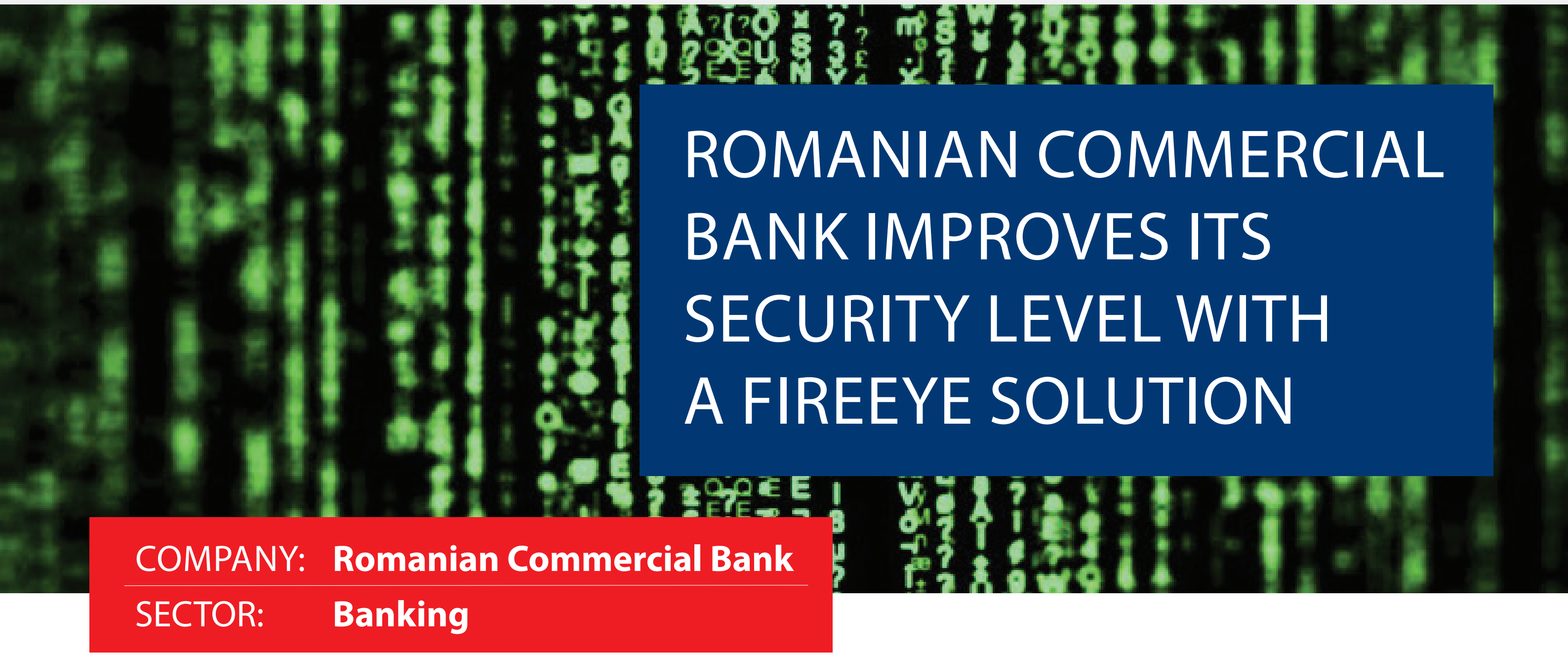
SOITRON GROUP

CASE STUDY



ROMANIAN COMMERCIAL BANK IMPROVES ITS SECURITY LEVEL WITH A FIREEYE SOLUTION

COMPANY: **Romanian Commercial Bank**

SECTOR: **Banking**

1 Requirements

- A complementary solution for already used applications and systems, capable of delivering timely protection against advanced cyber threats.

2 Solution

- FireEye Network Security (NX) security solution.
- Quick detection and addression of cyber attacks that exploit "0 Day" security holes type and "advanced malware" threats that cannot be detected in a timely manner.
- Uses conventional security tools based on signatures databases.

3 Results

- By implementing the FireEye solution, BCR obtained a superior speed of detection and a better reaction time in detecting and resolving security incidents that can be punctually identified, which offers the possibility to take measures at the workstation level.

> "The sustained growth of FireEye, nearly **50% per year,** and the diversity of its customers shows that the products of the company are highly appreciated by the customers who want to improve their speed of response in case of targeted multi-vector attacks, such as Advanced Persistent Threats. Currently, the IT security architecture of BCR provides the best commercially available protection over "zero day" attacks ."
>
> **GABRIEL MUȘAT**
> Tehnical and Marketing Director, Datanet Systems

Overview

Banking and financial institutions around the world are currently facing a rapidly growing diversity and number of threats that present a higher degree of complexity.

Faced with this ongoing challenge, the organizations are obliged to constantly reassess the effectiveness of protective tools and methods they use, and to adopt security solutions able to detect and block new types of cyber threats in a timely manner.

> "To be able to provide better and safer services to BCR's clients, we need, first of all, secure and 'clean' systems. Currently, this condition cannot be ensured only by using an antivirus and / or firewall, we need a more complex instrument, capable of performing advanced searches following models and action patterns, depending on the context, using different IPs carrying information etc. For us, all these requirements have been met by FireEye Network Security solution."
>
> **IANCU NICOLAE BOGDAN TURCU**
> Supervisor Security Management and Business Continuity, Romanian Commercial Bank

> "The value of a bank is not strictly given by the owned physical goods, but also by the value of information with which it operates. And this cannot exist without the computer security component, which has become an essential element in the functioning of any bank. Data security and integrity is to BCR an absolute priority, both in terms of compliance with market legislation and regulations, and also in terms of assuring its customers comfort. Security is an added value to any service that BCR will be delivering to its customers."
>
> **dr. CRISTIAN GOICEANU**
> Executive Manager of Security Management and Business Continuity, Romanian Commercial Bank

Technical capabilities

FireEye Network Security (NX) product series allow organizations to prevent, detect and rapidly respond to cyber attacks that exploit "0 Day" security vulnerabilities and advanced malware threats that cannot be detected in a timely manner by using conventional security tools based on signatures databases.

FireEye Network Security solution implemented at BCR performs a check on the entire Web traffic generated by the bank's employees, to identify any anomalies or threats and block eventual cyber attacks. The device receives a copy of the generated Web traffic, while the end user benefits from real traffic, which prevents the occurrence of the problems in the access area.

Solution and the implementation partner

New cyber attacks types are mainly using Internet as a propagation environment and allow attackers to quickly detect and identify the protection systems of the target-organizations, to compromise and take long-term control over key applications, for the purpose of data compromise and / or theft. The main vectors of infection that may carry malicious programs (delivered as executable files, PDF documents, Java objects, archives, etc.) are: Web traffic, file sharing and email traffic. New generation of exponents are advanced malware threats and multi-vector attacks having precise target, which cannot be effectively detected and blocked by traditional security solutions using identification technologies based on signature lists.

Incoming traffic received by the FireEye equipment runs through several virtual machines corresponding to work environments accessed by the end users. Virtual instances run multiple versions of the applications representing the two main ways to propagate threats - operating systems (workstations), Office suite, versions of Acrobat Reader, Java machines etc.

Other solutions used by the company did not provide visibility into all phases of a cyber attack and were not able to identify the types of attack in which the attacker firstly installs a non-detectable product.

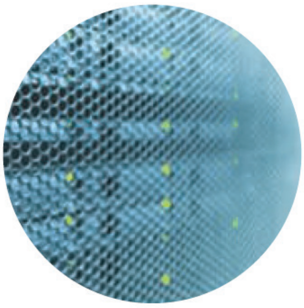
> “ With FireEye Network Security solution, we can minimize the potential impact of a security incident. The successful resolution of any crisis means, first of all, to minimize the negative impact and then solving the problems. Therefore, one of the key elements is the reaction time - we cannot take the risk of discovering such problems too late. ”
>
> **dr. CRISTIAN GOICEANU**
> Executive Manager of Security Management and Business Continuity, Romanian Commercial Bank

The FireEye Network Security solution automatically blocks threats at an early stage, if it identifies them (daily, FireEye runs over 50 billion analysis on virtual machines, with which it constantly updates the equipment ecosystem - every 60 minutes - regarding new types of emerging threats), or after these threats are captured and analyzed at the virtual machine level.

The solution automatically blocks potentially malicious file delivery, and also the communications with the command and control servers generated by these, in order to prevent network attacks and data theft.

Advantages and benefits

The main benefit attested by BCR using FireEye Network Security solution, is that the bank is able to detect and block threats more quickly compared to using conventional solutions. It offers to BCR a superior detection speed and reaction time in resolving security incidents. In this implementation performed by BCR, the FireEye solution is exclusively designed to detect and stop Advanced Persistent Threats.



Another advantage of the FireEye Network Security solution is that the product is almost completely “plug-and-play”. This meant for BCR reduced effort of eployment and integration, ease of setup and use, and eliminating the risk of traffic disruption, if there is a malfunction in equipment.

At the operational level, an important gain is that BCR is able to identify the threats in detail and therefore, has the opportunity to take measures at the workstation level, reducing the effort of detecting and solving the issues.

> “ The FireEye Network Security solution is a preventive mandatory component at the moment, the purchase decision being based on the idea of ensuring an additional security level. The FireEye project is part of the proactive strategy of BCR regarding the security zone and was designed to provide complementary protection for the products and solutions that the bank is using. ”
>
> **dr. CRISTIAN GOICEANU**
> Executive Manager of Security Management and Business Continuity, Romanian Commercial Bank

> "By intercepting the Web traffic of the users, the FireEye equipment runs different file types on the integrated virtual machines, and based on the recorded behaviors, it sets a level of risk for each file. The simulation of a workstation on a virtual machine is performed using a proprietary hypervisor. This is very important as most current malware codes are able to detect whether they are running in a virtual environment and based on this detection they can set an idle status to avoid being detected. On the other hand, the software component of the FireEye Network Security solution doesn't interact directly with the performed activities within the virtual machine. Practically, it works like an observer which launches alerts when it identifies a potential abnormal behavior that may represent a risk factor, and based on these alerts different decisions can be taken - investigating, blocking etc."

OCTAVIAN SZOLGA
Senior Security Consultant, Datanet Systems

Datanet
SYSTEMSINTEGRATION

Established in 1998, Datanet Systems is one of the leading system integrators for data networks, leader in unified communications systems, videoconferencing and infrastructure solutions for data centers.

Datanet Systems is the leading Cisco partner in Romania and develops business partnerships with international vendors such as EMC, VMware, Symantec, FireEye, LANDesk, Certes Networks, Aruba, Zoom International, Airwatch.

The company has a complete and competitive solutions portfolio at international standards in the following areas: communication infrastructure, data center and virtualization, unified communications, contact centers, customer interaction, and information security.

Datanet Systems has a team of over 50 people, totaling over 65 professional certifications. Starting with November 2009, Datanet Systems is part of Soitron Group SE.

BCR

Romanian Commercial Bank (BCR), a member of Erste Group, is the most important financial group in Romania, providing universal banking operations (retail, corporate & investment banking, treasury and capital markets), and covering specialty companies working on the leasing market, private pensions and housing banks.

BCR is Romania's No. 1 bank in terms of asset value (over €15 bn.), in terms of client base and in terms of savings and crediting. BCR is also Romania's most important financial brand, judging by the client trust rate and by the number of persons who consider that BCR is their main banking partner.

BCR uses a network of 22 corporate business centers and 23 mobile offices dedicated to corporate clients, and 551 retails units located in most communities inhabited by at least 10,000 citizens to provide a full range of financial products and services.

BCR is Romania's No. 1 bank running on the banking transactions market, since BCR customers have the largest ATM network at their disposal – over 2,100 ATMs and 13,500 POS terminals enabling customers to use their cards for shopping purposes, as well as the complete Internet banking, mobile banking, phone banking and e-commerce services.