28 June 2017

Synopsis

Scroll to read full summaries with links to news articles.

A major **cyber attack** has struck companies across the world for the second time in as many months. The **ransomware** attack has targeted critical infrastructure as well as shipping and banking sectors.

An alliance of 17 EU leaders have called on **EU Council** President **Donald Tusk** to set aside time for an EU wide summit on digital issues, with the 17 countries expressing interest in discussion of the EU's **digital single market policy**.

The **German Bundestag** has granted German law enforcement further powers to access **encrypted communications** in a greater number of instances. The law will allow **law enforcement** to use malware to watch encrypted communications in real time.

Israel and the **USA** have announced a new agreement to strengthen **cybersecurity** cooperation between the two countries.

Further **cyberespionage** tools alleged to have emanated from the **US** Government have appeared on the **Wikileaks** website. The new tool is believed to have allowed the **CIA** to access air-gapped computer networks through the use of infected flash drives.

Canada and **China** have announced an agreement to restrain from **cyber attacks** on each other's respective private sectors.

The **Chinese** Government have announced a new response plan to tackle future **cyberattacks** following a short legislative process.

Australia have announced plans to push for greater powers to access **encrypted messaging** as part of its intelligence alliance with the USA, UK, Canada and New Zealand.

ENISA have outlined the planned themes for this year's European Cyber Security Month in October. Amongst the planned events will be work to emphasise **cybersecurity skills**, **data protection** and the importance of cybersecurity in the workplace and home.

ICANN have released the final report of their study into the **Africa DNS market**, its first report of this kind in the continent.

For more information, visit the IEEE Internet Initiative website, and see *IEEE Global Internet Policy Monitor* past issues. Join IEEE Collabratec™ Internet Technology Policy Community discussions related to internet policy issues and to collaborate with other members of the global technical and policy communities.

IEEE Global Internet Policy Monitor

28 June 2017

Table of Contents

Synopsis 1

Europe 4
- Internet governance 4
- Cybersecurity 4
- Privacy 6
- Internet Inclusion 6

United States of America 6
- Internet governance 7
- Cybersecurity 7
- Privacy 7
- Internet Inclusion 9

Pan-Asia 10
- Internet governance 10
- Cybersecurity 10
- Privacy 11
- Internet Inclusion 11

Rest of the World 12
- Internet governance 12
- Cybersecurity 13
- Privacy 13
- Internet Inclusion 14

Global Institutions 15

Diary Dates 17

Europe

Internet governance

21.06.17

Euractiv

Estonia, Bulgaria and Austria 'presidency trio' outlines priorities

The three incoming presidencies of the EU Council, Estonia, Bulgaria and Austria have announced their priorities for their respective six month tenures. Estonia has announced its hope to focus on the EU's Digital Single Market during its presidency of the EU Council.

"Ministers representing the incoming Estonian, Bulgarian and Austrian presidencies of the Council of the EU outlined on Tuesday (20 June) their priorities, which seem to differ substantially.

Since 2008, the countries holding the rotating presidencies of the EU council work in "trios" and agree on 18-month joint programs, in an effort to be more coherent. Analysts have been critical as to the success of this effort."

22.06.17

Euractiv

Seventeen EU leaders ask Tusk for digital talks on 'highest level'

An alliance of 17 EU leaders have called on EU Council President Donald Tusk to set aside time for an EU wide summit on digital issues, with the 17 countries expressing interest in discussion of the EU's digital single market policy.

"On the eve of an EU summit, leaders from 17 EU countries have asked European Council President Donald Tusk for highest-level talks on EU digital policy, saying it was the single market's main engine and should receive stronger political support.

In a letter sent a day before the 22-23 June summit in Brussels, the leaders wrote that European unity needs a single market "of which the digital dimension is the main engine"."

Cybersecurity

24.06.17

Politico

UK Parliament hit by cyberattack

The UK Parliament has been targeted by a cyberattack that greatly affected the email system used by MPs.

"Cyber attackers struck the U.K. Parliament Friday night leaving MPs unable to access their emails if outside of Westminster today, according to the Telegraph.

Parliamentary authorities are working with Britain's National Cyber Security Centre to figure out the scale of the attack, the newspaper reported."

28.06.17

Reuters

Second major cyber attack in two months disrupts businesses around world

A major cyber attack has struck companies across the world for the second time in as many months. The ransomware attack has targeted critical infrastructure as well as shipping and banking sectors.

"A major cyber attack, believed to have first struck Ukraine, caused havoc around the world on Wednesday, crippling computers or halting operations at port operator Maersk, a Cadbury chocolate plant in Australia and the property arm of French bank BNP Paribas.

Russia's biggest oil company, Ukrainian banks and multinational firms were among those hit on Tuesday by the cyber extortion campaign, which has underscored growing concerns that businesses have failed to secure their networks from increasingly aggressive hackers."

Privacy

27.06.17

SC Media

Encryption-dodging hacking powers expanded for German law enforcement

The German Bundestag has granted German law enforcement further powers to access encrypted communications in a greater number of instances. The law will allow law enforcement to use malware to watch encrypted communications in real time.

"German law enforcement has been granted vast new hacking powers. The Bundestag - the German legislature - voted on June 22 to grant law enforcement the powers it needs to hack into, and spy on, smartphones and computers.

The ruling coalition government, made up of the conservative Christian Democrats and the centre-left Social Democrats, pushed hard for the law, arguing that the police will need to get around encryption if they are to do their job."

Internet Inclusion

27.06.17

Computer Weekly

BT launches free London Wi-Fi and phone calls

Public access to the internet in London is to be extended by BT the former state owned telecommunications company. BT is currently replacing traditional payphones with its own InLink street units that will provide both WiFi access and telephone coverage.

"London residents and visitors can now get free Wi-Fi and telephone calls after BT turned on its InLink street units which are replacing BT payphones in the UK capital.

There are plans to install 750 InLinks in central London and elsewhere in the UK over the next few years."

United States of America

Internet governance

26.06.17

The Hill

Trump administration unveils cyber pact with Israel

Israel and the USA have announced a new agreement to strengthen cybersecurity cooperation between the two countries.

"The Trump administration announced a new bilateral working group between the United States and Israel on cybersecurity.

Tom Bossert, White House homeland security and counterterrorism adviser, disclosed the new partnership to combat cyberattacks during remarks at an annual cybersecurity conference in Tel Aviv."

Cybersecurity

22.06.17

Reuters

Google pushes framework for law enforcement access to overseas data

The internet giant Google has called for greater discussion between US and international lawmakers on the access law enforcement is given to personal data stored overseas.

"Alphabet Inc's Google pressed U.S. lawmakers and the international community on Thursday to update laws on how governments access customer data stored on servers located in other countries, hoping to address a mounting concern for both law enforcement officials and Silicon Valley.

The push comes amid growing legal uncertainty, in the United States and across the globe, about how technology firms must comply with government requests for foreign-held data. That has raised alarm that criminal and terrorism investigations are being hindered by outdated laws that make the current process for sharing information slow and burdensome."

23.06.17

SC Media

Wikileaks releases CIA tool set which help malware onto air-gapped PCs

Further cyberespionage tools alleged to have emanated from the US Government have appeared on the Wikileaks website. The new tool is believed to have allowed the CIA to access air-gapped computer networks through the use of infected flash drives.

"WikiLeaks on Thursday dumped more leaked CIA documents with its latest Vault 7 disclosures, this time publishing materials from a tool suite called Brutal Kangaroo that allows attackers to indirectly infiltrate a closed network or air-gapped computer using a compromised flash drive.

The documents, dated between August 2012 and February 2016, reveal how CIA hackers would use the toolset to create a "custom covert network" within infected networks in order to conduct surveillance and launch executables."

23.06.17

The Hill

Dems push for more action on power grid cybersecurity

Nineteen leading Democratic Senators have called for a review by the Department of Energy into the cybersecurity protections of the USA's national power grid.

"Democratic senators are pushing for the Department of Energy "to conduct a thorough analysis of Russian capabilities with respect to cyberattacks on our energy infrastructure" after researchers detailed the malware used to blackout part of Ukraine's power grid in December

A letter dated Thursday to President Trump cosigned by 19 senators asks him to order the Energy Department to make such an inspection, chiding him for not conducting the analysis the first time the group sent him a request to do so on March 19."

28.06.17

Reuters

Second major cyber attack in two months disrupts businesses around world

A major cyber attack has struck companies across the world for the second time in as many months. The ransomware attack has targeted critical infrastructure as well as shipping and banking sectors.

"A major cyber attack, believed to have first struck Ukraine, caused havoc around the world on Wednesday, crippling computers or halting operations at port operator Maersk, a Cadbury chocolate plant in Australia and the property arm of French bank BNP Paribas.

Russia's biggest oil company, Ukrainian banks and multinational firms were among those hit on Tuesday by the cyber extortion campaign, which has underscored growing concerns that businesses have failed to secure their networks from increasingly aggressive hackers."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

26.06.17

Reuters

China, Canada vow not to conduct cyber attacks on private sector

Canada and China have announced an agreement to restrain from cyber attacks on each other's respective private sectors.

"China and Canada have signed an agreement vowing not to conduct state-sponsored cyber attacks against each other aimed at stealing trade secrets or other confidential business information.

The Canadian government, under pressure to show it is not being too soft on China, described the deal as a step toward dealing with Chinese espionage, the Globe and Mail reported on Monday."

Cybersecurity

28.06.17

Reuters

Second major cyber attack in two months disrupts businesses around world

A major cyber attack has struck companies across the world for the second time in as many months. The ransomware attack has targeted critical infrastructure as well as shipping and banking sectors.

"A major cyber attack, believed to have first struck Ukraine, caused havoc around the world on Wednesday, crippling computers or halting operations at port operator Maersk, a Cadbury chocolate plant in Australia and the property arm of French bank BNP Paribas.

Russia's biggest oil company, Ukrainian banks and multinational firms were among those hit on Tuesday by the cyber extortion campaign, which has underscored growing concerns that businesses have failed to secure their networks from increasingly aggressive hackers."

28.06.17

Strait Times

Beijing rolls out new intelligence law, cyber attack response plan

The Chinese Government have announced a new response plan to tackle future cyberattacks following a short legislative process.

"China's legislature passed a new intelligence law yesterday after an unusually brief round of discussions, a draft of which gave new powers to monitor suspects, raid premises and seize vehicles and devices.

Chinese President Xi Jinping has overseen a raft of legislation to bolster national security against perceived threats from both within and outside China."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

26.06.17

Reuters

China, Canada vow not to conduct cyber attacks on private sector

Canada and China have announced an agreement to restrain from cyber attacks on each other's respective private sectors.

"China and Canada have signed an agreement vowing not to conduct state-sponsored cyber attacks against each other aimed at stealing trade secrets or other confidential business information.

The Canadian government, under pressure to show it is not being too soft on China, described the deal as a step toward dealing with Chinese espionage, the Globe and Mail reported on Monday."

26.06.17

The Hill

Trump administration unveils cyber pact with Israel

Israel and the USA have announced a new agreement to strengthen cybersecurity cooperation between the two countries.

"The Trump administration announced a new bilateral working group between the United States and Israel on cybersecurity.

Tom Bossert, White House homeland security and counterterrorism adviser, disclosed the new partnership to combat cyberattacks during remarks at an annual cybersecurity conference in Tel Aviv."

Cybersecurity

21.06.17

SC Media

One quarter of Australian companies hit by phishing attack this week: Mailguard

A new security report has found that a quarter of Australian companies have been hit by a phishing attack that had originally targeted energy consumers.

"The phishing attacks against Australian energy customers grew yesterday with Mailguard reporting an enormous number of phishing attempts made centered on fake Origin Energy bills.

The attack is one of the largest recorded by MailGuard despite the fact that it ran for only a short period. Mailguard estimates the attack began around noon and ran into the later afternoon. The attack follows a similar barrage of phishing emails sent to EnergyAustralia customers earlier this week."

28.06.17

Reuters

Second major cyber attack in two months disrupts businesses around world

A major cyber attack has struck companies across the world for the second time in as many months. The ransomware attack has targeted critical infrastructure as well as shipping and banking sectors.

"A major cyber attack, believed to have first struck Ukraine, caused havoc around the world on Wednesday, crippling computers or halting operations at port operator Maersk, a Cadbury chocolate plant in Australia and the property arm of French bank BNP Paribas.

Russia's biggest oil company, Ukrainian banks and multinational firms were among those hit on Tuesday by the cyber extortion campaign, which has underscored growing concerns that businesses have failed to secure their networks from increasingly aggressive hackers."

Privacy

25.06.17

Reuters

Australia to seek greater powers on encrypted messaging at 'Five eyes' meeting

Australia have announced plans to push for greater powers to access encrypted messaging as part of its intelligence alliance with the USA, UK, Canada and New Zealand.

“Australia said on Sunday it will push for greater powers to tackle the use of encrypted messaging services used by terrorists and criminals at an upcoming meeting of ministers from the "Five Eyes" intelligence network.

The United States, United Kingdom, Canada, Australia, and New Zealand, will meet in the Canadian city of Ottawa next week, where they will discuss tactics to combat terrorism and border protection, two senior Australian ministers said.”

Internet Inclusion

No new items of relevance

Global Institutions

22.06.17

ENISA

Getting ready for the European Cyber Security Month 2017

ENISA have outlined the planned themes for this year's European Cyber Security Month in October. Amongst the planned events will be work to emphasise cybersecurity skills, data protection and the importance of cybersecurity in the workplace and home.

"100 days left for the launch of the European Cyber Security Month, the EU annual awareness campaign which takes place in October supported by ENISA and EC DG CONNECT with the participation of many partners from all over Europe.

"Cyber Security is a shared responsibility!" is the motto of the ECSM campaign. Preparation for this year's Cyber Security Month kick-off event is in collaboration with the Estonian Information Systems Authority. Taking place during the Estonian Presidency, the Estonian Ministry of Economic Affairs & Communication will be hosting the kick-off event at their premises in Tallinn on the 29th September 2017."

23.06.17

ITU

World Summit on the Information Society Forum 2017

ITU have produced a review of the 2017 WSIS Forum following its conclusion.

"A significant stride forward was achieved last week by the information and communication technology (ICT) for development community at the World Summit on the Information Society Forum 2017 (WSIS Forum 2017), attended by more than 2,000 stakeholders from 163 countries. Participants came together to share experiences, knowledge and perspectives; and to announce new tools and initiatives to use ICTs to advance the United Nations Sustainable Development Goals (SDGs) in such critical areas as ICT-centric innovation, accessibility, gender equality, youth empowerment, e-health and cyber security among many others."

24.06.17

ICANN

ICANN Releases its Final Report on Africa DNS Market Study

ICANN have released the final report of their study into the Africa DNS market, its first report in the continent.

"The Internet Corporation for Assigned Names and Numbers (ICANN) is pleased to announce the release of its Final Report on Africa Domain Name System (DNS) Market Study. This study serves as part of ICANN's outreach efforts to support and improve the regional DNS industry. The report is the first of its kind in the region, which includes 54 countries."

24.06.17

ICANN

Empowered Community Powers Triggered: FY18 Operating Plan and Budget, and Updates to Five-Year Operating Plan

ICANN have announced that the ICANN Board have formally adopted the organisation's Operating Plan and IANA Budget for the 2018 Financial Year.

"On 24 June 2017, the ICANN Board adopted ICANN's FY18 Operating Plan and Budget, the FY18 IANABudget, and updates to the Five-Year Operating Plan. Under ICANN's post-IANA Stewardship Transition Bylaws, the Empowered Community has the power to consider and, if they choose, to reject these documents before they go into effect.

ICANN's FY18 Operating Plan and Budget, the FY18 IANA Budget, and updates to the Five-Year Operating Plan are the result of 11 months of collaborative work by the organization, community, PTI Board, and ICANN Board Finance Committee."

Diary Dates

Modernising the regulations establishing the .eu top-level domain name – 05.05.17-04.08.17

European Commission

ICANN 59 – 26.06.17-29.06.17

Johannesburg, South Africa

16th European Conference on Cyber Warfare and Security ECCWS – 29.06.17-30.06.17

Dublin, Ireland

ITU WTDC-17 – 09.10.17–20.10.17

Buenos Aires, Argentina

ICANN 60 – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland