TRAPX SECURITY

CASE STUDY

FINANCIAL INDUSTRY BROKERAGE

Attackers Target Key Application Systems

Project Background - a Technology Evaluation

Our financial case study focuses on an institution integrated closely with a major stock exchange where we provided an installation of our product technology. Prior to our involvement, there were absolutely no indicators of malware infection or persistent threats visible to the customer. The customer had a strong industry suite of cyber defense products which included firewall(s) set in multiple zones, anti-virus suites, intrusion detection software, endpoint security and other specialized software. Our installation included a total of fifteen (15) VLANS serving both users and servers.

Within a short period of time, the TrapX DeceptionGrid identified a variety of ongoing attacks with accompanying data compromise. Multiple command and control points were discovered within key administrative and operational system user workstations. Further, multiple connections to the TOR anonymous proxy server were discovered. These are often used in conjunction with attacks to provide further protection for the attackers and their activity.

Other malware was detected that should have been detected by the anti-virus suite. The malware was remanufactured such that the behaviour changes were no longer detectable by the standard anti-virus suites. These additional threats included Worm.Win32.Viking.A, CnC.Win32.Generic, and TrojanDownloader:Win32/Small.ZYP. This tactic of morphing existing malware into undectable variants renders much of the existing cyber defense ineffective.

Critical and Confidential Financial Data Compromised

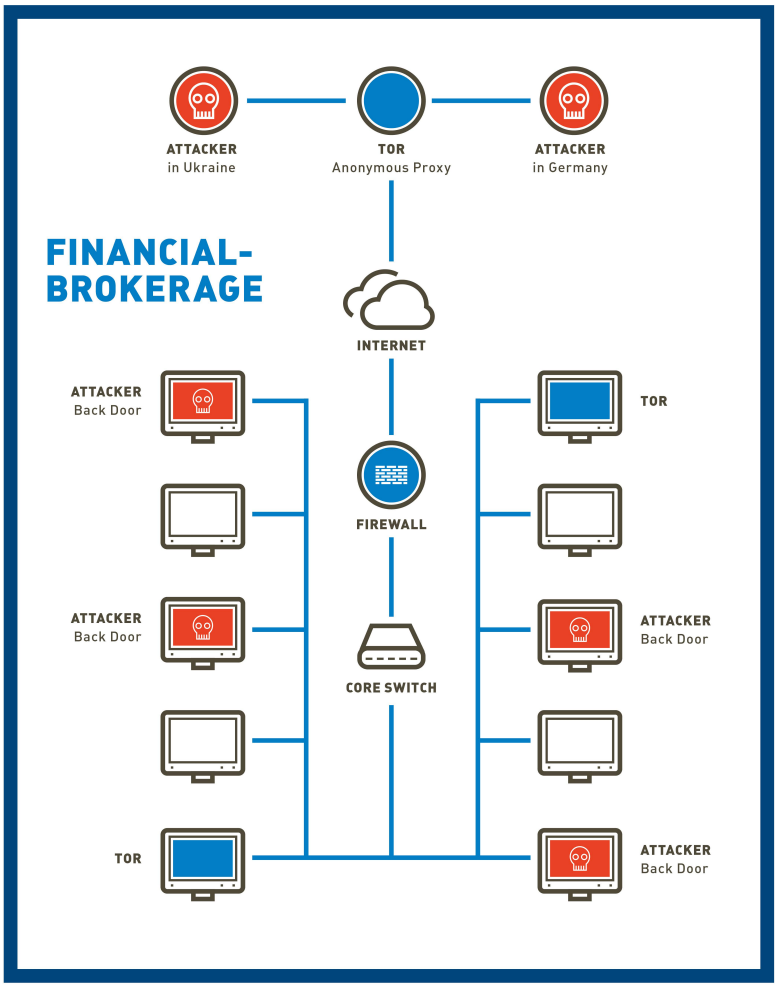
TrapX determined that critical and confidential financial data was being exfiltrated to multiple sites which included one location in Germany and two locations within the Ukraine. The scope of data compromise is still under investigation at this time. Lateral movement from any undiscovered command and control points enables our financial institution to identify and shut them down rapidly.

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