CASE STUDY

The Case of the Fools Gold Image

Security professionals today need to be on the lookout for threats coming from any direction – even from inside their organization. And when a threat is shared unknowingly, what needs to happen to identify and stop it?

Trustwave®

Client Spotlight

A US-based organization specializing in large-scale public utility work, specifically R&D for heating/cooling within large industrial environments, was expanding their operations in Asia.

The Challenge

To expedite the setup of IT systems in new locations in Asia, corporate IT shared a master or "gold image" to ensure consistent configuration and performance settings. What they didn't realize was that in addition to system setup details, the gold image was also sharing suspicious files to every new system deployed. These files did two things. They injected.dll libraries into running memory space to give a malicious actor remote command and control of the victim systems. They also created a cryptominer. A malicious actor with access to the systems and the cryptominer could then use the processing power of the organization's server network to perform cryptocurrency mining. This was the situation when this organization became a new client of the Trustwave Managed Detection & Response service. As part of the client onboarding process, Trustwave SpiderLabs threat hunters began a proactive threat hunt investigation into the organization's corporate network and new locations in Asia. The threat hunters quickly discovered something wasn't right in this organization's network.

> *"We weren't expecting the Trustwave SpiderLabs proactive threat hunters to discover that a member of our own team was spreading malware."*

The Solution

Trustwave SpiderLabs threat hunters follow a comprehensive approach to systematically target in on dangerous and complex threats. In investigating this organization, the hunters first identified suspicious internal SMB scanning activity on port 445. This indicated a malicious actor or group was looking for open ports over which to exploit the SMB vulnerability EternalBlue. Of special interest was that this scanning began immediately as new systems came online. Additional investigation identified the suspicious files on the gold image that were giving command and control access to remote users and dropping the cryptominer on new systems. Reverse engineering showed these files were consistent with malware from Dynamite Panda, a Chinese APT group known for targeting the US industrial base. The SpiderLabs threat hunters added this malware to the Trustwave threat intelligence database and devised unique endpoint use cases to identify and eradicate the malware throughout the organization's environment. The organization rebuilt its gold image and after an internal investigation, identified a senior IT staff member who was using company resources for personal cryptobanking.

Industry Threat

As organizations learn that attackers are dwelling unnoticed on their networks for months or even years (83 days is the average attacker dwell time according to a recent Trustwave Global Security Report), many are seeing the need to move beyond basic threat prevention and want to be more proactive in identifying and eradicating threats. One technique, threat hunting, has surged in popularity in recent years. Threat hunting is broadly defined as the manual practice of applying tools, tactics, procedures and intelligence to uncover advanced network attacks that have slipped past existing defenses.

> *"It's as important to assume you've already been breached and regularly look for attackers in your network as it is to put protection mechanisms in place."*

Trustwave®

CSFG-0419