TRAPX SECURITY

CASE STUDY

FINANCIAL INDUSTRY INSURANCE

Attackers Target Authentication Data

Project Background - a Technology Evaluation

Our financial case study focuses on a global insurance institution. Prior to our involvement, there were absolutely no indicators of malware infection or persistent threats visible to the customer. The customer had a robust industry suite of cyber defense products which included a firewall, anti-virus suites, intrusion detection software, endpoint security and other software.

Within a short period of time, the TrapX DeceptionGrid generated ALERTS and identified two malicious separate processes involved in unauthorized lateral movement within the insurance company network. Upon analysis it was determined that both of these malicious processes were communicating with multiple connection points in Russia.

These connection points in Russia and the other injected software captured worked together as an advanced password stealer. The attackers penetrated the network and had captured password information. This targeted theft of authentication credentials represented a serious threat to the integrity of the company's overall operations. At this time it has not been determined to what extent passwords were captured prior to detection.

Other malware of lower risk identified by DeceptionGrid included Trj/Downloader.LEK Trojan, TROJ_QHOST.DB Trojan, and the W32.Greypack worm. All of these were not detected by the customers existing cyber suite. Analysis suggests at least one of them might have been detected but the alerts were missed against the volume of overall alert traffic.

Critical and Confidential Authentication Credentials at Risk

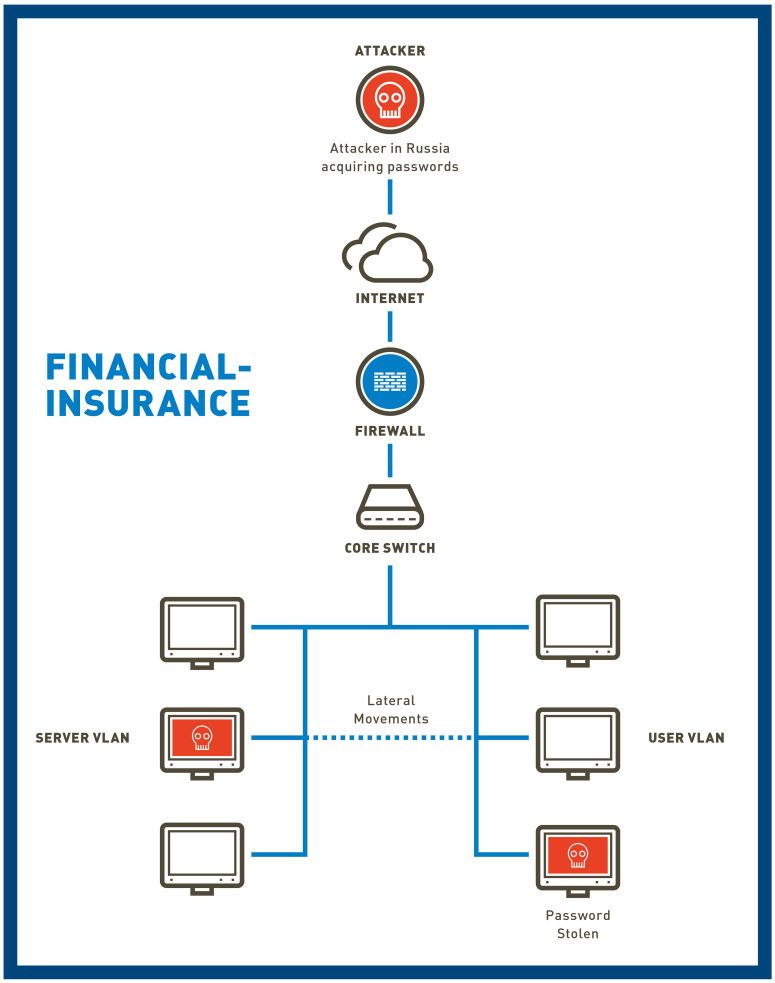
TrapX determined that critical and confidential password data was being exfiltrated to Russia. The scope of data compromise is still under investigation at this time and the global insurance firm has taken pre-emptive measures to replace credentials on suspected software systems.

DECEPTIONGRID **KEY BENEFITS**

- Defense Targeted for the New Breed of Malware. Our innovative deception based cyber security defense finds sophisticated malware and Zero Day Events that your existing vendors do not detect.
- Reduce or Eliminate Economic Loss. Better detection reduces the risk of economic loss due to destruction of enterprise assets, theft of data, and overall impact to business operations.
- Move Faster. Advanced realtime forensics and analysis empowers your security operations center to take immediate action to disrupt all attacks within the network perimeter.
- Compliance Benefits. Improve compliance capability to meet PCI, HIPAA, data breach laws and many other legislative requirements on a global basis.
- Lowest Cost of Implementation for Deception Technology. Deception based technologies have always been very powerful but very expensive and impractical to deploy at large scale. Now DeceptionGrid enables the use of this powerful class of defense at the lowest levels of cost to your enterprise.
- Compatible With Your Existing Investment. Deception technology can integrate with your existing operations and defense in depth vendor suites.

CASE STUDY

DeceptionGrid Discovered The Attack



DIFFERENTIATION

- Real-time detection of malware movement anywhere within the vLan in your enterprise.
- Reduction in the time to breach detection. We find malware unseen by other cyber defense software.
- No more big data problems. A TrapX alert is over 99% accurate and immediately actionable.
- Complete static and dynamic analysis of malware, even Zero Day Events, is automated and fast. Your Security Operations Center has everything they need to take action.
- Automated deployment of DeceptionGrid for your entire enterprise enables provision on a scale previously unattainable with legacy deception technology.
- Protect all vLans for identified malware, even Zero Day Events, when you find one instance of a threat in your networks. Our Threat Intelligence Center leverages our unique defense on a global basis.

About TrapX Security

TrapX Security is a leader in the delivery of deception based cyber security defense. Our solutions rapidly detect, analyze and defend against new zero-day and APT attacks in real-time. DeceptionGrid™ provides automated, highly accurate insight into malware and malicious activity unseen by other types of cyber defense. We enable a pro-active security posture, fundamentally changing the economics of cyber defense by shifting the cost to the attacker. The TrapX Security customer base includes global 2000 commercial and government customers around the world in sectors including defense, healthcare, finance, energy, consumer products and other key industries.

CONTACT US
TrapX Security, Inc., 1875 S. Grant St., Suite 570, San Mateo, CA 94402

+1-855-249-4453
www.trapx.com

Download our product: links on the bottom of our homepage via www.trapx.com

FOR SALES: sales@trapx.com
FOR PARTNERS: partners@trapx.com
FOR SUPPORT: support@trapx.com