Evaluating Endpoint Security Solutions Across the Cyber Kill Chain

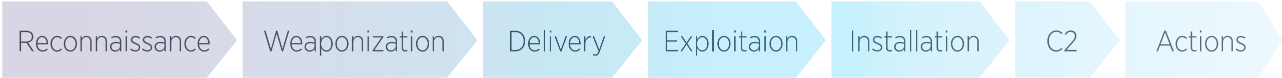
Whitepaper

SentinelOne

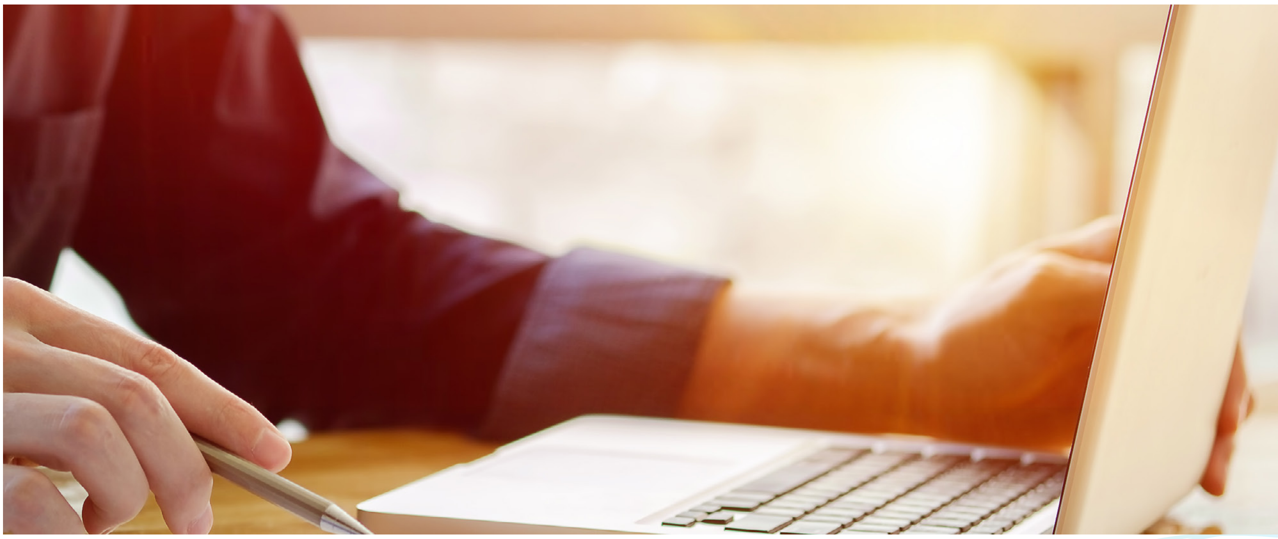
Introduction

The Cyber Kill Chain is an intelligence-led, trademarked framework developed by Lockheed Martin in 2011, following intrusion activity against their organization by threat actors of a persistent and sophisticated nature[1]. The kill chain measures the effectiveness of security assets across all types of threats, including Advanced Persistent Threats (APTs).

Not all threats are APTs, but advanced capabilities have begun to filter down to run-of-the-mill attackers. Regardless of their skill level, each cyber-threat roughly follows the diagram below. Time and risk increase from left to right.



Threats will appear differently based on where they fall along the kill chain. Concordantly, different tools are often deployed to defend endpoints at different stages. For administrators, the challenge is to protect endpoints at as many kill chain phases as possible, using the smallest number of tools.



Unauthorized Access: The Key Metric

How can administrators minimize product usage while maximizing security?

They need to understand which products can:

minimize the number of systems exposed to attack

&

minimize the time that systems spend exposed to attack

Endpoint security must be evaluated on its ability to minimize both metrics of unauthorized access. From the administrator's point of view, it is as dangerous to have one system exposed for two hundred days as it is to have twenty systems exposed for ten days. Malware authors know this as well. While APTs see value in long, slow, and stealthy campaigns, other bad actors such the author of FastPoS obtain better results by infecting many systems for a short time[2].

The kill chain thus sets up a very high standard for endpoint protection systems. Effective EPP goes both broad and deep, detects stealthy malware and conventional attacks, and limits any intrusion to the shortest amount of time.

Kill Chain Part One: Reconnaissance

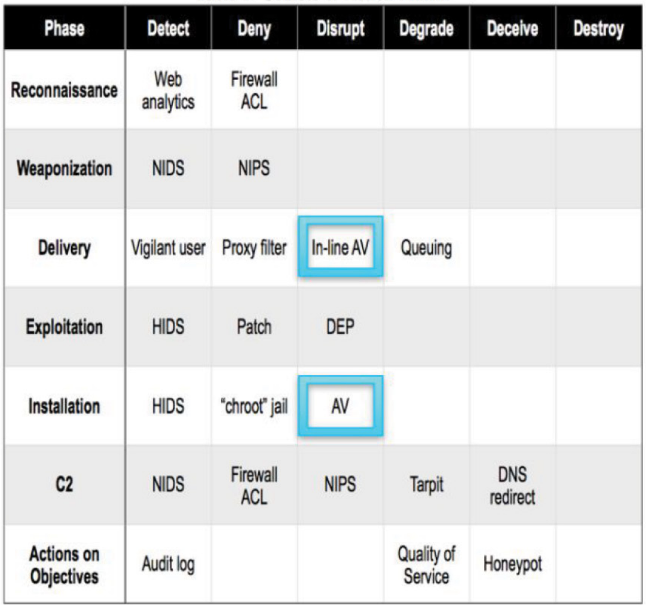
Per the diagram, the first stage of the kill chain is reconnaissance. This entails identifying what services and applications are in use and are allowed to pass security. For example, emails regularly pass through the firewall. An attacker might first try sending some emails to their targets in order to assess whether that application is secure, patched up to date, and scanned by antivirus.

As far as traditional endpoint security is concerned, there are only two chances to find malware in an email. The first is delivery—the AV might scan each email as it comes through the firewall. If that doesn't work, the second chance is installation. Say that the recipient clicks on a malicious attachment—traditional AV might notice a malware signature as it unfolds, and then take action.

This is the case for all traditional, signature-based AV products. No matter what delivery method is tried, the program is only effective during the delivery and installation phases of the kill chain.

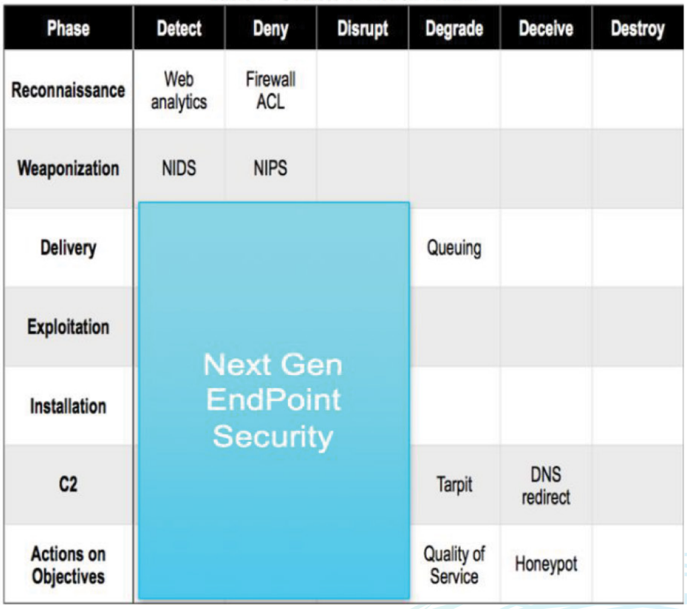
However, next generation endpoint protection can provide security functions at many stages of the kill chain, ranging from the delivery phase right through to the final actions on objectives phase. The diagram below illustrates the differences.

Table 1: Courses of Action Matrix



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Table 1: Courses of Action Matrix



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Next Gen EndPoint Security			Queuing		
Exploitation						
Installation						
C2				Tarpit	DNS redirect	
Actions on Objectives				Quality of Service	Honeypot	

Weaponization Phase

During the weaponization phase of the kill chain, a malicious payload disguises itself as a particular type of business application or operating system file type. Often these file types are Windows executable files, pdf documents, office documents, script files, archives, screensavers or shellcode and user manipulation payloads.

The measure of endpoint security solutions during the weaponization phase is their ability to apply checks consistently from a wide variety of payload vectors. It is possible to weaponize nearly every running process or application on an endpoint. Therefore, endpoint security must be prepared to monitor every running process on an endpoint in order to detect indicators of compromise.

Delivery Phase

Hackers can deliver threats into organizations in many ways, but social engineering, especially in the form of email, web applications, and USB drives, continues to be the most prevalent source for malware encounters. Social engineering is also quite effective. According to Verizon's 2016 Data Breach Investigations Report, targets open around one third of all phishing emails[3].

Malware delivery relies on human interaction to move into the next phase of the kill chain, exploitation. In order for exploitation to take place, the target must take an action such as viewing a file or page, opening an attachment, following a spoofed URL, or clicking a link.

Many of these actions come with warnings, but according to a joint study from Google and Brigham Young University, ninety percent of users ignore them[4]. Therefore, an EPP solution should operate regardless of the human operator’s awareness of risk, best practice usage, or level of care exhibited.

Exploitation Phase

Endpoints are compromised by the execution of the attacker's initial payload. Although a large and increasing number of malware variants are unique[5], most variants use similar underlying techniques. These can include manipulation of memory, corrupted office documents with macros, unpatched vulnerabilities in Flash or Java, etc.

These methods often require no interaction from the user. Exploit kits, for example, can infect users that visit a compromised website, even if they don't click a single link. Endpoint security solutions should offer broad protection from all forms of attack, and especially memory based attacks, such as heap corruption, use after free, and type confusion methods.

Installation Phase

The installation phase outlines the type of techniques that bad actors use to persist on systems. Essentially, malicious programs need to ensure that they start up again every time the computer is rebooted, without interaction from the user. Persistence methods include installing new files onto systems, injecting existing files with additional code, or placing their control of the system in memory without saving any files to disk.

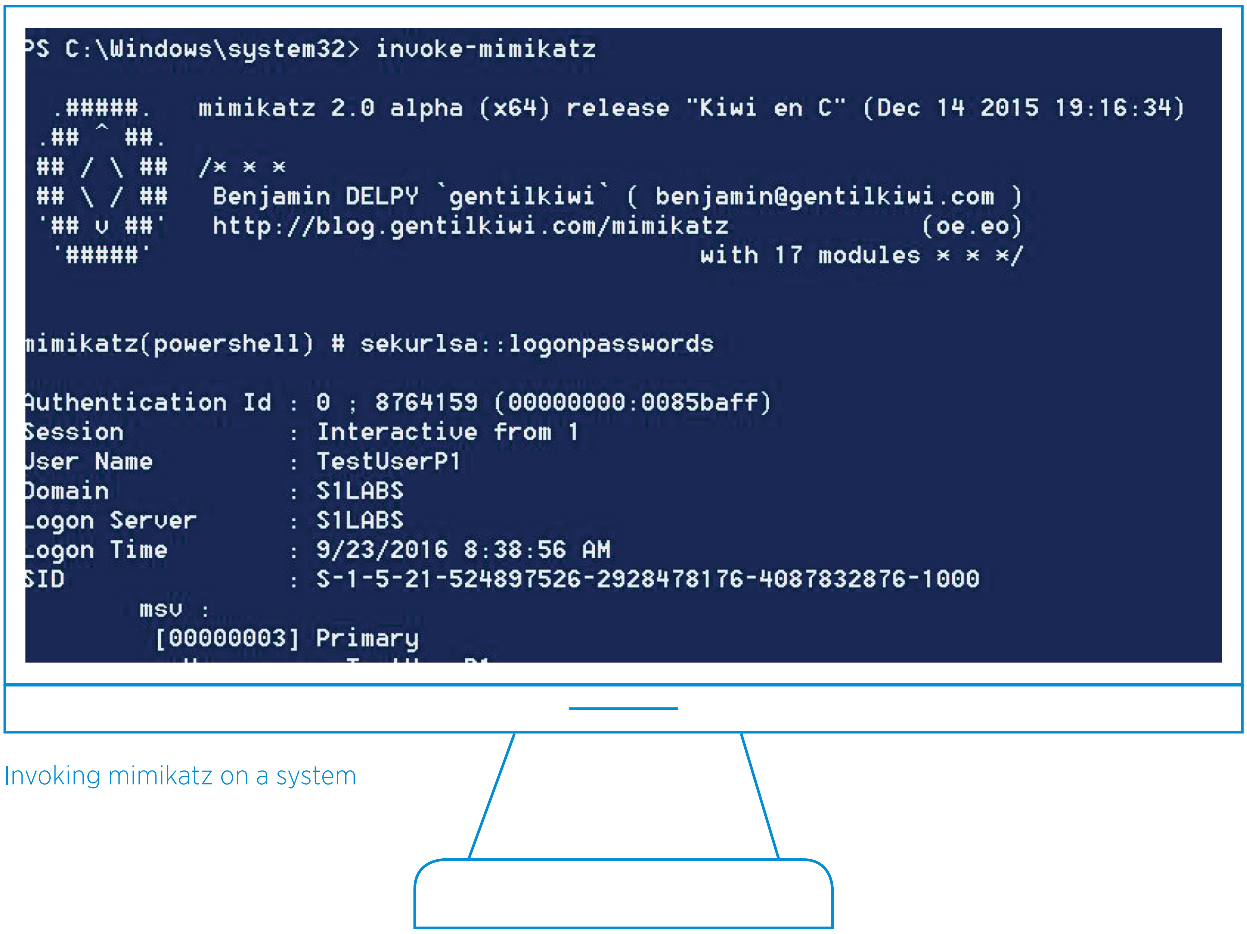
There are many encryption and obfuscation methods in use by the threat actors to bypass traditional AV. These range from custom wrappers and packers, switching off the ability of anti-virus to update itself with new checks, and bypassing the file system completely by loading payloads directly into memory. Protection from all evasive payload installation methods is critical to ensure the efficacy of endpoint security solutions.

C2

C2 stands for "Command and Control." Once successfully installed on a victim computer, the payload connects back to the threat actor to receive further instructions, conduct further manipulation, exfiltrate credential information, and other situational information. Good endpoint protection should be able to file unauthorized network connections under "suspicious activity" to flag or mitigate.

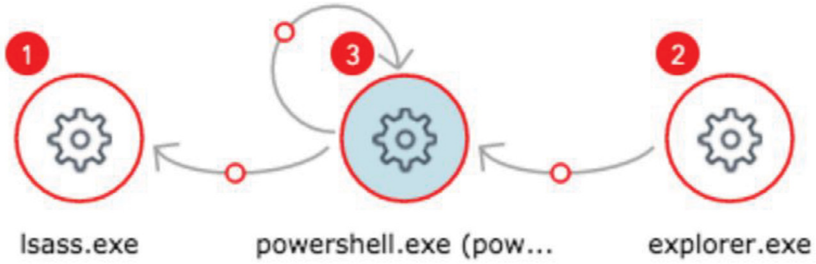
Actions on Objectives

Finally, APTs are characterized by taking control of the environment, moving laterally, gathering sensitive and controlled data, and staying undetected for long periods. At a functional level, executing a mimikatz payload in memory would be one type of activity that a next generation endpoint security solution should detect.

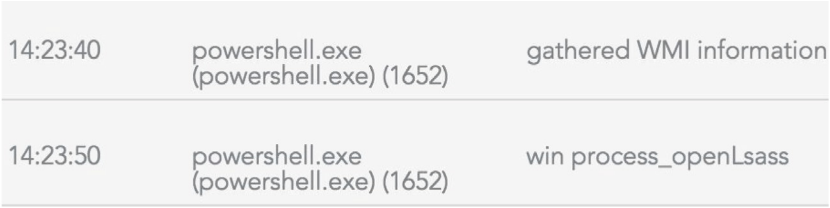


```
PS C:\Windows\system32> invoke-mimikatz

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 2015 19:16:34)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                   with 17 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 8764159 (00000000:0085baff)
Session           : Interactive from 1
User Name         : TestUserP1
Domain            : S1LABS
Logon Server      : S1LABS
Logon Time        : 9/23/2016 8:38:56 AM
SID               : S-1-5-21-524897526-2928478176-4087832876-1000
        msv :
         [00000003] Primary
```

Invoking mimikatz on a system



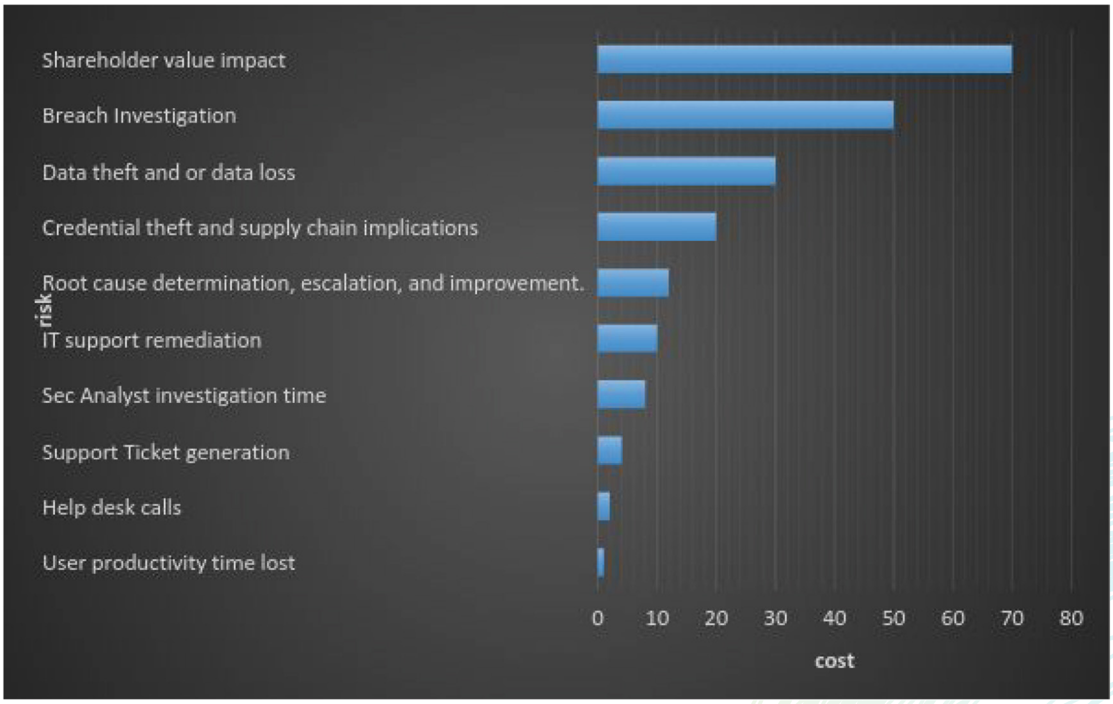
What Invoking Mimikatz locally looks like to a next gen endpoint security solution



14:23:40	powershell.exe (powershell.exe) (1652)	gathered WMI information
14:23:50	powershell.exe (powershell.exe) (1652)	win process_openLsass

Cost Factors

Individuals who choose to invest in next generation endpoint protection must select from two cost factors. First, when security solutions fail, the results cost an average of four million dollars[6]. The further along in the kill chain, the more intensive these penalties tend to become.



Secondly, protection itself costs money. Defense-in-depth means that companies need to have a firewall, IDS/IPS, antivirus, a SIEM, a security operations centre, and more. These costs add up. The separate components are expensive, but one must also consider the expense of integration, maintenance, and personnel.

Next generation endpoint security refutes the idea that defense must rely on expensive separate components. While traditional endpoint protection only covers two phases of the kill chain, its next-gen successor is active at nearly every point. As opposed to multiple layers of static defense, the next-gen solution is elastic.

To Evade the Pitfalls of the Kill Chain, Prepare for Turbulence

Turbulence is the concept that the functioning of endpoint security must not degrade in the real world, where chaotic and unpredictable things happen. Here are some real-world examples:

- A user plugs a USB into the laptop on the plane, in flight mode, and the system is not able to connect to the cloud to verify the files.
- IT support switches off a vital component feature because the sales team complain their system stops responding with it switched on.
- Threat actors move to a Java-based RAT because efficacy testing was done only on Windows executables.

The real world is chaotic. Administrators must be able to know that their endpoint protection solution will be effective—even if they're protecting flawed products and practices. No administrator can patch a standard enterprise to one-hundred percent readiness. Therefore, endpoint protection must function perfectly in less-than-perfect environments.

An acceptable AV solution must be able to flag reconnaissance attempts and pre-execution malware using cloud-intelligence. During the weaponization phase, the solution must be able to interrogate running processes in order to detect malicious activity.

The delivery and exploitation phase of the kill chain often occur faster than human administrators can respond. For this reason, an AV solution must do much of its work without human interaction—automatically mitigating threats. Since attackers often use novel methods, the solution must be effectively future-proof. No matter how ingenious the persistence mechanism, or how well-hidden the C2 channel, malware should not be able to escape notice.

Returning to the central principle of information security, the ultimate goal of endpoint protection is to reduce the number of systems infected, and the amount of time that those systems remain infected. Any AV solution must check many boxes to keep these metrics close to zero. The result, however, will be a network of endpoints and servers where hackers simply cannot gain a foothold.

For more information on SentinelOne, visit www.sentinelone.com. To schedule a demo tailored for your organization, visit www.sentinelone.com/contact.

Citations

1. www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
2. www.theregister.co.uk/2016/10/07/smash_and_grab_pos_pwners_ready_with_prexmas_malware_update/
3. www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. pubsonline.informs.org/doi/10.1287/isre.2016.0644
5. https://www.scmagazine.com/malware-variants-and-spam-rates-skyrocket-in-october/article/572525/
6. www-03.ibm.com/security/data-breach/