Anomali Intelligence Channels
Anomali Phishing and Fraud powered by Bayse

Security Teams can only be as effective as what they know is threatening their organisation. At a strategic level they need to understand the adversaries, malwares and campaigns targeting their regions and industries. They need to understand the likely anatomy of attacks and threats so they can proactively protect and prepare. At a tactical level they need to keep their frontline security controls up to date with blocking and detecting relevant IOCs so they can move swiftly and decisively against any actualized threat. They need to move with precision, velocity and impact to disrupt adversaries and their attacks, eliminating or minimising harm and assuring the secure and reliable operation of their business in the face of ever evolving cyber threats. From zero days to new malware to campaigns, phishing, fraud and attacks the best security teams are threat led security operations.

Anomali Intelligence Channels have been designed specifically around the key threat topics and domains faced by organisations. Anomali's Threat Research team have partnered with leading providers of this specialised intelligence ensuring high fidelity, low false positives and timeliness. The enriched taxonomy provided maximises its utility for strategic and tactical operational purposes – making sure you can trust and operationalize it where it counts, when it counts. The feeds stand in their own right but are also designed to work in conjunction with each other, increasing insight and amplifying impact and value for security teams.

BENEFITS AND BUSINESS VALUE

- Hone your security posture and preparedness to the next level in line with relevant adversaries, malwares, vulnerability exploits and attack methods.
- Increased visibility and early warning of threats targeting you.
- Increased productivity and reduced stress/burnout for threat intelligence and security teams.
- Increased return on security investment (RoSI) from your security front line protections and SIEM/SOAR security operations tier.
- Streamline workflows and playbooks for strategic and tactical intelligence – keeping pace with trends and ahead of threats.

The Threat from Phishing and Fraud

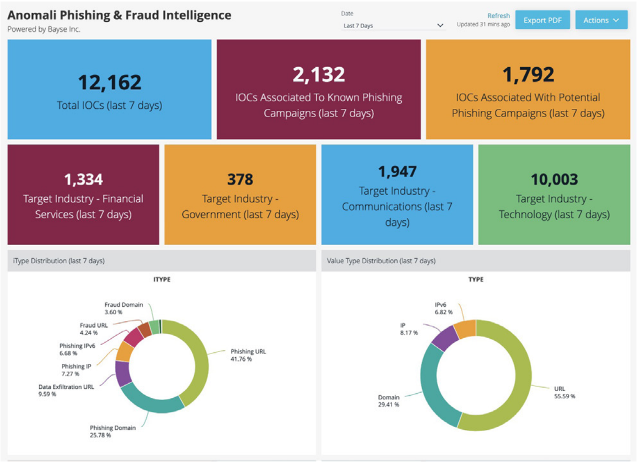
Phishing and Fraud are one of the most common sources of harm for organisations. It can be directed at employees to encourage click throughs and attachments to deploy infostealers, ransomware or other malware, or to specifically target business processes to commit fraud and criminality. It can directly impersonate your brand in order to cause harm to your customers or supply chain partners. Either way, staying on top of this threat is fundamental to securing your business, reputation, customers and employees alike.

The problem defenders face is the scope, scale and pace at which phishing and fraud is able to morph and adapt to try and stay a step ahead of protection and detection.

Key Capabilities

Through its rich analysis and taxonomy the Anomali Phishing and Fraud Intelligence Channel powered by Bayse provides comprehensive phishing & fraud indicators with key contextual information allowing customers to protect, detect & respond:

- Track ongoing phishing campaigns targeting one or more brands - these could be your own brands or those of key parts of your supply chain
- Track ongoing phishing campaigns related to organisations from a specific industry (e.g. Finance) - track what's going on in your own industry
- Identifies and tracks common phishing templates used across multiple attacks
- Over 90% of the phishing/fraud IOCs have the name of brand they are impersonating
- Over 90% of the IOCs have Industry of the specific brand they are impersonating
- IOCs for related exfiltration activity after successful phishing attempt
- Identifies primary purpose of phishing attack (e.g. credential stealing)
- SSL certificate info of phishing URL - cluster phishing by certificate issuer for tracking



Anomali Phishing & Fraud Intelligence
Powered by Bayse Inc.

Date: Last 7 Days

Refresh
Updated 31 mins ago

12,162
Total IOCs (last 7 days)

2,132
IOCs Associated To Known Phishing Campaigns (last 7 days)

1,792
IOCs Associated With Potential Phishing Campaigns (last 7 days)

1,334
Target Industry - Financial Services (last 7 days)

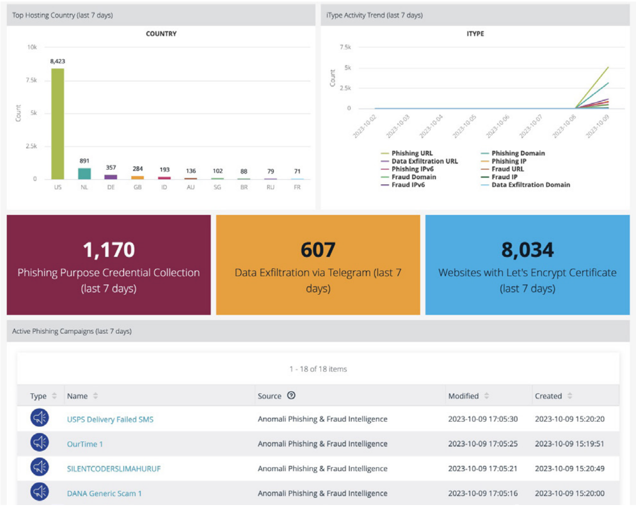
378
Target Industry - Government (last 7 days)

1,947
Target Industry - Communications (last 7 days)

10,003
Target Industry - Technology (last 7 days)

iType Distribution (last 7 days)

Value Type Distribution (last 7 days)



Top Hosting Country (last 7 days)

iType Activity Trend (last 7 days)

1,170
Phishing Purpose Credential Collection (last 7 days)

607
Data Exfiltration via Telegram (last 7 days)

8,034
Websites with Let's Encrypt Certificate (last 7 days)

Active Phishing Campaigns (last 7 days)

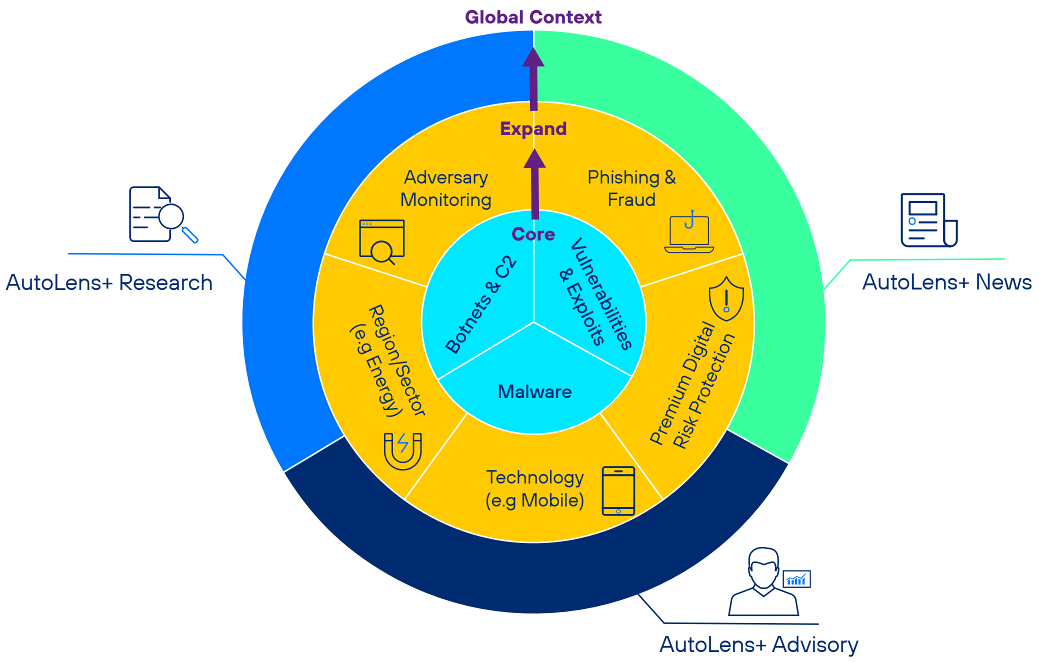
1 - 18 of 18 items

Type	Name	Source	Modified	Created
	USPS Delivery Failed SMS	Anomali Phishing & Fraud Intelligence	2023-10-09 17:05:30	2023-10-09 15:20:20
	OurTime 1	Anomali Phishing & Fraud Intelligence	2023-10-09 17:05:25	2023-10-09 15:19:51
	SILENTCODERSLIMAHURUF	Anomali Phishing & Fraud Intelligence	2023-10-09 17:05:21	2023-10-09 15:20:49
	DANA Generic Scam 1	Anomali Phishing & Fraud Intelligence	2023-10-09 17:05:16	2023-10-09 15:20:00

With all of the above information assembled and curated with the supplied and customisable/ extendible Anomali Intelligence Dashboard organisations can keep their CTI, SOC teams and business leaders on top of the threats whilst automating their proactive defences and providing rapid detection and response.

Amplification with the Anomali Intelligence Channels Family

The Anomali Phishing & Fraud channel is part of the family of the Anomali Intelligence Channels developed with leading specialist partners across the main threat domains facing organisations today.



STRATEGIC USE CASES

- **Keep the Business Informed**
  Maintain the business relevant security narrative for leaders and execs.
- **Identify & Track Trends**
  See the trends in actors and their tools methods and attacks.
- **Anticipate and Prepare**
  Prioritise the threat intelligence to establish daily SOC stand-up, situational awareness, playbooks, resilience and exercises.
- **Proactive Posture Prioritisation**
  Rapidly assemble the relevant threat intelligence to prioritise protective and detective control improvements and remediation of exposures.
- **Threat Hunting & Detection Engineering**
  Prioritise the threat intelligence to direct and scope new threat hunting and detections development.

TACTICAL USE CASES

- **SOC Automation**
  IOCs to front line controls.
- **Alert/Telemetry Enrichment**
  Rapidly associate all relevant intelligence with any observed suspicious alerts or telemetry.
- **Incident Response**
  Expand and enhance the view and understanding of incidents to maximise a coordinated and effective response across all facets of the attack.
- **Real Time Monitoring**
  Bond the intelligence to collected log data and telemetry to enhance/sensitize analysis for real-time threat detection and incident response.
- **Retrospective Forensic Analysis**
  If a breach does occur, the historical data collected and stored by the Anomali platform can be directly associated with the Phishing and Fraud Intelligence to enhance the forensic analysis and investigation of the security incident.

The Anomali Intelligence Channels act powerfully in their own right and in tandem amplify one another alongside the Anomali Security Platform to address the Strategic and Tactical use cases. This gives organisations the edge in assuring their businesses, disrupting and anticipating attacks and minimising harm and interruption to their business and their customers.

Amplification of Phishing & Fraud Intelligence with relevant members of the Anomali Intelligence Channels family:

Anomali C2 & Botnets Intelligence Channel:

expand context to understand the wider malicious infrastructure to broaden threat hunting and prioritise/optimise defense across the Network.

Anomali Autolens+:

expand globally to find relevant articles across news, advisories and researchers. Helps to understand the wider context and impact of the campaign and any associated elements.

Anomali Adversary Monitoring Intelligence Channel:

expand context to understand what adversaries are behind/associated with this campaign and understand wider motivation, objectives and methods esp wrt to region/industry.

ANOMALI