Newsletter September 2020

Center for Cyber Security and International Relations Studies

Upcoming Events

14th-16th September 12TH CONFERENCE O SECURITY AND CRYPTOGRAPHY FOR NETWORKS – Organized in cooperation wi IACR

27th September #RomHack2020 - cyber security conference

Cyber Policy, Diplomacy & Legal Framework

- Make the Internet Great Again?
  The internet's future will not be among those soundbites, but this issue will confront the next US administration. For the United States, the internet ain't what it used to be. Changes across multiple policy fronts over the past decade or more have converged to undermine U.S. power, interests, and ideas in cyberspace
- Changes to Japan's data privacy law echo Europe's GDPR
  Japan has made changes to its 2005 Protection of Personal Information (APPI) Act, bringing the bill closer in line with the EU's General Data Protection Regulation (GDPR). The latest tweaks, announced this month, cover data breach reporting and the use of facial recognition data gathered from devices such as security cameras
- Technologies of Freedom Enabling Democracy in Africa
  Over the past two decades, authoritarian governments in Africa, with more than a little help and inspiration from Chinese and Russian information control models, have tightened their grip on their national cyberspace by imposing internet censorship.
- Closing the Book on Huawei's Global Aspirations
  On August 17, the U.S. Department of Commerce announced that non-U.S. companies were prohibited from selling items produced with U.S. technology to Huawei. The decision follows restrictions imposed by the Commerce Department in May against companies using U.S. technology to manufacture Huawei-designed chips
- Ransomware attacks against SMEs fall sharply in Southeast Asia
  The number of ransomware attacks being launched against small and medium-sized enterprises (SMEs) in Southeast Asia has plummeted this year, according to data from Kaspersky. The cybersecurity firm says that the number of attacks it has detected and

blocked in the region fell from 1.4 million between January and June 2019 to around half a million in the first half of 2020 – a decline of more than 64%.

Cyber Security

- Apple Formally Adopts Human Rights Policy in the Wake of Criticism of Manufacturer Working Conditions & Freedom of Expression Issues

Most of the big tech companies have a formal human rights policy of some sort that is available online, usually a fairly boilerplate PR measure and legal compliance statement that Apple itself has published a version of in years past

- The Cyber Side of Vaccine Nationalism

In the COVID-19 pandemic, vaccine nationalism has become an important and controversial phenomenon. Rather than cooperate through global mechanisms to develop, manufacture, and distribute a vaccine against the coronavirus, countries with the means to do so have prioritized national access to a vaccine

- Postal Service Used Apps That Had 'Catastrophic' Vulnerabilities for Years
  The USPS Office of Inspector General found that the Postal Service was using several applications laded with vulnerabilities that could have led to a hack with a potential financial impact of over $1 billion.
- APT Groups Increasingly Targeting Linux-Based Devices
  APT groups are increasingly executing targeted attacks against Linux-based devices as well as developing more Linux-focused tools, according to an investigation by Kaspersky. This is as a result of a growing number of organizations' selecting Linux ahead of Windows to run their strategically important servers and systems, and the perception that the Linux operating system is safer and less likely to be targeted by malware as it is less popular.
- QBot, the banking trojan continues to make victims in the cyberspace
  QBot, also known as Qakbot and Pinkslipbot, is a prolific banking trojan that has been in business for over ten years (originally identified in 2008). According to a new report, a new malspam campaign carrying the QBot trojan resumed at the beginning of August, spreading globally in particular on US and European targets among government, military and manufacturing bodies

Cyber Warfare, Intelligence and Terrorism

- The notorious Lazarus group is attacking the world, an expert told CyberNews
  The infamous Lazarus hackers linked with North Korea are after money

and intelligence. CyberNews spoke to the security researchers who have been following Lazarus. They say these hackers are using highly sophisticated attack forms.

- Cyberwarfare: the New Frontier of Wars Between Countries
  While cyber space is the digital savior during this COVID-19 era, we are witnessing incidents related to cyber-attacks, hacking and data breaches, which highlights that the internet is not safe. It is imperative to be aware of cyberwarfare, as awareness is the first most important step to mitigating it.
- Iran says sabotage caused explosion at Natanz nuclear site
  Iran's Atomic Energy Organization has said an explosion last month that damaged the country's Natanz nuclear facility was the result of "sabotage".
- Russia, China and Iran hackers target Trump and Biden, Microsoft says
  The Russian hackers who breached the 2016 Democratic campaign are again involved, said the US tech firm. Microsoft said it was "clear that foreign activity groups have stepped up their efforts" targeting the election. Both President Donald Trump and Democrat Joe Biden's campaigns are in the cyber-raiders' sights
- New Zealand Stock Exchange Shut Down by DDoS Cyber Attack
  New Zealand's Stock Exchange Market (NZX) suffered cyber attacks for four days in a row, forcing the government to activate the country's National Security System. The NZX was forced to close on the fourth day of the attacks after crashing due to systems connectivity issues
- Hong Kong's internet freedom fighters: Big Tech should reconsider what data they collect
  Some of Hong Kong's internet freedom fighters would rather see tech giants leave Hong Kong. Ultimately, the companies will have to comply with the Chinese national security law and leave millions of Hongkongers vulnerable to surveillance.

Cyber Opportunities: Economy, Research & Innovation

- Microsoft's underwater data centre resurfaces after two years

Two years ago, Microsoft sank a data centre off the coast of Orkney in a wild experiment. That data centre has now been retrieved from the ocean floor, and Microsoft researchers are assessing how it has performed, and what they can learn from it about energy efficiency

- With TikTok, Oracle hopes its cloud infrastructure business goes viral
  Oracle is betting that by landing big cloud reference customers like TikTok and Zoom will be enough to get its infrastructure-as-a-service ambitions rolling.
- Could the Short-Term Future of Enterprise Cybersecurity Lie Within VPN?
  When we talk about cybersecurity, we often talk about the need to deploy sophisticated solutions to combat increasingly sophisticated attacks. As machine learning, artificial

intelligence, quantum computing, and other emerging technologies gain ground in the enterprise market legally, so to do bad actors seeking to use them in cyber-attacks.

- House Energy and Commerce Greenlights Bill to Explore AI, Blockchain Use for Consumer Safety
  Bipartisan legislation introduced last week that would direct a government-led look into using blockchain technology to better secure transactions and protect consumers from fraud gained a new path forward in Congress.
- How The Human And Machine Workforce Is Being Accelerated By COVID-19
  One of the most obvious benefits of employing robot "helpers" is that they cannot get sick, and are therefore able to take over risky jobs that would otherwise endanger human workers through frequent or prolonged physical contact with others.
- Demonstrating Scientific Data Integrity and Security in the Cloud
  Companies in the life sciences space often generate loads of data—that much is self-evident, but how to store it may not be so straightforward for the organizations themselves. While more and more organizations are shifting from on-premise to cloud-based storage systems (and will enjoy a competitive advantage of doing so), some may hesitate, fearing an inability to interpret or comply with regulations, or perhaps that their data will not be secure.

Italian Focus

- Italian Municipalities continue to block 5G even after the government ban
  Although the Simplifications decree prevents mayors from banning 5G networks, the orders against. With time risks and legal fees for cancellations

- Phishing, in Italy an increase in cases of the 'CEO scam'
  In our country, malicious computer activities known as "CEO scam" against important Italian companies and public administrations have increased. This was revealed by the Italian CSIRT, the new team born last May to manage the Italian national cyber-defense, set up at the Information Security Department (DIS).
- What do we know about the cyber attack at the University of Tor Vergata
  A ransomware has armored documents and research related to the coronavirus. The perpetrators of the violation are investigated. No ransom was asked
- Zhenhua case, Copasir investigates Chinese data.
  Parliament must investigate the filing of the data of almost 5,000 Italians by the Chinese pro-government company Zhenhua Data. Word of Antonio Zennaro, deputy and member of Copasir, who tells Formiche.net: if this is the model for the Silk Road of Health, there is little to be calm

European Focus

- Norwegian Parliament Hackered

The Norwegian parliament suffered a hacker attack, with the e-mail accounts of several ministers, MPs and employees being hacked.

- Coronavirus: Commission starts testing interoperability gateway service for national contact tracing and warning apps

  To exploit fully the potential of mobile proximity contact tracing and warning apps to break the chain of coronavirus infections and save lives, the Commission is setting up an interoperability gateway service linking national apps across the EU

- #Disinformation: EU presses social media firms to fight fake news

  Two years after agreeing to a self-regulatory code of practice to tackle disinformation, Facebook, Alphabet's Google, Twitter and other tech rivals must try harder to be more effective, the European Commission said on Thursday.

- European ISPs report mysterious wave of DDoS attacks

  More than a dozen internet service providers (ISPs) across Europe have reported DDoS attacks that targeted their DNS infrastructure. The list of ISPs that suffered attacks over the past week includes Belgium's EDP, France's Bouygues Télécom, FDN, K-net, SFR, and the Netherlands' Caiway, Delta, FreedomNet, Online.nl, Signet, and Tweak.nl.