TRAPX SECURITY

CASE STUDY

GOVERNMENT NATIONAL AGENCY

Multiple Attackers Penetrate National Agency

Project Background - a Technology Evaluation

Our case study focuses on a large national government agency. This agency has hundreds of employees and has multiple facilities disbursed over a large geographic area. This agency wanted to learn more about deception technology as part of their regular evaluation of cyber security vendors.

Massive Penetration by Attackers Detected in Multiple Areas

DeceptionGrid was placed into operation. Starting almost immediately and over the course of several weeks the government security operations command (SOC) team received multiple High Priority Alerts. This was one of the most massive attacks we have ever discovered.

We identified multiple attackers in several areas to include over five (5+) attackers using malware servers, over five (5+) attackers linking back data flow to botnet c&c servers and over fifty (50+) remote attackers using TOR anonymous proxy to hide source IP addresses. In some cases the malware was automatically trapped and injected into the sandbox for continued analysis. Multiple attackers had established command and control and had bypassed the complete array of existing intrusion detection, firewall, endpoint and perimeter cyber software defense.

Malware found included Cryptowall, P2P Malware, Trojan-Banker, Trojan-Ransome, Mobogenie.B and WS.Reputation.1.

Exfiltration of Data Discovered - Broadscale Remediation Required

It is clear that multiple attackers have successfully exfiltrated[1] data from this government agency. The attack vectors varied substantially and compromised workstations and servers across multiple departments. Required remediation was done on a broad scale and included re-provisioning of both workstations and servers. The government involved has been forced to either re-provision on a large scale, or, to perform more time intensive memory dump analysis to better understand the extent of the penetration by this varied mix of attackers.

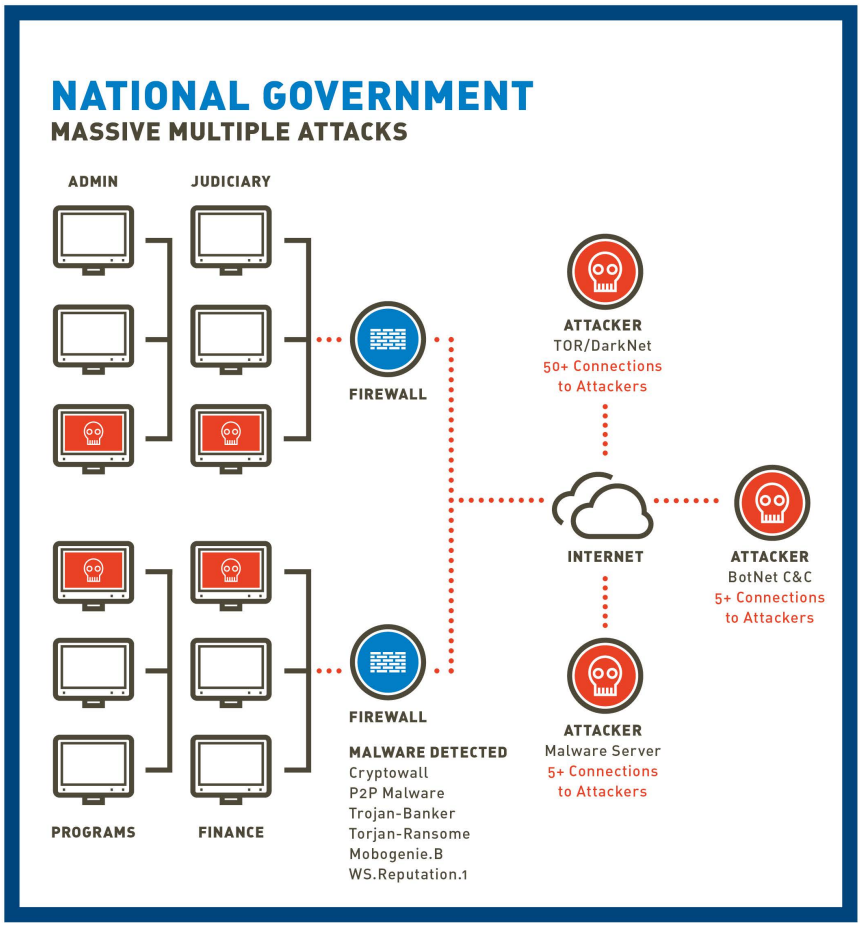
Source attacker IP adresses as known are confidential at this time and part of an ongoing criminal investigation.

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 Multiple Attackers on a National Government's Infrastructure



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