General overview on ransomware attacks, their impact on societies worldwide and critical infrastructure

Edvardas Šileris
Head of European Cybercrime Centre

Threat Assessment

How ransomware affects society and critical infrastructure?

Threat Assessment Ransomware

Supply Chain Vulnerabilities

New Extortion Techniques

Motivational Shift

Initial Access Brokers

Ransomware as a Service

Shift in targeted systems

Critical Infrastructure

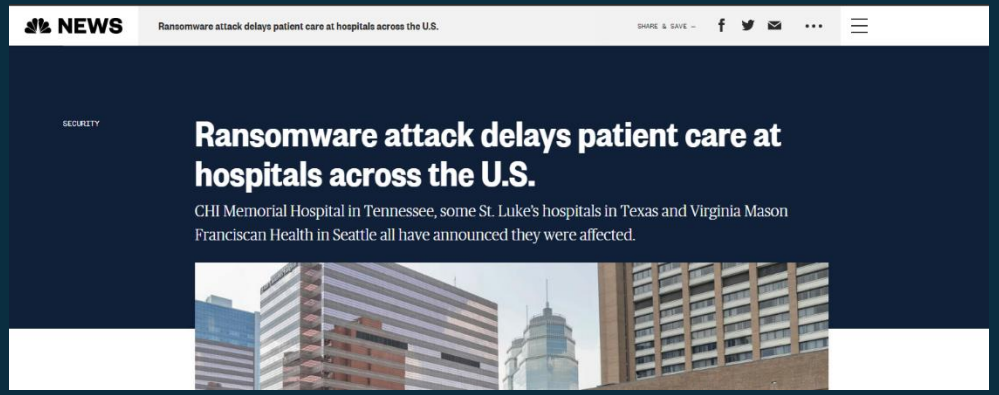
"Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens."

DG Home, https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en, 14/10/2022

What is happening in the world?

'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack

The infiltration of a major fuel pipeline is "the most significant, successful attack on energy infrastructure we know of."



Dutch supermarkets run out of cheese after ransomware attack

Computer giant Acer hit by $50 million ransomware attack

Tomorrow's headline:
An even bigger ransomware attack

Recent Operations

Operation 5th Element

Operation investigating ransomware attacks against critical infrastructure

Cyber attackers illicit activities have affected victims in 71 countries

More than 50 foreign investigators including 6 from Europol were deployed

12 high-profile suspects linked to ransomware attacks worldwide targeted

Over USD 52 000 in cash was seized, alongside with 5 luxury vehicles

Operation GoldDust

RO authorities arrested two individuals on Nov.2021 suspected of cyber-attacks deploying the Sodinokibi/REvil ransomware. 5 other **suspects have been arrested in PL (1), KW (1), and KR (3)**

The suspects are allegedly responsible for 7.000+ infections, which in total pocketed millions euros in ransom payments.

Operation GoldDust involved 17 countries, Europol, Eurojust and INTERPOL.

The arrests follow the joint international law enforcement efforts of identification, wiretapping and seizure of some of the infrastructure used by Sodinokibi/REvil ransomware family, which is seen as the successor of GandCrab.

VPNLab.net Takedown

Action part of EMPACT security framework objective *Cybercrime - Attacks Against Information Systems*

All 15 servers disrupted and seized

100+

businesses identified as at risk of cyberattacks. Law enforcement worked with the potential victims to mitigate their exposure.

The information exchange was facilitated in the framework of the J-CAT

VPNLab.net

The VPN offered shielded communications and internet access. Law enforcement took interest in it after multiple investigations uncovered criminals using this service to facilitate illicit activities such as malware distribution and ransomware attacks.


POLIZEIDIREKTION HANNOVER
Staatsanwaltschaft Verden
POLITIE
THIS DOMAIN HAS BEEN SEIZED
Since 17 January, 2022
International law enforcement, under the leadership of the Police Headquarters Hannover and the Verden Public Prosecutor's Office (Germany), has seized the domain vpnlab.net.
This service provided a platform for the anonymous commission of high value cybercrime cases, and was involved in several major international cyberattacks. This seizure follows a long-running international investigation by authorities in Germany, The Netherlands, Canada, the Czech Republic, France, Hungary, Latvia, Ukraine, the United Kingdom and the United States.
Law enforcement has now gained access to the vpnlab.net servers and seized the customer data stored within. The investigation regarding customer data of this network will continue..
VPNLA
NCA
National Crime Agency
POLICIJA
EUROJUST
EUROPOL

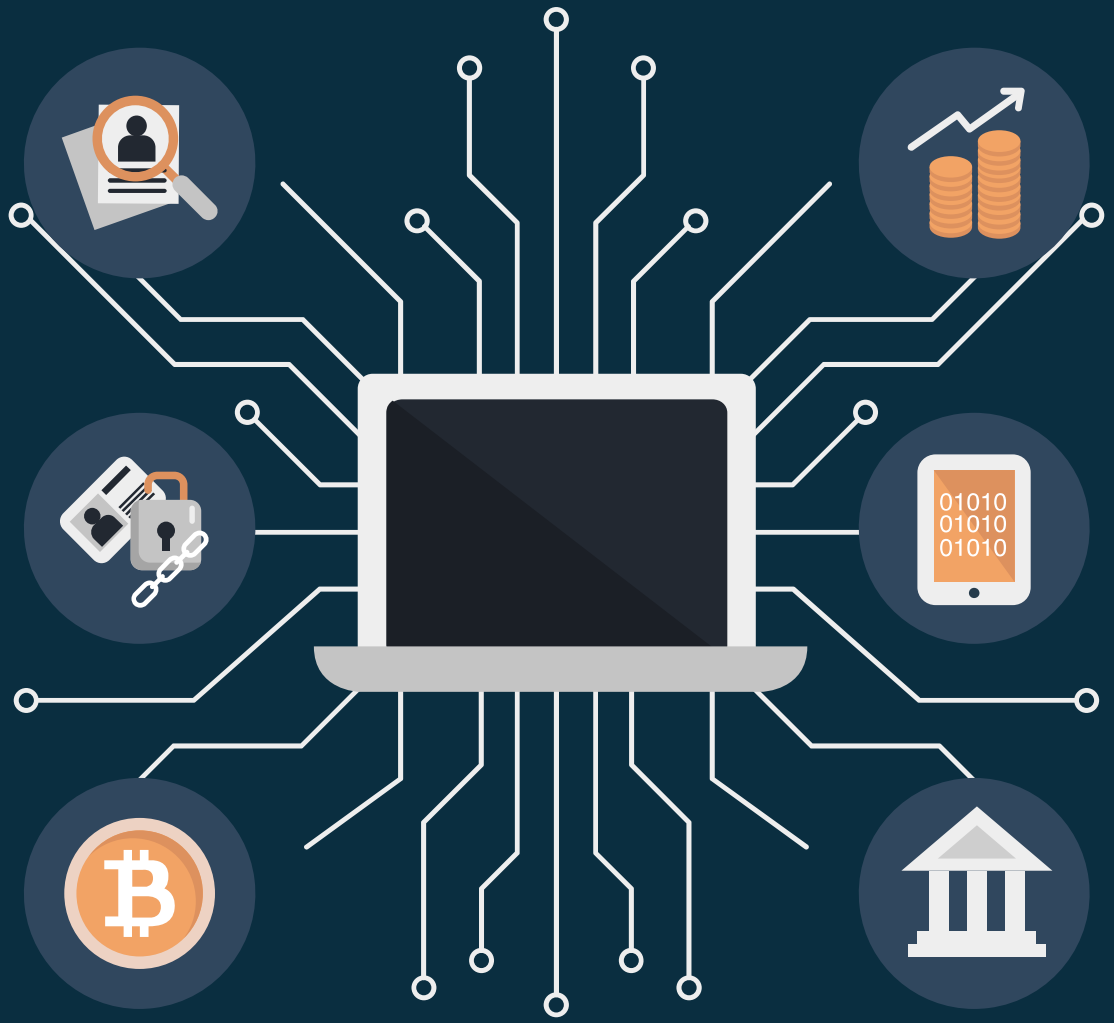
International Ransomware Response Model (IRRM)

J-CAT – EC3 International Ransomware Response Model (IRRM)

Experiential learning from hundreds of high-profile ransomware and facilitators investigations supported by EC3 since 2013 and J-CAT since 2014

Continuous proliferation & sophistication of ransomware threats since the 1980s

Mapping of existing cross-border ransomware initiatives (operational, tactical, strategic, prevention, PPPs)



20 Sept 2021 Brainstorming Workshop EC3-J-CAT

New international LE model based on the anatomy of a ransomware attack, different investigative avenues and the necessary response measure to thwart ransomware from a LEA standpoint

The new multi-faceted model aligned with and mainstreamed within EMPACT, US-EU Ransomware Taskforce, G7, US Counter Ransomware Initiative, etc.

EUROPOL EC3 European Cybercrime Centre | JOINT CYBERCRIME J-CAT ACTION TASKFORCE

Thank you for your attention

Any questions?

www.europol.europa.eu