Anticipating Cyber Attacks:

There's No Abbottabad in Cyber Space

Executive Summary

Cyber attacks, data breaches, and vulnerabilities have gone from esoteric ideas to a mainstream problem[1]. With that in mind, it would be quite attractive to predict attacks before they happen. Prediction could allow us to adjust defenses rather than perform expensive and reactive incident response which can include everything from deep forensics to throwing out millions of dollars worth of equipment. And not to mention massive reputation repair campaigns.

In the world of non-cyber warfare, criminality, and activism we try to predict attacks and violence before they happen. Attacks are never isolated, they are motivated by end goals that can inform analysis and they happen in cycles. We run extensive intelligence programs, executed by law enforcement and intelligence agencies. Programs assess the intent and capabilities of adversaries. (Example: What are China's military intentions as they relate to Taiwan and does China have the capability to execute military activity against Taiwan?)

In cyber, we face a different and sometimes frustrating world especially as it relates to generating meaningful insights and intelligence. However, there is also good news. As Oren Falkowitz, former USCYBERCOM Chief Data Scientist states it, "In cyber security the web balances being the platform to create attacks and being the source of information to prevent attacks." We can track the data trail of threats, attackers, methods, and operations *before* they execute attacks.

Predicting World Events

Predicting is hard. Yogi Berra quipped that it's tough to make predictions, especially about the future. Nevertheless, we've seen enormous steps over the last decade in terms of building meaningful predictive models, from forecasting elections[2] to local weather predictions.

We've seen progress in predicting offline activism, violence, crime[3], and war. Nathan Kallus from MIT has built very strong models using Twitter data to predict unrest in a series of countries around the world[4]. Simple insights such as how political unrest follows anniversaries, sometimes like clockwork, can yield strong predictions. (Example: The #Jan25 protests in Egypt over last three to four years[5].)

[1] http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/
[2] Nate Silver's 2012 book The Signal and the Noise: Why So Many Predictions Fail-but Some Don't
[3] http://www.cnn.com/2012/07/09/tech/innovation/police-tech/
[4] http://arxiv.org/abs/1402.2308
[5] http://en.wikipedia.org/wiki/Egyptian_Revolution_of_2011

Anatomy of Cyber Events and Actors

To understand cyber actors and related event let's separate them into three simple bins: hacktivism (e.g. Anonymous defacing a website, Syrian Electronic Army taking down the New York Times web-site), criminal (e.g. groups stealing money or identities online), and finally espionage (e.g. countries stealing state secrets or intellectual property).

Hacktivism

When we think of hacktivism we typically think of Anonymous and their attacks on companies, organizations, and countries. Over time, other groups have emerged with similar modus operandi; be it al-Qassam Cyber Fighters (QCF), Syrian Electronic Army (SEA), or AnonGhost. There are many ways to characterize these groups, but for our objective of prediction one of the most interesting approaches is to look at whether they pre-announce their activities.

Analyzing a large number of attacks from hacktivist groups, we see that some like Anonymous and AnonGhost always pre-announce their attacks, sometimes down to specific dates and targets. Others like QCF sometimes forecast attacks on ambiguous targets. And others like SEA never pre-announce their attacks. The differences are partially due to the methods employed (e.g. phishing attacks are never forecast) but also the desired public relations (e.g. attack on Israel vs. attack on Technion).

Cyber Crime

A common form of cyber crime is theft of money. Cyber criminals stealing money may do so by infiltrating ATM networks, transaction skimming from online banking systems, or threatening to lock up a computer unless a ransom is paid. There's little benefit to the attacker to pre-announce anything in these situations. Cyber criminals may be a single individual, but more likely complex networks of people spread around the world with multiple roles.

The activities of cyber criminals are likely long-term operations. They are unlikely to be of the movie style "hack a computer, extract $100M, and run off" – since in reality the last part, running off with $100M, is really hard. Money stolen electronically needs to be transferred, and eventually the cyber thieves will want to hit ATMs or other mechanisms for "hard cash[6]."

Espionage/APT Style – Targeted, Long-Term Attacks

Espionage attacks are in many ways similar to cyber crime. They are seldom focused on propaganda and rather on stealing information (e.g. email traffic from dissidents or blueprints for a new missile system). Since these type of attacks traditionally deal with more hardened targets (e.g. defense technology firm that is likely to have advanced cyber defense systems), they take a long time, target specific individuals through social engineering, and carefully take advantage of system weaknesses. Many times these attacks are referred to as APTs – which Mandiant nicely lays out in this description[7].

[6] Anonymous cryptocurrencies like Bitcoin are producing new opportunities here.
[7] http://www.mandiant.com/threat-landscape/anatomy-of-an-attack/

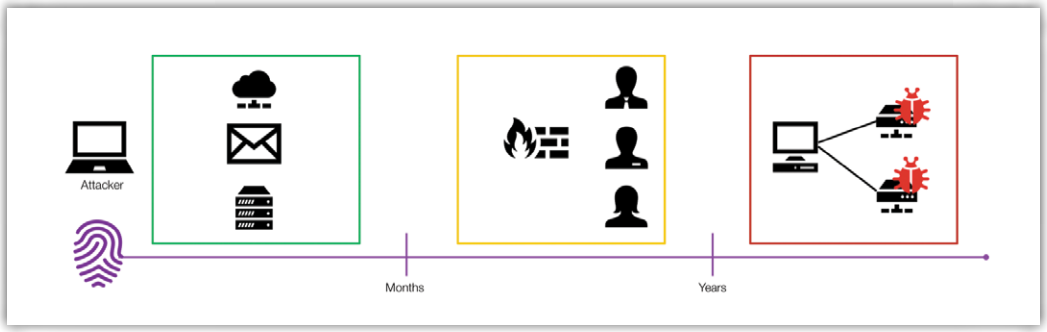

Figure 1

Targeted cyber attacks are campaigns with multiple distinct phases that unfold over many months and years[8].

Like cyber criminals, these actors are unlikely to forecast their activities and very careful to leave no trace of them either. Nevertheless, these campaigns correlate with political, economic and military objectives that are possible to analyze and maybe even predict. Likewise the human operators live real lives that runs on a calendar and clock that's quite possible to track.

Predicting Cyber Events

CISOs, even of very sophisticated organizations, tell us there is a de facto endless backlog of patching, upgrading, and tuning for existing infrastructure. If one were able to predict a cyber attack, the CISOs could better prioritize that work. They could educate employees on particular social engineering attacks. In extreme cases, a government or corporation may even shut down foreign internet access for limited time periods.

Given how important it is, how can we predict cyber attacks? We're not going to find a panacea, but even indications of an emerging threat can be interesting. And detection of intent can put us appropriately on guard.

Announced Hacktivism

The most obvious type of predictions are probably those based on hacktivists that "pre-announce" their attacks, like discussed above. This includes groups and collectives such as Anonymous, AnonGhost, and al-Qassam Cyber Fighters.

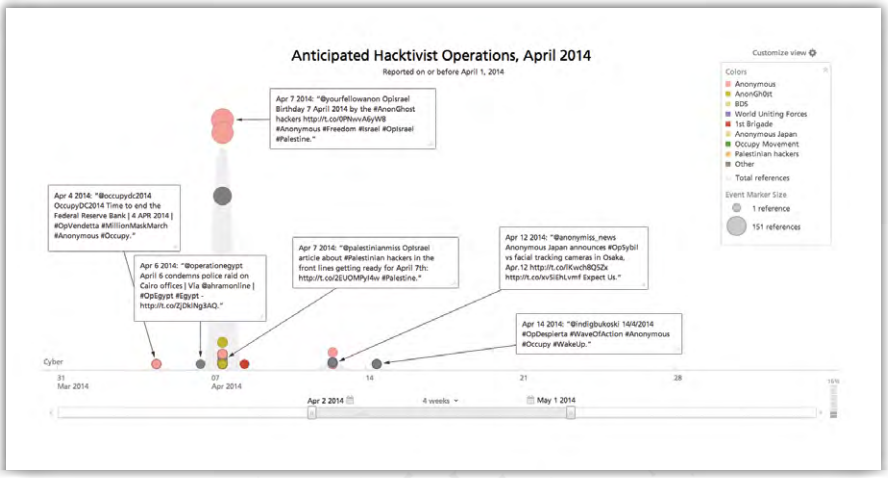

Figure 2

Observing the world as of April 1 we can observe OpIsrael being planned for April 7.

[8] Oren Falkowitz, Dismantling Cyber Delivery Systems

When observing an event like this, we may dive in to understand what operators/activists are involved, what methods they are looking to use, what targets they are looking to hit, etc. We may also check if these operators have previously launched successful attacks, and based on this assess credibility.

Anniversaries

Anniversaries are powerful organizing principles in political movements, activism, and terrorism – and can also be in cyber activities. The recent #OpIsrael campaign was on the anniversary of earlier such campaigns, which in itself is held on the eve of Holocaust Remembrance Day[9]. Over the years to come it's also likely we'll see more hacktivism around controversial dates, so understanding how key anniversaries fit into the context of corporations and organizations – depending on where you do business – can be important.

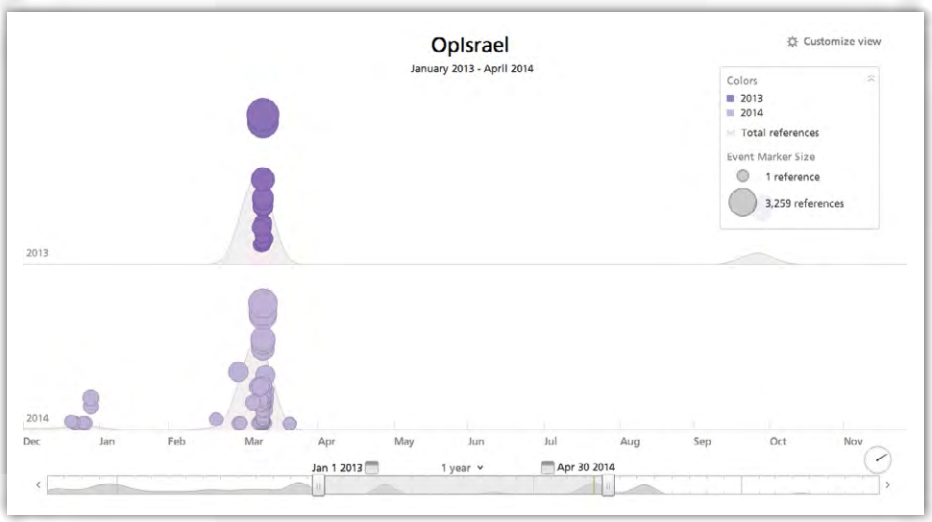

Figure 3

Anniversaries are often powerful organizers for terrorists, protesters, and hacktivists.

Pattern of Life

Moving beyond explicit call outs and anniversaries we find many other clues to when hacker organizations may strike. Behind every attack, be it a hacktivist or a sophisticated military operator, there's a human. Humans need to eat and sleep. They have families. They may have day jobs. This allows us to study their lives, so called pattern of life analysis. The below from Joint Force Quarterly[10] describes the use of surveillance techniques for pattern of life analysis.

› The purpose of this long dwell airborne stakeout is to apply multisensor observation 24/7 to achieve a greater understanding of how the enemy's network operates by building a pattern of life analysis. This is an important concept and has proven itself time and again with hundreds of examples of successful raids.

Pattern of life analysis can yield predictions about the whereabouts of a target and his movements and actions. In cyber we study when attacks happen and examine temporal patterns of weekdays, holidays, hour of the day to glean indications of when an organization is active. From the visualization below we can for example distinctly see how the Syrian Electronic Army lights up on Sundays after a Friday-Saturday lull, following the Syrian weekend.

[9] http://en.wikipedia.org/wiki/Yom_HaShoah
[10] Joint Force Quarterly, issue 50, 3d quarter 2008

Figure 4

Laying out day of week for attacks by various hacker groups yields distinct temporal fingerprints[11].

Similar patterns have been described in the APT1 study by Mandiant, indicating a potential China-based, professional and paid team.

"Hacker teams regularly began work, for the most part, at 8 a.m. Beijing time. Usually they continued for a standard work day, but sometimes the hacking persisted until midnight."[12]

Patterns like these are actionable; a media company that knows of attacks against competitors by the SEA should staff up their operations center on Sundays in response.

Trend Observation to Avoid Surprises

A total surprise sometimes in hindsight becomes part of an observable trend. Take the recent large scale data exfiltration from Target Corporation[13]. A key attack vector was the BlackPOS malware used to scrape data from point-of-sale (POS) systems. There was a clear rise in awareness about BlackPOS and other malware and its dangers to POS systems, well ahead of the actual attack (see below figure). Given the importance of POS systems at retailers you would imagine tracking trends regarding key technologies and threats to them would be a key operational activity (presumably now it is). Trend watching should be a core aspect of any threat intelligence operation.

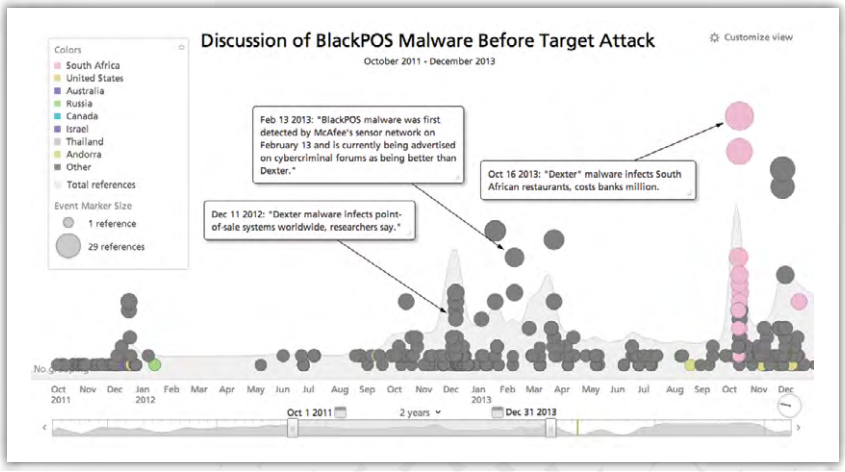

Figure 5

The attack on Target's POS system brought a long simmering security issue into the spotlight.

[11] Pattern of Life and Temporal Signatures of Hacker Organizations.
[12] Sign That Chinese Hackers Have Become Professional: They Take Weekends Off
[13] Sources: Target Investigating Data Breach

Generally, many of these scams (credit card scams or ATM skimming techniques) travel around the world. Techniques transfer through the underworld of forums. Regardless of approach there's a good opportunity for intelligence analysts to monitor trends of such scams and catch them before they hit home.

Anomaly Detection

Detecting cyber attacks has long been about detecting anomalies (traffic emerging from a bad IP range). Monitoring for patterns like this is important - however by the time we detect such patterns, it may be too late. In a very similar way we can track anomalies before they hit us:

› Is an attacker we know but haven't traditionally worried about changing his targeting? Example: The SEA went from targeting media companies to communication companies like Truecaller and Viber.

› Are groups starting to cooperate who previously have not? Example: Redhack, Anonymous, and SEA around OpTurkey[14]. This may lead to knowledge transfer making a known adversary more dangerous.

Technology Change Predicts Targeting

Technology change may provide signals for targeting. Due to both just a staggering number of targets available to a cyber operator, as well as an equally staggering number of technologies that are part of target surface areas, targeting may very well start with identification of the most convenient targets.

Recently, Microsoft very publicly pre-announced that Windows XP support would end in April 2014. Without new security patches, Windows XP became a very attractive target.

Likewise, Microsoft is known to release new security patches on the second Tuesday of each month in North America – *Patch Tuesday*[15], which, by the way, is a good example of organizational pattern of life. Knowing this pattern, we can then observe *Exploit Wednesday* – when attackers will seek out unpatched systems which may be wide open for fresh attacks.

So, What About Network Data as an Analytic Source?

The above reasoning and analysis is drawn exclusively from open sources of information. Traditionally, analysis in information security has focused on network traffic (e.g. anomalous patterns in firewall traffic.) Of course, techniques such as trend analysis and pattern of life studies can be applied here too. Better yet, combining traditional methods with understanding external threat factors and patterns can be very powerful.

There's No Abbottabad in Cyber Space

The reasoning in this paper may imply detecting patterns of malicious activities is easy, but nothing could be further from the truth. Many cyber attacks go undetected, sometimes forever. If an individual tries very hard to stay "out of sight" and perform targeted operations while leaving no traces then it will obviously be difficult to analyze threat activity, let alone make predictions. As an analogy, Osama Bin Laden stayed out of sight for a decade despite a full onslaught of intelligence agencies chasing him, a feat made possible through clever indirection between his influence structure and actual activities. Doing this and actively being a cyber operator is not easy. In fact, Bin Laden escaped so long partially by avoiding the internet like a plague.

[14] #OpTurkey: Syrian Electronic Army Joins Anonymous In Turkey Protests, Hacks Erdogan's Network To Access Staff Data
[15] http://en.wikipedia.org/wiki/Patch_Tuesday

"Heisenberg's Uncertainty Principle"

Will the act of observation lead to a change in behavior? Won't hackers just avoid these tactics, knowing their intelligence value to defenders? Some actors (e.g. hacktivists) rely on large groups of people working together and can only do so by generating open signals. Other groups need to turn their activities into post event PR and again will generate traces. Even the most sophisticated cyber criminals or government backed groups will generate traces in their choice of methods, their choice of micro (e.g. Chinese workday) and macro timing (e.g. around US military maneuvers), and their choice of objective. It is frankly unavoidable to leave traces.

Conclusion

Cyber attacks of various forms have been around since the birth of the internet and they are likely to be around as long as the internet is around. While there certainly are no crystal balls for predicting such attacks, there are many techniques we can apply to try get ahead. The internet itself provides an amazing source for generating predictive signals. We have the opportunity to take advantage of such signals – and it will lead us to a brighter future in security.

About Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.