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
- Financial Services
- Global Intelligence
- Legal and Regulations
- Pharmaceuticals
- Retail
- Technology
- Telecommunications
- Entertainment
- Defense
- Law Enforcement

Register Now for our December Webcast
Making the Business Case for Threat Intelligence

December 17, 1 pm ET

To adequately protect company assets and ensure business continuity in the face of today’s threats, organizations must be more proactive. Fortunately, many outside threats, actors and methods can be detected and studied in advance through open source Internet monitoring and intelligence analysis. In this webinar, we’ll discuss how you can make a practical case for deploying threat intelligence in your organization.

Top Incidents

Energy
- A new report finds that Iranian hackers have infiltrated major airlines, energy companies, and defense firms around the globe over the past two years in a campaign that could eventually cause physical damage. The report comes as governments scramble to better understand the extent of Iran's cyber capabilities, which researchers say have grown rapidly as Tehran seeks to retaliate for Western cyber attacks on its nuclear program.

Agribusiness
On December 9, 2014, Rainforest Action Network will be holding a Global Call-in Day targeting PepsiCo. They are urging supporters to call in to PepsiCo customer service numbers and providing scripts questioning and opposing the use of conflict palm oil in the company’s products.

Insurance/Healthcare

- A recent email phishing scam is targeting numerous organizations, including healthcare companies. More than 100 organizations have been attacked by cybercriminals for over a year, according to a report from FireEye, a security company. FireEye calls the online attackers FIN4, and explains that they don’t infect their victims with malware, but instead capture usernames and passwords to victims’ email accounts. From there they can read private email exchanges.

Financial Services

- For more than two years, pro-Iranian hackers penetrated some of the world’s most sensitive computer networks, including those operated by a US-based airline, automaker, natural gas producer, defense contractor, and military installation. In many cases, “Operation Cleaver,” as the sustained hacking campaign is being dubbed, has attained the highest levels of system access of targets located in 16 countries total, according to the security firm. Compromised systems in the ongoing attacks include Active Directory domain controllers that store employee login credentials, servers running Microsoft Windows and Linux, routers, switches, and virtual private networks. With more than 50 victims that include airports, hospitals, telecommunications providers, chemical companies, and governments, the Iranian-backed hackers are reported to have extraordinary control over much of the world’s critical infrastructure.

Global Intelligence

- Chinese news outlets reported that according to insiders at Samsung Electronics, the company may face a large-scale workforce reduction due to company profits reaching a three-year low point. It is rumored that the company may cut 20% of high level/executive positions, among which would include a 30% reduction in their mobile division.

Legal and Regulations

- Federal District Judge Paul Magnuson has ruled that banks that issued credit and debit cards to customers whose data was stolen in the December 2013 Target data breach could continue to litigate claims against Target for negligence and violation of Minnesota’s Plastic Security Card Act (“MPCSA”), Minn. Stat. § 325E.64.

Pharmaceuticals

- Foreign drug makers in China say they are concerned that recent regulatory delays could push back plans to introduce their newest medicines into the country by as many as two years.

Retail

- Researchers at Trend Micro have come across a sample of a new point-of-sale (PoS) malware that appears to be under development. Designated by the security firm as TSPY_POSLOGR.K, the threat relies on multiple components to carry out its mission, which makes it similar to a recently discovered variant of the notorious BlackPoS malware (TSPY_MEMLOG.A).

Technology

- The FBI is warning businesses about a new hacking threat in the wake of a vast attack on Sony Pictures last week. The threat comes from the same type of malicious software that infected Sony’s computer systems, a law enforcement official told CNN.
**Telecommunications**

- A data breach that affected Sony Pictures was initially thought to be the work of nation state hackers on behalf North Korea. Several media companies have since scrambled to protect their assets via increased security measures in wake of the attack. The FBI later confirmed that employees of Sony are being threatened by email by hackers assumed to be located in Bangkok, Thailand. The perpetrators of the attack have not yet been identified.

**Entertainment**

- Several professional athletes, including St. Louis Rams players, joined the "I Can't Breathe" protests on Sunday in memory of Eric Garner. Players paid tribute to the man who died after a chokehold by a New York police officer by displaying Garner's last words on their cleats, warmup shirts, tape, etc.

**Defense**

- Operation death click is an advanced persistent threat targeting the US defense industry. It uses social engineering, malvertising and real time bidding as its main tools to compromise victims’ computers, and utilizes digital advertising targeting technology to find victims. ODC is also defined as micro targeted malvertising — a combination of malvertising with targeted attacks.

**Law Enforcement**

- The Department of Justice is creating a dedicated cybersecurity unit within its Criminal Division which will serve as a central hub for law enforcement officials on legal guidance regarding the criminal electronic surveillance statutes that cover complex cyber investigations. The unit is intended to ensure that law enforcement’s electronic surveillance tools are effectively used, while also protecting the privacy of Americans.

**Energy**

- Environmental and anti-fracking groups on Wednesday launched a new campaign targeting Gov. Andrew Cuomo as his administration nears a final decision on hydraulic fracturing for natural gas. The campaign, #NotOneWell, which is being supported by Food & Water Watch, the Natural Resources Defense Council and other groups, will include billboards on busy Albany highways and radio advertisements across the state, according to the groups. They will also be rallying their followers to phone in to Cuomo’s office and chime in on social media, as well.

- The Center for Biological Diversity filed a notice of intent to sue the U.S. Interior Department for violating three federal laws by rubber-stamping offshore fracking in California's Santa Barbara Channel without evaluating its polluting effects on coastal communities or blue whales, sea otters and other marine wildlife.

- Gazprom, the Russian-owned energy behemoth, is suspected of funding anti-fracking protests in Eastern Europe, according to The New York Times. Russia reportedly sees fracking — a controversial drilling technology that has unlocked massive reservoirs of natural gas in the U.S. and elsewhere — as a threat to its domination of the European natural gas market.

- A new report finds that Iranian hackers have infiltrated major airlines, energy companies, and defense firms around the globe over the past two years in a campaign that could eventually cause physical damage. The report comes as governments scramble to better understand the extent of Iran's cyber capabilities, which researchers say have grown rapidly as Tehran seeks to retaliate for Western cyber attacks on its nuclear program.
The research and development manager at Sandia National Laboratories has been tapped to take over recovery efforts at the federal government’s troubled nuclear waste repository in southern New Mexico. The U.S. Energy Department’s Carlsbad Field Office made the announcement about Sean Dunagan’s appointment Thursday. He will officially begin his new duties at the Waste Isolation Pilot Plant next week. Dunagan replaces Tom Teynor, who returned to the Hanford Site in Washington state. A final accident investigation report is expected before the end of the year.

The DeSmog blog has posted reporting that in a newsletter to clients titled “Defending Your Company Against an Activist Attack,” Randal Simonetti from the consulting firm EFP Rotenberg, opines that in order to successfully combat an attack by an environmental group you must, “first consider the driving motive that supports the attacker’s existence.” According to Simonetti that driving motivation is money. “Funding is a primary driver of any activist organization’s behaviour,” writes Simonetti. The DeSmog blog post goes on to argue this point.

EDF Energy expects to give the go ahead before spring for construction of the UK’s first new nuclear reactor for 20 years, despite financial problems at its partner Areva and a warning on the difficulty of such projects. The comments from Vincent de Rivaz, EDF chief executive, came at a nuclear conference where senior industry figures raised fears of a skills and supply chain crunch at the £25bn Hinkley Point C power station in Somerset. De Rivaz admitted that delays at its Flamanville plant in France were a setback, but insisted they would not impact financially on the British project, which is using the same European pressurised reactor (EPR) technology.

A ProPublica analysis of federal government data adds new details to what’s known about the routes taken by trains carrying crude oil. Local governments are often unaware of the potential dangers they face.

Pilgrim Pipeline opponents in New York State are denying access to surveyors, calling it a “baseline of defense.”

The UK group Frack Free Ellesmere is hosting a rally at Ellesmere Port on December 14, 2014.

Agribusiness

Norwegian Food Safety Authority has denied approval to eight GMO fish feeds because they contained genes coding for antibiotic resistance. The fish feed industry had been given permission to use such feeds since 2008, but will now have to reapply for approval after the next year.

According to an order by new Indonesian president Joko Widodo, an audit will be carried out on the permits of companies that have cleared peatlands for palm oil cultivation. The news has been discussed on social media including the RAN-associated Forest Heroes, as well as Greenpeace.

On December 2, 2014, a press release was published at ran.org. The press release includes a link to a report published in December 2014 by Rainforest Action Network about a company merger in progress between BW Plantation (BWPT) and Green Eagle Holdings (GEH). The report discusses that risks to the environment posed by the merger. The merger would consolidate a large amount of uncleared forest under the control of one company. The press release lists BW Plantation as a new target for intensified scrutiny and accountability.

On December 9, 2014, Rainforest Action Network will be holding a Global Call-in Day targeting PepsiCo. They are urging supporters to call in to PepsiCo customer service numbers and providing scripts questioning and opposing the use of conflict palm oil in the company’s products.
Musim Mas has become the latest palm oil producer to adopt zero-deforestation policies for its palm oil production. According to the article in question at Mongabay.com, the policies take effect immediately and palm oil will be traceable to plantation by December 2016.

Four turkey and chicken farms in the Fraser Valley east of Vancouver, British Columbia, are under quarantine for avian influenza.

Tyson Foods Inc., the largest U.S. chicken producer, is holding off on its expansion plans in China after sales of allegedly out-of-date poultry from another U.S. supplier pared demand.

Insurance/Healthcare

A watchdog agency has identified a second list of security weaknesses in the Internal Revenue Services' systems that support Obamacare. A new report, dated September 29, 2014 but released on December 2, 2014 by the Treasury Inspector General for Tax Administration, says improvements are needed to ensure the security of information provided to the IRS by health insurers and pharmaceutical manufacturers for the Affordable Care Act program.

Threat actors are increasingly targeting PHI (Protected Health Information). Standard targets of identity theft, such as credit card numbers with related CDI and PIN information, are going for about one dollar per record on the black market. But a complete identity-theft kit containing comprehensive PHI credentials (including all personal data and related medical information) is worth up to $1,000 per record.

Most courts don’t prosecute auto premium evasion, and most states don’t even have laws against it. Only about 50 premium-evasion cases were prosecuted in the U.S. during the last two years, and most involved drivers who illegally bought coverage after being involved in a crash.

A recent email phishing scam is targeting numerous organizations, including healthcare companies. More than 100 organizations have been attacked by cybercriminals for over a year, according to a report from FireEye, a security company. FireEye calls the online attackers FIN4, and explains that they don’t infect their victims with malware, but instead capture usernames and passwords to victims’ email accounts. From there the attackers can read private email exchanges.

AMIA, an organization of about 5,000 biomedical and healthcare informatics professionals, recently wrote a letter to the House Committee on Energy and Commerce urging Congress to make changes to HIPAA to allow the use of PHI for certain "observational research" purposes without the need for patient consent.

Medicare spending on doctors who make house calls rose to $236 million in 2012 — a 40% increase since 2006. But the effort to help aging patients with limited mobility get medical care has been riddled with fraud due to lax regulations in some areas of the U.S. Nowhere is this more pronounced than in Michigan, where nearly a fifth of all the spending on Medicare home visits nationwide takes place. In 2012, physicians in Michigan received Medicare funds for home visits equal to 42 other states combined, a USA TODAY data analysis reveals. The result: more than $60 million in fraudulent billing by Michigan doctors in the past few years.

Seniors living in three states will need prior approval from Medicare before they can get an ambulance to take them to cancer or dialysis treatments. The change, which begins today, is part of a three-year pilot to combat extraordinarily high rates of fraudulent billing by ambulance companies in Pennsylvania, New Jersey and South Carolina.