UNIVERSITY OF JYVÄSKYLÄ
Team Finland

Coach: Mr. Panu Moilanen
Herranen, T., Lampinen, K., Pasanen, E. & Söderholm, A-I.

SITUATION REPORT

05/18/2018
12:00

TO: Clementine Klein, Head of Cybersecurity at the Office of the High Representative of the EU for Foreign Affairs and Security Policy

FROM: Team Finland

SUBJECT: Coordinated Cyber Attacks Against EU Healthcare Facilities May Lead to Fatalities

Between 0800hrs - 0900hrs on 17 May, a series of ransomware attacks (thought to have been perpetrated by the ISIS-affiliated Al Durka group) caused regional healthcare outages in France and Belgium. The attacks have impacted seventeen individual healthcare facilities using vulnerabilities in products used by between 1/4 to 1/3 of all EU healthcare facilities. No fatalities have yet been reported, but casualties are expected to occur if the attacks continue.

The following key security concerns have been identified following these attacks:

i. Current operational capacity in affected healthcare facilities does not meet the minimum required levels by health authorities. This is currently impacting the national health systems in France and Belgium.

ii. Patient data availability, integrity and confidentiality in the European Union is vulnerable to continuing and/or similar attacks and may lead to casualties or fatalities. Some member states may be more vulnerable than others, in part due to lax adherence to existing regulation.

iii. Ransomware attacks as a funding mechanism for terrorist and online criminal organizations are on the rise. No uniform policy on payment of these ransoms exists. Critical infrastructure beyond healthcare in the EU may be future targets for such attacks.

iv. The online activities of terrorist and criminal organizations are contributing to civil unrest and the recruitment of well-placed, highly-skilled individuals.

SUPPORTING INFORMATION

The attacks were neither sophisticated nor advanced but worked because of a lack of digital hygiene in vulnerable medical devices. Technical indicators match previous attack patterns of the ISIS-affiliated "Al Durka group", but no-one has claimed responsibility for the attack. The systems directly at risk by this attack represent a significant share of European healthcare services. The risk of escalation is significant.

These incidents followed a separate ransomware attack against Berliner Verkehrsbetriebe, the main public transport company in Berlin, on May 15. The ransom statement points to an online criminal group "NovAnoN". BVG believes they were not targeted for this attack. The attribution is still under investigation. The attack in Berlin didn't compromise the transit system but did disrupt BVG's operations until the ransom was paid, highlighting the vulnerability of critical infrastructure throughout the EU.

These cyberattacks come amidst high tensions in several member states (NL, FR, GE, GR) following recent "Black Bloc" riots. NovAnoN played a key role in spreading the riots through fake news and social media activities. Continuing cyberattacks could lead to injuries, fatalities and/or physical damage that could in turn fuel additional riots in affected member states.

Both NovAnoN and Al Durka operate without regards to borders and are well organized. NovAnoN has succeeded in attracting well-placed, highly skilled individuals into its ranks as demonstrated by the recent arrest of Ivo Rusnok. Al Durka is actively seeking to recruit similar high-level talent, as well as upgrade its cyber capabilities.

UNIVERSITY OF JYVÄSKYLÄ
Team Finland

Coach: Mr. Panu Moilanen
Herranen, T., Lampinen, K., Pasanen, E. & Söderholm, A-I.

DECISION DOCUMENT 05/21/2018 8:00 A.M.

Cyber Policy Questions:

i. How is operational capability restored in affected healthcare facilities and the overall national health systems in France and Belgium?
ii. How is patient data availability, integrity and confidentiality ensured in the European Union? How are similar attacks, that may lead to casualties or fatalities, avoided in the future?
iii. What is the best approach to prevent ransomware attacks on critical infrastructure and services across the European Union?
iv. What steps can be taken to degrade the online capabilities of terrorist and criminal organizations?

Policy Alternatives:

Nation State Lead Approach

i. **Nation States (FR/BE):** competent authorities (e.g. National CERT /CSIRT) focus resources to lead coordinated incident response on a national level
ii. **National NIS authority in each affected Member State:** accelerate the NIS directive implementation schedule
iii. **European Council (Commissioner of Security Union):** encourage faster implementation of NIS directive by nation states; build deterrence by defence; use GDPR for financial penalties as required
iv. **French Ministry of Interior:** conduct EU-wide information campaign to combat fake news
National law enforcement agencies & Europol: run false flag operations to prevent recruiting of key individuals by terrorist and criminal organizations

Public/Private Cooperative Approach

i. **Competent authorities in affected Member States (e.g. National CERT):** establish joint task force with private sector security partners and manufacturers to steer incident response
ii. **ENISA (CERT-EU):** act as a single point of contact for information, tools and best practise sharing between the public and private sectors in health care
iii. **ECSO:** build and maintain relationships with the cryptocurrency community to counter criminal activity; promote innovative cybersecurity solutions for various critical infrastructure and services
iv. **Europol:** strengthen partnership with national CERT's and ENISA; facilitate information exchange of terrorist and criminal online operations

EU Lead Approach

i. **ENISA (CERT-EU), National CERTs & National health care services:** conduct relevant incident response
Europol/EC3 & National law enforcement: conduct relevant criminal investigation
ii. **CSU and relevant national ministers:** develop guidelines to secure patient data as part of NIS directive implementation; develop budget proposal for enhancing healthcare information security
iii. **EU Commission:** devote resources to accelerate NIS directive implementation; strictly enforce NIS directive compliance; implement EU level policy to forbid ransom payments
iv. **EU INTCEN & National CERTs:** actively share operational information on related incidents
EU Commision: Increase cooperation with non-EU states to fight on-line activities of terrorists

Hybrid Approach

i. **Nation states and National CERTs:** provide funding and coordination of private sector experts (and manufacturers) to restore capability and patch vulnerabilities
ii. **National CERTs:** coordinate vulnerability assessment and patching of all EU healthcare systems
iii. **National NIS authority in each affected Member State:** accelerate NIS directive implementation
EU Commision: introduce legislation to ban use of cryptocurrencies by government organizations
iv. **Talos Group:** lead a task force to coordinate amongst private industry to identify and coordinate dismantling of criminal cyber command and control infrastructures
European Centre of Excellence to Counter Hybrid Threats: establish social media task force to identify and counteract fake news that incites criminal activities
ENISA: lead and coordinate EU cyber "neighborhood-watch" activities

Analysis and Impact of Policy Alternatives (SWOT):

Nation State Lead Approach

S: centralized incident response on national level easier to coordinate than international efforts
W: national resources possibly insufficient; does not promote the responsibilities of affected facilities
O: highlights importance of NIS directive implementation
T: covert actions & false flag operations may cause negative publicity if/when revealed

Public/Private Cooperative Approach

S: collaborative approach leads to better engagement of key players
W: private companies' goodwill limited; patch management enforcement is challenging
O: promotion of innovative solutions through private/public collaboration
T: coordination amongst multiple players increases execution risk

EU Lead Approach

S: long-term solutions actively driven by EU
W: short-term response lead by EU not optimal due to current organizational setup
O: further restrict terrorist organizations & strengthen EU security
T: undermines the development of cyber capabilities in local organizations

Hybrid Approach

S: non-dogmatic approach (employs right leadership); aggressive actions deter future attacks
W: risk of negative reactions to disclosures of some initiatives; NIS implementation acceleration difficult
O: clear justification to increase EU cyber security capabilities (offensive, defensive)
T: limit potential innovation of cryptocurrencies; escalated and/or violent reactions by criminal/terrorist orgs

Recommendation and Justification:

*Team Finland recommends the **Hybrid Approach** for the following reasons:*

- appropriate level of response to current severity of incidents
- maintains leverage by targeted actions on short, medium and long term goals; considerable potential to address any future escalation
- encourages participation, cooperation and development of all member states
- minimizes moving parts; clarifies actions and corresponding responsibilities in line with existing organizational mandates
- minimizes need for centralized or reworked communications; enables each organization to communicate within existing frameworks and capabilities
- future attacks are deterred by cooperative actions amongst private, national and EU organizations

UNIVERSITY OF JYVÄSKYLÄ
Team Finland

Coach: Mr. Panu Moilanen
Herranen, T., Lampinen, K., Pasanen, E. & Söderholm, A-I.

DECISION DOCUMENT	06/19/2018 9:00 A.M.

Analysis of the situation

Between June 15th and June 17th, NovAnoN has conducted a series of ransomware attacks against healthcare facilities leading to at least 10 deaths and overwhelmed healthcare services in France, Belgium, Austria and the Netherlands. Well known vulnerabilities that were several years old remained unpatched and enabled these attacks. They now threaten to spread across the EU and claim more lives.

Cyber Policy Questions:

1. How to protect human life in areas impacted by ransomware attacks?
2. How to prevent future ransomware attacks on EU healthcare facilities?
3. How to dismantle NovAnoN?

Policy Alternatives:

Member State Cooperation

1. **Member States**: declare a state of emergency to enable engagement of relief organizations and deploy military medical assistance to shore up the resourcing of affected facilities
2. **National CERTs**: drive coordination and best practice information sharing to lead pre-emptive actions such as patching known vulnerabilities, isolating unpatched systems, etc.
3. **National Heads of State**: designate NovAnoN as "an armed group" to petition the UN Security Council for relief, invoke article 5 with NATO for a cooperative response, and/or deploy the Member State's own military and intelligence services

NATO led

1. **Foreign Ministers of affected states:** invoke article 4 of the North Atlantic Treaty to underline the threat to their security, send a clear political message on the seriousness of the situation, and enable discussion on defence of state critical infrastructure against this new type of adversary
2. **NATO CIRC**: share cyber situational awareness information to enable identification of penetrated healthcare networks and enable focused, pre-emptive cyber security measures
3. **Affected member states:** invoke Article 5 and use the combined cyber-capabilities of the alliance of member states to unmask and destroy NovAnon

EU Lead Approach

1. **Council of the European Union**: approve disaster funding to support operational capability of healthcare facilities affected by the ransomware attacks
2. **ECSO**: launch standardization guidelines for security in healthcare, develop related education, training and certification; develop PPPs with consortiums such as the Talos Group to dismantle cybercriminal command and control infrastructure
3. **Europol**: conduct law enforcement and intelligence operations, including cyber and human intelligence operations, in conjunction with member states to unmask and destroy NovAnoN

Hybrid Approach

1. **Affected Member States:** declare a state of emergency to enable engagement of relief organizations and deploy military medical assistance to shore up affected facilities
2. **Foreign ministers of affected states:** invoke article 4 of the North Atlantic Treaty to underline the threat to security, send a clear political message of the serious of the situation, and enable discussion on how to jointly defend state critical infrastructure against this new type of adversary
   NATO CIRC: share cyber situational awareness information to enable identification of penetrated

healthcare networks and enable focused, pre-emptive cyber security measures

3. **INTERPOL task force**: conduct law enforcement and intelligence operations, including cyber and human intelligence operations in conjunction with member states to destroy NovAnoN

Analysis and Impact of Policy Alternatives (SWOT):

Member State Cooperation
S: centralized response on the national level provides faster action and is easier to coordinate; designation of NovAnoN as an "armed group" enables a wider range of legal responses
W: national resources alone are insufficient; requires cooperation and international engagement for any real teeth; potential overreach (Article 5 and UN Security Council)
O: engage and build meaningful working relationships on cyber security issues with key international organizations (NATO, UN Security Council)
T: designation of NovAnoN as an "armed group" increases their visibility and reputation, possibly strengthening them

NATO led Approach
S: strong political, industrial and military capabilities brought to bear on the crisis at hand
W: NATO action might not see tangible results, undermining its credibility; Russia might feel threatened by NATO activity and take counterproductive action
O: NATO can move from talks and planning to a more action based policy; provides the means to use resources of other member states
T: NATO could become a larger target of cyber-criminal activities; potential misalignment amongst member states due to expansion of the NATO mission

EU Lead Approach
S: collaborative approach; short-term funding to aid affected facilities; unified standards on cyber security in health care
W: collaboration could lead to insufficient investment in security by individual member states
O: increase diplomatic collaboration amongst the member states on cyber security issues
T: further damage to EU credibility if tangible results are not seen

Hybrid Approach
S: utilizes both cyber and real world initiatives to resolve the issues at hand
W: lacks centralized, dedicated mechanism to tackle NovAnoN
O: enhance the role of NATO and enable it to address this new type of threat
T: NovAnoN enhances its reputation and visibility, enabling it to grow

Recommendation and Justification:

*Team Finland recommends the **Hybrid Approach** for the following reasons:*

- utilizes both cyber and real world initiatives to resolve the issues at hand
- unlocks the use of military capabilities in cyberspace without escalating into armed conflict
- minimizes the moving parts; provides initiatives in line with existing organizational mandates