ISC

(BTech III CSE Sem 6 - Div A and B)

Jan-April 2024

Week#1 – Jan 5, 2024

Dhiren Patel

Lab next week – Classical Cryptography

- Substitution Cipher - Caesar Cipher
- Transposition ciphers - Rail Fence Cipher, Columnar cipher
- Plain text – original msg (readable text)
- Cipher text – transformed msg (encrypted)
- Transformation method / Algorithm
- Key

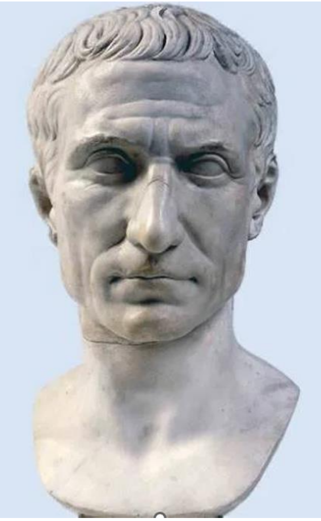
Caesar Cipher

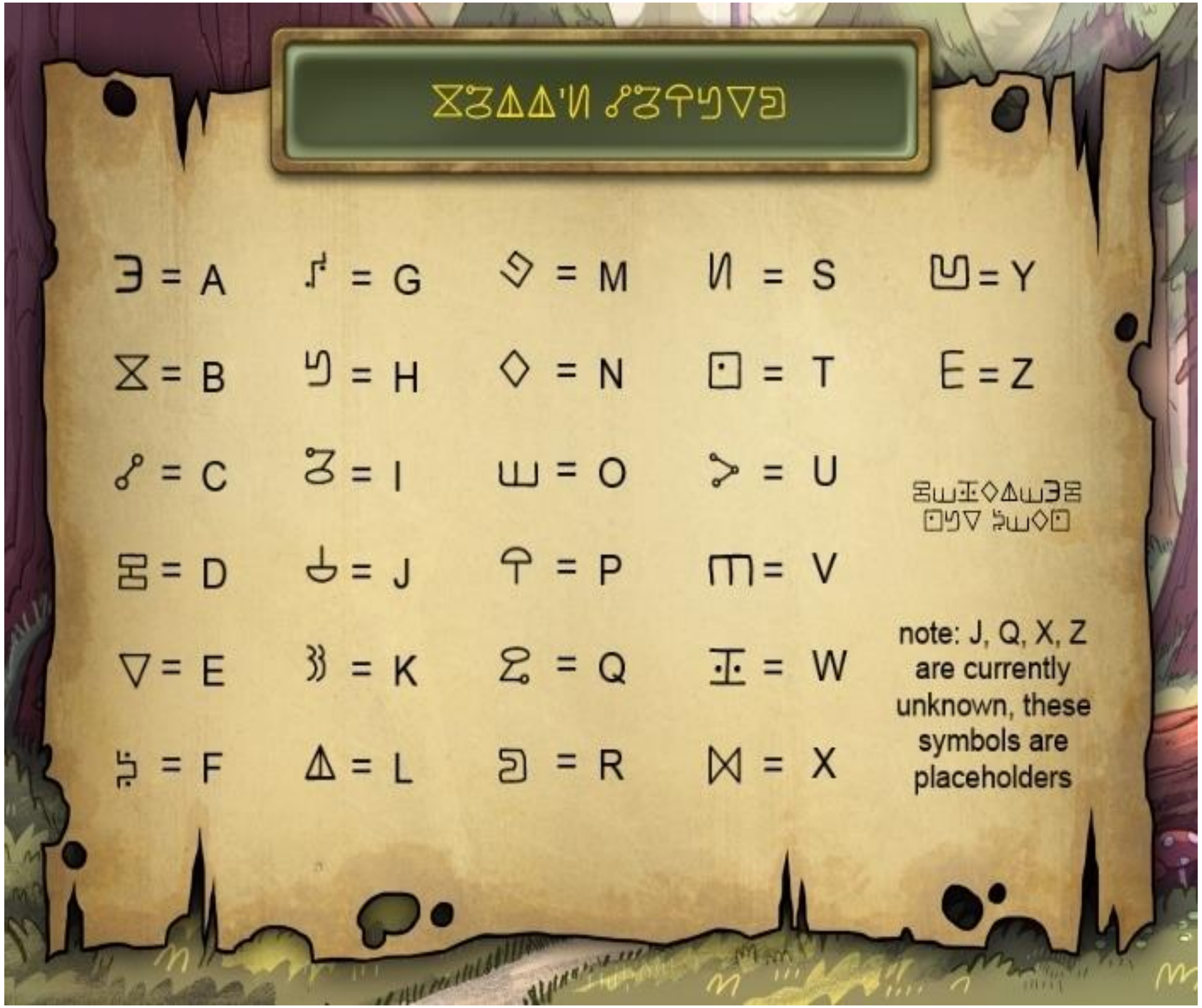
Julius Caesar

Roman Emperor/ Dictator

Born – 100 BC

Died – 44 BC





Decrypt the given word

- GUS (English word – encrypted using Caesar Cipher)

Caesar cipher and Monoalphabetic cipher

- Caesar Cipher – Shift letters of msg by k positions (k = key (integer between 1 to 26))
- E.g. DRP – encrypted as GUS with key = 3
- Mono-alphabetic – if same letter occurs again in msg, it will be transformed to same encrypted letter (e.g. all D in text will be G in cipher text)
- DHIREN AND DIMPLE

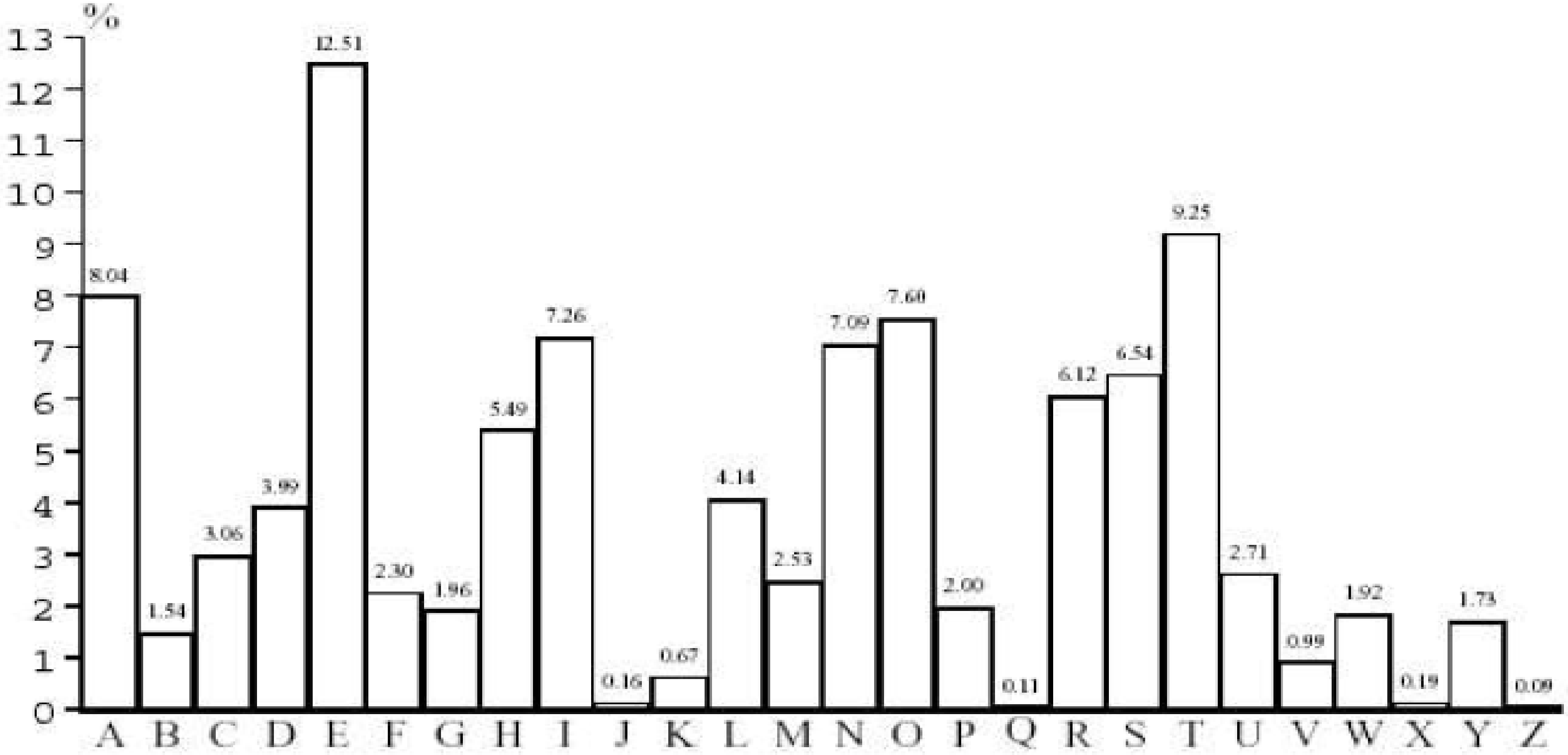
Caesar cipher (Shift cipher)

- an alphabetic shift through *k* characters (for some fixed *k*)
- Encryption is defined by
- $c_{\mathrm{i}} = e(m_{\mathrm{i}}) = (p + k) \bmod s$
- Decryption is defined by
- $d(c_{\mathrm{i}}) = (c - k) \bmod s$
- For English text, $s = 26$ and characters A through Z are associated with integers p=0 through p=25
- According to history, Julius Caesar used the key $k = 3$
- Write a program to implement Caesar Cipher – encryption, decryption, brute-force attack, frequency attack

Breaking Caesar cipher

- #1 Exhaustive key attack (Brute force approach)
- For msg in English – there are 26 keys, if you apply one after another on encrypted msg (C-1, C-2 ...), and observe txt, one of the transformed txt is readable.
- #2 Frequency analysis (Language characteristics)
- If you observe any long txt (article written in English), and count each letter's frequency, you find that letter E is appearing maximum times (125 times in an article of 1000 characters). Next is T appearing approx. 92 times.
- (i.e. if U is appearing max. times in encrypted text, it is actually E in msg. U – E = key!!!)

Frequency of single characters in English text



Caesar cipher is a substitution cipher (Mono-alphabetic)

- A letter is substituted by another letter from the same alphabet
- *Mono-alphabetic substitution*

- letters of the plain text alphabet are mapped on to unique letters throughout the entire message text

Returning back to the current World – ENISA THREAT LANDSCAPE 2023

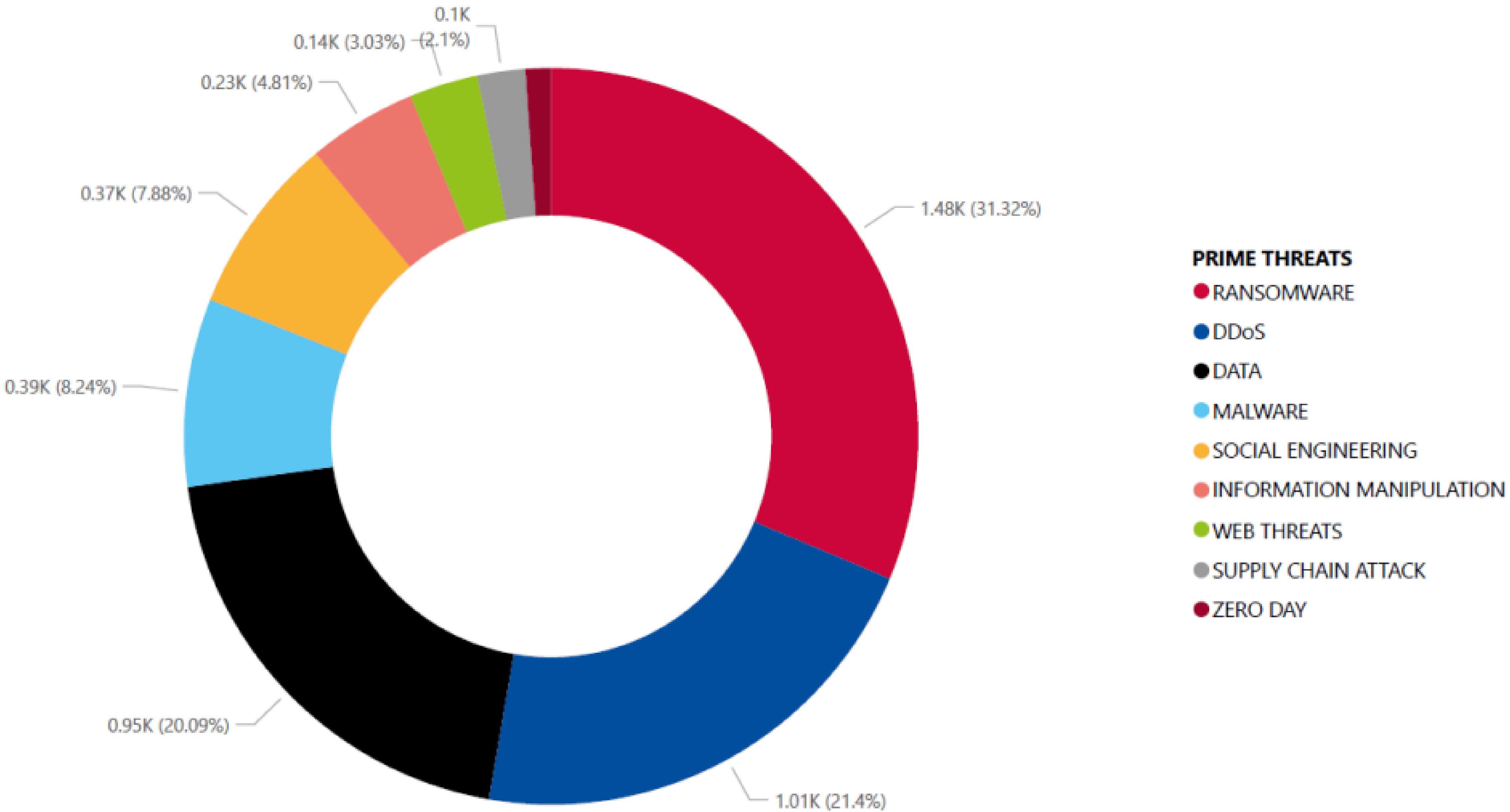
- Ref: The European Union Agency for Cybersecurity, ENISA Report (published in Oct 2023)
- ENISA is the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.
- Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.
- Applicable to India and the World

The prime threats identified

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats against availability: Denial of Service
- Threat against availability: Internet threats
- Information manipulation and interference
- Supply chain attacks

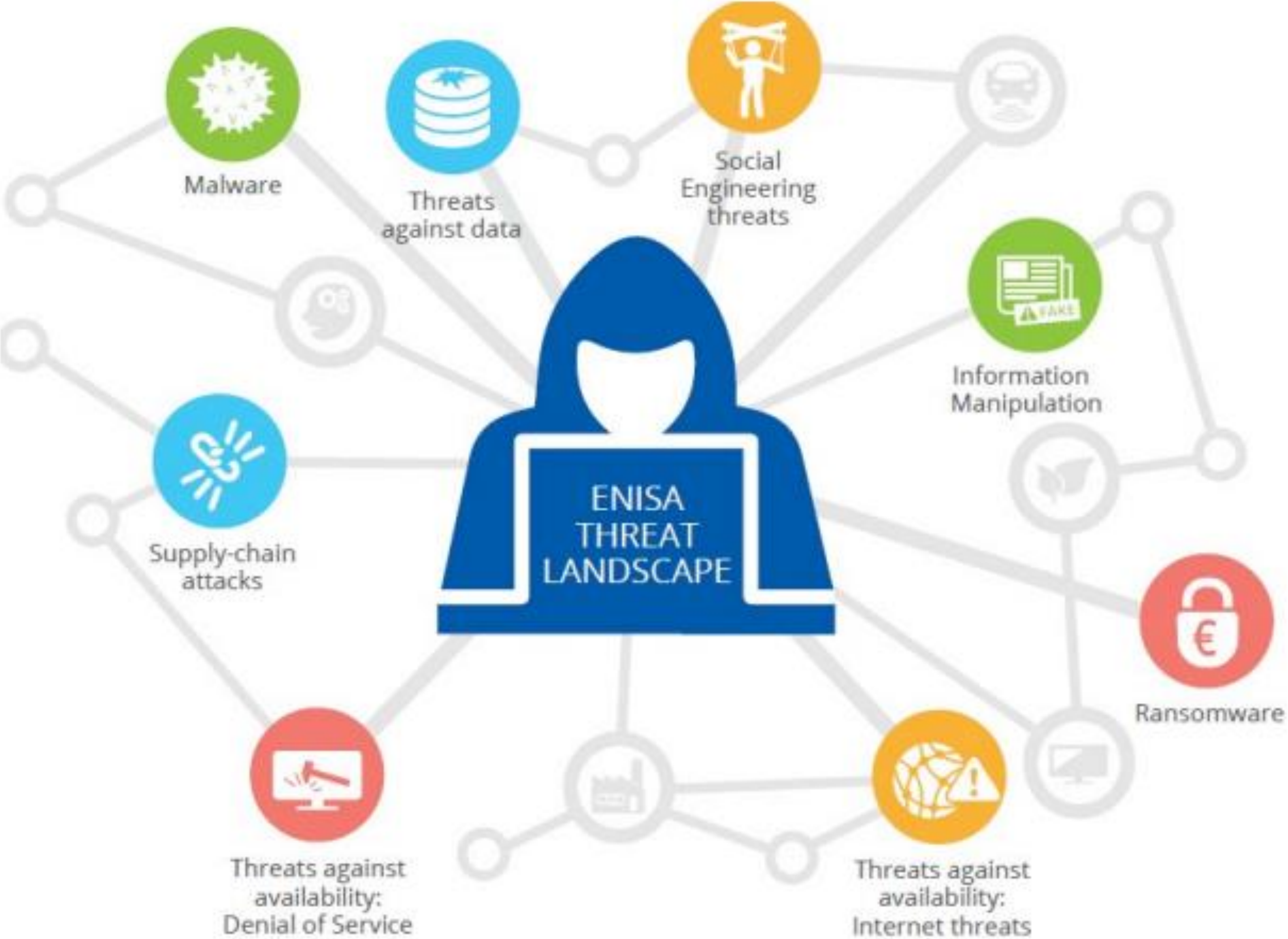
Most prominent attack vector

- DDoS and ransomware rank the highest among the prime threats, with social engineering, data related threats, information manipulation, supply chain, and malware following.
- A noticeable rise was observed in threat actors professionalizing their as-a-Service programs, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises.
- Cybercriminals increasingly target cloud infrastructures


0.1K (2.1%)
0.14K (3.03%)
0.23K (4.81%)
0.37K (7.88%)
1.48K (31.32%)
0.39K (8.24%)
0.95K (20.09%)
1.01K (21.4%)
PRIME THREATS
● RANSOMWARE
● DDoS
● DATA
● MALWARE
● SOCIAL ENGINEERING
● INFORMATION MANIPULATION
● WEB THREATS
● SUPPLY CHAIN ATTACK
● ZERO DAY

Sectors most targeted and affected

- public administration as the most targeted sector (~19%),
- followed by targeted individuals (~11%),
- health (~8%), digital infrastructure (~7%) and manufacturing, finance and transport.
- Information manipulation has been as a key element of Russia’s war of aggression against Ukraine has become prominent.


ENISA THREAT LANDSCAPE
Malware
Threats against data
Social Engineering threats
Information Manipulation
FAKE
Supply-chain attacks
Ransomware
€
Threats against availability: Denial of Service
Threats against availability: Internet threats

Key definitions

- Ransomware is defined as a type of attack where threat actors take control of a target’s assets and demand a ransom in exchange for the return of the asset’s availability
- Malware, also referred to as malicious code and malicious logic, is a term used to describe any software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity or availability of a system.

Examples

- Attack on Availability – ATM card (Enter wrong pin three times)
- Order Pizza for a friend (enemy?)
- Sending simultaneous multiple requests to server (e.g. g-mail)
- Password cracking program (as-a-service)
- Rainbow table (look up table of pre-computed passwords’ hashes)