CYBONET

Security Stack: Network Traps

CYBOWALL USES NETWORK TRAPS TO IDENTIFY LATERAL MOVEMENT

NETWORK TRAPS OVERVIEW

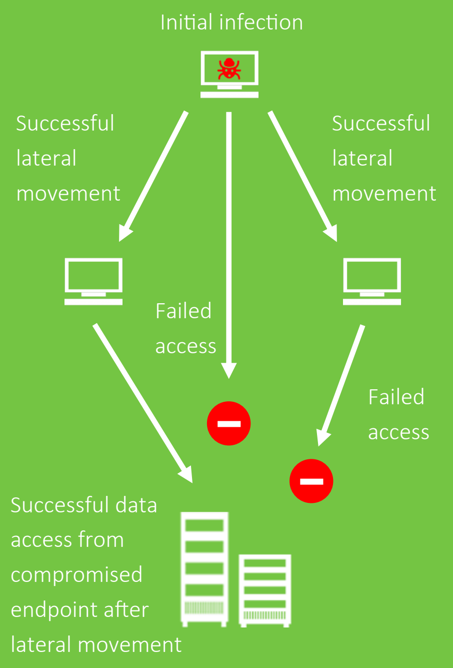
Network traps, sometimes referred to as ‘honeypots’ or ‘honey traps’ are an intrusion detection technique. They take the form of decoy endpoints distributed throughout the network that effectively lie dormant, ‘looking’ like a viable endpoint within the network. They act as a security resource whose value lies in being probed, attacked, or compromised; providing indications of intrusion if triggered or interacted with.

The information captured by network traps enables the building of attacker profiles, in order to identify preferred attack methods, and it allows for an in-depth examination of unwelcome users during and after network trap use. New vulnerabilities and risks to various operating systems, environments and programs, including viruses and worms, can be identified, and network traps provide material for further study.

The network trap is set up to look just like a regular system - including files and directories - to attract attackers to connect to it so that their actions can be studied. It should be configured in a way that is difficult, but not impossible, to break into; exposing it deliberately to an attacker in search of an attractive target. By loading network traps with monitoring and tracking tools, every step and trace of activity left by an attacker can be captured in detail and recorded in a log for further investigation.

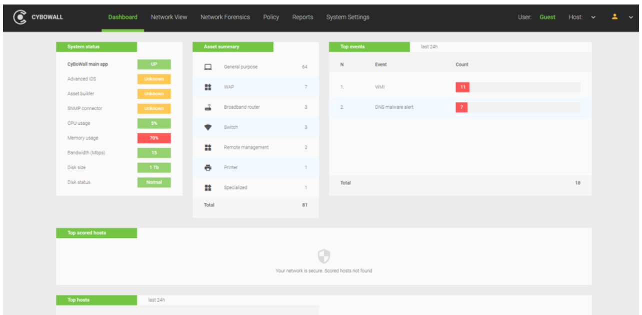
LATERAL MOVEMENT AT A GLANCE

Lateral movement commonly refers to any techniques used by a cyber attack once it has breached the network to move within the perimeter and search for key data and assets.


Initial infection
Successful lateral movement
Successful lateral movement
Failed access
Failed access
Successful data access from compromised endpoint after lateral movement

HOW DOES CYBOWALL EMPLOY NETWORK TRAPS?

The Cybowall solution integrates network traps to enable insight into lateral movement between endpoints and detect threats originating within the network by serving as a trip wire for active attacks.



System status

CyBoWall main app	UP
Advanced IDS	Unknown
Asset builder	Unknown
SNMP connector	Unknown
CPU usage	5%
Memory usage	70%
Bandwidth (Mbps)	15
Disk size	1 Tb
Disk status	Normal

Asset summary

General purpose	64
WAP	7
Broadband router	3
Switch	3
Remote management	2
Printer	1
Specialized	1
Total	81

Top events last 24h

N	Event	Count
1.	WMI	11
2.	DNS malware alert	7
Total		18

Top scored hosts

Your network is secure. Scored hosts not found

Top hosts last 24h

This distributed deception grid prevents attacks in several ways. First, it slows down and stops automated attacks, such as worms or autorooters, which randomly scan an entire network to identify vulnerable systems that can be placed in a 'holding pattern'. Second, network traps can deter human attacks by sidetracking the attacker, leading them to devote attention to activities that cause neither harm nor loss.

In this way, the network traps built in to the Cybowall solution reveal attackers that have already breached a network's perimeter defenses, and enable the organization to analyze, mitigate and report any such breaches.

NETWORK TRAPS - ONE ELEMENT OF A MULTI-VECTOR SOLUTION

Network traps comprise one element of Cybowall's multi-vector approach to strengthening information security and protecting against today's cybersecurity challenges. By themselves, network traps have a narrow field of view and can only see activity directed against them. An attacker who identifies a network trap could avoid it and still infiltrate the organization. Network traps do not therefore replace other security mechanisms. Instead, they work with and enhance an organization's overall security architecture.

Cybowall's approach is to combine network trap capabilities alongside other technologies for maximum network visibility. It integrates asset mapping, vulnerability assessment for patch management prioritization, threat detection, actionable event correlation and reporting. With a Sensor that sits out of line and takes a copy of all network and internal traffic via TAP/Port Mirroring, Cybowall functions as an Intrusion Detection System (IDS) at the network level. Cybowall also utilizes an Agentless Scan that leverages, amongst other technologies, WMI capabilities to collect detailed forensic data and correlate it with known Indicators of Compromise (IOC). Connected directly to the network's core switch via SNMP, Cybowall's user interface provides a single pane of glass view for easy management, continuous network visibility and effective breach detection.

NEXT STEPS FOR YOUR ORGANIZATION

Cybowall can empower your organization to meet today's cyber security challenges by leveraging multiple technologies within one intuitive and affordable solution to detect, investigate and report on information security breaches.

Read our ***Cybowall overview*** *or contact* ***info@cybonet.com***