THREAT WARRIOR

What ThreatWarrior Detects

Threat Vectors, Detection Methods, and Potential Impact if Attacks Go Undetected By Other Solutions

In today's rapidly evolving threat landscape, organizations must be proactive in securing their networks against an ever-growing array of Indicators of Compromise (IOCs) and potential security risks. Implementing a robust Extended Detection and Response (XDR) solution is crucial for Chief Information Security Officers (CISOs) and security practitioners striving to safeguard their organizations from advanced threats, such as beaconing, botnets, command-and-control (C2) traffic, DNS anomalies, lateral movement, ransomware, and zero-day exploits, among others.

With attackers employing increasingly sophisticated techniques and relentless persistence to infiltrate networks, exfiltrate valuable data, or wreak havoc, the importance of having an effective XDR solution to identify and mitigate these risks cannot be overstated. By investing in a comprehensive XDR solution, organizations can significantly enhance their security posture, empower their security teams, and ultimately protect their most critical assets.

Below is a list of IOCs and potential security risks that ThreatWarrior XDR excels at both detecting and equipping security teams to swiftly and effectively execute response activity. It is a representative - by no means exhaustive - list.

Each IOC / potential security risk is accompanied by a brief explanation of ThreatWarrior's detection approach, as well as the potential impact of having it go unnoticed in your network.

Security Issue Type: Indicators of Compromise (IOCs)		
Security Issue	**ThreatWarrior Detection**	**Impact If Undetected**
Beaconing	Periodic and regular communication patterns between an infected host and a C2 server - like Emotet, Trickbot, APT29 (CozyDuke, CozyBear), Cobalt Strike, Hancitor (Chanitor), and JhoneRAT - are identifiable by ThreatWarrior, as the platform delivers visibility into all communication across a network.	Beaconing may indicate botnet presence or other malicious activity.
Botnets	If machines on the network are participating as part of a botnet, ThreatWarrior will discover this unusual traffic. It will see new, anomalous traffic patterns emerge as the botnet communicates with its owner and wreaks havoc, inside or outside your network.	Botnets can be the agents of Distributed Denial of Service (DDoS) attacks, spam campaigns, malware distribution, click fraud, and unauthorized access to systems.
Command-and-Control (C2) Traffic	ThreatWarrior would see unusual external communication from C2 agents on impacted devices, as well as have opportunities to perform deep packet inspection and match that traffic against signatures of C2 systems known to the threat intel community.	Evidence of attacker control of compromised systems and coordinated attacks.
DNS Anomalies	ThreatWarrior can detect a range of DNS anomalies, each with its own impact potential: 1. Unusual query patterns: A sudden increase in the volume of DNS queries or a large number of queries to rarely accessed or suspicious domains 2. DNS tunneling: Attackers use DNS tunneling to hide malicious traffic within DNS queries and responses 3. Domain Generation Algorithms (DGAs): Generation of a large number of random-looking domain names 4. Connection to known malicious domains 5. Fast Flux: Unusual patterns of frequent changes in DNS records. 6. Non-standard DNS traffic: Use of non-standard ports for DNS queries or responses, or the presence of unexpected or malformed DNS packets.	1. Possible indication that a device is infected with malware or involved in a cyberattack 2. Used for data exfiltration, C2 communications, or security control bypass 3. Attacker trying to make it difficult for security tools to block C2 operations 4. A device is compromised or trying to connect to a C2 server 5. Attacker may be trying to hide the true location of their infrastructure 6. Possible attempt to evade detection or exploit DNS protocol vulnerabilities

Security Issue Type: Indicators of Compromise (IOCs)		
Security Issue	**ThreatWarrior Detection**	**Impact If Undetected**
Encryption and Tunneling	ThreatWarrior would detect the use of non-standard encryption or tunneling protocols.	Data exfiltration, C2 communication, evasion of security monitoring, and unauthorized access. These risks arise when attackers use encrypted channels or tunneling to hide malicious activities, bypass security controls, or maintain stealthy control over compromised systems.
Lateral Movement	ThreatWarrior delivers complete visibility into all network activity and will identify attempts to access multiple systems, unusual authentication events, or privilege escalation.	Potential unauthorized access to multiple systems, data exfiltration, privilege escalation, and persistent network compromise.
Malware	Due to its use of multiple engines, ThreatWarrior can identify malware activity in numerous ways. It can observe the IP addresses of known malware servers and identify those risks, use threat information on data signatures to identify threats and anomalous behavior, recognize differences in normal machine communication, detect abnormal server connections, and more. Our use of unsupervised neural networks enables users to identify even novel or signatureless malware.	It depends on the malware, but could lead to privilege escalation, lateral movement, persistence, data exfiltration, malware deployment, C2 communication, tampering with system logs, disabling security tools, exploiting additional vulnerabilities, sabotage or disruption.
Misconfigured ACLs	ThreatWarrior helps security analysts spot misconfigured ACLs by providing comprehensive visibility into actual network boundaries.	Misconfigured Access Control Lists (ACLs) open the door for unauthorized access, data leakage, privilege escalation, and insider threats.
New Connections	If ThreatWarrior observes new devices added to the network, it will recognize these as abnormal and escalate for review. Additionally, ThreatWarrior will identify any new virtual connections such as virtual machines, security groups, compute instances and more.	New connections can present security risks such as unauthorized access, malware propagation, data exfiltration, and exposure to potentially compromised devices.

Security Issue Type: Indicators of Compromise (IOCs)		
Security Issue	**ThreatWarrior Detection**	**Impact If Undetected**
Policy Breaks	ThreatWarrior allows administrators to define compliance/policy rules. For example, a company may have a policy that restricts employees from using Dropbox. Dropbox is a widely used, legitimate service that would pass an engine test, unless specified otherwise. Additionally, if Dropbox was being utilized when ThreatWarrior was installed, it would view the use of Dropbox as normal behavior. By providing the compliance engine with information about Dropbox, it becomes possible for the administrator to set alerts when the use of Dropbox is observed on the network.	Rule/protocol breaks can result in unauthorized access, data leakage, network disruptions, and exploitation of vulnerabilities.
Port Scanning	Port scans will appear to ThreatWarrior as anomalies where a familiar machine makes unusual connections on unusual ports to other familiar machines.	Attacker use of port scans can lead to detection evasion, brute-force attacks, service disruption, vulnerability exploitation, and reconnaissance for advanced attacks.
Protocol Anomalies	ThreatWarrior alerts on unusual or non-standard uses of network protocols. Unauthorized communication, visits to blacklisted websites, or other activity outside of business-defined protocols will be detected by ThreatWarrior.	Possible indication of unauthorized access, data leakage, malware distribution, or exploitation of vulnerabilities. Deviations from established communication protocols typically indicate attempts to bypass security measures, exploit software weaknesses, or engage in malicious activities.

ThreatWarrior XDR delivers:

FASTER THREAT DETECTION

FASTER THREAT INVESTIGATION

FASTER THREAT RESOLUTION

Security Issue Type: Indicators of Compromise (IOCs)		
Security Issue	**ThreatWarrior Detection**	**Impact If Undetected**
Public IP Communicating with Private IP Over Port 445	ThreatWarrior detects public IP addresses communicating over port 445 with private IP addresses. Port 445 is used for the Server Message Block (SMB) protocol, a network file sharing protocol that allows applications to read and write to files and request services from server programs on a network. SMB is primarily used for providing shared access to files, printers, and other network resources within local networks and, in some cases, over the internet. ThreatWarrior's deep packet protocol engine can classify traffic on a protocol basis and then determine if traffic behavior appears anomalous. As an example, certain traffic types should always be encrypted end-to-end, regardless of whether transported over an internal or external network. Discovering unencrypted traffic, in this case, will trigger an alert.	Unauthorized access, malware propagation, and potential exploitation of vulnerabilities. These risks arise from the exposure of the SMB protocol - commonly used for file sharing and network services - making it a target for attackers seeking to compromise systems or spread malware like ransomware.
Ransomware	ThreatWarrior detects ransomware through unusual connections to familiar machines, unusual connections from familiar machines, or unusual traffic patterns as the infection spreads. ThreatWarrior can also detect privilege escalation, IP scans, and data exfiltration as ransomware gangs attempt to steal your data.	Ransomware can result in operational disruption, financial loss, data loss, reputation damage, legal and regulatory consequences, supply chain disruptions, and even loss of competitive advantage.
Suspicious or Unauthorized File Transfers	ThreatWarrior can observe atypical data connections, or connections using network protocols and addresses that are suspicious. Unusually large data transfers or transfers during suspicious time frames will cause an alert.	Suspicious or unauthorized file transfers can be the root of data exfiltration, malware distribution, C2 communication, insider threats, loss of confidentiality, intellectual property theft, as well as legal and regulatory risks.

Security Issue Type: Indicators of Compromise (IOCs)		
Security Issue	**ThreatWarrior Detection**	**Impact If Undetected**
Unauthorized Data Access	ThreatWarrior will observe entities talking to each other in atypical ways. For example, if a machine on the network reaches out and connects to a database server when it has never done so before, it will be identified as a possible threat, requiring further review. This could be customized to allow for threat warnings based on connections that originated outside of the local network, or for machines not on a whitelist the user can create.	Unauthorized data access can result in data breaches, loss of privacy, financial loss, legal and regulatory penalties, reputation damage, loss of intellectual property, disruption of operations and increased security costs.
Unauthorized Port Scans	ThreatWarrior can identify unauthorized scans from inside or outside the network.	Unauthorized port scans can underpin reconnaissance, detection evasion, and targeted attacks.
Unusual Traffic Patterns	ThreatWarrior can detect unexpected spikes in network traffic, repeated connections to suspicious IP addresses, or unusual data transfers.	Possible indicators of data exfiltration, malware distribution, C2 communications, and reconnaissance for advanced attacks.
Zero-day Exploits	Zero-day refers to a previously unknown vulnerability in software, hardware, or firmware that hasn't been publicly disclosed or patched by the vendor. ThreatWarrior leverages unsupervised neural networks to self-learn normal behavior patterns, requiring no prior knowledge of a threat to determine its anomalous behavior. The system can raise alerts to zero-day exploits without being trained on vulnerability fingerprints.	The potential impact depends on the exploit design, but it could lead to anything along the lines of privilege escalation, lateral movement, persistence, data exfiltration,

Security Issue Type: Potential Security Risk		
Security Issue	**ThreatWarrior Detection**	**Impact If Undetected**
Bitcoin Mining	Bitcoin mining generates telltale traffic patterns as machines communicate with command and control systems, and the peer-to-peer blockchain network. ThreatWarrior would observe the frequent, unusual connections to unusual destinations, and notify security teams of possible Bitcoin mining.	Bitcoin mining can lead to productivity loss and unauthorized resource consumption. It can also be the harbinger of malware infection, compliance and legal risk, network security vulnerabilities, and insider threats.
Improperly Decommissioned Devices	ThreatWarrior utilizes a custom rules engine that simplifies the tracking and recording of data transfers. This enabled a managed IT provider to identify that transfers were happening and in one case that it was done outside of the requirements that the organization, its CEO, and its stakeholders set in place for the data transfer. The custom rules engine provides a method to verify data integrity processes that speeds up the work of acknowledging, investigating, resolving, and containing unauthorized data transfers from any device - improperly decommissioned or otherwise.	Improperly decommissioned devices pose security risks such as data leakage, unauthorized access, and potential malware infection.
Peer-to-Peer Networks	Like Bitcoin or TOR, ThreatWarrior will detect other unauthorized peer-to-peer networks as familiar machines connecting to unfamiliar machines with unusual ports and protocols.	Unauthorized P2P networks open the door for malware distribution, exposure of sensitive data, network vulnerabilities, legal risk, unwarranted resource consumption, privacy risk, and compromised file integrity/trust.
Phishing Attacks	Not all insider attacks are carried out by nefarious insiders. Some happen through unaware insiders who are victims of phishing. Should a user be socially engineered into opening an attachment or clicking a link and inadvertently installing malware on their machine, the behavior of the machine will change as the malware begins to operate. ThreatWarrior will detect these changes – connections to non-typical servers, scanning for other machines, etc. – and raise alerts.	Undetected phishing attacks can result in credential theft, financial loss, data breaches, malware infection, business disruption (through ransomware) or espionage.

Security Issue Type: Potential Security Risk		
Security Issue	**ThreatWarrior Detection**	**Impact If Undetected**
TOR Network	If a machine on the network is communicating with The Onion Router (TOR), ThreatWarrior will observe connections to unusual machines over unusual ports. If it is acting as a TOR relay, it will also observe unusually large amounts of chatter to unusual machines.	Unchecked TOR communications can lead to malicious exit nodes, compromised anonymity, access to illegal content, or association with criminal activity.

Summary

ThreatWarrior's XDR solution provides unparalleled security by leveraging advanced machine learning techniques, unsupervised neural networks, and cutting-edge cyber defense strategies to automatically identify true signals across network, endpoint and identity data.

ThreatWarrior consistently outperforms traditional solutions in identifying legitimate threats. It not only detects ongoing threats that other solutions miss, but also uncovers past exploits that have gone unnoticed. Its comprehensive approach to monitoring network traffic, both north-to-south and east-to-west, enables a more accurate understanding of each client's network, behavioral patterns, and usage characteristics.

At a time when adversaries are proliferating, becoming more skilled, stealthier, and able to leverage artificial intelligence against you, ThreatWarrior XDR adds a sophisticated layer of threat detection and response that tips the scales back in your favor.

About ThreatWarrior

ThreatWarrior is a global leader in cybersecurity solutions, offering innovative threat detection and response solutions to help organizations protect critical data and infrastructure. Powered by deep learning and neural network technology, ThreatWarrior NDR and ThreatWarrior XDR integrate appropriate network, endpoint, and identity data with advanced threat intelligence to deliver real-time detection and response, threat hunting, and a prioritized view of vulnerabilities. Either solution extends threat detection and response across your IT/OT infrastructure to eliminate blind spots, find indicators of compromise, and stop in-progress threats before they disrupt your business.

THREAT WARRIOR

info@threatwarrior.com

threatwarrior.com

844.463.9440