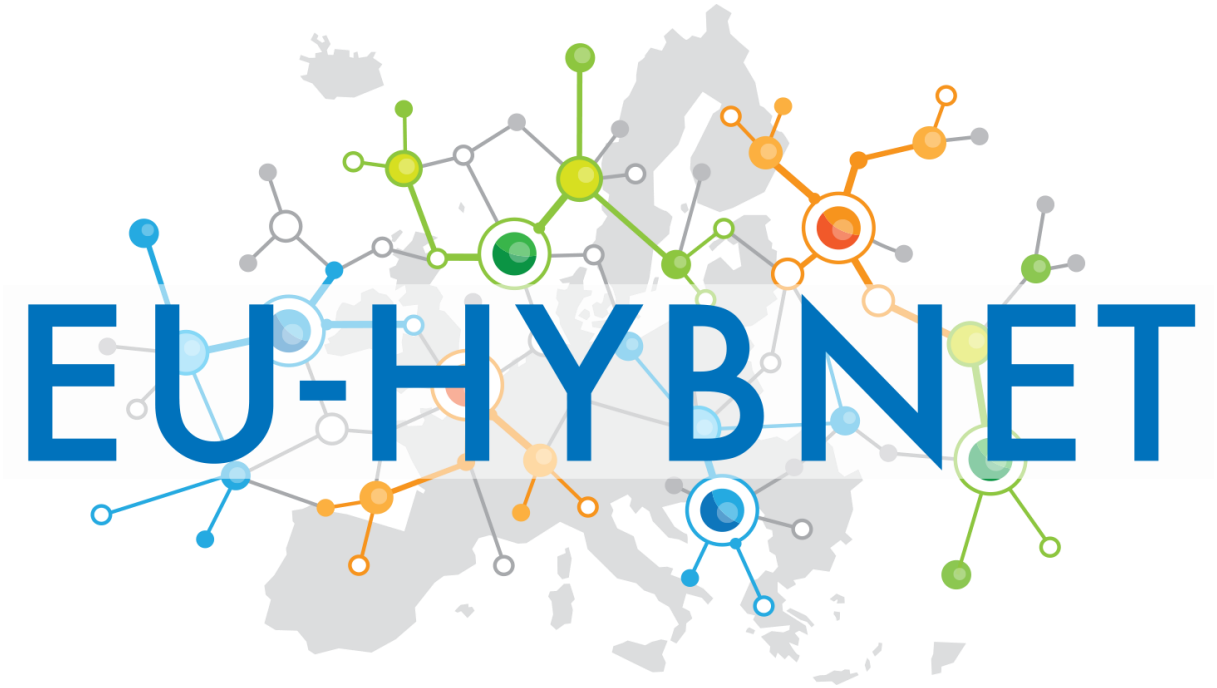
EUROPEAN POLICY BRIEF



Empowering a Pan-European Network to Counter Hybrid Threats

Fame on social media, a new currency of cybercrime?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

EU-HYBNET Policy Brief No 4 - Fame on social media, a new currency of cybercrime?

- The novel exposure of cybercriminal groups in the public space brings with it a brand-new set of challenges and opportunities
- From 2013 to the present, ransomware attacks have become more sophisticated, and cybercriminals have set up groups that work just like any company, diversifying its products and selling them to third parties
- The emergence of public dissemination channel claiming attacks, polling leaks and disseminating technical advice elicits commentary and publicity which creates a social media pressure
- State sponsored cyberwarfare on an unprecedented scale is an unexpected consequence of the Russian invasion of Ukraine
- The public attention that these attacks are getting, and the normalization of cybercrime as a valid, publicly lauded, even state sponsored activity is also attracting users from a younger generation
- A strong and fast answer to this new reality is needed, where technical expertise must go hand in hand with timely communication, flexible strategies to attract new talent and, above all else, a true information exchange platform at European level that can be used as a knowledge repository.

Introduction

EU-HYBNET project's principal objective is to bring together practitioners and stakeholders to identify and define their common requirements for countering hybrid threats by undertaking an in-depth analysis and prioritisation of gaps and needs. The project conducts research and highlights innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which will lead to creating a roadmap for success and solid recommendations for uptake, industrialisation, and standardisation.

This policy brief addresses the trend of democratisation of cyber operations, combining it with the availability of disruptive technology and fame acquisition strategies that individuals may display as determinants of cyber operations. The paper will analyse the reasons behind this new trend, and the opportunities and challenges that such exposure brings to law enforcement authorities and the research community.

Data and methods used

The policy brief was written together with EU-HYBNET Network member VOST Portugal. The analysis and recommendations are built on the EU-HYBNET 2nd Gaps and Needs workshop and the 2nd Future Trends Workshop results. EU-HYBNET's 2nd gaps and needs analysis had already identified that the power to harm systems, societies, infrastructures on a dire level had undergone a degree of democratisation. This finding was further addressed in the 2nd Future Trends workshop, which identified *instrumentalization of social networks* as one of the megatrends that will have most relevant hybrid threat implications in the mid-term future.

Main Findings

Cybercriminal groups have usually operated in the shadows as little was known about their operations, methodology, exploits and targets. The last 18 months have witnessed the creation of accounts on social media, and the creation of public channels in platforms like Telegram and blogs on the web, that work like official channels for dissemination of information, seamlessly producing viral information about cyber-attacks and exploits. The novel exposure of cybercriminal groups in the public space brings with it a brand-new set of challenges and opportunities. In August 2022, Lockbit cybercrime group said that anyone tattooing their logo would receive $1,000.00 in crypto currency. Photos of people with the tattoo started to emerge on social media a month later. Analysing this type of marketing stunt, Ohad Zaidenberg, Threat Intel Strategic Leader at AB InBEv, resumed this moment best:" Fame is their new currency." In October 2022, "Team One

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Fist", after claiming to have "silenced" Russia's GONET satellite network, wrote on Twitter: "it's critical to have good quality media releases as propaganda/psyops is even more important". Observation of the drivers of cyber operations, attacks and criminality suggests a higher degree of decentralisation, individualisation and a general distribution of capacities. This trend denotes the growing importance of group or individual fame strategies as activity determinants.

From Anonymous to RaaS

Since 2003, the word Anonymous is associated to an informal global group of hackers that use the internet to disrupt services provided by targets chosen by the majority of its members. High profile attacks, although not always technologically complex, have made Anonymous the first cybercriminal group to also be a global brand and media entity – in the sense that it also publishes content with an editorial consistency to it. Anonymous was born in a fringe social network, 4Chan, and used it to plan, discuss, and deploy attacks that aimed at disrupting, in any way possible the operations of the target.

While the group was targeting the Church of Scientology, PayPal, RIIIA, the US Justice Department and the FBI, the official websites of the Egyptian and Tunisian government during the "Arab Spring" and ISIS, following the Paris' terrorist attacks, other movements were exploring the possibilities given by the appearance of the deep web through Freenet, the thesis project of University of Edinburgh student Ian Clarke, who set out to create a "Distributed Decentralised Information Storage and Retrieval System.", that gave way to the appearance of the Tor Project, which was released in 2002 and launched a browser in 2008. With the creation of Tor, users could now browse the internet completely anonymously and explore sites that were deemed part of the "dark web." Far from the public eye, these groups started to specialize in cyber-attacks whose only aim was to make a profit from their illegal activity by stealing data and selling it in bulk on deep web forums. Ransomware attacks started to be a threat, even if its relevance - and weight on the total cyber-attacks - only took off with the appearance of cryptocurrencies, especially Bitcoin.

From 2013 to the present, ransomware attacks have become more sophisticated, and cybercriminals have set up groups that work just like any company, diversifying its products and selling them to third parties in what is known as RaaS (Ransomware as a Service). However, the majority of these attacks, and the groups behind it, stayed hidden until recently. The reasons for this are twofold: targets are reluctant to disclose attacks they've endured, and cybercriminals were not into the habit of disclosing their targets, methods, and profits.

The social media pressure

This obscurity created an attribution void that started to be exploited by newcomers to the cyber-criminality scene by bringing information out of the deep web forums to public social media and messaging platforms. Telegram channels and Twitter accounts started to publicize targets, making polls letting the community decide which leaks to publish first, and taking authorship of attacks. While the cyber security community was sceptical about the veracity of some of the announcements, the public at large, and general media outlets, started to connect high level cyberattacks, mostly ransomware, to certain groups with a presence in social media and public messaging systems.

The appearance of these dissemination channels, and the content they were publishing - claiming targets, exploits, and publishing leaks - turned some of these groups into social media stars, with a following and reach that started to shed some light on these groups' daily operations, attracting more attention, and creating the need to produce new content for these groups, which started to claim all kinds of attacks. While the cyber security community continued to be - even more - sceptical about some of the claims being publicly advertised, the media and the public at large started to publicize and widely share these claims. While reliable

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

data regarding the internal discussions of most of the groups is inherently difficult to access, it's fair to link the appearance of social media accounts and telegram channels connected to cyber criminal groups with an emerging need to correct, and claim authorship of, the claims made by others. These corrections, which were already being shared within the cyber security community, started to reach a wider audience via social networks, and these groups embraced the power of social media to disseminate information and recruitment. But the relevance of social media for cyber-criminals did not stop here. Social media channels are now being used to counter the victims assessment of attacks, as we've seen recently with the TAP Air Portugal breach, where the company's first reaction was to deny that any user data had been breached, only for the group behind the attack immediately exposing, on social media, personal data from the airline's clients.

State sponsored cyberwarfare

The Russian invasion of Ukraine created an unexpected epiphenomenon: state sponsored cyberwarfare, usually an even more covert activity, made it to the headlines when Ukraine announced the establishment of an "IT Army" that anyone could join on Telegram. This public announcement was rapidly followed by declarations of well-established cybercriminal groups, joining the cyberwar and by taking sides. Ensued a public race to claim the most attacks, the most targets and the most exploits. Public exchanges took place between some of the groups and "Anonymous" with the formers claiming ownership of some of the attacks "Anonymous" were publicly claiming. These exchanges, planned or not, consolidated some of these groups' social media accounts, and their dissemination channels, as rising stars on social media.

Challenges and opportunities

The novel exposure of cybercriminal groups in the public space brings with it a brand-new set of challenges and opportunities. This became clear when the infamous CONTI Group publicly declared their support to Russia only to find their whole structure and chat logs exposed on Twitter. Even if the origin of the leak is still not clear, the fact remains that due to this exposure researchers and law enforcement authorities got the opportunity to have a prime look at how the group was structured, its inner workings, and its daily operational problems and, most importantly, who were those in charge. But CONTI was not the only victim of this social media self-exposure. LAPSUS$ Group and RAID Forums are other examples of how this social media exposure resulted in the temporary shutdown of these operations. The reported daily amount of attacks and leaks, now amplified in social networks and mass media outlets, are creating a trove of information that will take months, if not years, to analyse. In a rapidly changing environment this information overload can be distracting and lead to the dispersion of resources.

The public attention that these attacks are getting, and the normalization of cybercrime as a valid, publicly lauded, even state sponsored activity is also attracting users from a younger generation that, up to now, didn't have the knowledge - or skills - to dive deep into a certain type of forum. This shift in terms of accessibility fosters a sense of belonging to something bigger. It creates recruitment opportunities and incentives for cybercriminal groups, it grows the potential for new victims and widens the arch of prospective targets. Cybercriminal groups are using this newfound fame to finance themselves - either by request for donations, selling of merchandise, but also publicly calling for those with access to corporate and critical infrastructures to cooperate in return of monetary compensation to breach those entities. Moreover, the use of publicly traded RaaS packages, exponentially creates the potential for more disruption by criminal actors that, to this point, were not involved in cybercrime: availability of solutions and ease of use, allied to a public awareness of success by the cybercriminal groups on social media, gives these groups a larger target audience to sell their solutions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Recommendations

This fourth EU-HYBNET policy brief recommendations correspond to the European Union Cybersecurity and European Union Security Union strategies. While both strategies prioritize among other focus areas, the need to foster and improve collaboration or share information between EU Member States - the EU Security Union Strategy emphasize as one of the key actions to deter and tackle on time evolving threats, including cybercrime and hybrid threats. There is no reason to believe that the social media presence of these groups will fade away, on the contrary. Cybercriminal groups have found that public notoriety can be used as a weapon towards their targets, and a good resource for recruitment. In the light of this rising and fast evolving trend, the project recommends that:

- Reckoning with this new state of reality requires **technical expertise, timely situational awareness and communication, talents attractiveness**. **Using existing exchange platforms, such as the NIS and other Coordination groups at European level** should be intensified.
- Based on the principle that no infrastructure is safe from an attack, a bigger effort has to be made to **create sound security measures within organizations**, taking into account that remote work, which will be more and more prevalent in the future, brings with it new challenges**.**
- Cyber-criminal groups can exploit their social media fame-seeking and public exposure in identifying persons-of-interest in organizations, by monitoring who joins or follows their dissemination's channels. With social engineering being used in lots of high-profile attacks, internal social media policies connected with strong digital security enforcement are no longer optional, but mandatory. The interest that these public groups create in a younger generation should not be overlooked as it's both an opportunity and a threat. It is suggested to create **targeted communication campaigns and educational programs** to make use of this interest in cyber security, in order to prevent that some of this talent will join cyber-criminal groups or create their own.

Research Parameters

EU-HYBNET is a 5-year EU funded project aiming to build a sustainable Pan European network of security stakeholders, especially security practitioners, to collaborate with each other in order to increase the capacity on a European level to counter hybrid threats. To achieve its goal, the project is organised in four Core Themes, namely 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication. These Core themes will provide an opportunity to focus on all hybrid threat domains, especially interfaces between the domains, ensuring that the project delivers coherent results in relation to the conceptual framework model countering hybrid threats. In this context, practitioners are invited to express their needs in countering hybrid threats, which were later prioritised as the most urgent and crucial ones. Following the above, the project identifies the most promising technologies and innovations that could address the needs of the end users and develops a roadmap for their uptake and industrialisation, providing standardisation recommendations. Research outputs from the project will be presented in a series of policy briefs, position papers and recommendations. The formulation of these outcomes will take place in close collaboration with stakeholders, who are included in the project activities from its outset, thereby maximizing its intended impact.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Project identity

Project name: Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
Coordinator: Laurea University of Applied Sciences, Finland

Consortium:

1. Arctic University in Norway (UiT), Norway
2. Bundeswehr University (COMTESSA), Germany
3. Central Office for Information Technology in the Security Sector (ZITiS), Germany
4. Espoo City and Region (Espoo), Finland
5. Estonian Information Systems Authority (RIA), Estonia
6. The European Centre of Excellence for countering Hybrid Threats (Hybrid CoE), Finland
7. European Organization for Security (EOS), Belgium
8. France Ministry for an Ecological and Solidary Transition (MTES), France
9. International Centre for Defence and Security (ICDS), Estonia
10. Joint Research Centre EC (JRC), Italy
11. KEMEA, Greece
12. Laurea University of Applied Sciences (Laurea), Finland
13. Lithuanian Cyber Crime Centre of Excellence for Training, Research and Education (L3CE), Lithuania
14. Maldita, Spain
15. The Mihai Viteazul National Intelligence Academy (MVNIA), Romania
16. The Netherlands Ministry of Defence (MoD), Netherlands
17. Norwegian Directorate for Civil Protection (DSB), Norway
18. Polish Platform for Homeland Security (PPHS), Poland
19. Polish Internal Security Agency (ABW), Poland
20. Research Institutes in Sweden (RISE), Sweden
21. SATWAYS, Greece
22. TNO, Netherlands
23. Universita Cattolica Sacro Cuore (UCSC), Italy
24. University of Rey Juan Carlos (URJC), Spain
25. Valencia Local Police (PLV), Spain

Funding scheme: Horizon2020 Secure Societies Programme, General Matters-01-2029 call. GA No. 883054
Duration: May 2020 – April 2025
Budget: 3 496 837,50 €
Website: https://euhybnet.eu/

For more information: Laurea / Coordinator Päivi Mattila paivi.mattila@laurea.fi

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054