

European Commission - Horizon 2020 DS-07-2017

Cybersecurity PPP: Addressing Advanced Cyber Security Threats and
Threat Actors



REactively Defending against Advanced
Cybersecurity Threat

D7.2: Initial Dissemination Plan[†]

Abstract: This deliverable discusses the initial **Dissemination** and **Communication Plan** of the ReAct project.

Contractual Date of Upload	November 2018
Actual Date of Upload	November 2018
Deliverable Security Class	Public
Editor	Evangelos Markatos
Contributors	<i>REACT</i> partners
Quality Assurance	C. Papachristos, M. Christodoulaki

[†] This project is funded by the European Commission (Horizon 2020 - DS-07-2017) under Grant agreement no: 786669.

The *REACT* consortium consists of:

FORTH	Coordinator	Greece
STICHTING VU	Beneficiary	The Netherlands
UNIVERSITY OF CYPRUS	Beneficiary	Cyprus
EURECOM	Beneficiary	France
RUHR-UNIVERSITAET BOCHUM	Beneficiary	Germany
SYMANTEC	Beneficiary	France

Document Revisions & Quality Assurance

Internal Reviewers

1. Meltini Christodoulaki (FORTH)
2. Christos Papachristos (FORTH)

Revisions

Version	Date	By	Overview
0.1	25/11/2018	Evangelos Markatos	Version ready for review
0.2	28/11/2018	Evangelos Markatos	Addressed the comments of the reviewers

Table of Contents

TABLE OF CONTENTS.....	5
TABLE OF FIGURES.....	6
1 EXECUTIVE SUMMARY	8
2 INTRODUCTION TO THE REACT PROJECT AND APPROACH.....	9
3 DISSEMINATION	11
3.1 THE DIMENSIONS	11
3.1.1 Objectives.....	11
3.1.2 Target Groups.....	11
3.1.3 Dissemination Mechanisms.....	12
3.2 THE DISSEMINATION PLAN.....	13
3.2.1 Phase 1: (year 1).....	13
3.2.2 Phase 2: (year2).....	14
3.2.3 Phase 3: (year 3).....	15
3.3 KEY PERFORMANCE INDICATORS (KPIs)	15
3.4 ACKNOWLEDGING EU FUNDING	17
3.4.1 The relevant text.....	17
3.4.2 Disclaimer	17
4 COMMUNICATION	18
4.1 THE DIMENSIONS	ERROR! BOOKMARK NOT DEFINED.
4.1.1 Objectives.....	18
4.1.2 The Target Groups.....	18
4.1.3 Communication Mechanisms	18
4.2 THE COMMUNICATION PLAN.....	19
4.2.1 Phase 1: (year 1).....	19
4.2.2 Phase 2: (year 2).....	22
4.2.3 Phase 3: (year 3).....	23
5 DISSEMINATION ACTIVITIES AND PROJECT IDENTITY	24
5.1 LOGO.....	24
5.2 WEB SITE	24
5.2.1 Partners Section.....	25
5.2.2 Publications Section.....	26
5.2.3 Contact Us Section.....	27
6 SOCIAL NETWORKS	28
6.1 TWITTER.....	28
6.2 FACEBOOK.....	28
6.3 LINKEDIN	29
7 FILE HOSTING.....	31
8 CONCLUSION	33

Table of Figures

<i>Figure 1: How a computer is protected “without” the ReAct technology and how it is protected “with” the ReAct technology.</i>	9
<i>Figure 2: European Emblem</i>	17
<i>Figure 3: Deliverable Template</i>	20
<i>Figure 4: Presentation Template</i>	21
<i>Figure 5: Project Poster</i>	22
<i>Figure 6: The Logo of the ReAct project</i>	24
<i>Figure 7: Home page of the ReAct project web site</i>	25
<i>Figure 8: Partners page of the web site</i>	26
<i>Figure 9: Twitter profile of ReAct</i>	28
<i>Figure 10: Facebook profile of ReAct</i>	29
<i>Figure 11: LinkedIn profile of ReAct</i>	30
<i>Figure 12: OwnCloud of ReAct</i>	32

1 Executive Summary

This document presents the dissemination and communication plan of the project ReAct.

Section 2 gives a short introduction to the project. Section 3 is dedicated to the Dissemination of the project. It presents the objectives of the Dissemination Activities, the target groups (or stakeholders), the planned dissemination activities per year, the Key Performance Indicators (KPIs) and finally the proper way to acknowledge the EU funding. Section 4 is dedicated to the communication activities of the project. Since this deliverable is due at M6, some dissemination/communication activities have already started. Towards this direction, section 5 presents the activities with respect to the project identity (logo, website, etc.), and section 6 presents the project's presence on and plan for the social media.

The document presents the answers to the important dissemination and communication questions including:

- Who are the relevant **stakeholders**?
 - See sections 3.1.2 and 4.2.
- What will be the dissemination **activities per year**?
 - See sections 3.2.1 to 3.2.3.
- What will be the communication **activities per year**?
 - See sections 4.4.1 to 4.4.3.
- What are the Dissemination and Communication **Objectives** of the project?
 - See sections 3.1.1 and 4.1.

2 Introduction to the ReAct project and approach

Security is a vital property for every operational system and network. As systems become more powerful and, in many aspects, more complex, advanced cyber-attacks impose new threats for important operations of our society.

Computer systems assist core functions of hospitals, energy centers, logistics, and communications, to name a few, and compromising such systems may have severe consequences for everyone of us. Despite the evolution of computer systems, current security defenses, although they have been substantially improved in the last decade, seem not really enough to stop advanced cyber attacks. Systems still suffer from vulnerabilities, despite the many active or passive defenses in place that have been developed in the last decades.

In the ReAct project we believe that the core of this problem is that cyber attackers are almost always one step ahead of the cyber security researchers and practitioners. Indeed, cyber attackers are the first to strike, and while researchers try to figure out what happened, attackers have all the time in the world to plan their next strike. In ReAct we advocate that we should change the rules of the cyber attackers' game and challenge the asymmetry. Instead of following the cyber attackers, researchers should try to forecast where attackers will strike next and to use this information (i) to fortify potential targets to withstand the attack and (ii) to wire targets up with forensic hooks and make them "forensics ready". To make all this possible at a reasonable performance cost, ReAct proposes the use of **selective fortification**, a mechanism that combines traditional passive and active defense approaches into a new reactive mode of operation. ReAct takes advantage of the partners' rich background in software hardening and instrumentation for immediate delivering effective patches by selectively armoring the vulnerable parts of a program.

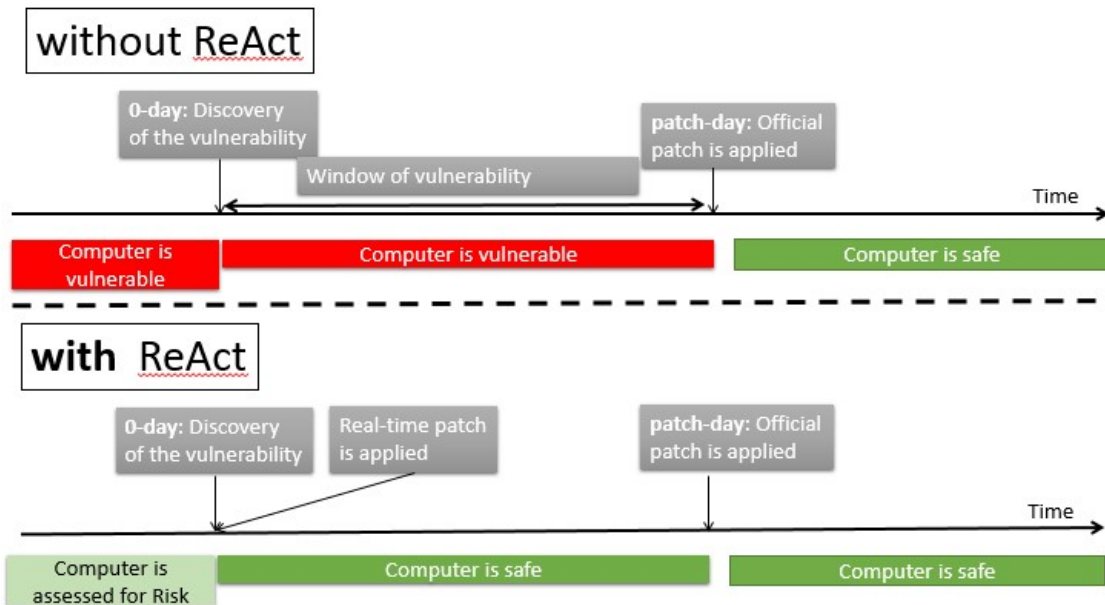


Figure 1: How a computer is protected “without” the ReAct technology and how it is protected “with” the ReAct technology.

The figure above shows clearly the situation “without” the ReAct project and “**with**” the ReAct project.

Let us try to describe the situation as it is today (i.e. “without” the ReAct project). Let us assume that we have a system that has a vulnerability. Let us assume that the vulnerability is eventually discovered at some point in time which we call “0-day” in the figure above. Obviously before that date the computer was vulnerable (shown with the red bar “Computer is vulnerable”). Unfortunately, even after the vulnerability is known but before the system is patched, the computer is still vulnerable (shown as the second red bar in the figure). ReAct proposes to change this and protects the computer as much as possible during these two time intervals. For the second time interval (i.e. after the vulnerability is discovered but before the patch is applied) ReAct proposes selective fortification: a mechanism to neutralize the vulnerability and protect the computer before the official patch is ready (or applied). ReAct proposes to try to protect the computer even before the “0-day”, that is, even before the vulnerability is discovered. This can be done by assessing the risk of the computer and if the computer is found at high risk (without knowing the exact nature of the vulnerability), (i) identify the computer and (ii) provide some mechanisms to protect it.

3 Dissemination

3.1 The dimensions

3.1.1 Objectives

The overarching goal of the Dissemination is to maximize the impact of the project through the spreading of its results to the interested stakeholders. In particular, the individual dissemination **objectives** of the project are to:

- [OBJ1]: maximize the **impact** of the project
- [OBJ22]: achieve maximum **visibility** among all interested stakeholders
- [OBJ3]: create **liaisons** with the broader constituency
- [OBJ24]: **attract** potential users and/or market stakeholders
- [OBJ5]: encourage the **uptake** of the project's results

3.1.2 Target Groups

The identified target groups of the dissemination efforts of the project include:

- **Researchers**
 - individuals and groups engaged in research in the area of cybersecurity
- **Policy makers**
 - this group includes Institutions of Member States as well such as ECSO, NIS Platform, etc.
- **Business** and innovation community
 - including SMEs and larger corporations
- **Standards**-defining Organizations
 - such as TAXII and STIX OASIS
- The **General Public**
 - this is a very broad category which includes all citizens who would have some interest in our work
- **H2020 projects**
 - this is the set of projects in the area of cybersecurity which are funded by the H2020 Framework Program

Target Group	What do they need?	How can ReAct help this Target Group?
Researchers	Researchers need state of the art results in the area of cyber security so that they can solve open problems and/or built upon the described solutions.	<ul style="list-style-type: none">• produce high quality research• publish in well-known venues
Policy Makers	Policy Makers need easy-to-use statements backed by substantial research	<ul style="list-style-type: none">• produce high quality research results• translate these research results into “actionable” items
Business and Innovation	The Business and Innovation community need results of applied research that are close to the market and can be	<ul style="list-style-type: none">• high quality research results that can be used by innovation communities

Community	commercialised with little effort	
Standards	They need knowledgeable security people who can contribute to needs as required	<ul style="list-style-type: none"> • participate in meetings
General Public	The general public needs better security protection and improved awareness	<ul style="list-style-type: none"> • high quality research results that can be integrated in services that may eventually reach the general public • white papers and similar publications that is easily understood by the general public
H2020 projects	H2020 projects need complementarity in their activities and synergies in order to reach a critical mass that can make their impact felt	<ul style="list-style-type: none"> • collaboration in event/workshop organization • common participation (with other H2020) in events

3.1.3 Dissemination Mechanisms

To achieve the maximum benefit, we plan to use a variety of dissemination mechanisms. We think that each dissemination mechanism can effectively address one or a small number of target groups. Thus, by tuning the dissemination mechanism to the target group we believe we will have higher impact. Among the dissemination mechanisms we plan to use are the following:

- **DM1** - Scientific **publications**: in conferences and journals.
 - These are scientific publications that convey specific results of the project. In this category we also include white papers, position papers and publications that convey results to a broader audience.
- **DM2** - Participation in **conferences** and various related events.
 - There are two kinds of conference we have in mind: (i) scientific conferences (where novel research results are being published) and (ii) broader events including commercial events, stakeholder events, policy events, EU events, etc.
- **DM3** - Building a **community** of all interested stakeholders.
 - We envision two kinds of interactions:
 - *Occasional* interactions. For example, a person arrived to our web site (e.g. as a result of a Google search), browsed the papers, downloaded one or two documents and left. The same person will not likely return to the web site, unless as a result of another occasional event (such as a google search)
 - *Repeated* interactions. These are users who repeatedly interact with our material. They may follow our twitter account, they may repeatedly visit the web site, they may periodically receive emails. DM3 is related to building a community of users who will have repeated interactions with our project.
- **DM4** - Collaboration with other **H2020 projects** via concertation events, cPPP events, relevant CSA projects, etc.

- The European Commission under the H2020 Framework has funded a large number of Research and Innovation projects in the area of cybersecurity. Although each of the projects has different goals and work plan, collaborating with them can be beneficial. For example, disseminating our results to other H2020 projects may (i) provide us feedback, (ii) reduce duplication, and (iii) may create new possibilities through the combination of our results with another project's results.
- **DM5 - Open Source software repositories.**
 - These are repositories that are accessible (if open) by all people. That is everybody can download and build the tools, although, few people will be able to update the source code. Such repositories are easily searchable and through a common interface (usually git) enable the developed code to reach a large number of people.

3.2 The Dissemination Plan

We envision the Dissemination Plan to follow three phases:

- Phase 1: First year of the project
- Phase 2: Second year of the project
- Phase 3: Third year of the project

3.2.1 Phase 1: (year 1)

During the first year of the project we have already started working (i) towards putting together the dissemination infrastructure of the project and (ii) towards starting the first dissemination activities. With respect to specific Dissemination Mechanisms we envision the following activities:

- **DM1: Scientific Publications in Conferences and Journals**
 - We plan to have the first publications (possibly including position and white papers). Actually at the time of this writing we have already the first publications published:
 - Radhesh Krishnan Konoth, Marco Oliverio, Andrei Tatar, Dennis Andriesse, Herbert Bos, Cristiano Giuffrida, Kaveh Razavi. ZebRAM: Comprehensive and Compatible Software Protection Against Rowhammer Attacks. In Proceedings of the 13th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2018). Carlsbad, CA, USA. October, 2018.
 - Stephan van Schaik, Cristiano Giuffrida, Herbert Bos, Kaveh Razavi. Malicious Management Unit: Why Stopping Cache Attacks in Software is Harder Than You Think. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD, USA. August, 2018.
 - Ben Gras, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida. Translation Leak-aside Buffer: Defeating Cache Side-channel Protections with TLB Attacks. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD, USA. August, 2018.
 - Robert Gawlik, Thorsten Holz. SoK: Make JIT-Spray Great Again. In Proceedings of the 12th USENIX Workshop on

Offensive Technologies (WOOT 18). Baltimore, MD, USA. August. 2018.

- **DM2:** Participation in conferences and various events
 - We have participated in USENIX Security 2018, WOOT 2018, and we plan to participate in OSDI 2018, ICT 2018, and in several other events based on the publications
- **DM3:** Build a community of interested stakeholders
 - Inform key organizations
 - Consult with relevant stakeholders
 - Create and disseminate promotional material
 - Engage the external Advisory Board and their connections
 - Participate in policy-related meetings and events
- **DM4** - Collaboration with other H2020 projects via concertation events, cPPP events, relevant CSA projects, etc.
 - We included ReAct in **cyberwatching.eu** community. Through this community we participate in events which are connected to all H2020 projects in the area of cybersecurity.
 - The Coordinator of the project has been elected **Chair of SGW 6.3 of the ECSO¹ WG6** which is charged with the development of the Strategic Research and Innovation Agenda.
 - We collaborated with the **ASTRID², SPEAR³, CYBER-TRUST⁴, SHIELD⁵, and 5GENESIS⁶** projects to create a proposal for a NetSoft Joint Workshop on “Cyber-Security Threats, Trust and Privacy management in Software-defined and Virtualized Infrastructures”.
- **DM5:** Open Source Software Repositories
 - We do not envision to have any source code ready to be released in year 1.

3.2.2 Phase 2: (year2)

During the second year of the project we expect to have more mature results to disseminate. Thus, the dissemination will use the Dissemination Mechanisms as follows:

- **DM1:** Scientific Publications in Conferences and Journals
 - We expect the publication of tools and more mature results.
- **DM2:** Participation in conferences and various events
 - Participation in tier-1 and other conferences
 - Dissemination in partner's events such as the European Researcher's Night night
- **DM3:** Build a community of interested stakeholders

¹ <https://ecs-org.eu/>

² https://cordis.europa.eu/project/rcn/214855_en.html

³ https://cordis.europa.eu/project/rcn/214857_en.html

⁴ https://cordis.europa.eu/project/rcn/214839_en.html

⁵ <https://project-shield.eu/>

⁶ https://cordis.europa.eu/project/rcn/218507_en.html

- Capitalize on and expand the efforts of the previous year
 - Engage community developers through software releases
- **DM4** - Collaboration with other H2020 projects via concertation events, cPPP events, relevant CSA projects, etc.
 - Participate in cyberwatching.eu events
 - Participate in the activities of ECSO (European CyberSecurity Organization)
- **DM5**: Open Source Software Repositories
 - Initial contributions to **git** repository

3.2.3 Phase 3: (year 3)

During the third year of the project we expect to have ready tools and results to disseminate. Thus, the dissemination will use the Dissemination Mechanisms as follows:

- **DM1**: Scientific Publications in Conferences and Journals
 - We expect the publication of tools and more mature results.
- **DM2**: Participation in conferences and Various events
 - Participation in tier-1 and other conferences
 - Dissemination in partner's events
- **DM3**: Build a community of interested stakeholders
 - Elaborate on the activities of the previous years
 - Creation of vertical communities with specific focus
- **DM4** - Collaboration with other H2020 projects via concertation events, cPPP events, relevant CSA projects, etc.
 - This collaboration will focus on concrete actions including:
 - Demos
 - Formation of new consortia
 - Collaborations in EU fora (such as ECSO, etc.)
 -
- **DM5**: Open Source Software Repositories
 - Mature contributions to **git** repository

3.3 Key Performance Indicators (KPIs)

Associated with the above Dissemination Mechanisms are Key Performance Indicators (KPIs) as follows:

Dissemination Mechanism	Target Value	Summary	Who?
Participation and Publications in	40	Publications in Conferences is one of the primary mechanisms to promote new knowledge and state of the art results. ⁷	All partners

⁷ One might want to see a detailed list of conferences and papers here. For example, "paper on topic A will appear in IEEE Symposium on Security and Privacy 2019". Unfortunately, this cannot be done:

Conferences			
Publications in journals	5	Publications in Archival journals is a good mechanism to promote results that have a lasting value – probably for several years after the end of the project.	All partners
Invited Talks	30	Invited talks in Organizations and Conferences is an immediate way to present the results face to face to the audience.	All partners
Engagement in Social Media	50 actions per year	Social media is a timely way to transmit small bits of information about the results of the project. Actions in Social Media are short, quick, and timely: tweets, posts, etc. For example, the goal of these actions is not to describe a scientific paper, but to mention the publication of the paper and give its main results in no more than one sentence.	Leader: FORTH All partners contribute as relevant
Booths in Public Events	5	Booths in public events is an effective way to connect with people who may have not heard of the project and may not follow it on social media and the web. We capitalize on the fact that people went there for the interesting event and they get the opportunity to be introduced to ReAct.	FORTH, RUB, VUA, Symantec
Booths in business events	1	Business events are more focused towards business people. Although public events may draw researchers, students, and even the general public, business events are more focused towards scoping out the business landscape and putting a stake into it.	Symantec
Reach out to SMEs	3	Reach out to SMEs using multipliers such as Digital Hubs, SME associations, etc.	All partners
Reach out to Industry	20 contacts	Create business contacts with Industry. These will be individuals that work in the industry of IT (or related field) who will be contacted about the project.	All partners

-
- Top-tier conferences and journals are highly selective having an acceptance rate of 20% or even lower. Thus, projecting that a paper will be published, say, in IEEE Symposium on Security and Privacy 2019 cannot be said with certainty.

3.4 Acknowledging EU funding

3.4.1 The relevant text

Any publicity, including at a conference or seminar or any type of information or promotional material must specify that the project has received EC research funding and display the European emblem



Figure 2: European Emblem

All publications shall include the following statement:

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 786669

3.4.2 Disclaimer

The dissemination information should use the following disclaimer:

The content of this website (Views expressed / Documents published here) reflects the views only of their author (s). The European Commission/ Research Executive Agency are not responsible for any use that may be made of the information it contains.

4 Communication

4.1 Objectives

The individual communication objectives of the project are:

- **[C1]:** increase awareness about the project among the broader community
- **[C2]:** create a community of potential users
- **[C3]:** create an avenue for the potential exploitation of the project's results

4.2 The Target Groups

The target groups of the communication activities are the same as the target groups of the dissemination activities:

- **Researchers**
 - individual and groups engaged in research in the area of cybersecurity
- **Policy makers**
 - this group includes Institutions of Member States as well
- **Business** and innovation community
 - including SMEs and larger corporations
- **Standards-defining Organizations**
 - such as TAXII and STIX OASIS
- **The General Public**
 - this is a very broad category which includes all citizens who would have some interest in our work
- **H2020 projects**
 - this is the set of projects in the area of cybersecurity which are funded by the H2020 Framework Program

4.3 Communication Mechanisms

We plan to use modern digital mechanisms that can deliver our communication message instantly all over the globe. These mechanisms include:

Mechanism	Who?
[CM1]: The project's web site: this will be the single-stop shop for all information related to the project.	FORTH
[CM2]: Online Social Media including twitter, LinkedIn, and Facebook.	Editor: FORTH. Contributions from all partners
[CM3]: Traditional Media including blogs, news articles, etc.	All partners

[CM4]: Communication Material including logo, project identity, press releases, etc.	FORTH
---	-------

4.4 The Communication Plan

We envision the Communication Plan to follow three phases: one phase for each year of the project

4.4.1 Phase 1: (year 1)

- **CM1:** The web site

What	Deadline	Status
Web site creation	M1	Done
Feeding the web site with content	-	Ongoing

- **CM2:** Online social media

What	Deadline	Status
Creation of Twitter, Facebook, and LinkedIn accounts	M1	Done
Updating the accounts with content	-	Ongoing
Improve visibility of the accounts, increase followers, likes, impact, etc.	-	Ongoing

- **CM3:** Traditional Media

What	Deadline	Status
Creation of Press releases, blog posts and similar communication activities	M12	Created

- **CM4:** Communication Material

What	Deadline	Status
Creation of project logo, presentation templates, poster	M1	Created
Creation of factsheet, brochure, promotional material	M12	Ongoing
Improve visibility of the accounts, increase followers, likes, impact,	-	Ongoing

etc.

European Commission - Horizon 2020 DS-07-2017
Cybersecurity PPP: Addressing Advanced Cyber Security Threats and
Threat Actors



REactively Defending against Advanced Cybersecurity Threats

Dx.x: <Deliverable Template>[†]

Abstract: Oratio nominavi intellegebat an nec, ne vis ridens REACT intellegam. Ex liquyam, expetenda scribentur nec, cu magna omnis sed, illum option constituam qui et. Quo dolore labitur REACT cu, an proluvaret constituto. Vivendum urbanitas pro no, est id laudem appareat scrip-torem, et sit accumsan gloriatur. Eu ridens consulatu per. Vim ex perpetua democritum elaborarete

Contractual Date of Upload	July 2018
Actual Date of Upload	July 2018
Deliverable Security Class	Public
Editor	Name1 Surname1
Contributors	All REACT partners
Quality Assurance	Name2 Surname2

[†] This project is funded by the European Commission (Horizon 2020 - DS-07-2017) under Grant agreement no: 786669.

The REACT consortium consists of:

FORTH	Coordinator	Greece
STICHTING VU	Beneficiary	The Netherlands
UNIVERSITY OF CYPRUS	Beneficiary	Cyprus
EURECOM	Beneficiary	France
RUHR-UNIVERSITAET BOCHUM	Beneficiary	Germany
SYMANTEC	Beneficiary	France

www.react-h2020.eu

- 2 -

June 01, 2018

Figure 3: Deliverable Template



Figure 4: Presentation Template


ReAct mission:

- Fight software exploitation.
- Mitigate Advanced Cybersecurity Threats in a timely fashion

Connect with ReAct

 @react_h2020 – http://twitter.com/react_h2020

 <http://fb.me/reacth2020>

 <http://www.linkedin.com/in/reacth2020/>

Project Facts

- Duration:
2018-2021
- Coordinator:
FORTH
- Contact:
Prof. Evangelos Markatos
FORTH, Greece
markatos@ics.forth.gr
- Funding:
European Union
Research & Innovation
Programme
Grant No. 786669

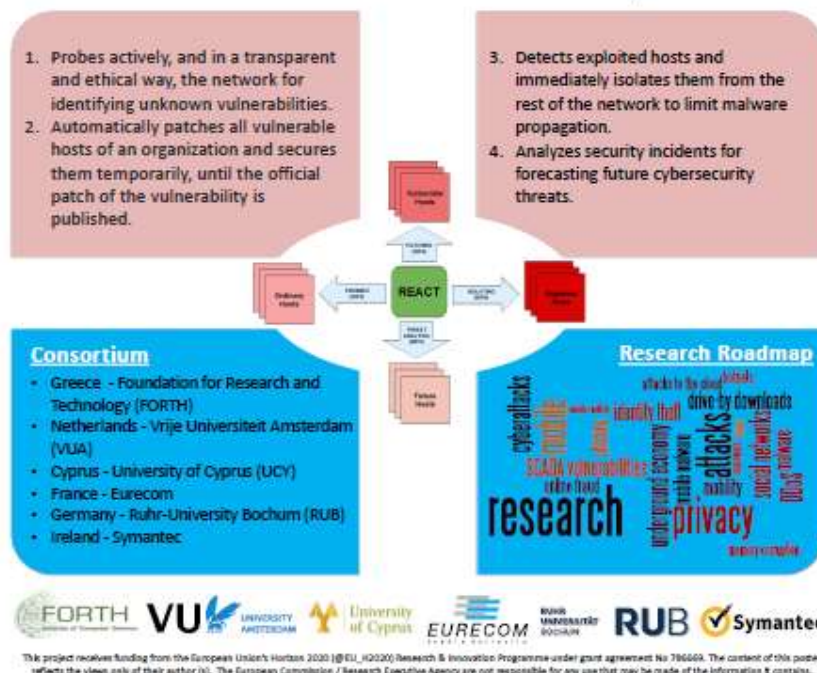


Figure 5: Project Poster

4.4.2 Phase 2: (year 2)

- **CM1:** The web site
 - Regular updates with deliverables and papers⁸.

⁸ In the proposal we envisioned the use of Google Analytics to help us understand how to optimize the presented information. Unfortunately, after the implementation and deployment of GDPR, collecting (and sharing with Google Analytics) personal data requires the consent of the individuals. This creates two new challenges:

- Collect access patterns only for users who consent to this. This may limit the validity of our conclusions as it will apply only to users who consent to the collection and transfer of their data to Google analytics.
- Find some new way (i.e. not Google Analytics) to analyze user's access patterns.

- **CM2:** Online social media
 - Regular updates, follow/monitor accounts and hashtags, retweet, etc.
- **CM3:** Traditional Media
 - White papers and contributions to popular press.
- **CM4:** Communication Material
 - Revise/update created communication material
 - Publish articles in project-related venues.

4.4.3 Phase 3: (year 3)

- **CM1:** The web site
 - Updates, provide interactivity/feedback, user experience optimization.
- **CM2:** Online social media
 - Provide frequent updates, promote project's outcomes,
 - Upload material, reproduce important material,
 - Recruit attendees for events and workshops, contribute to policy-related discussions
- **CM3:** Traditional Media
 - Press Releases, articles in popular press
- **CM4:** Communication Material
 - Update/revise material, prepare final communication kit

5 Dissemination Activities and Project Identity

5.1 Logo

We have developed a logo for the project. It is simple and easy to recognize at all scales: small, medium, and large.



Figure 6: The Logo of the ReAct project

5.2 Web Site

We have developed a web site for the project. It describes the project and serves as a single-stop shop for the various information provided by the project: publications, deliverables, etc. It also provides pointers to the social media accounts of the project: facebook, linkedin, and twitter.

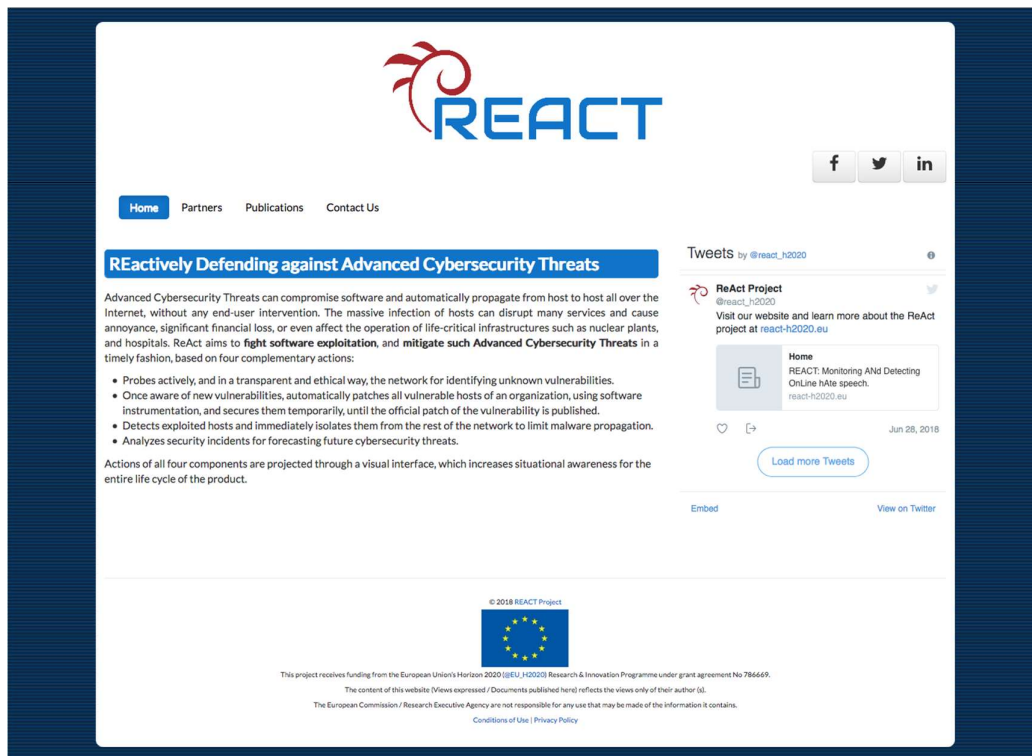


Figure 7: Home page of the ReAct project web site

5.2.1 Partners Section

A short profile for each of the project partners is provided through the Partners section of the website. A general description and the official partners' logos have been included in this page, for the visitor to have a clear view of the consortium and their roles in the project. The name of each partner contains a link to the webpage of the relative organization.



Figure 8: Partners page of the web site

5.2.2 Publications Section

This section will make available to the public all the documents published by the project. As the list of published documents will expand both in length (i.e. more conference papers) and in diversity (i.e. inclusion of deliverables) it is expected that more frames will be added to this section. The title of each paper will be added to this page as soon as its acceptance notification is received. The full text of the paper or a

link to the paper on the publisher website will be added at the same time or shortly after.

5.2.3 Contact Us Section

The Contact Us page contains a contact form allowing visitors to contact project consortium and submit comments, questions, or suggestions, and in general provide feedback and some interactivity. The email address of the visitor is required in order to reply.

6 Social Networks

Currently, ReAct presence has been established in *Facebook*, *Twitter* and *LinkedIn*.

6.1 Twitter

Twitter is the most popular news networking service where users interact with short posts known as “tweets”. Initially, tweets were restricted to 140 characters but in the last year this limit was doubled. The Twitter profile of ReAct can be seen on Figure 9. Twitter feed has been also integrated to the website in the form of the *news feed* in the right part of the front page.

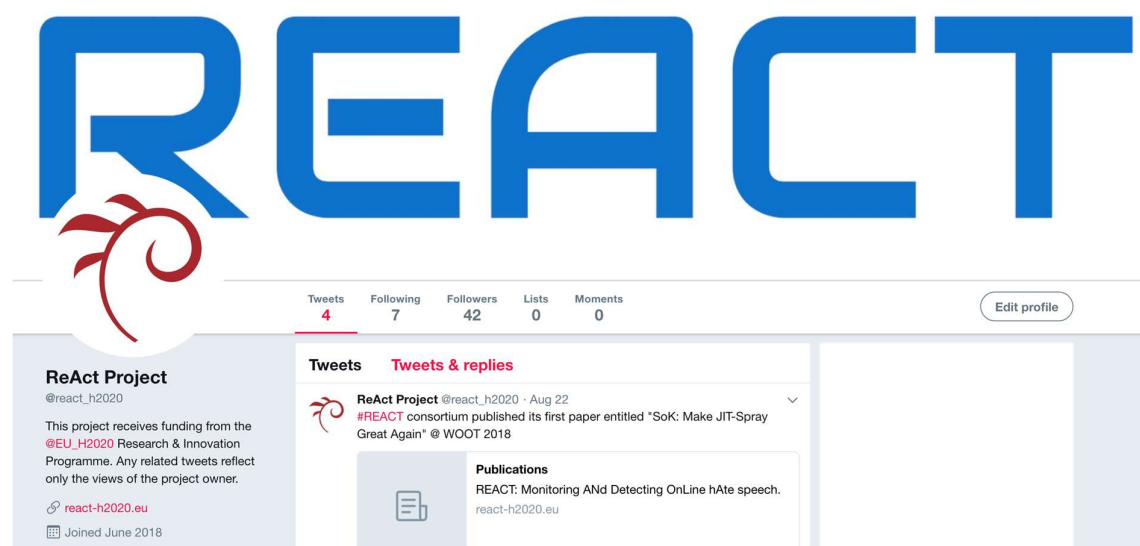


Figure 9: Twitter profile of ReAct

6.2 Facebook

Facebook, launched in February 2004, is a free and very popular networking platform that enables users and communities to maintain profiles, upload media files and stay in touch with the public. Facebook is much more complex than Twitter as it works as a social platform that allows many independently developed applications to run. A page was created for the ReAct project on Facebook which can be seen on Figure 10.

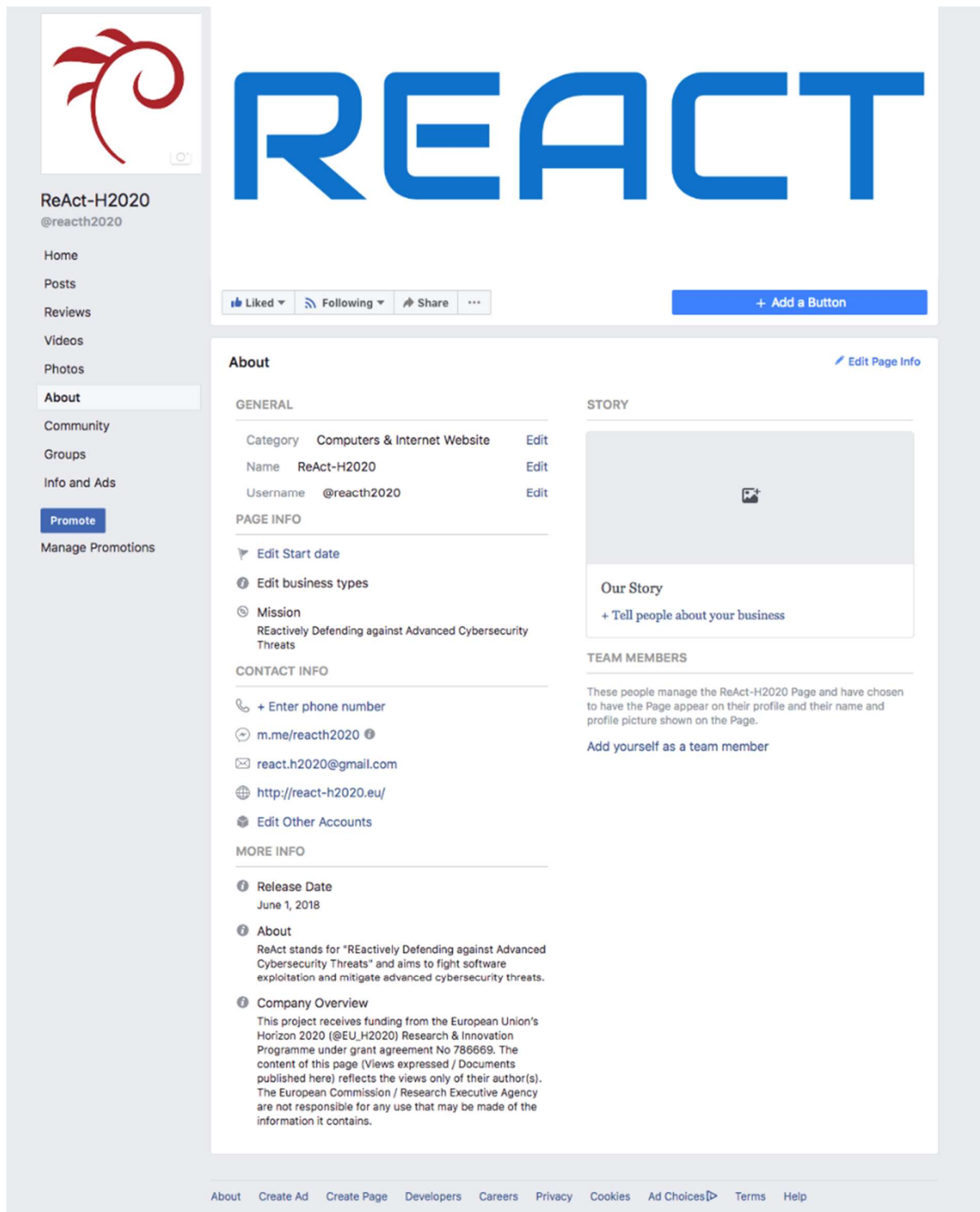


Figure 10: Facebook profile of ReAct

6.3 LinkedIn

LinkedIn is another popular social networking platform specifically used for business. Its main goal is to connect registered users that they know each other professionally. The LinkedIn profile of ReAct can be seen on Figure 11.



The image shows a screenshot of the LinkedIn profile for the ReAct Horizon project. At the top, the word "REACT" is written in large, bold, blue capital letters. To the left of the text is a circular logo featuring a stylized red flame or leaf design. Below the logo, the text "ReAct Horizon" is displayed, followed by "H2020 Project at Foundation for Research and Technology - Hellas (FORTH)" and "Greece". To the right of this text, there are three icons with corresponding text: a building icon for "Foundation for Research and Technology - Hellas ...", a document icon for "See contact info", and a group of people icon for "See connections (6)". Below this information, there are two buttons: a blue button labeled "Add profile section" with a downward arrow, and a white button labeled "More...". A horizontal line separates this header from the main content area. The main content area contains two paragraphs of text. The first paragraph states: "ReAct stands for 'REactively Defending against Advanced Cybersecurity Threats' and aims to fight software exploitation and mitigate advanced cybersecurity threats." The second paragraph states: "This project receives funding from the European Union's Horizon 2020 (@EU_H2020) Research & Innovation Programme under grant agreement No 786669. The content of this page (Views expressed / Documents published here) reflects the views only of their author(s). The European Commission / Research Executive Agency are not responsible for any use that may be made of the information it contains."

REACT

ReAct Horizon
H2020 Project at Foundation for Research and Technology - Hellas (FORTH)
Greece

[Add profile section](#) [More...](#)

ReAct stands for "REactively Defending against Advanced Cybersecurity Threats" and aims to fight software exploitation and mitigate advanced cybersecurity threats.

This project receives funding from the European Union's Horizon 2020 (@EU_H2020) Research & Innovation Programme under grant agreement No 786669. The content of this page (Views expressed / Documents published here) reflects the views only of their author(s). The European Commission / Research Executive Agency are not responsible for any use that may be made of the information it contains.

Figure 11: LinkedIn profile of ReAct

7 File Hosting

ReAct partners use the ownCloud platform for file hosting and sharing of consortium documents. ownCloud is a free open source software for data synchronization, file sharing, and remote storage of documents. It is written in the PHP and JavaScript scripting languages and supports several database management systems, including SQLite, MariaDB, MySQL, OracleDatabase, and PostgreSQL.

File access is provided through a web interface or from mobile devices via mobile applications for iOS and Android and from desktop clients available for PCs running Windows, Mac OS, or Linux.

In Figure 12 we can see the web interface of the ReAct repository. The ownCloud user interface contains the following fields and functions:

- **Apps Selection Menu:** Located in the upper left corner and by clicking the arrow a dropdown menu opens to navigate to user's various available apps.
- **Apps Information Field:** Located in the left sidebar and provides filters and tasks associated with user's selected app. For example, when the Files apps is used, a special set of filters for quickly finding files is shown.
- **Application View:** The main central field in the ownCloud user interface. This field displays the contents or user features of the selected app.
- **Navigation Bar:** Located over the main viewing window (the Application View), this bar provides a type of breadcrumbs navigation that enables migration to higher levels of the folder hierarchy up to the root level (home).
- **New Button:** Located in the Navigation Bar, this button enables the user to create new files, new folders, or upload.
- **Search Field:** The user can click on the magnifier in the upper right hand corner to search for files.
- **Personal Settings Menu:** The user can click on her ownCloud username, located to the right of the Search field, to open the Personal Settings dropdown menu. Personal page provides settings and features such as:
 - Links to download desktop and mobile apps
 - Server usage and space availability
 - Password management
 - Name, email, and profile picture settings
 - Group memberships o Interface language settings
 - Manage notifications
 - Social media sharing buttons
 - ownCloud Version information



The screenshot shows the OwnCloud web interface. On the left is a sidebar with navigation options: 'All files', 'Favorites', 'Shared with you', 'Shared with others', 'Shared by link', 'Tags', and 'External storage'. The main area displays the contents of the 'ReAct' folder. At the top of this area is a breadcrumb 'ReAct' with a '+' icon to its right. Below this is a table listing the folder's contents. The table has columns for 'Name', 'Size', and 'Modified'. Each row represents a folder, with a folder icon, the folder name, a share icon, a three-dot menu icon, the size, and the modification time.

Name	Size	Modified
Deliverables	2.4 MB	seconds ago
FORTH_admin	112 KB	a month ago
Grant_Agreement	29 MB	2 months ago
Proposal	140.4 MB	3 days ago
Templates	1021 KB	an hour ago
WP1	19.7 MB	a day ago

Figure 12: OwnCloud of ReAct

8 Conclusion

This deliverable presents the Dissemination and Communication Plan of the ReAct project. To do so, we have identified (i) the objectives of these activities, (ii) the target groups of these activities and (iii) the dissemination/communication mechanisms we plan to use. Some of the communication/dissemination activities have already started, including the web site, the social media, some initial publications/presentations etc.

We believe that this Dissemination/Communication plan should be updated regularly to identify and pursue new opportunities that may arise in Dissemination and Communication.

9 Glossary

- TAXII: Trusted Automated Exchange of Intelligence Information
- STIX: Structured Threat Information Expression
- OASIS: Organization for the Advancement of Structured Information Standards
- H2020: Horizon 2020 Work Programme
- DM: Dissemination Mechanism
- CSA: Coordination and Support Action
- cPPP: contractual Public Private Partnership
- EC: European Commission
- ECSO: European Cyber Security Organization
- WG: Working Group
- SWG: Sub-Working Group
- IT: Information Technology
- EU: European Union
- SME: Small Medium Enterprise
- KPI: Key Performance Indicator