Competition Instructions

Your team will take on the role of experienced cyber policy experts invited to brief the European Union Agency for Cybersecurity, ENISA (formerly European Network and Information Security Agency), which has been called to address an evolving cyber crisis. For the purposes of this exercise, ENISA is made up of European leaders in cyber security policy (including heads of state, heads of government, ministers of defense and foreign affairs, directors of intelligence services, and representatives from the private sector).[1]

This briefing document contains fictional information on the background and current situation involving an international cyber crisis seriously affecting the telecom infrastructure and services in a Member State of the European Union. The incident notionally takes place in April and May 2024. The scenario presents a fictional account of developments and both public and private reports on the international cyber crisis.

The parties to this fictional international cyber crisis are:

- Tango Inc;
- Titan Communications;
- The European Union;
- ENISA – the European Union Agency for Cybersecurity.

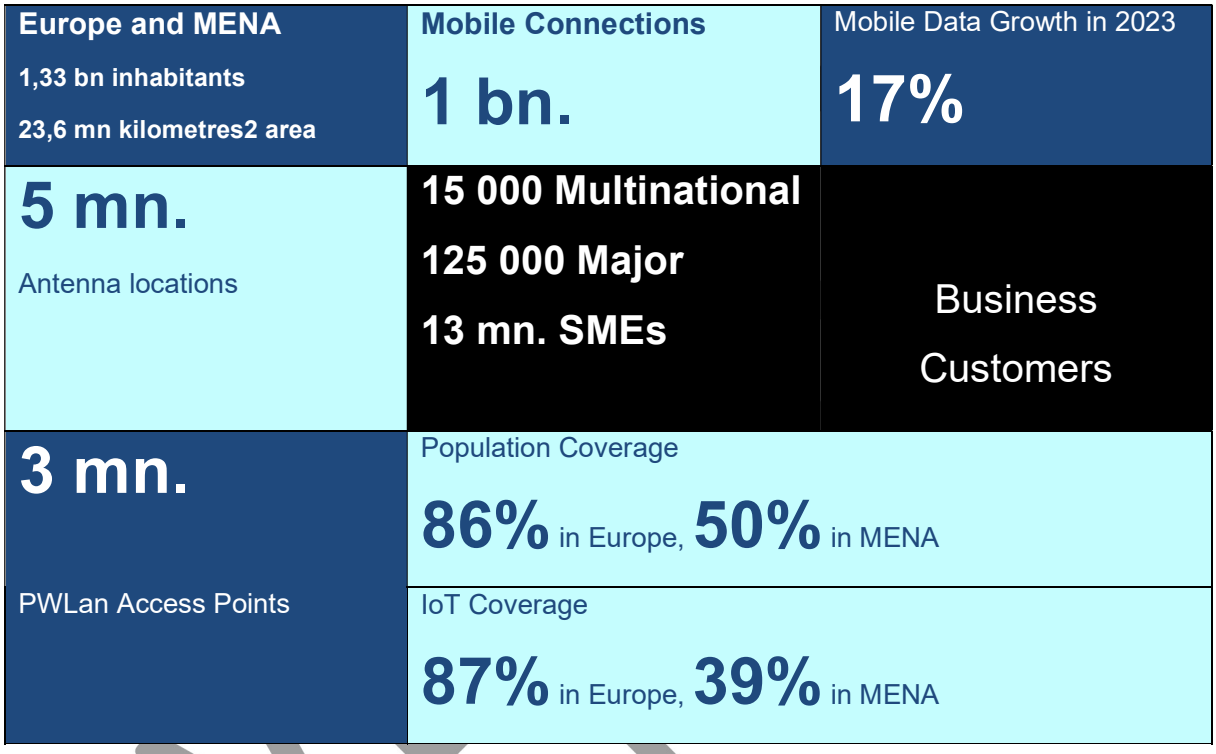
Tango Inc

Tango Inc has developed a product which combines a social media application, multiple mini-swarm drones with high-resolution cameras and built-in AI, that enables the user in real time to present his/her perceived reality. What makes this a success, is that this perceived reality can be shared with user's followers. Furthermore, everyone that buys this product will be part of a gamification/scoring system that, depending on how many followers a user has, brings the user higher on the charts. The user is incentivized to be high on the chart as this enables the user to free travel, globally, and uncover new areas. However, voices of concern are raised from various Western-intelligence agencies of the likelihood that the Tango Inc is linked to the country's "State Intelligence Agency." The concerns are that each user of this new product could be a potential spy. Furthermore, this new product is being classified as "dual use" technology. Finally, telcos *(should define)* responsible for the underlying technological infrastructure have raised concerns that because each product comes with six mini-swarm drones, there's a likelihood this will heavily burden the underlying technology in a crisis.

[1] The Political and Security Committee in reality is made up of EU Ambassadors representing their countries. More information: https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-security-committee/

Titan Communications Titan Communications is the largest company providing telecommunication services, IT and entertainment services in the Europe and MENA-region. The company has some subsidiaries active in the MENA-region. Titan Communications not only offers residential customers an extensive range of TV channels, mobile telecommunications services, and IT services, it also provides services to the EU, Governments of Member States, and business customers. Furthermore, Titan Communications is currently rolling out 5G infrastructure as demands in bandwidth are expected to increase. Figure 1 provides some figures.

Figure 1. *Titan Communications statistics of span, connections, and growth.*



Titan Communications is also classified as critical national infrastructure (CNI) in many European countries and MENA-region countries. 15 years ago, many multinational networking and telecommunications companies existed. Due to rapid technological advancements and an aggressive market competition, many mergers and acquisitions have occurred leaving to a handful of companies with global footprints left.

ENISA

In the universe in which this exercise is situated, ENISA, has been elevated to the EU-agency that drafts, develops, and implements Cybersecurity policy. The agency is also responsible for EU Cyber Defense, which consists of defensive cyberspace operations and offensive cyberspace operations. In an international cyber crisis, the organization holds significant authority on Cyber Defense. The organization can submit requests to the Member States to generate cyber effects through offensive cyberspace operations. The offensive cyber capability lies within the Member States, and offensive cyberspace operations are conducted only after a request to generate effects is submitted.

The Political and Security Committee of the EU

The Political and Security Committee (PSC), is a body of the *Council of the European Union*. As such it upholds a consensus-based approach amongst member state representatives to devise pan-European responses to potential crises.

The PSC is responsible for the EU's Common Foreign and Security Policy (CFSP) and the Common Security and Defense Policy (CSDP). The Committee therefore actively:

- monitors the international situation;
- recommends strategic approaches and policy options to the Council;
- provides guidance to EU crisis entities such as the Committee for Civilian Aspects of Crisis Management (CIVCOM), the European Union Military Committee (EUMC), the European Union Institute for Security Studies (EUISS);
- and ensures political control and strategic direction of crisis management operations.

The PSC meets at least twice a week to keep track of the international situation. In a crisis, the PSC can hold significant authority. The Council may authorize decision-making capabilities to the Committee throughout the duration of a crisis management operation. One of the ways the PSC can exercise this authority is to adopt EU Decisions under the CFSP framework. EU Decisions are a specific type of EU legislation which are only binding on the specific Member State or entity to which they refer.

Also of note is that, at this moment in time, **all European states** are facing dramatically increased healthcare demands as a new virus, ALPHA-24, spreads across the European continent. This highly infectious respiratory disease was originally identified in Kusandra, a small fictional country in South East Asia in January 2024, before spreading uncontrollably across the world and being declared a pandemic in late March 2024. Europe in particular is preparing for a 'first wave' of infections and hospitalizations, with the vast majority of member states imposing some form of national lockdown or social restrictions. Some hospitals are already starting to reach maximum capacity.

Finally, the Russian-Ukraine war that started on 24 February 2022 is still ongoing. The operational tempo in the war changes due to weather conditions and related implications on military vehicles. However, the cyber attacks have seen a consistent level of engagement. Cyber operations have included distributed denial of service attacks (DDoS), ransomware attacks to support the war, destructive attacks, and cyber-enabled disinformation operations. In parallel, new AI-driven language models have improved rapidly. ChatGPT has evolved over the past two years to include improved language models. Threat actors are looking for ways to access the models and use them to impersonate world leaders, to conduct spear-phishing-attacks, and for monetary gain.

In this universe, the Council of the EU has authorized the PSC to choose a course of action on behalf of the EU to ensure Europe's security, including in telecommunications. The ALPHA-24 pandemic has been classified as a threat to the Union and so is a PSC mandated issue. In this scenario, the PSC is made up of European leaders (including heads of state, heads of government, ministers of defense and foreign affairs, directors of intelligence services, and representatives from the private sector), whereas in reality the PSC meets at the EU-ambassador level. In addition, for the purposes of this exercise, ALPHA-24, a disease much like the COVID-19 circumstances, nations around the world face extreme challenges while responding to the novel and fictitious ALPHA-24 in this scenario. All other political and security concerns reflect the EU's actual, real-life situation.

The Exercise

Your team needs to provide information on the full range of policy response alternatives available to respond to this crisis and present recommendations to ENISA. You are to consider as facts the following pages and appendices in formulating your response.

You will use the fictional scenario material presented to perform three tasks:

1. **Written Policy Brief:** Write a 500-word brief discussing the key elements and security concerns that the task force must understand. The written task is meant to not only test your team's ability to summarize the scenario, but more importantly to explain the reasons and confidence levels behind your analysis of the key issues and implications of the ongoing international cyber crisis. The 500-word Written Policy Brief is to be sent through email to cyber-competition@gcsp.ch by LATEST 29 MARCH 2023 at 2359 o'clock GENEVA TIME. Late submissions may receive a penalty.
2. **Oral Policy Brief:** Prepare a ten-minute oral presentation outlining possible policy options and recommending one to the task force.
3. **Decision Document:** Teams will also be required to submit a "decision document" accompanying their oral presentation at the beginning of the competition round. The decision document must be submitted to cyber-competition@gcsp.ch by LATEST 1700 hrs. Geneva time, 12 April 2023. The "decision document" will be maximum one page outlining the team´s policy response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation. Judges will be given only 2 minutes to read the document before the presentation begins.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- **Don't fight the scenario**. Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- **Think multi-dimensionally**. When analyzing the scenario, remember to consider implications for other organizations and domains (e.g., private sector, military, law enforcement, information operations, diplomatic, etc.) and incorporate these insights along with cyber security.
- **Be creative**. Cyber policy is an evolving discourse, and there is no single correct policy response option to the scenario information provided. There are many ideas to experiment with in responding to the crisis.
- **Analyze the issues**. The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various official publications from entities such as the European Union or derived from original news sources whilst others have been invented by the authors. All scenario content is intended for academic, simulation purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated or named organization, actual or fictional.

Briefing

From: ENISA

Re: Titan Communications concerned with its infrastructure not coping if Tango Inc launches its new product.

Date: April 10th, 2024

ENISA has established an international and multi-stakeholder task force to solicit policy solutions to respond to an evolving international cyber crisis. The task force is made up of national security advisors from the governments of European countries, representatives from European Union security and foreign policy agencies and as well as private-sector representatives.

Given the nature of this international cyber crisis, this group of European leaders wants to assemble a range of possible policy response alternatives before determining a course of action to announce in the next task force meeting **on 10 May 2024**. Your oral policy brief recommendations must analyze the possible strengths, weaknesses, opportunities, and threats of each proposed policy response alternative before recommending the one best course of action. To do so, you will apply your understanding of cyber security, national and international law, foreign policy, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

When generating each of your policy response alternatives, teams should at a minimum consider the following potentially conflicting interests at the national, EU and international level. These are provided as suggested starting points and are not meant to limit your policy responses.

Immediate Response vs. Delayed Response
What actions should be considered, if any, and by who? What actions should to be taken immediately after the incident versus those that should be taken later?

Government Response vs. Private-Sector Response
What actions should be led by the private sector in response to the reports and incidents and what actions should be taken under government leadership? Actions to consider may include public acknowledgements, preventive and pre-emptive defensive actions, and offensive actions.

Unilateral Response vs. Multilateral Response
Should there be a unilateral or multilateral response within Europe? What about international organizations like the United Nations or NATO?

Direct Response vs. Indirect Response If action is to be taken, should it be a direct or indirect response to the incident? Should those responding act in secret, or reveal their cyber capabilities? Should no action be taken?

Additionally, this Intelligence Brief is accompanied by several documents that may assist your team in preparing its policy response alternative recommendations for the task force:

Appendix 1 – Industry Press Release.

Appendix 2 – Op-Ed: Top Titan Communications CEO Personal Comment.

Appendix 3 – Interview with Top Titan Communications CEO.

Appendix 4 – Internal Government Briefing.

Appendix 5 – Twitter feed from a reporter.

Appendix 6 – Confidential Intelligence Report on Breach of Security.

Appendix 7 – Intercepted communication.

Appendix 8 – Corporate Risk Assessment Survey

Appendix 9 – Internal Memo Titan Communications

Appendix 1 – Industry Press Release.

TANGO INC

01 January 2024

AI-Powered Immersive Technologies for Expanding Your World

Tango Inc is proud to announce the release of AI-powered immersive technologies that will expand your physical world. The product combines our own social media application, multiple mini-swarm drones with high-resolution cameras, and built-in AI. This enables you, in real time, to expand your reality and turn it into how you perceive it.

No longer will you have to experience car queues, smog, or grey-dark days. Through our AI-powered tools, you can choose pre-designed worlds or items to remove your gloomy days. If this is not enough, you can create your own worlds or expand your current one. You no longer need to pay expensive flight tickets to visit your favorite places! Say that you still want to visit your favorite places, but you are deterred due to costs, how about sharing your world with others? That's right! You can also share your customized world to your family, friends, and colleagues!

The more likes and followers you get, the higher up in the score-ladder you will be. Every month, the top three on the score-ladder will receive a paid trip to a chosen destination! Now, it is possible for you to combine the best of what immersive technologies can offer, the world, and your mind.

Appendix 2: Op-Ed

The Urgent Need for Tech Giants to Share the Burden of Network Infrastructure Costs

12 February 2024

Dear valued customers and stakeholders,

As the CEO of Titan Communications, I want to raise a critical issue that affects not only our company but the entire telecommunications industry. The rapid growth of tech giants such as Google, Facebook, and Amazon have led to a surge in internet traffic that our networks were not designed to handle. While we welcome innovation and progress, the burden of maintaining a telecoms network advanced enough to support tech giant products and services cannot be borne solely by telecoms companies.

One of the main points of conflict in this regard is the lack of contribution from tech giants towards the costs of network infrastructure. Unlike telecoms companies, tech giants are not subject to the same regulations and fees for using our networks, yet they benefit greatly from them. This creates an unequal and unsustainable situation that threatens the integrity of the entire telecommunications industry.

From a cyber security perspective, the situation is even more concerning. Recently, we conducted lab tests on a new service by Tango Inc, and the results were alarming. The service was taking more broadband traffic than the Tango Inc had stated, and we suspect that their devices may have security vulnerabilities., we urge Tango Inc and other tech giants to be transparent about their usage of our networks and contribute their fair share to ensure their products and services can operate safely and efficiently.

As cyber security threats become more sophisticated and pervasive, it is crucial that we maintain a robust and resilient telecommunications network. This requires a shared responsibility and investment from all stakeholders, including tech giants. We urge them to recognize the importance of network infrastructure and contribute their fair share towards its maintenance and development.

In conclusion, it is time for a fair and equitable sharing of the burden of maintaining our telecommunications networks. Tech giants must acknowledge their responsibility to contribute to the costs of the infrastructure they depend on, or risk undermining the very foundation of our industry. Let us work together to ensure a secure, reliable, and sustainable telecommunications network for all.

Thank you for your attention.

Sincerely,

Jane Doe

CEO, Titan Communications

Appendix 3 – Op-Ed: Interview with Titan Communications CEO.

The Guardian

‘Teledodging’: the state of our networks

Jane Doe: “The infrastructure may not hold – millions may lose access”

Published: 03 March 2024

1,188

Telecommunication operators have concerns that networks may not hold when tech giants’ products have led to a surge in internet traffic. What are the implications of this? We discussed this and more with the CEO of Titan Communications, Ms. Jane Doe.

Interviewer: Good afternoon and thank you very much for accepting our invitation to this interview to discuss this product launch of Tango Inc, we read your op-ed in euro**news**. and are excited to hear more about the issue your company has been facing and its larger implications for larger security issues across the EU.

CEO: It's my pleasure, thank you very much for inviting me.

Interviewer: So, tell me about your company, trends, and challenges.

CEO: Well as you know we are Titan Communications, a telecommunications company that specializes in providing telecommunications services like Internet connection, entertainment services, and mobile solutions. We are the largest EU telecom operator operating in Europe and the Middle East and northern Africa region. We provide connection to 1.33 billion customers in a 23.6 Mn square kilometer area. In addition, we are providing the infrastructure so the people can do their finances, buy their groceries, and educate themselves. We are also providing businesses with the opportunity to do business to business work. These are just a couple of the things that our infrastructure helps people to do.

Interviewer: That's great to hear and indeed, you are helping a lot of people. What are your thoughts on Tango Inc’s latest AI powered immersive technologies product?

CEO: I think the product as such is very interesting. I mean just having the possibility to visit new places from where you're standing is very environmentally friendly. I mean you don't have to travel a lot if you decide not to travel and in essence your carbon footprint is 0. However, we have

some concerns. One of our concerns is that even though Tango Inc has stated that its proprietary protocol is very lightweight and will not require high bandwidth we believe it to be the opposite. Our concern lies within the fact that you have this software combined with six mini drones. Having six drones constantly whirling around you recording high quality 8K content isn't likely to consume low bandwidth. We believe all these technologies going on at the same time may cause service disruptions.

Interviewer: This is indeed a serious concern. What are your plans to address it?

CEO: We're currently in talks with the Tango Inc to work out a solution that does not lead to service disruptions. We have kindly asked them to provide more information about their proprietary protocol, we have asked them to do our own lab tests, but to no avail. Tango Inc has in multiple locations stated that we do not need to worry. However, we do worry because this could cause problems for our networks and in extension, our users. our internal discussions or that we must expand or investments and make the network more resilient. However, these investments cost a lot of money.

Interviewer: You mentioned earlier service disruptions, what do you think the impact could be?

CEO: Well, I mentioned that our users would suffer. However, the potential implications could be global in nature.

Interviewer: Can you please explain?

CEO: Well, it could have larger global implications. Also, because they're using a proprietary protocol, we are unsure about how safe it is, or what they may be sending. We have seen in the past how companies used proprietary software only to find out it was vulnerable and exploited by threat actors to conduct successful cyber attacks.

Interviewer: This is definitely a serious concern, and you seem to have a lot on your table. I wish you great luck in your future meetings with the Tango Inc. Thank you for speaking with me today.

CEO: Thanks for having me.

Appendix 3 – Internal EU Memo.

To: European Commission

Subject: Network Failure During Recent Product Launch

Date: 10 March 2024

Dear Commissioners,

I am writing to provide you with an overview of the recent network failure that occurred during a highly anticipated product launch. The failure resulted from a record high of 140 million requests per second that affected certain parts of the world infrastructure, causing a cascading effect, and disrupting network services.

The product launch was coordinated with a global scale server infrastructure deployment and a live stream of the launch event. The proprietary communications protocol used during the launch was designed to provide 100% privacy, indirectly improving security. However, the combination of the new protocol and loading balances in the underlying infrastructure caused a global DDoS attack.

The network failure affected several critical services, including emergency services, financial institutions, and government agencies in Belgium, The Netherlands, Germany, France, and Italy. We immediately launched an investigation into the incident and are working to identify the root cause of the problem.

We are also working closely with other affected countries to share information and coordinate our response efforts. We have reached out to relevant industry partners and stakeholders to ensure that they are aware of the situation and taking necessary precautions.

As this incident underscores, the security of our digital infrastructure is of utmost importance. We must continue to invest in the development and deployment of robust cyber security measures to protect against malicious attacks that can cause significant harm to our economy and society.

We recommend that all government agencies and critical infrastructure providers review their cyber security measures and take steps to improve their readiness and response capabilities. We also urge industry partners to take responsibility for the security of their products and services and work with us to prevent future attacks.

We will continue to keep you updated on the situation as it develops. If you have any questions or concerns, please do not hesitate to contact us.

Sincerely,

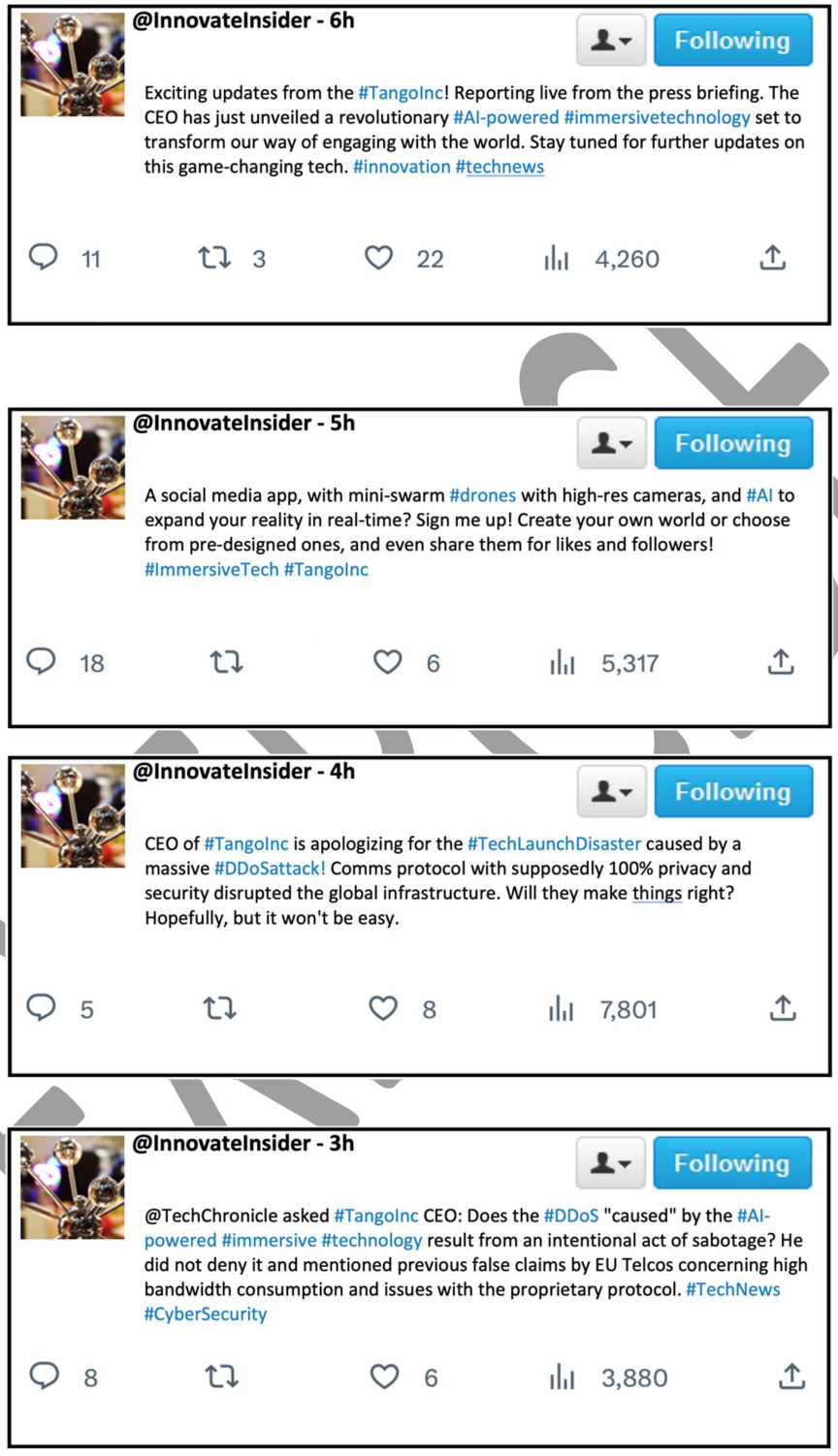
John BEŔEĊ

Head of Cyber Security

BEREC

Appendix 4 – Twitter feed from a reporter.

Date: 01 January 2024



Appendix 5 – Confidential Intelligence Report

FOR: EU's High Representative for Foreign Affairs and Security Policy

Subject: Breach of Security

Date: 05 April 2024

Threat Level: Severe

Type of Attack: Breach of Security, Network South

Hostile Actor: Unidentified

Threat Actor Language: English

Key Points

- On 1 April 2024, analysts discovered unusual activity that has been officially designated as a series of IOCs leading towards a likely DDoS attack on an EU network. Several recorded occurrences have been reported as IOCs with high confidence.
- IOCs that have been confirmed to date include high levels of unusual network traffic, increases in database read volume on several accounts, five cases of suspicious system file changes, and forty cases of anomalous logins. Further cases of IOCs are still being examined. Some of the identified unusual web traffic has indicated non-human behavior.
- It is highly likely that at least one security breach in the network has occurred. The total number of successful security breaches has not yet been identified, but analysts are continuing to discover additional types of IOCs to further confirm security breaches.

While the direct link between Tango Inc and State Intelligence Agency has not yet been officially confirmed, there is a possibility that individuals working in Tango Inc have national security interests and are affiliated with State Intelligence Agency's Cyber Espionage Unit with malicious intent.

In conducting further investigations into the breach(es), potential affiliation links between hostile state actors and Tango Inc will be examined. There is cause for concern regarding espionage activity stemming from Tango Inc employees and users; commercial activity of products manufactured, sold, and distributed by Tango Inc have the potential to include harmful software or other features for malicious intent.

The detection of various IOCs is especially concerning and will be further investigated by our analysts. We are flagging this ongoing development to pay special attention to the possibility of espionage among Tango Inc and the relation to user intent. Further products and services from Tango Inc will be analyzed in order to detect behavior indicative of espionage.

Appendix 6 – Intercepted communication.

INFORMATION CLASSIFICATION: SECRET

SUBJECT: Communication between hackers in a group chat

Date: 02 December 2023

KeepingCyber > Hi All, we're here to put together a plan of action against Tango Inc, and construct some ideas for targets. Let's make sure we keep any specific references to our individual skills in our other chat channels, to avoid any possible detection for ongoing surveillance on here.

Mousepad > Ready to get right to it. I've been following Tango Inc for some time now. It looks like based on their recent marketing schemes and overall business plan schedules, they're planning for a big product release, bigger than some of their most recent developments.

TryHDMI > Is now the time to plan something against them? Do we have any insider information on timing and if this is right to do right now? We can always wait for their next fiscal year.

KeepingCyber > We've done the background work and it looks like now is the time to plan this. We have a couple different options of where and how to hit them. Let's try to hit them hard and find the right kind of targets to hit.

TryHDMI > Are we thinking internal targets? What's the best move for the biggest impact?

Mousepad > Internal, external, hardware, software, many options, and targets exist. Some targets take longer to detect and are more likely to receive bad press once they've been discovered.

KeepingCyber > Sounds good! I think it's better to switch to the 'Tango Channel' and continue the discussion there.

Mousepad > @KeepingCyber, I saw what you did there: 'Tango Channel' hahaha.

Appendix 7 – Corporate Risk Assessment Survey

4 UR Safety CO

On 20 February 2024, **iffy**™ found a risk assessment survey from December 2020, conducted by one of the Big Two Consultancy firms. It reveals that organizations within information- and telecommunications technologies, networking, and software- and immersive tech (SIT) have shared major fears.

88% of the asked executives highlight fears for cyber attacks.

73% say that insider threats are growing. The main cause is believed to be that employees are directly contacted by ransomware groups asking them to execute malware in the companies they work at. Should they comply, the employee will get 20% of the ransom.

53% say that corporate espionage is increasing. The main cause is that Mergers and Acquisitions have been increasing. Companies are becoming bigger and bigger, and fewer. The competition is fierce, and any means are taken to collect information on a competitor for competitive advantages.

Appendix 8 – Internal Memo Titan Communications

Titan Communications

DATE: 8 April 2024.

TO: allStaff@titanco.com

Introduction

On 2 April 2024, a suspected DDoS attack and potential security breaches were detected on the network. This report aims to provide a comprehensive technical overview of the incident, the IOCs that were discovered, and the measures that the company is taking to address the issue.

Incident Overview

The attack was identified as a sophisticated operation that led to a critical failure of the load balancer. This resulted in high levels of unusual network traffic and rendered affected services unusable. The critical failure of the load balancer caused an outage of the entire service that it is responsible for distributing traffic. This resulted in degraded performance alternated with complete unavailability of the service for end-users.

This incident highlights the growing trend of DDoS attacks as more developers rely on the cloud to build and host their applications. In 2023, Titan Communications observed a 76% increase in the monthly number of events that were detected in April 2023, indicating an increase in DDoS attacks linked to Tango Inc's new Immersive Technology deployment, and their proprietary protocols.

The most common DDoS attack vectors detected were TCP SYN floods, UDP reflection, and DNS reflection attacks.

- TCP SYN flood is a type of Distributed Denial of Service (DDoS) attack where an attacker sends a large number of TCP SYN requests to a target server, but never completes the handshake process by sending the final ACK packet. The server keeps waiting for the final ACK packet, which ties up system resources and eventually leads to the server becoming unavailable to legitimate traffic. TCP SYN floods are simple and effective, and can be mitigated through various means, such as rate limiting, TCP SYN cookies, and firewall rules.
- UDP reflection is a type of Distributed Denial of Service (DDoS) attack in which the attacker sends a large volume of User Datagram Protocol (UDP) packets to a targeted server or network, with the source IP address of the packets spoofed to appear as if they are coming from the victim's IP address. The targeted server or network then sends a response back to the victim's IP address, flooding it with traffic and overwhelming its resources, causing it to become unavailable to legitimate users. The attacker can achieve a greater effect with less traffic by exploiting the amplification effect of UDP protocols such as DNS, NTP, or SNMP, which can generate large responses to small requests.
- DNS reflection, one of the oldest UDP reflection vectors, was the most common, accounting for 16.5% of all infrastructure-layer events detected. TCP SYN floods were the second most common at 13.8%.

These attacks attempt to reflect and amplify packets off legitimate services running on the internet, which overwhelms the ability of the application to process packets or establish new connections on behalf of legitimate users.

The most common application-layer attack observed was linked to Tango Inc's new Immersive Technology launch. This event was a significant cause of increased volumetric events detected in the relevant period, leading to infrastructure-layer attacks.