Ransomware Incident Response

Cyber Security Services

TICTAC

CYBER SECURITY + DATA RECOVERY

The State you are now

- Data is not available
- Business Interruption
- Financial Damage & Legal Implications & Liabilities
- A hacker was inside your network
- Third Party liability
- Possible Data Leak Issues

Data is not available

- No Access to your critical files
- No Access to your CRM / ERP / Databases / Accounting / Invoicing
- You don't know if you will ever be able to reclaim your data and you rely on hacker's intentions and capabilities
- Your backups are not working / They are compromised

TICTAC
CYBER SECURITY + DATA RECOVERY

Business Interruption

- Some files may have been lost forever
- Your company cannot easily return in normal operation after the breach
- There is no specific Timeline for returning to normal business

TICTAC
CYBER SECURITY + DATA RECOVERY

A hacker was inside your network

- Your credentials were probably compromised
- You don’t know if they are still inside
- Even if you restore your data, you still don’t know if they left an open communication with your infrastructure
- Think for one moment: If you were inside your infrastructure with total access, what would you do to blackmail you? This is what probaly the hacker will do.

TICTAC
CYBER SECURITY + DATA RECOVERY

Third Party liability

- In case you have integrations with third parties (Clients/Vendors) that the hackers will move to their infrastructure, too (Lateral Movement)
- In case you have third party data in your network and they are breached, you have Legal and financial Liability to third parties

TICTAC
CYBER SECURITY + DATA RECOVERY

Data Leak Issues

- The following data is usually leaked by hackers:
  - Employee Data (Covid Lists)
  - Patents (Private Research)
  - Financial Information (Shareholder's data)
  - Legal (Legal agreements under NDA)
  - Commercial (NDAs and third party information)
- The hackers probably made a copy of some files and transferred them outside your network
- They can blackmail you for Data Leak

TICTAC
CYBER SECURITY + DATA RECOVERY

Financial Damage, Legal & Liabilities

- Under the European Law (GDPR Compliance) you bare responsibility to protect all sensitive data inside your network upon severe Financial and Legal Penalties
- You are obliged to notify the local authorities for any Cyber Security data breach within 72 hours
- You are obliged to notify all your employees for the data breach and possible credentials are compromised
- You are obliged to notify all your Vendors / Clients in case you hold on sensitive data
- The local authorities have the right to inspect your infrastructure current status and fine your Organization up to 4% of total revenues and max. 20.000.000 euros
- The Tax Authorities have the right to fine the Organization in case of total loss of all tax records

TICTAC
CYBER SECURITY + DATA RECOVERY

TICTAC
CYBER SECURITY + DATA RECOVERY

Fact: Your infrastructure was vulnerable

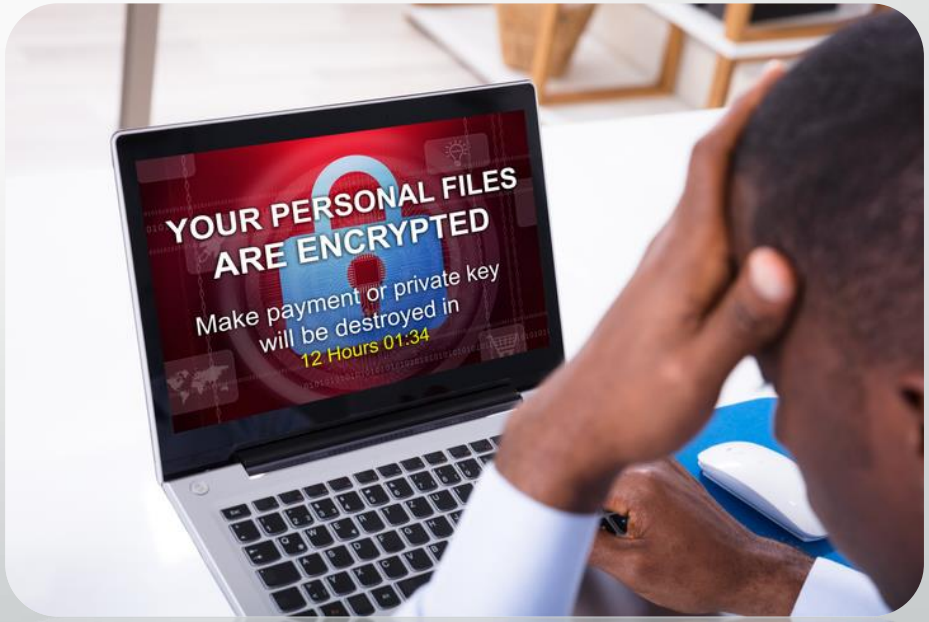
- Since a non authorized person was inside your premises, he can still be inside or he can make a new breach in the near future.
- Let's identify some very serious cyber security issues.
  - **Your current protection didn't prevent the attack** (Endpoint Security, Antivirus, Firewall)
  - **Your backups didn't work as they should have**
  - You don't know if files left your infrastructure without notice
  - You don't know how he got in and how long he was inside
- You must change protection solutions and strategy
- Cyber Security in these days is not Set & Forget – It needs 24/7 monitoring and proper setup. We can help you with that

TICTAC
CYBER SECURITY + DATA RECOVERY

Ransomware Incident Response procedure

- We have handled thousands of Ransomware Attacks & Incidents successfully so we understand the organizations' current status and the management's agony
- We carry out a specific procedure according these are the steps:

1. Identification of the Ransomware Variant in our Lab
2. Classification of the Ransomware Variant and its behavioral analysis through database resources from similar incidents around the world
3. Web and Dark Web research in partners and private forums for possible decryptor or reverse engineering methods
4. Identify if the attackers are capable of providing a solution (Proof of Concept)
5. Price Negotiation & Communication with the hacker's team through secure & anonymous infrastructure
6. Research for reference regarding the credibility of the hacker's team
7. Cryptocurrency facilitation of the payment in case you decide to carry out a payment to the hacker's team
8. Reporting for Cyber Insurance & Local Authorities
9. Threat Intelligence Report (if requested from the client)
10. Cyber Exposure Analysis for leaked credentials and (if requested from the client)
11. External perimeter Cyber Posture and Company's Cyber Rating (if requested from the client)



TICTAC
CYBER SECURITY + DATA RECOVERY

What we can offer to your organization

1. Ransomware Incident Response
2. Perform Fast Digital Forensics
3. Protect the infrastructure during the incident
4. Legal Consultation
5. Protect & Monitor your infrastructure from Future Incidents with Managed Cyber Security Services
6. Reporting & Documentation for Insurance
7. Cyber Insurance

TICTAC
CYBER SECURITY + DATA RECOVERY

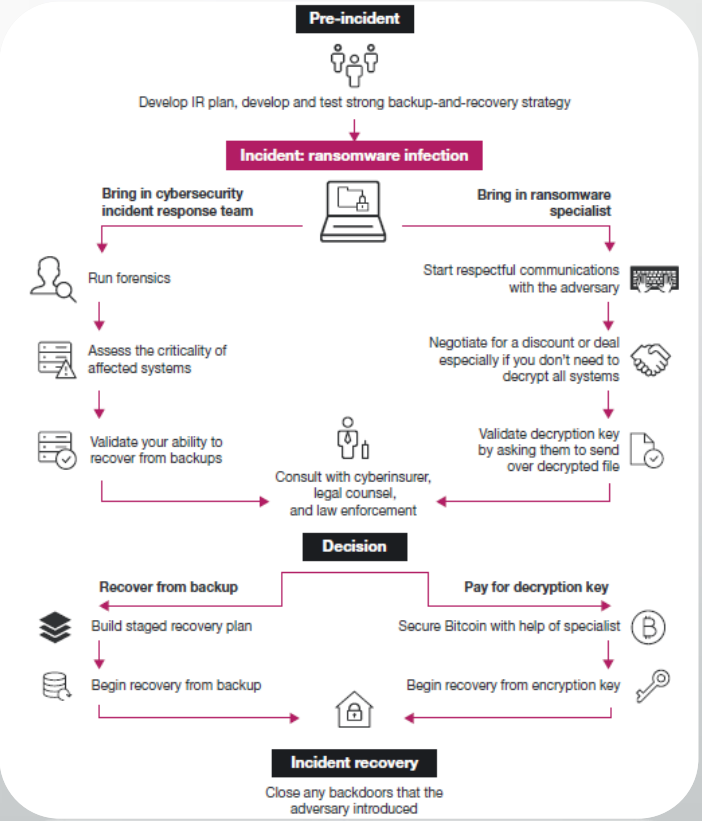
Perform Fast Digital Forensics

- Identify if the hacker is still inside your network
- Find evidence about malicious activity
- Identify the initial date of the infiltration from the attack
- Identify if data has been leaked from your infrastructure
- **3 days after the full deployment of our tools (software agents) we will finish the forensics investigation**
  - When the attack started?
  - Which endpoint started the attack?
  - How the attacker penetrated your system?
  - What data was leaked?
- Identify & categorize any malicious external activity to your infrastructure

TICTAC
CYBER SECURITY + DATA RECOVERY

Ransomware Incident Response

- Evaluate the current State of the data loss
- Protect your encrypted state of the data which is crucial
- Investigate Data Recovery possibilities
- Investigate Reverse Engineering Options for Files Decryption
- Initiate & Handle Hacker's Communication & Negotiation
- Provide instructions & guidance regarding the payment



Protect the infrastructure during the incident

- Install & Monitor remote agents throughout all your endpoints to monitor any malicious activity within the network
- Protect Endpoints & Servers against a new Files Encryption Attack
- Protect your backups & implement a Disaster Recovery Policy
- Apply Sandbox to any unknown application

TICTAC
CYBER SECURITY + DATA RECOVERY

Legal Consultation

- Provide Legal Advise and explain your typical obligations for reporting the incident
- Handle the appropriate Steps in order to avoid Legal Implications

TICTAC
CYBER SECURITY + DATA RECOVERY

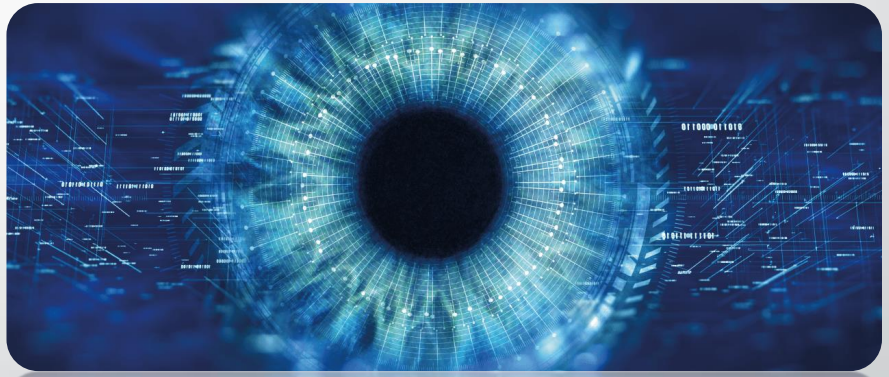
Protect & Monitor your infrastructure from Future Incidents

- IT Support does not prevent Cyber Security Attacks
- Cyber Security Services are offered to prevent Cyber Security Incidents that can cause Business Interruption & Financial Losses
- Our job is to consult your IT Team and to monitor your infrastructure
- Security Operation Center Services (Monitor for any malicious actions & activity 24/7/365)
- Provide bulletproof Endpoint Protection along with monitoring
- Collect Logs from Endpoints & Servers and analyze every suspicious move
- Virtual CISO (Cyber Security Officer) Services

TICTAC
CYBER SECURITY + DATA RECOVERY

Threat Intelligence & Cyber Exposure

- Provide a Threat Intelligence report for the Threat Actors
- Behavioral Analysis of the Threat Actor team
- Strategy of the negotiation based on the Threat Intelligence Report
- Cyber Exposure analysis for leaked credentials
- Cyber Rating & External Perimeter Cyber Posture



TICTAC
CYBER SECURITY + DATA RECOVERY

Cyber Security Insurance

- Protect your business from the unknown
- Consultation for your infrastructure
- Proposal from multiple vendors

TICTAC
CYBER SECURITY + DATA RECOVERY

Success Rates

- Our team has handled more than 500 ransomware incidents between 2019-2021. We have handled negotiations up to 25.000.000 USD
- Our negotiators usually achieve a reduction of the ransomware price from 10-80% depending on the ransomware family
- We have about **98% success rate to get the files decrypted** in cases where our team gets involved from the beginning of the incident.

TICTAC
CYBER SECURITY + DATA RECOVERY

Incident Response Methodology

- Collect Sample of Encrypted and un-encrypted files from Client along with the ransomware note
- Identification of Ransomware variant and research if there are possible decryptors or reverse engineering solutions available
- Contact with the Hacker team to identify the Ransomware demand
- Credibility assessment of the Threat Actor team to identify the negotiation tactic based on previous cases, in our extensive database of incidents
- Threat intelligence report provision for the threat actor team
- Perform Proof of Concept for the Hacker team in order to prove that they have the correct decryptor
- Consultation with the client regarding the coordination of the incident to minimize business interruption and define the cost of data loss and data exfiltration
  - Backing up the current encrypted state and securing these backups
  - Identifying sources of data within the infrastructure
  - Looking for unencrypted data with the infrastructure
- Initiation of the negotiation process based on the final strategy meeting with the clients Executives
- Reporting for the incident

TICTAC
CYBER SECURITY + DATA RECOVERY

Some of our Clients

TICTAC
CYBER SECURITY + DATA RECOVERY

We are here for you

Contact Us

www.tictac.gr | www.tictaclabs.com

Tichis 2, 16777, Elliniko, Athens, Greece

Tel. +30 2106897383

info@tictac.gr