NATO
OTAN

NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD

Proactive cyber defense through emerging technologies

VERSION 3 October 2024

Agenda

1. NATO and Cyber
2. Geopolitical threats
3. Dynamics in the ecosystem
4. Use your weapons wisely

Intro

Dr. Manfred Boudreaux-Dehmer

NATO Chief Information Officer

boudreaux-dehmer.manfred@hq.nato.int

NA

Washington Treaty

32 Member nations

Purpose is to guarantee freedom and security of its members through political and military means

Cyber at NATO

Embedded in NATO’s core tasks

Threats are increasing in frequency and sophistication

Cyber is a military domain

Focus on

- Protecting our networks
- Conducting operations
- Helping Allies enhance national resilience
- Providing a platform for consultation and collective action

Geo

Russia

China

North Korea

Iran

Russia

800% increase of attacks immediately after invasion

Massive disinformation campaigns

China

Biggest global threat

40 “Advanced Persistent Threat” groups

North Korea

Wide-ranging financial activities (>$1B per year)

Iran

Increased threat tied to Iran and Hezbollah

National Cyber Security Centre

NEWS

UK and allies e
tactics of Russ

New advisory reveals evolving tac
as more organisations move to c

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENC

Home / Topics / Cyber Threats and Advisories / Nation-State C

Na

Chin
Advis

breadth, depth, and sophistication of the People's Republic of China (PRC) state-sponsored

CSO

Home • Industry • North Korea's state hacking program is varied, fluid, and nimble

by Cynthia Brumfield
Contributing Writer

North Korea's state hacking program is varied, fluid, and nimble

News Analysis
Oct 30, 2023 • 10 mins

North Korea's evolving and flexible hacking structure encompasses a wide range of malicious activity beyond stealing from cryptocurrency exchanges, fueled by a small but nimble cyber workforce.

Related content

News analysis
Three new advanced threat gr
organizations last year

ion and

ps
llah

al

ginning
are,
g

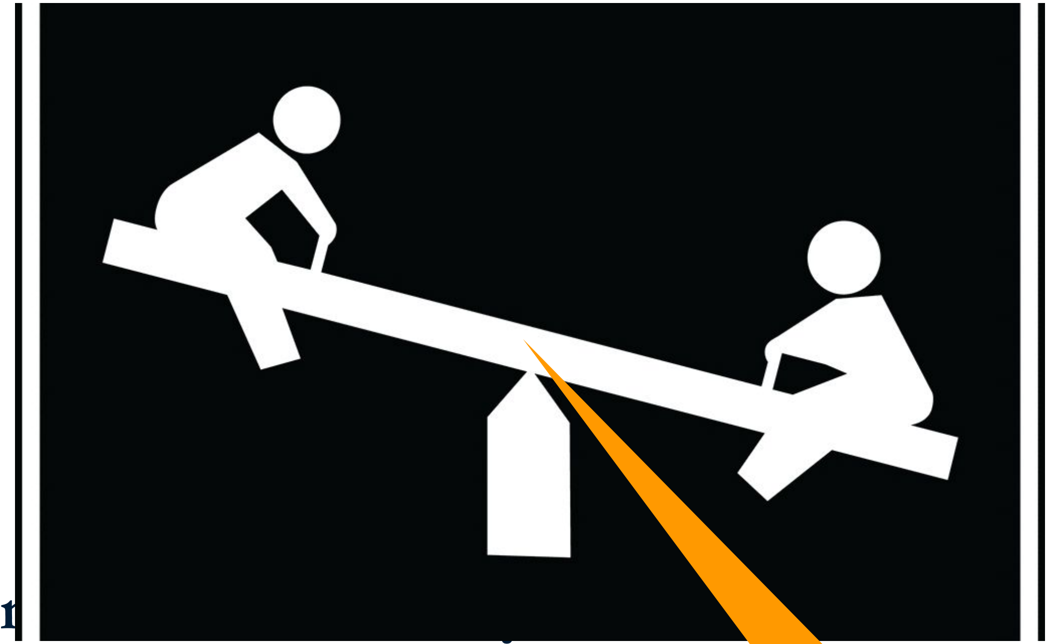
Directorate. 7/10, according to a report have been engaged in
of the last two and a half months, The report, which summarizes the main cyber attacks published by Israel's
intelligence, methods, and tools with each other. notes that most of these groups share

Thr

- Extortion
- [✓ Hacktivism/ Reputation]
- [✓ Identity Theft]
- Crypto Jacking
- Bullying
- [✓ Espionage]
- [✓ Political]

Threat Vectors

- Malware
- DDoS
- SQL-Injection / Cross-Site-Scripting
- Insiders
- Password Brute-Force
- DNS-Spoofing
- Man-in-the-Middle
- Social Engineering
- URL-Poisoning
- Ransomware
- Botnets



Equalize load distribution

Dy

Strong presence of asymmetry

- Attacker investment and risk = low
- Defender investment and risk = high

Method 1: Inflict damage on attacker

- Disruption or destruction – Offensive Cyber Operations (prerogative of nations – not private industry, not NATO)
- Public attribution – technically difficult, politically sensitive, and only marginally effective
- Sanctions – impose economical damage (nations)

Method 2: Deny benefits for attacker

- Risk awareness
- Knowledge of your environment
- Information hyper-triangulation
- Step-up defense through technology

Use your weapons wisely…

Risk awareness

Knowledge of your environment

Information hyper-triangulation

Step-up defense through technology

Know your environment very well: threat intelligence, ongoing comprehensive vulnerability assessments, risk register (and crown jewels) must be up-to-date

Need an automated Asset, Configuration, and Patching Management solution

“Put your SOC on steroids” through AI – SIEM needs to make sense out of billions of data points

- Spot anomalies and triangulate for attack vector and kill-chain detection
- Uncover (and learn from) anomalous user behavior

This needs two more slides…

Step-up defense through technology

LEARNING

- Consistent training of entire workforce – from junior analysts to senior leaders
- Use Adaptive Learning (AL) solutions

DATA CENTRICITY

- Imperative to tag data with classification (e.g. level of confidentiality)

IDENTITY ACCESS MANAGEMENT (IAM)

- Secure access to resources on-site or remote
- IM = who should have access (with MFA!)
- AM = access control at resource / object level

ZERO TRUST

- More of a mindset than a specific technology
- Not an excuse to “fill in the moat”
- Get serious about implementation

Step

Secure Access Service Edge (SASE)

- SD-WAN secure web gateways (cloud native)
- Cloud access security brokers supporting “Firewall as-a-Service” and Zero Trust network access

ADAPTIVE SECURITY

- Adjust and refine network layout to adapt to an incident (without human intervention)

ARTIFICIAL INTELLIGENCE

- Use AI – for SIEM (advanced correlation / triangulation)
- Use AI – for Adversary Emulation (the “pen testing on steroids”)

POST QUANTUM CRYPTOGRAPHY

- Risk to public-key cryptosystems with advent of Quantum Computers
- NIST introduction of Federal Information Processing Standards (FIPS) in August 2024
- Ready for prime time – not much time left…

Q & A