Ο αντίκτυπος της ΤΝ στον Κυβερνοχώρο: Βεβαιωθείτε ότι η πρόοδος προστατεύεται

AI's Impact on Cyberspace: Ensure progress is protected

George Christou
Corporate Channel
Development Manager

Digital Security
Progress. Protected.

The importance of data feeds in AI

- Knowledge based
- Data feeds
- Machine “Training”
- Outcome

AI & Machine Learning

ESET LiveGrid®
(Cloud Reputation)

Human Expertise

ESET LiveSense®
Multilayered security technology

How AI is becoming a threat

- Evolution with Genetic & Automation algorithms
- Clever ways in bypassing intrusion detection or evade security mechanisms
- Cleverer and more creative Scams
- Automated and faster collection of data
- Faster and smarter creation and evolution of malware
- Increasing threats and frequency of attacks in general

Sandworm APT Group Overview

Reference Names	Sandworm Team (Trend Micro) Iron Viking (SecureWorks) CTG-7263 (SecureWorks) Voodoo Bear (CrowdStrike) Quedagh (F-Secure) TEMP.Noble (FireEye) ATK 14 (Thales) BE2 (Kaspersky)
Country	Russia
Sponsor	State-sponsored, GRU Unit 74455
First Seen	2009
Motivation	Sabotage && Espionage
Method	Zero-days, Malware, Spearphishing
Targeted Industries	Education, Energy, Government, Telecommunications

Cyber threat trends 2022-2023

On the rise: Cyber attacks on Critical Infrastructure


Sandworm uses a ne
version of ArguePat
attack targets in Uk
Europe's quest for
independence – and how
cyber-risks come into play
Soaring energy prices and increased geopolitical tensions amid the Russian invasion of Ukraine bring a sharp focus on European energy security
André Lameiras
James Shepperd
29 Mar 2022 - 11:30AM
Industroyer: A cyber-wea
that brought down a p
grid
welivesecurity BY ESET
HermeticWiper: New
data-wiping malware hits
Ukraine
undreds of computers in Ukraine compromised just ho
umber of Ukrainian websites
Editor
b 2022 - 10:32AM
Critical infrastruc
cyberattack for
you mi
CaddyWiper: New wiper
malware discovered in
Ukraine
third time in as many weeks that ESET researchers have spotted previously
aim at Ukrainian organizations
Menu
100 days of war in
How the conflict is
out in cyberspace
It's been 100 days since Russia invaded Ukraine, and we
the conflict
Industroyer2: Industro
reloaded
This ICS-capable malware targets a Ukrainian energy company
ESET Research
12 Apr 2022 - 11:28AM
I see what you did there:
A look at the CloudMensis
macOS spyware
Previously unknown macOS malware uses cloud storage as its C&C channel and to exfiltrate documents, keystrokes, and screen captures from compromised Macs
Marc-Etienne M.Léveillé
19 Jul 2022 - 11:30AM

NIS2 DIRECTIVE

What changes will (Network & Information Security) NIS2 bring?

Besides providing a wider and more detailed scope (see above), NIS2 will bring about the following changes/updates (compared to the original NIS which allowed much flexibility that led to vulnerabilities):

NIS2 security requirements

NIS2 Directive sets out a framework of strengthened security requirements. The measures shall be based on an "all-hazards approach" that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include "at least" the following:

(a) policies on risk analysis and information system security;
(b) incident handling;
(c) business continuity, such as backup management and disaster recovery, and crisis management;
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
(g) basic cyber hygiene practices and cybersecurity training;
(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
(i) human resources security, access control policies and asset management;
(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Compliance Deadline: 17 October 2024

The NIS2 Directive will apply to companies with over **50 employees** and over **€10 Million yearly turnover**. Critical infrastructure, which includes digital infrastructure in NIS2, is affected by the regulations regardless of size.

NIS2 will set the baseline for cybersecurity risk management in these industries and sectors:

- Transport (**E**)
- Energy (**E**)
- Banking and financial market infrastructure (**E**)
- Healthcare (**E**)
- Water supply and waste (**E**)
- Public administration (**E**)
- Aerospace (**E**)
- Digital infrastructure and digital service providers (**E**)
- Postal and courier services (**I**)
- Waste management (**I**)
- Food production, processing and distribution (**I**)
- Manufacturing of medical devices (**I**)
- Chemical and pharmaceutical production (**I**)
- Digital Providers (**I**)

All medium-sized and large organizations operating within these sectors fall under the NIS2's scope. These are classified to *Essential* (**E**) and *Important* (**I**) entities

Essential entities:

Must have a pro-active supervision and it is necessary to comply with NIS2 at all times.

Important entities:

Will be monitored after an incident of non-compliance is reported.

ESET Approach to Security

Products & Services

Deployment | Optimization | Health Check | MDR | Threat Intelligence | Training | Support

ESET PROTECT — unified cybersecurity platform

ESET Inspect — XDR-enabling component

IT Operations

Device Control | Mobile Device Mgmt. | Web Control

Firewall Mgmt. | HW & SW Inventory | Rogue Device Mgmt.

Security Management

Endpoint Detections | Automated Response | LiveGuard Detections

Cloud Office Security | Encryption | Multi-Factor Auth.

Security Operations

Threat Hunting | Incident Response | IOC Search

Forensics | Enriched Context | Detection Rules

ESET LiveSense multilayered technologies

UEFI Scanner | LiveGrid Protection | Advanced Machine Learning | LiveGuard Sandbox | DNA Detections | Network Attack Protection | Script Scanner & AMSI | Secure Browser

Ransomware Shield | Anti-Spam | Anti-Phishing | Anti-Scam | Exploit Blocker | Advanced Memory Scanner | Deep Behavioral Inspection | Brute-Force Attack Protection

Endpoints | Servers | Mobiles | Cloud Workloads | Mail / SharePoint | Integrations

Proactive Approach

- Endpoint Security & Threat Hunting
- Cloud Sandboxing
- Vulnerability & Patch Management
- Encryption
- Threat Intelligence
- Insider Threat
- Staff Trainings

Reactive Approach

- Cybersecurity Playbook
- Firewall
- Root Cause Analysis
- Block Unauthorized Access
- Disaster Recovery

“Cybersecurity is a race between the good guys and the bad guys,
and it's just a matter of who gets to the finish line first.”
- Mikko Hypponen

Thank You!

Digital Security
Progress. Protected.