TRAPX SECURITY

CASE STUDY

# TECHNOLOGY SOFTWARE VENDOR

## Attackers Target Software Company

### Project Background - a Technology Evaluation

Our case study focuses on a leading software vendor that provides software through cloud services to their customers in healthcare. This customer's information technology team invested very substantially in defense-in-depth cyber defense software. Their security operations center regularly detected malware and was able to routinely remediate all of these known incidents.

The customer had a strong industry suite of cyber defense products which included firewalls, anti-virus suites, intrusion detection software, endpoint security and other software. Our initial installation included over ten (10) vLANS.

DeceptionGrid was placed into operation. Almost immediately the customer information technology staff received multiple High Priority Alerts. These included identified suspicious activity and led to the discovery of several network misconfigurations. Several internal internet addresses were exposed to the internet and open to a variety of high risk protocols. Inbound connections from attackers were operational via SSH, Telnet and Remote Desktop. A TOR (anonymous proxy) obfuscated web crawler had mapped all of the exposed hosts.

Some of the malware was automatically trapped and injected into the sandbox by DeceptionGrid for continued analysis. The attackers had multiple command and control points and had bypassed the complete array of existing security.

### Multiple Concurrent Attackers Detected and Remediated

A full investigation continued as DeceptionGrid continued to monitor and capture malware movement. Multiple command and control point in six (6) workstations were linked to attackers in Beijing China, Moldava, and the multiple locations within Ukraine. Dozens of workstations had to be re-provisioned to eliminate access. Manual memory dump and analysis was required across many information technology assets to identify the full scope of the extensive and previously undetected attacker activity.

### Scope of Data Theft Remains Indeterminate

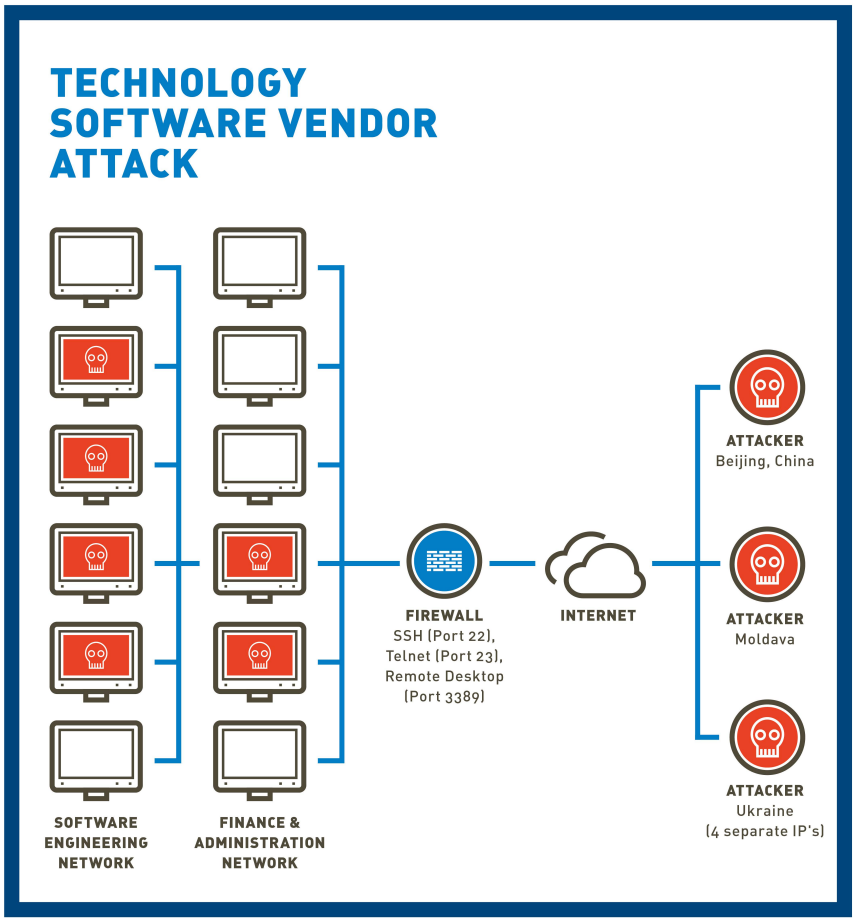
Multiple attackers accessed this technology company's networks workstations and servers. The scope of intellectual property data exfiltration and theft is unknown but under continued investigation.

## 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 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