TRAPX SECURITY

CASE STUDY

GOVERNMENT
LAW ENFORCEMENT

Attackers Target Law Enforcement Data

Project Background - a Technology Evaluation

Our case study focuses on a prominent law enforcement agency. This agency has responsibility for many activities which may include highly sensitive investigations into organized crime and terrorist activity. This agency is always interested in improving their cyber defenses and has a large budget dedicated to technology acquisition. Priorities for this agency include the protection of the confidentiality of their ongoing operations, internal processes and their personnel.

This agency conducted a survey of technology vendors and wanted to learn more about deception technology. They were familiar with legacy honeypot technology and found it to be far to expensive to implement both in terms of resources and financial cost. This agency was very cautious and had partitioned several networks within the enterprise. Some were to be used for highly confidential (classified) data only - others for data of lesser confidentiality.

Advanced Persistent Threat Leverages Lapse in Protocol

DeceptionGrid was placed into operation. Within one week the customer security operations (SOC) team received a High Priority Alert indicating the lateral movement of an advanced threat. The malware was automatically trapped and injected into the sandbox for continued analysis. The attackers had established sophisticated command and control and had bypassed the complete array of existing intrusion detection, firewall, endpoint and perimeter cyber software defense.

A full investigation continued as DeceptionGrid continued to monitor and capture malware movement. The agency's security operations team determined that there was an internal breach in their protocol. A connection, in breach of the agency's operting procedures, was found between their secure network and one of the less secure networks (lower security rating). This breach in protocol enabled the attacker's access .

Exfiltration of Data Discovered and Halted

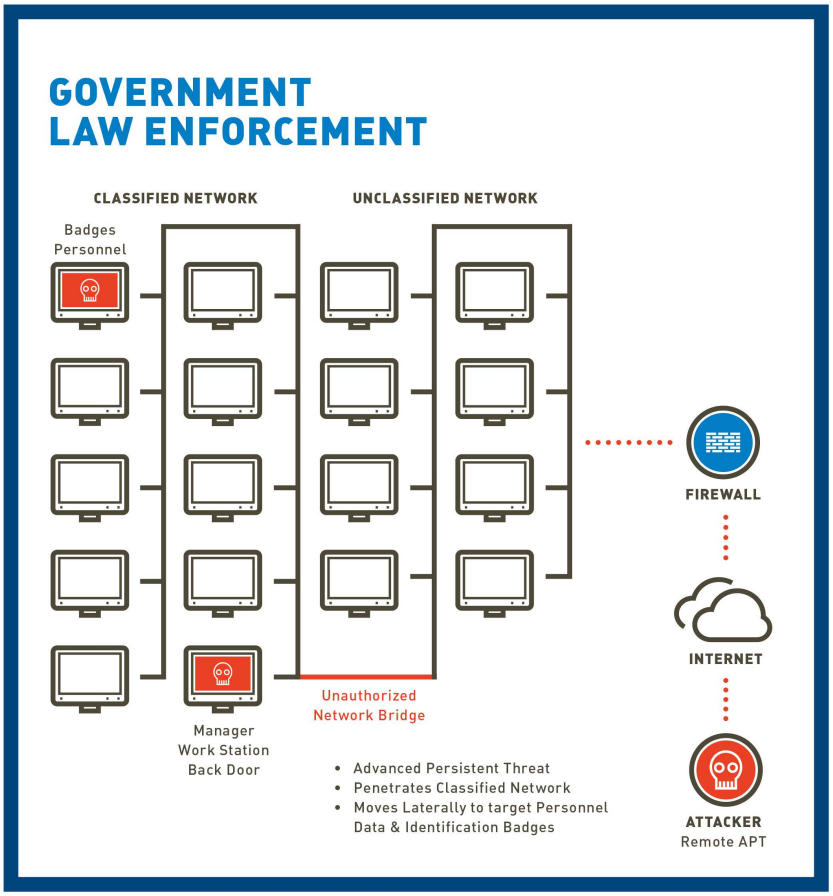
The attacker was found to have moved without detection throughout the law enforcement agency network and servers. There were over ten explicit lateral movements made prior to detection by DeceptionGrid. The attacker found and exfiltrated data including the confidential records of agency personnel, their I.D information, their photographs and other highly confidential data. DeceptionGrid enabled the agency to disrupt the attack and then confidently restore normal security protocols.

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 Detects a Breach in a Classified Network



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