



Adversary Centric Intelligence

CONTENTS

INTELLIGEAR: ADVERSARY FOCUSED INTELLIGENCE.....	2
ADVERSARY FOCUSED INTELLIGENCE COMPONENTS.....	2
DELIVERABLES.....	4
ADVERSARY FOCUSED INTELLIGENCE PORTAL.....	5
INTEGRATIONS.....	8

IntelliGear: Adversary Focussed Intelligence

Volon's IntelliGear benefits organizations by providing Adversary Focused Intelligence, which includes contextual insights into imminent threats. This helps them to respond faster to incidents, better understand their attackers and get ahead of the adversaries by safeguarding their assets.

Monitor & Collect	Monitor variety threat sources & utilize proprietary collection platform to collect external threats via automated means
Prioritize	Organize intelligence based on customer's organization threat landscape
Analyze	Analyze the collected information to reduce false positives and meticulously rate for relevance
Validate	Utilize highly experienced HUMINT to validate the information
Contextualize	Utilize Volon's rich database to contextualize the information and apply Volon's confidence ratings
Deliver	Deliver to customer via means Flash reports & Threat Reports via Customer Portal

Who	▶		Adversary
What	▶		Incident
When	▶		Timeline
Why	▶		Motivation
Where	▶		Geography
How	▶		TTP

Adversary Focused Intelligence Components

Adversary Centric intelligence provides comprehensive coverage of Dark Web, Open Source and Technical Threat Indicators from dominant and emerging threats. The intelligence includes threat actor insights to help organizations proactively assess risks, look for vulnerabilities in the existing setup and increase the security awareness of their staff.

The Adversary centric intelligence includes

- Darknet/Deep web monitoring
- Human intelligence (HUMINT)
- Open-Source Intelligence (OSINT)
- Technical Intelligence (TECHINT)

DARKNET/ DEEP WEB MONITORING

Volon collect, categorize and disseminate threat intelligence based upon Organization profile and relevance from various Darknet Forums/Sites/IRC/I2P sites. This helps Organization to identify, profile and mitigate the risks.

HUMINT (Human Intelligence)

Volon deploys Human Intelligence, which involves direct human interaction and engagement with threat adversaries in Darknet in the exclusive 'invite only forum'. It also includes 121 interaction with Darknet threat actors to obtain direct & exclusive intelligence and supporting information/evidence in order to build more context to the intel finding.

OSINT (Open-Source Intelligence)

Volon collection experts will collect and prioritize intelligence using OSINT and sum it up with all possible contextual information which is collected via other private sources, which will allow Organization to correlate the information which is being spoken in public media with solid context provided in our reporting.

The various avenues from where open-source data will be collected are

- Social Media
- Instant Messaging (IRC/Jabber)
- Pastie Sites (like Pastebin)
- GitHub Repositories
- Blogs & News sites

TECHINT (Technical Intelligence from various campaigns)

Volon monitors campaigns and report detailed IOCs, technical information for direct consumption by Organization's SOC team. This helps to protect against campaigns such as:

- Phishing Attacks
- Ransomware attacks
- APT (Advanced Persistent Threats) group campaigns
- Malwares campaigns
- Vulnerability exploitation

The TECHINT reports published on the Intelligear portal also have mapping with MITRE ATT&CK Framework.

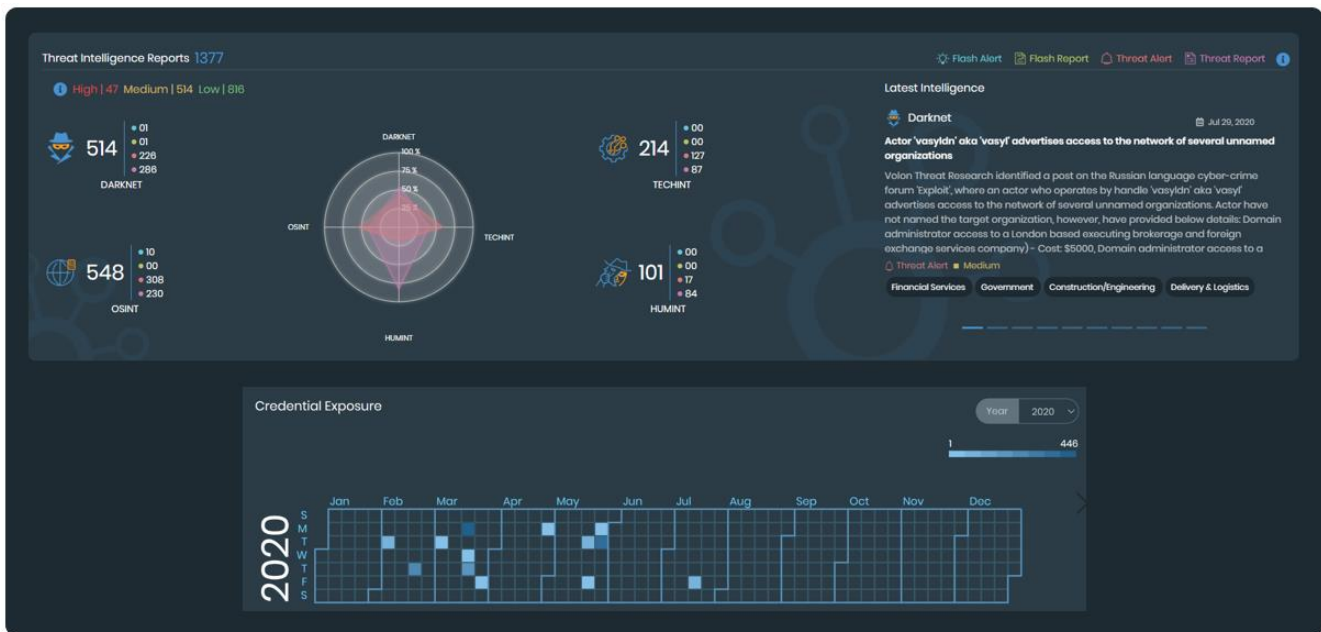
Deliverables

Sr no.	Service Component	Deliverable
1	Darknet monitoring	A finished intelligence report with confidence ratings based upon relevance to targeted organization. The report shall contain collected evidence (threat actor claims, credential leaks, exploits/vulnerability info, access proofs etc), nature of threat and our analysis on the same.
2	HUMINT	A finished intelligence report with confidence ratings based upon relevance to targeted organization. The report shall contain collected evidence (chat transcript, proof of attack, methods of breach etc), nature of threat and our analysis on the same.
3	OSINT	The OSINT reports which are published will contain extensive coverage of Motivations such as Hacktivism, Defacement and latest attack vectors along with actionable IOC, which will allow Organization to correlate the information which is being spoken in public media.
4	TECHINT	<p>The TECHINT reports covers actor motivations (Cybercrime/Cyber espionage) , tools and infrastructure which will contain observables like</p> <ul style="list-style-type: none">• IP Address• Malware Hash• URL• Domain <p>Malware analysis /reverse engineering technical report will also be provided on Organization request.</p>

Adversary Focussed Intelligence Portal

Volon deliver intelligence via customised Customer Portal which is focused on customer profile and sector, overall aim is to provide relevant and actionable intelligence with ability to be consumed by multiple teams of a security organisation of the Organization.

Dashboard



Dashboard provides a single view with summary of all threats for the customer, this include reporting from Darknet, Credential Leaks, Technical Intelligence. Flash reports with "High" relevance is also available for customers to view directly.

Threat Report

Threat Alert - 202007142236 Ver 1.0
Download Report

HUMINT | Online Engagement

Actor 'friendofthejews' aka 'franknox' advertises access to the Fortimail email gateway of an Indian conglomerate holding company

Jul 14, 2020 | Medium

Volon Confidence Rating

Threat Alerts provide timely information and initial findings about security issues, vulnerabilities, exploits, darknet advertisement posts discovered by Volon Threat Research from variety of sources such as Darknet, Media Articles, Security Blogs, Social Media, etc.. The Threat Alerts contain limited information and could be updated later to turn into Threat Reports with detailed analysis.

Threat Summary:

On July 14, 2020, Volon Threat Research received a private message on an instant messaging application 'Jabber' from an actor who operates by handle 'friendofthejews' aka 'franknox' on the Russian language cyber-crime forum 'Exploit'. Over the private engagement, actor advertises access to the Fortimail email gateway of an Indian conglomerate holding company, Essel Group [www.esselgroup.com].

The actor has also shared a proof of access screenshot, showing the organization's mail server domains. The IP address of the Fortimail gateway is also visible in the screenshot, the details about which are listed below:

- IP address: 61.95.174.200
- IP Location: India, Mumbai Bharti Airtel Ltd.
- Issuer: DC=com, DC=esselgroup, CN=esselgroup-ESSELADC-CA
- Port(s) open: 443 (TCP)

Along with Essel Group, in the past, actor advertised access to the Fortimail gateway belonging to several organizations including Bankintor (Report ID: 2020071258935), Horizon Credit Union and Companhia Brasileira de Trens Urbanos (Report ID: 2020071380276).

For access to the Essel Group, the actor has quoted a price of \$10,000.

Threat Detail:
About Actor:

Associations

Source: F- Cannot be judged
Information: 2- Probably true

friendofthejews | franknox

Cyber Crime **Motivation**

South Asia

Media **Sector**

Vulnerability & Exploitation Account(s) Compromised

Related Reports

Darknet

2020071380276
Actor 'friendofthejews' aka 'franknox' advertises access to the Fortimail email gateway of 2 organizations falling unde...

Threat Alert | Medium

Financial Services Government

HUMINT

202007258935
Actor 'friendofthejews' aka 'franknox' advertises access to the Fortimail email gateway of the Spanish financial...

Threat Report | High

Financial Services

Threat Actors/Motivations

Actors & Reports

623 Actors

- teamkalvinsecteam (32 Reports)
- Lazarus Group (17 Reports)
- ShinyHunters (12 Reports)
- Bassterford (9 Reports)
- drumflu (9 Reports)

Motivation & Tags

344 Data Breach

280 Malware

Vulnerability & Exploitation

- [Early Warning] Proof-of-Concept released for Critical CVE-2020-147 flaw (Medium) Jul 26, 2020
- Recent discovery of Blue Mockingbird API targeting servers in India for... (Medium) Jul 26, 2020
- [Early Warning] (Update) Actor 'dav01' aka 'polvas' advertises 0-Day RCE... (Medium) Jul 25, 2020
- [Early Warning] NSA Urgently Warns on Industrial Cyberattacks, Triconex... (Medium) Jul 25, 2020
- [Early Warning] Vulnerability in Cisco Firewalls Exploited Shortly After... (Medium) Jul 25, 2020

Data Breach

- Actor 'random12345' advertises access to network file storage server of an... (Low) Jul 26, 2020
- Actor 'ShinyHunters' shared databases of multiple organizations (Low) Jul 26, 2020
- Actor 'ShinyHunters' released a new batch of databases belonging to sever... (Low) Jul 27, 2020
- Actor 'Chandler Bing' shared the database of an American sales enableme... (Low) Jul 27, 2020
- Ex-employee deleted the data of an Indian IT firm (Low) Jul 27, 2020

HUMINT

- Actor 'Bassterford' advertises access to an American government agency (Low) Jul 26, 2020
- Actor 'Stari4ok' advertises access to the network of an Indian financial... (Medium) Jul 26, 2020
- [Early Warning] (Update) Actor 'dav01' aka 'polvas' advertises 0-Day RCE... (Medium) Jul 26, 2020
- Actor 'EranM' advertises access to the network of an American healthcare... (Low) Jul 26, 2020
- Actor 'hanash' aka '13ak' advertises access to an American insurance... (Medium) Jul 23, 2020

Early Warning Reports

The image shows a screenshot of a security dashboard with two threat alert cards. The top card is titled 'Threat Alert - 2020072087260 Ver 1.0' and features a blue icon of a person wearing a mask. The text of the alert reads: 'Darknet | Raid Forum [Early Warning] Actor '3xpl01td3v00' advertises an exploit for CVE-2020-6287 - A Vulnerability in SAP NetWeaver Application Server'. It is dated 'Jul 20, 2020' and has a 'Medium' severity level. A 'Download Report' button is visible in the top right corner. The bottom card is titled 'Threat Alert - 2020072379489 Ver 1.0' and features a blue icon of a gear with a person inside. The text reads: 'Technical Intelligence | Blog Post Indicators associated with the Lazarus Group new malware framework known as MATA targeting various industries, including Technology, e-commerce and internet service provider'. It is dated 'Jul 22, 2020' and has a 'Medium' severity level. A 'Download Report' button is also present in the top right corner.

Integrations

Volon's modular intelligence output enables third party integration utilizing much easier connection methods. These industry standard methods such as REST API / STIX/TAXII provide easy methods to ensure data flow across multiple systems.

Dashboard Integration

Volon can provide integration options to ensure Volon's intelligence data is able to ingest in the Intelligence aggregator platforms or third party TIP (Threat Intelligence Platforms) to help customer in order to remove dependency for additional layer of dashboard and enable Customer to collect and analyse all intelligence information at single console

SIEM & SOAR Integration

Technical IOCs can be integrated with any SIEM with the help of RESTful API or STIX/TAXII distribution system. Volon can provide steady contextualized Intelligence feeds to SIEM and SOAR to enable SOC analyst link the indicators identified from internal system to External intelligence provided by Volon.

VOLON

Volon Cyber Security
www.volon.io