

CommTouch – RPD™ Technology
Network Based Protection Against Email-Borne Threats



- **Email-borne Virus Detection:** Like spam and phishing messages, each virus message can be packed differently in terms of its content and the characteristics of the executable files that include the virus. However, email-borne viruses and in particular worms, can be received from legitimate and trusted email sources that might have been previously infected and were unintentionally distributing the virus to others. Like spam and phishing, email-borne virus attacks often last for very short durations.
- **Inbound vs. outbound detection:** The positioning of the detection mechanism also raises additional challenges. Detecting spam as it enters or leaves a network requires different approaches. Inbound traffic is typically accompanied by a high percentage of spam. Outbound traffic typically consists of a majority of legitimate email increasing the chance for false positives (clean email detected as spam). Finding lower volume outbound spam also requires a dedicated approach.

The Commtouch approach

The Commtouch approach is based on the understanding that all threat outbreaks share some common characteristics, including:

- Most email messages within the outbreak have been altered to make it difficult to set blocking rules based on content analysis.
- Most outbreaks include millions of email messages to maximize the highest possible response rate and the greatest ROI for the attacker. Some attacks though, will be considerably smaller.
- Most outbreaks are released within a short period of time, requiring a real-time solution to detect the outbreak to limit or avoid the damage that can be incurred.
- The originators of the attacks invest heavily in disguising their origin to make it difficult to track the message back to them.

Message Patterns

Outbreaks which distribute spam, phishing, and email-borne viruses or worms, consist of messages intentionally composed differently in order to evade commonly-used filters. Nonetheless, all messages within the same outbreak share at least one or more unique, identifiable patterns or values which can be used to distinguish the outbreak. Some examples of these identifiable values:

- In the case of spam the objective is to lead the recipient to the same commercial web sites that can be classified as spam.

- Pseudo-random combinations of the characters from the subject and body of the email will be repeated in an outbreak.
- Different spam attacks are often launched from the same network of zombie machines that can be blacklisted.
- In the case of phishing, the objective is often to lead the victims to the same set of faked URLs.
- Email-borne viruses always contain the same malicious code (otherwise it is a different virus or another instance of the same virus).

All these are recurring values of typical outbreaks. These values are called the 'message patterns' of the outbreak. Any message containing one or more of these unique patterns can be assumed with a great deal of certainty to be part of an outbreak and therefore spam.

Message patterns can be divided into:

- Distribution patterns – the characteristics of the senders (how many, location) and the volume of the emails sent over a period of time.
- Structure patterns – random combinations of text from the header, and body of the message as well as URLs that are found to be repeated in different messages. An example of this approach is shown below. Note that no content analysis is required.



Spam/phishing patterns extracted from message



取/m取

三最機是般

The challenges of message pattern classification include:

- Determining which message patterns identify outbreaks without generating cases of false positives. All outbreaks attempt to disguise messages as legitimate email correspondence pretending to arrive from trusted sources and therefore, solutions that are based on pattern analysis must be able to tell the difference between 'good' and 'bad' patterns and avoid making mistakes.
- Extracting and analyzing these patterns before the outbreak ends. Most outbreaks have a relatively short lifecycle measured in only a few

Commtouch – RPD™ Technology

Network Based Protection against Email-Borne Threats

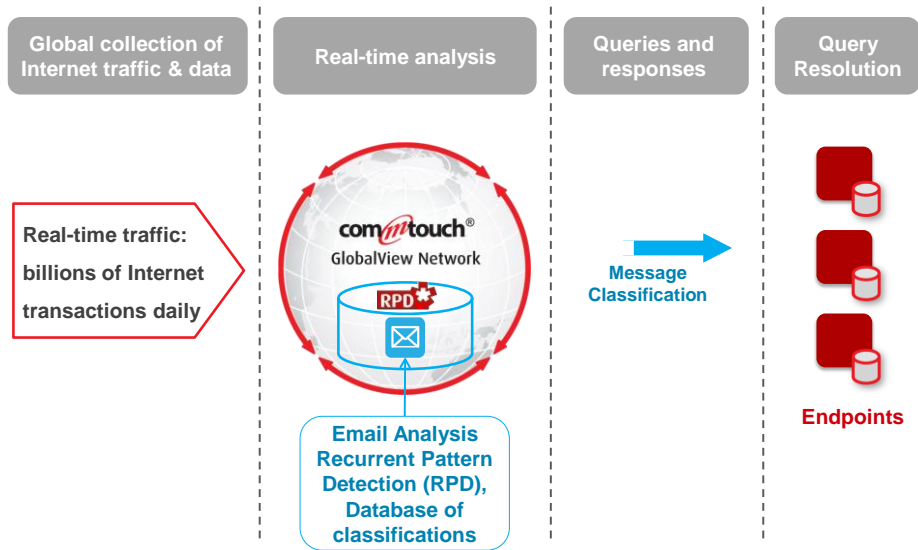
hours. Therefore, any solution that does not detect and classify messages in real-time will only be effective towards the end of the outbreak, when most of the damage has already been done.

The challenges are made more complex by the fact that each new outbreak usually introduces completely new patterns that were not previously analyzed and are therefore unknown to the pattern analyzer. Because spammer tactics are constantly evolving, it is necessary to proactively identify new patterns in real-time in order to determine new outbreaks as they are released.

Recurrent-Pattern Detection (RPD™) Technology

Recurrent Pattern Detection (RPD) technology overcomes the challenges listed above to detect and classify all types of email-borne threat patterns in real-time. RPD is hosted in the Commtouch GlobalView Network, which proactively analyzes billions of Internet transactions daily.

RPD, based on Commtouch’s U.S. patent #6,330,590, extracts and then analyzes relevant message patterns, which are used to identify email-borne outbreaks. RPD classifies both distribution patterns and structure patterns and the analysis results are stored in a vast database of classifications. In addition to identifying new threat patterns, RPD is also used to modify or enhance classifications of already-identified message patterns. Local instances of RPD are used in the GlobalView Network to accurately detect low volume or regional Outbound Spam in conjunction with Commtouch’s Outbound Spam Protection service.



Message patterns are extracted from the message envelope, headers, and body with no reference to the message content.

RPD therefore has the following additional advantages

- RPD can be used to identify outbreaks in **any language, message format, and encoding type**.
- New outbreaks are identified **within minutes**.
- RPD is designed to **distinguish** between the patterns of solicited mass emails which represent legitimate business correspondence, such as **newsletters**, from those of unsolicited spam.
- Commtouch uses RPD in a **highly scalable** environment to deliver extremely **high performance** rates.
- RPD technology is **fully automated** and requires no human intervention.
- To ensure maximum privacy and business confidentiality, RPD analyzes hashed values of **message patterns** and **not** the 'open' values nor the **message content**.

RPD identifies nearly 100% of incoming threat messages with almost no cases of false positives. It is language-agnostic and is equally effective for all message formats and encoding types.

Summary

To effectively combat email-borne threats, a successful solution must address a growing number of challenges. Commtouch's RPD is a proactive detection technology that continues to outwit those who continue to invent new methods to propagate email-borne threats because it does not rely on the contents of the email and therefore, it is able to detect spam in any language and in every message format including: images, HTML, non-English characters, single and double byte character sets, etc. RPD technology offers:

- High spam detection rate with almost no cases of false positives
- Early detection of virus threats
- Protection against phishing attempts
- Content-agnostic threat protection
- Multi-language threat detection
- Multi-format threat detection

RPD is used within Commtouch's Anti-Spam, GlobalView Mail Reputation, Outbound Spam Protection and Zero Hour Virus Outbreak Protection services. These services are available for fast integration into a wide range of service provider and vendor environments. Because RPD uses future-proof pattern analysis, it also provides the best protection of investment for service providers and vendors of messaging and security applications.

About Commtouch

Commtouch® (NASDAQ: CTCH) provides proven Internet security technology to more than 150 security companies and service providers for integration into their solutions. Commtouch's GlobalView™ and patented Recurrent Pattern Detection™ (RPD™) technologies are founded on a unique cloud-based approach, and work together in a comprehensive feedback loop to protect effectively in all languages and formats. Commtouch's Command Antivirus utilizes a multi-layered approach to provide award winning malware detection and industry-leading performance. Commtouch technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, enabling our partners and customers to protect end-users from spam and malware, and enabling safe, compliant browsing. The company's expertise in building efficient, massive-scale security services has resulted in mitigating Internet threats for thousands of organizations and hundreds of millions of users in 190 countries. Commtouch was founded in 1991, is headquartered in Netanya, Israel, and has a subsidiary with offices in Sunnyvale, California and Palm Beach Gardens, Florida.

Visit us: www.commtouch.com and blog.commtouch.com
Email us: info@commtouch.com
Call us: 650 864 2000 (US) or +972 9 863 6888 (International)

Copyright© 2011 Commtouch Software Ltd. Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch, Authentium, Command Antivirus and Command Anti-malware are registered trademarks, of Commtouch. U.S. Patent No. 6,330,590 is owned by Commtouch.

commtouch®
Real Security. In Real Time.