Welcome to the Cyveillance Weekly Trends Report

Greetings from Cyveillance, the leader in open source threat intelligence. Since threat intelligence is constantly evolving, we publish this newsletter to keep our customers updated on the latest threats to various industries. Each week, we’ll send you highlights from our analyst research reports. You can unsubscribe at any time. For the latest security news stories throughout the day, you can also follow us on Twitter, or to view the latest security articles from Cyveillance experts, subscribe to our blog.

In this Issue:
- Top Weekly Incidents
- Energy
- Agribusiness
- Insurance /Healthcare /Pharmaceutical
- Financial Services
- Global Intelligence
- Legal and Regulations

New White Paper: Social engineering in a Web 2.0 world has evolved to a fine art, characterized by highly targeted, customized attacks. Download this whitepaper to learn more about what steps you can take to protect your organization.

Top Incidents

Energy

- Bloomberg reports the Obama Administration will propose new rules for transporting crude oil by rail, aimed at reducing speeds and requiring sturdier tanker cars. The rules are a reaction to a spate of derailments and explosions that have plagued the rail transportation of crude oil in North America recently, as the drilling and tracking boom has driven the amount of crude oil hauled by train to new heights. While the specifics
remain unknown, two unnamed sources told Bloomberg that the rules will include slower speed limits for trains to reduce accidents, and thicker hulls for the tanker cars to provide more protection should a derailment occur. They also said the new rules would apply to the rail shipment of ethanol biofuel.

**Agribusiness**

· On July 24, 2014, Sustainable Pulse reported on the Congressional briefing with prominent doctors, scientists, and business leaders. The participants urged Congress to push Obama to oppose the approval of Enlist Duo. Those who participated in the briefing included Dr. Philip Landrigan of Mount Sinai School of Medicine, Dr. Catherine Thomasson of Physicians for Social Responsibility, John P. Wargo, Ph.D. of Yale University, Doug Gurian-Sherman, Ph.D. of Center for Food Safety and Gary Hirshberg of Stonyfield Farm and the advocacy group Just Label It.

**Insurance/Healthcare/Pharmaceutical**

· A recent survey of 800 knowledge workers worldwide has found that 68 percent of professionals are exposing their companies' confidential information by failing to remove hidden data from documents they share with customers, suppliers or colleagues. That's happening even though 65 percent of employees believe it's their responsibility to ensure that sensitive company data is not leaked.

**Financial Services**

· Researchers have stated that criminals have been bypassing the Android-based two-factor authentication systems in use at 34 banks across four different countries, as part of a sophisticated spear-phishing and malware campaign that's been dubbed 'Operation Emmental.' Related attacks were first discovered about five months ago and have been actively targeting customers of financial services firms not just in Switzerland, but also Austria, Sweden, and starting in May, Japan. Operation Emmental attacks begin with spear-phishing e-mails, sent in a customer's local language that have malware attached. If users execute the malware, which may be disguised as a Windows update tool, the malware changes their system's settings to point to an attacker-controlled Domain Name System, thus allowing attackers to eavesdrop and control all HTTP traffic. The malware also installs its own Secure Sockets Layer certificate. To make the attack difficult to spot, the malware then deletes itself, leaving only the altered configuration settings.

**Global Intelligence**

· The Wall Street Journal's news graphic storage systems were breached this week. The systems have since been taken offline in order to isolate the attacks, but no damage was identified. However, the case is not closed and investigators are still looking into what is not the first attack on WSJ information systems. China was accused of hacking incidents against the major newspaper dating back to February 2013.

**Legal and Regulations**

· The National Labor Relations Board (NLRB) decided six social media related cases in the past three months, which resulted in five losses and only one victory for employers. These cases highlight the need for all employers to scrutinize their social media policies in an effort to determine whether employees reasonably would read them to prohibit discussion about the terms and conditions of employment for the mutual aid and benefit of the workforce, the applicable standard under Section 7 of the National Labor Relations Act (NLRA or “the Act”) for protected concerted activity.
Energy

- DeSmog.ca reports that John Paul Fraser, a former lobbyist for Enbridge Inc., is now the newly appointed head of the B.C. government’s communications branch.

- There is a renewed effort to find a permanent solution for the UK’s growing stockpile of nuclear waste comes after Cumbria council vetoed a proposed waste dump site in January 2013. But a new approach will not allow any one level of local government to veto future site decisions. The plan allows for communities to get up to £1m a year for about five years whilst local consultations take place. If the community moves to accepting exploratory drilling, which would take five to 15 years, they would get up to £2.5m a year, meaning a total of over £40m before a decision is taken on whether or not to build the waste burial facility. Additional and much higher community investment would follow a decision to build the facility. There is no cap on the number of communities that could apply for local consultation.

- The Sierra Club intends to hold Colorado Gov. Hickenlooper to his word that “every discussion about water should start with conservation.” Hickenlooper has instructed the Conservation Board (CWCB) to develop the first state-wide water plan.

- Bloomberg reports the Obama Administration will propose new rules for transporting crude oil by rail, aimed at reducing speeds and requiring sturdier tanker cars. The rules are a reaction to a spate of derailments and explosions that have plagued the rail transportation of crude oil in North America recently, as the drilling and tracking boom has driven the amount of crude oil hauled by train to new heights. While the specifics remain unknown, two unnamed sources told Bloomberg that the rules will include slower speed limits for trains to reduce accidents, and thicker hulls for the tanker cars to provide more protection should a derailment occur. They also said the new rules would apply to the rail shipment of ethanol biofuel.

- Pressure is growing on NRC Commissioner William Magwood to resign his position over conflict of interest charges stemming from his acceptance of a position as head of the OECD’s nuclear promotional arm, the Nuclear Energy Agency, while staying at the NRC, whose charter forbids promotion of nuclear power, for many months before beginning his new position.

- The European Commission is set to propose only modest new targets for energy efficiency, according to a draft document seen by Greenpeace Energydesk. The proposals are likely to suggest a target below 30% for 2030, lower than previous internal documents but in line with a leak earlier this month.

- Construction on the Rockaway Lateral natural gas pipeline in Brooklyn was briefly halted on July 19 when protesters entered a gate and stormed into the drilling site while chanting, “Go home, go home!” Saturday’s protest was the latest escalation in an 11th-hour campaign to halt the construction of the 26-inch pipeline, which will carry fracked natural gas under high pressure from an interstate transmission line off the coast into Brooklyn.

- A post announcing the latest national organizing call for August’s #RiseTogether mobilization indicates that the event now has 23 member groups.

- A train derailment last week in Seattle has heightened concern over energy trains in Washington State.

- Greenpeace has joined with Inuit activists to protest Canadian plans to use seismic testing to gauge Arctic oil and gas reserves.

- Greenpeace has issued a new plea to LEGO employees to advocate against renewing
LEGO’s partnership with Shell Oil.

- Albany County, NY is pushing a tough new oil train law.
- The Sierra Club is organizing rallies this week in Washington, DC, Denver, Atlanta, and Pittsburgh in order to demonstrate public support for a new EPA standard.

---

**Agribusiness**

- On July 24, 2014, Sustainable Pulse reported on the Congressional briefing with prominent doctors, scientists, and business leaders. The participants urged Congress to push Obama to oppose the approval of Enlist Duo. Those who participated in the briefing included Dr. Philip Landrigan of Mount Sinai School of Medicine, Dr. Catherine Thomasson of Physicians for Social Responsibility, John P. Wargo, Ph.D. of Yale University, Doug Gurian-Sherman, Ph.D. of Center for Food Safety and Gary Hirshberg of Stonyfield Farm and the advocacy group Just Label It.

- Several sources have written about the federal court case that started Wednesday, July 23, 2014 surrounding a new law going into effect next month in Kauai County. Four seed companies involved in the lawsuit are looking to stop the law before it goes into effect. The arguments of the case surround the question of whether or not the county has the authority to regulate GMO and pesticide use or whether that authority is superseded by the federal/state authority already in place.

- According to a post by the Facebook page Oregon Right To Know on July 23, 2014, the Secretary of State has certified the request for GMO labeling legislation by voters in Oregon. Initiative 44 will be put on the November ballot in Oregon, and if passed, the law requiring GMO labels on all foods would go into effect, January 1, 2016.

- On July 23, 2014, Sustainable Pulse posted an article about an alleged Glyphosate poisoning outbreak in the Canindeyu region of Paraguay. According to reports, 33 people (18 children included) have shown symptoms of poisoning. A 3-year-old and 6-month-old both died Tuesday, shortly after nearby fields were sprayed with Glyphosate weed killer. Government officials have ruled out poisoning from the herbicide, though the two children have been sent to the capital, Asuncion, for detailed autopsies.

- On July 21, Center for Food Safety published a press release reporting that the Vermont Public Interest Research Group (VPRIG) and Center for Food Safety (CFS) have formally announced their plans to help Vermont defend its GE food labeling bill, Act 120. The groups have filed legal papers to help in the defense of the state’s new law.

- Prices have for live cattle this week have hit all-time highs. Early this week some feed yards passed on packer bids of $162 per cwt. for fed cattle—about $5 per cwt higher than the previous record high. Friday morning live cattle sales were reported by USDA’s Market News service at $164 to $166. This spike came ahead of two USDA reports on cattle feed numbers scheduled for release Friday afternoon. Reports are expected to show drops in feed numbers from last year.

- NPR reported that many companies in the food industry are “Quietly Dumping GMO Ingredients” following consumers’ growing demand for non-GMO foods. But even as these companies create GMO-free products, many of these corporations are fighting state initiatives that would require them to give consumers more information about their ingredients.
Insurance

- A recent survey of 800 knowledge workers worldwide has found that 68 percent of professionals are exposing their companies' confidential information by failing to remove hidden data from documents they share with customers, suppliers or colleagues. That's happening even though 65 percent of employees believe it's their responsibility to ensure that sensitive company data is not leaked.

- Women & Infants Hospital (WIH) of Rhode Island first reported a data breach involving unencrypted backup tapes containing ultrasound images from two of its ambulatory sites that went missing back in Spring of 2012. WIH will settle a data breach that impacted 12,127 patients from Massachusetts and 1,877 residents from other states by paying $150,000 in penalties.

- In a new trend, crooks are trying to rip off insurance companies by targeting motorists and their cars. Planned auto insurance fraud has been huge in large cities for decades, but investigators say it now has established a real presence in Utah.

- A California court has given final approval for a settlement in a consolidated class action lawsuit against insurer Health Net related to a 2011 breach that affected about 2 million individuals.

- The Department of Health and Human Services (HHS) has proven how important it considers the Notices of Privacy Practices (NPPs) as part of the HIPAA Privacy Rule by both offering sample NPPs last year and recently introducing its NPP challenge winners.

- MobilexUSA formally notified affected Indiana patients of a possible breach of protected health information on Wednesday. As a precautionary measure, the company has retained on behalf of affected patients the services of Kroll Inc., a global leader in risk mitigation and response with extensive experience helping people who have sustained an unintentional exposure of confidential data.

- Sloane Stecker Physical Therapy, PC recently notified 2,000 patients of a breach after it learned that certain protected health information, including names, addresses, telephone numbers, and potentially other private information, was taken without its authorization from its secure computer network.

- BYOD poses some of the biggest privacy and security risks facing the healthcare sector, but the efforts of the new IBM/Apple alliance could help address concerns about using personally owned mobile devices.

- Car crash scams are becoming increasingly sophisticated, with the latest wrinkle involving organized groups gaining access to medical clinics to cash in on lucrative payouts for phony insurance treatments.

Pharmaceutical

- The Food and Drug Administration is warning doctors not to use compounded drugs from a Texas specialty pharmacy due to risks of contamination. The agency says FDA inspectors recently uncovered unsanitary conditions at Unique Pharmaceuticals' plant in Temple, Texas. The inspections revealed production problems in several lots of drugs that were supposed to be sterile.

- The All Party Pharmacy Group is calling for urgent action to address the continuing problem of medicines shortages in the UK, and is warning of snowballing problems seen for the first time in the supply of generic drugs.
Financial

Activism

- Housing activists held an anti-eviction protest on July 21st at Seattle [WA] City Hall in support of a local family facing a perceived unjust eviction from a leading U.S. bank.

- Housing activists last week held an anti-eviction blockade in St. Louis, MO in support of a local family facing eviction by a leading U.S. bank.

- Housing activists in Chicago, IL held an anti-eviction protest on July 26th in support of a local resident facing eviction by a government sponsored enterprise for housing.

- Housing activists will hold an anti-eviction protest at an eviction hearing on July 31st at a district court in Detroit, MI in support of a local resident facing eviction by a government sponsored enterprise for housing.

- A petition addressed to the US Justice Department, Indiana Attorney General’s Office, and Consumer Financial Protection Bureau accused a leading U.S bank, and government sponsored enterprise for housing, of violating the homeowners property rights.

- Pro-Palestine activists will hold protests on the 5th day of every month, starting on August 5th in front of a leading U.S. investment firm that’s known to invest in companies that allegedly profit from the Israeli occupation of Palestine.

- A Democratic congressional candidate for Florida will hold a rally in support of a local housing activist against “bad acting banks” on July 30th at the county court in Punta Gorda, Florida.

Information Security Risk

- A hacker breached the databases of a leading U.S. business newspaper by exploiting a SQL injection vulnerability in one of their web-based graphics systems and offered its stolen data for sale for 1 BTC apiece ($620).

- Researchers discovered that malware originally created for the purpose of government espionage, dubbed Gyges, is now undergoing a transformation as hackers are using the software to make their own rootkits and ransomware more sophisticated and harder to detect. It likely originated from Russia, and is virtually invisible and capable of operating undetected for long periods of time. Gyges uses sophisticated anti-tampering and anti-detection techniques as well as lesser known injection techniques. The malware waits for user inactivity before operating — in direct contrast to popular methods that activate when a user is active — which helps it avoid detection by sandbox-based security tools. The malware also uses a hooking bypass technique that exploits a log bug in Windows 7 and 8, both x86 and x64 versions, contains anti-debugging and anti-reverse-engineering defenses, and uses a “protector,” Yoda, which obscures malicious activity by converting the application into sections.

- Security researchers claim that the Tinnybank (Tinba) Trojan is now targeting banks in the Czech Republic by being attached to spam emails masquerading as legitimate debt notification emails from the government.

- Researchers have stated that criminals have been bypassing the Android-based two-factor authentication systems in use at 34 banks across four different countries, as part of a sophisticated spear-phishing and malware campaign that’s been dubbed ‘Operation Emmental.’ Related attacks were first discovered about five months ago and
have been actively targeting customers of financial services firms not just in Switzerland, but also Austria, Sweden, and starting in May, Japan. Operation Emmental attacks begin with spear-phishing e-mails, sent in a customer’s local language that have malware attached. If users execute the malware, which may be disguised as a Windows update tool, the malware changes their system’s settings to point to an attacker-controlled Domain Name System, thus allowing attackers to eavesdrop and control all HTTP traffic. The malware also installs its own Secure Sockets Layer certificate. To make the attack difficult to spot, the malware then deletes itself, leaving only the altered configuration settings.

- The U.S. law enforcement agency is investigating a series of credit card breaches involving a nonprofit 501(c)(3) organization that provides job training, employment placement services, and other community-based programs for people who have disabilities.

- A Russian ransomware threat ‘Simplocker’ that encrypts files stored on the SD memory cards of Android devices has been updated to target English-speaking users with FBI-themed alerts. The malware app was first identified in early June, and at the time, it was the first malicious program for Android devices that used file encryption to extort money from victims. The original variant was indicative of a work in progress and displayed ransom notes exclusively in Russian. But now Simplocker is being sold on underground forums and actively distributed to users, so it’s no longer just a proof of concept. A new variant found recently displays a message to victims in English that masquerades as an alert from the U.S. Federal Bureau of Investigation about illegal pornographic content being found on the device. The victims are instructed to pay a so-called fine of US$300 through a payment service called MoneyPak.

- Researchers said attackers suspected of residing in Russia raided Swiss bank accounts with a multi-faceted attack that intercepts SMS tokens and changes domain name system settings. That tactic was accomplished by malware that manipulated victims’ DNS settings and installed an SSL certificate for the phishing sites before wiping itself clean to remove evidence of infection.

- German authorities said the website of a European Central Bank was breached and contact information for event registrants stolen. The breach came to light when a hacker attempted to obtain a ransom to return stolen data to the bank. Breached data included e-mail addresses and other contact information, which were stolen from a public-facing ECB website. But the theft was from a database that is separate from any internal system, which is designed for event registration. The bank says no internal or market-connected systems were breached.

- Researchers identified a new generation of ransomware called ‘Trojan-Ransom.Win32.Onion.’ The new malware makes it extremely difficult for researchers to detect the threat actors behind it because it hides the command and control servers in the Tor anonymity network. In addition the use of an unorthodox cryptographic scheme also makes file decryption impossible, even if the traffic is intercepted between the Trojan and the server. The researchers said these improvements make Trojan-Ransom.Win32.Onion a highly dangerous threat and one of the most technologically advanced encryptors out there.

**Legal, Litigation, Regulatory Risk**

- A housing activist and a local resident in Anoka, MN claimed she lost her home because a government sponsored enterprise for housing illegally foreclosed on her by accelerating her loan balance. The activist filed a lawsuit against the enterprise in Hennepin County Court.

**Operational Risk**

- The Organization for Economic Co-operation and Development (OECD) last month at its
Global Forum on Responsible Business Conduct in Paris published a series of letters clarifying banks’ human rights responsibilities under UN Guiding Principles on Business and Human Rights. The letters date from November and December 2013, but have now been published for the first time.

- Saudi Arabia’s cabinet authorized overseas financial institutions to trade equities in the Tadawul and gave the Capital Market Authority scope to determine the timing. The CMA said in a statement, it is preparing to publish rules for qualified foreign financial institutions. Saudi’s exchange is currently limited to investors from the six-nation Gulf Cooperation Council.

- Turkey’s main stock exchange halted for about one hour shortly after it opened on July 22nd due to a glitch.

- A publicly traded Chinese company that sells and trades in imported automobiles publicly stated that it vigorously opposes a grossly unfair and damaging plan by a US post-trade financial services company to impose a ‘Global Lock’ on its securities. The CEO of the company argued that his China-based company should not be so severely punished after years of willing compliance with all applicable U.S. regulations.

- Two environmentalist groups continue to pressure U.S. investment banks to divest from companies engaged in mountaintop removal (MTR) coal mining operations in Appalachia. One of the groups recently passed out to nearly every West Virginia legislator two-dozen peer-reviewed articles backing up their claims about MTR destruction. The groups state that they are finding it easier to work outside the halls of government than within them to stop MTR destruction, and started an aggressive divestment campaign to compel banks to stop financing MTR projects.

Reputational Risk

- A post made on a popular Social Media site claimed several leading U.S. banks are amongst some of the major investors in private prisons in the U.S., and therefore encourages activists to boycott those financial institutions.

Global Intelligence

China

- 7/21/2014 - China Labour Bulletin reports that the Yue Yuen shoe factory in Dongguan, Guangdong Province site of the largest strike in China in recent memory, will be the nucleus of efforts by the Guangdong Federation of Trade Unions to institute a system of democratic trade union elections across the province within the next five years.

- 7/21/2014 – Nearly 300 workers went on strike at QLT Golf Supplies company in Shenzhen’s Bao’an District due to a dispute concerning employee benefits. Workers were able to reach a broad compromise with factory management and normal operations resumed the following day.

- 7/25/2014 – Microsoft plans to lay-off 18,000 employees by year-end, among which 12,500 will be cut from the recently acquired Nokia business. Reports also claimed 3000 positions will be cut in Beijing and Tianjin.

- On 7/20/2014, a Chinese news outlet report BigBoss, a source for iPhone news, jailbreak applications and guides speculated to experienced hacker attacks.

- On 7/22/2014, a Chinese technology news outlet reports iOS devices contains multiple backdoor services that could be use by law enforcement agencies, the U.S. National
Security Agency, or other malicious organizations to bypass iOS encryption, steal sensitive personal information.

- On 7/22/2014, a Chinese cyber security news outlet reports a WordPress plugin called MailPoet might contains security vulnerability that could be exploited by hackers and gain complete control.

- On 7/22/2014, a Chinese news outlet reports the number malwares targeting mobile devices in 2nd quarter of this year is 3 times the number of malwares comparing to the same period of last year.

- On 7/22/2014, a Chinese news outlet reports 3 active malwares targeting Android devices. They are Backdoor.Typideg, Backdoor.Kivars, Android.Selfmite. According to the article, Android.Selfmite is a trojan disguised as banking application to obtain user information.

- On 7/23/2014, a Chinese news outlet reports a security vulnerability on Linux that could be exploited by hackers to obtain Linux system's root privileges.

- On 7/23/2014, a Chinese cyber security news outlet reports Arbor Network, experienced frequent DDoS attacks over the first half of this year. According to the article, Arbor Network experienced more than 100 100GB/sec-DDoS attacks.

- On 7/25/2014, a Chinese technology news outlet reports that a security researcher at Chinese University of Hong Kong recently discovered a new method of hacking into Google Talk by exploiting vulnerabilities in Android. According to the researcher, an attacker can use Google Talk's search function to easily hack into and take control over a victim's device remotely.

Germany

- Skimming attacks on German ATM are at a record low. While 251 attacks were registered in 2013, only 84 ATM were compromised during the first six month of 2014. During this time, criminals were able to steal €1.4 million, also a sharp decline from 2013. Damages in the amount of €8.4 million were reported for the first six month of 2013 and €11.3 million for all of 2013. Industry insiders credit recent technology upgrades with the decline, e.g. payment cards with electronic chips instead of magnetic stripes would make it harder for criminals to use stolen card data. All 94 million debit cards in Germany now feature the chip technology, the same is true for all of the 60,000 ATM and additional 720,000 retailer terminals. Consequently, most transactions involving stolen card data is said to happen in countries still using the old magnetic stripe technology, e.g. Brazil, Sri Lanka, Indonesia, India, and the US.

Malaysia

- On 7/16/2014, a Malaysian news outlet reports boycotting Israel products and businesses will cripple Israel's economy and weakening its aggression towards Palestine.

- On 7/21/2014, a Malaysian news outlet reports unhealthy air pollution index at several areas in Penang Island due to the haze condition.

- On 7/23/2014, a Malaysian news outlet reports death related to dengue fever is still rising.

- On 7/16/2014, a Malaysian news outlet reports private firms in Malaysia are joining forces with Health Ministry to fight against increasing dengue fever cases in Malaysia.

North America

- The Wall Street Journal's news graphic storage systems were breached this week. The
systems have since been taken offline in order to isolate the attacks, but no damage was identified. However, the case is not closed and investigators are still looking into what is not the first attack on WSJ information systems. China was accused of hacking incidents against the major newspaper dating back to February 2013.

- On 7/23/2014, a news outlet reports security officers for Apple protested outside of an Apple store in San Francisco against a long term dispute over labor conditions.

### Legal and Regulations

#### Worldwide

- The FTC recently updated the Children’s Online Privacy Protection Rule (COPPA) Frequently Asked Questions (“FAQs”) section of its website to provide additional guidance with respect to interpreting the COPPA amendments. Specifically, the FTC made revisions to FAQ H.5, which focuses on obtaining parental consent through the collection of credit or debit card information; FAQ H.10, which focuses on obtaining parental consent through third party apps; and FAQ H.16, which focuses on third party platform liability for obtaining verifiable parental consent for app developers.

- Illinois Attorney General Lisa Madigan and the National Consumers League held a news conference to discuss data breach and identity theft, and advocate for new federal laws, including a national data breach notification law, and a new federal agency to investigate large-scale data breaches.

- The National Labor Relations Board (NLRB) decided six social media related cases in the past three months, which resulted in five losses and only one victory for employers. These cases highlight the need for all employers to scrutinize their social media policies in an effort to determine whether employees reasonably would read them to prohibit discussion about the terms and conditions of employment for the mutual aid and benefit of the workforce, the applicable standard under Section 7 of the National Labor Relations Act (NLRA or “the Act”) for protected concerted activity. The six cases are: Hoot Winc, LLC, Case No. 31-CA-104872 (May 19, 2014); Lily Transp. Corp., Case CA-108618 (April 22, 2014); Durham School Servs., L.P., 360 NLRB No. 85 (April 25, 2014); Professional Elec. Contrs. of Connecticut, Inc., Case No. 34-CA-071532 (June 4, 2014); Laurus Tech. Inst., 360 NLRB No. 133 (June 13, 2014); Landry’s Inc., Case No. 32-CA-118213 (June 26, 2014).

- New gTLD registrations continues to flourish. There was speculation (by the .xyz registry, but also by others) that “.xyz” would be the next “.com” and so far it does not disappoint. “.xyz” is by far the most popular new TLD so far. The “.com” domain is home to over 114,000,000 registrations, so “.xyz” is not even close to being the next “.com” but this is definitely a domain to watch and consider registering. Here is the list of the top ten new gTLDs: 1. “.xyz” (397,153 registrations); 2. “.berlin” (137,361 registrations); 3. “.club” (89,829 registrations); 4. “.guru” (66,515 registrations); 5. “.photography” (41,785 registrations); 6. “.wang” (40,715 registrations); 7. “.email” (36,636 registrations); 8. “.link” (34,941 registrations); 9. “.在xiuni7EBF” (33,965 registrations); and 10. “.today” (32,091 registrations).