Anomali Mobile Threat Defense

Mobile Specific Malware Intelligence

Implementing a Bring Your Own Device (BYOD) policy can be a double-edged sword for your organization. While it can provide numerous benefits, it also increases the attack surface area for malware, making it more challenging to maintain a secure environment. The proliferation of personal devices in the workplace creates new, previously unseen actions that attackers can exploit to infiltrate systems, putting your organization's sensitive data and operations at risk. As such, your organization must have Malware intelligence specific to mobile operating systems to scan against those installed malicious applications.

Anomali's Mobile Threat Defense Intelligence Channel is here to help.

This Intelligence Channel provides a real-time, global, curated feed of observables that have been sandboxed to understand the context and to ensure they specifically relate to mobile operating systemslike Android and iOS.

This channel is excellent for organizations that have policies like Bring Your Own Device (BYOD) or tools like Mobile Device Management (MDM) in place. Using the intelligence from this channel in combination with MDM will allow the automated scanning of installed applications against the observables in the channel to alert the security team if malicious or vulnerable applications are installed on these devices.

This Intelligence Channel is powered by PolySwarm, whose incentive-based marketplace enlists an extensive global network of technologies from expert malware researchers and anti-virus engines to continuously source and accurately grade the very latest malware intelligence. Anomali's Threat Research team then curate the intelligence provided.

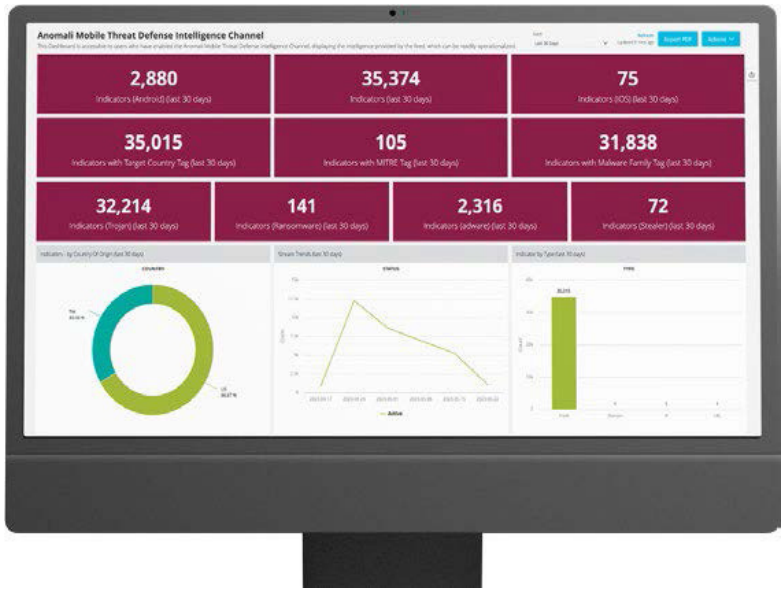
Thanks to this partnership, Anomali can provide its customers with world-class, constantly up-to-date malware intelligence at a fraction of the cost of purchasing feeds from other providers.

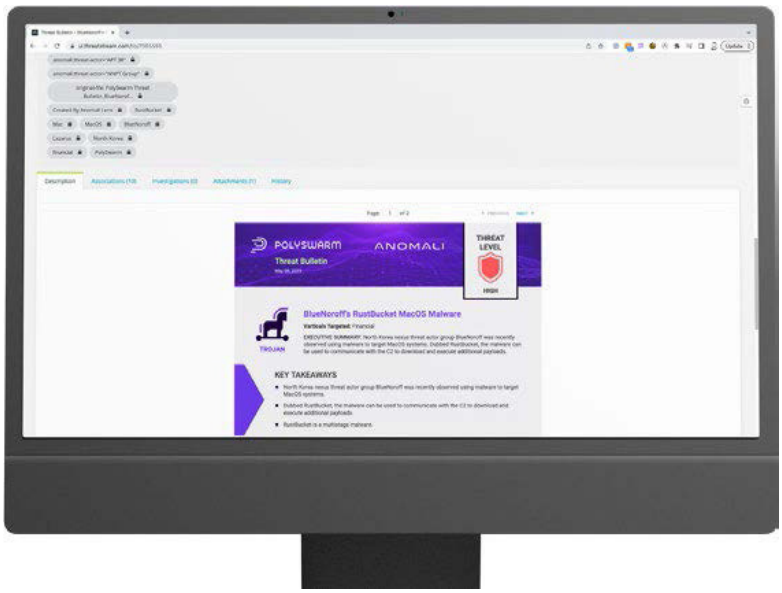
KEY BUSINESS VALUE

- Increased visibility and early warning of targeted mobile threats
- Increased brand protection of consumer-facing mobile applications
- Reduce exposure to potential breaches from employee mobile devices
- Increased productivity of Threat Intelligence and SOC Teams
- Streamline CTI team workflows

KEY CHANNEL BENEFITS

- Global malware and ransomware coverage, all of which is sandboxed
- Complimentary to Anomali Malware Intelligence Channel
- Detailed C2 information
- Extensive tagging for effective automation and team analysis
- Unified Malware naming
- Integrated Risk Scoring directly in Threatstream
- Mitre TTP support
- Detailed ThreatStream
- Dashboard to quickly operationalise indicators
- Enriched Observables with further information





PREMIUM MALWARE THREAT REPORTS

- Mobile Malware Premium Threat Reports
  - Provides Associated Mitre TTP's
  - Threat Level indicators (e.g. Low, High)
  - Type of Report (e.g. Situational Awareness, Campaign)
- Insight into new mobile APT campaigns and trending threat families
- Gain valuable insights and context that are actionable
- Uncover specific industry and geography-related issues
- Published 2-3x per week

Key Use Cases

CTI/SOC Automation

Extensive tagging and scoring provide an easy way to collect and disseminate intelligence downstream

Threat Hunting

Intelligence on mobile specific malware and ransomware

Telemetry enrichment

Comprehensive tagging and C2 information

Incident Response

Mitre TTP details, with associated IOCs for automated dissemination

Vulnerability management prioritization

CVE information and numeric threat scoring

ANOMALI