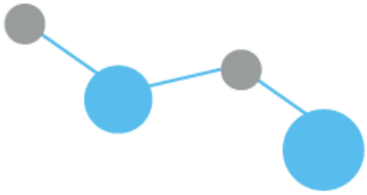
VOLON

CYBER THREAT INTELLIGENCE FOR

FINANCIAL SERVICES

THREAT INTELLIGENCE USE CASES FOR THE FINANCIAL /BANKING/INSURANCE SECTOR



THREAT LANDSCAPE

Financial services industry has always remained a high profile target for cyber threat actors since many years. Over period of time the attack sophistication has increased exponentially which has increased the scale of attacks weather it was targeted by regular Cyber Criminals motivated by financial gain or hacktivists motivated by political or ideological beliefs.

According to recent study, the finance sector's average per incident cost increased from $12.97 million in 2014 to $18.28 million in 2017; well above the 2017 average of all other industries at $11.7 million. While malware attacks were among the least costly for financial services at $5.46 million per incident on average, malicious insiders cost $169 million, phishing/social engineering cost $196.6 million, and denial-of-service attacks $227.7 millionr.

Following are primary factors which builds overall Threat Landscape for Financial Services industry

Banking Malware / Botnets

- Dridex
- Trickbot
- Gozi
- Ramnit
- Zeus/Zeus Panda

Cyber Crime Underground

- SWIFT Based Attacks
- Darknet Marketplace
- Network Compromise
- Ransomware
- Credential Breaches

Card Fraud / Stealing

- Card Markets /Shops
- Plastic Cloning
- Cash-out services
- Gift Cards Fraud

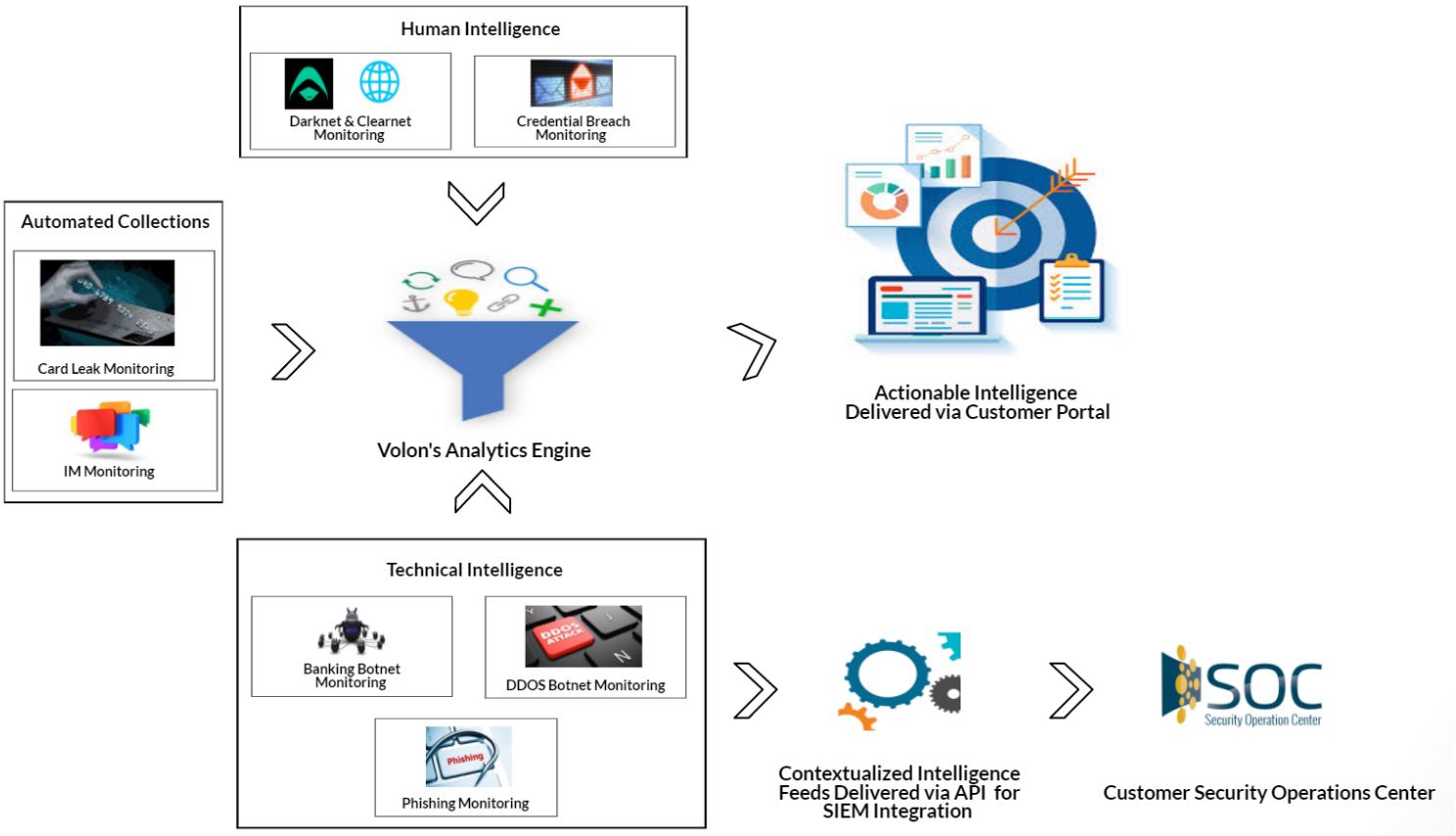
DDOS & Hacktivists

- Mirai and Pbot attacks
- DDOS as service
- Anonymous Collective

THREAT INTELLIGENCE OFFERINGS

Volon's dedicated threat research team for financial services curates specialized output for customers. With unmatched monitoring capabilities linked to threat landscape of every customer to provide actionable intelligence.

Managed Threat Intelligence clubbed with contextualized technical feeds along with real-time alerts and reporting backed with specialized Human Intelligence (HUMINT) , Open Source Intelligence (OSINT) and Technical Intelligence (TECHINT) will ensure end to end coverage of external threat and adversary insights.



Outcomes

Volon's unique process of initial customer threat scoping helps to identify customer specific actionable intelligence insights. Financial services sector specific observable via specialized HUMINT operations are delivered via customer portal. Volon's HUMINT research capability provides adversary focused insight with context such as Intent, Motivation and TTP.

Data generated via Technical Intelligence can be consumed via Volon's Intelligence Portal or can also be directly ingested by customer's SIEM platform to integrate with SOC operations.

VOLON

CONNECT WITH US FOR MORE INFORMATION

https://www.volon.io

info@volon.io