VOLON

Volon® is a boutique cyber security firm that offers specialized solutions for corporate and governments in Cyber Threat Intelligence.

Our intelligence team deploys HUMINT and OSINT to bring the actionable intelligence backed by machine learning and analytics.

CYBER THREAT PREDICTIONS: 2018

CONTACT US

3 Floor, EFC Business Centre,
Marisoft 3, Marigold Complex,
Kalyani Nagar, Pune, 411014
Maharashtra, India

+91 7798299399
+91 9860050511

info@volon.io
www.volon.io

VOLON

OUR PRODUCTS

INTELLIGEAR THREAT INTEL:

MANAGED SOLUTIONS:
* Darknet
* OSINT (Open Source Intelligence)
* Social Media
* Cyber Crime Tracking
* DDOS Intelligence

PLATFORMS:
* DeepScope - Darknet Monitor
* Card Leak Monitor
* Credential Monitor
* Underground Actor Monitor
* Breach+Defacement Monitor
* Social Media Monitor
* OSINT Monitor

FEEDS:
* Threat Intelligence Feeds

#OP SANDBOX

"On-Premise" solution, which enables customers to identify and analyze malicious files without sharing with third party providers.

#OP FUZZ

* Industry leading security testing methodology to help Customers Fuzz Test the code/application before final release.
* Identify Logical Programming Bugs missed in source code audit
* Automated Discovery and Reporting
* Fully Managed support

CYBER HEALTH ASSESSMENT

Assess security health insights of an organization.

INTELLIGEAR DECOY

The decoys (Honeypots) are installed at strategic points in customer's network that helps them to look at infections and attack patters on their network. Customers use intelligence to improve and harden their network security posture.

CYBER TRAINING & EDUCATION

* Cyber Threat Hunting
* Fuzzing
* Open Source Intelligence
* Customized Training Programs

TORNADO: ANTI PIRACY

* Designed for Film & Media Industry
* Stop Piracy at the Source
* Enhance monetization gain to rightful content owner

VOLON

2017 RECAP

An eventful year that saw extreme sophisticated adversary tactics from cyber threat actors with motivation ranging from "Nation-State" attacks involving elections in countries to financially motivated Ransomware attacks that disrupted business operations of some of
the largest organizations.

Here is our list of top 5 cyber attacks patterns that gathered most attention in 2017:

.

RANSOMWARE

Equation Group (Associated with NSA) security/hacking toolset leak by "Shadow Brokers" gave NSA tools in the hands of threat actors. These were used to carry out large scale "Ransomware" attacks such as WannaCry, Petya & Locky on public/private sector organizations.

DATA BREACHES

The global organizations such as Verizon, Deloitte, Uber & Equifax admitted to severe data breach.
Among Indian bigwigs, Reliance JIO, Indian Internet Registry (IRINN) & Zomato were hit.

DDOS

"DDOS for hire services" have been quite popular in underground marketplace.
In 2017, Ransom DDOS was one of the favorite for many threat actors, where they demand ransom for not carrying out a DDOS on victim. “Armada Collective” and “Fancy Bear” groups have been in news for use of this TTP.

CREDENTIAL RE-USE

Even though credential re-use has been a long-standing threat, Mark Zuckerberg’s twitter account hack this year generated huge media attention.
People often keep similar credentials to access multiple platforms. In an event of a breach attackers try to gain access to all the accounts of the user through hacked passwords.

ATTACKS ON IOT

In line with their growing use in 2017, the IOT devices also came under increased cyber attacks. In many instances, IOT devices were compromised and used in large scale botnet operations.
Mirai, Reaper and Bricker Bot are few examples of widescale use of IOT Botnet

VOLON

2018 PREDICTIONS

2018 will see automated cyber attacks for the first time. Threat actors would deploy automation techniques to carry out their operations and attack vectors/TTPs would move to a much advanced level that will beat best of security infrastructure.

Here is what we believe would be the top 5 cyber security threats to watch out for in 2018:

.

ATTACK ON CRYPTOCURRENCY

The surge in valuation and high trading activity of crypto currencies would make them a target for attack in 2018. Cyber criminals will bring out new TTPs to attack and steal crypto currencies.
The recent attacks on crypto exchange like “Coinbase” and “Bitfinx” has seen millions wiped out.

IOT SMART MALWARE

In 2017, the attacks on IOT have been mostly limited towards widespread compromise of end user internet routers.
With IOT devices slated for the highest ever growth in 2018, we could see new Linux variant for mass IOT device compromise. Possibility of Ransomware to move in IOT/Smart home sector cannot be ruled out.

NATION - STATE

Nation-State threat actors will continue attacks and play a much bigger role due to ongoing increased geopolitical tensions involving North Korea, South Asia and Middle East.

AUTOMOBILE

2018 could see cyber criminals increasingly carry out attacks on smart automobiles including cars. (The increased use of technology in smart/autonomous/driverless automobile has made it a lucrative segment for threat actors.)
Car hacking has been a popular topic of research in various conferences and US FBI has also warned of increase in car hacking incidents in times to come.

DATA BREACHES & USE OF ARTIFICIAL INTELLIGENCE

2018 will see cyber criminals apply techniques to discover and disrupt machine learning models used by defender.
The threat actors for the first time will deploy Artificial Intelligence to conduct attacks on multiple targets.

THE TEAM

KAPIL GUPTA
CO-FOUNDER

Kapil has over 19 years experience performing multiple consulting, business development and operations profile in technology & finance sector.
Before founding Volon, he was based in Stockholm, Sweden and worked at Capgemini where he led consulting assignments and business development for Nordics clients.
Previously he worked at a Private Equity Fund (True North/India Value Fund) owned Digital Media firm in London and before that at Steria, a European listed company as a Member of India Operations Board. He spent his early career in M&A and Corporate Finance advisory at Ernst & Young and GE Capital in United States.
Kapil studied at London Business School and is also a qualified Chartered Accountant.
He can be contacted at 'kapil.gupta@volon.io'

MUSLIM KOSER
HEAD-PRODUCTS & TECHNOLOGY

Muslim has over 20 years of Information Security Experience with core focus on Cyber Threat Intelligence, Cyber Risk Management and Cyber security consulting. Before Volon, he worked at FireEye Inc (US listed Cyber Security Company) where he headed their Cyber Threat Intelligence Research team and before that at iSIGHT Partners (later acquired by FireEye Inc) as one of the initial employees where he set up their Cyber Threat Intelligence research team.
Previously, he was based in Malaysia working for Network Security Solutions and headed their information security consulting practice. Muslim is also credited with establishing national level CERT (and also for a foreign Asian country) and consulting for various corporate CSIRTs.
Muslim holds Masters in Electronic and Communication from Devi Ahilya University.
He can be contacted at 'Muslim.Koser@volon.io'

CONTACT US

3rd Floor, EFC Business Centre,
Marisoft III, Marigold Complex, Kalyani Nagar, Pune, 411014
Maharashtra, India
+91 7798299399
+91 9860050511
info@volon.io
www.volon.io

For more information on Volon, please visit:
www.volon.io

VOLON