Deloitte.

Private and confidential
2016

Cyber Incident Response
Fast, Thorough, Decisive

- 70–90% of malware samples are unique to an organization
- In 60% of cases, attackers are able to compromise an organisation's security within minutes
- 50% of employees open emails and click on phishing links within the first hour of receiving them

Source: https://msisac.cisecurity.org/whitepaper/documents/1.pdf

Cyberattacks can result in loss of data, finances and reputation, along with IP theft and operational disruptions. Additionally, they have legal implications.

MODUS OPERANDI OF CYBERATTACKS

THREAT ACTORS - THE PEOPLE INVOLVED

- Non-state actors
- Organised crime syndicates
- Ideological groups
- Individuals

ACTOR ECOSYSTEM - WHO SUPPORTS THEM

- Malware authors
- Hosting entities
- Payment processors
- Domain generators
- Command and control
- Money mules

TOOLS, TACTICS AND PROCEDURES

- Social engineering
- Botnets
- Phishing
- Ransomware and doxing
- Exploits
- Website compromise
- DDoS Password theft
- Evasion tactics

THREAT VECTOR - THE CHANNELS USED

- Suppliers and partners
- Employees
- Mobile devices
- Smart devices
- Customers
- Email

KEY ORGANIZATIONAL CHALLENGES

IT COMPLEXITY

- Endpoint diversity, with evolved IT structures supporting aspects like Bring Your Own Device (BYOD)
- Unauthorised devices connected to the organisation network
- Hosting new IT initiatives around cloud computing
- Demand for innovative IT solutions and real-time access to information across various devices
- Access provided to third-party entities

OPERATIONAL CHALLENGES

- Reliance on signature-based controls
- Limited data encryption
- Reliance on device-focused monitoring
- Insufficient skills/staffing in the IT security area

PROCESS/GOVERNANCE CONSTRAINTS

- Limited change control process
- Lack of business risk alignment
- Limited security of the Software Development Life Cycle (SDLC)
- Improper business risk alignment
- Limited extent of asset mapping to risks
- Inadequate/irregular training and awareness for employees

AS ORGANISATIONS WITNESS RISING CYBERATTACK INCIDENTS, ONE OF THE KEY ASPECTS TO CONSIDER IS INCIDENT RESPONSE AND CONTAINMENT.

An effective incident response begins with intelligent investigation

- Looking at the right things, not necessarily everything
- Following the logical leads, not all the leads that exist
- Getting the right intelligence and information resources
- Applying automation and using analytical techniques to expedite the investigation

HOW CAN DELOITTE HELP ORGANISATIONS WITH INCIDENT RESPONSE AND CONTAINMENT?

Conduct a comprehensive investigation

This is done to:

- Understand the potential scale of the incident
- Detect the locations of potentially compromised systems
- Identify, preserve and examine logs available for the incident
- Determine any priority systems or logs with a tier-based system for further collection and examination
- Identify if an immediate, remote assessment or collection is required

Assess damages

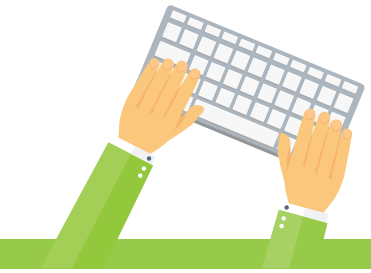
Assessing the damage caused is vital to ascertaining the data accessed or exposed. It also provides an understanding of the information that the perpetrator might have sought for. We assess the damages by looking at the:

- Files accessed
- Indicators of file use and adversary intelligence gathering
- Files potentially or actually breached
- Hacker's immediate steps after the attack

Assist with response plan

Our cyber forensic specialists can assist you with a cyber incident response plan that addresses:

- Responsibility matrix in the event of an incident
- Root cause analysis and right diagnosis (situational analysis of the potential impact such as impacted parties, information involved, etc.)
- Remediation plan



Please reach out to:

Rohit Mahajan
APAC Leader & Head - Forensic
Financial Advisory
Tel: +91 22 6185 5180
Email: rmahajan@deloitte.com

Jayant Saran
Partner
Forensic Financial Advisory
Tel: +91 124 679 3607
Email: jsaran@deloitte.com

Jimmy Mate
Senior Manager
Forensic - Financial Advisory
Tel: +91 20 6624 4610
Email: jmate@deloitte.com