

Trend Micro™ Premium Support and InterScan™ Web Security Appliances Avert Disaster for Large Italian Bank

Banks require perhaps the most stringent of all security measures and technologies to guard sensitive customer and corporate data and maintain 24x7 continuity of connections with global markets and partners. As web-based threats escalate, one bank in Italy remains vigilant in the deployment of best-in-class solutions.

.....

“Trend Micro has done a great job for us, and we completely entrust our top-level anti-malware, anti-spyware, and anti-spam to the company’s solutions and expert advice.”

— Information Security Manager
One of the top five banks, Italy

VIGILANT SECURITY EFFORTS

Due to its extensive and sensitive information assets, a large bank in Italy diligently focuses on the dynamic challenge of securing its corporate network and systems. Besides protecting more than 15,000 clients and servers, the bank is part of an international banking community and must oversee operations that extend into many foreign branch offices. A long-time fan of Trend Micro technology and support, the bank prefers to remain anonymous so as to maintain confidentiality about the details of its security solutions.



.....

KEY BENEFITS

- Comprehensive protection from multiple threats
- Protection against Web-based attacks, before they hit clients and servers
- Proactive threat notification with 24x7 access to a team of security experts
- Easy, centralized management and extensive monitoring and reporting

Through the years, the company has established a company-wide security strategy to take advantage of as many best-in-class solutions as possible. Trend Micro has been a valued partner since 1999 and the bank has been among the earliest to adopt several enterprise offerings:

- Trend Micro Enterprise Protection Strategy
- Trend Micro OfficeScan™ Client/Server Edition
- Spam Prevention Solution
- Trend Micro Damage Cleanup Services
- Premium Support Services

.....

.....

“The Italian Job event was a vivid demonstration of how well protected we are by the Trend Micro InterScan Web Security Appliance and how quickly Trend Micro reacts to new threats.”

— **Information Security Manager**

One of the top five banks, Italy

.....

“Trend Micro has done a great job for us, and we completely entrust our top-level anti-malware, anti-spyware, and anti-spam to the company’s solutions and expert advice,” said the information security manager at the bank. “Trend Micro technology is continuously evolved and enhanced to combat the latest threats. The whole Trend Micro team works very well together to address our unique needs and respond to our situation—we know we are in good hands.”

ADDING PROTECTION FROM WEB-BASED BLENDED THREATS

The bank deploys solutions at multiple points in the network to maximize protection from email, Web, and blended threats. Employees must adhere to strict rules and policies for Web behavior, but even so, the company wanted to tighten security against the increasing numbers of Web-based attacks to make sure that unwanted content did not infiltrate the network during downloads or visits to partner sites.

As soon as it became available, the bank purchased four Trend Micro InterScan Web Security Appliances to scan and block traffic before it reaches servers and desktops. The bank was particularly interested in several capabilities of the new appliance:

- Identifying Web domains known to be producers of spam, viruses, spyware, and other threats
- Ability to scan content in addition to analyzing the source of information arriving at the gateway
- Strict monitoring and control capabilities from a centralized location, to define and oversee download policies
- Real-time and scheduled reporting of network activity

A TEST OF ITS DEFENSES

The virus named the “Italian Job” hit after the bank had introduced the InterScan Web Security Appliances. This major attack eventually infected more than 6,000 sites throughout all of Italy, and impacted more than 15,000 Internet users during the first week after it appeared. The Italian Job is an example of the latest blended threats. In this particular case, malware infiltrated several legitimate Web sites in Italy. These sites related to tourism and travel, entertainment, autos, and adult content. When visitors went to these sites, they were redirected to another site and two Trojans were downloaded unknowingly to the visitors’ PCs. The downloader program—JS_DLOADER.NTJ—exploited browser vulnerabilities to hack into target systems. One of the downloaded Trojans would then go on to download an information stealer, while the other Trojan would act as a proxy server to allow a remote user to anonymously connect to the Internet by stealing the connection on the infected PC.

At the time the Italian Job first appeared in Italy, the bank was in a particularly vulnerable state. A migration was in progress, changing out some old systems for new. In the interim state, some systems were visible to proxy servers but not yet configured into the network that was protected by the Trend Micro appliances. The result was that the Italian Job made its way into parts of the under-construction network. As the attack started to spread, systems being protected by Trend Micro OfficeScan began blocking the threat, but the increase in activity threatened to impact system performance and therefore users. Simultaneously, Trend Micro Control Manager™ showed the bank’s IT team that there was an increase in blocking activity relative to certain parts of the network.

RAPID RESPONSE

The attack originated on a Friday in June. By Saturday, Trend Micro released Web Reputation and URL filtering database updates to block the downloader and Trojans. Since the InterScan Web Security Appliances protected most of the bank's network, the threat was automatically neutralized for most systems. The bank was then able to resume normal Web activities, without being vulnerable to this attack.

Working with Trend Micro Premium Support, the bank quickly deployed a fix to the portion of the network that was under construction and avoided any detrimental affects on user services. The Technical Account Manager (TAM) used his knowledge of the network and solutions deployed to architect a solution that could protect the older systems and the new target systems during the final stages of the migration. Once the migration was complete, the appliances automatically protected all of the systems.

"The Italian Job event was a vivid demonstration of how well protected we are by the Trend Micro InterScan Web Security Appliance and how quickly Trend Micro reacts to new threats," said the bank's security manager. "On the part of the network protected by the appliances, the Italian Job infections were blocked, and the fast response of our TAM made sure that our older systems were also protected until we could migrate them onto the main network. We are sharing our results with our parent company so that they can learn from our experience and enjoy the same level of protection that we have with Trend Micro."

It is highly likely that this type of attack will occur again. These Web-based, blended, for-profit attacks take advantage of several characteristics of today's networks:

- Javascript and the other Web-2.0 related technologies are highly vulnerable.
- Malware toolkits are available for sale on the Internet and are frequently updated, making it easy for hackers to learn how to deploy these attacks.
- Automated tools and technologies, such as bots, enable speedy proliferation of malware and crimeware.

Trend Micro offers several products and solutions that fight these attacks by blocking URLs from infected sites and scanning for malware and spyware downloads.

TREND MICRO PRODUCTS

- **Trend Micro OfficeScan Client/Server Edition**
<http://us.trendmicro.com/us/products/enterprise/officescan-client-server-edition/index.html>
- **Trend Micro Control Manager**
<http://us.trendmicro.com/us/products/enterprise/control-manager/>
- **Trend Micro InterScan Web Security Appliance**
<http://us.trendmicro.com/us/products/enterprise/intercan-web-security-appliance/index.html>



Copyright © 2007. Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, InterScan, OfficeScan, Trend Micro Control Manager, and Trend Micro Damage Cleanup Services are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice.

SS06ITBANKIWSA071002IT

www.trendmicro.com