NETSCOUT Threat Vault

Mike McNerney
sr. Director Product Management – Threat Intelligence
Why is NETSCOUT Threat Vault Important?

1. Increase and promote NETSCOUT’s credibility and brand recognition in the eco-system.

2. Organize our Threat Intel assets for external consumption.

3. Monetize our intelligence capabilities beyond what’s directly relevant for our products.
NETSCOUT Threat Vault

IoCs
Contextual Details
Integration Consulting
Threat Landscape Consulting
NETSCOUT Threat Vault

Coverage

**Reputation**
- Indicator based
- Policy oriented
- Network focused IPs, Domains, URLs, MD5s, Mutex, Register Key, etc.

**Context**
Rich contextual information derived from wide range of data sources available via API

- Dynamic Updates for Accurate, Timely Protection
- Threat Validity and Prioritization

**Industry standard formats (STIX, CSV, etc.) for easy integration**

- Attack Infrastructure and Methods
- Gauge Risks
- Prioritize Security Operation Tasks
- Take Proactive Measure with Confidence
# NETSCOUT Threat Vault

## Coverage

### Threat Indicator Categories

<table>
<thead>
<tr>
<th>Location-Based Threats</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Traffic Anonymization Services</td>
<td></td>
</tr>
<tr>
<td>• TOR</td>
<td></td>
</tr>
<tr>
<td>• Proxies</td>
<td></td>
</tr>
<tr>
<td>• Sinkholes</td>
<td></td>
</tr>
<tr>
<td>• Scanners</td>
<td></td>
</tr>
<tr>
<td>• Others</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email Threats</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Spam</td>
<td></td>
</tr>
<tr>
<td>• Phishing</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Targeted Attacks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• APT</td>
<td></td>
</tr>
<tr>
<td>• Hactivism</td>
<td></td>
</tr>
<tr>
<td>• RAT</td>
<td></td>
</tr>
<tr>
<td>• Watering Hole</td>
<td></td>
</tr>
<tr>
<td>• Rootkits</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mobile</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mobile C&amp;C</td>
<td></td>
</tr>
<tr>
<td>• Spyware</td>
<td></td>
</tr>
<tr>
<td>• Malicious Apps</td>
<td></td>
</tr>
</tbody>
</table>

### Malware Coverage

<table>
<thead>
<tr>
<th>Malware</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Webshell</td>
<td></td>
</tr>
<tr>
<td>• Ransomware</td>
<td></td>
</tr>
<tr>
<td>• Fake Anti Virus</td>
<td></td>
</tr>
<tr>
<td>• Banking</td>
<td></td>
</tr>
<tr>
<td>• Cryptocurrency</td>
<td></td>
</tr>
<tr>
<td>• Social Network</td>
<td></td>
</tr>
<tr>
<td>• DDoS Bot</td>
<td></td>
</tr>
<tr>
<td>• Dropper</td>
<td></td>
</tr>
<tr>
<td>• Ad Fraud</td>
<td></td>
</tr>
<tr>
<td>• Worm</td>
<td></td>
</tr>
<tr>
<td>• Credential Theft</td>
<td></td>
</tr>
<tr>
<td>• Backdoor</td>
<td></td>
</tr>
<tr>
<td>• Point of Sale</td>
<td></td>
</tr>
<tr>
<td>• Others</td>
<td></td>
</tr>
</tbody>
</table>
## NETSCOUT Threat Vault

### Use Cases

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Enterprises</th>
<th>Service Providers / MSSPs</th>
<th>Gov. Agencies</th>
<th>CERTs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Intel. Operationalization – Integrate into 3rd Party Security Solutions</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Research</td>
<td>Investigation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Increase MSSP Service Effectiveness &amp; Accuracy</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infected Traffic Blocking</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Operation and Research focused offering**
NETSCOUT Threat Vault

Key Value Differentiators

High Fidelity

Contextual Rich
Proof – IoCs in NTV

Highly selective and unique IoCs for optimal edge protection

Curated: 100%
Unique: >80%
NETSCOUT Threat Intelligence
What Makes Up ATLAS Intelligence?
Impactful Threat Intelligence

Impactful Intelligence = Dedicated Expertise + Global Collections + Rigorous Process
People

ATLAS Security Engineering & Response Team (ASERT)

Industry renowned elite security research group

Key influencers of NETSCOUT Security Solution

Collection and analysis of malware at the scale of Internet for over a decade

Collaborate with hundreds of CERTs and government agencies

Focus. Expertise. Dedication
Collections
Unparalleled Data Collection

Botnet Monitoring System
Monitoring and tracking 50+ botnets activities

Product Feedback Data
- 350+ Sightline deployments worldwide
- 200+ APS / AED deployments worldwide
- Attack information, malware matches, etc.

Sinkhole
Maintain 5000+ domains. Over 100+ malware families check in from all over the world

Scanner
Operate a full 10Gbps scanner, capable of scanning the entire IPv4 address space in minutes

Public Data Sources
High quality public data source

Private Intel. Partners
20+ malware sharing partners

Commercial Intel. Feeds
Complementary commercial threat intelligence feeds

Darknet Forum Monitoring
Partnership with Underground Forum/Darknet monitoring organizations

Honeypot
IoT Honeypots deployed around the world capturing exploitation attempts, brute-force botnet propagation, and DDoS attacks.

Private Intel. Partners
20+ malware sharing partners

Commercial Intel. Feeds
Complementary commercial threat intelligence feeds

Darknet Forum Monitoring
Partnership with Underground Forum/Darknet monitoring organizations

Honeypot
IoT Honeypots deployed around the world capturing exploitation attempts, brute-force botnet propagation, and DDoS attacks.

Scanner
Operate a full 10Gbps scanner, capable of scanning the entire IPv4 address space in minutes
Process

Enrichment
- Geo-location
- NAIC
- ASN

mCorral Engine
- Deep Behavioral Analysis
- Recursive Introspection & Extraction

Validation
- Age. Severity
- Blacklist. Whitelist
- Reputation. Sinkhole. Abuse

10+ year malware analysis expertise. 200,000+ malware samples processed daily
ATLAS Intelligence - Differentiation

Industry renowned elite security research group

Unparalleled data collections

Deep Behavioral Analysis

Recursive Introspection / Extraction

Accurate & effective scoring

People. Collection. Process
Thank You.

Mike.McNerney@netscout.com

www.netscout.com