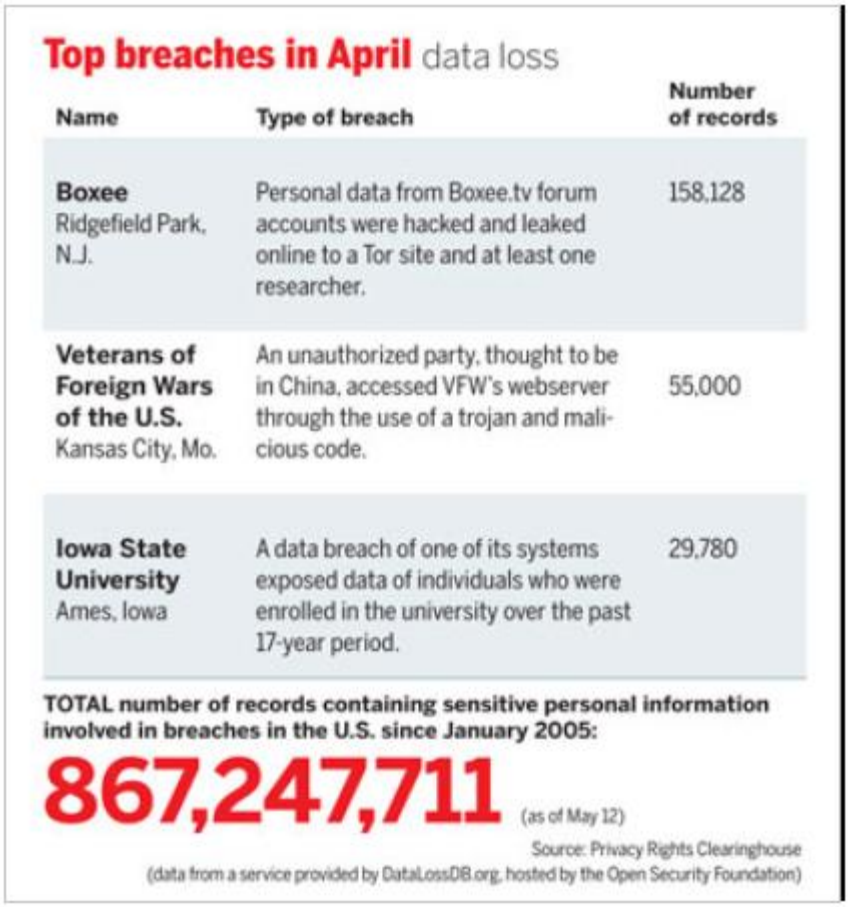
GLOBAL THREAT INTELLIGENCE ASSESSMENT JUNE 2014

Executive Summary:

In the month of June 2014 there were 3 top breaches that caused a loss of data within the range of 242,908 personal records. This is just one aspect of loss due to compromises due to criminal activities as well as state actors today within the realm of hacking. This report is being presented to you to give insight into what is happening in the world today and this last month online and in corporations where information security is involved.

This month has seen more activities from not only nation state actors but also defenders within the US working towards stopping them. Crowdstrike, Fireeye, and others have put out reports on actors and methods that are currently attacking infrastructures both private and public. In this report you will see some of the highlights from global events that is germane to your understanding of the threatscape today.



Top breaches in April data loss

Name	Type of breach	Number of records
Boxee Ridgefield Park, N.J.	Personal data from Boxee.tv forum accounts were hacked and leaked online to a Tor site and at least one researcher.	158,128
Veterans of Foreign Wars of the U.S. Kansas City, Mo.	An unauthorized party, thought to be in China, accessed VFW's webserver through the use of a trojan and malicious code.	55,000
Iowa State University Ames, Iowa	A data breach of one of its systems exposed data of individuals who were enrolled in the university over the past 17-year period.	29,780

TOTAL number of records containing sensitive personal information involved in breaches in the U.S. since January 2005:

867,247,711 (as of May 12)

Source: Privacy Rights Clearinghouse
(data from a service provided by DataLossDB.org, hosted by the Open Security Foundation)

Report Highlights:

- OpenSSL had another vulnerability found that could cause compromise of people's credentials.
- Iranian hackers attempted to socially engineer and spearphish numerous defense base users with LinkedIn, Facebook, and Twitter
- A social engineering campaign was launched against the author of this report via LinkedIn in an attempt at intelligence gathering
- The Russian state has allegedly launched attacks using the HAVEX RAT which attacks SCADA and ICS systems (Energy Sector)
- The Syrian Electronic Army attacks Reuters website and defaces it in an propaganda campaign
- The Dyreza RAT bypasses SSL sessions by stealing credentials and is attacking larger bank users
- ANONYMOUS is planning an OP on ISIS funding states

- ISIS/ISIL leveraging Twitter for propaganda and recruitment purposes
- SEA (Syrian Electronic Army) Compromises and defaces Reuters website

Global Threats

Open SSL:

Summary:

Post the Heartbleed vulnerabilities disclosure, attackers have been working on other vulnerabilities within the code for SSL (Secure Sockets Layer) encryption. This is the encryption that protects internet traffic and has been the standard for many years. As of June 5th a new vulnerability was released and has been since patched in the code by the makers of SSL.

The attack allowed for a "Man in the Middle" attack that could have led to decryption of traffic and loss of credentials and data. This means that an intermediary machine would have to be in the middle of the traffic for this to work. This attack is feasible and it has been recommended that all instances within your environment that are vulnerable to this should be patched as soon as practicable.

From OpenSSL.org

*The attack can only be performed between a vulnerable client *and* server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1. Users of OpenSSL servers earlier than 1.0.1 are advised to upgrade as a precaution*

This attack though and Heartbleed show an inherent security problem with commonly used protocols or software like this due to the prevalence of use and the level of compromise that could come from exploiting this type of bug.

Social Engineering via LinkedIn: NEWSCASTER

Summary:

On May 28th iSight Partners put out a report on an alleged Iranian phishing and social engineering campaign that used some common tactics for APT (Advanced Persistent Threat) actors. This campaign started in or around August 2013 and continued up until the roll up after this report was put on the internet.

The site above posed as an on air radio station as well as a news site catering to topics that defense base individuals would be interested in. In tandem with this or at least in parallel, the adversary also created a group of accounts on Twitter, Facebook, and LinkedIN to socially engineer targets and backstop the fictitious site.

The parallell attack consisted of socially engineering employees and heads of departments up to and including high level brass in the military and C level exectuives from places like Pratt & Whitney and other companies that make defense hardware. Once users had accepted LinkedIN requests or Facebook requests they would be enticed to go to the Newsonair site to read the news and perhaps listen online. The links sent to the targets would then be drive by sites for infection or simple sites that requested users credentials to enter their site for content. These attempts would then perhaps net the adversary the users credentials to Outlook (one particular attack was a page that presented an outlook login) and thus compromising their email as well as perhaps other access such as VPN (depending on implementations)

According to the iSight report the gambit of socially engineering people via Facebook and LinkedIN worked well enough to gather approximately two thousand users “friending” or adding the fictitious (cutout) accounts that the adversary had created to mine for access. Given the numbers accredited to have been within the friends/linkedin connections it is a high probability that the adversary had at least some insight into the workings of their targets habits and perhaps even may have elicited access through the drive by attacks as well as perhaps SE data from unaware targets.

Analysis:

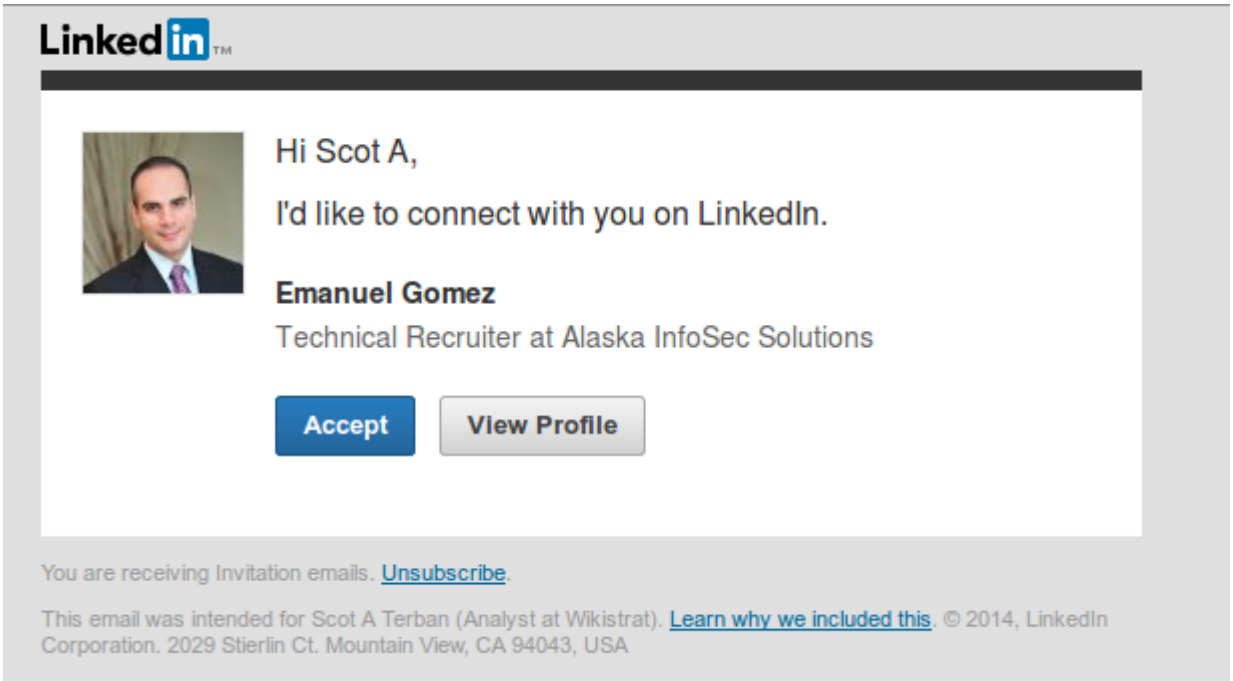
This campaign is not important or of note in its modus operandi generally as APT goes but it is an object lesson that should be heeded. The melding of the SE with the drive by attacks show how easy it is to attempt to get users to compromise their systems as well as their personal/corporate data through social media attacks.

Where this may in fact be an Iranian actor (not nation state but instead a hacker/group in Iran looking to carry out a campaign under the rubric of political fervor) we have also seen actors like the Lampeduza Republic (carders who attacked Target) use the same APT tactics to affect their goal of stealing PCI data.

Given that social media is so prevalent today, it is a given that campaigns are ongoing within the space and that our users as well as our executives could fall prey to these attacks by other adversaries than APT (Nation-state or other) As such we should insure that our education on Phishing as well as Social media attacks and SE should continue if not actually expand. This is the current and future of pivot attacks that will continue to be the means by which attackers break into companies and extract data.

Another factor to take into account is the endpoint where traffic is going on the internet. In the case of newsonair the IP space was located physically in DFW (Texas) but the end point of the data trail leads to Iran and a server within the Islamic Republic. IDS and SIEM can help to determine traffic patterns to such places outside of the country and should be leveraged to determine where data is ex-filtrating to. In the case of this team the SIEM and IDS solutions actually caught the traffic (hits on sites) as well as malware telemetry and remediation tools stopped the malware from compromising machines.

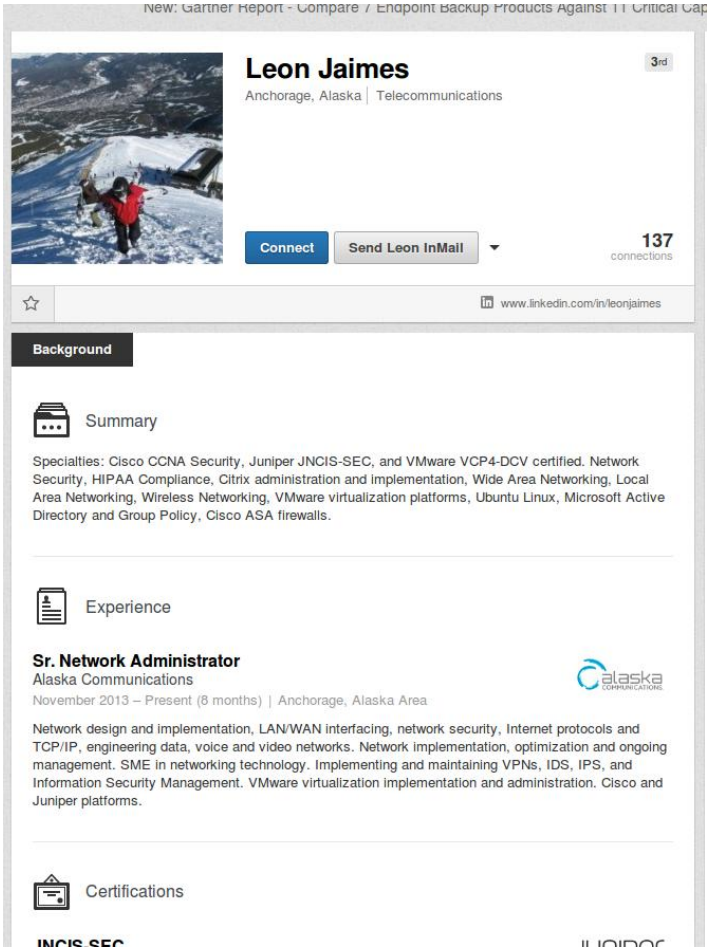
Social Engineering via LinkedIn: Personal Account

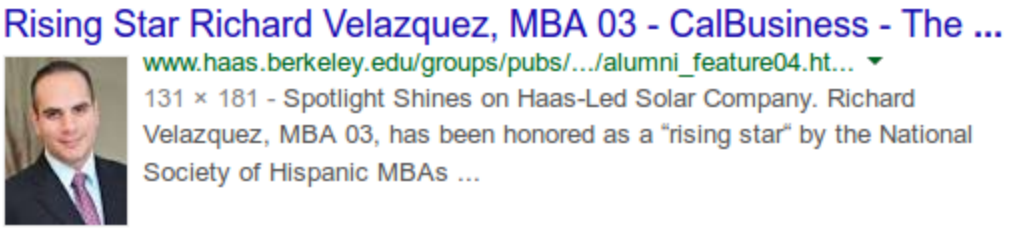


Summary:

I personally received this invite from an alleged recruiter. Upon inspection of the account I found that the user had inconsistencies in their profile and began digging into it. Once I took the headshot and put it into an image search engine I was able to determine that the person in it certainly was not the person they claimed to be in LinkedIn.

By using the email address attached to the account I was able to then look up the metadata on the real person behind the account. This person does live in Alaska and purportedly works for a telco there. Having tracked him further using the email account provided in the LinkedIn profile I was able to track much of his life because he had placed it all online for anyone to see. This included an arrest report in 2013 for being drunk and trespassing in a residence.





Analysis:

The analysis for this incident follows much of what is discussed in the NEWSCASTER report. The takeaway is that your social media profile can lead to corporate or personal compromise. Care should be taken as to what you share and with whom on such sites as LinkedIn, Facebook, Twitter, etc as they can be used to create a dossier on you for further attacks.

In the case of this attempt, the user had poor OPSEC (Operational Security) and thus his legend (cover story) lacked credibility as well as leaving bread crumbs to follow easily to his real name and location. I personally do not list the companies I am employed by because of such attacks and leakage of information that would be counter to security. As such, this attacker was looking for what he had hoped was a target with entre into the government and military spaces that I listed in past jobs that I had had.

** Note at 6am 6/30/14 the user had 109 connections within the federal and MIL space**

HAVEX RAT (Russia)

```
scan_LAN        proc near               ; CODE XREF: scan_LAN4+13E↓p
                push    ebp
                push    edi
                mov     edi, [esi]
                xor     ebp, ebp
                push    ebp
                push    offset asc_10030D58 ; "****************************************"...
                call    write_to_file2
                mov     edi, [esi]
                push    ebp             ; int
                push    offset aStartFinging_1 ; "Start finging of LAN hosts...\n"
                call    write_to_file
                add     esp, 10h
                push    ebp             ; lpNetResource
                push    ebp             ; int
                mov     ecx, esi
                call    recursive_WNetEnumResourceW
                mov     edi, [esi]
                test    al, al
                jnz     short loc_10001427
                push    ebp             ; int
                push    offset aFindingWasFaul ; "Finding was fault. Unexpective error\n"
                call    write_to_file
```

image from F-Secure blog

Summary:

The HAVEX RAT (Remote Access Tool) has been leveraged by Russian APT to attack specific industries that now include power systems and energy companies. This actor group has modified the RAT and their modus operandi to attack SCADA and ICS systems (Supervisory Control and Data Acquisition) in hopes of perhaps carrying out supply chain attacks on those systems. This is the 43rd

iteration of this RAT tool in use by this actor (RU) This group also has used the "LightsOut Exploit Kit" watering hole attack as well to carry out attacks (http://pastebin.com/qCdMwtZ6) according to MalwareMustDie and Cisco.

Crowdstrike designates this group "*Energetic Bear*" and currently this month showed them to be active and being reported on by the press.

Further analysis by Symantec HERE having named it DRAGONFLY

Analysis:

This group of alleged Russian attackers has been active for some time now (circa 2012) and have been seeking data from systems within the energy sector. Given that Russia is a large player in the energy sector it is easy to assume that their motives are for state/private consumption within the energy space. The attacks have been not only on US assets but also on French and other countries companies that they have interests in. As a whole, this group is believed to be nation state but it can be seen as perhaps a co-owned endeavour on the part of the state and the oligarchs who run the large petro and other energy concerns within the former USSR.

With the advent of the HAVEX RAT's SCADA/ICS functionality though it can be an assumption that attacks on those systems could be used in ways that could help the Russian state's prices on energy consumables as well as further other deeper state desires of the Putin government. An attack by an adversary with a horse in the game and geopolitical with monetary repercussions on the supply chains of certain competitors would place the Russian government in a better position globally if not regionally.

Crimeware

(DYREZA) SSL BYPASS RAT

Summary:

Dyreza is a new RAT that has a special method of gathering intelligence. This malware performs an SSL bypass allowing credentials to then be passed in the clear as a kind of man in the middle attack. It in fact steals the credentials in the targets browser thus nullifying the encrypted session altogether. Currently the primary targets of this malware/RAT have been Bank of America, Natwest, Citibank, RBS, and Ulsterbank. This malware campaign also has been cited to have an adversary set that is planning on turning this into a malware as a service model of business. They have set up money "mules" and are seeking to make this a global campaign that one can buy into as a full pipeline from compromise to money movement and laundering.

Analysis:

While this RAT and group (Assumed to be Russian with the naming of Dyreza) are ambitious they have failed to program encrypted comm's into their model thus SIEM and IDS traffic will easily capture and stop their activities. While their approach is novel, they are not as yet a true threat to a larger swath of corporations due to their technical limitations. It is also assumed that these new players are attempting to cash in on the void that was left by the GoZeus takedown recently. Until such time as they next iteration includes encrypted C&C this group should not be considered a major threat actor.

APT Activities

China

Summary:

Crowdstrike reported on a new PLA unit active online today attacking corporations and government entities naming the unit (Unit 61486) as well as some of the players involved by name. In what is called OSINT (Open Source Intelligence) the Crowdstrike team reported on the actual names of PLA members who comprise this unit including pictures and personal details. Crowdstrike is calling this group "Putter Panda" and they are primraily attacking the government, defense, and technology research sectors.

PLA Unit 61486 focuses their exploits against popular productivity applications such as Adobe Reader and Microsoft Office to deploy custom malware through targeted email attacks (i.e. SpearPhishing)

Currently there are 13 groups/cells within the Chinese PLA active today as APT (Advanced Persistent Threats)

Analysis:

Attribution is a troublesome thing in hacking and cyber warfare but the data presented by Crowdstrike is compelling enough to say that they in fact were right. However, the usefulness of such reports is called into question as relations with China sour and the legalities surrounding all of this preclude any solid action of merit. In the case of the Putter Panda report and their doxing of the PLA players it may be a moot point. Outing these players will not necessarily change their tactics as we have seen from the Mandiant reporting on CN activities in the past. In the case of the Mandiant report those actors changed some of their activities but on the whole they fell back into the same practices.

On the legal front outing such sources of attacks also may in fact lead to some sort of naming and shaming at a political level that the US may leverage but I personally unsure of it's efficacy. As we have seen to date the US and the globe lack the proper legal means to attack these problems as well as politically there are no common grounds for countries to apply warfare as separate from civil actions taken by individuals perhaps at the governments behest. In the case of the PLA they are military however, many of their proxy actors are private citizens that are motivated by patriotism and perhaps monetary incentives to carry out these attacks.

On the whole this is just another common APT group within the arcology of Chinese APT who's OPSEC (Operational Security) was lacking and thus they re-used information or aligned information and backstopping for their campaigns with personal data. This allowed OSINT (Open Source Intelligence) analysts to easily follow Wang Dong's trail back to his own personal accounts with

photographs etc. While this is a marketing coup for Crowdstrike the efficacy as mentioned above is still questionable on outing these players.

Iran *(See above NEWSCASTER campaign)*

Russia*(See above HAVEX RAT campaign)*

Syria/SEA (Syrian Electronic Army)

Summary:

The SEA attacked and compromised the Reuters website on June 22nd 2014. This attack followed the usual protocol of defacement by the Syrian Electronic Army and its leader Th3Pr0. The SEA is a group that has formed to fight on the web in a propaganda war of web defacements for the Assad regime. It seems that this hack against the Reuters site was carried out via an attack on a third party vendor who had access to key systems. Someone from SEA fooled a company employee, into giving up their password and then used the access to Taboola's Backstage platform to change the header in the Reuters widget, and thus to deface the page.

Analysis:

It is debated whether or not the SEA is considered to really be a nation state actor or not. As yet it is indeterminate if the SEA has backing from the Assad regime (i.e. money and support) but is something that should be watched and thought about. Such instances of anarchy and propaganda online are much more common post the Anonymous and LulzSec incidents from 2010 on and the model is now popular with online movements.

For the most part SEA's attacks are more propaganda than anything on the level of espionage or acts of warfare. It is debatable whether or not SEA is really capable of much more than defacements but it may also be that the actors within this group may have been holding back on more serious actions. Given their penchant for SE attacks to gather access it is very possible that they could carry out more devastating attacks against their targets internal systems.

It is the recommendation of this assessment that a little of both applies here.

HACTIVISM:

ANONYMOUS: OP: NO2ISIS

Summary:

Anonymous has announced that it plans on attacking ISIS/ISIL funding sources and state backers. In an operation they are calling OP: NO2ISIS Anonymous claims they will be attacking the sources of funding for the group that is presently taking over large sections of Iraq. The three primary targets of Op: No2ISIS will be Turkey, Saudi Arabia, and Qatar but may include other targets as they get intelligence implicating other countries or individuals.

Anonymous plans to attack these sources of funding because they claim that ISIS is not something they can attack online as they are fighting a ground war in Iraq and Syria. Another reason that the Anonymous collective has targeted ISIS is because ISIS took over the account @theanonmessage (an Anon account) and feels that this operation would suffice for retribution against the newly minted terrorist organization. It is not possible to know what real damage Anonymous can have against the funding of ISIS nor perhaps against ISIS itself due to the primary modus operandi of distributed denial of service may or may not have any effect on those targeted.

OFFICIAL ANNOUNCEMENT:

http://www.youtube.com/watch?v=qkwVzsJ_Www

Analysis:

It is of note that Anonymous feels moved to target the funding structure of ISIS for a couple of reasons. Firstly, a frontal attack on ISIS, as they say in their media is hard because ISIS is in fact fighting a ground war in Iraq. However, ISIS does use Twitter and other social media very effectively in a propaganda and recruitment war and this could be attacked rather easily by a group such as Anonymous. This cognitive dissonance on the part of the Anon's makes them look a bit more impotent than they would like on the whole and this operation will likely hardly be a win in any book against ISIS or their funding feeds. This operation will likely have little to no effect on ISIS nor their funding and it is the opinion of this assessment that Anonymous would be better served by attacking the ISIS media wing instead. By degrading the ISIS capabilities for propaganda and recruitment Anonymous might play a better role within the GWOT.

PSYOPS & PROPAGANDA

ISIS/ISIL (Islamic State of Nineveh)

#الدولة_الإسلامية
#ISIS Special Forces deployed to avoid mistake in choosing targets with the best performance. pic.twitter.com/hO5rbAhuSX

Reply Retweet Favorite More

Summary:

The ISIS (Islamic State of Iraq and Syria) has been in a media jihad for some time now and it has accelerated this campaign with the current takeover of sections of Iraq that it has been carrying out. ISIS has a media arm that has been using social media such as Twitter (as seen above) to leverage the internet in a propaganda war as well as a recruitment drive. The group has not only been using twitter with individual accounts but also has created a twitter application that allowed the terrorist organization to use other accts to geometrically reach a larger audience. The tool would be loaded on to user systems and had an API function that allowed the user to put in their credentials and authorize the app to post ISIS jihadi media posts to all of the followers of that account.

Analysis:

ISIS has been rather novel in their use of Twitter online. Their creation of an application to bypass Twitter's own systems is interesting to see as well as it's inherent means of doubling or quadrupling their messages getting out through proxy accounts. (i.e. users allowing themselves to be the conduit of the media jihad) As a means of propagandizing their war in Iraq as well as a tool for recruitment (which has been rising since their campaigns both digitally and on the ground have taken off) ISIS has harnessed the internet and social media in a way that the old guard of Al Qaida never did. This is clearly an advance and should be noted not only from the position of the GWOT but also any other movement that might learn from ISIS and begin their own propaganda wars using social media as the primary medium.

MILITARY FACEBOOK PSYOPS TESTING

Summary:

Facebook has recently published a 2012 study in the March issue of the Proceedings of the National Academy of Sciences. The study was to determine

whether it could alter the emotional state of its users and prompt them to post either more positive or negative content, the site's data scientists enabled an algorithm, for one week, to automatically omit content that contained words associated with either positive or negative emotions from the central news feeds of 689,003 users. This study found that it could manipulate those users emotions to a certain degree by said manipulation.

According to an abstract of the study, *"for people who had positive content reduced in their News Feed, a larger percentage of words in people's status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred."* The study was partially funded by the Army Research Office -- an agency within the U.S. Army that funds basic research in the military's interest according to a press release from Cornell University.

Analysis:

While this type of testing is a normative thing within the psychology sphere, the problem that many have latched onto is that the US military funded this one. The assessment of this story and the study itself does lead one to believe that on the whole the military as well as Facebook have some ethical questions to face about this. Facebook surely is looking to manipulate their users for purposes of sales and the synergy of that in tandem with the military's desire for PSYOPS tools is rather assured. By using social media like Twitter or Facebook, the millitary as well as other actors could manipulate populaces en mas with these techniques and this is a dangerous precedent to set.

GLOBAL INTELLIGENCE ANALYSIS:

Summary:

Overall this report has been put together to show a high level approach to global trends in threats online. The actors are varied from criminal syndicates, to nation state actors and spies, to global jihadist movements abroad. Truly the internet and computers have brought a new and very extensible means of espionage,

terror, and manipulation of peoples through social media, hacking, and other means within the digital realm.

As we have been seeing the technologies are becoming easier to master for many to use guerrilla tactics and unconventional warfare online to further their goals. Whether that be a nation state like Russia using malware to effect the supply chains of other nation states energy companies or Ukrainian syndicates seeking to steal masses of personal data along with credit card numbers and pins we are seeing a change in paradigms digitally. All of the attacks written about in this report are fodder for the reader to consider the technological landscape today and the types of attack methods as well as goals that predicate them.

The takeaways from this June report are the following bullet points:

- **Social engineering has always been a staple but now that social media is in the mix it's use is much more devastating to organizations**
- **Malware tools are constantly being upgraded or created anew with various attack vectors that leverage phishing/spearphising/ and social media attacks**
- **Globally, intelligence gathering techniques are no longer solely the purview of nation state actors and their spy agencies alone.**
- **Propaganda and misdirection are becoming more popular not only with nation state actors but also terrorists and criminal gangs**

APPENDIX A: LINKS

http://www.stockhouse.com/news/press-releases/2014/06/10/akamai-warns-fortune-500-of-high-risk-threat-from-zeus-crimeware

http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?_r=0

http://www.openssl.org/news/secadv_20140605.txt

www.crowdstrike.com/.../CrowdStrike_Global_Threat_Report_2013.pdf

http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/

http://www.darkreading.com/vulnerabilities---threats/advanced-threats/a-dyre-new-banking-trojan/d/d-id/1278620

http://www.zdnet.com/chinese-army-group-hacks-us-satellite-partners-crowdstrike-7000030353/

http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fcdn0.vox-cdn.com%2Fassets%2F4589853%2Fcrowdstrike-intelligence-report-putter-panda.original.pdf&ei=ooOxU97iNYWqyATRqoKQDg&usg=AFQjCNHzq5qbTVgD8V-gwGKo_-naV9GG5Q&sig2=6TYhWyIHI4ZfRjO0NbyUxg&bvm=bv.69837884,d.aWw

http://www.eweek.com/security/third-party-service-providers-scrutinized-after-seas-reuters-hack.html

http://www.forbes.com/sites/jasperhamill/2014/06/27/anonymous-hacktivists-prepare-for-strike-against-isis-supporters/

http://www.kshb.com/news/us-government-helped-fund-facebook-experiment-that-manipulated-users-emotions