
CYBONET

NETWORK TRAPS: Using Distributed Decoys for Proactive Threat Detection

Prevention Is Ideal – Detection is a Must

Networks continue to expand through the inclusion of additional devices of all varieties (BYOD, tablets, printers, coffee machines, etc.) and the continued union of cloud and on premise applications. This business environment is enhanced and further complicated through the varied activities of users operating within the network. Users who, in parallel to the evolving global business environment, are accessing information from many sources, interacting with a myriad of additional endpoints in equally scattered networks, and whose own judgements and limited understanding of security best practices are continuously pushing organizations and their networks into greater unknown territories. In such an environment, businesses must contend with a cyber threat landscape that is continuously shifting and asymmetrical. Cyber criminals, by virtue of their clandestine and offensive position, hold the upper hand when it comes to penetrating a network and exploiting the vast weaknesses inherent in the modern business environment.

This ever shifting, dynamic network reality has made proactive detection capabilities a growing necessity for any business harboring critical intellectual property in digital format, a distinction that increasingly spans all verticals and company sizes. As security analysts have reached consensus on the need to complement endpoint and network protection solutions with Endpoint Detection and Response Solutions, Gartner has further sharpened by defining the situation as a need to move away from incident response to what they term ‘Security Protection as a Continuous Process’. Advanced targeted attacks can easily bypass traditional, signature based prevention mechanisms like firewall and anti-virus protection that are particularly vulnerable to sophisticated zero-day attacks and Advanced Persistent Threats. Attacks will inevitably circumvent traditional blocking and prevention mechanisms, and it is therefore key to detect the intrusion in as short a time as possible to minimize the hacker's ability to inflict damage and/or extract sensitive organizational information.

Network Traps: From Deception to Detection

Deception tactics in cybersecurity are designed to move the cybersecurity strategy of an organization from a reactive to a proactive defense. Deception Technology is defined as any technology that aims to disrupt an attacker's activities by purposefully misdirecting or misleading the intruders so that they reveal themselves and, in the best possible scenario, their true intentions.

Network Traps, sometimes referred to as ‘Honey Pots’ or ‘Honey Traps’, are a form of Deception Technology that exist in parallel to an organization’s real network and endpoint assets. The Network Traps are ‘decoy’ end points distributed throughout the network environment and that effectively lay dormant; ‘looking’ like a viable endpoint within the network. Network Traps are designed to not only be ‘preyed’ upon by attackers, but to collect, log and often initiate responses within a broader Endpoint Detection and Response Solution. The very nature of Network Traps means that if the trap has been triggered or interacted with, it is an indication that there is some level of intrusion.

Lateral Movement: APT Malware in the Network

One attribute that underscores almost every advanced threat is persistence. Unlike a traditional bank robbery or shoplifting ring, modern cyber criminals tend to move slowly and methodically within a network, aiming to take their time, gather information, and generally lay low for extended periods. Even with some sophisticated behavioral analysis tools, cyber attacks can be overlooked due to the low profile way that they can mimic normal, lateral/internal network behavior. Advanced Persistent Threats' operating guidelines are based on this concept of lateral movement. Once attackers are in, they slowly and quietly collect data and analyze it to plan their attack. When they reach a machine, attackers attempt to extract valuable data.

False Positives: Information Overload Can Undermine Security Effectiveness

In the modern business environment, with its myriad endpoints and the continuous emergence of new, critical business applications - all within a distributed network environment - traditional Endpoint Detection and Response Solutions are subjected to a limitless source of information and alerts. Often, given the nature of the work environment, this dynamic information and data can signal a near endless procession of alerts that, more often than not, indicate harmless, normal behavior and network traffic. These 'false positives', when harmless activity is flagged as a threat, can quickly undermine the effectiveness of an EDR Solution by failing to adequately distinguish between real breaches within the network versus activity that falls within the normal bounds of 'business as usual'. Such a muddling of the threat landscape leads to an ineffective implementation of the solution and often, due to low confidence from the administrator, low adoption of the solution itself.

Because false positives can undermine confidence so quickly, it is important that a threat detection solution is supplemented with deception technology that can complement the system. Network Traps provide a detection system with a tool that mitigates almost completely against any false positive alerts. This is because Network Traps lay 'dormant' and are only engaged if an attacker 'finds' them and begins interacting with the trap itself. With firewalls and antivirus software, it can often take months to realize a breach occurred, but deception technology triggers alerts the moment an attacker 'trips the wire'.

Identifying APT Breaches: Multiple Protocols Are Key

The evolving threat landscape means that APT malware comes in many forms and varieties. Network services speak specific languages and these languages are known as protocols. When they were first deployed, it was sufficient for a successful Network Trap to comprise of opening a port, waiting for a piece of malware to connect to the port and then simply downloading that malware for analysis. Today, APT has grown in sophistication and an effective Network Trap must be capable of credibly interacting with malware across a wide range of protocols. Amongst those protocols that are often exploited for APT are Server Message Block (SMB), Hypertext Transfer Protocol (HTTP), HTTPS, File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Microsoft SQL Server (MSSQL) and Voice over IP (VoIP).


CYBONET