Lumeta IPsonar

SOLUTION BRIEF

Operationalizing Threat Intelligence using Lumeta IPsonar plus Cyber Threat Probe

Network Situational Awareness coupled with external threat intelligence service feeds identifies Botnets, Zombies and other Cyber Threats

Organizations are at constant risk of infiltration by known bad actors on the Internet or the Dark Web, and need to be proactive about trying to prevent attacks. Cybersecurity professionals are asking . . .

- Can known threat or malware IP address space on the Internet be reached from within the enterprise network?
- Has any of the internal network infrastructure become a zombie participant in a botnet?
- Do any of our trusted network assets show up on blacklists? On Shadowserver or attacker lists?
- Are any of our trusted network assets behaving as TOR relays/bridges/devices?
- Is our organization harboring devices using known Trojan or malware ports?

The Lumeta Cyber Threat Probe provides authoritative answers to these questions, helping organizations quickly detect zombie infections and other threats from bad actors. With the Cyber Threat Probe, threat intelligence (from external commercial and open source feeds) is made actionable by utilizing existing capabilities of the Lumeta IPsonar network situational awareness platform to correlate a comprehensive index of an enterprise's networked IP address space against known threats. As soon as new threat intelligence becomes available, the Cyber Threat Probe will report against the new threats immediately and sends out alerts. The Cyber Threat Probe includes the ability for user-defined views to highlight findings and ease remediation.

The Cyber Threat Probe is a plugin for Lumeta IPsonar (point-in-time view), available at no additional cost.[1]

IT professionals can use the Cyber Threat Probe for the following use cases:

- Zombie/Bot Hunting – Determine whether or not any enterprise assets are malware infected infrastructure.

- TOR Relays/Bridges – Identify any enterprise assets acting as TOR relays/bridges potentially for nefarious purposes.

- Known Malware Command and Control (C2) Servers – Determine whether or not there is connectivity from inside the network.

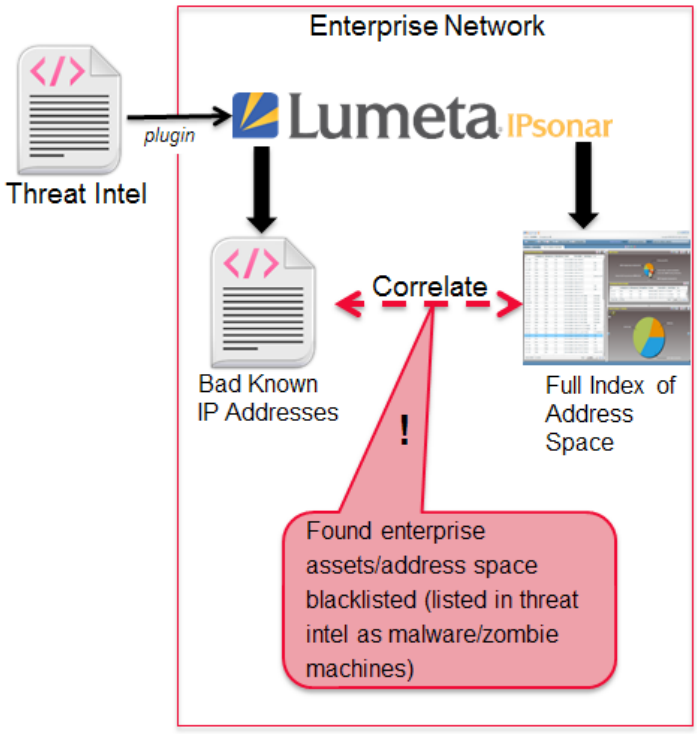
- TOR Exit Nodes – Determine whether or not there is connectivity from inside the network.

- Trojan or Malware Ports – Identify any internal network use of known malware infection signature ports, Trojan ports or other vulnerable ports.

[1] *Lumeta IPsonar version 6.1+. Clients with an active subscription or maintenance agreement can download the Cyber Threat Probe from Lumeta's support site.*

Zombie/Bot Hunting

Purpose: Determine whether or not any trusted/enterprise assets are malware infected infrastructure participating in a C2 botnet; or part of blacklists, Dropnets, Shadowserver or attacker lists.



How It Works:

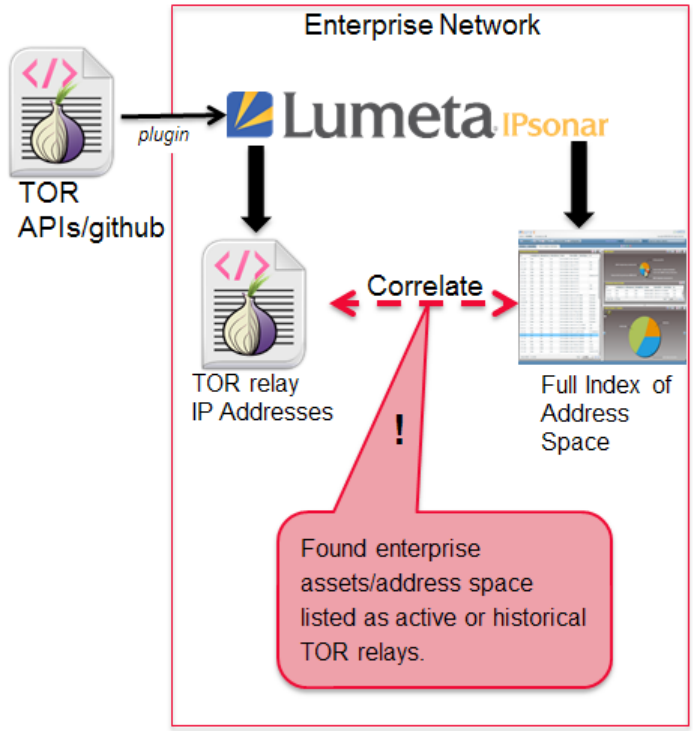
1. Parse open source and closed source intelligence feeds and repositories to enumerate known bad servers and networks (e.g., known to be participating in a zombie army), and associated attributes as available.

2. The Cyber Threat Probe correlates IPsonar's full index of the enterprise IP address space against known bad IP addresses from Step 1. CTP identifies devices on publicly routable addresses on your network (e.g., perhaps servers located in a DMZ or directly accessible via public IP addresses) that are also on the known bad IP address list.

3. Any IP addresses found on both lists are potentially compromised enterprise assets. CTP raises a flag regarding any machines that are blacklisted (listed in threat intelligence as malware/botnet machines).

Identification of Internal TOR Relays/Bridges

Purpose: Determine whether or not any trusted/enterprise assets are acting as current or past TOR relays/ bridges, potentially for nefarious purposes (botnet/zombie, malware).



How It Works:

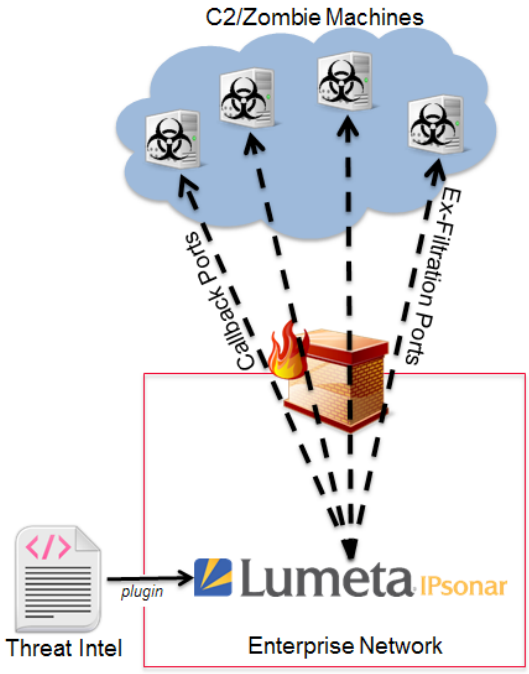
1. Parse/collect a list of current TOR relay/bridge nodes. Optionally, query the database of historical nodes.

2. The Cyber Threat Probe correlates IPsonar's full index of the enterprise IP address space against the IP address list from Step 1. CTP identifies devices on publicly routable addresses on your network that are also on the known TOR relay/bridge node list.

3. Any IP addresses found on both lists are enterprise assets that are listed as an active (or historical) TOR relay. CTP flags devices that are behaving as relays/ bridges.

Validation of No Access to Known Malware C2 Servers

Purpose: Determine whether or not active security controls prevent call back to known zombie/C2 networks and servers.



How It Works:

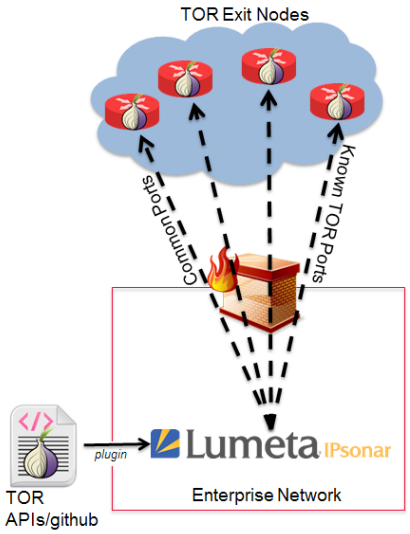
1. The Cyber Threat Probe ingests open source and closed source threat intelligence feeds and repositories; then parses them to enumerate known bad servers and networks and associated attributes as available.

2. IPsonar uses the intelligence parsed in Step 1 as the target list for a scan to assess whether it can reach known C2 botnets. It initiate a TCP based scan that uses Network Discovery, Host Discovery, and Service Discovery.

3. Perspective of the scan is from inside the network out to the targets.

Validation of No Access to Known TOR Exit Nodes

Purpose: Determine whether or not active security controls prevent call back to TOR exit nodes.



How It Works:

1. The Cyber Threat Probe ingests threat intelligence feeds and parses/collects a list of current TOR exit nodes.

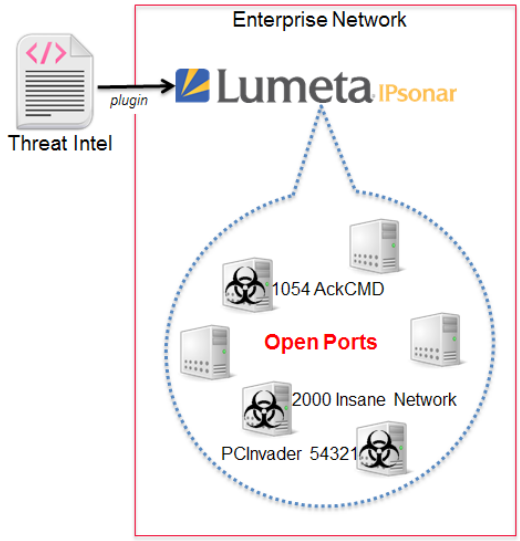
2. IPsonar initiates a TCP based scan that uses Network Discovery, Host Discovery, and Service Discovery. Targets for this scan are based on the intelligence parsed in Step 1. Ports attempted to connect with will contain known common ports and known TOR ports.

3. Perspective of the scan is from inside the network out to the targets.

Identification of Any Internal Use / Accessibility of Known Trojan or Malware Ports

Purpose: Determine if cyber controls are preventing malware call back, C2 channels, and data exfiltration.

- Malware Infection Signature Ports – Commonly used malware exploit ports which should be non-responsive but are actually responding
- Vulnerable Ports – Ports which should be non-responsive but are actually responding (e.g., prohibited ports which are often used for **lateral movement or exfiltration** like FTP, SSH, RDP, WMI, DISA Red Ports List)



How It Works:

1. Parse open source and closed source intelligence feeds and repositories to enumerate known bad ports and services.

2. Perform Service Discovery (ESI Port Discovery) scans internally using the port list generated in Step 1.

3. Report on ports that respond as open, closed or inconclusive. Open bad ports indicate possible malware is running on the system. Closed ports may indicate that steganography-based port knocking exists.