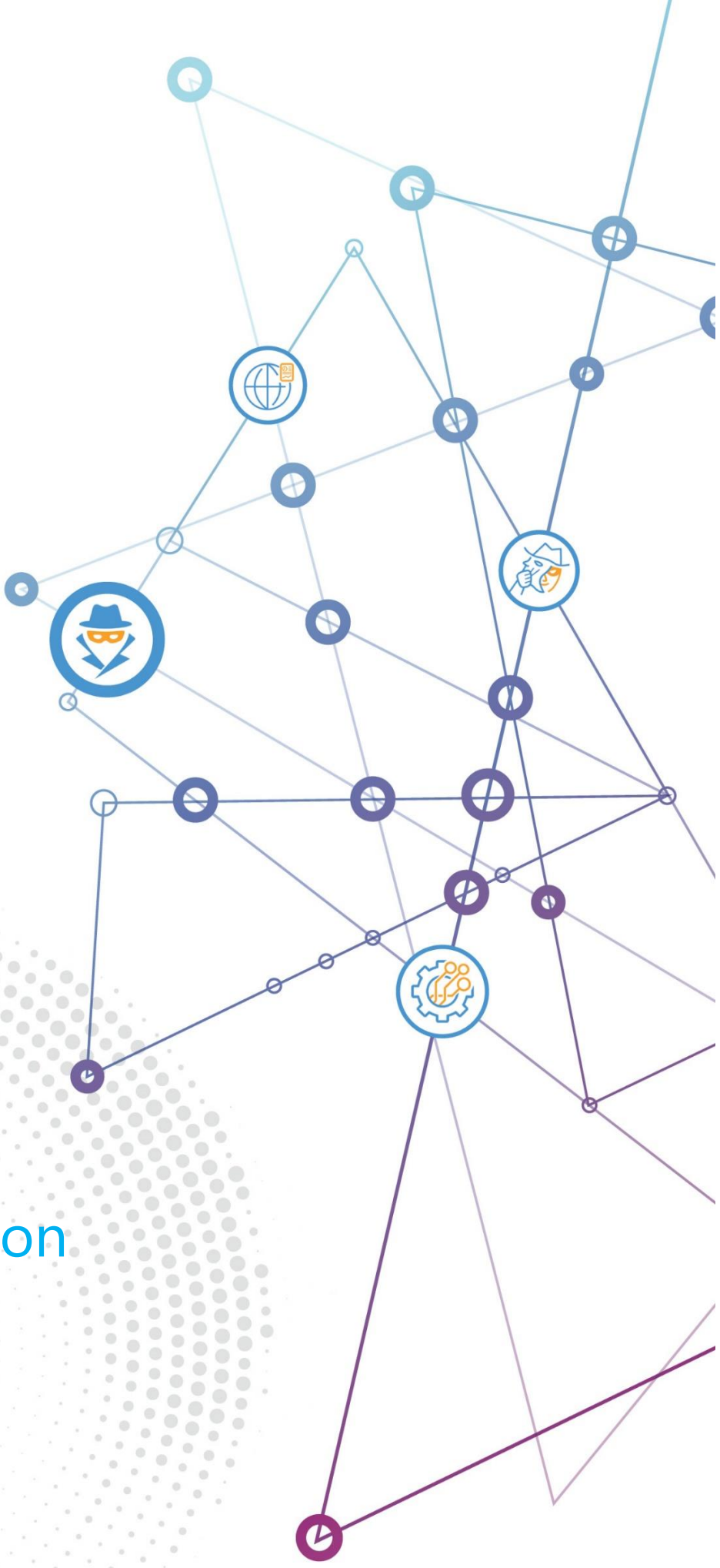
Intelligear
Managed Threat Intelligence



Brand Protection Intelligence

Use Case

VOLON

Brand Attacks

Brand Abuse is the most wide-spread online cyber-attack that threat actors use to target organizations. Threat actors impersonate a brand by setting up phishing sites, typo squatting domains, creating rogue apps, using organizations' leaked credentials and via social media campaigns.

The foremost risk for brands whose customers falls victim to attacks is that they associate any loss (monetary or personal) with the impersonated brand. Eventually it severely affects brand's reputation, trust and deter customers to associate with the same brand again.

According to hacking statistics for 2020-2021:

62 Compelling Hacking Statistics 2021: Data on Common Attacks, Impact & Prevention - Financesonline.com)

- ✓ 55% of phishing sites used target brand names and identities in their URLs.
- ✓ More than 80% of breaches that used hacking involved brute force or the use of lost or stolen credentials.
- ✓ On average, there were nearly three attempts per month at hijacking corporate social media accounts. Every year, takeover attempts occur around 30 times per institution.
- ✓ 32% of supply chain attacks targeted utility software. On the other hand, 24% targeted application software. Meanwhile, 12% targeted the code repository.
- ✓ During the first half of 2020, there was a 95% increase in executive/VIP-related threat activity for social media profiles. In total, there were 1.2 million incidents for more than 7,000 executives with highly public social media profiles.
- ✓ Botnets are used for launching disinformation campaigns using inauthentic social media, DDoS attacks, and other malicious acts. Bots can make up for 60% of overall web traffic. However, less than half of these can be declared as bots. These make tracking and blocking botnets challenging. (Council to Secure the Digital Economy, 2020)
- ✓ A survey revealed that 91% of people know that using the same password or variation puts them at risk. However, 66% always or mostly use the same password. (LastPass, 2020)

Customer Case (Large IT Cloud Based Service Provider)

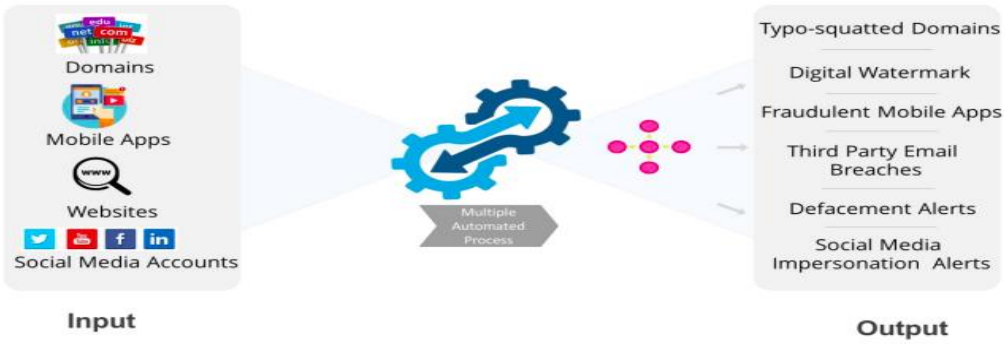
The organization is one of the leading Cloud Based Service Provider catering to a wide range of customer across the globe. Their end customer would include several Fortune 500 clients.

Customer Business Challenge:

Lack of visibility of Brand Abuse & External Threats: The existing security setup did not provide means to identify external threats and attacks on their Brand. The lack of visibility not only posed a threat to the organization but indirectly to their end client's brand and data for whom Volon's customer managed cloud implementation projects.

Volon Solution: Brand Protection and Takedown

Volon implemented Brand Protection Intelligence Solution using the proprietary algorithms to detect phishing attacks, typo-squatting, defacements, rogue apps, credential leaks and brand impersonation in social media.



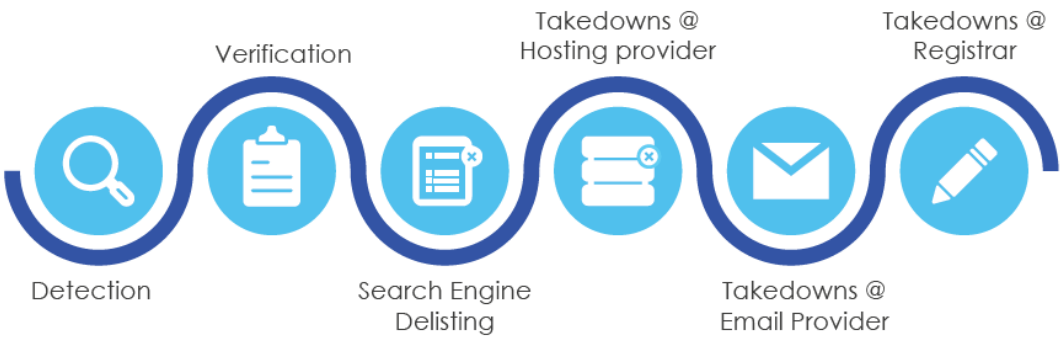
Solution capability included:

1. Identification analysis and reporting of cyber threats based upon customer profile/ threat landscape
2. Comprehensive analysis of threats by using AI/ML engine, and TTPs used by threat actors.
3. Continuous tracking of threat actors affecting India & global regions to help attribution of threat.

The AI/ML advantage:

4. AI helped gather & map digital threats to customer profile and identify threat vectors that could impact customer environment.
5. AI helps to optimize the fast, large-scale collection and categorization and analysis of the threats, reduced Human analytic efforts to a fraction
6. Quickly translate language and lingo of threat actor across various languages and identify chatter and discussion to alert customer mentions in Darknet/ Social-Media

For Takedowns, Volon used their proprietary and DMCA process that includes sending notices to the offending party, hosting providers and registrars under provisions of Local and International Law to demand the takedown on account of impersonation/phishing etc.



Outcome:

Brand Protection solution provided full visibility to various Digital Threats e.g. Credential Compromise, Phishing Attempts and Rogue Apps etc on a continuous basis via IntelliGear Web Portal. This allowed the customer to gain advance intelligence and proactively act towards preventing further attacks on their Brand. Thus Brand Protection helped customer to protects its Brand value, Trust, Integrity and Reputation benefits.

Volon Cyber Security

www.volon.io