Advanced Threat Protection with Dell SecureWorks Security Services

Table of Contents

Summary

Actors behind advanced threats have a toolbox of exploit techniques at their disposal. They often combine several intrusion tools and techniques in order to compromise and maintain access to their target.

The advanced threat actor will evade security controls and most CISOs acknowledge this reality. Malware, phishing, social engineering, and endpoint vulnerabilities provide fertile ground for advanced threat actors looking to penetrate your defenses and set up shop inside your network.

Across both the private and public sectors, IT security organizations are fighting an ongoing battle against sophisticated adversaries. To do so, security professionals are mostly relying on technology such as firewalls, Intrusion Detection Systems, Intrusion Prevention Systems and the like to protect their environments from a range of cyber threats. However, these technologies are proving insufficient in the battle against advanced threat actors.

This paper distinguishes what an advanced threat is, the actors, their motives and processes, and provides a roadmap of Dell SecureWorks services to help clients enhance their security posture to better detect and resist advanced threats.

What are Advanced Threats?

An "Advanced Threat," in simplest terms, is a targeted threat or exploit.

Advanced or targeted threat actors deliberately select an organization and mount campaigns to penetrate security defenses and gain access. The actors have specific motivations which include financial enrichment, the attainment of competitive advantage, the collection of intelligence, the theft and exploitation of intellectual property, and embarrassment or harm to your organization. An Advanced Persistent Threat represents the most organized, sophisticated and committed threat among targeted threats.

Advanced or "targeted" threats are different from your every day, generic, broad-based threats in their application – they are targeted. By their very nature, Advanced Threats introduce the complexities of motives, objectives and identities of actors. Effective IT security organizations of the future must establish capabilities to identify these actors, understand their motives and work to stop them from achieving their objectives.

How do advanced threat actors operate?

The "Kill Chain"

The Kill Chain is the high-level framework or workflow that targeted threat actors employ in their efforts to compromise the target. Disrupting any part of the chain means that the attacker's efforts are thwarted. It's important to note that for each targeted attack, the lower-level details (i.e. malware and tradecraft used, what's being targeted, etc.) of the kill chain will vary.

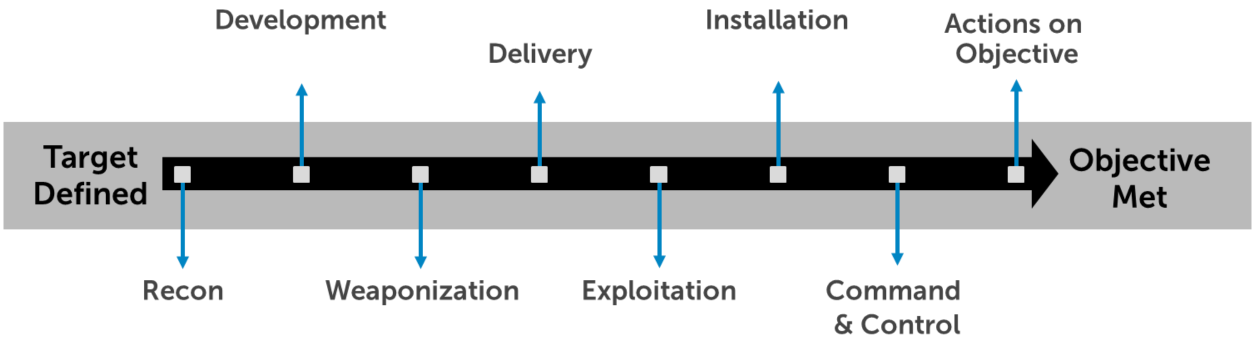

Figure 1: The Kill Chain

Steps of the Kill Chain

1. **Reconnaissance**: This defines how the Threat Actor or Actor Group gathers information previous to and during the computer network operations they engage in. This may be through open source research, scanning, Web, the theft of intellectual property, or human sources.
2. **Development**: This step is used to capture useful information about the development of infrastructure and tools behind the target's operations.
3. **Weaponization**: Weaponization describes the "coupling of a remote access Trojan with an exploit into a deliverable payload.
4. **Delivery**: This step describes the transmission of the tools into the victim organization. The most common forms of delivery take the forms of Scan&Exploit, Credential-Access, Spearphish, Web-Delivery, or Physical delivery.
5. **Exploitation**: Exploitation describes the methods used to execute the malicious code. This step details whether the adversary use new 0-days, appears to acquire 0-days and exploits 2nd hand, or relies upon social engineering to trick users.
6. **Installation**: Installation describes the methods and artifacts left behind by the actor while implanting malicious code on compromised systems. These artifacts can include notable aspects of the installation, and unique installation tools.
7. **Command and Control**: Command and Control describes the methods used to interact with compromised resources left within the organization. This activity extends beyond communicating with implants to include hosts used to login with collected credentials, as exfiltration end points, and to interact with web shells.
8. **Action on Target**: Once the actor(s) gains access to compromised infrastructure, the actor(s) takes specific actions to finalize meeting their objective. For example, if the attacker's objective was to acquire credit cardholder data, the attacker would seek to exfiltrate that information at this stage.

The kill chain is a variable process, depending on the threat actors involved, their preferred tradecraft, the mission and other factors. Advanced threat actors do not always perform the stages above in their entirety. It's only the most sophisticated threat actors that follow a very deliberative and organized process in their efforts. Advanced Persistent Threat actors do likely follow a more formalized and staged approach to target, penetrate and exploit the targeted organization.

Advanced Threat actors will pursue a path of least resistance using simpler tools and exploits first, and graduate their level of sophistication as successes or setbacks dictate. Some actors may adapt and customize their Tactics, Techniques and Procedures (TTP) to predict and circumvent your security controls and standard incident response practices during the course of their exploit and infiltration.

Many Advanced Threat actors may not be concerned about covering their tracks after they have accomplished their initial goals whereas an Advanced Persistent Threat actor may lie in wait to exploit your network again in the future.

We recommend reading "Lifecycle of the Advanced Persistent Threat" white paper for more detailed discussion of Advanced Persistent Threats as a complement to this discussion.

Addressing the Threat

Breaking the kill chain

IT and IT Security's challenge is to disrupt the targeted attacker's kill chain or lifecycle at the earliest point possible.

There are core capabilities that must be present for any organization to effectively defend, resist and respond to Advanced Threats. These areas can be divided into four main areas: Know, Detect, Disrupt, and Eradicate.

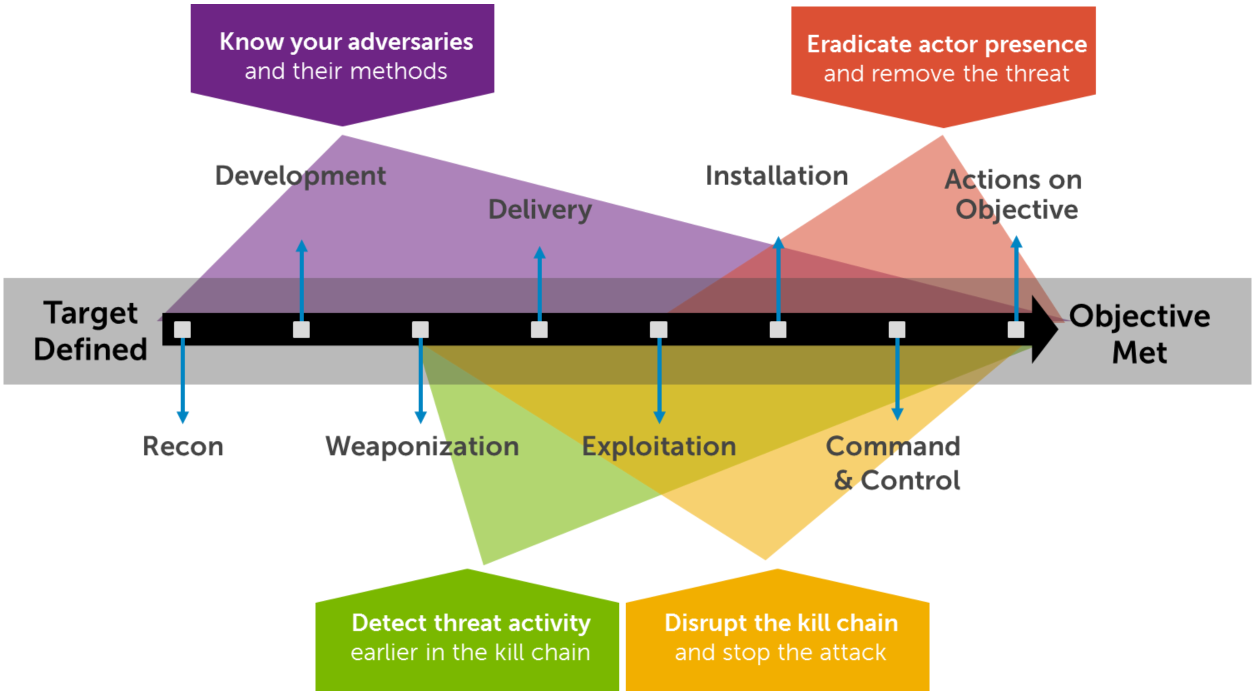

Figure 2: Breaking the kill chain

Know your adversaries and their methods

Organizations should look to deploy forward intelligence capabilities that provide actionable information on Advanced Threat actors and their operations. Regardless of the intelligence's generalized or specific nature, the intelligence must be actionable to enhance the organization's security posture and educate security professionals to threats.

Detect threat activity earlier in the kill chain

Security teams must have full visibility into the operations and security of their systems, networks and assets. Organizations must evaluate their current security architecture and consider recalibrating security policies to ensure that the right information is being collected and correlated to give security professionals a view of the "big picture" across your networks, information and assets. This big picture view may be instrumentation in a dashboard representation. Having visibility into what is happening behind the firewall is just as important as what is trying to penetrate the firewall from the outside.

Disrupt the kill chain and stop the attack

Security leaders must evaluate the capabilities of operations and personnel. Leaders must answer whether their operations are efficient and effective and if not, how they can be improved. This includes assessing the expertise and constraints on that expertise to monitor and address threats in real time.

Eradicate actor presence and remove the threat

Because there is no "silver bullet" to protect against Advanced Threats 100 percent of the time, organizations must evaluate their capability to respond effectively to an incident.

Containing a problem rapidly and effectively can make all the difference. Security professionals should take an introspective look at their organization to determine if the organization is adequately prepared to respond effectively to a breach by an Advanced Threat actor. Many organizations are looking at a breach as a "when" and not an "if." It is critical your organization has a Computer Security Incident Response Plan (CSIRP) in place detailing roles and responsibilities, and that the plan is detailed and tested.

How Dell SecureWorks Can Help

Based on our conclusion that successful defense against advanced threats requires integrated threat intelligence, security operations and incident response capabilities, Dell SecureWorks has developed a portfolio of service options to address the challenge posed by targeted threats.

Dell SecureWorks Advanced Threat Services elevate your defenses with key capabilities needed to effectively resist targeted threats. Fueled by Dell SecureWorks Counter Threat Unit™ (CTU) intelligence, Advanced Threat Services help you anticipate your attackers, detect their tradecraft, disrupt the kill chain and eradicate their presence in your environment.

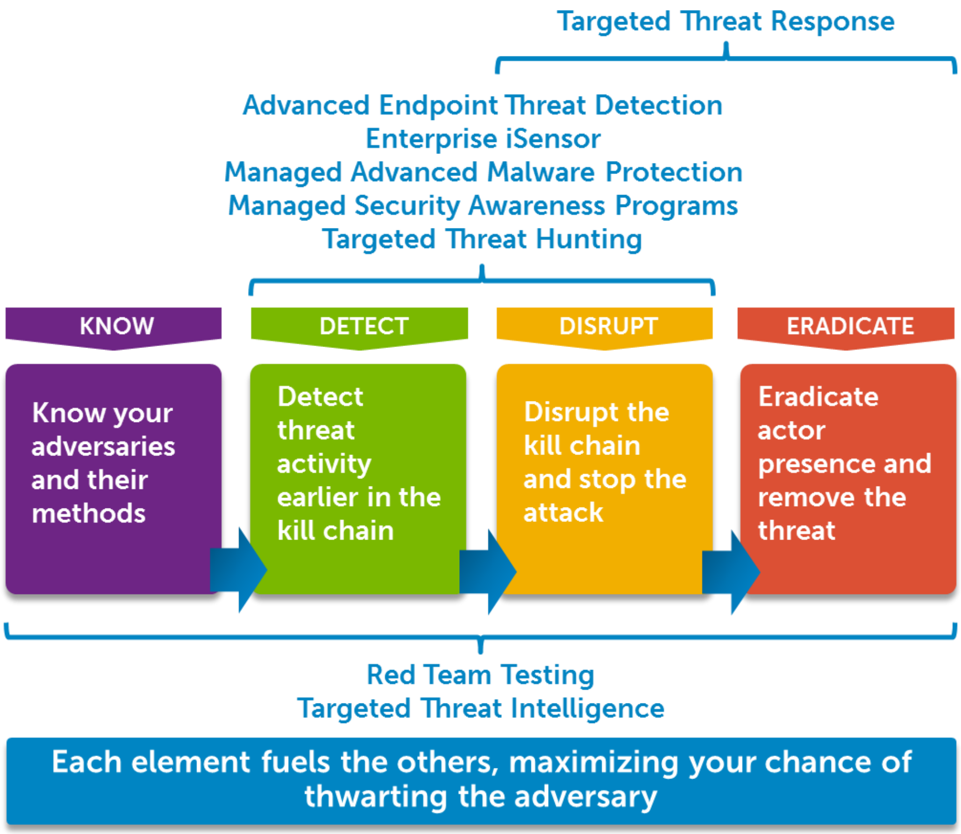
Targeted Threat Response
Advanced Endpoint Threat Detection
Enterprise iSensor
Managed Advanced Malware Protection
Managed Security Awareness Programs
Targeted Threat Hunting
KNOW
DETECT
DISRUPT
ERADICATE
Know your adversaries and their methods
Detect threat activity earlier in the kill chain
Disrupt the kill chain and stop the attack
Eradicate actor presence and remove the threat
Red Team Testing
Targeted Threat Intelligence
Each element fuels the others, maximizing your chance of thwarting the adversary

Figure 3: Advanced Threat Services applied to the challenge posed by targeted threats

Know, Detect, Disrupt and Eradicate Capabilities

Know your adversaries and their methods

How Dell SecureWorks Can Help	Dell SecureWorks Services
With our broad visibility and relationships, Dell SecureWorks' CTU researchers are able to identify threats in advance, assess their severity and provide recommendations for protecting your assets before damage is done. Services are tailored to meet the unique environments of our customers, with threats mapped to their assets and delivered to the right people in the organization through a variety of customizable methods.	Targeted Threat Intelligence Red Team Testing **Other services:** Global Threat Intelligence

Detect threat activity earlier in the kill chain

How Dell SecureWorks Can Help	Dell SecureWorks Services
Dell SecureWorks helps you see what's happening across your environment. We can evaluate your architecture, helping you recalibrate your security policies to ensure that the right information is being correlated to your team to form a view of the big picture across your networks, information and assets. We can help you detect active intrusions by threat actors who are being watched by the CTU. Receive immediate alerts when suspected APTs are detected. Improve your employees' effectiveness at detecting and resisting APT attacks.	Advanced Endpoint Threat Detection Enterprise iSensor Managed Advanced Malware Protection (MAMP) Managed Security Awareness Targeted Threat Hunting **Other services:** Targeted Threat Intelligence

Disrupt the kill chain and stop the attack

How Dell SecureWorks Can Help	Dell SecureWorks Services
Dell SecureWorks helps you optimize the efficiency and availability of your security so your staff can focus on initiatives that move the organization forward. We can help you get 24x7x365 coverage of your environment and help you disrupt active intrusions by threat actors who are being actively watched by the CTU.	Advanced Endpoint Threat Detection Enterprise iSensor Managed Advanced Malware Protection (MAMP) Managed Security Awareness Programs Targeted Threat Hunting **Other services:** Targeted Threat Intelligence

Eradicate actor presence and remove the threat

How Dell SecureWorks Can Help	Dell SecureWorks Services
Dell SecureWorks can help you with your "Plan B" and minimize any impact of a successful penetration of your network and systems. We can help you develop a strong Incident Response plan within your organization and test your IR plan. Should you experience an incident, we can conduct a forensics investigation to determine the full extent of the breach following evidentiary procedures. In addition, we conduct malware code analysis to understand the unique nature of the threat, as needed.	Targeted Threat Response **Other services:** CSIRP Development CSIRP Gap Analysis IR Tabletop Exercises Targeted Threat Intelligence

Targeted Threat Intelligence

Targeted threat intelligence services allow organizations to identify and assess targeted threats and the actors behind them, gain insight into ongoing exploits at a detailed level, and take proactive steps to defend against them.

Services include:

- The **Targeted Threat Surveillance** service proactively provides contextual, researched, actionable host and network threat indicators specific to your organization to inform your customer protection and response processes.
- The **Enterprise Brand Surveillance** service provides real-time monitoring of information outlets and communications to identify threat actors targeting your organization, so you can quickly and

effectively prepare countermeasures to protect your networks, systems, data and brand reputation.

- The **Executive Threat Surveillance** service monitors and assesses risk posed to your executives, specific personnel, and organization.

Red Team Testing

Red Team Testing simulates a real-world attack against your organization using blended threat scenarios that test the effectiveness of your security defenses, policies and staff.

Managed Advanced Malware Protection

Managed Advanced Malware Protection (MAMP) detects and blocks advanced malware delivered via email and web content, often used by Advanced Threat Actors.

Enterprise iSensor

The Dell SecureWorks Enterprise iSensor IPS service helps you eliminate malicious inbound and outbound traffic around the clock, without the burden of device or signature management, and without increasing in-house headcount.

The service performs in-line deep packet inspection of inbound and outbound network traffic using multiple integrated defensive technologies to identify and block real security events that require attention. The subscription includes hardware, support, managed and monitored service, and thousands of unique countermeasures developed by our CTU research team.

Targeted Threat Hunting

The Dell SecureWorks Targeted Threat Hunting service searches your networks to identify the presence of compromises and entrenched threat actors operating in your environment.

Powered by CTU Special Operations, the Targeted Threat Hunting service leverages elite cyber threat intelligence and decades of combined experience countering targeted adversary tradecraft. Our highly experienced security experts, armed with CTU proprietary hunting technology, perform a deep inspection of your environment to identify targeted threat indicators and indications of attacker presence.

Targeted Threat Response

The Targeted Threat Response service provides rapid containment and eradication of threats, minimizing the duration and impact of a security breach. Leveraging elite cyber threat intelligence and global visibility, the CTU Special Operations team helps you respond to and recover from even the most complex and large-scale security incidents involving targeted actor tradecraft.

Advanced Endpoint Threat Detection

The Advanced Endpoint Threat Detection service will improve your security situational awareness by warning you when endpoints may have been compromised and will accelerate your remediation effort by pinpointing exactly which systems are compromised, how they were compromised, and how you can remediate.

Managed Security Awareness Programs

Security Awareness Training solutions help you assess your current Information Security Awareness Training programs, design new programs by top IT security advisors and provide specialized training to address areas of greatest concern to your organization. Going beyond compliance, Security Awareness Training Solutions change employee behavior and reduce risk to your organization.

About Dell SecureWorks

Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Dell SecureWorks' Information Security Services help organizations proactively fortify defenses, continuously detect and stop cyber-attacks, and recover faster from security breaches.
For more information, visit
http://www.secureworks.com.

For more information, phone 877.838.7947 to speak to a Dell SecureWorks security specialist.