Core Threat Intelligence:

Actionable Adversary Focused Threat Intelligence

Improvements in incidents response:

- 28% see better context, accuracy and/or speed in monitoring & incident handling
- 63% note Threat Intelligence improved visibliity into attack methods
- 51% see faster and more accurate detection and response
- 48% cite reduction in incidents through early prevention due to Threat Intelligence

750 MILLION DEVICES OBSERVED

1.2 TRILLION DNS QUERIES / DAY

13.8 BILLION DOMAINS CATALOGUED

Introduction

Core's Threat Intelligence, an 'Adversary Focused' threat intelligence service, enumerates the Internet destinations used by individual threat actors and malware families covering:

- APTs
- Nation-state Actors
- Cyber Espionage
- Ransomware
- RATS
- Banking Trojans & Financial Fraud
- Information Stealers
- Spam, DDoS, Clickfraud, and Adware

Core's Threat Intelligence details the complex relationships between threat actors, their command and control network infrastructure, and the malware samples they use and includes detailed threat research reports on the intent of the threat actor and their historical intentions

Take Back Control Of You Network

Actively Block Malicious Command & Control

Sever the kill chain by using Core's Threat Intelligence to block communications to known command and control servers.

Identify Infections Communicating with Adversaries

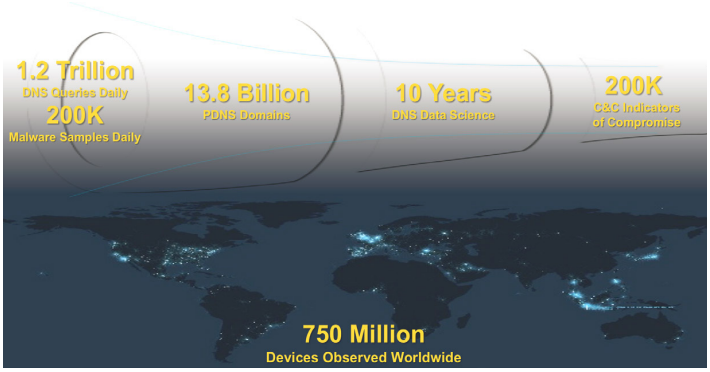
Pinpoint infections with confidence that have evaded your traditional defenses by matching network activity with Core's Threat Intelligence.

Provide Context to Active Incidents

Stop the guess work and use Core's Threat Research reports to provide context to the intent of your adversaries.

Turning Data Into Intellgence

As threats adapt and grow, Core's threat researchers and machine learning experts use data science to identify and track adversaries and their command and control networks. Unlike other threat intelligence vendors that rely on aggregating intelligence from hundreds of researchers manually investigating malware, Core's Threat Discovery Center automatically harvests raw global DNS and malware communication data, extracting relationships and utilizing predictive security analytics to produce threat intelligence that shows the complex relationship between malware and command and control for threat actors and malware families.



How Core Threat Intelligence Is Delivered

Core's Threat Intelligence is dynamically generated and updated multiple times a day. Subscribing to the Core Threat Intelligence service allows customers to easily import the JSON structured threat intelligence feed into their:

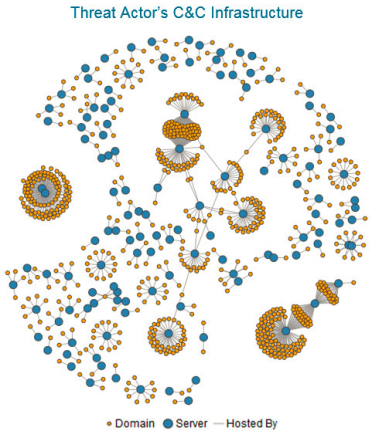
- Threat Intelligence Platforms
- SIEMS and Log Aggregators
- In-house threat intelligence data repositories
- In-line blocking solutions such as NGFW, Web Proxies, and IPS

Core's Threat Intelligence is sold as an annual subscription.

Enhancement Offerings

Combine Core's Threat Intelligence offering with Core's Passive DNS that maps the current and historical activity of domains and IPs on the Internet, Core's Passive DNS (PDNS) provides Incident Response, Fraud, and Security Operation Center teams the richest source of contextual, factual DNS activity data to investigate, mitigate, and protect against cyber threats. Core's PDNS database is the industry's largest, mapping 13.8 Billion domains to IPs with over 1.2 Trillion DNS queries observed a day from over ¾ Billion devices. Armed with facts on the activity of malicious actors, security professionals can:

- Identify when a domain or IP has become malicious
- Correlate with threat intelligence to provide context to a security event
- Enumerate fast flux C&C infrastructure
- Classify entire IP blocks to be treated as malicious
- Track threat actors as they change their infrastructure
- Spot patterns in operators / actors using shared infrastructure and hosting
- Estimate volumes of victims, rate of growth, and if a domain is still active C&C
- Discover specific malicious activity, especially for malicious use of dynamic DNS providers' infrastructure
- Investigate fraudulent use of corporate branding



Core's Threat Intelligence keeps a continuous mapping of malicious actors' infrastructure

ABOUT CORE SECURITY

Core Security provides market-leading, threat-aware, identity, access and vulnerability management solutions that provide actionable intelligence and context needed to manage security risks across the enterprise. Solutions include multi-factor authentication, provisioning, Identity Governance and Administration (IGA), Identity and Access Intelligence (IAI), and Vulnerability Management (VM). The combination of these solutions provides context and shared intelligence through analytics, giving customers a more comprehensive view of their security posture so they can make better security remediation decisions and maintain compliance

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

blog.coresecurity.com | p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

CORE SECURITY