23:35:60
Business Strategy
ATP
Advanced Threat Protection
Protect your organization against ransomware, advanced persistent threats and targeted attacks

ADVANCED THREAT PROTECTION

Effective protection against emerging and Advanced Persistent Threats (APTs)

In recent years, cyberattacks have increased in number, typologies, and severity, targeting company information systems and individuals with the aim of stealing internal and external data and other valuable intellectual property.

The proliferation of new channels of communication and the use of mobile devices for both personal and business purposes (BYOD), increases the attack opportunity and, consequently, the potential benefit for cyber-criminals.

More than ever, companies must be aware of the importance of implementing a proper security strategy, by deploying environment specific tools for protecting digital communications.

The enterprise communications security landscape is expected to be driven by the following trends:

- A growth in the number of **sophisticated hackers** with the ability and resources to launch cyber-attacks, which at the same time will be increasingly difficult to detect.
- **Ransomware/Cryptoware** will continue to be one of the most important threats.
- **Mobile technologies** are one of the main source of concern in the emerging panorama of security threats, specifically due to BYOD adoption and he risks associated with the loss or theft of devices.
- Targeted attacks, website defacing, and hijacking of social media communication channels will increase.
- **Email** will continue to be the most important attack vector, with cybercriminals trying to trick end users into downloading malicious payloads.
- The volume of personal data that form our *digital fingerprint* as well as the information with a business nature, will have a huge economic value for cybercriminals, who seek links, correlations identities and sell that information to the highest bidder.
- More stringent definition of obligations and requirements in **data protection laws, in the European Union and other regions**, requiring companies to assume liability and warranty about data protection.

Our mission: Remove the hackers' advantage

Most organizations rely on low overhead prevention techniques, such as firewall and antivirus solutions and intrusion prevention systems. However, these tools are insufficient, and data breach incidents show that detection in real time must be improved with advanced threat protection solutions (ATP).

The primary benefit offered by advanced threat protection systems is the ability to prevent, detect, and respond to new zero-hour sophisticated attacks.

ATP

Advanced Threat Protection

Spamina ATP solution is **an additional malware protection layer** that sits of top of the Spamina's antispam and antimalware stack.

Spamina ATP incorporates the following technologies:

- File & URL Sandboxing Analysis
- Advanced Premium Antivirus Engine

The service is fully integrated into the Spamina administration panel, providing IT managers with full configuration control and auditing, as well as reporting and service status (dashboard). Likewise, users are promptly notified when received emails are submitted for analysis, and when clicking on URL links that are deemed potentially dangerous.

Advanced Premium Antivirus Engine (APAV)

APAV is a signature based AV engine enabling:

- Highly effective and fast signature-based detection, whose engine identifies and stops a broad range of malware hidden in email attachments.
- Discovery of all samples of known family of malware and their mutations.
- Effective identification of fast-changing threats, leveraging a large distributed network of sensors.
- Behavioural analysis: proactive detection of zero-day threats based on continuous monitoring to detect emerging threats.
- Handling of applications' reputation: APAV reduces false positives for applications by keeping an up-to-date list of executables which are known to be malware-free.

File Sandboxing Analysis

Sandboxing is a security mechanism that executes a program in a controlled environment so that its actions can be analyzed and the effects contained. Sandboxing analysis is frequently used to test unverified emails/programs that may contain a virus or malicious code and links in real time, without allowing the software to harm the end user's access device.

Spamina ATP is powered by a second generation sandboxing technology, which leverages the Complete runtime Environment Instrumentation (CEI) to perform exhaustive object checks that uncover malware even when employing the most sophisticated evasion techniques.

Spamina ATP solution performs dynamic analysis of attachments in the sandbox prior to delivery, ensuring that emails received by end users are safe from virus, ramsonware and zero-day malware.

Spamina's ATP file sandboxing features:

- Complete kernel-level visibility, so that at all times the sandbox knows the actions being carried out by sample program and by the host operating system.
- Effective detection of attempts by the target program at interfering with the sandbox or evading tracking.
- Manipulation and interaction with the subject of the sandbox to elicit behaviours.
- Version-less detection, so that the ability to identify malware is not dependant on the specific software set that may be installed on the end user's environment.
- Dormant code analysis, which allows the identification of latent malware hidden in a program. Such code section may be detected even if they are programmed to be activated later.

Spamina URL Sandboxing

URL sandboxing identifies attacks targeting vulnerable browsers. Typically, malware campaigns as well as targeted attacks send a URL in the email main body, teasing the user to click on it, at which time the malware itself is installed or actions are carried out on the victim's device to leave it open for future abuse.

Spamina's URL check rewrites links included in emails so that whenever the user clicks on it, the URL is verified. The URL is verified in the sandbox and if any suspicious behaviour is detected, the user receives an alert and the access is blocked.

The IT manager may define exceptions so that trusted domains may be exempted from rewriting.

File types analysed

The following table lists the file types are currently analysed in the Spamina ATP sandbox.

Category	Supported types
Executable	- PE and EXE files, including 32 and 64-bit programs and DLLs - MS-DOS programs (EXE/COM) - OS X Mach-O executables - User-mode and kernel-mode binaries - Microsoft installer files (.msi) - Android Applications (.apk) - Java archives (.jar) and compiled files (.class)
Document	- Microsoft Office Word documents (.doc, .docx, .docm, .rtf) - Microsoft Office Excel documents (.xls, .xlsx, .xlsm) - Microsoft Office PowerPoint (.ppt, .pptx, .pptm) - Hangul Office documents (.hwp) - PDF Documents (.pdf) - PDF XML documents (.xpf) - Microsoft Help files (.chm) - ActiveMime docs - WordPerfect (.wpd)
Archives	- BZIP, GZIP, XZ, ZIP, 7Z, RAR, LHA/LZH - Microsoft Cabinet archives - TAR file - Apple .DMG and .pkg archives
Scripts	- JavaScript, Jscript - Scripting languages (BAT and PowerShell) - VBA scripts
Media	- Adobe Flash (.swf), with support for the FWS, CWS, ZWS variants.

Web objects analysed

The following table lists the object types that are subjected to analysis by Spamina URL sandbox.

Object type	Description
Flash	Analyzed under an instrumented Flash player within Internet Explorer. Monitors executed ActionScript code. Detects characteristics of malicious activity, for instance: exploit for specific vulnerabilities, and obfuscation attempts.
JavaScript	Script elements, eval() calls DOM manipulation, and several JS specific functions
ActiveX	Analysis of most IE plugins loaded via ActiveX/COM Identification of ActiveX instantiations. Tracking of all function calls, including their names, parameters and return values.

Flexible licencing model

Spamina ATP is an add-in for Cloud Email Firewall and Parla Mailbox.

It includes granular subscription so that a customer may have the service for:

- The whole company (all domains and users)
- Specific domains.
- Individual users. The IT manager enables or disables the service for specific users.

SPAMINA SOLUTIONS

Cloud Email Firewall

ATP Advanced Threat Protection

Parla Secure Cloud Email

hi! ParlaMI Secure Instant Messaging

Cloud Email Archiving

Cloud Email Encryption & DLP

About Spamina

SPAMINA, is a European-based security company that develops and provides corporations with flexible and Secure Digital Communications. Managing and mitigating cyber-crime related risk is critical. Widely known electronic communications means such as email, as well as the increasingly used instant messaging, are channels where the corporate digital assets can be jeopardized. Simile Fingerprint Filter® proprietary technology protects corporate networks from advanced and zero-day threats. Spamina provides with a safe communication environment where business continuity, service scalability and cost-effectiveness are ensured.

Our cloud services range from enterprise secure email platform, enterprise mobile management, email & IM gateway protection to archiving and encryption & DLP solutions for legal compliance.

A cloud environment involves storage and transfer of digital information. Spamina is subject to the most demanding EU regulations in terms of data protection and is committed to ensuring the highest security standards for digital safeguard.

More information:

Phone: +34 91 368 77 33

sales@spamina.com

www.spamina.com

SPAMINA
Securing Digital Communications