watchguard.com

Understanding Cyber Attacks

panda
a WatchGuard brand

Index:

1. Introduction
2. Understanding the Cyber Kill Chain
3. The Extended version of the Cyber Kill Chain
4. Panda Adaptive Defense 360 at the Cyber Kill Chain
5. An anatomy of a ransomware attack and how Panda Adaptive Defense 360 protects your company
6. References

panda
a WatchGuard brand

1.Introduction

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

Most organization have the means to detect known attacks, although a few of these can still slip by. 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.

Understanding 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 cyber-attack lifecycle model, called the Cyber Kill Chain (CKC), and its extension to the entire network and how Panda Adaptive Defense Service covers the whole lifecycle at the endpoint level.

This Cyber Kill Chain 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 attack's 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 it.

Keep in mind that the most valuable assets of an organization are stored at the endpoints and servers. Therefore all 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 organization's critical assets, stopping adversaries at the endpoint level automatically decreases the probability of success of any cyber attacker, while simplifying the efforts to break the chain and significantly increasing the efficiency and effectiveness of the security operations.

2.Understanding the Cyber Kill Chain

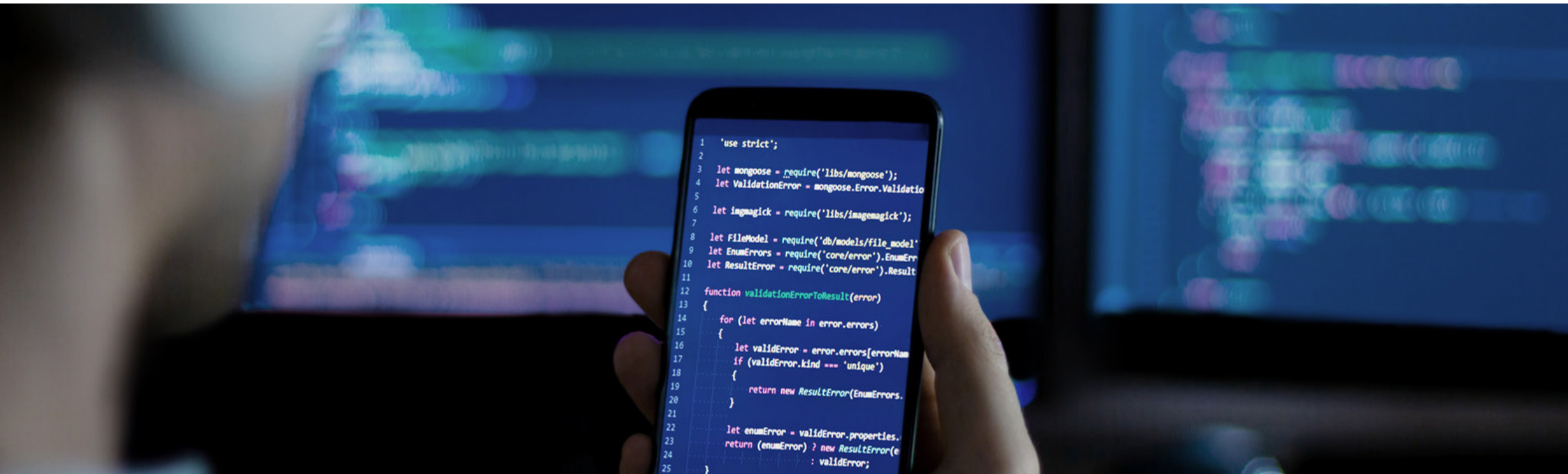
The Cyber Kill Chain framework was originally published by Lockheed Martin as part of the Intelligence Driven Defense model[1] for the identification and prevention of cyber intrusions activity.

The model identifies what adversaries must complete in order to achieve their objective by targeting the network, exfiltrating 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 that all attacks go through and therefore stopping them at this level enormously increases the chance of 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 Cyber Kill Chain

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 and 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.

External Cyber Kill Chain II

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 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, and the 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. 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, not linear. Once an adversary enters the network, he begins the Cyber Kill Chain again, 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 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.

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 unprofitable for them.

Internal Reconnaissance

In this stage, adversaries have access to a single user's workstation and will data mine 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

Attackers take 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, to gain lateral movement within the network, manipulating individual targeted machines.

The Cyber Kill Chain

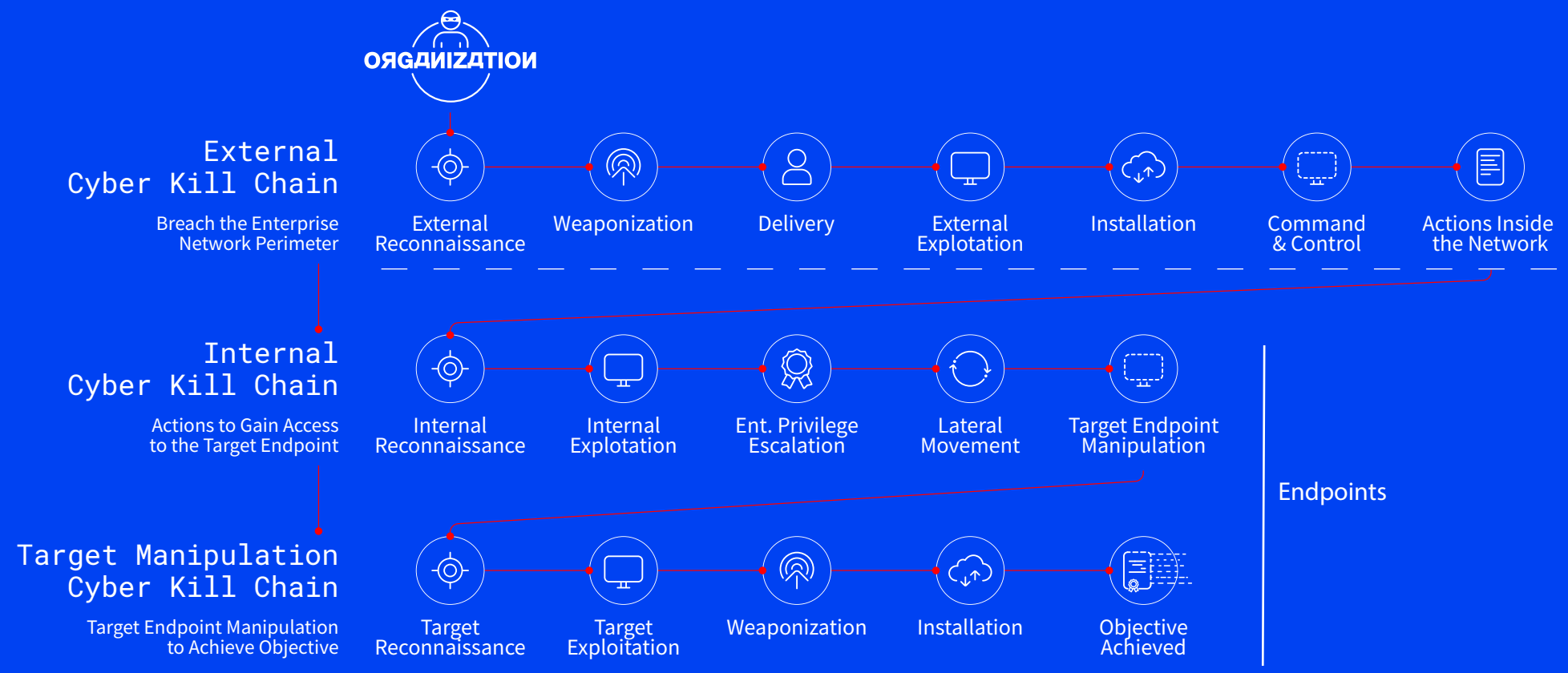


Figure 1. The Extended Cyber Kill Chain. Actions to gain access to the target endpoint and endpoint manipulation to achieve attacker's objective.

4.Panda Adaptive Defense 360 and 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.

WatchGuard's multi-layered security with Panda Adaptive Defense 360 helps ensure that the Cyber Kill Chain is always interrupted and attackers are turned away empty-handed.

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

An organization' s 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.

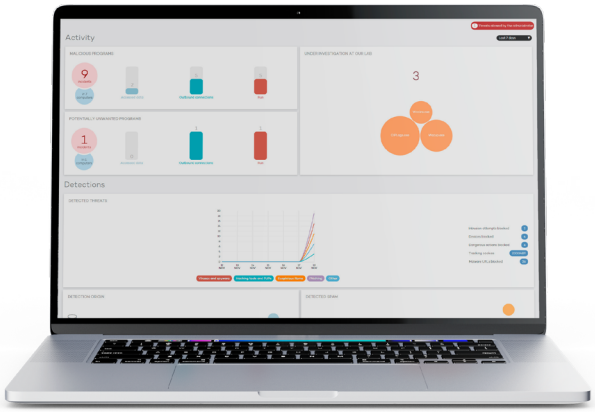
An organization's security strategy has to takes into consideration how an attack is executed, from outside and especially from inside, since attackers once in the network, are insiders with access to endpoints and their assets.

The traditional security approach should be extended with methods based on an understanding of the Cyber Kill Chain, providing technologies that are able to stop attackers from gaining access to the the endpoints, and 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 attack phases, aligning an organization's security to the same success criteria as those of their adversaries.

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

Panda Adaptive Defense 360 addresses these security issues by preventing, detecting and responding to the most advanced techniques that adversaries use at every stage of the extended Cyber Kill Chain. It helps security teams design a security strategy aligned to the extended Cyber Kill Chain without adding headcount thanks to its intelligent endpoint detection and response (EDR).



Panda Adaptive Defense 360 core pillars

Known Malware Prevention

Looking only 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, such as signature-based analysis, generic signatures, heuristics, firewall, URL reputation, contextual detections, vulnerability management, application control, and other capabilities that can greatly mitigate risk.

What's more, Panda Adaptive Defense 360 leverages the Collective Intelligence feature to classify any unknown application. **Collective Intelligence** represents the consolidated and incremental knowledge repository of all applications, binaries and other files containing interpreted code, both trusted and malicious.

This repository in the Cloud is continuously fed by the AI system and by the expert analysts, and it is at the same time continuously being queried by the solutions and services of Panda Security, prior to any execution.

Advanced and Unknown Malware Detection

Panda Adaptive Defense 360 detects and blocks 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 endpoint 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.

These three principles are the fundation of the **Zero-Trust Application Service**. This service classifies applications as malware or legitimate prior to letting only the trusted execute on each endpoint. Since it is a fully automated service, it does not require any input or decision from the end user or from the security or IT teams.

panda
a WatchGuard brand

Contextualized Behavior Detection

The continuous monitoring of the activity at the endpoint allows the agent to act as a sensor and inform the Cloud platform not only about the files being run, but also about their context of execution (what happened right before, which users are trying to run which command or application, which network traffic is generated, which data files are being accessed, parameters, etc).

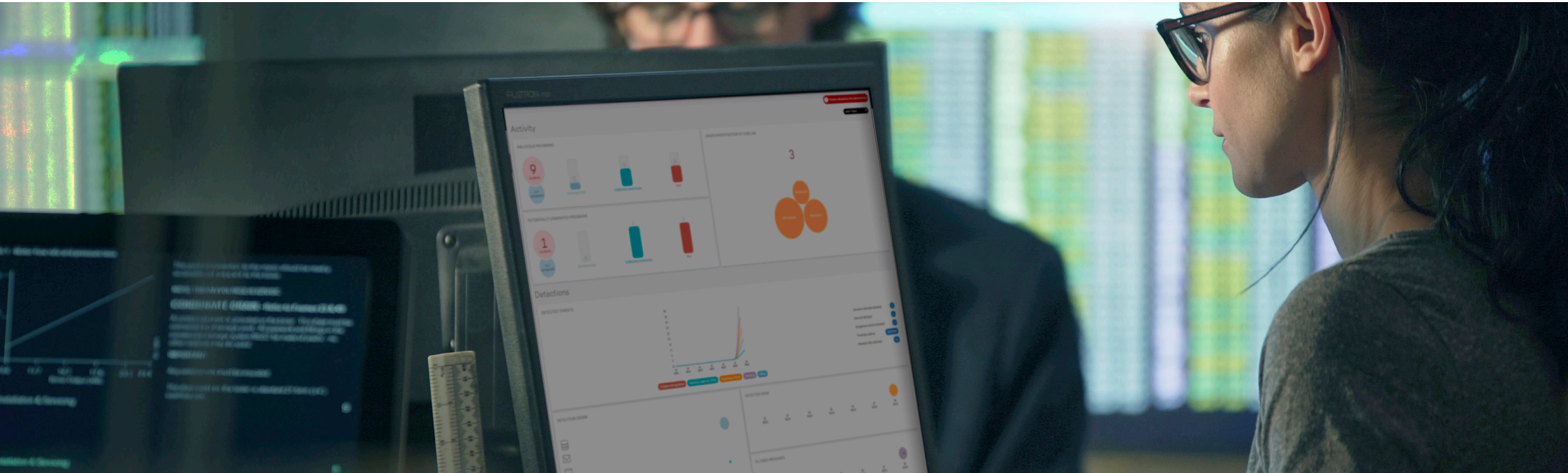
This allows the identification, first at the endpoint, of abnormal behaviour or suspicious activity and their categorization as indicators of attack (IoAs), with a high degree of confidence and without false positives.

Dynamic Exploit Detection

During the exploitation stage of the extended Cyber Kill Chain, attackers use exploits to target code-level vulnerabilities so they can breach applications and systems, and 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 360 detects 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 exploitation attempt.

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.



Panda Adaptive Defense 360 in the Cyber Kill Chain

Prevention and Mitigation

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 mitigates the attack, by blocking any unknown application execution until it is validated as trustable by our machine-learning system and cybersecurity team; by blocking any suspicious activity linked with threat actors techniques; 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 an open door to new attacks. Panda Adaptive Defense 360, in those residual cases in which malware is allowed to run, restores endpoints to their pre-malware, trusted state.

Visibility

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, dealing with adverse publicity and the like.

Panda Adaptive Defense 360 provides 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 actions.

Remote Response

When remote systems are the targets for attackers and get compromised, IT or security teams need to work quickly to understand the attack and take action to remediate. The responders need remote system visibility and access since users can't walk a laptop over to IT.

Panda Adaptive Defense empowers IT and security teams with deep endpoint visibility to rapidly investigate incidents and fully understand emerging threats; moreover, it gives them direct system access and the ability to quickly run a wide variety of commands to contain attackers and remediate remote hosts, such as isolating endpoints from the network – preventing communication to and from other endpoints to stop the spread of the attack – and killing processes by restarting the endpoint.

With these capabilities Panda Adaptive Defense 360 can dramatically reduce the time needed to respond to attacks – wherever they happen – and get the organization back to business quickly.

Panda Adaptive Defense 360 in the Cyber Kill Chain

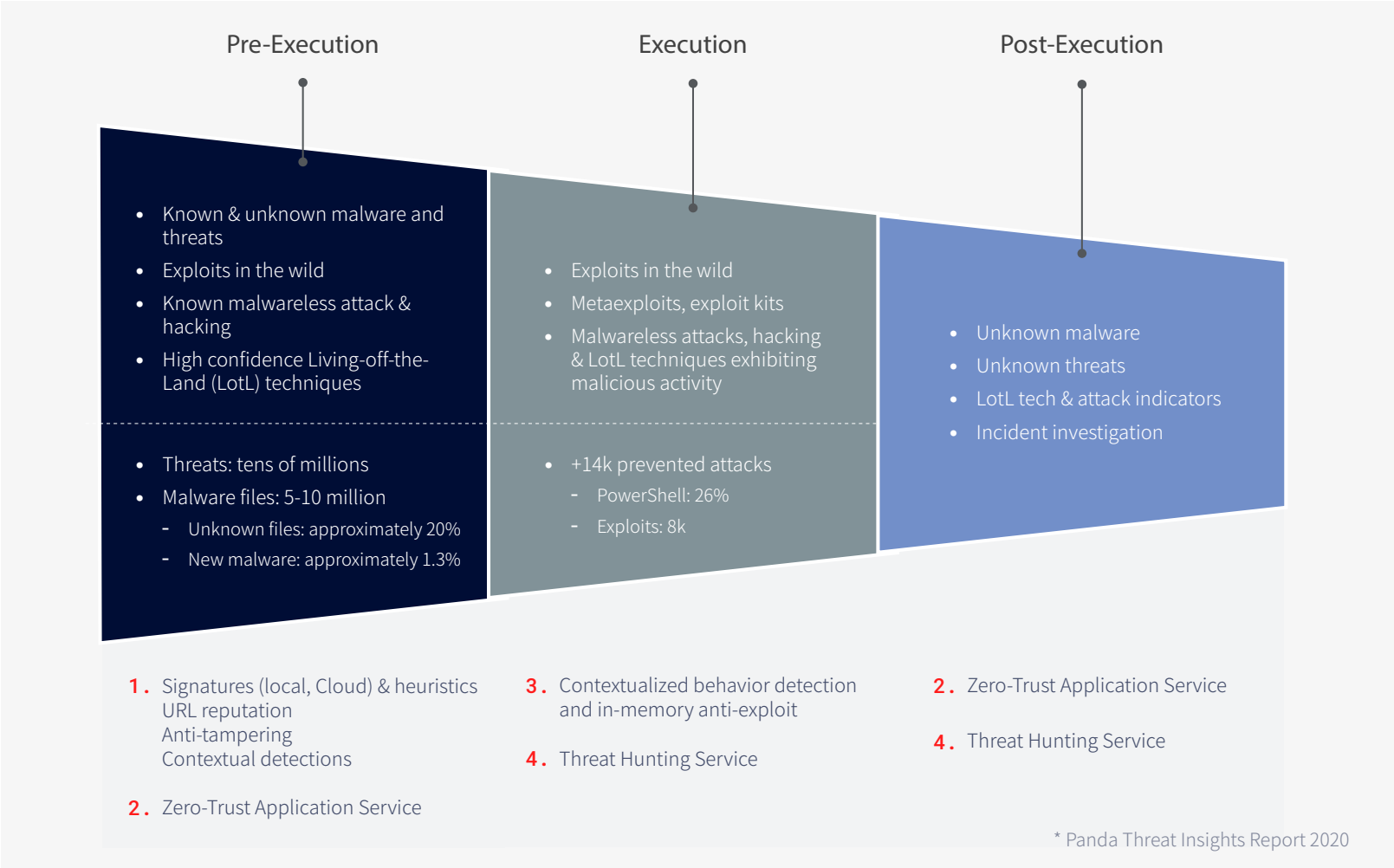


Figure 2. Adaptive Defense 360 security pillars during the extended Cyber Kill Chain.

5. An anatomy of a ransomware attack and how Panda Adaptive Defense 360 protects your company

Figure 3 illustrates how Panda Adaptive Defense 360 addresses each stage of the kill chain in a ransomware attack and shows how it can prevent and stop ongoing attacks before the damage is done.

Often, the attacker uses simple techniques to get the first foothold in any targeted endpoint, most of the time using social engineering such as phishing. A user receives an email prompting them to click a link or download a malicious file.

STEP 1

At this point, AD360 will immediately act by:

- Blocking malicious emails with the Email Antispam technology.
- Preventing access to known malicious URLs with the URL Filter.

STEP 2

In the event the threat actor isn't blocked, and the end user accesses the malicious website that has been compromised, several malicious actions can happen, such as exploiting a browser vulnerability or downloading a Microsoft Office file with a malicious script.

In any case, Adaptive Defense 360 will block the attacker with the anti-exploit technologies, either with the in-memory anti-exploit module that blocks known and unknown exploits, or with the macro prevention or the context-based detection that denies malicious script executions.

STEP 3

Let's assume the worst-case scenario in which the threat actor is able to drop ransomware into the device. Panda Adaptive Defense 360 will prevent the compromise by blocking the malware download by either checking against the local generic signatures and scanning the file with heuristic technologies or by querying our Collective Intelligence in the Cloud.

Generics signature-based detection refers to the detection and removal of multiple threats using a single signature. The starting-point for generic detection is that successful threats are often copied by others, or further refined by the original authors. The result is a spate of ransomware variants, each one distinct but belonging to the same family. In many cases, the number of variants can run into the hundreds, thousands or even tens of thousands.

The heuristics scan is a set of techniques to inspect files based on hundreds of file characteristics. It determines the likelihood that a program may take malicious actions when run on a user's computer, blocking and removing it before it arrives at the endpoints.

STEP 4

So far, we've been looking at technologies that work to block threat actors but can't guarantee that no malicious applications are running on the endpoint. However, they significantly reduce the amount of work to be processed by the Zero-Trust Application Service, which is the next protection layer in the Cyber Kill Chain. So, let's assume the ransomware is downloaded and tries to be executed on the endpoint to begin its malicious and evasive behaviors.

At this time, the Zero-Trust Application Service identifies the binary as unknown, denies its execution, uploads it to the Cloud and automatically classifies the payload with a complex and comprehensive cluster of ML algorithms, combining hundreds of attributes, many of them obtained from detonating the sample in a real environment in our Cloud infrastructure.

The classification occurs, 99.98% of the time, in real time, as there is no need to supervise the results. Only in exceptional cases do our cybersecurity experts need to complete the classification, as new suspicious behaviors could have been identified in the process.

In any case, the result of these Cyber Kill Chain defenses is a true zero-trust model in which no malicious applications, binaries, or processes are executed.

panda
a WatchGuard brand

STEP 5

When threat actors are able to get into the endpoints without using malicious applications, then other components of the layered protection take central stage in the Cyber Kill Chain. For example, if the threat actor gets control of an endpoint, gains persistence, and starts exploring the network searching for new endpoint targets using Living-of-the-land techniques, then the context-based detection technologies will block the attempt to abuse the use of systems tools, such as PowerShell.

STEP 6/7

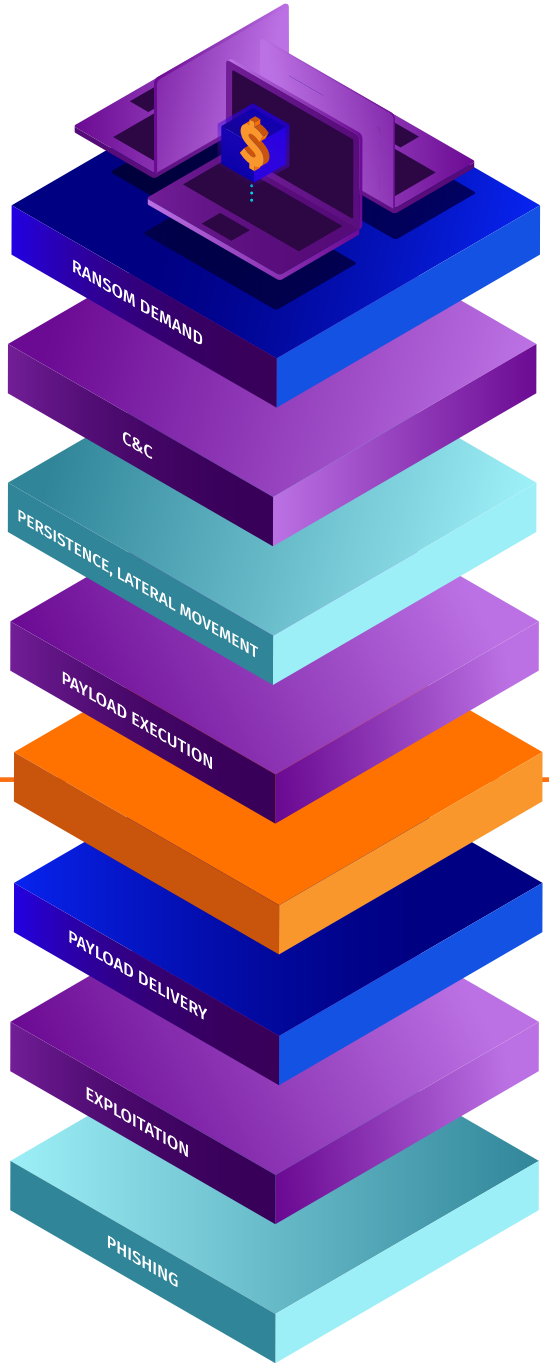
The key component in this effective implementation of the zero-trust model is the fact that every activity at the endpoint is being monitored in real time and evaluated by the Zero-Trust Application Service and by the Threat Hunting Service that detects and investigates suspicious activity, notifying or blocking confirmed malicious activity at the endpoints.

Extend your visibility and protect your organization regardless of physical location. Try Panda Adaptive Defense 360

https://www.watchguard.com/wgrd-products/demos-free-trials

An Anatomy of a Ransomware Attack

Layered Protection Panda Adaptive Defense 360



1. **User is sent an email prompting them to click a link or download a malicious file.**

   Block malicious email with **Antispam.**

   Prevent access to known malicious URLs with **URL filtering.**

2. The website exploits a **browser vulnerability** or **downloads a MS office file** with a malicious script (Drive-by download attack).

   Block known browser exploitation with **anti-exploit technology.**

   Block unknown exploitation with **in-memory anti-exploit technology.**

   Block script execution with **macro detection or context-based detection.**

3. After the user **clicks, the ransomware** is delivered to the endpoint.

   Block threats after lookup to the **Cloud-based repositiory.**

   Block known/unknown **generalist signatures & heuristics.**

4. Ransomware executes on the endpoint and **begins its malicious and evasive behaviors.**

   Zero-Trust Model: any unknown binary coming from "outside" (email, web, network, device) is blocked until classified.

   Zero-Trust Application Service automatically classifies the payload in the Cloud with **ML and real environment.**

No malicious applications, binaries or process are executed.

No malicious applications, binaries or process are executed.

5. Once the threat actor controls an endpoint, **they explore the network and search new targets** (LotL Techniques).

   Block abusive usage of systems tools (PowerShell) with **context-based detection.**

   Block malicious behavior exhibited during execution with **contextualized behavior detection.**

6. Ransomware attempts to retrieve encryption key **from a command and control server.**

   The Zero-Trust Application Service denies malware execution.

7. Ransomware begins the process of encryption of files on the endpoint. **Message displayed confirms the presence of ransomware** on the endpoint and provides instructions for paying the ransom.

   In any case, all process are continually being monitored and reclassified by the **Zero-Trust Application Service.**

   Telemetry is being monitored and analyzed by the **Threat Hunting Service.**

panda
a WatchGuard brand

6.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 by 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 attacks 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.

panda
a WatchGuard brand

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com | pandasecurity.com

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an/if and when available basis. ©2020 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Panda Security are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE67388_110520

For more information visit our website