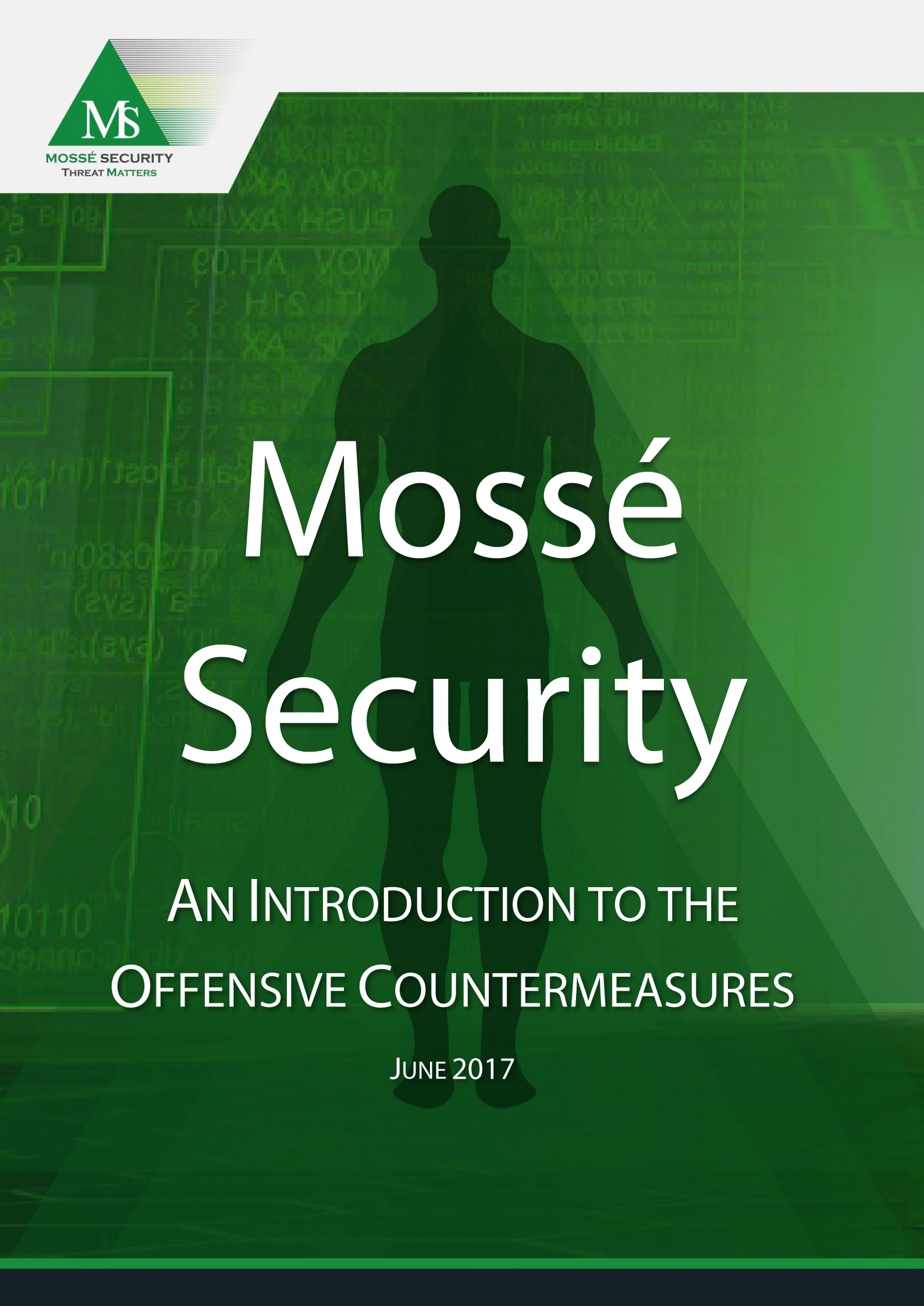
MOSSÉ SECURITY
THREAT MATTERS
Mossé Security
AN INTRODUCTION TO THE OFFENSIVE COUNTERMEASURES
JUNE 2017

EXECUTIVE SUMMARY

This whitepaper introduces the Offensive Countermeasures. The Offensive Countermeasures is a security strategy that creates consequences for the attackers who hack our computers. We hold the tenet that if resources are not spent on tracking and disrupting the attackers, then we are, by omission, allowing them to try new ways to breach our defences and to come back later to steal even more from us.

At a high-level, the Offensive Countermeasures consists of a wide range of power instruments such as: negotiation, psychological warfare, cyberwarfare, economic warfare, information warfare and prosecution.

We're showcasing an anonymised case study where our company used Offensive Countermeasure tactics to discover the individuals behind ongoing attack campaigns against one of our clients. We confirmed the identities of the adversaries using GPS tracking and social engineering techniques. In the end, we issued them a cease and desist letter with an expressed threat that legal and law enforcement actions would be taken if the attacks did not stop immediately. The Offensive Countermeasures aimed to stop their ongoing attack campaigns, and stop they did.

A common misconception about the Offensive Countermeasures is that it consists of illegally hacking back the hackers. In our case study, however, we show that none of the tactics employed were illegal. Furthermore, it cost our client significantly less to employ Offensive Countermeasures than investing in hiring more IT security personnel or purchasing new security technologies that most likely would have proven ineffective against a persistent adversary.

Therefore, we conclude that until worthwhile consequences are imposed by defenders and law enforcement onto the adversaries, computer hacking will continue.

INTRODUCTION

Information security professionals have at their disposal numerous approaches to build a cyber security programme. The most common approaches are to comply with industry standards, align to best-practice frameworks, use risk-based decision models, and follow common sense information security principles.

In our view, one area in which many of those approaches have historically fallen short is the failure to focus their understanding on how attackers think and operate when they target organisations. Because of this failure, we consistently see clients fail to implement countermeasures that create real consequences to the adversaries hacking them, and thus making them cease their attack campaigns.

In this article, we begin with offering the reader a general overview of the cyber adversaries, followed by our proposed explanation as to why information security defences solely based on following logical steps without considering the psychology of the attackers, are ineffective. And finally, we introduce Offensive Countermeasures in a greater detailed panorama, and share case studies.

PART 1: UNDERSTANDING ADVERSARIES

When referring to cyber adversaries, we generally categorise them based on their motive, geographical location, organisational structure, and skill level.

The most commonly known attacker categories are: criminals, terrorists, activists, disgruntled employees, insiders, intelligence agencies, military units, kids, and industry competitors.

Once we understand the attackers' motivations and what matters to them, only then we can begin to influence them to stop their attacks. Thus, let's begin with an understanding of the main motivations for individuals to hack.

MOTIVATIONS

Most attackers are financially, politically, or philosophically motivated.

The overall industry consensus is that cyber criminals have made hundreds of millions of dollars from ransomware attacks since 2015. Some even say that ransomware may be an industry worth as much as one billion dollars a year.

In 2015, the Australian government also publicly announced that Chinese intelligence services penetrated the Bureau of Meteorology's (BOM) network[1]. BOM has network links into numerous federal government agencies, including the Department of Defence.

Now that we understand what motivates adversaries to hack into computer networks, let's look at the top computer crimes they commit to achieve their goals.

TOP COMPUTER CRIMES

The top crimes conducted by cyber attackers against organisations are listed in this diagram:

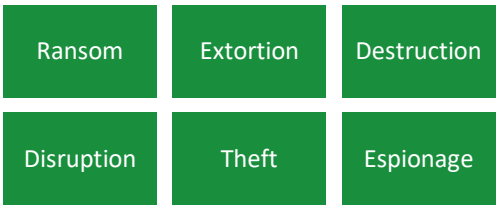

Figure 1 – Top Computer Crimes

Let's turn ourselves to the most common attack techniques cyber adversaries employ.

TOP ATTACK TECHNIQUES

The most common attack techniques employed by computer hackers are:

- Ransomware, whereby attackers encrypt the work files of employees and companies and request a ransom payment to be retrieved.
- Data Theft, whereby attackers steal the data stored in company databases and resells it onto illegal e-commerce websites hosted in anonymous parts of the Internet.
- Deny of Service, whereby attackers prevent companies from operating by rendering IT assets unavailable. The victims are then extorted if they want to resume business operations.
- Money Transfers, whereby attackers coerce companies to process money to fictitious employees and suppliers maliciously registered in business management software.
- Espionage, whereby attackers record the microphone and the webcams of their victims, alongside stealing their documents and the emails. The intelligence

collected is then sold to competitors and used to gain an edge on the victims.

The top consequences of those attacks for companies are financial losses and damage to reputation.

WHY WOULD THEY HACK ME?

Too many business owners believe that their company holds nothing of value that could attract cyber threat actors. This misconception leads business owners to have a false sense of security that in effect makes them easier targets.

What many business owners have not yet realised is that attackers find creative ways to make money from assets built by law-abiding people simply by exploiting vulnerabilities in their computer systems.

For example, a very common attack employed by cyber criminals consists of registering a new fictitious supplier into the company's business management software and raises an invoice to be paid to that supplier.

So long as there will be money to be made from hacking computer systems, there will always be malicious individuals trying to compromise computer networks.

HACKERS ARE NORMAL PEOPLE

Whilst we refer to adversaries as "hackers" and "attackers", they are normal people that can be influenced through a multitude of ways. Let us demystify the adversaries by looking at some profiles:

The following is a picture of Sergey Taraspov, the hacker who wrote the malware used to steal credit card numbers from Target USA:

Figure 2 – BlackPOS Malware Author

The following is an image of the building in Shanghai where hundreds of military personnel - part of China's PLA Unit 61398, work from to hack organisations worldwide.

Figure 3 - PLA Unit 61398

The following is a picture of some of the top Chinese military personnel wanted by the FBI for committing computer crimes against US companies.

Figure 4 – Five Officers in PLA Unit 61398

The following is a picture of Peter Nash, an Australian citizen living in Queensland who acted as a forum moderator for one of the largest underground e-commerce websites called Silk Road:

Figure 5 – Underground Black-Market Moderator

NOT ALL HACKERS ARE BAD PEOPLE

Whilst all attackers act outside the law and their actions have, without reservations, real impacts on their victims, we should stay clear from demonising them.

In some cases, top IT engineers are held hostage by cartels and mafias who may hurt their families if they do not build cyber weapons that are then used to steal money and hold companies ransom.

For those who have joined government organisations, and hacking is simply their job.

ATTRIBUTES OF COMPUTER HACKERS

Now that we better understand who the adversaries are and why they hack, we'll offer some key points regarding their psychology that may explain why preventive security defences are ineffective at deterring them.

Attackers Don't Give Up Unless They're Forced To

Attackers are not deterred by security defences they cannot defeat. Neither do security defences make them give up and move on. Quite the opposite happens. They view strong defences as rewarding challenges to overcome.

The only cases where we have seen attackers "give up" was when they were arrested by law enforcement authorities, or when the defenders used economical, operational and psychological punishments that made them not want to try again.

Even in such circumstances, there are no guarantees that the attackers will completely stop! Even after having spent time in prison, they may not have given up on a life of cybercrime.

Attackers Come Back

Just in the same way that hackers never give-up, attackers are never truly finished with a target.

Hackers may go away for a while, then return to check whether they can gain anything new from previous targets.

Attackers Use the Least Effort Required to Get In

Attackers use the least effort required to breach into their targets' networks and remain undetected.

Even advanced cyber attackers will employ very basic attack techniques if the strength of the defences they are facing do not require them to use more advanced methods.

For example, attackers may follow this methodology when attempting to compromise organisations:

Step 1. **Spear-phishing**: If that doesn't work,

Step 2. **Password Guessing**: If that doesn't work,

Step 3. **Find & Exploit Known Vulnerabilities**: If that doesn't work,

Step 4. **Find Unknown Vulnerabilities**: If that doesn't work,

Step 5. **Hack the WIFI**. If that doesn't work,

Step 6. **Plant Physical Backdoors**: If that doesn't work,

Step 7. **Wait and Repeat**: Follow this process again in 30 days.

Attackers don't give up. But they do follow an attack process that can be predicted. And that gives the defenders an unprecedented edge to track, catch, deceive, and disrupt them.

Let's explore in more depth why our current security strategies are failing us.

PART 2: WHY ARE OUR SECURITY STRATEGIES FAILING US?

Our industry's primary approach to cyber security has been to use strategies and frameworks aimed at demonstrating that reasonable steps were taken to prevent and respond to breaches.

The problem is that none of those "reasonable steps" consider the psychology and constraints of the people behind the keyboard hacking us.

Another industry that once faced a similar challenge is the hostage negotiation industry.

Let's look at what the information security industry could learn about dealing with cyber threat actors from two senior hostage negotiators.

NEVER SPLIT THE DIFFERENCE

In his book on negotiations called "Never Split the Difference", former FBI lead international hostage negotiator, Christopher Voss, recounts the kidnapping of Jeffrey Schilling.

Schilling was an American citizen captured and held hostage for 8 months in the Philippines by the militant Islamic group

Abu Sayyaf led by Abu Sabaya, who had a long history of rape, murder and beheadings:

Figure 6 – Abu Sabaya

Sabaya demanded a 10 million-dollar ransom for the release of Jeffrey Schilling.

In Sabaya's mind, the ransom money was for "war damages" caused to his people for over 500 hundred years of oppression.

In the end, Christopher Voss helped negotiate the price down to zero using negotiation techniques aimed at making Sabaya feel understood.

Mr. Voss instructed his lead negotiator, Benjie, to repeat every detail that Sabaya had shared about war damages in the last 7.5 months of negotiating back to him.

After 10 minutes of Benjie repeating "the World according to Sabaya" to Sabaya, he fell silent for a minute and then said the words "that's right". And from that point onwards, Sabaya never mentioned money again.

Voss explains in his book that his team used emotional intelligence to appease Sabaya, and that technique also helped guarantee the hostage's safety.

According to Voss, when dealing with criminals, emotional intelligence (EQ) plays a more important role than intellectual intelligence (referred to as "IQ").

EMOTIONS ARE "IT"

Christopher Voss, arguably one of the most experienced hostage negotiators in the world, has been an outspoken critic of negotiation strategies based solely on logic because he and the FBI quickly realised that threat actors are first and foremost emotional beings.

According to him, the FBI learnt that negotiations must be based on emotional intelligence rather than on logical steps.

Similarly, the information security industry must realise its objective is to influence the adversaries – not to develop more complex frameworks and strategies that fail to consider the psychology of adversaries.

TERRORISTS AT THE TABLE

Should governments negotiate with terrorists?

Jonathan Powell, the former Chief of Staff to Tony Blair, argues in his book, "Terrorists at the Table" that without negotiating with terrorists, we will never end armed conflict.

According to Powell, no threat groups that have political and financial support can be defeated without negotiations.

He advocates a process based on contacting the enemy, building a communication and engaging in negotiations that, in some cases, may take years to yield positive results.

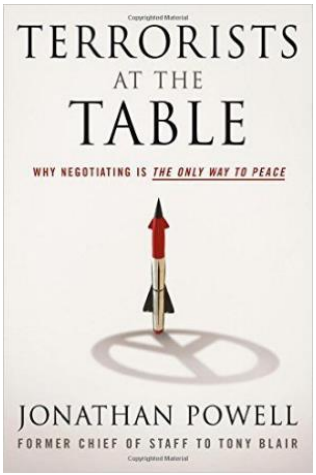

Figure 7 – Book "Terrorists at the Table"

Some key points Powell mentions in his book are:

- It can take a long time for terrorists to understand what are acceptable demands and what are not. Throughout the negotiation process they may continue their attacks whilst remaining open to constructive discussions.
- Terrorists are normal people with families and dreams. There have been numerous cases where terrorists have made conscious efforts to negotiate with governments because they became tired of being fugitives.

Similarly, the information security industry will never end cyber-attacks without engaging directly with the adversaries through a multitude of countermeasure instruments aimed at discouraging them or turning them into allies.

PART 3: USING OFFENSIVE COUNTERMEASURES

When an attack group successfully conducts a massive security breach, it is only a matter of days until other groups attempt similar attacks against other companies in the same industry as the first victim.

That is because prevention, detection and response activities do not influence the adversaries enough.

Examples of complementary offensive countermeasures that should be used in conjunction with one another are:

- Negotiation – Coming to an agreement with the attackers that guarantees hacking campaigns are stopped or reduced.

  For example, if the attacker is a teenager, the victim company should consider hiring him or her and spending time training them on ethics. Another example includes the US successfully negotiating a cyber agreement with China to reduce attacks against US companies.

- Psychological Warfare – Negatively affecting the attackers' morale to make them reduce or cease their attacks.

  A good starting point for private companies is to issue adversaries cease and desist letters.

- Cyber Warfare – Destroying or disrupting the adversaries' IT assets.

  That may include releasing the source code of their malware on the Internet in a way that will force the adversaries to rebuild their entire hacking infrastructure.

- Economic Warfare – Discovering how the adversaries are funded, removing their source of income and making sure they cannot pivot to other income sources.
- Information Warfare – Infiltrating adversary groups and disseminating false information to turn members against each other. Thereby dismantling the groups and cancelling their operations.
- Political Warfare – Discrediting the motivations of the adversaries to remove their political support and therefore cause them to dismantle.
- Law Enforcement – Getting the adversaries arrested and sent to prison.

HACKING BACK

In some cases, the instruments of influence outlined above may require defenders to "hack back" the attackers to find their identities, understand their motives and organisational structure. With that information, defenders can design a well thought out plan to dismantle the adversaries' operations.

The consensus in the information security industry is that hacking back is a bad idea because it could cause an escalation in violence and it may be illegal.

Though, the reader should note that many of the offensive countermeasures presented in this article can be achieved without breaking the law or even hacking into the computers of the hackers.

In many cases, adversary groups can be infiltrated and the necessary information can be extracted using fingerprinting and social engineering techniques.

For example, the Honey Badger tool offered in the Active Defense Harbinger Distribution can be used to capture sufficient intelligence to track computer hackers.

The following image shows how John Strand used Honey Badger to track and call an attacker who attempted to hack Strand's website:

Figure 8 – Honey Badger

With one phone call to the attacker, Strand emotionally disrupted and scared the attacker enough to make sure he would not attempt any further attacks.

CYBER ATTRIBUTION

Attribution based on cyber indicators is not a bulletproof method to identify adversaries. Rather cyber attribution offers a starting point for security teams to engage in other attribution techniques such as human intelligence.

Social engineering, infiltration of adversary groups, acquisition of agents, and proactive surveillance can rapidly confirm or infirm attribution theories based on cyber data (e.g. malware analysis, goals and TTPs).

In the end, the best way to confirm the identity of attackers may simply be to call the suspects. Defenders will soon realise that they can learn more information about their adversaries from a 10-minute phone call with them than hours of investigative work!

WHAT'S LEGAL

The following lists the activities that the law allows the private sector to effectuate:

- Deception
- Discretisation
- Disinformation
- Prosecution
- Threat hunting
- Threat intelligence
- Negotiations
- Infiltration through invitation
- Surveillance (without hacking their computers)
- Disruption:
  - Defeating their tools, tactics, techniques and procedures (TTTPs) on your network
  - Publishing their TTTPs on the Internet
  - Publishing their identities on the Internet
  - Convincing them to move on to other targets

WHAT'S ETHICAL?

Some argue that it is not ethical for private companies to directly engage in hacking-back or infiltrating adversary groups.

From a philosophical standpoint, we agree with people who hold this tenet. In practice. however, we acknowledge that the adversaries sometimes place the defenders in impossible situations.

As one Chief Information Security Officer once told us: "If attackers stole files worth 500M to us and we knew the files were stored by them on a server in Vietnam. Do you really think we wouldn't hack into that server to delete the files to prevent the breach from escalating any further?"

Mossé Security's position is that the Offensive Countermeasures should exclusively be used for self-defence purposes.

Strict policies and procedures should be created, implemented and followed to prevent team members from acting outside a clearly defined scope of actions.

The Offensive Countermeasures Team should consist of senior security personnel with a proven track record of professional discipline, a good understanding of what is legal, what is not, and they should operate in absolute discretion.

When engaging in negotiations with the adversaries, professional negotiators should be hired.

HOW DANGEROUS CAN DISRUPTING ADVERSARIES BE FOR DEFENDERS?

Some cyber attackers are dangerous criminals or intelligence agencies that should not be engaged directly.

In case where direct engagement is not possible, we recommend political and information warfare. One way this can be done is informing the public and the government of illegal activities committed against Australian companies and citizens. A professional public relations company should be hired.

The goal of successful political and information operations should be to lobby the government to provide additional assistance to companies that are not considered critical infrastructure, and that do not have sufficient internal resources to defend against dangerous criminals or foreign governments.

Hacking events between 2015 and 2016, in the United States and elsewhere, have demonstrated that the private sector can make reducing cyber-attacks a top priority for prime ministers and presidents.

HACKING TEAM CASE STUDY

Hacking Team was an Italian security company that sold espionage and surveillance cyber weapons to multiple governments around the world.

In 2015, a hacker known as "Phineas Fisher" published all of Hacking Team's cyber weapons onto the Internet[2]. Because of this data breach, Hacking Team lost many (possibly all) of its clients and the Italian government revoked the company's license to sell cyber weapons outside of Europe without special permission.

This case study demonstrates how successful the Offensive Countermeasures can be. They stopped an advanced cyber attacker by causing them significant economic, political, reputational and cyber damages.

CLIENT CASE STUDY

In response to multiple attack campaigns conducted against one of its clients, Mossé Security deployed bespoke Microsoft Word document "honeypots" (hacker detection and tracking systems).

Within 10 days of the honeypots deployment, Mossé Security located the street where the attackers were located by capturing their IP's GPS location.

Because we knew what data the adversaries were stealing from our client's network, we discovered a single organisation matching the profile of a potential competitor company located within 100 metres of the GPS coordinates extracted. On their website, the competitor company advertised similar products to our client.

A private investigator was hired in the attackers' city and the direct phone number of the competitor's Chief Executive Officer (CEO) was discovered.

A phone call was then issued to the CEO on a day where we knew with certainty that their agent was attacking our client's network. We used social engineering techniques over the phone to confirm that this company were indeed behind the attacks.

What further confirmed the identity of the adversaries was that within minutes of our phone call to them their agent disconnected from the client's network.

In parallel of this tactic, the client hired a local law firm and issued a cease and desist letter to attackers that was hand delivered to them the next day. This action further reinforced to them that legal actions would be taken if hacking activities did not stop immediately or if the intellectual property stolen was used again for commercial purposes.

Whilst those tactics cannot guarantee with certainty that the adversaries will not try to compromise our client again, successful threat intelligence and psychological warfare proved effective. Eight (8) months after the application of Offensive Countermeasures were integrated, the attackers have not been seen coming back.

HOW CAN COMPANIES EMPLOY THE OFFENSIVE COUNTERMEASURES?

Companies that want to use Offensive Countermeasures must first build successful threat hunting and threat intelligence programmes to detect, analyse and deanonymize the adversaries they are facing.

Then, they can use the following process as a template to get started:

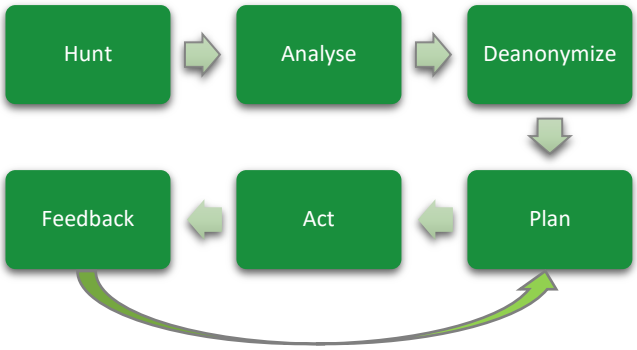

Figure 9 – Offensive Countermeasure Process

- **Hunt:** Detect as many adversarial tactics and techniques as possible on the network. The ATT&CK Matrix presents a good starting point for defenders to list many of those tactics and techniques.
- **Analyse:** Profile the adversaries:
    - Motivations
    - Goals
    - Tactics, Techniques, Procedures (TTPs)
    - Tools
    - Known IT infrastructure
- **Deanonymize:** Security teams can use cyber deanonymization techniques such as "honey badgers" and "honey documents" to obtain geolocation coordinates of the attackers and infer their identities.
- **Plan:** Once the adversaries have been identified, defenders can strategize what the best tactics and approaches may be to make the attackers go away.
- **Act:** This is the countermeasures execution phase.
- **Feedback:** The security team communicate daily or bi-daily the progress of Offensive Countermeasure missions with senior management. Further decisions are then made following the OODA Loop.

WHAT MAKES FINDING AND DISRUPTING ADVERSARIES A SUCCESSFUL APPROACH TO CYBER SECURITY?

The Offensive Countermeasures are made possible because attackers struggle to maintain the security of their own IT systems. They also tend to lack the discipline to follow strict operational security procedures that would keep them from

being identified over long periods of time.

Some of the cases we have monitored indicate that many adversaries brag about their hacking exploit to their friends, take shortcuts in their procedures, have falling out with their team members that then gave them up, and do not apply critical and high-risk security patches on their machines within 30 days!

For example, in 2013, journalist Brian Krebs used open source intelligence techniques to track-down and discover the identity of one of the top black-market salesman selling the credit card numbers stolen in Target USA's network that same year[3].

The following picture shows Andrew Hodirevski from Ukraine aka "Rescator":

Figure 10 - Andrew Hodirevski

Also, a security research project called "OnionScan" led security researcher Sarah Jamie Lewis to show that many illegal websites hosted in dark-web (TOR) were subject to basic infrastructure and application vulnerabilities[4] which could allow law enforcement and security teams to discover the real IP address of the websites or hack them.

CONCLUSION

In this article, we have presented the main categories of cyber threat actors and covered specific examples of individuals and groups behind major breaches.

We have demonstrated that adversaries do not give up and that they will hack their victim numerous times unless the defenders use Offensive Countermeasures to influence them, disrupt their operations, remove their political support, or get them arrested.

Compliance and framework based activities provide a false sense that reasonable steps are being taken to stop the attackers. When in reality they make companies invest the minimum effort possible to tick a box in a long list of criterion instead of investing in making sure that the adversaries stop their activities.

It is paramount that information security professionals come to the realization that traditional prevention, detection and response security activities must be augmented with Offensive Countermeasure activities if they ever want to stop the adversaries.

REFERENCES

[1] ABC News 2016 – Bureau of Meteorology hacked by foreign spies in massive malware attack, report shows
[2] Phineas Fisher's Hack Story: https://pastebin.com/raw/0SNSvyjJ
[3] Brian Krebs 2013 - Who's Selling Credit Cards from Target?
[4] Hackfest 2016 - Sarah Jamie Lewis presented "Untangling the Dark Web: Unmasking Onion Services"