5 July 2017

Synopsis

Scroll to read full summaries with links to news articles.

Mariya Gabriel has been officially confirmed by the European Parliament as the **EU's** newest Commissioner for the **Digital Economy and Society**. A vote by national governments is expected within the next week to likely rubberstamp the decision.

Researchers from **F-Secure** have suggested that the hackers behind the **NotPetya** malware outbreak last week may have had access to computer exploits developed by the **NSA** before their publication by the **ShadowBroker** organisation.

Internet privacy advocates have challenged the latest move by security ministers of the **Five Eyes** alliance to introduce security **backdoors** to **encrypted communications** for the use of law enforcement.

Eugene Kaspersky has offered to turn over his company's computer codes to the **US** authorities in a bid to quash concerns that the company's **security** products have been infiltrated by the **Russian Government**.

Facebook have successfully completed the second test of their new **Aquila drone**, designed to provide **internet coverage** to remote areas traditionally inaccessible to traditional internet delivery systems.

Of the countries affected by the **NotPetya** malware last week, new research has shown that in the Asia Pacific region, **India** was most affected.

The **Chinese** Government have shut down the country's leading **VPN** service, GreenVPN, greatly increasing the strength of the ruling party's **Great Firewall**.

Nadav Argaman the head of the **Israeli Shin Bet** security agency has used the Israel **Cyber Week 2017** events to reveal that the country has successfully fended off over 2,000 lone wolf **cyberattacks** in the last year.

The government of **Ghana** have appointed **Albert Antwi-Boasiako** as the country's new Cyber Security Advisor. Mr Antwi-Boasiako is a leading **cybersecurity** expert and has previously worked as part of the Interpol Global Cybercrime Expert Group.

ENISA has published a new report identifying the outcomes of its 2016 **cybersecurity** exercises and proposed next steps for the development of EU wide responses.

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

5 July 2017

Table of Contents

Europe

Internet governance

04.07.17

Euractiv

Gabriel confirmed as new EU digital chief

Mariya Gabriel has been officially confirmed by the European Parliament as the EU's newest Commissioner for the Digital Economy and Society. A vote by national governments is expected within the next week to likely rubberstamp the decision.

"Mariya Gabriel was confirmed Tuesday (4 July) as the next EU digital Commissioner and will become the youngest person ever to take on a top Commission post.

MEPs approved Gabriel, a 38-year-old centre-right Bulgarian MEP, during a European Parliament plenary session, with 517 votes in favour, 77 against and 89 abstentions."

Cybersecurity

28.06.17

SC Media

Three-quarters of UK orgs suffer DNS attacks, half of those had data stolen

A report by EfficientIP has revealed the level of poor awareness relating to DNS attacks both in the UK and Globally amongst IT professionals.

"If not secured properly, DNS attacks could cost businesses over $2 million (£1.5 million) annually in data exfiltration, loss of business or application downtime, says a new report from EfficientIP.

According to the report, 94 percent claim DNS security is critical for their business. This is unsurprising as in the last 12 months, 76 percent of organisations around the world have been subjected to a DNS attack and a third suffered data theft."

30.06.17

Computer Weekly

NCSC rolls out four measures to boost public sector cyber security

The UK's National Cyber Security Centre has revealed four new measure as part of its Active Cyber Defence programme designed to protect the UK Government and other public bodies.

"The National Cyber Security Centre (NCSC) is rolling out four measures for government departments and "arms-length" public bodies to improve basic cyber security.

The measures are part of the Active Cyber Defence (ACD) programme, which is intended to tackle –in a relatively automated way – a significant proportion of the cyber attacks that hit the UK."

01.07.17

Ars Technica

NotPetya developers obtained NSA exploits weeks before their public leak

Researchers from F-Secure have suggested that the hackers behind the NotPetya malware outbreak last week may have had access to computer exploits developed by the NSA before their publication by the ShadowBroker organisation.

"The people behind Tuesday's massive malware NotPetya outbreak might have had access to two National Security Agency-developed exploits several weeks before they were published on the Internet, according to clues researchers from antivirus F-Secure found in some of its code.

EternalBlue and EternalRomance, as the two exploits were codenamed, were two of more than a dozen hacking tools leaked on April 14 by an as-yet unknown group calling itself the Shadow Brokers. Almost immediately, blackhat and grayhat hackers used EternalBlue to compromise large numbers of computers running out-of-date versions of Microsoft Windows. Within a week or two, blackhats started using EternalBlue to install cryptomining malware. No one really noticed until the outbreak of the WannaCry ransomware worm on May 12, which infected an estimated 727,000 computers in 90 countries."

02.07.17

BBC

Russia behind cyber-attack, says Ukraine's security service

Security services in Ukraine have alleged that Russia is responsible for the recent NotPetya global malware attack.

"Ukraine says it has proof that Russian security services were involved in the cyber-attack that targeted businesses around the world earlier this week.

The country's security service, the SBU, said it had obtained data that points to a link with an attack on the nation's capital, Kiev, in December."

04.07.17

Reuters

Germany big target of cyber espionage and attacks: government report

A new report by the German government has identified an increase in espionage and cyberwarfare directed at the country from Russia, Turkey and China.

"Germany is a big target of spying and cyber attacks by foreign governments such as Turkey, Russia and China, a government report said on Tuesday, warning of "ticking time bombs" that could sabotage critical infrastructure.

Industrial espionage costs German industry billions of euros each year, with small- and medium-sized businesses often the biggest losers, the BfV domestic intelligence agency said in its 339-page annual report."

Privacy

03.07.17

IT Brief Australia

Encryption with backdoors? Internet advocates call out Five Eyes leaders for 'shortsighted' tactics

Internet privacy advocates have challenged the latest move by security ministers of the Five Eyes alliance to introduce security backdoors to encrypted communications for the use of law enforcement.

“Major internet advocacy organisations such as InternetNZ are asking government officials to defend strong encryption and encryption technologies.

A Five Eyes ministerial meeting was held in Canada last week, in which encryption and major law changes surrounding the topic were in the spotlight.”

Internet Inclusion

No new items of relevance

United States of America

Internet governance

No new items of relevance

Cybersecurity

30.06.17

SC Media

Bipartisan bill aims to generate cyber hygiene best practices

A new bill has been introduced in the US Senate to create a baseline for standards and best practises for the country's cyber infrastructure. The bill also would instruct the Department of Homeland Security to carry out a risk assessment of the cybersecurity threat posed by Internet of Things devices.

"A bill introduced Thursday by the chairman of the Senate Republican High-Tech Task Force is intended to establish voluntary cyber hygiene best practices for companies and consumers.

"With cybercriminals growing bolder in their attacks, strengthening our cybersecurity infrastructure remains one of my top priorities in the Senate," according to a statement from Sen. Orrin Hatch, R-Utah, who unveiled the bipartisan bill. "Cyberattacks threaten our economy and inflict untold damage on thousands of Americans. Fortunately, proper cyber hygiene can prevent many of these attacks. This bill will establish best practices for cyber hygiene that will help Americans better protect themselves from enemies online."

01.07.17

Ars Technica

NotPetya developers obtained NSA exploits weeks before their public leak

Researchers from F-Secure have suggested that the hackers behind the NotPetya malware outbreak last week may have had access to computer exploits developed by the NSA before their publication by the ShadowBroker organisation.

"The people behind Tuesday's massive malware NotPetya outbreak might have had access to two National Security Agency-developed exploits several weeks before they were published on the Internet, according to clues researchers from antivirus F-Secure found in some of its code.

EternalBlue and EternalRomance, as the two exploits were codenamed, were two of more than a dozen hacking tools leaked on April 14 by an as-yet unknown group calling itself the Shadow Brokers. Almost immediately, blackhat and grayhat hackers used EternalBlue to compromise large numbers of computers running out-of-date versions of Microsoft Windows. Within a week or two, blackhats started using EternalBlue to install cryptomining malware. No one really noticed until the outbreak of the WannaCry ransomware worm on May 12, which infected an estimated 727,000 computers in 90 countries."

02.07.17

The Hill

Kaspersky willing to turn over source code to US government

Eugene Kaspersky has offered to turn over his company's computer codes to the US authorities in a bid to quash concerns that the company's security products have been infiltrated by the Russian Government.

"Eugene Kaspersky is willing to turn over computer code to United States authorities to prove that his company's security products have not been compromised by the Russian government, The Associated Press reported early Sunday.

"If the United States needs, we can disclose the source code," said the creator of beleaguered Moscow-based computer security company Kaspersky Lab in an interview with the AP."

Privacy

03.07.17

IT Brief Australia

Encryption with backdoors? Internet advocates call out Five Eyes leaders for 'shortsighted' tactics

Internet privacy advocates have challenged the latest move by security ministers of the Five Eyes alliance to introduce security backdoors to encrypted communications for the use of law enforcement.

“Major internet advocacy organisations such as InternetNZ are asking government officials to defend strong encryption and encryption technologies.

A Five Eyes ministerial meeting was held in Canada last week, in which encryption and major law changes surrounding the topic were in the spotlight.”

Internet Inclusion

30.06.17

USA Today

Facebook's Internet-delivering drone takes flight

Facebook have successfully completed the second test of their new Aquila drone, designed to provide internet coverage to remote areas traditionally inaccessible to traditional internet delivery systems.

“Facebook's solar-powered, Internet-providing drone successfully completed its second test flight over the Arizona desert last month.

The aircraft, called Aquila, aims to provide Internet access to remote corners of the world by transmitting a signal that can be received on the ground within a 60-mile radius.”

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

29.06.17

Petya ransomware cyberattack: India worst hit in Asia pacific region, claims Symantec

Of the countries affected by the NotPetya malware last week, new research has shown that in the Asia Pacific region, India was most affected.

"India has been the worst hit in the Asia-Pacific region by the 'Petya' ransomware that has claimed thousands of victims globally, security software firm Symantec today said. Globally, India ranked as the seventh most impacted nation.

Ukraine, the US and Russia were among the worst hit by Petya that struck organisations across the world earlier this week. Other countries that were impacted included France, the UK, Germany, China and Japan."

01.07.17

Ars Technica

NotPetya developers obtained NSA exploits weeks before their public leak

Researchers from F-Secure have suggested that the hackers behind the NotPetya malware outbreak last week may have had access to computer exploits developed by the NSA before their publication by the ShadowBroker organisation.

"The people behind Tuesday's massive malware NotPetya outbreak might have had access to two National Security Agency-developed exploits several weeks before they were published on the Internet, according to clues researchers from antivirus F-Secure found in some of its code.

EternalBlue and EternalRomance, as the two exploits were codenamed, were two of more than a dozen hacking tools leaked on April 14 by an as-yet unknown group calling itself the Shadow Brokers. Almost immediately, blackhat and grayhat hackers used EternalBlue to compromise large numbers of computers running out-of-date versions of Microsoft Windows. Within a week or two, blackhats started using EternalBlue to install cryptomining malware. No one really noticed until the outbreak of the WannaCry ransomware worm on May 12, which infected an estimated 727,000 computers in 90 countries."

05.07.17

Reuters

U.N. survey finds cybersecurity gaps everywhere except Singapore

The ITU's cybersecurity survey has demonstrated that countries with emerging economies are proving better able to defend their cyberspace than the world's richest countries.

"Singapore has a near-perfect approach to cybersecurity, but many other rich countries have holes in their defenses and some poorer countries are showing them how it should be done, a U.N. survey showed on Wednesday.

Wealth breeds cybercrime, but it does not automatically generate cybersecurity, so governments need to make sure they are prepared, the survey by the U.N. International Telecommunication Union (ITU) said."

Privacy

No new items of relevance

Internet Inclusion

03.07.17

Bloomberg

China's Great Firewall Gets Tougher as Popular VPN Shut Down

The Chinese Government have shut down the country's leading VPN service, GreenVPN, greatly increasing the strength of the ruling party's Great Firewall.

“Getting around the Great Firewall, the system used by China to control internet access, just got harder with a popular virtual private network forced to cease operating on orders from the government.

GreenVPN sent a notice to customers that it would stop service from July 1 after “receiving a notice from regulatory departments,” without elaborating on those demands. VPNs work by routing internet traffic to servers in another location, such as the U.S., that is beyond the reach of Chinese filters.”

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

29.06.17

SC Media

Israel Cyber Week 2017: cyber beat off 1,000s of 'lone wolf attacks'

Nadav Argaman the head of the Israeli Shin Bet security agency has used the Israel Cyber Week 2017 events to reveal that the country has successfully fended off over 2,000 lone wolf cyberattack in the last year.

"Israel has defended itself from more than 2,000 cyber- "lone-wolf attacks" said Nadav Argaman, director of Israeli security agency, Shin Bet, speaking at Cyber Week 2017 in Israel.

Shin Bet has succeeded "by means of technological, intelligence and operational adjustments, to thwart more than 2,000 potential lone wolf terrorists last year," Argaman said. Israel joins the UK which also admitted this week that it engages in offensive cyber-attacks."

30.06.17

Ghana News

Ghana government appoints Interpol Expert as Cyber Security Advisor

The government of Ghana have appointed Albert Antwi-Boasiako as the country's new Cyber Security Advisor. Mr Antwi-Boasiako is a leading cybersecurity expert and has previously worked as part of the Interpol Global Cybercrime Expert Group.

"The Ghana government has appointed a Cyber Security Expert with the Interpol Global Cybercrime Expert Group (IGCEG), Albert Antwi-Boasiako as Cyber Security Advisor.

A statement released here signed by Issah Yahaya, Chief Director at the Ministry of Communications said Antwi-Boasiako will oversee the implementation of the country's National Cyber Security Policy and Strategy (NCSPS)."

30.06.17

ABC News (Australia)

Cyber warfare unit set to be launched by Australian Defence Forces

Australia has incorporated cybersecurity into its national military for the first time with the launch of a new information warfare unit that will both defend the country from cyber attacks, whilst also conducting its own offensive operations.

"Australia's military is undergoing a major transformation, with the launch of a new information warfare unit.

The ABC has learned the team will launch within days and will be a central part of Australia's defence operations."

01.07.17

Ars Technica

NotPetya developers obtained NSA exploits weeks before their public leak

Researchers from F-Secure have suggested that the hackers behind the NotPetya malware outbreak last week may have had access to computer exploits developed by the NSA before their publication by the ShadowBroker organisation.

"The people behind Tuesday's massive malware NotPetya outbreak might have had access to two National Security Agency-developed exploits several weeks before they were published on the Internet, according to clues researchers from antivirus F-Secure found in some of its code.

EternalBlue and EternalRomance, as the two exploits were codenamed, were two of more than a dozen hacking tools leaked on April 14 by an as-yet unknown group calling itself the Shadow Brokers. Almost immediately, blackhat and grayhat hackers used EternalBlue to compromise large numbers of computers running out-of-date versions of Microsoft Windows. Within a week or two, blackhats started using EternalBlue to install cryptomining malware. No one really noticed until the outbreak of the WannaCry ransomware worm on May 12, which infected an estimated 727,000 computers in 90 countries."

02.07.17

BBC

[Russia behind cyber-attack, says Ukraine's security service]

Security services in Ukraine have alleged that Russia is responsible for the recent NotPetya global malware attack.

"Ukraine says it has proof that Russian security services were involved in the cyber-attack that targeted businesses around the world earlier this week.

The country's security service, the SBU, said it had obtained data that points to a link with an attack on the nation's capital, Kiev, in December."

Privacy

03.07.17

IT Brief Australia

[Encryption with backdoors? Internet advocates call out Five Eyes leaders for 'shortsighted' tactics]

Internet privacy advocates have challenged the latest move by security ministers of the Five Eyes alliance to introduce security backdoors to encrypted communications for the use of law enforcement.

"Major internet advocacy organisations such as InternetNZ are asking government officials to defend strong encryption and encryption technologies.

A Five Eyes ministerial meeting was held in Canada last week, in which encryption and major law changes surrounding the topic were in the spotlight."

Internet Inclusion

No new items of relevance

Global Institutions

30.06.17

ENISA

Cyber Europe 2016: Key lessons from a simulated cyber crisis

ENISA has published a new report identifying the outcomes of its 2016 cybersecurity exercises and proposed next steps for the development of EU wide responses.

"While a new ransomware campaign (Petya) is still ongoing, and a few weeks only after the WannaCry outbreak, the report sheds light on the preparatory steps taken by authorities and industry to respond to such cyber attacks.

Over 1 000 participants from all 28 EU Member States, along with Switzerland and Norway, joined last year in a simulated crisis which lasted for over 6 months, culminating in a 48-hour event on 13 and 14 October 2016."

05.07.17

ITU

ITU Global Cybersecurity Index 2017 shows improvements and strengthening of global cybersecurity agenda

ITU have produced an analysis of the agency's 2017 Cybersecurity Index, in the report the agency praises the improvements made to tackle various cybersecurity threats and has encouraged countries to continue to act to make the internet a more secure and safer environment.

"ITU, the United Nations specialized agency for information and communication technology, has published the Global Cybersecurity Index 2017 (GCI-2017), which measures the commitment of ITU's 193 Member States to cybersecurity and is the second in this index series.

The GCI-2017 measures countries' commitment to cybersecurity and helps them to identify areas for improvement. Through the information collected, it aims to illustrate the practices in use so that ITU Member States can identify gaps and implement selected activities suitable to their national environment – with the added benefits of helping to harmonize practices and fostering a global culture of cybersecurity."

Diary Dates

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

European Commission

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