TRAPX SECURITY

CASE STUDY

GOVERNMENT
PROVINCIAL - CITY - MUNICIPALITY

City Government Under Silent Attack

Project Background - a Technology Evaluation

Our case study focuses on a medium sized city government serving a constituent population of over 250,000. This city government has hundreds of employees. Their information technology team wanted to learn more about deception technology as part of an evaluation cycle they had planned earlier in the year. Most of their server based information technology is managed in-house within a single data center. Servers and applications are accessible to city government employees through mobile devices, laptops and desktop based workstations. They have a standard mix of cyber defense software but do not have any substantial protection for their mobile computing (non-windows devices) environment.

Penetration by Attackers Detected in Multiple Areas

DeceptionGrid was placed into operation and rapidly generated alerts associated with Botnet C&C operations. Over five (5+) botnet C&C operations were detected linking back to attackers.

These botnets were found in several departments to include budgets, planning, administration and more. In some cases the malware was automatically trapped and injected into the sandbox for continued analysis. It appears that a small number of multiple attackers had successfully established command and control and had bypassed the existing cyber defense suite of software.

Malware found included CNC.Win32.Generic, CNC.Zeus and TroanJSFakebyScreen.B. Normally, defense-in-depth cyber suites would detect some of this malware. In this case, as in many others, the re-manufacture of standard malware yields a new variant which cannot be easily detected by standard tool-sets.

Exfiltration of Data Under Investigation

The attacker has likely exfiltrated data but the full extent of the attack is unknown. IP addresses link back to France and the Netherlands. Source attacker IP adresses as known must remain confidential.

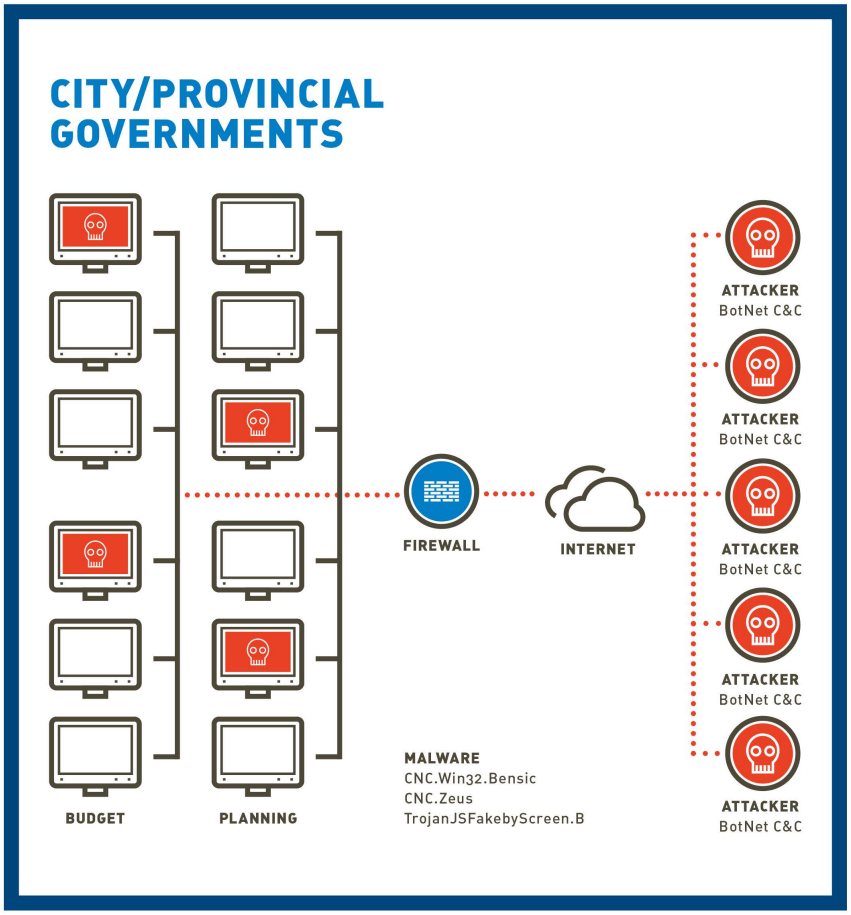
The attacks were, in part, socially engineered through a targeted email campaign. An investigation continues to better understand how the compromise occurred so that city government employees can be better trained on how to avoid or minimize occurrences in the future.

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 Attackers in Critical City Government IT 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