- Failing to protect against malware download via links in messages leaves the network partially protected

7 http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Securing Email in the Age of Mobility and Targeted Attacks

In the face of consumerization and the rise of numerous mobile platforms, OSs, and handheld devices, enterprises need to adopt a multilayered and proactive strategy to protect their classified, proprietary information and business-critical assets.

Employ a multilayered approach to security.

Each security solution plays a distinct role in protecting an organization's infrastructure. A defense strategy that integrates technologies like web reputation, email authentication, and IP reputation may be the most effective way to secure one's organization against emerging multifaceted threats. When implementing a comprehensive security solution, identifying and understanding the user types in an organization is crucial because employees have different needs and issues.

Use a comprehensive mail server security solution.

Businesses need security products with an effective email security component, capable of detecting not only malicious attachments but also malicious web links.

At the speed by which threats continuously develop, a reputation technology that directly correlates with a global threat intelligence resource will provide better protection for company assets. Security solutions that only scan email attachments and/or overlook URLs within email attachments cannot provide sufficient protection. Businesses need security products equipped with an effective email security component that is capable of detecting both malicious attachments and malicious web links in the email body. Because new threats can use thousands of URLs in a single campaign, traditional antispam techniques that rely on sourcing and periodic updates will face challenges.

Integrate email security in one's corporate defense.

Enterprises need to recognize that attackers and cybercriminals know emails are an effective means to instigate attacks. Exploit documents associated with targeted attacks are difficult to differentiate from normal documents. A solution capable of uncovering known and zero-day exploits in attachments like Adobe PDF, Microsoft® Office®, and other document formats can offer a more advanced defense. The volume of emails with malicious links that lead to compromised websites is also on the rise.[8] To improve their resilience from today's emerging and more sophisticated threats, businesses should incorporate email security in their defense line-up. An enhanced web reputation technology that links to a threat information with big data analytics the Trend Micro™ Smart Protection Network™ can enhance one's defenses to the most recent threats. Found in solutions like Trend Micro™ ScanMail™ Suite, this will offer the extensive protection enterprises will need.

In the age of mobility and targeted attacks, enterprises need to consider all aspects of email communication, including email specifics from malicious attachments to malicious URLs in order to reduce risk for enterprises. A mail server security solution, like ScanMail™ Suite for Microsoft® Exchange™, that not only blocks emails embedded with malicious web links but also those with document attachments that contain malicious links will prepare and safeguard organizations from risks beyond traditional email threats.

8 http://about-threats.trendmicro.com/RelatedThreats.aspx?language=au&name=Blackhole+Exploit+Kit+Spam+Runs%3A+A+Threat+Vortex%3F

TREND MICRO INCORPORATED

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