panda

Understanding Cyber-Attacks

Part I. The Cyber-Kill Chain.

Adaptive Defense

pandasecurity.com/intelligence-platform/

Table of Contents.

1. Introduction.

The changing threat landscape reality and the frequency, sophistication and targeted nature of adversaries requires an evolution of security operational practices to a combination of **prevention, detection and response of cyberattacks**.

Most organizations have the means to detect known attacks, although a few of these can still occur. What has been historically difficult is stopping unknown attacks, which are specifically tailored to get around the latest protections by changing signatures and patterns of behavior.

Many organizations have made significant investments in creating their own threat hunting team and/or in delegating to Managed Service Providers the inevitable and critical task of continuously evolving their defensive techniques and search for better tools and ways to keep their intellectual property and digital assets secure.

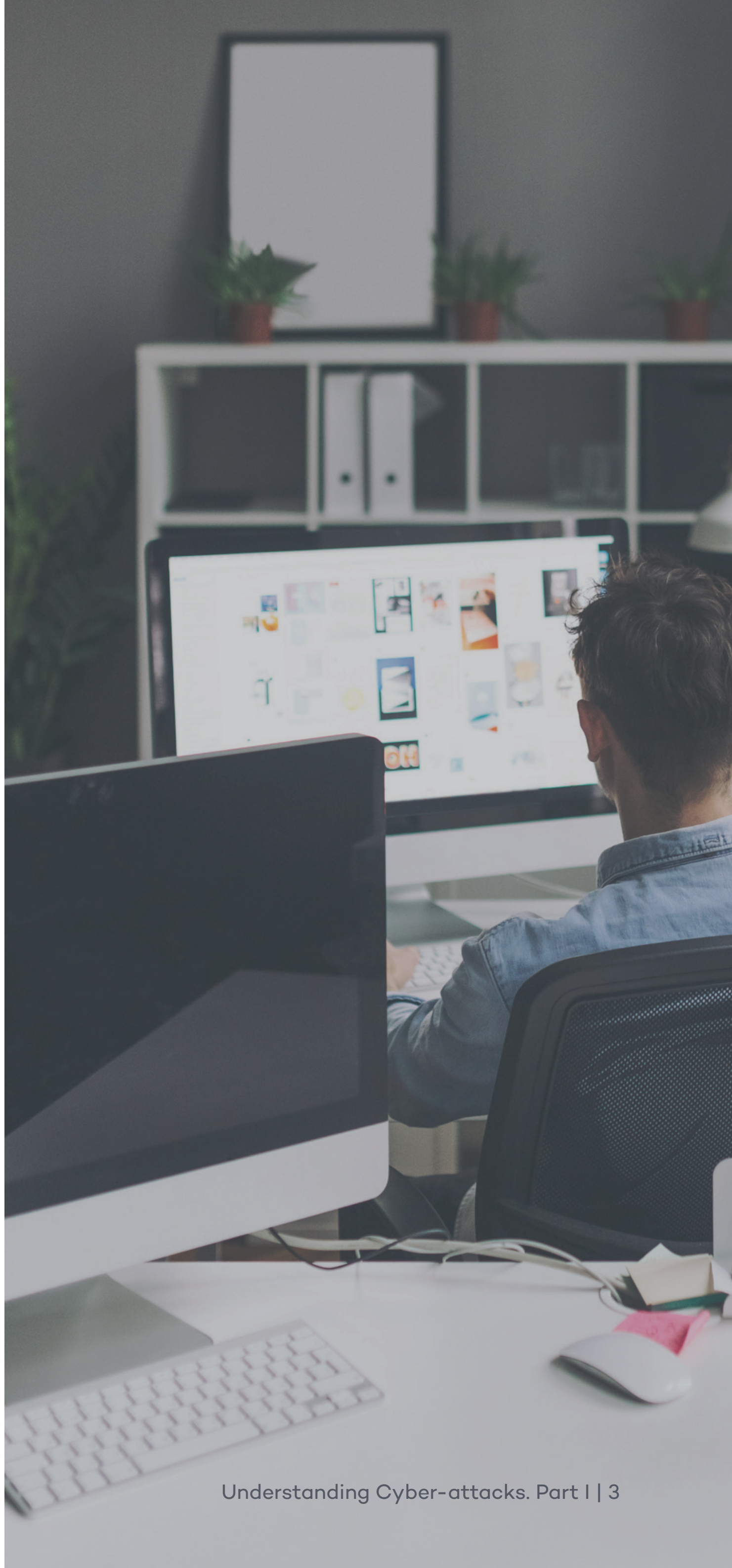
The understanding of how these adversaries work and the map of the organization's defense strategy to their lifecycle shows how they can detect, stop, disrupt and recover from an attack and where their security operations need to be reinforced.

This report helps security teams understand the well-known cyberattack lifecycle model called the Cyber-Kill Chain (CKC) and its extension to the entire network and how Panda Adaptive Defense Service cover the whole lifecycle at the endpoint level.

This Cyber-Kill Chain, and its extension to the whole network, is an excellent tool to understand how organizations can significantly increase the defensibility of their environment by catching and stopping threats at each phase of the attacks' lifecycle. The Kill Chain teaches us that while adversaries must completely progress through all phases for success, we "just" need to stop the chain at any step in the process to break the attack.

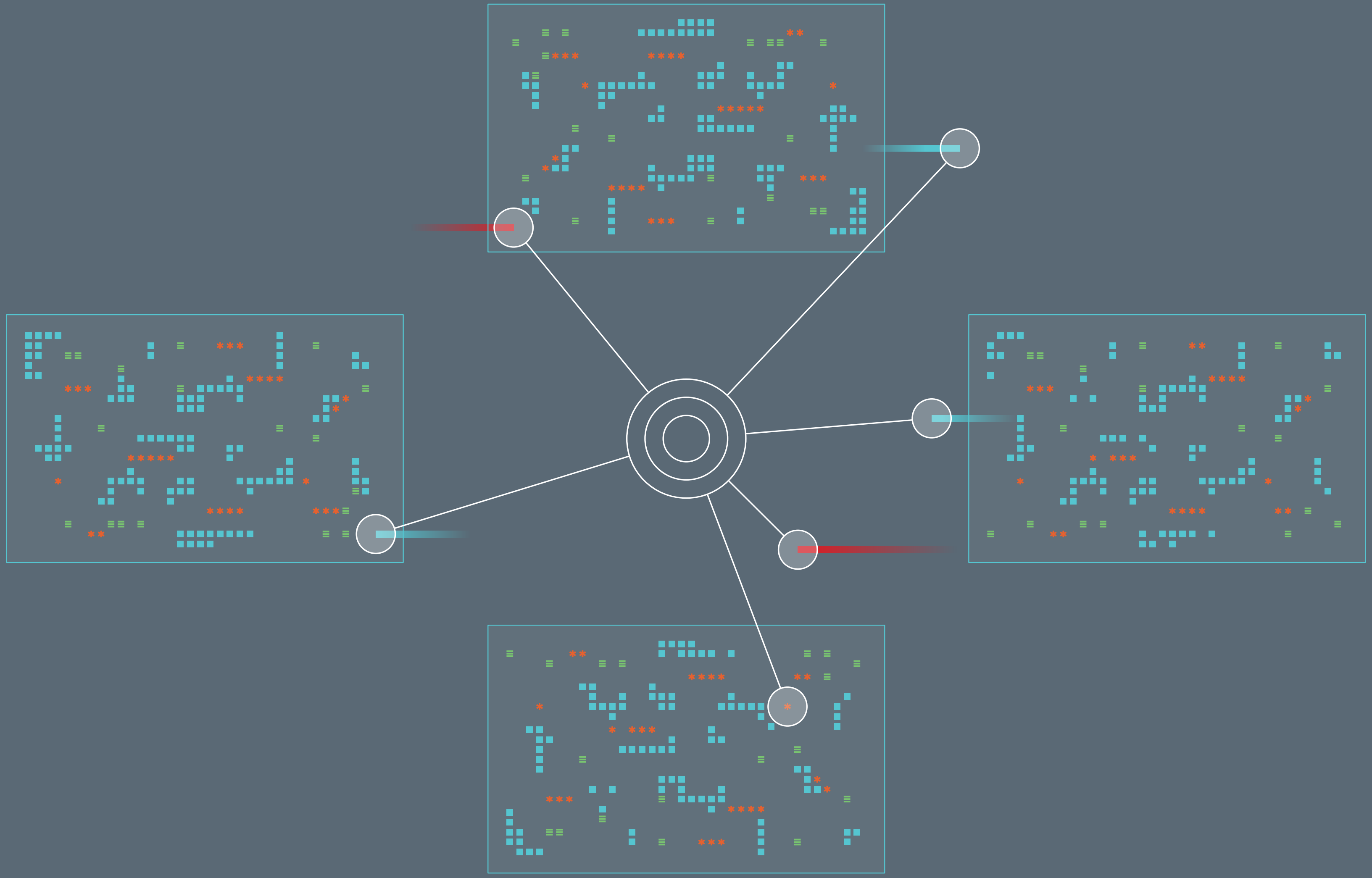
Keep in mind that the most valuable assets of an organization, and sometimes uncontrolled, are stored at the endpoints and servers. Therefore all the attackers will want to reach them to gain access to these critical assets, Stopping adversaries at the endpoint drastically reduces the likelihood of success of any cyber-attacker, simplifying efforts to break the chain and significantly increasing the efficiency and effectiveness of security equipment.

As all attackers hit the endpoints to gain access to the organizations critical assets, stopping adversaries at endpoint level automatically decreases the probability of success of any cyber attacker, while simplifying the efforts to break the chain and significantly increases the efficiency and effectiveness of the security operations.



Panda Adaptive Defense Service helps all these organizations and their internal or external Security operation teams improve their ability to **prevent, detect and respond to threats by addressing them across the whole cyber-attack lifecycle** whenever they hit the endpoint.

Beside it **Managed Service** provides threat data and threat Intelligence to them to know their adversaries and improve their defenses.



2. Understanding the Cyber-Kill Chain.

The Cyber Kill-Chain framework, was originally published by Lockheed Martin as part of the Intelligence Driven Defense model[1] for the identification and prevention of cyber intrusions activity.

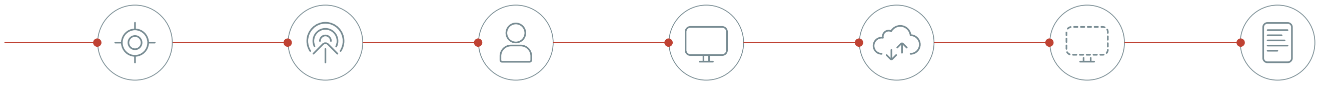
The model identifies what the adversaries must complete in order to achieve their objective, by targeting the network, exfiltration data and maintaining persistence in the organization.

Thanks to this model we learned that stopping adversaries at any stage breaks the chain of attack. Adversaries must completely progress through all phases for success. We, the defenders, just need to block them at any stage for success.

We will see in the next section that the endpoint is an inevitable point where all attacks go through and therefore stopping them at this level enormously increases the chance in breaking any cyber-attack. The rate of success will be greater if they are stopped at early stages in the chain.

Besides, every intrusion, and the trails that it leaves at the endpoint, is a chance to understand more about our adversaries and use their persistence to our advantage. **A better understanding of adversaries and their trails allows for a more effective design of defenses**.

The Cyber-Kill Chain states that to carry out their misdeeds, adversaries must always follow six basic steps:



External Reconnaissance

This stage can be defined as the phase of target selection, identification of organization details, industry-vertical-legislative requirements, information on technology choices, social network activity or mailing lists.

The adversary is essentially looking to answer these questions: “Which attack methods will work with the highest degree of success?” and of those, “Which are the easiest to execute in terms of our investment of resources?”

Weaponization and Packaging

This takes many forms: Web application exploitation, off-the-shelf or custom malware (downloaded for reuse or purchased), compound document vulnerabilities (delivered in PDF, Office or other document formats) or watering hole attacks[2].

These are generally prepared with opportunistic or very specific intelligence on a target.

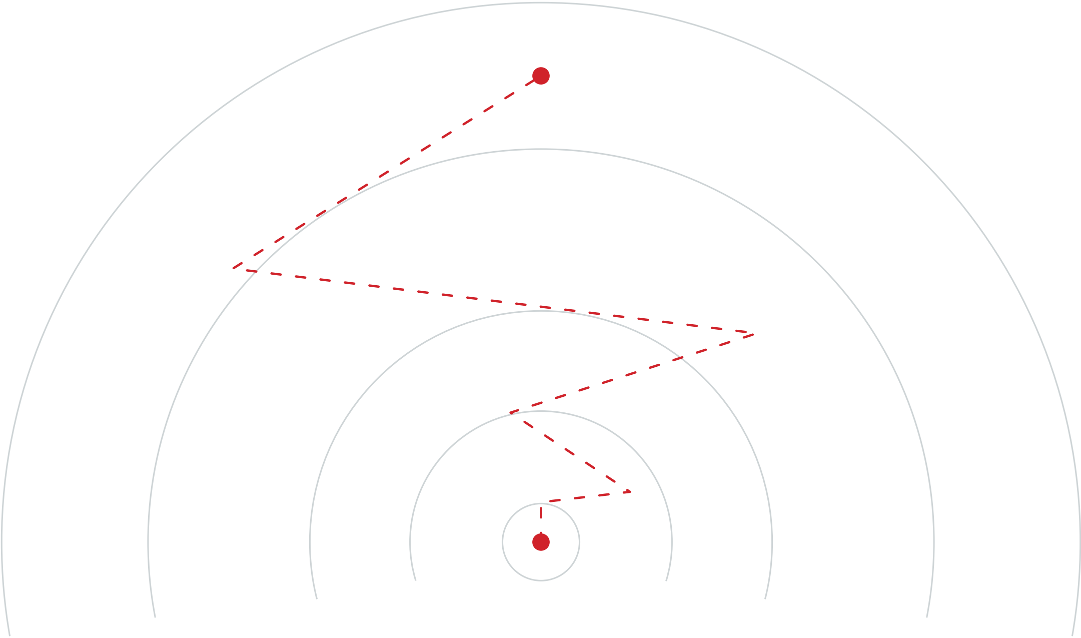
Delivery

Transmission of the payload is either target-initiated (for example, a user browses to a malicious Web presence, leading to an exploit delivering malware, or they open a malicious PDF file) or attacker-initiated (SQL injection or network service compromise).

Exploitation

After delivery to the user, computer or device, the malicious payload will compromise the asset, thereby gaining a foothold in the environment.

This is usually by exploiting a known vulnerability for which a patch has been made previously available. While zero-day exploitation does occur, depending of the victim, in a majority of cases it is not necessary for adversaries to go to this expense.



Installation

This often takes the form of something that communicates actively with external parties. The malware is usually stealthy in its operation, gaining persistence at the endpoints where it has able to access. The adversary can then control this application without alerting the organization.

Command and Control

In this phase, adversaries have control of assets within the target organization through methods of control (often remote), such as DNS, Internet Control Message Protocol (ICMP), websites and social networks. This channel is how the adversary tells the controlled "asset" what to do next and what information to gather.

The methods used to gather data under command include screen captures, key stroke monitoring, password cracking, network monitoring for credentials, gathering of sensitive content and documents. Often a staging host is identified to which all internal data is copied, then compressed and/or encrypted and made ready for exfiltration.

Actions on Targets

This final phase covers how the adversary exfiltrates data and/or damages IT assets while concurrently dwell time in an organization. Then measures are taken to identify more targets, expand their footprint within an organization and -most critical of all- exfiltrate data.

The CKC is then repeated. In fact, a critical point with the CKC is that it is circular, and not linear. Once an adversary enters in the network, he starts again with the CKC in the network, with doing more reconnaissance and making lateral movement inside of your network.

In addition, it is necessary to keep in mind that while the methodology is the same, adversaries will use different methods for steps of the internal kill chain once inside, versus being outside the environment.

In fact, once the attacker is inside the network, it becomes an insider, a user with privileges and persistence, and this prevents the organization's security teams from suspecting the attack and realizing that it is already in the advanced stages of the extended model of the Cyber-Kill Chain.

External Cyber-Kill Chain

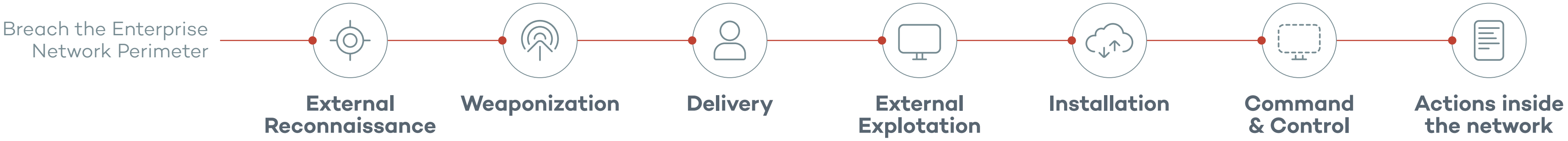


Figure 1. Diagram of the Stages in the Cyber-Kill Chain from Perimeter to the Endpoint. The Extern Cyber-Kill Chain.

3. The Extended version of the Cyber-Kill Chain.

The Cyber-Kill Chain is a circular and non-linear process, where the attacker makes continuous lateral movement inside the network. The stages that run within the network, are the same as those used when the goal was to access the network although using different techniques and tactics.

The combination of the External and Internal Cyber-Kill Chain in the industry is called, the Extended Cyber-Kill Chain. That means adding more steps, which are actually the same set, only preceded by the word internal, so the Cyber-Kill Chain becomes the Internal Cyber-Kill Chain with its own stages, internal reconnaissance, internal weaponization and so forth.

Each of the attack phases once inside a victim's network can take anywhere from minutes to months, including a final wait time when an attack is in place and ready to go.

Note that the attacker will hold off for the optimal time to launch in order to get the most impact.

The reconnaissance and weaponization phases can take months.

It is difficult to interrupt these phases as they are carried out without connecting with the attacker. This is why it is of vital importance that the security measures at the endpoints analyze and supervise all the systems and applications that run in the devices. It will significantly hinder the work of the attackers, and the attack will become not profitable for them.

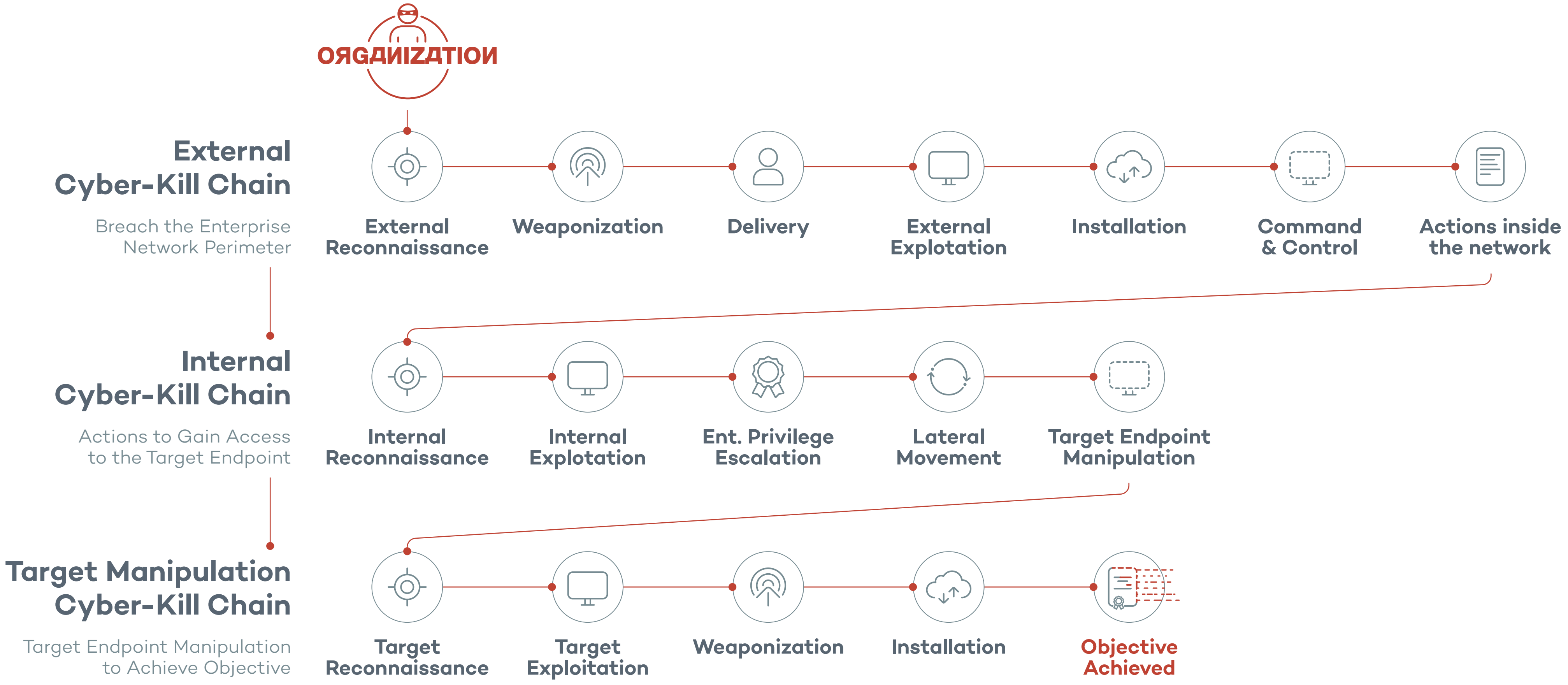
Internal Reconnaissance

In this stage, adversaries have access to a single user's workstation and will datamine it for local files, network shares, browser history, and access to wikis and SharePoint. The objective is to figure out how that machine might help map the network and enable moving to more valuable assets.

Internal Exploitation

By taking advantage of missing patches, web application vulnerabilities, broadcast protocols, spoofing or even something as simple as default credentials, that allow attackers to go from workstations to servers using **privilege escalation, lateral movement within the network and manipulating individual targeted machines**.

Figure 2. The Extended Cyber-Kill Chain. Actions to gain access to the target endpoint and endpoint manipulation to achieve attacker's objective.


ORGANIZATION
External Cyber-Kill Chain
Breach the Enterprise Network Perimeter
External Reconnaissance
Weaponization
Delivery
External Explotation
Installation
Command & Control
Actions inside the network
Internal Cyber-Kill Chain
Actions to Gain Access to the Target Endpoint
Internal Reconnaissance
Internal Explotation
Ent. Privilege Escalation
Lateral Movement
Target Endpoint Manipulation
Target Manipulation Cyber-Kill Chain
Target Endpoint Manipulation to Achieve Objective
Target Reconnaissance
Target Exploitation
Weaponization
Installation
Objective Achieved

4. Panda Adaptive Defense at the Cyber-Kill Chain.

Attackers have goals and are willing to expend a certain amount of resources to achieve them. If endpoint security mechanisms can boost the cost – whether monetary, personnel or time – above the value the attackers expect to reap, then they will succeed less often or even decide not to attack that organization.

Panda Security's mission is that it happens always in our customers, and, in light of the results, this is exactly the outcome of being protected with Panda Adaptive Defense.

All organizations have to be ready to ask what it would do if the adversary has access to the internal corporate network, usernames and passwords, all documentation and specifications of the network devices, systems, backups and applications and respond immediately.

Organizations' assets and endpoint security strategy's larger goal should be to build a more resilient enterprise. It won't prevent all attacks, but it will stop more and in earlier stages. One of the objectives is to have efficient defense mechanisms of the extended Cyber-Kill Chain in order to slow down attackers, make it more and more expensive to continue and make it as difficult as possible to move them to each subsequent stage.

If adversaries can't achieve their objective in a way that makes economic sense, they will go after different objectives or after similar objectives with a different Target organization.

Organizations' security strategy has to takes into consideration how an attack is executed, from outside and especially from inside, since attackers once in the network, are insiders with access to endpoints and their assets.

The traditional security approach should be extended with methods based on an understanding of the Cyber-Kill Chain and providing technologies that are able to avoid the attackers gaining access to the endpoints but also to stop them at any possible stage during the Internal Cyber-Kill Chain.

Mapping the defense strategy to the extended CKC model shows how the organization can prevent, detect, disrupt and recover throughout attacks' phases, aligning organization's security to the same success criteria as those of adversaries.

This is difficult to achieve due to a number of factors: applications have increased both in complexity and interconnectedness, applications are vulnerable because most software isn't developed using security principles and people. Employees and partners also remain a main risk vector and an open door to attacks based on social engineering.

Panda Adaptive Defense and Panda Adaptive Defense 360 addresses core pillars that, delivered in the form of a **managed service, prevent and detect the most advanced attack technics and tactics at every stage of the extended Cyber-Kill Chain**. It helps organizations' security teams design a security strategy aligned to the extended Cyber-Kill Chain.

5. Adaptive Defense and Adaptive Defense 360 core pillars.

Known Malware Prevention

Looking for known threats won't protect against variants or unknown attacks, but extending it with additional security layers can preventively stop known threats when they are being delivered into the endpoint. Panda Adaptive Defense 360 uses a vast collection of reputation services to proactively block attackers during the delivery stage using data from the cloud.

Advanced Malware Detection

Panda Adaptive Defense and Panda Adaptive Defense 360 detect and block unknown malware and targeted attacks, thanks to a security model based on three principles: continuous in depth monitoring of all applications running in the endpoints, automatic classification of endpoints' processes using big data and machine learning techniques in a cloud-based platform, and the possibility, should a process not be automatically classified, of an expert technician analyzing the behavior in depth.

Dynamic Exploit Detection[3]

During exploitation stage of the extended Cyber-Kill Chain, attackers use exploits to target code-level vulnerabilities so they can breach applications and systems, install and execute malware. Internet downloads are a common vector for carrying out exploit attacks. Panda Adaptive Defense and Panda Adaptive Defense 360 provide dynamic anti-exploit capabilities to protect against both application and memory- based attacks.

Panda Adaptive Defense and Panda Adaptive Defense 360 detect and blocks the actual techniques used by attackers during the exploitation stage- for example: heap spraying, stack pivots, ROP attacks and memory permission modifications – but moreover it dynamically detects unknown attacks by monitoring all processes running on devices, and correlates data through machine learning algorithms in the cloud being able to stops any known and unknown attempt of exploitation.

Adaptive Defense Anti-exploit technologies will stop the adversary in the early stage of the internal attack by identifying when a trustable application or process is being compromised.

Mitigation

A next generation endpoint Protection has to prevent and detect attackers during the different stages of the Cyber-Kill Chain, however detection has to be followed by quick mitigation during inception stages of the attack kill chain.

Panda Adaptive Defense 360 automatically and timely mitigates the attack, by quarantining the malware, by killing a compromised process, or even by completely shutting the system down in order to minimize damage.

Remediation

During execution, malware often creates, modifies, or deletes system file and registry settings and changes configuration settings.

These changes, or remnants that are left behind, can cause system malfunction instability or even a open door to new attacks.

Panda Adaptive Defense 360 restores endpoints to its pre-malware, trusted state.

Forensics

Within the changing threat landscape reality and with the frequency, sophistication and targeted nature of adversaries, there shouldn't be any security technology claiming to be 100% effective, and therefore the ability to provide real-time endpoint forensics and visibility is a must.

Corporate cybersecurity teams need to have a plan in place for dealing with reporting breaches, contacting law enforcement or dealing with adverse publicity and the like.

Panda Adaptive Defense and Panda Adaptive Defense 360 provide clear and timely visibility into malicious activity throughout an organization. This visibility allows security teams to quickly assess the scope of an attack and take appropriate responses.

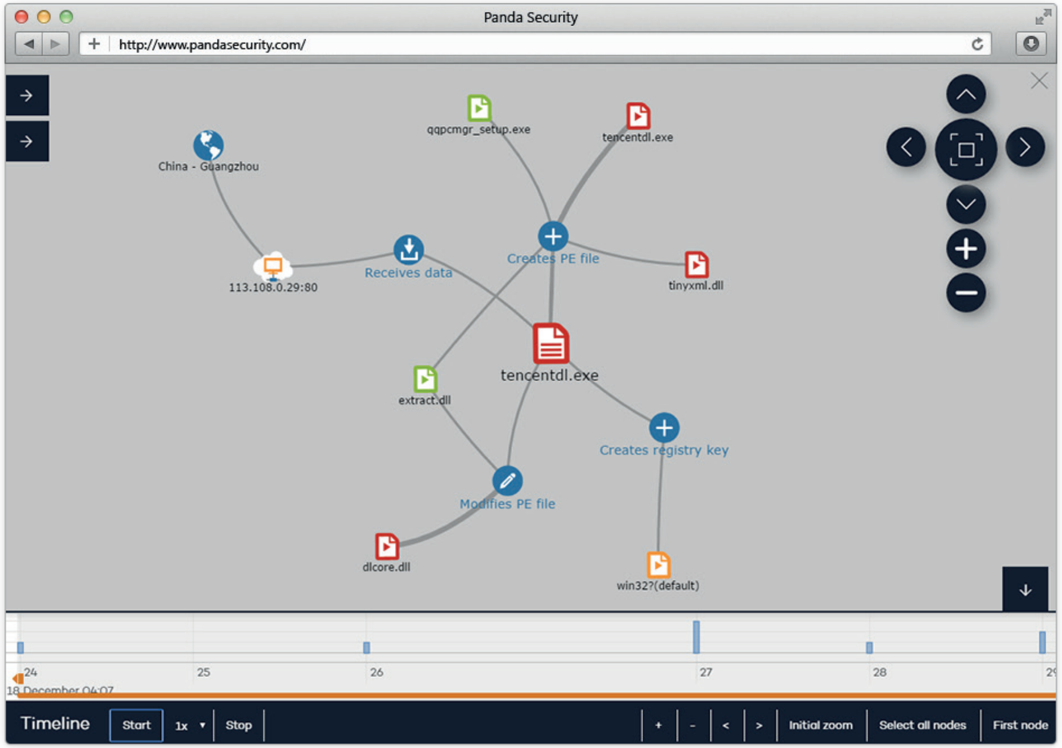


Figure 3. Attack lifecycle graph of forensic analysis.

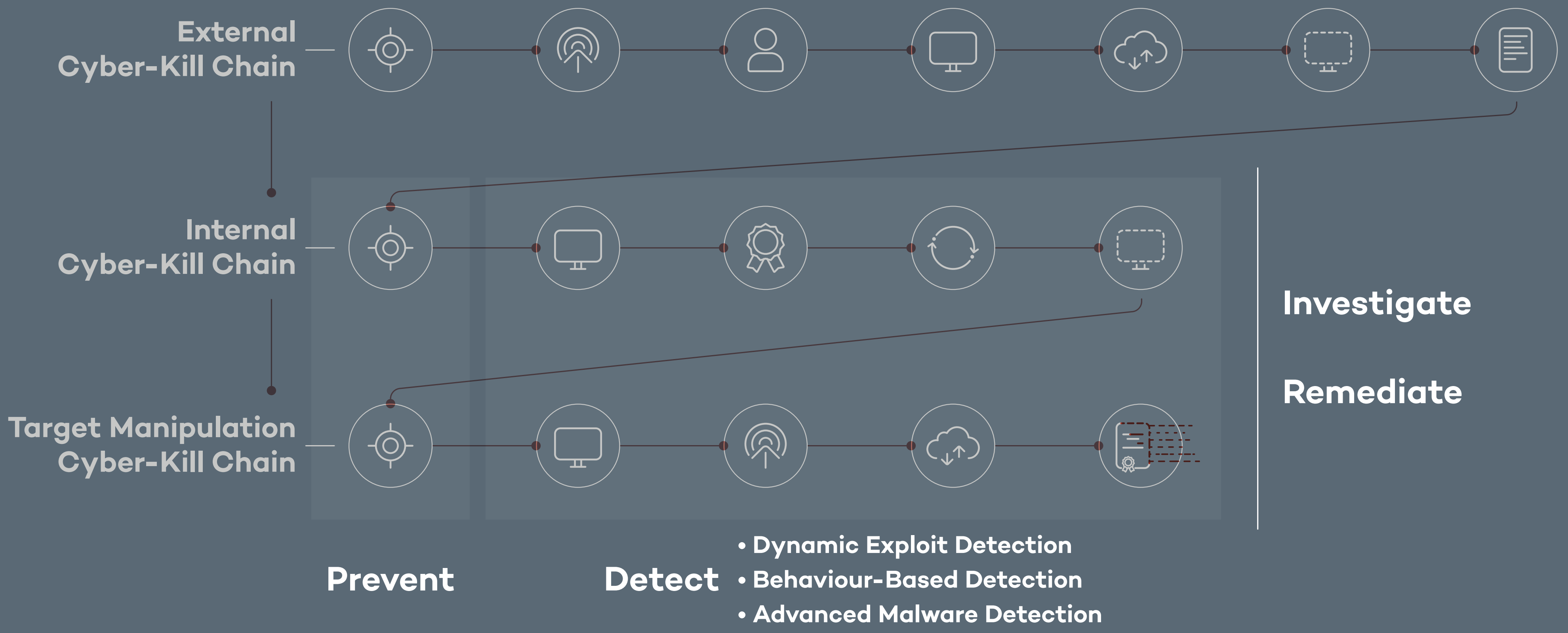


Figure 4. Adaptive Defense 360 security pillars during the extended Cyber-Kill Chain.

References.

- Lockheed Martin's Cyber-Kill Chain: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- Sean T. Mallon, Strategic Cybersecurity Leader & Executive Consultant, at Black Hat 2016: Extended Cyber kill chain
- Mitre's Cybersecurity Threat-Based Defense
- Microsoft's Security Development Life Cycle
- Gartner Research, G00298058, Craig Lawson, 07 April 2016

[1] Eric M. Hutchins,Michael J. Cloppert, and Rohan M.Amín, Ph.D.,Intellígence-Dríven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kili Chains.

[2] **Watering hole attacks**. A specific kind of targeted attack where the victim belongs to a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

The malware used in these attackers typically collects information on the user. Attackers looking for specific information may only attack users coming from a specific IP address. This also makes the attackers harder to detect and research. The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes

Relying on websites that the group trusts makes this strategy efficient, even with groups that are resistant to spear phishing and other forms of phishing.

[3] **Dynamic Exploit Detection** is the Panda Security innovative technology based on monitoring all running processes at the endpoint or server and its analysis in the cloud by machine learning (ML) technologies oriented to detect attempts of trusted application exploitation.

The goal of this new technology is to stop attacks on workstations and servers in the very first stages of the Cyber-Kill Chain. Containing the attacker and hindering their access to the device to such an extent that the profitability of the attack suffers will discourage further attempts, and therefore result in a higher detection rate.

More info at:

pandasecurity.com/intelligence-platform/

Let’s talk:

+34 900 90 70 80

pandasecurity.com

panda