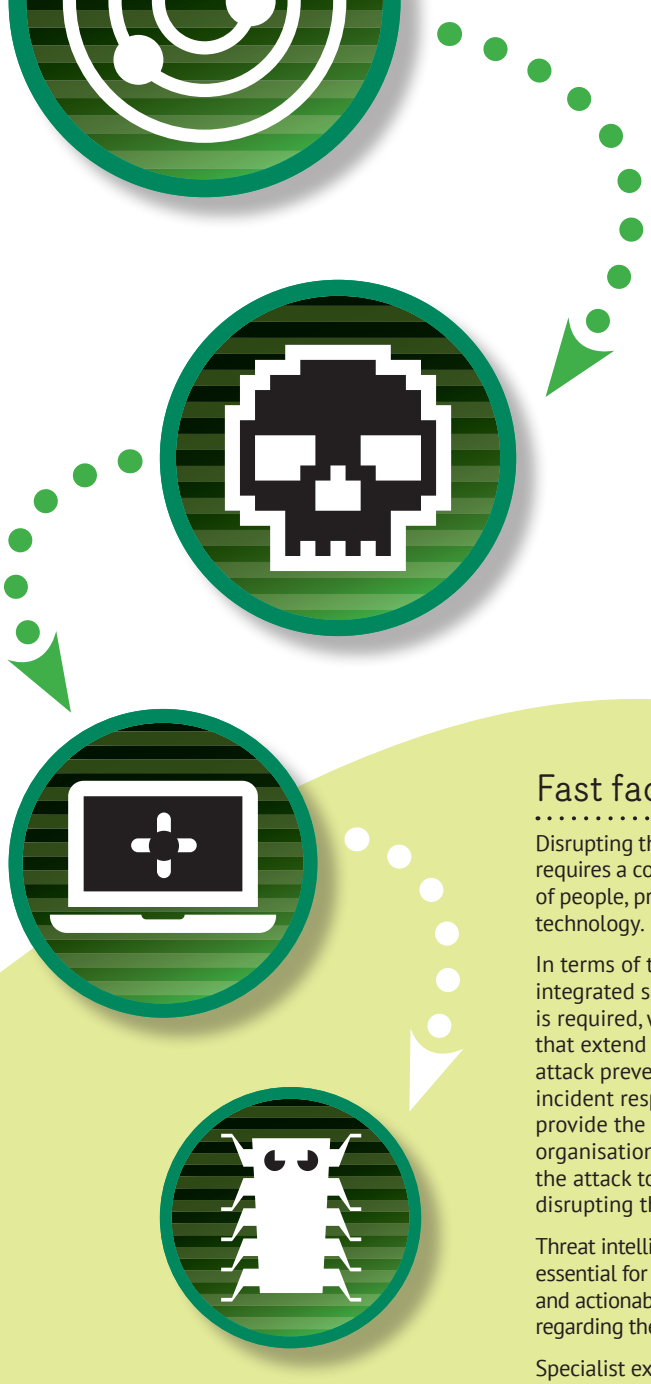
Turning the tables on cyber criminals

...using the cyber kill chain framework to protect your organisation

author • **Fran Howarth**



Executive summary

THE KILL CHAIN is a concept that has been borrowed from the military. It describes the phases that are involved in an attack. It came into use in the commercial sector in 2011 when Lockheed Martin coined the phrase "cyber kill chain" to describe the phases that are involved in any advanced targeted attack on computer networks. These are: reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and action.

Every phase of the kill chain provides an opportunity to disrupt attacker activity using a combination of people, processes and technology. The earlier that an attacker can be disrupted, the easier and quicker it is for an organisation to mitigate the threat and prevent serious interruption to their operations, as well as preventing the consequences and costs of a full-blown assault.

Any organisation, whatever its size or line of business, could be the target of an advanced attack. This document describes what options are available for disrupting attackers at each stage of the kill chain.

Fast facts

Disrupting the kill chain requires a combination of people, processes and technology.

In terms of technology, an integrated security platform is required, with capabilities that extend from initial attack prevention to eventual incident response. This will provide the visibility that organisations need throughout the attack to aid then in disrupting the kill chain.

Threat intelligence feeds are essential for providing insight and actionable intelligence regarding the latest threats seen.

Specialist expertise is necessary alongside technology to help organisations to be better able to disrupt the kill chain and to build up their resilience to attacks.

The bottom line

Today's threat landscape is increasingly insidious, with attacks increasingly targeted and harder to defend against. Yet attacks tend to follow similar patterns, with attackers needing to follow a fairly uniform series of steps in order for their attacks to be successful. This uniformity is increased by the use of commodity elements during attacks, such as off-the-shelf tools for installing malware on target systems or for the command and control infrastructure.

By understanding what those phases are and the options that are available to them for countering the attack at any of those phases organisations will be in a much better position to defend their networks and safeguard sensitive information.

The onus is on organisations to learn how to leverage the cyber kill chain framework to understand their risk posture and to assess any vulnerabilities within their security programmes. This will help them to remain vigilant and to prepare themselves as well as possible, taking into account the current threat landscape and how it is evolving. This requires the use of threat intelligence feeds as well as talking to peers and using the services of specialists. They should ensure that all employees are aware of security risks and their role in preventing themselves from falling victim.

Visibility is key to planning and executing and effective response. This means that end-to-end, integrated technology controls need to be in place, from the point of entry of the attack through the kill chain to the point where attackers look to achieve their objectives, which are often to steal sensitive and valuable information. Information regarding events seen at every stage in the kill chain and how they are connected with each other enables better decision making regarding actions to take, making incident response much easier.

The threat landscape worsening

CYBER SECURITY has been identified as the biggest common threat facing organisations and governments alike with a number of high-profile breaches having been seen against both corporate and public agencies. Apart from the disruption to operations that cyber attacks cause, any organisation can suffer brand, reputational and financial damage as a result.

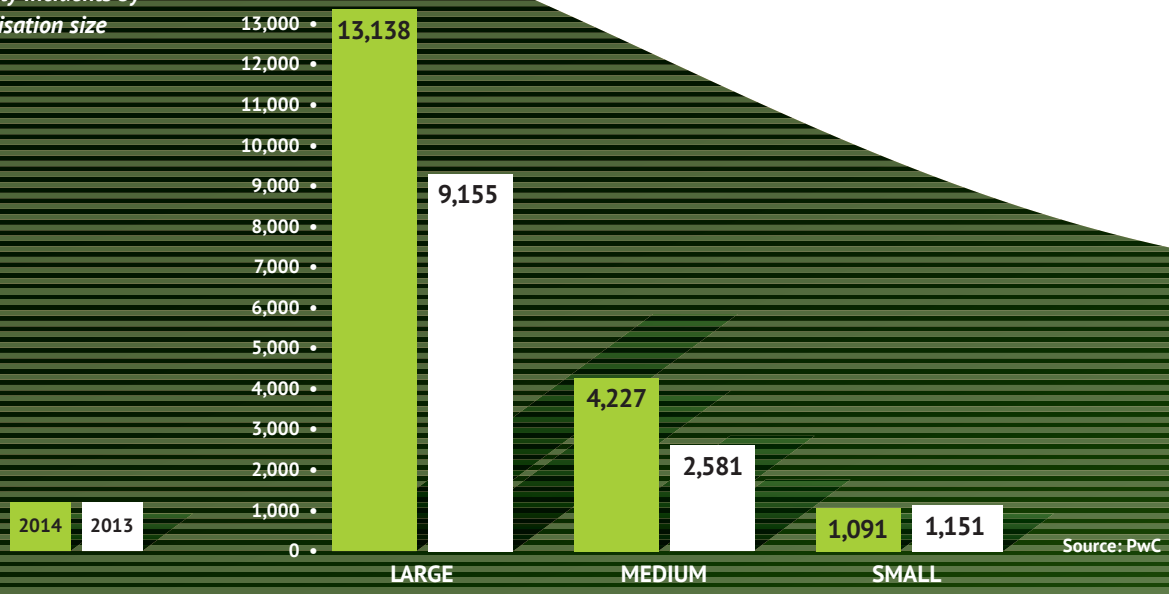
Organisations of any size can be a target, as seen in **Figure 1**, as smaller organisations are increasingly being seen as a conduit into larger organisations, and because medium and small organisations often do not have security practices that are on a par with larger organisations. But a cyber security attack can be disastrous for any organisation. The Ponemon Institute estimates that 90% of small businesses that have information stolen go out of business within three years.

Cyber security concerns are also increasing. A recent survey by Osterman Research found that more than 50% of organisations are becoming more focused on data breaches because of very well publicised and high-profile breaches seen recently, especially those targeting the retail sector. More than half of organisations, at 55%, indicate that detecting and preventing data breaches is among their highest priorities for 2015, with 9% stating it is their highest priority.

Cyber attacks are also becoming more sophisticated and harder to defend against. Whilst opportunistic attacks still occur, often deploying botnets for en masse attacks, targeted attacks are now the order of the day and are much harder to defend against. There are any number of shadowy figures involved in such attacks, from those with a grudge to bear who are looking to harm an organisation, often for ideological purposes, to organised criminal groups looking to steal information for competitive or financial gain, and nation states involved in espionage. Many such attackers are not only highly motivated, but they often have the resources available to them that rival those of a multinational.

The stakes are high and organisations have a lot to lose if attacks are successful. According to the Ponemon Institute, for 85% of organisations, preventing an attack is very difficult and a further 57% find attacks difficult to isolate, 56% to block and 46% to detect.

Figure 1: Security incidents by organisation size



The kill chain: how attackers work

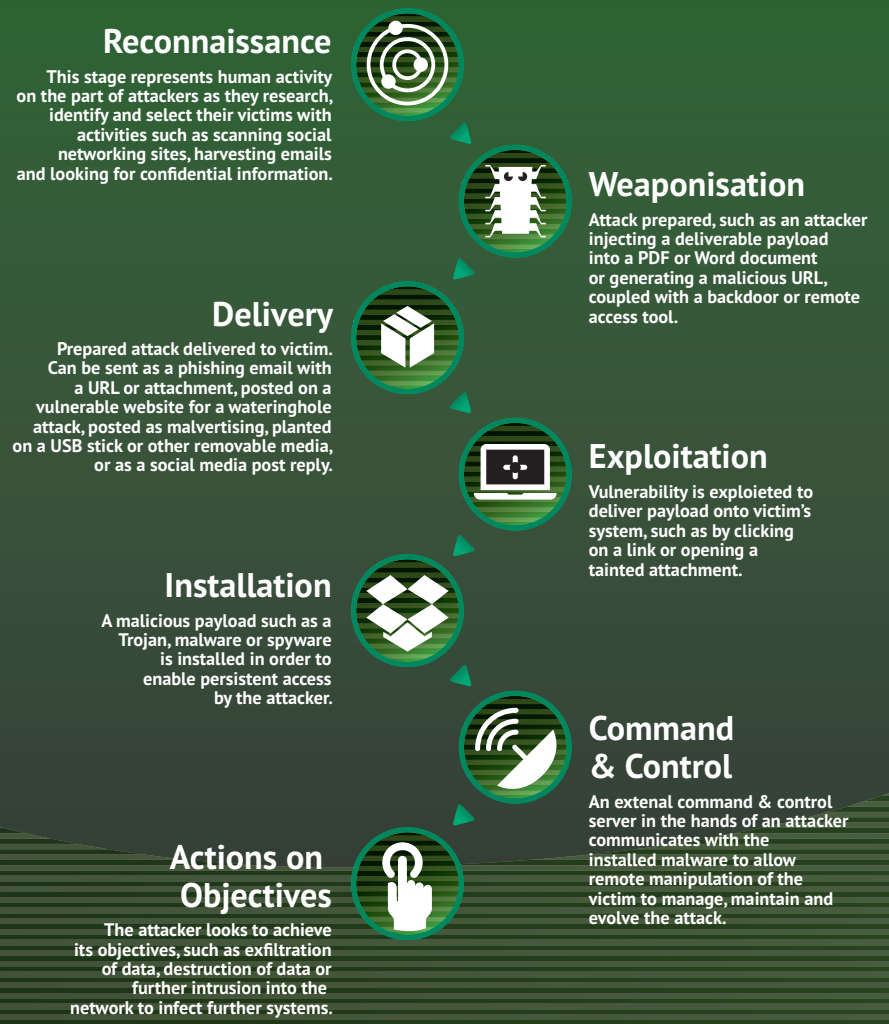
THE KILL CHAIN is a concept that was originally developed by the military to describe the structure of an attack and the phases that are followed. In a military setting, those phases are target identification, dispatch force to the target, taking the decision to attack and ordering the attack, and the eventual destruction of the target.

Another term that was coined by the military is advanced persistent threat, used to facilitate discussion of intrusions into civilian organisations without revealing classified information. It came into general parlance in 2010 when Google announced that it and some 30 other technology vendors, defence contractors and large enterprises had been the victim of a concerted targeted attack that used social engineering, targeted malware and monitoring technologies to seek out and exfiltrate reams of data of critical or high value to the victim organisations. Such attacks are often now referred to as advanced targeted attacks.

The term kill chain has also spilled over into commercial use. In 2011, defence contractor Lockheed Martin adapted the concept of the kill chain to information security. It describes the phases that adversaries go through in conducting advanced targeted attacks with the purpose of detecting and disrupting the attack at the earliest possible phase in the chain in order to limit the damage as far as possible.

The cyber kill chain is illustrated in **Figure 2**.

Figure 2: The cyber security kill chain



Source: Lockheed Martin

This cyber kill chain model serves both as a framework for understanding how criminals operate as well as a tool to defend against targeted attacks. According to the Ponemon Institute, it is a lifecycle approach that allows information security professionals to proactively remediate and mitigate advanced threats as part of the organisation's intelligence-driven defence process. In a recent survey that it undertook, 67% of respondents stated that they are familiar with the term. Among respondents, a full 84% of respondents indicated that the model was helpful is defending against cyber attacks, as shown in **Figure 3**.

One of the main benefits of the kill chain model is that it allows an organisation to understand an attacker's weak spots which, again according to Ponemon, is the most important feature of any security intelligence system for 72% of respondents, followed by neutralising an attack before it happens for 69%, and slowing down or halting the attacker's computers at 56%.

By using the kill chain model, organisations can turn the tables on attackers to disrupt their operations, prevent attacks and improve their overall security posture.

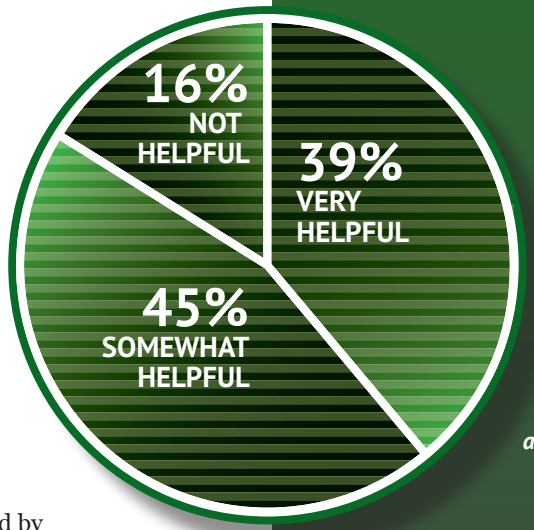


Figure 3: How helpful is the cyber kill chain for cyber security defences and strategy?

Source: Ponemon Institute

Using the kill chain to understand attackers

EACH OF THE STEPS in the kill chain can give visibility into what attackers are doing and what they are looking to achieve. Staging an attack can be expensive, leading some attackers to use cheaper alternatives at some stages.

For example, in order to improve success rates, they might invest heavily in purchasing zero-day exploits or in designing new weaponisation techniques, leaving them with less money for other phases of attack so that they might choose existing botnets for the delivery stage or a command and control channel that is already known about. This both improves an organisation's chances of detecting the attack and can allow it to work backwards through to the early stages of the attack to gain a better understanding of it and to ascertain whether it has been seen in other parts of the organisation. This will also help them to gauge whether the attack was a one-off or a sustained attack. But gaining that visibility requires a combination of people, processes and technology – albeit not all in equal measure at every phase in the chain. The approach taken may also vary depending on the size and maturity of the organisation since smaller companies likely have fewer human resources at their disposal.

Reconnaissance

The first phase of the kill chain – reconnaissance – involves human activity on the part of would-be attackers and is seemingly the most difficult to disrupt. However, there are a number of actions organisations can take to defend themselves at this stage:

- Firstly, they should look to limit the amount of information about the organisation and its employees that is publicly available. Employees should be educated in the dangers of posting corporate or too much personal information online, such as on social networking sites. Whilst this is not easy to control, it will increase the time and effort involved in targeting specific individuals. On the organisation's part, it should consider what information it publishes and should look to limit any that could make it a target. For example, it should ensure that employee contacts are not widely available, posting just those that are needed to corporate websites and perhaps ensuring that they are in a different format to those used for general employees to prevent email address guessing. Details about assets such as web servers and physical locations should also be limited where possible in order to narrow down the list of targets that attackers could exploit.
- The use of threat intelligence can also help at this stage to build a picture of possible threat actors and their favoured tools, techniques and procedures. Such intelligence feeds can help to pinpoint command and control servers that have been identified, spam that is seen in the wild, the reputation of IP addresses and email senders in terms of who is hosting malware and the historical behaviour of attackers. This will help organisations to build out a clearer understanding of the threats that they face and where attacks could potentially come from.

> "Email has become almost ubiquitous. Organisations would be shut down without email, so it has become the main channel of attack."
>
> **Andy Herrington,** Fujitsu

Using the kill chain to understand attackers ctd.

Weaponisation and delivery

The weaponisation phase is one that organisations perhaps influence the least, since this is when the attacker is preparing their attack by infecting payloads, generally into documents, and generally those that organisations use the most for business records and communications, such as Word and PDF. However, many exploits use vulnerabilities in document formats that have already been discovered and for which patches are available. A good practice is to ensure that all such patches have been applied. Once weaponisation has taken place, attackers will look to deliver their attacks to the intended victims, relying on emails in the vast majority of cases. It is estimated by Verizon Business in its 2015 data breach investigations report that 95% of all advanced targeted attacks attributed to state-sponsored actors and two-thirds of cyber espionage attacks use phishing emails as the delivery mechanism. It estimates the overall success rates of phishing campaigns as being from 10% to 20%. Organisations of all types are being targeted with phishing campaigns, but the proportion of small and medium organisations is increasing.

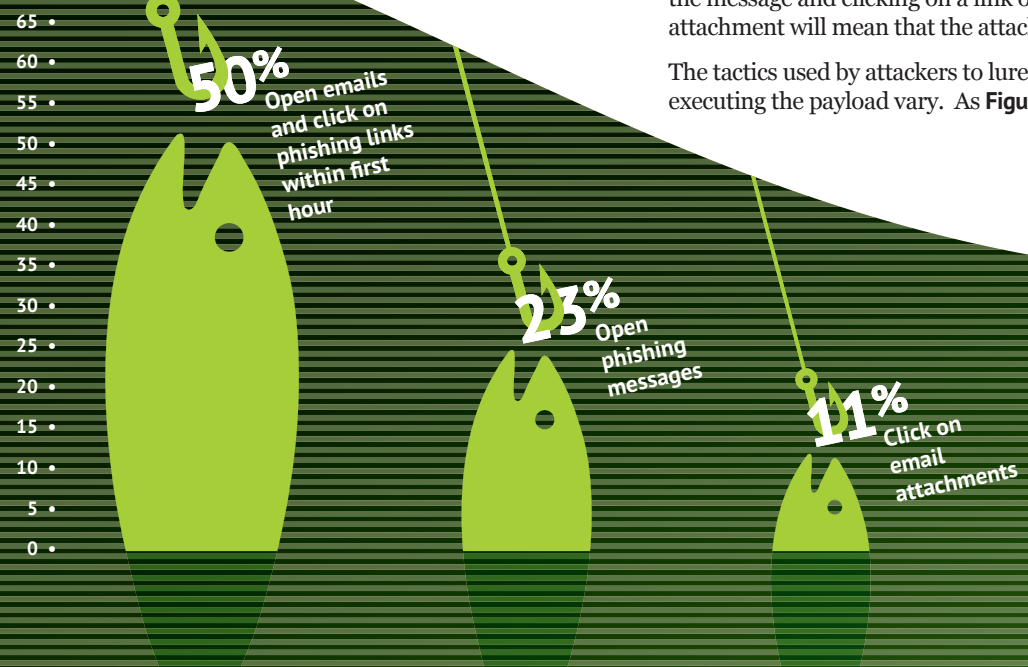
Exploitation and installation

Once the weaponised message has been delivered to the intended victim, the attackers must rely on the recipient to take action in order for the payload to execute. As **Figure 4** shows, almost a quarter of recipients of phishing messages still open them, showing that such campaigns are often successful. In a sustained attack where a number of people in an organisation are targeted, just one person opening the message and clicking on a link or opening an attachment will mean that the attack is successful.

The tactics used by attackers to lure recipients into executing the payload vary. As **Figure 5** shows, sometimes malicious URLs that take users to compromised websites tainted with malware are favoured, often using subject matter likely to interest the recipient of the message. The use of URLs is attractive to attackers as they can send a user a URL link that is benign at the time that it is sent in order to defeat defence, but that turns malicious after that investigation. URLs can also be tainted with exploit kits, which can be used to tailor attacks to specific environments encountered.

In late 2014, the use of weaponised attachments saw a large spike that is continuing. This spike has been caused by the use of malicious macro code in attachments that execute their payloads once a recipient clicks the "Enable content" button. According to Proofpoint, the attractiveness of using tainted macros is that their use has low upfront and maintenance costs compared to other methods of attack, delivering the greatest return on investment. They are also highly successful at evading both traditional defences based on signatures and reputation, with initial detection rates by such controls consistently being 5% or less, and they are also able to evade newer behavioural sandboxes. They can also deliver exploits that are not tied to any specific operating system or application.

Figure 4: Response of recipients to phishing emails



Source: Verizon Business data breach investigations report 2015

The Dridex malware macro

The Dridex malware strain is a banking Trojan developed to disrupt and gain financially from financial transaction systems and to commit fraud. It has been deployed in email phishing campaigns. The attack starts with a well-formed email with an attachment tainted with the Dridex macro, purportedly from an institution such as a bank and is polymorphic, so is difficult both to detect and respond to. According to Andy Herrington, head of cyber professional services at Fujitsu, campaigns using Dridex are being seen on an industrial scale, with around 180 million email addresses having been targeted. Once a computer has been affected, Dridex collects bank account and other personal information in order to gain access to the financial information of the affected individual. The best ways to counter Dridex are to use sandbox-based breach detection technology and to disable macros.

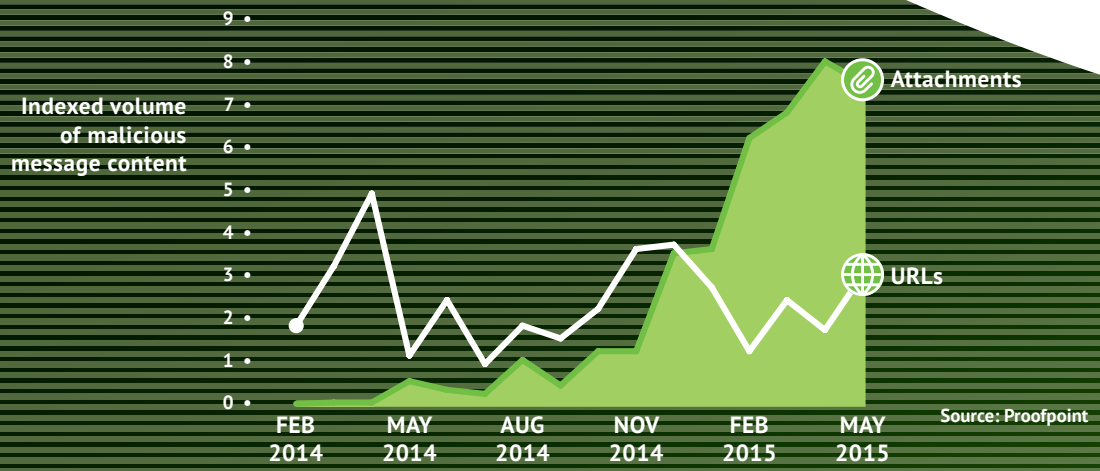
To guard against the damage that can be caused by malicious emails, organisations should deploy a combination of human effort and technology.

In terms of technology, organisations should deploy technology that looks for advanced weaponised mails and attachments at the gateway as emails come into the organisation. Any that are suspected as being malicious should then be sent to a sandbox for further investigation. Organisations should look for advanced sandbox technology that can even deal with exploits that include extra layers of obfuscation to avoid detection by regular sandboxes. Where a malicious or suspicious URL is encountered, the technology should be capable of rewriting the URL and sending all traffic resulting from users clicking on the URL to a separate server for checking. All URLs should be inspected at the time when they are clicked, rather than merely relying on reputation, with advanced sandboxing techniques used that undertake full dynamic behavioural analysis. Only then can an organisation be sure that malicious URLs are correctly identified. This is especially important since some URLs that are benign when initially sent to a recipient are then subsequently weaponised, turning bad just a few minutes before the user clicks on them.

Threat intelligence is also important, both for alerting to new threats as they are seen and for inputting new information regarding malware strains and their behaviour into the database as they are seen. Such information feeds are key for protection and detection systems as they provide access to the latest threats seen, allowing for decisions to be made in real time based on the latest information.

But technology in itself is not sufficient. According to the Enterprise Strategy Group, of the reasons given for the success of targeted attacks, lack of user knowledge about security risks, leading to actions such as users clicking on unknown links or opening emails from unknown sources, was the top risk cited, at 38% of respondents. This makes user security awareness training essential, conducted at regular periods to reinforce messages.

Figure 5:
Malicious message trends



Source: Proofpoint

Using the kill chain to understand attackers ctd.

Command & control and actions on objective

The command & control phase of the kill chain is where attackers establish a command channel for remote manipulation of the victim's system – so-called 'hands-on access'. This is the first point in the kill chain at which attackers have a direct interface with the systems that they have infected. Among the methods used are remote access Trojans and rootkits. Tools such as these enable attackers to steal data by exfiltrating it to a remote command & control server under their management, or to perform other acts such as altering or destroying data.

In order to reduce the time taken for remediation, it is important to use technology to monitor all activity in order to root out any malicious activity that has got past defences and has moved laterally across the network. In particular, it is important to monitor for and find any communications channels that have been set up to allow an attacker to move data out of the network. By detecting such channels, controls such as firewalls can be instructed to block the activity or to contain it – an activity that can prevent the attacker from realising that their deeds have been uncovered. This is especially important for reducing the time taken to remediate threats and to prevent data from being leaked out of the organisation. Threat intelligence feeds should also be monitored at this stage since they will provide information about command and control servers that have already been found through reputation services so that outbound communications to them can be blocked.

DLP controls are also useful for preventing sensitive information from being exfiltrated by continuously monitoring internal data flows to see where attackers are farming internal systems for data and pulling it back to a staging server ready to be encrypted and packaged for exfiltration.

Figure 6 illustrates what is involved in terms of technology and processes for disrupting the kill chain.

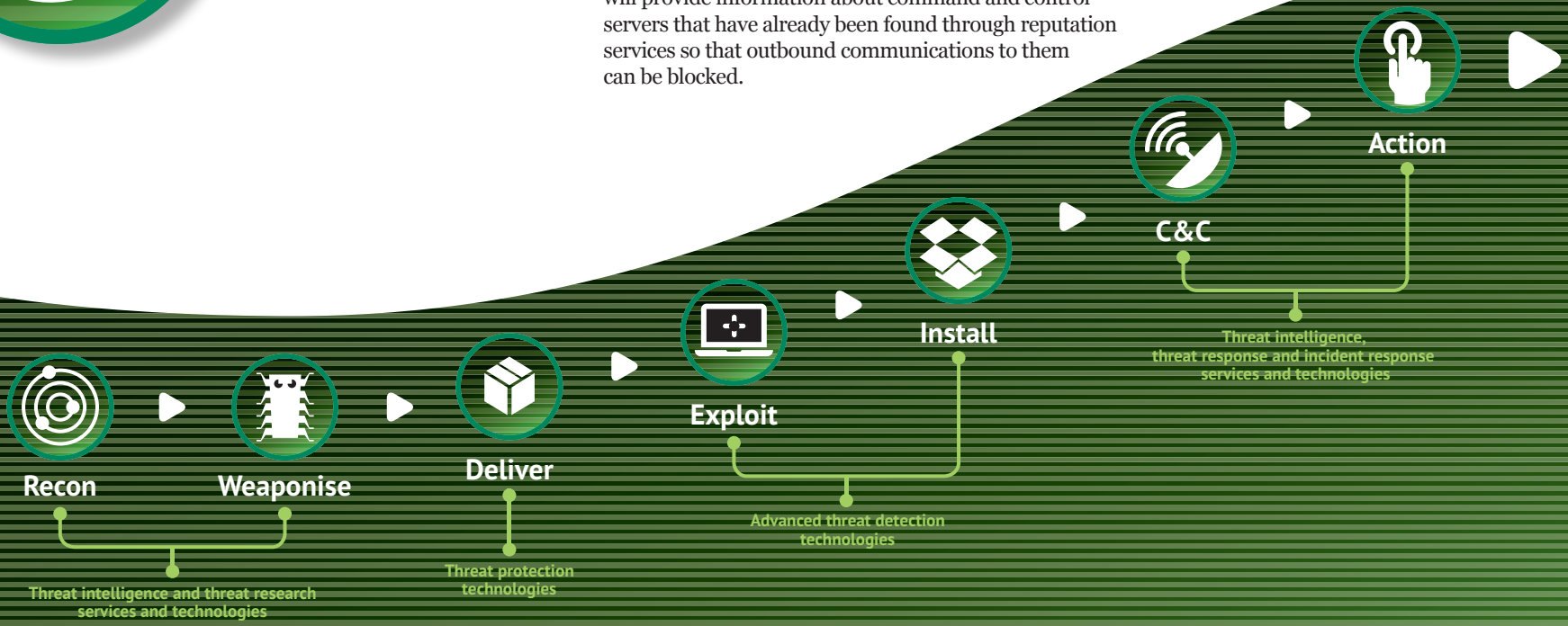


Figure 6: Mapping controls to the Kill Chain

The need to integrate threat protection and incident response

Integration between threat detection and incident response is critical for stopping advanced targeted attacks and for defeating the kill chain. Only through tight integration are organisations afforded the visibility across all security data that they need in order to take informed decisions regarding incident response.

According to Richard Davis, field product and solutions manager EMEA for Proofpoint, this requires a platform with integrated capabilities right through the kill chain, from the point of entry to incident response. The system should look to detect threats when emails, attachments and other messages, such as social media messages, enter the gateway of the network, looking for those that have potentially been weaponised. These should then be passed to a sandbox, where they are opened and behaviour observed, such as whether it is attempting to download malware, contains a malicious URL, or exhibits suspect behaviour in the macro or code. The sandbox should be capable of observing malicious behaviour even in payloads that use extra layers of obfuscation in order to defeat basic sandboxes.

To guard against even the most recent, previously unseen threats, the platform should have threat intelligence capabilities integrated with it in order to provide actionable intelligence regarding what threats the organisation faces, combined with multiple suggested responses in order to aid in timely actions to prevent data exfiltration and lateral movement of malware through the network by providing the necessary context regarding what the threat is attempting to do. Contextual factors provided by threat intelligence include attacker details, threat type, sandbox analysis results, reputation data and visibility as to who in the organisation is being targeted. It should also provide intelligence regarding command and control infrastructure seen worldwide. The platform should provide detailed forensics, including indicators of compromise and information on the tools, techniques and procedures used in a specific attack, showing the progression through the kill chain, from initial payload delivery through to malware execution and intelligence on the command and control infrastructure used by the threat action. This information then enables algorithms to be developed that look for further evidence of security incidents and hidden threats so that appropriate countermeasures can be selected in order to respond to an incident, such as containing the threat or preventing data exfiltration.

The human factor

Technology has a large part to play in disrupting the kill chain, but it is not always by itself sufficient. There are several points along the kill chain where humans often need to be involved. According to Andy Herrington, head of cyber professional services at Fujitsu, the use of advisory services can aid organisations in disrupting the attack chain at the earliest possible point in order to limit potential damage.

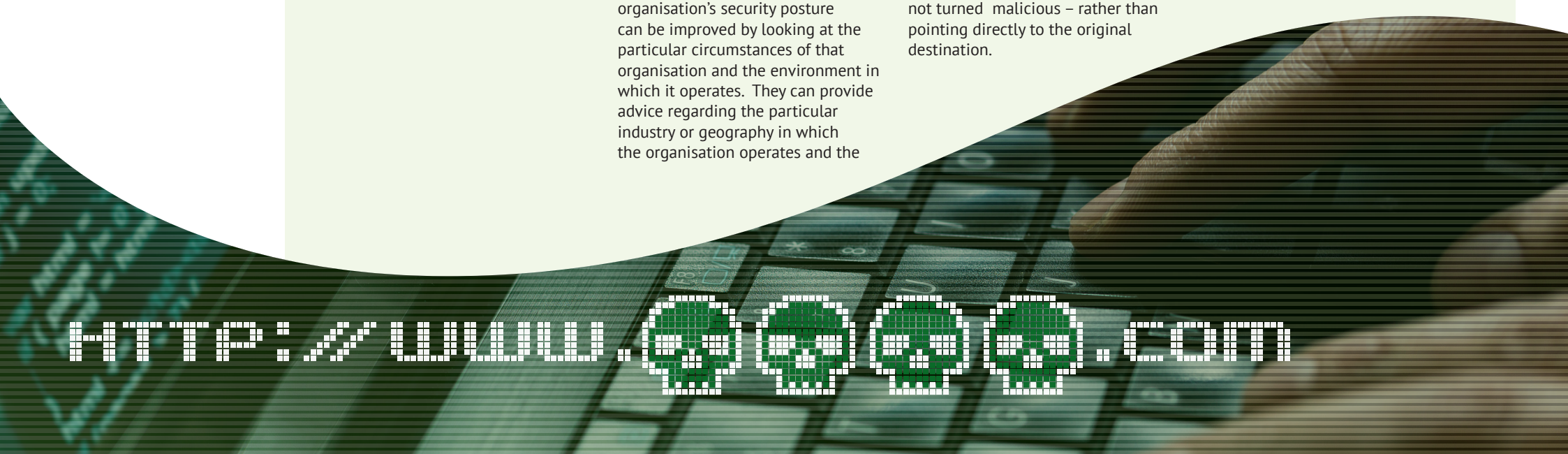
Consultants can look at a particular organisation's network in order to help develop the best strategy for disrupting the kill chain, ensuring that the organisation has the technology and capabilities in place that are most likely to stop attackers in their tracks – even where they are using advanced capabilities that look to defeat defences. Herrington gives the example of the Dridex worm, the payload of which is changed on a daily basis. To deal with this, threat intelligence experts scour the dark net for intelligence, which can then be fed back into monitoring capabilities in order to beef up defences. In this way, such services can add extra value by combining the necessary capabilities of people, processes and technology.

By adding the human factor, an organisation's security posture can be improved by looking at the particular circumstances of that organisation and the environment in which it operates. They can provide advice regarding the particular industry or geography in which the organisation operates and the threats that are being seen that are specific to those circumstances so that response capabilities can be better tailored to the particular need. In this way, the costs associated with incident response can be reduced as threats can be prevented from escalating at an earlier stage, saving time and money associated with the clear up.

Another area in which using external advisors can help is in situations where a potential threat is not initially caught. For example, an email may be received by an organisation with a URL link in it that is not malicious at the point the email is received, but is later weaponised. Technology can help by rewriting the URL and ensuring that it passes through a service when clicked to ensure that it has not turned malicious – rather than pointing directly to the original destination.

Should the URL be deemed to have been weaponised, the information can be sent through to the threat intelligence platform along with a notification alert for further investigation into the potential threat so that countermeasures can be developed to defeat it.

One further area requiring the human factor is in following up with users and raising awareness of threats. For example, consultants can investigate which users are being targeted the most or which are more likely to click on tainted links of open attachments. Those users can then be singled out to receive further training in order to make sure they are better prepared and understand the overall risks.



Summary

THE CURRENT MANTRA IS *"it is not if, but when and how often"* an organisation will suffer a security breach. None can afford to be complacent. The kill chain is a framework that any organisation can use to its advantage in order to turn the tables on attackers and disrupt their activity. The earlier that an attack can be disrupted, the easier it is to stop the attack's progress and to limit the damage caused. This requires a combination of people, process and technology, each of which is of varying importance at different phases of the attack chain.

As a start, organisations can use the kill chain framework to aid in risk assessments to uncover risks and vulnerabilities concerning people, processes and technology, using it as a benchmark to understand the risks that are faced. In terms of technology, organisations need to ensure that they have adequate controls in place throughout the kill chain cycle, right through from trying to protect themselves from threats entering the network to preventing the attacker from achieving their objectives. In terms of processes, organisations should have plans in place with clearly defined processes, especially regarding the response process, which should be tested and reviewed regularly. Where people are concerned, it is essential that all employees are trained so that they are aware of the dangers that the organisation faces and their role in maintaining a secure posture. Cyber drills are an effective way of ensuring that messages are getting through.

In all these areas, it is useful for organisations to talk to their peers to share information and experiences, especially those in similar lines of business or a particular region. This will help to gain a better understanding of the threats faced in order to better hone response capabilities. Vigilance and visibility are key in order to be able to understand the threat landscape and what it means for a particular organisation and to join up the dots from the evidence that is provided by security controls across the network.

2nd Floor
145–157 St John Street
LONDON EC1V 4PY
United Kingdom

Tel: +44 (0)207 043 9750
Web: www.Bloor.eu
email: info@Bloor.eu

July 2015