P

ECHO

www.echonetwork.eu

The COVID-19 Hackers Mind-set

ECHO WHITE PAPER #1

ISSUED 8 APRIL 2020

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

Abstract

Monitoring the cybersecurity landscape and the increase of COVID-19 related cybercrimes reporting by cyber experts and law enforcement agencies worldwide, the ECHO network of cybersecurity centres has joined forces to establish its COVID-19 Cyber Defence Alliance. Its aim is to support all initiatives that aim at protecting the EU member states, key services and critical infrastructure from cyber attacks. By developing innovative ideas, hands-on guidance and solutions to tackle the COVID-19 cybersecurity threats, it will contribute to increase cybersecurity for the EU, the member states, its companies and citizens.

This white paper on the COVID-19 hacker's mind-set is a first outcome of this combined effort. On 6 April 2020, ECHO experts from 15 member states discussed together in two teams the COVID-19 hackers mind-set. The main conclusion is that this pandemic offers cyber attackers unique opportunities to leverage existing attack tactics, techniques and procedures to exploit new opportunities created by a massive increase of employees working from home, children using home computers for schooling, as well as the human factor and emotions caused by the pandemic. Regardless of the motives behind a hack (profit or societal disruption), there are now ample opportunities and methods to leverage the COVID-19 pandemic to engage in criminal cyber activities. This white paper gives an overview of a number of these; however, the list is not exhaustive and constantly evolving.

It is important to act now, in order to pre-empt short, medium and long term damage to our digital society and infrastructure. Basic COVID-19 specific cyber awareness messages for the general public, easy to understand and share, should be disseminated on a daily basis. Similarly, specific information for companies and sectors should be made available through early warning information sharing networks, in order to ensure that they also take appropriate measures to protect themselves and our economy against cyber crime.

The diverse, pan European cyber security ECHO network will continue to develop innovative ideas, hands-on guidance and solutions to tackle the COVID-19 cybersecurity threats.

Keywords: cyber security, COVID-19, attack vectors, attackers profiles, transversal issues, mitigation measures.

Contents

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

Introduction

Monitoring the cybersecurity landscape and the increase of COVID-19 related cybercrimes reporting by cyber experts and law enforcement agencies world wide, the ECHO network of cybersecurity centres (ECHO) has joined forces to establish its COVID-19 Cyber Defence Alliance. Its aim is to support all initiatives that aim at protecting the EU member states, key services and critical infrastructure from cyber attacks.

By combining the expertise of its diverse, pan European network the ECHO network will develop innovative ideas, hands-on guidance and solutions to tackle the COVID-19 cybersecurity threat. Short term activities include the organisation of hackathons to identify relevant assets and vulnerabilities, identify potential attack methods and define and test possible mitigation measures, such as a COVID-19 cyber attacks specific Early Warning System.

The first online hackathon took place on 6 April 2020, where our experts from 15 members states discussed together in two teams the COVID-19 hackers mind-set. The main findings are detailed in the following paragraphs. Future hackathons will refine and operationalize these results in line with the cybersecurity products and services the ECHO network is currently developing.

If you want to receive future white papers or are interested in the ECHO project and joining the network, please contact us: info@echonetwork.eu or visit our website: https://echonetwork.eu/

Main findings

General considerations

The general conclusion is that currently, to a large extent the approaches and the technology being used by hackers is the same as it was before. However, there are two differences. Firstly, the significant, often improvised transition to online working and schooling. Secondly, hackers are now exploiting the fact that the human factor is an even bigger weakness than before. He or she is afraid of getting ill, is concerned about family and friends, and is at home with ample time to search the web for more information on the pandemic. This concern, angst and (perceived) lack of information can lead to a lower threshold of being suspicious before clicking on a link, downloading a file, installing a plugin, inserting personal data on a website. People have a higher cyber risk acceptance level because of the COVID-19 pandemic and can therefore become more vulnerable, more easily exploitable as a target for hackers.

Profile of the attacker

Three profiles of potential threat actors are identified: the criminal hacker, the hacktivist and the nation state supported hackers group. The terrorist hacker has briefly been discussed, but not further elaborated as it was seen to fall under a sub-type of the hacktivist or nation state hacker.

The main goal of the **criminal hacker** is profit in different forms: bit coins directly paid or for instance access to a national customs database in order to hack the inspection algorithm. The shift to online working and schooling resulting from the COVID-19 pandemic offers the criminal hacker a major new opportunity to hack into personal and small, medium and large corporate networks.

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

The **hacktivist** is concerned about the levels of governmental control on society as a result of the measures taken to control the spread of the COVID-19 pandemic. This is seen as a power grab or a conspiracy to control the population. The actions taken aim at creating disruption in the midst of the pandemic.

The interest of the **nation state supported hackers group** is to disrupt another nation state, for instance by spreading disinformation to influence the trust between citizens and their national and supra-national governmental institutions. During the COVID-pandemics trust between citizens and authorities is of crucial importance for effective crisis management and a speedy return to a recovery phase. Spreading disinformation can slow down this process and even affect geopolitical alliances.

Nation state hacker groups could also deliberately target critical services, to create additional chaos and fear in the midst of the pandemic, such as hospitals or logistics supply chains. They could also use the opportunity to get a foothold inside critical infrastructure or government networks for later use.

Modus operandi of attack

Several attack vectors were discussed in combination with the different profiles of the attackers.

- **Emails**
  Emails are seen as a primary attack vector, with different ways to tempt the recipient to for instance open an attachment, download a file and/or click on a URL-link visiting a cloned website, or fool the victim with a spoofed email. It was noted that for specific online conference applications, a spike has been recorded of related domain names registrations, thus allowing for the creation of cloned webpages.

  Multiple different attack scenarios were discussed:

  - Emails posing as a national health organisation or the WHO and asking the user to click on a link to read an urgent update on how to protect yourself against the virus, or to open and read an attached file that is in reality a weaponized pdf file.
  - Emails enticing to discover the real truth about COVID-19, feeding in on the conspiracy theories.
  - Emails asking to donate money to a local hospital or nursing home to buy personal protective equipment (PPE).
  - Emails asking to trace the delivery of a parcel, taking advantage of the major shift to home delivery. Users are asked to make an appointment for a drive by, of course requiring them to provide personal data.
  - Emails mimicking nursing staff asking to wire money to help a family member, desperately in need of medical treatment.
  - Emails asking to buy COVID-19 test kits online, linked to a fraudulent page.
  - Emails from medical insurance company asking to check your health insurance and make sure that your policy is up to date.

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

- Emails from medical insurance company informing that due to the COVID-19 workload, it is migrating to a new customer system and requires the user to login and provide his/her Social Security data in order to make sure that he/she that stays covered by the health insurance.

- Emails mimicking the national civil protection authority and asking to download a health tracking device or clicking on a link to register as "corona-free" citizen.
- Emails targeting employees of key institutions in the fight of COVID-19 (WHO, DG SANCO, national health ministry) in order to break into that network and send out fake fake news/warnings, etc.

- Cloned webpages and emails targeting SME´s transition to work online, exploiting their lower cybersecurity awareness and competence levels (larger corporations are better protected). Large amounts of small ransomware infections are also economically interesting for hackers.

- Emails mimicking the telecom operator, offering for free to increase the Internet speed, increase the volume of data for this month, the storage capacity, etc. by clicking on a link and inserting the users phone number or credentials.

- Spoofed email from the company about an urgent meeting later that day about the financial state of the company and temporary lay-offs. Clicking on the link, leads to a pop-up to download a viewer, which is infected with malware.

- **SMS/Whats App messages**
  Another attack vector is SMS messages with links to cloned websites from authorities. The SMS pretends to say this is an up to date urgent information regarding your city or town, and that you need to check in now to make sure that you're registered so that in case of a massive outbreak of COVID-19 in your area, we can come and protect/help you. The link in the message links to a cloned website, where the user inserts his/her personal data.

- **Remote access and BYOD (Bring your own device) usage**
  The sudden shift to online working could not be properly prepared by many companies. This results in insufficient numbers of corporate laptops that are available for staff members. The consequence is that employees use their own device for teleworking. Home PCs may be particularly vulnerable because they typically don't necessarily comply with the company policy in terms of endpoint protection. Consequently, a lot of these devices will be more vulnerable for all types of exploits such as browsers and office tools that are not up-to-date, plugins and PDF viewers that are not up-to-date, and so on. In addition, these personal devices often are of dual use (parents' work and children's schooling) and the shift to online working requires the installation of online conferencing plug-ins, apps and other software. If these installs are malicious or not properly configured, then they will create new opportunities for all types of criminal exploits.

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

- **Remote access and critical infrastructures providers**
  Critical infrastructure providers such as energy providers have control rooms that historically have been stand-alone, without any remote access. Recent years have seen a shift to allow remote access, be it very carefully. However, due to the COVID-19 pandemic, this limited pace is now speeding up significantly and increasingly remote access is enabled, due to the business continuity requirements. If not properly set up, this can create serious vulnerabilities that can be utilized now or at a later date.

- **Medical devices**
  The increased need for and production of ventilators and other medical equipment raised the concern that this is a perfect time to integrate malware or chips into the equipment, as the need for speed of production can affect negatively the testing and cyber security protocols of these devices. Such vulnerabilities can then be exploited in the long term to affect the health infrastructure.

- **COVID-19 mobile applications**
  The market for COVID-19 related mobile applications is dynamic. World-wide online hackathons are organised to "Hack the crisis" and many innovative ideas for applications are being developed or already available for download. Examples are: Waze for supermarkets to track the queues in front of your local supermarket, contact tracking based on Bluetooth and secret tokens, applications that warn you if someone gets closer by than 1.5 metres and applications that preform checks on patients in quarantine (e.g. to SMS a picture with geographical meta data within 15 minutes). Such applications can be used as attack vectors to steal personal information. In addition, for the contact tracking and patient control apps there are concerns about privacy, data integrity and cyber security. Because of the pandemic the attack surface for hackers targeting mobile apps has increased dramatically since users who normally do not easily install apps will now more easily be coerced to install apps.

Transversal or inter-sector issues

In terms of transversal and inter-sector issues, it was noted that our societies are strongly relying on logistics for basic supplies (food, utilities, medical, etc.). Targeting the logistics of a harbour, or an airport with the aim of breaking logistic systems with a ransomware or any other attack could be a potential target for a nation state hacker group to create chaos.

Mitigation measures

One major mitigation measure to take quickly is to make the general public especially aware of the fact that especially during these hard times they will be targeted as a potential victim by cyber hackers. Now even more than before they need to act responsibly in cyberspace and be cyber aware.

Disseminating specific and easy to share messages explaining how hackers can exploit the COVID-19 pandemic is advisable. The ECHO network COVID-19 Cyber Defence Alliance has started a widespread online campaign, with these potential exploits, to warn citizens against risks.

For companies the main mitigation measure discussed was to prioritize a specific vulnerability assessment of home users connected over VPN to the corporate network. It is important to restrict home computer access to the assets in

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

the corporate network and introduce additional choke points. As an example when full access to a central file sharing system is provided over VPN this could potentially allow a home computer that is infected by a ransomware to encrypt critical files and cause major economic damage to the company. Home PCs should therefore only be allowed a restricted access to the corporate services. Access to the file sharing system could for instance be implemented through a web interface with manual uploads, rather than through automatic synchronisation.

At a pre-emptive level it is also important to fast-track the development of COVID-19 specific Early Warning Systems, where public, private and non-governmental organisations can securely share information. The ECHO project is developing such a system and will test the beta version of the system shortly, specifically targeting COVID-19 related cyber threats.

Conclusions

The COVID-19 pandemic offers cyber attackers unique opportunities to leverage existing attack techniques to exploit opportunities created by the increasing number of home workers and shared home computers also used for remote schooling, as well as social engineering targeting the human being and the emotions caused by the pandemic. Regardless of the motive behind the hack (profit or societal disruption), there are now ample opportunities and methods to leverage the COVID-19 pandemic to more successfully engage in criminal cyber activities. This white paper gives an overview of a number of these; however, the list is not exhaustive and constantly evolving.

It is important to act now, in order to pre-empt short, medium and long term damage to our digital society and infrastructure. Basic COVID-19 specific cyber awareness messages for the general public, easy to understand and share, should be disseminated on a daily basis. Similarly, specific information for companies and sectors should also be made available through information sharing networks, in order to ensure that they also take appropriate action to protect themselves and our economy against cyber crime.

The diverse, pan European cyber security ECHO network will continue to develop innovative ideas, hands-on guidance and solutions to tackle the COVID-19 cybersecurity threats. If you want to receive future white papers or are interested in the ECHO project and joining the network, please contact us: info@echonetwork.eu or visit our website: https://echonetwork.eu/

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

References

The following online resources were shared by the hackathon participants and are useful starting points for further orientation:

Overview of cyber attacks and threats related to the global pandemic

https://www.webarxsecurity.com/covid-19-cyber-attacks/
https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/
https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/
https://hotforsecurity.bitdefender.com/blog/cybercriminals-move-quickly-in-uk-to-abuse-distress-over-coronavirus-pandemic-22736.html
https://www.smh.com.au/national/nsw/absolute-perfect-time-for-cybercriminals-to-attack-as-businesses-work-from-home-20200327-p54el7.html
https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats#
https://www.techradar.com/news/zoom-related-domain-names-grow-significantly-as-malware-threat-rises
https://www.schneier.com/blog/archives/2020/04/cybersecurity_d.html

News articles on attacks on the heath infrastructure

https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak
https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934