MUSTARD

NETWORK SECURITY

Stop Malware - before it calls home!

Detect silent, periodic check-ins signalling a compromised device.

24/7	≤1hr	0.95+	5-in-1
PASSIVE MONITORING	ALERT RESPONSE	BEACON CONFIDENCE	SECURITY ENGINES

THE PROBLEM

Your Antivirus Won't Catch This

Modern malware rarely announces itself. Instead, it installs silently, then reaches out to its operator via short, regular, encrypted messages — **beacons**. Once a live command channel is confirmed, attackers push further: lateral movement, data exfiltration, ransomware deployment.

Traditional defences inspect files and signatures. Beacons don't look like malware. They look like background traffic — which is exactly the point.

Ransomware Pre-staging

Operators verify access and map the network before encrypting — beacons are the first sign something is wrong.

Persistent Access Trojans

RATs check in every few minutes. Signature scanners see a normal process. Beacon analysis sees the pattern.

Stealthy Data Exfiltration

Small, consistent payloads sent at fixed intervals are invisible to volume-based anomaly detection.

Supply-chain Implants

Trusted software can be compromised. Even legitimate-looking traffic must be profiled for periodic behaviour.

THE SOLUTION

Behavioural Network Monitoring

BeaconButty routes between your LAN and the internet and tracks and scores every connection without any packets being blocked or delayed.

Rather than matching against known-bad signatures, it measures *behaviour*: connection regularity, consistent payload sizes, unusual destination profiles. These statistical patterns survive encryption and obfuscation.

Beacon Scoring

RITA v5 scores every host on periodicity, jitter, packet size consistency, and connection duration.

Intrusion Detection

Suricata IDS monitors signatures in parallel, covering exploit attempts and known malware.

Threat Intelligence

Destination geo-location, ASN reputation, Tor exit node detection, and domain entropy analysis.

Asset Inventory

Automatic LAN discovery via ARP, DHCP, and Nmap — OS detection and open-port visibility.

False Positive Control

A managed registry suppresses known-benign traffic, keeping alert volumes meaningful not noisy.

Instant Alerts

Slack notifications with configurable severity thresholds and suppression windows per alert type.

A Five-Layer Detection Pipeline

1 **Passive Packet Capture** `Zeek 8`

Zeek monitors all LAN traffic on the internal interface — passively, with zero impact on throughput. Every TCP/UDP connection is logged with full metadata: timestamps, bytes transferred, connection state, and duration.

2 **Beacon Scoring Engine** `RITA v5.1.1`

Hourly, RITA imports Zeek connection data and runs statistical analysis per (source IP → destination) pair. It scores each pair on four axes: connection periodicity, inter-arrival jitter, consistent byte size, and connection duration.

3 **High-Performance Storage** `ClickHouse`

Beacon scores, connection records, and alert history are stored in a columnar time-series database on NVMe SSD. Sub-millisecond queries across weeks of data allow the web dashboard to serve results instantly even on constrained hardware.

4 **Intrusion Detection Overlay** `Suricata IDS`

Suricata runs concurrently, applying thousands of community and commercial ruleset signatures against live traffic. Alerts are correlated back to the asset inventory via MAC address and IP, so you always know which device triggered which rule.

5 **Reporting, Alerting & Web Dashboard** `Flask · AWS Lambda · Slack API`

A Flask web application provides real-time visibility across all detection layers. A daily 07:00 report summarises top beaconing hosts. Slack alerts fire within minutes of a high-confidence detection — with configurable thresholds and suppression windows.

DETECTION COVERAGE

What BeaconButty Catches

Periodic C2 Beacons
Statistical jitter and periodicity scoring catches malware check-ins regardless of obfuscation.

Tor Exit Node Contacts
Connections to known Tor infrastructure are flagged immediately — a reliable indicator of compromise.

Threat Intel Hits
Destinations are checked against curated threat intelligence feeds. Known bad IPs and domains.

Exploit Attempts
Suricata rules cover active exploit sigs — CVE payloads, shellcode patterns, and protocol abuse.

Excessive DNS Queries
Hosts generating unusually high DNS query volumes — a common indicator of C2 location attempts.

New & Rogue Devices
New LAN devices trigger an immediate notification.

ALERT CRITERIA

Prioritised, Intelligent Alerting

HIGH PRIORITY

- Beacon score ≥ 0.95
- Persistent strobe traffic
- Threat intel match
- Tor exit node contact
- Suricata P1 rule
- Service down (Zeek / CH / Suricata)
- WAN unreachable
- Disk > 90% full

MEDIUM PRIORITY

- New device on LAN
- Health check failure
- Beacon score 0.80–0.94
- High DNS volume host
- Suricata P2/P3 alerts
- Firewall policy change
- Daily summary digest