BDATA
Innovating Security

# Realtime Malware Hunting and Response


BDATA Solution Inc

| WWW.BDATA.CA | Info@bdata.ca

# Table of Contents


1. Summary 2

2. Multilayer Cyber Security 2

3. What is malware hunting 3

4. Why do we need malware hunting and response 3

5. How malware hunting works on BIoT-enabled devices 3

6. Malware hunting and response using BIoT Mobile App/Platform 3

1. Conclusion 5

## 1. Summary

BDATA is a global cyber security service and technology provider that assists customers in achieving the highest level of cyber security for their OT infrastructure.

BIoT Security Technology has a lightweight multilayer cyber security solution which enables companies to achieve cyber security compliances concerning TSA, IECT 62443, ISO, NIST, HIPAA, and other local and international standards.

BIoT Security technology ensures complete autonomy and auditing of cyber security vulnerabilities, device log management, firewall management, and device immutable authentication without the need of 3rd party generated certificates, instead of using immutable device-based fingerprint authentication to ensure that every connected device with servers is authenticated.

At BDATA, we provide a cyber security solution based on Zero Trust & aligned with the security by design framework.

BDATA's scope of supply includes the following.

- BIoT Integration with Azure IoT Hub / AWS IoT Hub / Other clouds
- Device-based fingerprint authentication
- Realtime malware hunting

## 2. Multilayer Cyber Security

BIoT Security Technology is a lightweight multilayer cyber security that ensures the highest level of protection and 80% cost savings compared to other cyber security solutions, which includes all the primary layers of cyber security in the basic version, ensuring the following.

- Device-based authentication
- End–to–End Data Encryption (Security by design Virtual Private Network)
- Intrusion Detection
- Firewall Management
- Incident Response
- Malware hunting and response
- Endpoint Inventory Management
- Endpoint Log Monitoring
- Secure File Transfer

## 3. What is malware hunting?

Even though customers' cyber security programs are designed as multilayer to protect from advanced cyber-attacks, but still no system can be completely protected; that's why it's essential to consider the additional cyber defences on top of the existing cyber security layers, which enable the customer to monitor if there is malware file added in the system, so that response can be autonomously activated and such malware can be identified and remove in real-time.

## 4. Why do we need malware hunting and response?

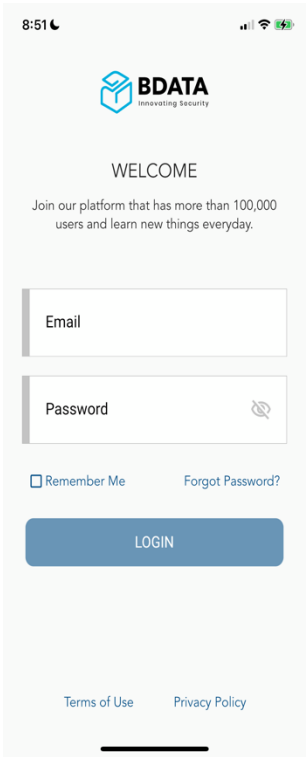
As per the world economic forum report published in Jan 2022, on average, it takes ten months for a customer to detect if there is any malware deployed on their network or not. Companies must implement real-time malware detection to stop cyber-attack or reduce damages.

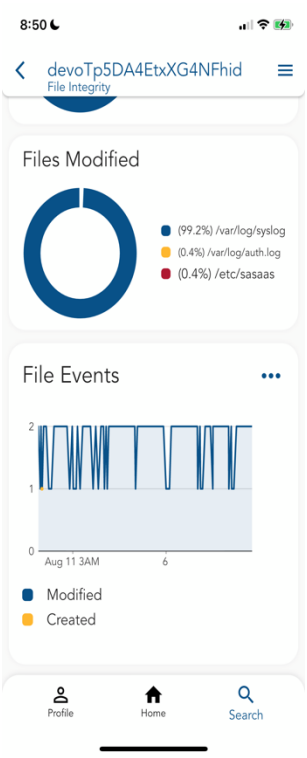
## 5. How malware hunting works on BIoT-enabled devices

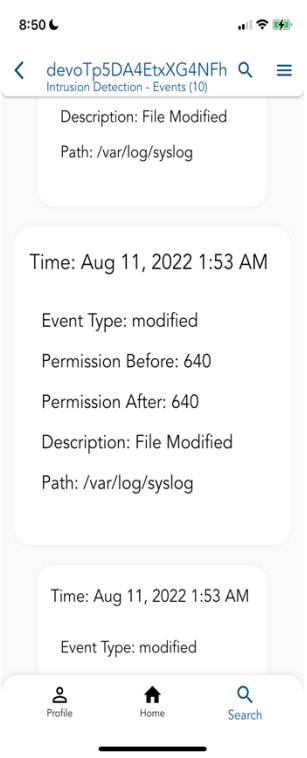
Malware hunting combines the methodology of file integrity and system integrity along with anomaly detection on the device to ensure a proactive and ever-evolving approach to detecting anomalies and strange patterns as well as in real-time monitor system folders to identify if there is any file added, deleted, or modified and various other indicators of compromise.

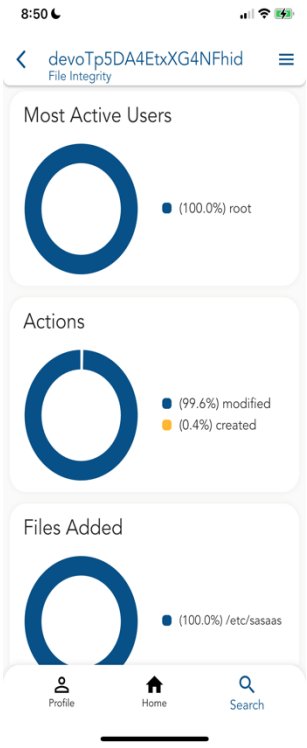
## 6. Malware hunting and response using BIoT Mobile App/Platform

BIoT Security Technology enables companies to monitor cyber security alerts in real-time on their mobile phones using BIoT Security technology, easy-to-use mobile apps for IOS and Android phones and tablets.

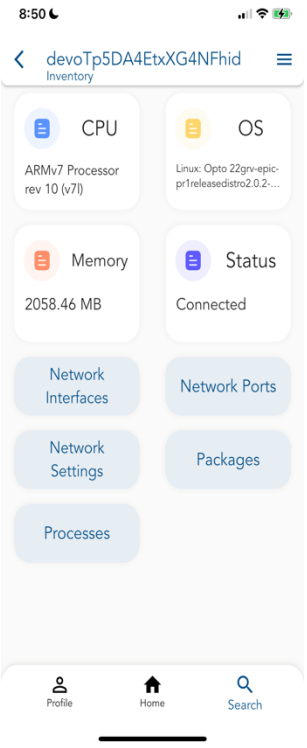

8:51
BDATA
Innovating Security
WELCOME
Join our platform that has more than 100,000 users and learn new things everyday.
Email
Password
Remember Me
Forgot Password?
LOGIN
Terms of Use
Privacy Policy

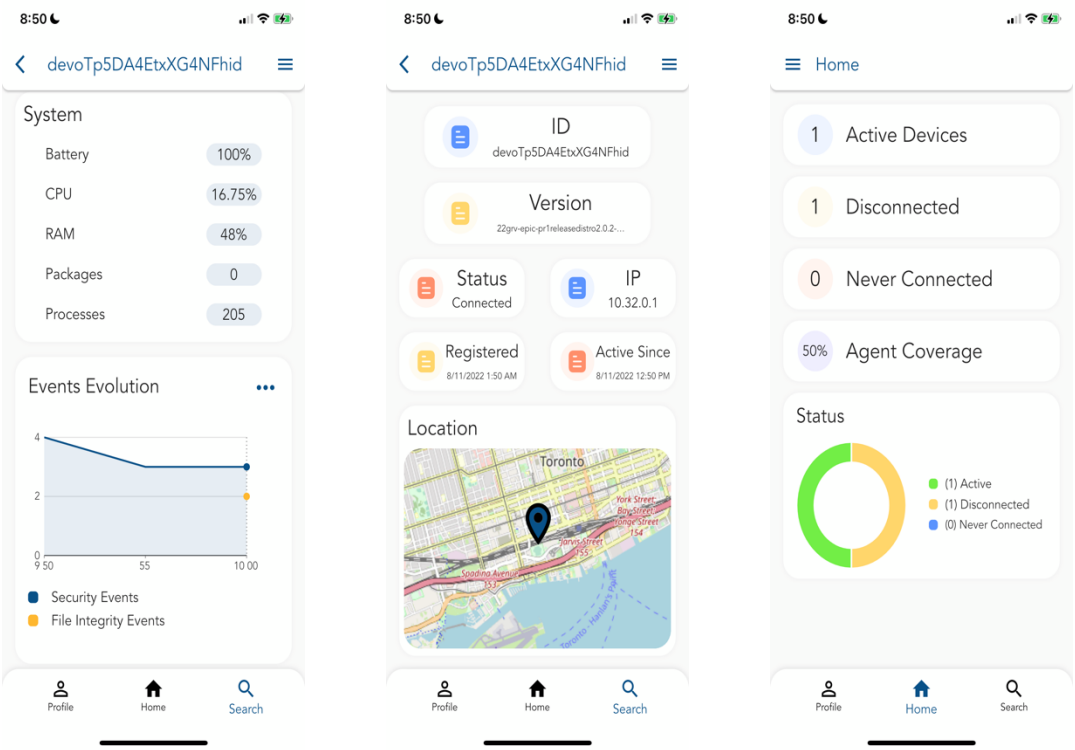

8:50
devoTp5DA4EtxXG4NFhid
File Integrity
Files Modified
(99.2%) /var/log/syslog
(0.4%) /var/log/auth.log
(0.4%) /etc/sasaas
File Events
2
1
0
Aug 11 3AM
6
Modified
Created
Profile
Home
Search


8:50
devoTp5DA4EtxXG4NFh
Intrusion Detection - Events (10)
Description: File Modified
Path: /var/log/syslog
Time: Aug 11, 2022 1:53 AM
Event Type: modified
Permission Before: 640
Permission After: 640
Description: File Modified
Path: /var/log/syslog
Time: Aug 11, 2022 1:53 AM
Event Type: modified
Profile
Home
Search


8:50
devoTp5DA4EtxXG4NFhid
File Integrity
Most Active Users
(100.0%) root
Actions
(99.6%) modified
(0.4%) created
Files Added
(100.0%) /etc/sasaas
Profile
Home
Search


8:50
devoTp5DA4EtxXG4NFh
Inventory - Processes (205)
Process: init
User: 000
Group: 000
PID: 1
Parent PID: 0
VM Size: 1761280
Command: init [5]
Arguments:
Process: kthreadd
User: 000
Group: 000
Profile
Home
Search


8:50
devoTp5DA4EtxXG4NFhid
Inventory
CPU
ARMv7 Processor rev 10 (v7l)
OS
Linux: Opto 22grv-epic-pr1releasedistro2.0.2-...
Memory
2058.46 MB
Status
Connected
Network Interfaces
Network Ports
Network Settings
Packages
Processes
Profile
Home
Search




## 1. Conclusion

Cyber-attacks are currently, on average, detected after ten months, which means that hacker is freely moving within the compromised network and stealing data, and credentials, and waiting for the right time to cease the entire network and demand for ransomware; that's why companies need to have malware hunting implemented in their system so that any ransomware deployed can be detected in real-time.

BIoT Security is a multilayer cyber security technology with malware hunting implemented as part of the proactive approach, which helps customers to detect malware deployment in real-time and initiate automated responses to delete the malware and secure the device's entire network.