TRAPX SECURITY

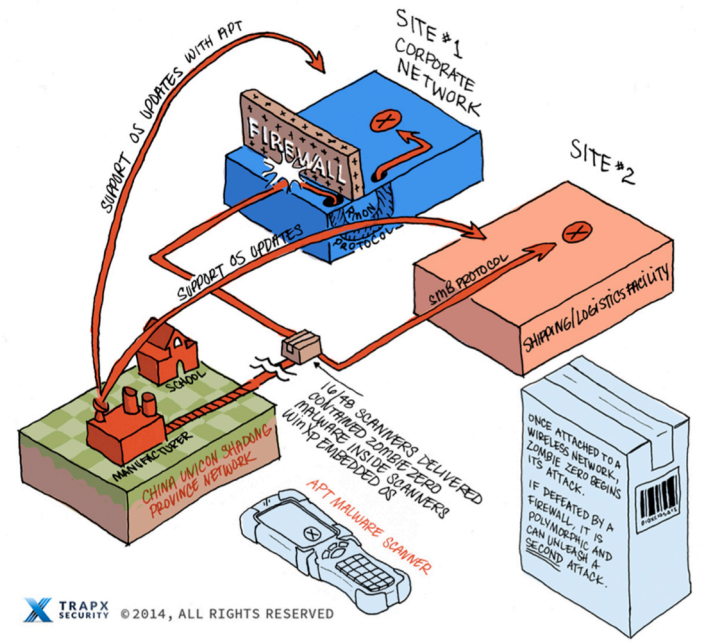
Anatomy of the Attack: Zombie Zero

The Anatomy of the Attack: Zombie Zero

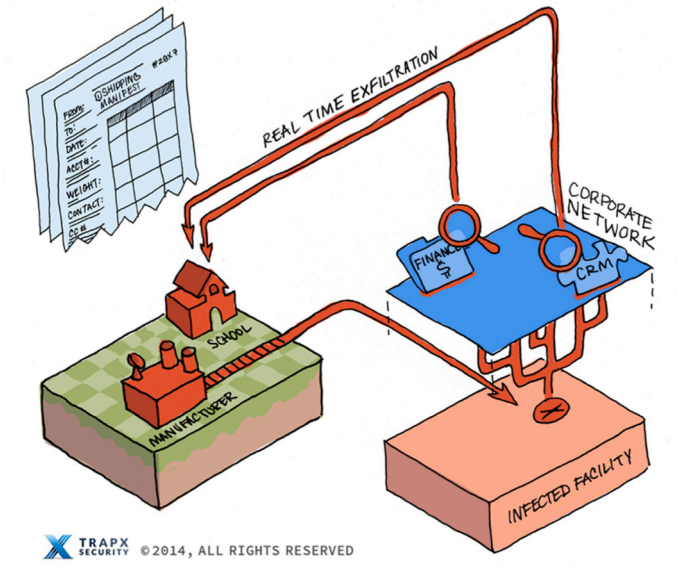
Zombie Zero

- **Zombie Zero is a suspected nation-state sponsored attack** on targeted logistics and shipping industries.
- **Variants of this Advanced Persistent Malware** have recently been seen in manufacturing sectors as well.
- **Weaponized malware was delivered into customer environments** from the Chinese factory responsible for selling a proprietary hardware/software scanner application used in many shipping and logistic companies around the world.
- **The same hardware product with a variant of this malware was sold and delivered** to a manufacturing company as well as to seven other identified customers.
- **The malware was embedded in a version of Windows XP installed on hardware** at manufacturer's location in China.
- **Malware also persisted in the Windows XP** embedded version located at the Chinese manufacturer's support website hosted in China.

1. ZOMBIE ZERO APT DELIVERY SYSTEM TO THE SHIPPING AND LOGISTICS INDUSTRY VIA HARDWARE SCANNER



2. ZOMBIE ZERO APT COMMAND AND CONTROL NETWORK ESTABLISHED



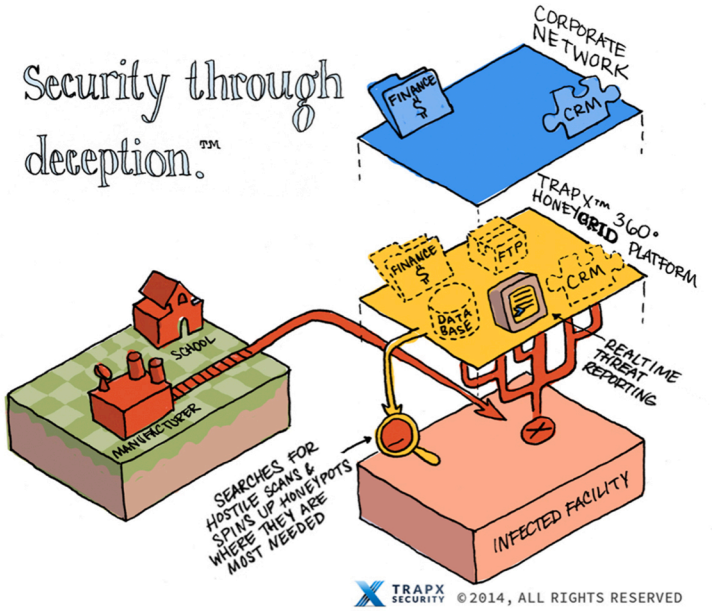
Description of the Chinese hardware/ software scanner application and the user company's security environment:

- **Items being shipped/transported are scanned as they are loaded/offloaded** from vehicles such as ships, trucks, and planes.
- **This scanned data (origin, destination, contents, value, to, from, etc.) is transmitted** to the corporate ERP via an exterior wireless network.
- **The customer deployed scanners at two major distribution sites.** Site 1 had a firewall between the corporate production network and the end-point scanner wireless network that provided community of interest (COI) separation between computing environments. Site 2 had no firewall between the

corporate production facility network and the end-point scanner wireless network.

- **The customer had deployed significant defense-in-depth security,** using all market-leading brands of firewalls, IPS, IDS, mail gateways, and agent-based products.
- **ERP was from one of the top** three market-leading vendors.
- **The customer installed security certificates on the scanner devices** for network authentication, but because APT malware from the manufacturer was already installed in the devices, the certificates were completely compromised.

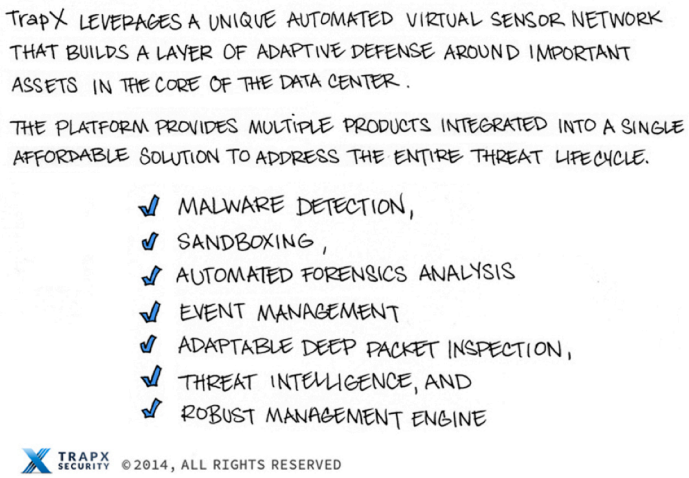
3. TrapX DETECTION AND INTERDICTION



Description of Zombie Zero APT behavior:

- **Once the scanner was attached to the wireless network** and put into production, it immediately began an automated attack on the corporate environment using the SMB protocol (port 135/445). At Site 1, where the customer had network segmentation using a firewall, the malware SMB attack was defeated. However, this malware was polymorphic and launched a second automated attack leveraging the RADMIN protocol (port 4899) that successfully infected more than nine servers. The secondary attack was successful at defeating the corporate firewall at Site 1. Because Site 2 had no corporate firewall, the SMB attack was successful.

4. HOW WE'RE DIFFERENT



- **The customer had deployed 48 total scanners** from the Chinese manufacturer; 16 of the scanners were infected with the APT malware.
- **All scanner attacks targeted very specific corporate servers.** The attack looked for and compromised servers that had the word 'finance' in their Host name (a Host name is an English word representing a computer number/address). This particular ERP system handles all aspects of corporate transactions including, but not limited to, corporate financial data, customer data, and detailed shipping and manifest information.
- **The attack successfully located the ERP financial server** via automated means and compromised it.

- **Stage two of the attack facilitated the upload of a "stand-by" weaponized payload** from the scanner that established a comprehensive command and control connection (CnC) to a Chinese botnet that terminated at the Lanxiang Vocational School located in "China Unicom Shandong province network". A second payload was then downloaded from the botnet that established a more sophisticated CnC of the company's finance server. A secondary stealth botnet CnC network (the owner of the IP address was masked) was also established and terminated at a location/facility in Beijing. It should be noted that the Lanxiang Vocational School has been previously linked to on-line attacks of Google and was implicated in the famous Operation AURORA attack two years ago.
- **The Chinese manufacturer of the scanner is located** in the same physical area of the Lanxiang Vocational School.
- **Exfiltration of all financial data and ERP data was achieved,** providing the attacker complete situational awareness and visibility into the logistic/shipping company's worldwide operations.