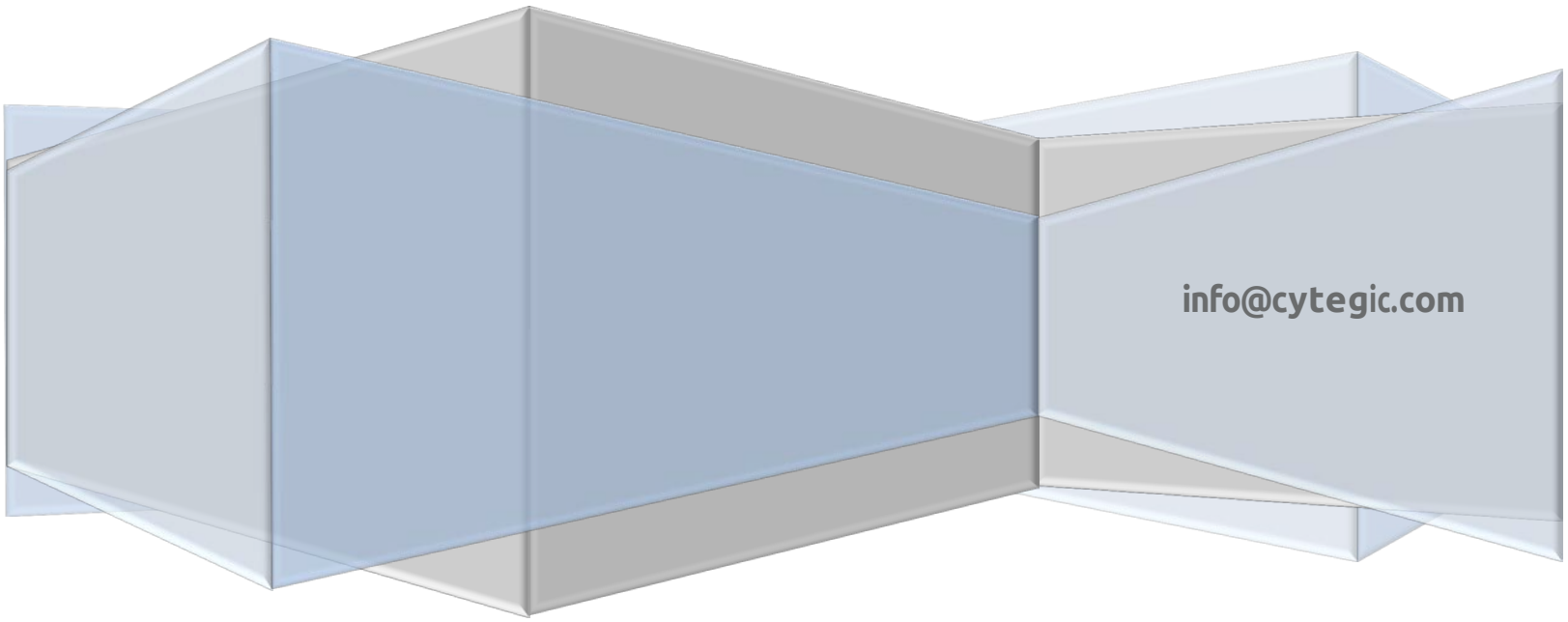
cytegic

Intelligence Update

2014 Summary and Forecast



info@cytegic.com

Introduction

Cytegic continuously monitors the cyber threat landscape and analyzes various inputs to identify threat agents, attacks and controls, based on geo-political regions and business sectors. Our DyTA machine monitors thousands of quality sources (both structured and unstructured), detects daily, weekly and monthly trends, changes and events and incorporates them into Cytegic's methodology and systems. DyTA enables a quick, understandable and actionable cyber-threat forecast.

The following is a high-level summary of developments and trends from **2014** that have been included in our CIAC Intelligence Packages, and forecast for **2015**. The trend analysis and forecast are based on our events database and are represented here as an example of DyTA's capabilities. These are pushed to local installations of the Cytegic DSS, and are correlated to the local environment defense posture for actionable intelligence.

For daily updates, follow us on twitter: *www.twitter.com/Cytegic*

Executive Summary

2014 Major Rising Trends and 2015 Forecasts:

- **The Proliferation and Monetization of Advanced Attack Methods -** In the past year, there has been a significant rise in the monetization process of advanced cyber tools. This means lower-capability attackers may be able to implement high-end tools and techniques simply by purchasing them or their blueprints off the shelf on black markets. Some of the major indicators for this trend are the constant rise in capability and usage of modified spyware by rouge political- or industrial-espionage groups, and of cryptoware for ransom by financial hackers. Attackers of different resources and skills are already using tools which were in the past used solely by nation-states and organized cyber-crime syndicates, and we predict this trend will continue to rise in the near future (even if we'll see large-scale law enforcement busts and counter-campaigns as in the past year).
    - **Action Item: Keep malware lists and vulnerability patches up-to-date**

- **Tool-Kits and Exploit-Kits Becoming More Available and More Aggressive -** Throughout the past year we have seen adaptive exploit-kits and even cyber-attack dashboards becoming available for purchase and implementation. This means that organizations will deal significantly more with pre-engineered attack vectors which include every part of the kill-chain (from reconnaissance, through penetration and navigation, and up to execution and exfiltration) in one click. This trend and the previous one are best represented by the Vawtrak Crimeware-as-a-service tool, and by the Regin spy-kit.
    - **Action Item: Implement Defense-in-Depth strategies and a high-level phishing awareness**

- **A Rise in the Use of Legitimate Actions and Tools -** While in the past, attackers were identified as external of internal, today it is not so clear-cut. This means that more and more attackers and attack vectors already leverage legitimate business and IT actions, tools, processes and privileges, and will continue to do so, to access

sensitive data without being tagged as an intruder by internal controls. This can be seen in cyber-campaigns which leveraged Dropbox communications, security updates and other legitimate processes. Additionally, even leveraging an internal employee may become a rising threat and can be considered as abusing legitimate actions, as seen in campaigns in Eastern-Europe and Africa.

  - **Action Item: Implement high-level anomaly detection tools, hardening and segregation of duties and privileges**

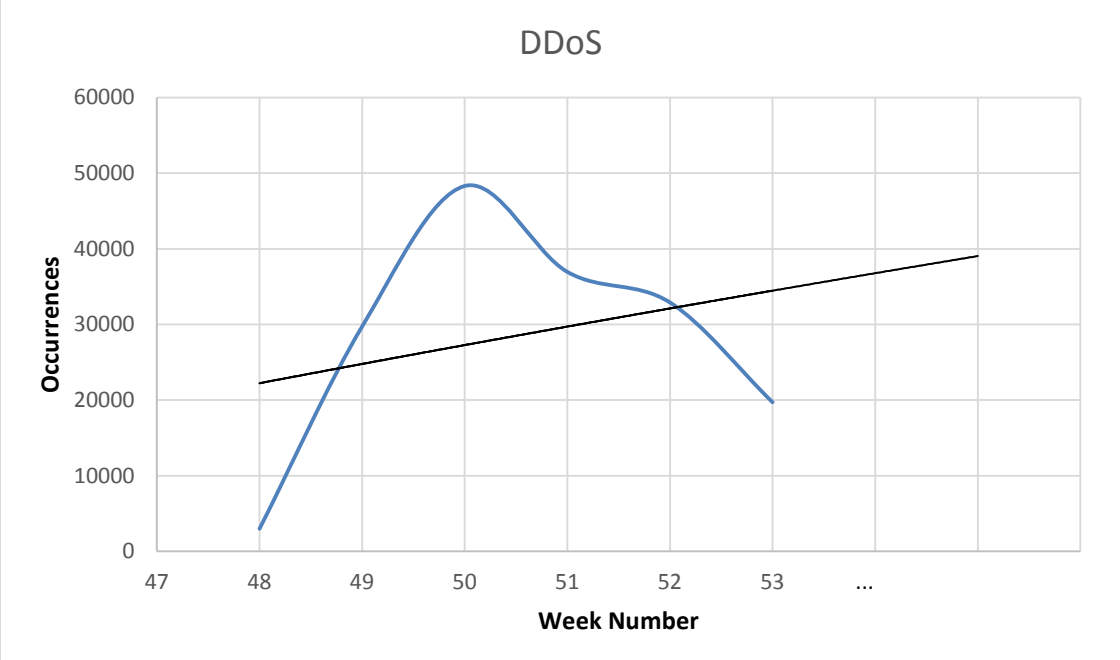
- **The Actions of Companies and Organizations Also have Cyber-Reactions and National-Level Consequences -** As seen in the infamous Sony breach, even "innocent" actions by a specific company may trigger devastating cyber-consequences for that company and even on a national level. While until recently it was clear that companies are liable for their customers' sensitive information (i.e. the trends we predicted last year regarding the rise in PII theft and large-scale payment card theft), now they need to understand that they are also liable for their entire eco-system (vendors, partners, banks, government, etc.).
  - **Action Item: Understand who your potential enemies are, what their capabilities are and what might trigger them to attack; use preemptive measures before planed actions and enable quick recovery procedures**

For the following trends, we've attached a snapshot of the last 6 weeks of data collected and analyzed using our DyTA intelligence machine.

- **DDoS Just Won't Die -** While many predictions in previous years foresaw the decline of DDoS as a widespread and effective attack method, the actual cyber field has proven otherwise, as we forecasted last year. DDoS attacks were of the most widely used attack methods in the past year, and their width and strength kept rising (up to 400Gbps recently). In the coming months, we'll continue to see not only hacktivists or sensationalists trying to make headlines by blocking access to high-profile sites or services, but also financial hackers using DDoS for distraction or ransom, and even nation-level DDoS attacks - such as the recent North-Korea internet blackout, which was not unprecedented (Estonia and Georgia for example).

  The chart below emphasizes the point we've discussed - DDoS usage shows a steady rising trend line, which lacks sudden surges as other attack methods.

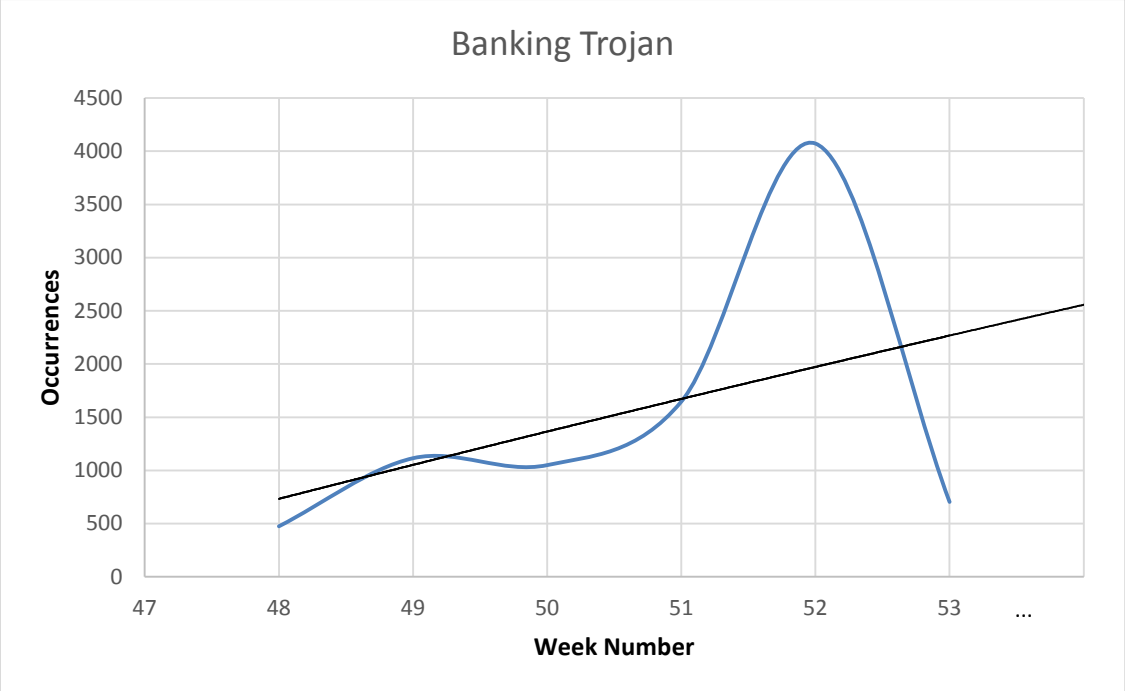
  - **Action Item: Implement DDoS mitigation tools and services and be aware of DDoS-as-Distraction**



- **Banking Trojans, Banking Trojans and More Banking Trojans -** From ATM skimmers and malware, through mobile banking MitM trojans and the "good"-old Zeus family, to the unique adaptive malware used against JPMorgan, this year continued to be dominated by banking trojans. Not even large-scale assaults against Zeus' and the Blackhole exploit kit's C&C infrastructure and handlers, managed to put more than a dent in the dominance and effectiveness of the overall banking trojan field. We predict that 2015 will be no different and that banking trojans will continue to evolve and adapt and pose a significant threat to banks and banking users together.

  The chart below shows an interesting pattern we have analyzed, that while during the holiday season banking trojans lag behind other financial attacks, after the holiday shopping hype there is a sharp rise in the usage of banking trojans.

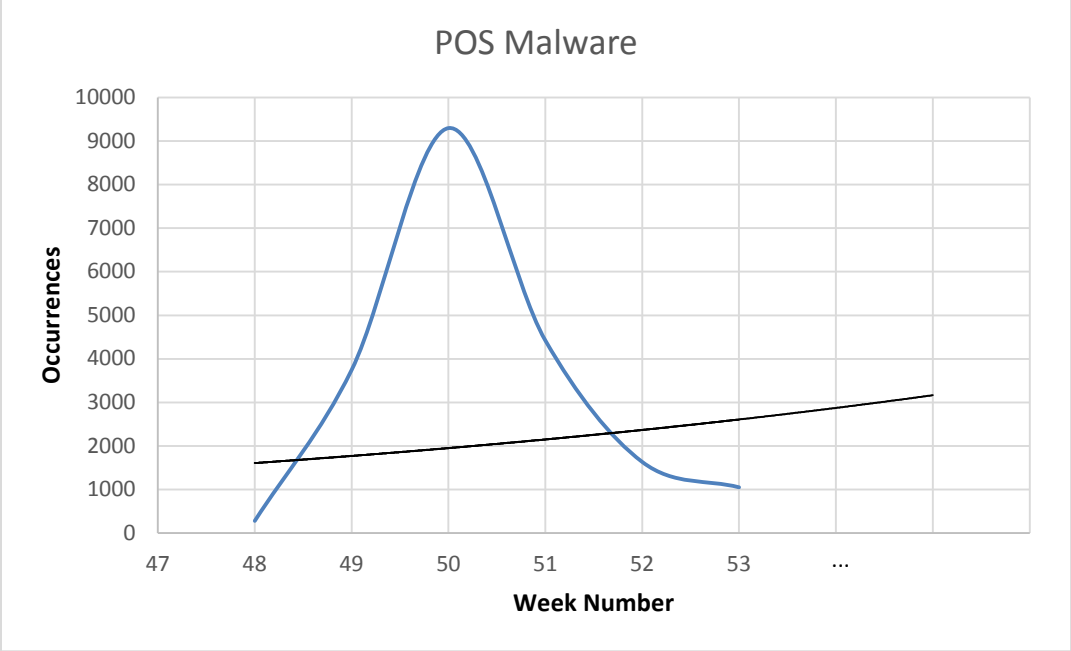
  - **Action Item: Educate your clients regarding the threat and how to prevent it, implement strict 2-factor authentication to prevent fraud, and implement anti-malware controls on network and endpoint devices such as ATMs**



- **POS Malware -** And, naturally, no 2014 summary is complete without mentioning the meteoric rise of POS malware, especially in the US. While a year ago Target and Neiman Marcus drew most of the attention to the retail sector, throughout the year we have seen POS malware spread, sometimes through POS vendors, to food chains, hotels and even parking lots (yes, Parking Lots!). As we predicted last year, POS malware was among the top cybercrime trends of the year and we assess the threat will continue to be dominant in the coming months.

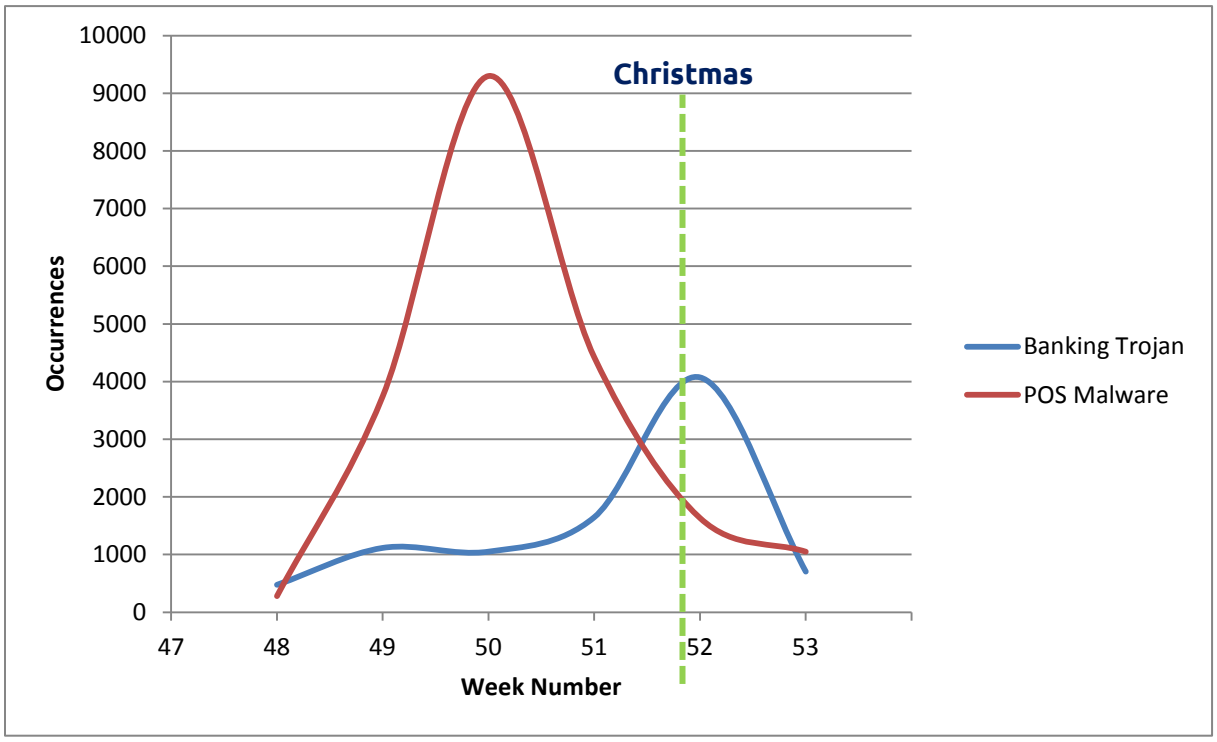
  The chart below is a beautiful representation of the reoccurring pattern during the end of the year period, where the week before Christmas sees a sharp rise in POS malware, a rise that coincides with holiday shopping habits.

  - **Action Item: Implement strict vendor management and anti-malware controls on your network and endpoint devices, especially in stores**



And to make things even clearer, the following overlying chart shows the shift in financial attack methods during the end of the year and the holiday season.

It is quite clear to see the pattern - financial attackers target point-of-sale terminals during the shopping weeks before Christmas, and then shift their scope back to banking trojans and "year-long" attack methods:



2014 Most Notable Campaigns

Nation-Level Attacks and Espionage Campaigns

Cyber-Espionage campaigns ruled a major part of the threat landscape in the past year. As mentioned in our updates throughout the year, the cyber-espionage field is divided into 2 main aspects - political espionage and industrial/financial espionage. In most cases, these espionage campaigns consisted of highly-advanced, and in many situations never-before-seen, tools and capabilities. While in 2013, the APTs gained most of the headlines, 2014 was identified by advanced spyware with the Regin espionage-kit shining most brightly. Additionally, the destructive attack on Sony, proved that seemingly naïve actions by a company may trigger a nation-level attack with severe consequences.

1. **The Regin Espionage Campaign -** In November, Regin, a highly-sophisticated espionage tool was discovered, which targeted governments, infrastructure operators, businesses, researchers, and private individuals around the world for several years[1]. Among its most prevalent targets were Saudi-Arabia and Iran, and researchers are claiming it seems the espionage kit was developed by a Western intelligence agency. Regin is one of the most sophisticated back-door Trojans ever discovered. It is a customizable and powerful framework that allows its handlers to target specific organizations with advanced multi-stage and stealthy attacks. This campaign emphasizes the constant rise in the sophistication levels of intelligence gathering malware, by nation-states or rogue espionage groups.
2. **The Sony Case -** Sony Pictures was the victim of one of the most severe cases of corporate hacks, after attackers managed to infiltrate its internal systems and copy huge amount of sensitive corporate data. The attackers, named GOP, belonging to, or supporting the North-Korean regime, attacked Sony's internal systems while bringing every computer in the network off-line. While at first it seemed that the attackers were merely after sensation, leaking unpublished movies, it quickly became clear that they managed to go after much more

[1] http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance

sensitive information, claiming they have some 100TB of data. The attackers copied corporate data including contracts, financial plans, sales details, employee personal information and even passwords (from a folder literally named "Passwords"). This attack was done as retaliation for the company's plan to release a movie embarrassing North-Korea's Kim Jong-un.

3. **DarkHotel APT[2] [3] -** Also in November, Kaspersky Labs revealed an APT campaign, nicknamed Darkhotel, which targeted high ranking executives from various sectors, staying in hotels in East-Asia. The campaign consisted of compromising Wi-Fi networks at luxury hotels in order to target specific individuals. The attack vector was a downloader which misused Adobe updates, under the pretense of a hotel's "welcoming package". After that, keyloggers and other data stealing malware were injected into the victims' devices. The most interesting part of this campaign in the level of sophistication of the attack vector and the focus level, targeting very specific executives in specific locations. These suggest reconnaissance, planning and high level of execution, which are mostly used by nation-state or nation-backed attackers. According to Kaspersky, the attackers are Korean-speaking and we assess they might be a rogue espionage group or financial hackers set on targeting confidential financial data or IP.
4. **The Iranians Proved Their Cyber Skills -**
    a. **Operation Cleaver[4] -** Nation-backed espionage groups from Iran conducted long cyber-espionage operation, targeting critical infrastructure organizations in fields such as energy, oil and gas, transportation and government. Most of the targets were from North-America and Europe, but many others were based in Middle-Eastern countries such as Kuwait, the UAE, Saudi-Arabia and Israel. The thing most interesting about the operation was the nature of the assets

[2] http://www.esecurityplanet.com/network-security/darkhotel-apt-campaign-targets-traveling-executives.html
[3] http://www.darkreading.com/vulnerabilities---threats/advanced-threats/korean-speaking-cyberspies-targeting-corporate-execs-via-hotel-networks/d/d-id/1317361
[4] http://www.darkreading.com/attacks-breaches/with-operation-cleaver-iran-emerges-as-a-cyberthreat/d/d-id/1317861

targeted. While in most cyber-espionage campaigns attackers target IP, technical information and other business related assets, in this operation it seems that the attackers were after sensitive critical processes, network topologies and electricity infrastructure. This issue points to the possibility that the attackers focused on gaining a foot in the door for a future doomsday attack.

This operation emphasizes the fact that the Iranian regime's cyber capabilities are high and that they a force to be reckoned with. Moreover, it emphasizes the fact that political cyber-spies and political cyber-warriors are basically the same entity, with just the directive differentiating between them.

b. **Sophisticated Iranian Social-Engineering Campaign Targeted High-Ranking American and Israeli Officials**[5] **-** In another interesting espionage campaign, during a three-year period, Iranian hackers, probably nation-backed, targeted high-ranking American and Israeli officials using different social-media channels. This elaborate campaign consisted of a fake news agency's website (newsonair[dot]org) and a network of fake social-media accounts, which were used to convince the targeted individuals of the "reliability" of the attackers and their approach. The attackers' objective was to gain the trust of their "persons of interest" and then infiltrate their systems in-order to achieve a foot-hold in those systems and exfilitrate sensitive data. Among the targets were military officers, politicians, diplomatic core, defense contractors and government officials from the US, Israel and several Middle-Eastern countries including Iraq, Syria and Saudi-Arabia.

5. **Molerats are Back**[6] **-** After being spotted late last year by researchers at FireEye, Middle-Eastern hackers related to the 'Molerats Campaign' have surfaced again, targeting multiple European and Middle-Eastern government organizations and at least one financial institution in the U.S. Most of the

[5] http://securityaffairs.co/wordpress/25355/hacking/iranian-hackers-social-media.html
[6] http://www.securityweek.com/middle-east-hackers-target-government-departments-us-financial-institution

attacks occurred during May 2014, and have reused the same command and control infrastructure and tactics as previous attacks. Among the victims are Palestinian and Israeli targets, the governments of Turkey, Slovenia, Macedonia, New Zealand, Latvia, the US, and the UK, several European government organizations and even the BBC. Molerats campaign use off-the-shelf RAT kits such as PIVY (Poison Ivy) and Xtreme RATs, and manipulate targets using decoy documents with content focusing on active conflicts in the Middle East. This campaign comes to show that 'cyber-espionage' campaigns in, and from, the Middle-East continue to be a live and relevant threat, and that government organizations in USA, Europe and the Middle-East need to take that into account.

6. **Epic Turla campaign**[7] **-** In august, researchers have identified a follow-up political-espionage campaign to Turla, called Epic. This campaign targeted government organizations and diplomatic corps worldwide, and specifically in Europe and the Middle-East. The attack methods used in this campaign include a variety of 0-day attacks, spear-phishing, social-engineering and watering-hole attacks. It shares some of its code and encryption mechanisms with Turla, which was used widely in the past year. This campaign is unique due to the high level of flexibility and the way the code adapts to different security scenarios.
7. **Machete campaign targeting Latin America**[8] **-** Another interesting political-espionage campaign which was discovered in August, is dubbed Machete. This campaign is unique due to the fact that it specifically targets intelligence services, governments and political targets in Spanish speaking countries, specifically in Latin-America. The campaign's code allows access to the files on the targeted machine and exfiltrating them to a remote server. It can also be used for keylogging, capturing audio through the computer's microphone, grabbing screenshots, getting the geographical location of the system and snapping pictures with the webcam[9].

[7] http://threatpost.com/epic-operation-kicks-off-multistage-turla-apt-campaign/107612
[8] http://www.infosecurity-magazine.com/news/machete-apt-hacks-south-america/
[9] http://news.softpedia.com/news/Machete-Espionage-Malware-Targets-Spanish-Speaking-Countries-455929.shtml

8. **Citadel Used Against Petrochemical Companies in the Middle-East**[10][11] **-** Researchers at Trusteer have uncovered a cyber-espionage campaign against petrochemical companies in the Middle-East. What was interesting about this campaign was the reuse of the old and familiar Citadel banking trojan, which was originally built to steal money. According to the company, the trojan was repurposed to target specific URLs, such as the companies' webmail, and "ambush" users before beginning to record credentials and send them to a C&C server. These credentials were later used to read and send messages, and preform spear-phishing attacks against interesting individuals.

[10] http://threatpost.com/citadel-variant-used-in-attacks-against-middle-eastern-petrochemical-companies/108293
[11] http://www.infosecurity-magazine.com/news/citadel-trojan-targets-middle-east/

Hacktivism Campaigns

As in recent years, hacktivists continued to take a big part in the cyber world and draw headlines throughout the world. The Anonymous collective, its Middle-Eastern affiliates and independent and powerful groups such as the Syrian Electronic Army, RedHack and AnonGhost were the most active; with DDoS, data dumps through SQLi and defacements being the most used TTPs.

1. **International Sporting Events -** This year has seen two major international sporting events which drew many attentions from the cyber community. The football world cup in Brazil and the winter Olympics in Sochi were accompanied with harsh accusations regarding corruptions and poor working conditions.
   Before the world cup in Brazil, Anonymous declared[12] they are planning a major campaign against sponsors of the FIFA World Cup in Brazil. They were protesting the corruption by the local government, saying it was neglecting and hurting the local poor population. Among the companies named in Anonymous' threat was Emirates Airlines, Coca-Cola and more. This is similar to the threats and attacks that happened prior and during the Sochi Winter Olympics, in which local government and participating organizations were targeted.
2. **Conflicts Between Nations**
   a. **Israel-Hamas** - the most prominent case of the Israeli-Arab cyber-conflict was during Operation Protective Edge in the summer.
      Hacktivists, some supposedly aided by nation-states, attacked Israeli websites and infrastructures in protest of the conflict in Gaza. Political activists, led by Anonymous, continued in their #OpSaveGaza cyber-campaign and targeted mostly Israeli government and defense forces websites. On one occasion, the hacktivist collective claimed to have taken down the Mossad's website, and in fact for several minutes the website showed an error message[13]. In the midst of actual defacement

[12] http://hackread.com/anonymous-hackers-cyber-attack-brazil/
[13] http://www.hackersnewsbulletin.com/2014/08/anonymous-live-mossad-israeli-govt-websites.html

and DDoS attacks and attempts, the hacktivists also tried to perform physiological warfare, claiming they were able to take down tens of critical government websites. In fact, none of the websites in the hacktivists' list was active and we believe the publication was merely meant to glorify Anonymous' attempts[14].

As in many Middle-Eastern conflicts in the past, we continued to see ricochets of attacks targeting Western websites, in protest of alleged support of Israel. In several cases, hacktivists and sensationalists from Arab or Muslim countries defaced local government websites in the US, and left a message in support of Palestine[15][16]. US and European government websites are common targets for politically motivated attackers and should tighten security during Israeli-Arab conflicts.

b. **Russia-Ukraine -** During the tensions and clashes in eastern Ukraine, between Russia and Ukraine, hacktivists, sensationalist and other politically motivated hackers played a major role in the conflict. The attackers from both sides mainly tried to hold the other side back by causing technical and communication damage, and to embarrass them by dumping sensitive data and defacing high-profile websites. Among the most active and successful groups were the Ukrainian Cyber Troops and Cyber Berkut[17].

c. We have seen similar activities in this year's conflicts and tensions between China and Vietnam, China and Japan, Pakistan and India, Indonesia and Australia, and many others.

3. **Internal Conflicts and Political Issues**

a. **The Syrian Electronic Army -** The Syrian Electronic Army (SEA), the pro-Assad hacktivist group, drew many headlines throughout the year, mainly by targeting high-profile Western media outlets. This includes

[14] http://countercurrentnews.com/2014/08/new-anonymous-op-takes-down-israeli-government-websites-in-huge-counter-hack/
[15] http://hackread.com/city-of-dubois-website-hacked-palestine/
[16] http://hackread.com/moroccan-hackers-hack-saratoga-county/
[17] http://www.bbc.com/news/world-europe-30453069

The Times, Forbes, NBC, The Telegraph, The Independent, and much more. The most interesting aspect about the SEA is that it keeps changing its tactics and techniques in order to achieve its goals, and by that, differentiating itself from the "hacktivist" definition and field. This could be seen during the attacks Western media, which used Gigya.com as an attack vector for defacement. The SEA used similar tactics when they leveraged Outbrain and Taboola for the same purpose. Moreover, the SEA has positioned itself as a minor technology leader, when it published a dedicated Linux OS for hacktivism purposes. The fact that the SEA continued to be such a main player throughout the year signals that the same will continue to happen in the near future, and that the Syrian internal (?) conflict will continue to draw casualties from outside Syria and the Middle-East.

b. **Anonymous attacks Ferguson police**[18][19] **-** After the shooting of an African-American teen in Ferguson, Missouri, by the police, protesters took to the streets and harsh clashes occurred between the sides. The hacktivist collective Anonymous very quickly declared they will start a cyber-campaign dubbed #OpFerguson against local law-enforcement forces. They lived up to their threat and began targeting police, National-Guard and local government websites in Missouri. The attacks consisted of the usual Anonymous TTP's - DDoS, SQLi and defacement attempts. Additionally, Anonymous made an effort to uncover the identity of the cop who allegedly shot the unarmed teen. This is a common practice for Anonymous, which they have implemented several times in the past.

c. **Hong-Kong Democracy Protests -** During the pro-democracy protests in Hong-Kong many of the activist movements and their supporters were targeted by different attack methods, in order to discourage them from continuing. The Chinese government, or its affiliates, targeted the

[18] http://www.hotforsecurity.com/blog/anonymous-targets-ferguson-missouri-in-opferguson-ddos-attack-on-local-pd-web-site-9949.html

[19] http://www.hacksurfer.com/posts/anonymous-takes-on-ferguson-continues-pattern-of-targeting-police

protestors with mobile malware and advanced DDoS tools, and several companies which supported the protestors were targeted by DDoS attacks. As retaliation, many Chinese government websites were defaced and DDoS'ed as part of #OpHK. This emphasizes the observed trend where hacktivists almost automatically align themselves with protestors, regardless of the cause, and start a cyber-battle with government entities.

Most Notable Developments regarding Financial Hackers

Financial Hackers, whether individuals, groups or organized crime syndicates, took the lion's share of activity in in the cyber field throughout the recent year. This is a continuation of past years, where the main trend that surfaced this year was the spread and ease of use of what was once considered highly-advanced attack methods, which were out of the cyber-crime's reach. Due to the fast monetization process that the field has seen, financial hackers with lower-means and capabilities may purchase off-the-shelf exploit-kits, attack methods and cybercrime-as-a-service tools, without having the technical knowledge once needed to implement them. The most widespread TTPs for financial hackers (other than Spam, or email scams) were banking trojans and POS malware.

1. **POS Malware -** During the past year we've reported about the constant rise is the use of POS malware, especially in the US, and especially against large retailers (but not only). According to Kaspersky, the number of companies affected by the famous Backoff malware may be up to 1000 and that number is constantly rising[20]. The activity-level of financial-hackers against retailers and other companies which process many credit-card transactions was high throughout the year. The last part is important - POS malware is relevant not only to Target, Home Depot, Kmart, Staples and similar retailers, but rather to every company and organization that handles payments. This would explain financial-hackers targeting Dairy Cream, Jimmy John's and other "non-trivial" targets, such as parking lots.

   The most prevalent POS malware types include the Soraya malware family, which is based on Zeus and Dexter, and Backoff. What differs the recent incidents is the injection method and the attack vector through which the attackers were able to insert the malware into the targeted systems. For

[20] http://www.computerworld.com/article/2600625/malware-vulnerabilities/backoff-malware-infections-are-more-widespread-than-thought.html

instance, in Jimmy John's case, attackers leveraged a POS vendor in order to install the malware into hundreds of end-points[21].

The use of POS malware and the targeting of payment details have become so widespread that due to the large flood of credit and debit-card information in underground markets, a need for dedicated software to ease the monetization of these cards came up. Researchers at Intercrawler recently revealed a payment gateway cyber-crime software, which, according to them, can send batches of stolen card charges to multiple gateway processors, automating their returns before banks can catch the fraud[22]. The platform, called "Voxis", can be purchased in underground markets, and basically automates the purchasing process, mimicking human behavior to avoid detection. It allows criminals (not just cyber-criminals) to process several cards at any given time, through 32 different payment gateways (including PayPal) and even autofill missing CVV info. This development comes to show the way the underground market answers a rise in demand, and emphasizes that targeting credit-card information will continue to be a rising trend in the near future.

2. **Internal Threats** [23] **-**
    a. A former employee of the Israeli Leumi-Card credit card company has managed to steal personal information about several million Israeli customers before he was dismissed. The employee then sent a blackmail email to his former employers, threatening them with exposure of the data. While the employee was quickly arrested in Thailand and it seems that no sensitive data was published, this incident should be considered as a case-study for internal cyber-attacks, alongside the Snowden case.
    b. In an unusual "cyber" attack, an IT employee form Nigerian Skye bank, managed to steal up to $40m. The insider thief apparently conspired with a criminal gang to access the bank's computer system and inflate

[21] http://news.softpedia.com/news/PoS-Vendor-Signature-Systems-Informs-of-Credit-Card-Breach-Affecting-324-Restaurant-Locations-460160.shtml
[22] https://www.intelcrawler.com/news-23
[23] http://news.softpedia.com/news/Former-Employees-Blackmail-Bank-Get-Arrested-465182.shtml

the balances of various accounts[24]. The employee, who worked in the bank's IT department, is said to have provided the gang with physical access to the bank's servers, disguised as weekend maintenance personnel. The money was redirected to bogus accounts and the gang was apparently in the process of withdrawing the funds when the theft was spotted[25].

Insider threats are a major concern for banks and financial services, which invest a lot in fending off external threats but are at constant risk by their employees. Bank security personnel need to make sure they implement strict internal HR policies and procedures to make this threat as low as possible. Internal attackers are by default highly dangerous due to the fact that they act from within the organization, thus making all the preventive outer-layer defense controls irrelevant. Moreover, most of their malicious actions are extremely difficult to detect due to the fact that they use legitimate tools and, in most cases, privileges. In order to defend themselves against such attackers, organizations must make sure to adhere to strict internal controls such as segregation of duties, hardening of end-point, network and other devices, and refine their recruiting processes.

3. **Banking Trojans -** Banking trojans, as mentioned, were a major part of the cyber-crime field in the past year, and while the POS malware incidents drew more attention, the use of banking trojans may have had larger, more direct, financial consequences. Banking trojans have become widespread and much more easy to purchase and implement, and we saw them being used all over the world mainly against online and mobile banking users and against ATMs. Other than the infamous Zeus family, which continued to grow in efficiency and sophistication, here are a few interesting developments in the field:

[24] http://www.finextra.com/news/fullstory.aspx?newsitemid=26446
[25] http://nakedsecurity.sophos.com/2014/09/15/nigerian-bank-it-worker-on-the-run-after-40m-cyber-heist/

a. **Qbot[26] -** A report by Proofpoint revealed the actions and M.O. of a highly sophisticated cyber-crime group originating from Russia. The group performed an organized campaign targeting mostly US-based systems and online banking accounts. This was done using a huge botnet, named Qbot (or Qakbot), which consisted of 500k infected systems. This botnet lifted account credentials for over 800k online banking transactions, especially targeting five of the largest US banks.

   The attack vector consisted of compromising WordPress sites with purchased admin credentials, uploading malware to legitimate sites and infecting clients who visited those sites - a vector similar to watering-hole techniques. Most of the compromised systems ran Windows XP, which makes sense due to the fact that Microsoft ended support for this OS earlier this year, making it much more vulnerable[27].

b. **Tyupkin Against ATMs[28] -** Financial hacking groups in Eastern-Europe were able to steal millions of dollars from ATMs around the world using the Tyupkin malware. This malware, which is inserted using a CD, forces the ATMs to dispense cash, without the use of forged credit-cards. The infected ATMs all ran a 32-bit version of Windows and were discovered mostly in Russia but also in the US, India and even Israel. The most recent variation of the malware is equipped with anti-detection mechanisms and is able to neutralize security controls[29].

   As mentioned in our previous updates, ATM attacks, specifically using malware are on the rise throughout the world, and they are becoming more efficient and easy to implement.

c. **Dyre Trojan Continues to Spread[30] -** During the year, we reported how financial hackers began targeting Salesforce users with the Dyre banking

[26] http://www.proofpoint.com/threatinsight/posts/the-insider-view-of-a-russian-cybercrime-infrastructure.php
[27] http://www.darkreading.com/cloud/how-one-criminal-hacker-group-stole-credentials-for-800000-bank-accounts/d/d-id/1316484
[28] http://securityaffairs.co/wordpress/28993/cyber-crime/tyupkin-malware-steal-atms.html
[29] http://arstechnica.com/security/2014/10/dozens-of-european-atms-rooted-allowing-criminals-to-easily-cash-out/
[30] http://www.net-security.org/malware_news.php?id=2902

trojan. The trojan is known for targeting banking and financial customers in order to still their credentials using a Man-in-the-Middle attack that can bypass the SSL mechanism. This month, it was revealed that Swiss banks were targeted by the trojan, which is delivered through spam emails that include a PowerPoint attachment containing an exploit for the "Sandworm" CVE-2014-4114 vulnerability in Windows[31].

d. **Tiny Banker Trojan -** Tiny Banker, AKA Tinba, trojan in known for its light weight but high effectiveness. It was discovered in 2012 in Turkey and has since been expanding to other countries. It can inject HTML fields into websites when it detects a user has navigated to a banking site, asking for a range of sensitive[32]. This month, Avast showed that Tinba has been modified to target banks and financial institutions in the US (Wells Fargo, BofA and Chase, among others). This customization of Tinba comes after its source code was leaked in July, an event which may have led to its adoption by financial hackers who up until now were not able to use it (mainly because of its off-the-shelf price).

   This emphasizes the trend we have highlighted in our previous update - more and more financial hackers, with lower resources and skills, are able to use sophisticated attack methods, due to the proliferation of advanced tools. This causes a rise in threat levels for individual financial hackers[33].

[31] http://news.softpedia.com/news/Swiss-Banks-Targeted-By-Dyre-Trojan-Attackers-Leverage-Glitch-in-Windows-463622.shtml
[32] http://www.csoonline.com/article/2684173/malware-cybercrime/tiny-banker-malware-targets-us-financial-institutions.html
[33] http://www.seculert.com/blog/2014/09/tiny-tinba-trojan-could-pose-big-threat.html

Major Vulnerabilities

This year has seen a peak in global, widespread vulnerabilities, which managed to draw headlines outside of the cyber-security world. This is due to the fact the more and more people and organizations are grasping the possible severe consequences such vulnerabilities have on daily business and activities. Among the most interesting and widespread vulnerabilities were:

1. **The Heartbleed vulnerability**[34] - In April, researchers have uncovered a critical vulnerability in recent versions of OpenSSL, a technology that allows websites to encrypt communications with visitors. Quickly after the publication of the vulnerability, financial hackers released a simple exploit kit that can be used to steal usernames and passwords from vulnerable sites, as well as private keys that sites use to encrypt and decrypt sensitive data. According to the Heartbleed website[35] - "The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eaves-drop communications, steal data directly from the services and users and to impersonate services and users". The exploit allows attackers to grab 64K of memory from a server. The attack leaves no trace, and can be done multiple times to grab a different random 64K of memory[36].
2. **Bash "Shellshock" Vulnerability –** In September, researchers have uncovered a critical vulnerability (CVE-2014-6271) in the GNU Bourne Again Shell (Bash), the text-based, command-line utility on multiple Linux and Unix operating systems. The vulnerability is critical due to the widespread use of this system globally. According to security reporter Brian Krebs, it was discovered that if Bash is set up to be the default command line utility on systems, it opens those systems up to specially crafted remote attacks via a range of network tools

[34] http://krebsonsecurity.com/2014/04/heartbleed-bug-exposes-passwords-web-site-encryption-keys/
[35] http://heartbleed.com/
[36] https://www.schneier.com/blog/archives/2014/04/heartbleed.html

that rely on it to execute scripts[37]. Despite several different patches already issued, attackers are exploiting this vulnerability to perform large-scale DDoS and Remote Code Execution attacks. More severe is the fact that several worms have been discovered which use this vulnerability to install malware on vulnerable systems. Shellshock has been compared to Heartbleed, due to the widespread nature and potential damage, but in fact, unlike Heartbleed, which only allows attackers to read sensitive information from vulnerable web servers, Shellshock potentially lets attackers take control over exposed systems. This vulnerability increases the potential threat for many attackers, including financial hackers, political cyber-warriors and competitors engaging in cyber-espionage. This vulnerability was put to use on several occasions:

a. **Attackers Leveraging the Vulnerability[38] -** Since the vulnerability was disclosed, attackers began leveraging it on a global scale. Incapsula stated that according to their systems, attack using the vulnerability have reached nearly 2000 per hour. The offending IP's were widely dispersed (though many were US-based) and the majority of the attacks consisted of Scanners, attempting to verify the existence of the vulnerability on different systems. The rest of the attacks consisted of attempts to establish remote access, and DDoS malware. According to the data presented, the attacks are global, with a slight emphasis towards the US[39]. According to Trend Micro, they have witnessed targeted attacks using the Bash vulnerability, against government institutions in Brazil[40] and financial institutions in China[41].
b. **A Collection of Exploit Seen in the Wild[42] -** Malware and exploit writers were not lazy, and very quickly Bash exploits started to appear in the wild. Among those, which any and all attackers may implement, are

[37] http://krebsonsecurity.com/2014/09/shellshock-bug-spells-trouble-for-web-security/
[38] http://www.incapsula.com/blog/shellshock-bash-vulnerability-aftermath.html
[39] http://news.softpedia.com/news/New-Average-For-Shellshock-Attacks-Over-1-970-Incidents-Every-Hour-460407.shtml
[40] http://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-updates-bashlite-ccs-seen-shellshock-exploit-attempts-in-brazil/
[41] http://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-exploit-attempts-continue-in-china/
[42] https://isc.sans.edu/diary/Shellshock%3A+A+Collection+of+Exploits+seen+in+the+wild/18725

vulnerability check scanners, bots exploiting the vulnerability itself to install nods, installers that inject vulnerable systems with a shell to perform remote code execution, and more.

3. **POODLE Vulnerability -** The world was barely recovering from Heartbleed and Shellshock, which rendered numerous systems vulnerable worldwide, and another severe vulnerability has been uncovered. POODLE (Padding Oracle On Downgraded Legacy Encryption), CVE-2014-3566, disclosed by Google researchers, is a vulnerability in SSL 3.0 which allows interception and compromise of supposedly secured data[43]. POODLE attack targets the protocol itself, unlike Heartbleed which was a flaw in OpenSSL. This attack requires a MitM position and code on the client side to open numerous SSL attempts against a vulnerable server, only then can it steal cookies from the target[44].

   While the easiest way to deal with this vulnerability is to disable the SSL 3.0 protocol, patches have already been issued. Still, it is recommended to check for this vulnerability on all systems[45].

[43] http://blog.whitehatsec.com/what-you-need-to-know-about-poodlessl-3-0-vulnerability/
[44] https://community.qualys.com/blogs/laws-of-vulnerabilities/2014/10/16/sslv3-and-poodle-attacks
[45] http://blog.whitehatsec.com/what-you-need-to-know-about-poodlessl-3-0-vulnerability/