invincea®

White Paper

Know Your Adversary:

An Adversary Model for Mastering Cyber-Defense Strategies

www.invincea.com

Contents

© Copyright 2015 Invincea, Inc. All rights reserved.

Executive Summary

Cybersecurity continues to grow as one of the hottest markets to invest in today, but remains one of the most misunderstood fields in information technology. The relentless headline-grabbing data breaches are causing unprecedented spending in cybersecurity technologies and people, which in turn is driving more new companies and investment in cybersecurity, launching ever more new products.

Lost in the mix of new technologies, approaches, and remarkably similar marketing is the engineering, science, and art in designing an enterprise security architecture that can withstand attacks from advanced adversaries.

To design an effective security architecture, you must first model your adversary and their tactics. For instance, if you design a castle and moat to keep out raiding barbarians, but do not realize the barbarians have canons that can breach castle walls from afar, then your architecture is wholly ineffective against the threat you face.

Previous attempts to model adversaries and enterprise defenses have been useful at a fairly abstract level. However, none developed adversarial playbooks that can be tested against defensive playbooks. We believe this missing element is crucial to understanding the range of adversary attacks that a given defensive posture will likely withstand, and those to which it – and the enterprise more broadly – remains unprotected.

In this paper, we present a reference adversarial model and sample playbooks used in adversarial campaigns. We also develop a defense model and defensive playbooks representative of different sized organizations. The model is extensible to accommodate new adversarial tactics as they evolve with time. Likewise, the defense model and playbooks are configurable to enable specific scenarios and gaming against different adversarial playbooks. Just as importantly, we recommend the consideration of cost in the model. This enables realistic defense modeling by allowing participants to gauge the impact of trading one technology or product for another, given budget constraints.

The goal of this paper is to provide a rational basis for architecting enterprise defenses to optimize protection against the most likely adversarial campaigns. By modeling adversarial playbooks and analyzing the coverage provided by various defense architectures, an enterprise security team can develop a clear understanding of the protection and gaps of each security architecture. The models included are configurable and extensible to match evolving threats and defensive postures. A companion website with a modeling and simulation tool is being developed to allow real-time configuration and simulation of attack playbooks, to estimate how well each architecture would withstand various attack scenarios.

© Copyright 2015 Invincea, Inc. All rights reserved.

1. Know Your Adversary: Adversarial Modeling

Many threat intelligence firms proudly announce campaigns they have detected against unwitting targets with colorful names ranging from pandas and kittens to unintelligible monikers. Other firms have simply numbered them.

Lost in this mix of cute adversary names and logos and the embellished marketing surrounding these campaigns is the vital question of whether a given adversary poses a real risk to your organization.

Therefore, it is critical to "know thy enemy" in order to properly architect and manage one's defenses. For instance, if you are a small business and have little of value to a nation-state adversary, it probably does not make sense to invest in technologies and people to defend against such actors. Likewise, if you hold dossiers on all federal employees and contractors with security clearances, you should invest in advanced threat protection technologies, people, and processes at a level commensurate with the threat and the consequence of losing such data. If your defenses don't reflect your adversary's objectives, budget, and tactics, you will probably suffer a material data breach at some point.

Several attempts at adversarial modeling are notable, including the Lockheed Martin Cyber Kill Chain (see below); Mandiant's version (a minor variation of the Lockheed Martin model); DoD Joint Publication 3-13, 2006; and MITRE's ATT&CK Matrix.

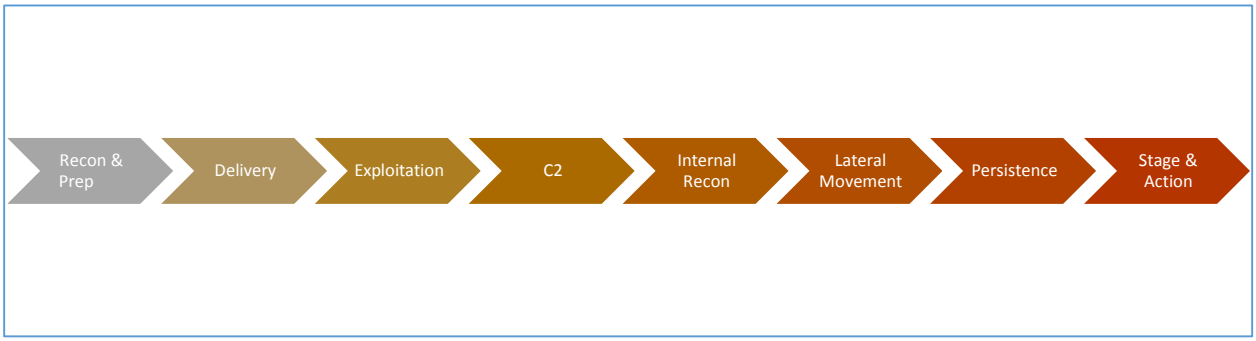

Figure 1: Lockheed Martin Cyber Kill Chain

The Cyber Kill Chain is useful for modeling a particular type of adversary – advanced persistent threat actors – and their campaign stages. The Kill Chain by itself is incomplete, however, and insufficient for engineering a defense strategy. It lacks detail regarding the adversary itself, and the adversary's objectives, tactics and techniques. Putting these together, we can begin to construct adversarial playbooks, which can be used to test defense strategies.

Adversary Model

We present here an adversary model with the following attributes:

- Adversary Type (AT)

© Copyright 2015 Invincea, Inc. All rights reserved.

- Campaign Objective (CO)
- Campaign Vehicle (CV)
- Campaign Weapon (CW)
- Payload Delivery (PD)
- Payload Capabilities (PC)

Each attribute is populated below with examples. The model is extensible as adversaries and their objectives and tactics evolve.

1.1 Adversary Type (AT)

Select one:

1. Script kiddy
2. Hacktivist, hacking collectives
3. Insider threat
4. Cyber terrorist
5. Commercial hacking (for theft of IP, customer data, etc.)
6. Cyber-crime
7. Nation-state intelligence agency
8. Nation-state cyber warfare

1.2 Campaign Objective (CO)

Select one or more:

1. Account take-over
2. Botnet farming
3. Identify fraud
4. Data control for extortion
5. Wire fraud
6. DDOS
7. Click-fraud
8. Data record theft
9. Intellectual property theft
10. Intelligence collection
11. Data munging
12. Data destruction
13. System destruction
14. Corporate shaming/political agenda

1.3 Campaign Vehicle (CV)

Select one:

1. Spear-phish with link/attachment
2. Compromised legitimate website
3. Malicious website
4. Malvertising
5. Social engineering

© Copyright 2015 Invincea, Inc. All rights reserved.

6. Insider threat
7. Remote login
8. Physical media (USB/DVD)
9. Supply chain

1.4 Campaign Weapon (CW)

Select one or more:

1. IE, Firefox, Chrome exploit
2. Adobe Flash exploit
3. Oracle Java exploit
4. Microsoft Silverlight exploit
5. Microsoft Office macro
6. Adobe Reader exploit
7. User-installed malware
8. Socially engineered remote access

1.5 Payload Delivery (PD)

Select one or more:

1. Executable file – pre-assembled
2. Executable file – just-in-time assembly on-host
3. Process hijacking/ROP
4. Scripting
5. DLL injection/side-loading

1.6 Payload Capabilities (PC)

Select one or more:

1. Backdoor for remote access
2. Privilege escalation
3. Keystroke logging
4. Screen capture
5. Browser data munging
6. Ransomware
7. Adware, click-jacking
8. Network mapping
9. Lateral movement
10. Command and control
11. DDOS
12. Data discovery
13. Data archiving
14. Data exfiltration
15. Data corruption
16. Data destruction
17. System wiping
18. Patching known vulnerabilities

© Copyright 2015 Invincea, Inc. All rights reserved.

2. Enterprise Security Modeling

Now that we have an understanding of adversary types and tactics, we can model enterprise defenses. The NIST Cyber Security Framework (CSF) shown in Figure 2 is rapidly gaining acceptance within both the federal and commercial segments.

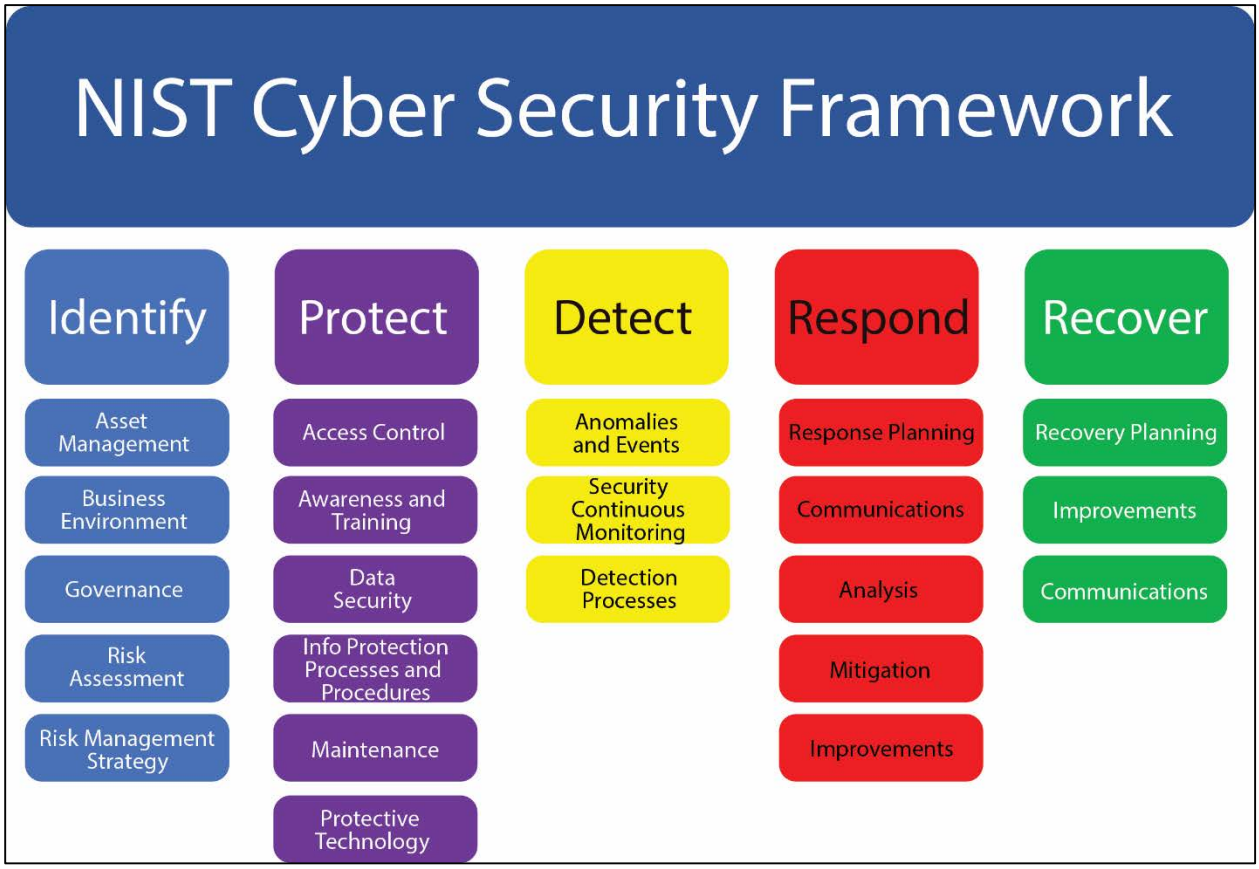

Figure 2: NIST Cyber Security Framework

The NIST CSF is a way of thinking about defense activities. Like the Cyber Kill Chain, it is a broad model on which to organize defense strategies. However, it does not provide guidance for enterprise security architectures. The framework also lacks any view of adversaries or adversarial playbooks. In other words, the model is built at a higher level and does not address the adversary model.

Since our goal is to realistically model a defense architecture against the attacks that enterprises are likely to experience, we represent enterprise architectures at a level of detail that is useful for simulating against adversarial playbooks.

© Copyright 2015 Invincea, Inc. All rights reserved.

We define an enterprise security architecture in three primary categories:

- Perimeter network defenses
- Endpoint defenses
- Response and recovery

The perimeter and endpoint defenses are designed to detect and rapidly stop threats, while response and recovery is intended to respond to compromises.

Enterprise Security Architecture

2.1 Perimeter Network Defenses

1. Firewall, router (standard and next-generation)
2. Web proxy, data loss prevention filtering
3. Network intrusion detection (IDS) or prevention (IPS) system
4. Network sandbox
5. Email security
6. Log aggregation, log analysis, SIEM
7. Command and control monitoring
8. Threat intelligence, threat aggregation

2.2 Endpoint Defenses

1. Asset discovery, patch management & configuration
2. Anti-virus (standard and next-generation)
3. White-listing, application control, system integrity monitoring
4. Containerization
5. Multi-factor authentication, PIV/CAC authorization
6. Data/disk encryption
7. Privilege management
8. Secure remote access/VPN
9. Anomaly detection / behavioral monitoring
10. Data loss prevention

2.3 Response and Recovery

1. SOC response orchestration
2. Endpoint breach query & confirmation
3. Endpoint quarantine
4. Endpoint forensics collection
5. Malware analysis
6. Endpoint re-image, remediate
7. Endpoint back-up restoration

In Figure 3, we map this enterprise security architecture to the NIST Cyber Security Framework (CSF). In addition, we provide example of vendors in each architecture category.

© Copyright 2015 Invincea, Inc. All rights reserved.

NIST Cyber Security Framework		Enterprise Defense Controls	Product Vendors
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Cisco, Check Point, Sophos, Intel McAfee
	1.1.2	- Next Generation	Palo Alto Networks
	1.2	Web Proxy Filtering, DLP	Blue Coat, Websense, Zscaler, Vontu
Detect	1.3	Network IDS	Cisco Sourcefire
	1.4	Network Sandbox	FireEye, Palo Alto, LastLine, Cyphort, McAfee
	1.5	Email Gateway Security	ProofPoint
	1.6	Log Aggregation, SIEM, Log Analysis	HP ArcSight, IBM QRadar, LogRhythm, Splunk
	1.7	Command and Control Monitoring	Damballa, FireEye
	1.8	Threat Intelligence, Threat Aggregation	iSIGHT Partners, ThreatStream
	2	**Endpoint Security Defenses**	
Identify	2.1	Asset Discovery, Patch Management, Configuration	Microsoft, IBM BigFix, Symantec Altiris, Tanium
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, McAfee, Trend Micro, Sophos
	2.2.2	- Next Generation AV (machine learning)	Cylance
	2.3	White-listing, App Control, Integrity Monitoring	Bit9, Microsoft, Tripwire
	2.4	Containerization	Invincea, Bromium
	2.5	Multi-factor Authentication, PIV/CAC	RSA, CA, Symantec
	2.6	Data/disk Encryption	Intel McAfee, Symantec, Sophos
	2.7	Privilege Management	
	2.8	Secure Remote Access/VPN	Cisco, RSA
Detect	2.9	Process Monitoring/Anomaly Detection	Invincea, CrowdStrike, Cybereason, CounterTack, Microsoft EMET, Palo Alto TRAPS
	2.10	Data Loss Prevention	Vontu, Digital Guardian
		3. Response and Recovery	
Respond	3.1	SOC Response Orchestration	CSG Invotas
	3.2	Endpoint Breach Query & Confirmation	FireEye Mandiant, Tanium
	3.3	Endpoint Quarantine/Isolation	Invincea, FireEye Mandiant
	3.4	Endpoint Forensics Collection	RSA ECAT, Carbon Black, Guidant, EnCase
	3.5	Malware Analysis	Invincea, EnCase, Cisco ThreatGrid, Cuckoo
Recover	3.6	Endpoint Re-imaging, Remediation	Ghost, Tanium
	3.7	Endpoint Data & System Restoration	Code42

Figure 3: Enterprise Security Architecture with NIST CSF Mapping

The enterprise security architecture model is extensible to other controls, with the listed product vendors being a representative set, not a complete list. By considering cost as well, enterprises can begin to optimize defenses against threats given a specific annual budget.

Since a single enterprise architecture will not apply to all enterprises, we define four target types (TT):

1. Individual / home
2. Small business / federal agency / military base
3. Mid-size business / federal agency / military command
4. Large business / federal department / military service

These are organized roughly by the resources each organization type can commit to defenses.

© Copyright 2015 Invincea, Inc. All rights reserved.

3. Adversarial Playbooks

Now that we have defined adversarial and defensive security models, we can construct adversarial playbooks to "run" against defensive playbooks.

Adversaries have inherent advantages over defenders, given their broader freedom to operate. Adversaries can choose the target, the timing of their attack, and the range of tactics used in a particular campaign.

Defenders, on the other hand, typically do not know who will attack, when, or what tactics are likely to be used against them. Most notably, while the adversary can be extremely agile in picking targets and methods, the defender must operate with a largely fixed infrastructure based on prior years' cybersecurity investments and current corporate/IT policies.

3.1 Developing an Adversarial Playbook

When launching a campaign, the threat actor uses an adversarial playbook, whether formal and explicit, or a learned method that has been practiced over time. These playbooks are likely to change based on objective and target.

3.1.1 Adversarial Playbook Template

We define an adversarial playbook with the following information:

1. Adversary type
2. Target (organization) type
3. Campaign objective
4. Campaign vehicle
5. Campaign weapon
6. Payload delivery
7. Payload capabilities

Figure 4 shows an example playbook that a nation-state intelligence agency might run in a campaign against a mid-size federal agency.

© Copyright 2015 Invincea, Inc. All rights reserved.

Playbook 3	Nation-State Intelligence Collection		
	Adversary Type	AT 7	Nation-state intelligence agency
	Target type	TT 3	Mid-size federal agency
	Campaign Objective	CO 8	Data record theft (capture employee records)
	Campaign Vehicle	CV 1, 2	Spear-phish; compromised legitimate website
	Campaign Weapon	CW 2	Adobe Flash exploit (unknown, 0-day) via IE
	Payload Delivery	PD 2	Executable file – just-in-time assembly on-host
	Payload Capabilities	PC 1, 2, 8, 9, 10, 12, 13, 14, 18	Backdoor, pivot, data collection, exfiltration
Recon & Prep	Step 1	Identify target by mission objective and employee emails	
Delivery	Step 2	Send spear-phish campaign to 30 users [CV 1]	
Delivery	Step 3	Redirect clicked links to compromised vacation website [CV 2]	
Exploitation	Step 4	Exploit Flash (via IE); download code chunks; re-assemble [CW 2, PD 2]	
Exploitation	Step 5	Drop unknown executable mission package [PC 1, 2]	
C2	Step 6	Command and control to mission team [PC 10]	
Internal Recon	Step 7	Identify other machines on network [PC 8]	
Lateral Movement	Step 8	Compromise other machines on network [PC 9]	
Persistence	Step 9	Persist by closing known vulnerabilities, infecting other machines [PC 18, 9]	
Stage & Action	Step 10	Find data, archive, exfiltrate [PC 12, 13, 14]	

Figure 4: Nation-state intelligence agency playbook against mid-size federal agency

The playbook references the Cyber Kill Chain model and shows each of the steps involved in the campaign. Note the playbook highlights the freedom the adversary has in choosing the attack tactics.

As another example, Figure 5 shows a playbook that a cyber-crime gang might employ in a campaign against a small business, where the objective is wire fraud on payroll day.

Playbook 2	Cyber-Crime		
	Adversary Type	AT 6	Cyber-crime
	Target type	TT 2	Small business
	Campaign Objective	CO 5	Wire fraud
	Campaign Vehicle	CV 1	Spear-phish, with attachment
	Campaign Weapon	CW 5	Office macro
	Payload Delivery	PD 1, 5	Executable download (unknown malware); DLL side-loading
	Payload Capabilities	PC 3, 4, 5, 10, 14	Keystroke logging, screen capture, browser data munging, data exfil
Recon & Prep	Step 1	Identify target by purchased list	
Delivery	Step 2	Send spear-phish email [CV 1]	
Exploitation	Step 3	Run macro, drop executable, load DLL in browser [CW 5, PD 1, PD 5]	
C2	Step 4	Command and control to botnet server [PC 10]	
Stage & Action	Step 5	Alert when wire transfer occurs [PC 3, 4]	
Stage & Action	Step 6	Change account info & transfer funds to adversary account [PC 5]	

Figure 5: Cyber-crime gang playbook against small business

In this playbook, there are fewer steps and different tactics involved. The particular tactics the adversary uses of course can be changed either to reflect current exploit kits or successive attempts to breach the target.

4. Defensive Playbooks

As noted earlier, adversaries have more freedom to operate than defenses. Defense teams' playbooks are therefore more constrained and less agile than those employed by adversaries.

© Copyright 2015 Invincea, Inc. All rights reserved.

Some example playbooks for defense are given below.

Playbook 2	TT 2: Small Business		
		Enterprise Defense Controls	**Product Vendors**
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Cisco, Check Point, Sophos, Intel McAfee
	1.2	Web Proxy Filtering, DLP	Blue Coat, Websense, Zscaler, Vontu
	2	**Endpoint Security Defenses**	
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, McAfee, Trend Micro, Sophos
	2.5	Multi-factor Authentication, PIV/CAC	RSA, CA, Symantec
	2.6	Data/disk Encryption	Intel McAfee, Symantec, Sophos
	2.8	Secure Remote Access/VPN	Cisco, RSA
	3	**Response and Recovery**	
Recover	3.6	Endpoint Re-imaging, Remediation	Ghost, Tanium
	3.7	Endpoint Data & System Restoration	Code42

Figure 6: Small business playbook

Playbook 3	TT 3: Mid-size business / federal agency / military command		
		Enterprise Defense Controls	**Product Vendors**
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Cisco, Check Point, Sophos, Intel McAfee
	1.1.2	- Next Generation	Palo Alto Networks
	1.2	Web Proxy Filtering, DLP	Blue Coat, Websense, Zscaler, Vontu
Detect	1.3	Network IDS	Cisco Sourcefire
	1.4	Network Sandbox	FireEye, Palo Alto, LastLine, Cyphort, McAfee
	1.5	Email Gateway Security	ProofPoint
	1.6	Log Aggregation, SIEM, Log Analysis	HP ArcSight, IBM QRadar, LogRhythm, Splunk
	1.7	Command and Control Monitoring	Damballa, FireEye
	2	**Endpoint Security Defenses**	
Identify	2.1	Asset Discovery, Patch Management, Configuration	Microsoft, IBM BigFix, Symantec Altiris, Tanium
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, McAfee, Trend Micro, Sophos
	2.4	Containerization	Invincea, Bromium
	2.5	Multi-factor Authentication, PIV/CAC	RSA, CA, Symantec
	2.6	Data/disk Encryption	Intel McAfee, Symantec, Sophos
	2.7	Privilege Management	
	2.8	Secure Remote Access/VPN	Cisco, RSA
	3	**Response and Recovery**	
Respond	3.2	Endpoint Breach Query & Confirmation	FireEye Mandiant, Tanium
	3.3	Endpoint Quarantine/Isolation	Invincea, FireEye Mandiant
	3.4	Endpoint Forensics Collection	RSA ECAT, Carbon Black, Guidant, EnCase
Recover	3.6	Endpoint Re-imaging, Remediation	Ghost, Tanium
	3.7	Endpoint Data & System Restoration	Code42

Figure 7: Mid-size business / federal agency / military command playbook

These playbooks are configurations of the enterprise security architecture presented in

© Copyright 2015 Invincea, Inc. All rights reserved.

Section 2, and are of course configurable to any particular enterprise's current or aspirational architecture.

5. Let's Play a Game

Now that we have defined Adversarial Playbooks and Defensive Playbooks, and have a model from which these playbooks can be created, it is straightforward to run a simulated "game" and see how a particular defensive playbook fares against a given adversarial playbook.

The most effective way to determine the outcome of a simulated attack is to develop attack coverage maps by defense technology types. Figure 8 shows an attack coverage map with a set of offensive tactics listed across the top and a set of defensive technologies down the side. Each defensive technology – and each playbook of multiple technologies – has coverage gaps against different adversarial tactics. For example, if an adversarial playbook involved a watering hole attack with file-less scripting, then the adversary would win against this example playbook.

Defense Control	Example Vendor	Ping Recon	Spear-Phish with Link	Watering Hole Attack	Malvertising with 0-Day	Known Malware	Unknown Malware	File-less Scripting	Malicious Office Macro
Standard Firewall	Cisco	◆	◆						
Web Proxy	Blue Coat		◆			◆			
Network IDS	Cisco Sourcefire		◆			◆			
Network Sandbox	FireEye		◆			◆			
Email Gateway Security	ProofPoint		◆						
SIEM	HP ArcSight								
Threat Intelligence	iSIGHT		◆						
Standard Anti-virus	Intel McAfee					◆			
Next-Gen Anti-virus	Cylance					◆	◆		
Patch Management	IBM BigFix								
App Whitelisting	Bit9					◆	◆		
Breach Confirmation	FireEye Mandiant					◆			

Figure 8: Attack coverage map of security technologies and adversarial tactics

If an enterprise is concerned about an adversarial playbook employing any of the tactics in

© Copyright 2015 Invincea, Inc. All rights reserved.

Figure 8 for which there is no current coverage, then the defensive playbook will need to add additional technologies for these tactics.

Figure 9 shows another sample coverage map with additional defensive technologies to cover these adversarial tactics.

Defense Control	Example Vendor	Ping Recon	Spear-Phish with Link	Watering Hole Attack	Malvertising with 0-Day	Known Malware	Unknown Malware	File-less Scripting	Malicious Office Macro
Standard Firewall	Cisco	◆	◆						
Web Proxy	Blue Coat		◆			◆			
Network IDS	Cisco Sourcefire		◆			◆			
Network Sandbox	FireEye		◆			◆			
Email Gateway Security	ProofPoint		◆						
SIEM	HP ArcSight								
Threat Intelligence	iSIGHT		◆						
Standard Anti-virus	Intel McAfee					◆			
Next-Gen Anti-virus	Cylance					◆	◆		
Patch Management	IBM BigFix								
App Whitelisting	Bit9					◆	◆		
Breach Confirmation	FireEye Mandiant					◆			
Process Monitoring / Anomaly Detection	Invincea		◆	◆	◆	◆	◆	◆	◆
Containerization	Invincea		◆	◆	◆	◆	◆	◆	◆

Figure 9: Attack coverage map with advanced threat protection on endpoints

Note in Figure 9 that with endpoint containerization and process monitoring capabilities, the coverage map now protects against additional tactics in this adversary's playbook.

The attack coverage maps shown above are a simplified approach to defining likely outcomes for adversarial tactics. The model can be refined to allow non-binary coverage maps, for example using probability distributions for attack coverage given a particular defense control. For instance, a Flash exploit might or might not succeed depending on whether the target

© Copyright 2015 Invincea, Inc. All rights reserved.

machine is patched for that vulnerability. This can be represented by a probability distribution that can be parameterized.

For clarity, however, we use a simplified model in this paper to run some game scenarios.

5.1 Game 1: Miscreant Hacker vs. Home User

To illustrate how to test adversarial playbooks against defensive playbooks, we run two scenarios. In Game 1, we take a less capable actor working against a not well-defended home user.

The adversarial playbook and defensive playbook are shown in Figure 10 below.

Playbook 1	**AT1: Miscreant hacker**			
	Adversary Type	AT 1	Script kiddie	
	Target type	TT 1	Individual/home user	
	Campaign Objective	CO 1	Account take-over	
	Campaign Vehicle	CV 1, 3	Spear-phish, malicious link	
	Campaign Weapon	CW 2	Flash exploit (known, unpatched)	
	Payload Delivery	PD 1	Executable download (unknown)	
	Payload Capabilities	PC 3, 10, 14	Keystroke logging, C2, data exfiltration	
Recon & Prep	Step 1	Identify target by purchased list		
Delivery	Step 2	Send spear-phish email [CV 1]		
Delivery	Step 3	Redirect to malicious webpage [CV 3]		
Exploitation	Step 4	Exploit, Download & run executable [CW 2, PD 1]		
Exploitation	Step 5	Capture keystrokes when visiting banking sites [PC 3]		
C2	Step 6	Command and control to botnet server [PC 10]		
Stage & Action	Step 7	Exfiltrate account information [PC 14]		

VS.

Playbook 1	**TT 1: Individual/Home user**			
		Enterprise Defense Controls	**Product Vendors**	
	1	**Perimeter Network Defenses**		
Protect	1.1	Firewall, Router		
	1.1.1	- Standard	Broadband provider (cable router)	
	2	**Endpoint Security Defenses**		
Protect	2.2	Anti-virus		
	2.2.1	- Standard AV (signature-based)	Symantec, Intel McAfee	

Figure 10: Adversarial playbook vs defensive playbook for simple adversary and not well-defended user

Using the simplified attack coverage map in Figure 11, we see the adversary wins this battle.

© Copyright 2015 Invincea, Inc. All rights reserved.

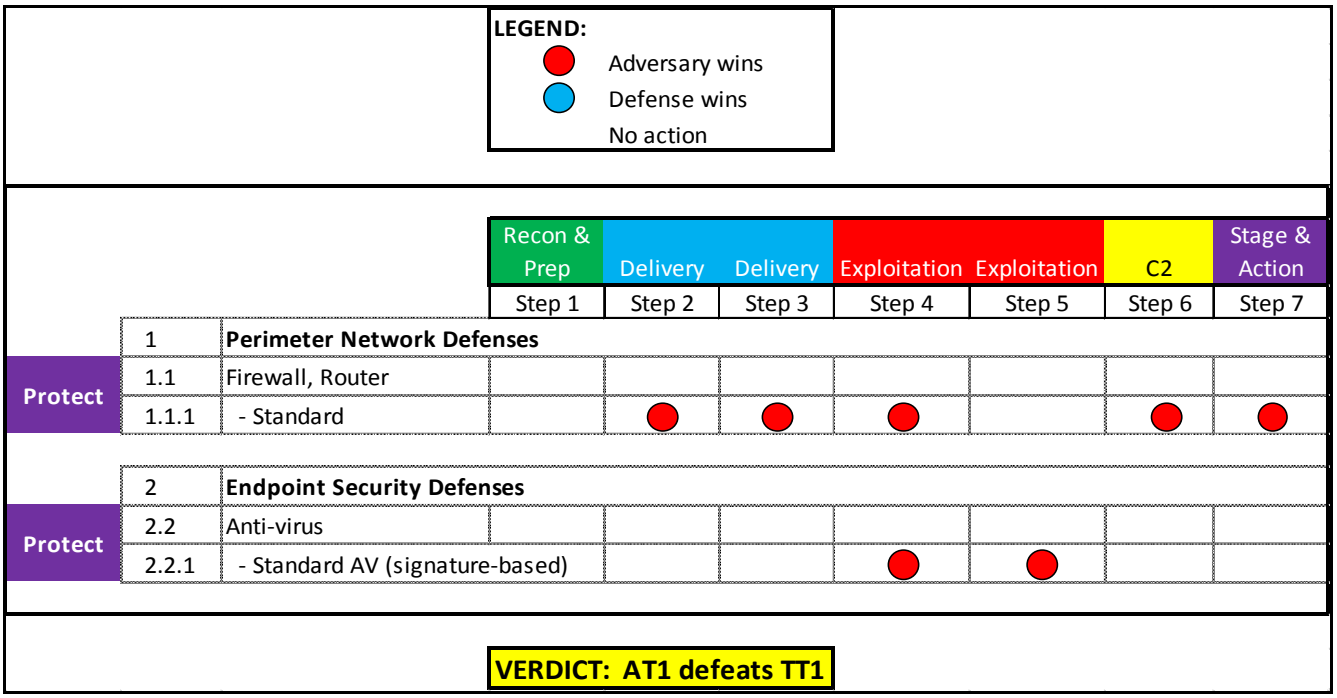

Figure 11: Running the game for the adversarial playbook and defensive playbook in Figure 10

The game takes place as the series of steps in the adversarial playbook, which are compared to the defensive playbook at each step. These steps are linked in the Cyber Kill Chain shown above. Stopping the attack at any step along the way breaks the intrusion chain and kills the attack. In Figure 11, the adversary wins at each step and therefore succeeds in the objective of account take-over.

5.2 Game 2: Nation-State Intelligence Agency vs. Mid-Size Federal Agency

The next game shows a more sophisticated adversary – a nation-state intelligence agency – running a campaign (playbook) against a mid-size federal agency.

Figure 12 shows an adversarial playbook for this actor and campaign. Note how the steps in this adversarial playbook map to the Cyber Kill Chain, with the objective of discovering and exfiltrating employee records stored by the targeted federal agency.

Below the adversarial playbook is the defensive playbook for this mid-size federal agency. The network, endpoint, and response architecture are shown, along with the particular controls employed in this sample defensive playbook. Naturally, the selection of the particular playbooks on offense and defense is completely flexible. As mentioned earlier, adversaries can change their playbooks much more easily and quickly, while defenders are limited in how often and quickly they can change their controls and configurations.

© Copyright 2015 Invincea, Inc. All rights reserved.

Playbook 3	Nation-State Intelligence Collection		
	Adversary Type	AT 7	Nation-state intelligence agency
	Target type	TT 3	Mid-size federal agency
	Campaign Objective	CO 8	Data record theft (capture employee records)
	Campaign Vehicle	CV 1, 2	Spear-phish; compromised legitimate website
	Campaign Weapon	CW 2	Adobe Flash exploit (unknown, 0-day) via IE
	Payload Delivery	PD 2	Executable file – just-in-time assembly on-host
	Payload Capabilities	PC 1, 2, 8, 9, 10, 12, 13, 14, 18	Backdoor, pivot, data collection, exfiltration
Recon & Prep	Step 1	Identify target by mission objective and employee emails	
Delivery	Step 2	Send spear-phish campaign to 30 users [CV 1]	
Delivery	Step 3	Redirect clicked links to compromised vacation website [CV 2]	
Exploitation	Step 4	Exploit Flash (via IE); download code chunks; re-assemble [CW 2, PD 2]	
Exploitation	Step 5	Drop unknown executable mission package [PC 1, 2]	
C2	Step 6	Command and control to mission team [PC 10]	
Internal Recon	Step 7	Identify other machines on network [PC 8]	
Lateral Movement	Step 8	Compromise other machines on network [PC 9]	
Persistence	Step 9	Persist by closing known vulnerabilities, infecting other machines [PC 18, 9]	
Stage & Action	Step 10	Find data, archive, exfiltrate [PC 12, 13, 14]	

VS.

Playbook 3	TT 3: Mid-size business / federal agency / military command		
		Enterprise Defense Controls	**Product Vendors**
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Cisco, Check Point, Sophos, Intel McAfee
	1.1.2	- Next Generation	Palo Alto Networks
	1.2	Web Proxy Filtering, DLP	Blue Coat, Websense, Zscaler, Vontu
Detect	1.3	Network IDS	Cisco Sourcefire
	1.4	Network Sandbox	FireEye, Palo Alto, LastLine, Cyphort, Intel McAfee
	1.5	Email Gateway Security	ProofPoint
	1.6	Log Aggregation, SIEM, Log Analysis	HP ArcSight, IBM QRadar, LogRhythm, Splunk
	1.7	Command and Control Monitoring	Damballa, FireEye
	2	**Endpoint Security Defenses**	
Identify	2.1	Asset Discovery, Patch Management, Configuration	Microsoft, IBM BigFix, Symantec Altiris, Tanium
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, Intel McAfee, Trend Micro, Sophos
	2.4	Containerization	Invincea, Bromium
	2.5	Multi-factor Authentication, PIV/CAC	RSA, CA, Symantec
	2.6	Data/disk Encryption	Intel McAfee, Symantec, Sophos
	2.7	Privilege Management	
	2.8	Secure Remote Access/VPN	Cisco, RSA
	3	**Response and Recovery**	
Respond	3.2	Endpoint Breach Query & Confirmation	FireEye Mandiant, Tanium
	3.3	Endpoint Quarantine/Isolation	Invincea, FireEye Mandiant
	3.4	Endpoint Forensics Collection	RSA ECAT, Carbon Black, Guidant, EnCase
Recover	3.6	Endpoint Re-imaging, Remediation	Ghost, Tanium
	3.7	Endpoint Data & System Restoration	Code42

Figure 12: Nation-state intelligence agency vs. US federal mid-size agency

© Copyright 2015 Invincea, Inc. All rights reserved.

Now we can "game" a match between these two playbooks and see how well the defense fares against this adversarial playbook.

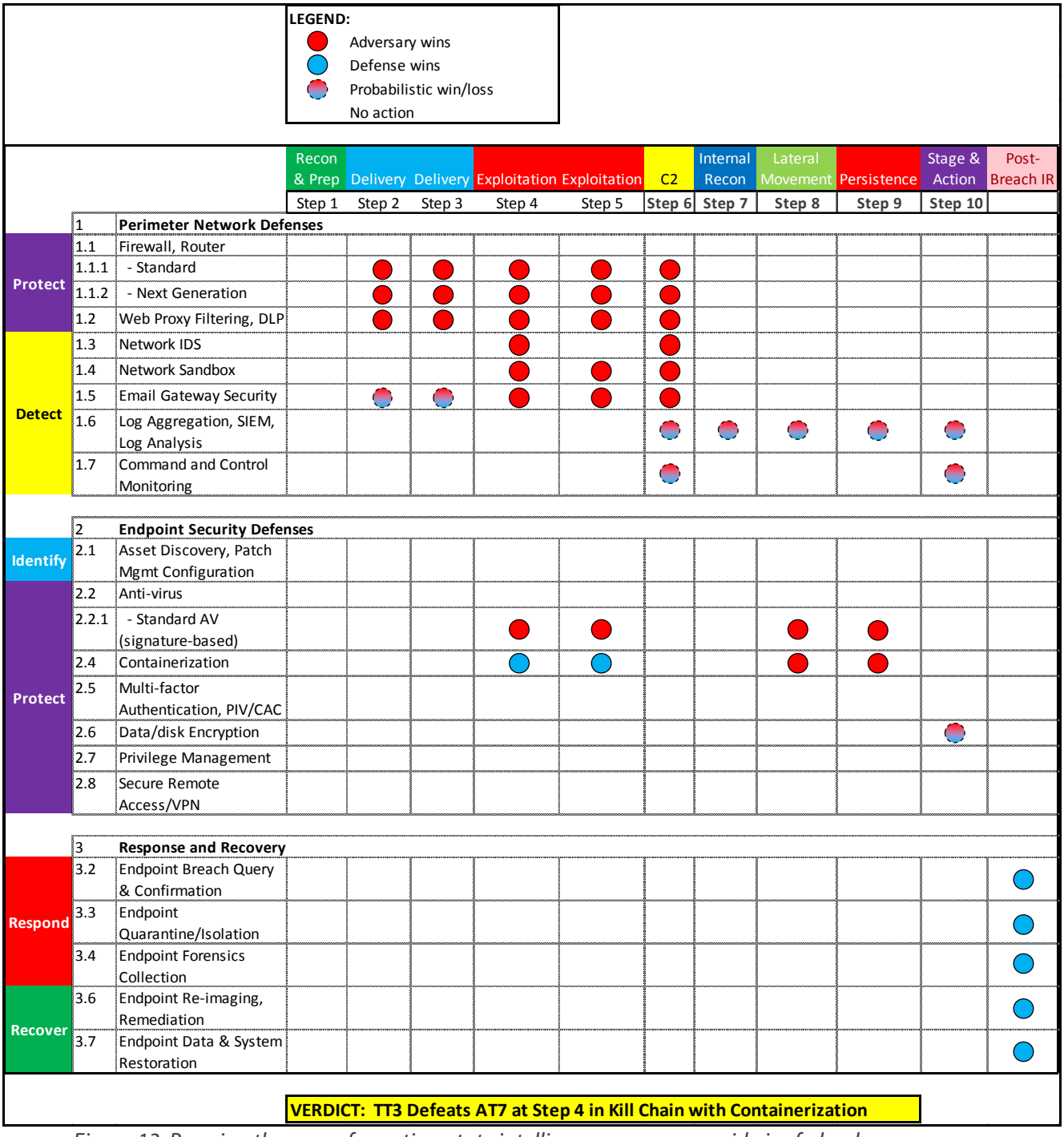

Figure 13: Running the game for nation-state intelligence agency vs. mid-size federal agency

The result of simulating this nation-state campaign against the mid-size federal agency with this defensive playbook is shown in Figure 13. Note we model probabilistic coverage of some

© Copyright 2015 Invincea, Inc. All rights reserved.

of the attack space with some of the defensive controls, where indicated by the gradient-shaded circles.

In this example, the defensive playbook defeated the adversarial campaign playbook because endpoint containerization in Steps 4 and 5 broke the kill chain – *defense wins!*

6. Conclusions

Enterprise security architects have long lacked a formal model for making sound architectural choices. Security in the absence of an adversarial model and attack coverage map is grasping in the dark at best. All too often enterprise security architects buy what they are sold or what seems the latest hot product based on marketing and word of mouth. As a result, security leaders can make uninformed choices and, even worse, remain unaware of their exposed attack surface and risk of breach.

In this paper, we have presented a model for offense and defense strategies that allows enterprise architects to analyze how an architecture or choice of security controls addresses the threats their enterprises are likely to face. By considering cost in the model, a security team can see the protection impact of trading one technology for another, given a limited budget. For instance, when adversaries move to an attack model featuring Just-in-Time Malware Assembly that evades solutions such as network sandboxing, as they did in the first half of 2015, the defense model can be adjusted to adopt a solution that defeats this tactic, subject to budget constraints.

The Invincea model references established frameworks including the Lockheed-Martin Cyber Kill Chain and the NIST Cyber Security Framework, for both offensive and defensive strategies. However, we have extended these to develop specific playbooks and an approach for running the playbooks against each other in a simulated game to determine likely outcomes.

Community involvement is welcomed and will be applied to generate more playbooks and continue to capture new adversary tactics as they evolve.

A companion web-based simulation tool is being developed that will allow information security teams to configure their current or aspirational architectures, select one or more adversary types, and then run simulations from randomly selected adversarial playbooks to understand how well their architectures defend against those playbooks. Organizations can then use this insight to make informed architectural choices to defend against the most relevant and significant threats they face. It is Invincea's hope that this model and tool will bring clarity to the challenge of building a sound enterprise security architecture.

© Copyright 2015 Invincea, Inc. All rights reserved.

7. Appendix

7.1 Adversary Playbooks

Playbook 1	Miscreant hacker			
	Adversary Type	AT 1	Script kiddie	
	Target type	TT 1	Individual/home user	
	Campaign Objective	CO 1	Account take-over	
	Campaign Vehicle	CV 1, 3	Spear-phish, malicious link	
	Campaign Weapon	CW 2	Flash exploit (known, unpatched)	
	Payload Delivery	PD 1	Executable download (unknown)	
	Payload Capabilities	PC 3, 10, 14	Keystroke logging, C2, data exfiltration	
Recon & Prep	Step 1	Identify target by purchased list		
Delivery	Step 2	Send spear-phish email [CV 1]		
Delivery	Step 3	Redirect to malicious webpage [CV 3]		
Exploitation	Step 4	Exploit, Download & run executable [CW 2, PD 1]		
Exploitation	Step 5	Capture keystrokes when visiting banking sites [PC 3]		
C2	Step 6	Command and control to botnet server [PC 10]		
Stage & Action	Step 7	Exfiltrate account information [PC 14]		

Playbook 2	Cyber-Crime			
	Adversary Type	AT 6	Cyber-crime	
	Target type	TT 2	Small business	
	Campaign Objective	CO 5	Wire fraud	
	Campaign Vehicle	CV 1	Spear-phish, with attachment	
	Campaign Weapon	CW 5	Office macro	
	Payload Delivery	PD 1, 5	Executable download (unknown malware); DLL side-loading	
	Payload Capabilities	PC 3, 4, 5, 10, 14	Keystroke logging, screen capture, browser data munging, data exfil	
Recon & Prep	Step 1	Identify target by purchased list		
Delivery	Step 2	Send spear-phish email [CV 1]		
Exploitation	Step 3	Run macro, drop executable, load DLL in browser [CW 5, PD 1, PD 5]		
C2	Step 4	Command and control to botnet server [PC 10]		
Stage & Action	Step 5	Alert when wire transfer occurs [PC 3, 4]		
Stage & Action	Step 6	Change account info & transfer funds to adversary account [PC 5]		

© Copyright 2015 Invincea, Inc. All rights reserved.

Playbook 3	Nation-State Intelligence Collection		
	Adversary Type	AT 7	Nation-state intelligence agency
	Target type	TT 3	Mid-size federal agency
	Campaign Objective	CO 8	Data record theft (capture employee records)
	Campaign Vehicle	CV 1, 2	Spear-phish; compromised legitimate website
	Campaign Weapon	CW 2	Adobe Flash exploit (unknown, 0-day) via IE
	Payload Delivery	PD 2	Executable file – just-in-time assembly on-host
	Payload Capabilities	PC 1, 2, 8, 9, 10, 12, 13, 14, 18	Backdoor, pivot, data collection, exfiltration
Recon & Prep	Step 1	Identify target by mission objective and employee emails	
Delivery	Step 2	Send spear-phish campaign to 30 users [CV 1]	
Delivery	Step 3	Redirect clicked links to compromised vacation website [CV 2]	
Exploitation	Step 4	Exploit Flash (via IE); download code chunks; re-assemble [CW 2, PD 2]	
Exploitation	Step 5	Drop unknown executable mission package [PC 1, 2]	
C2	Step 6	Command and control to mission team [PC 10]	
Internal Recon	Step 7	Identify other machines on network [PC 8]	
Lateral Movement	Step 8	Compromise other machines on network [PC 9]	
Persistence	Step 9	Persist by closing known vulnerabilities, infecting other machines [PC 18, 9]	
Stage & Action	Step 10	Find data, archive, exfiltrate [PC 12, 13, 14]	

Playbook 4	Nation-State Attack Against Oil Refinery		
	Adversary Type	AT 8	Nation-state cyber warfare unit
	Target type	TT 4	Large Business (Oil & Gas Production)
	Campaign Objective	CO 12, 13	Damage gasoline production capacity
	Campaign Vehicle	CV 2	Watering hole attack
	Campaign Weapon	CW 3	Java exploit (known, unpatched)
	Payload Delivery	PD 1	Executable download (encrypted payload)
	Payload Capabilities	PC 1, 2, 8, 9, 10, 12, 13, 14, 17	Backdoor, lateral movement, data discovery, exfil, system wiping
Recon & Prep	Step 1	Identify target by mission objective, set up watering hole [CV 2]	
Exploitation	Step 2	Exploit target's browser when visiting watering hole [CW 3]	
Exploitation	Step 3	Download & run executable, remote login [PD 1, PC 1, PC 2]	
C2	Step 4	Command and control to botnet server [PC 10]	
Internal Recon	Step 5	Identify other machines on network [PC 8]	
Lateral Movement	Step 6	Compromise other machines on network [PC 9]	
Persistence	Step 7	Persist by closing known vulnerabilities, infecting other machines [PC 18, 9]	
Stage & Action	Step 8	Find data, archive, exfiltrate [PC 12, 13, 14]	
Stage & Action	Step 9	Destroy data, wipe systems [PC 16, 17]	

© Copyright 2015 Invincea, Inc. All rights reserved.

7.2 Defense Playbooks

Playbook 1	TT 1: Individual/Home user		
		Enterprise Defense Controls	**Product Vendors**
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Broadband provider (cable router)
	2	**Endpoint Security Defenses**	
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, Intel McAfee

Playbook 2	TT 2: Small Business		
		Enterprise Defense Controls	**Product Vendors**
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Cisco, Check Point, Sophos, Intel McAfee
	1.2	Web Proxy Filtering, DLP	Blue Coat, Websense, Zscaler, Vontu
	2	**Endpoint Security Defenses**	
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, Intel McAfee, Trend Micro, Sophos
	2.5	Multi-factor Authentication, PIV/CAC	RSA, CA, Symantec
	2.6	Data/disk Encryption	Intel McAfee, Symantec, Sophos
	2.8	Secure Remote Access/VPN	Cisco, RSA
	3	**Response and Recovery**	
Recover	3.6	Endpoint Re-imaging, Remediation	Ghost, Tanium
	3.7	Endpoint Data & System Restoration	Code42

© Copyright 2015 Invincea, Inc. All rights reserved.

Playbook 3	TT 3: Mid-size business / federal agency / military command		
		Enterprise Defense Controls	**Product Vendors**
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Cisco, Check Point, Sophos, Intel McAfee
	1.1.2	- Next Generation	Palo Alto Networks
	1.2	Web Proxy Filtering, DLP	Blue Coat, Websense, Zscaler, Vontu
Detect	1.3	Network IDS	Cisco Sourcefire
	1.4	Network Sandbox	FireEye, Palo Alto, LastLine, Cyphort, Intel McAfee
	1.5	Email Gateway Security	ProofPoint
	1.6	Log Aggregation, SIEM, Log Analysis	HP ArcSight, IBM QRadar, LogRhythm, Splunk
	1.7	Command and Control Monitoring	Damballa, FireEye
	2	**Endpoint Security Defenses**	
Identify	2.1	Asset Discovery, Patch Management, Configuration	Microsoft, IBM BigFix, Symantec Altiris, Tanium
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, Intel McAfee, Trend Micro, Sophos
	2.4	Containerization	Invincea, Bromium
	2.5	Multi-factor Authentication, PIV/CAC	RSA, CA, Symantec
	2.6	Data/disk Encryption	Intel McAfee, Symantec, Sophos
	2.7	Privilege Management	
	2.8	Secure Remote Access/VPN	Cisco, RSA
	3	**Response and Recovery**	
Respond	3.2	Endpoint Breach Query & Confirmation	FireEye Mandiant, Tanium
	3.3	Endpoint Quarantine/Isolation	Invincea, FireEye Mandiant
	3.4	Endpoint Forensics Collection	RSA ECAT, Carbon Black, Guidant, EnCase
Recover	3.6	Endpoint Re-imaging, Remediation	Ghost, Tanium
	3.7	Endpoint Data & System Restoration	Code42

© Copyright 2015 Invincea, Inc. All rights reserved.

Playbook 4	TT 4: Large business / federal department / military service		
		Enterprise Defense Controls	**Product Vendors**
	1	**Perimeter Network Defenses**	
Protect	1.1	Firewall, Router	
	1.1.1	- Standard	Cisco, Check Point, Sophos, Intel McAfee
	1.1.2	- Next Generation	Palo Alto Networks
	1.2	Web Proxy Filtering, DLP	Blue Coat, Websense, Zscaler, Vontu
Detect	1.3	Network IDS	Cisco Sourcefire
	1.4	Network Sandbox	FireEye, Palo Alto, LastLine, Cyphort, Intel McAfee
	1.5	Email Gateway Security	ProofPoint
	1.6	Log Aggregation, SIEM, Log Analysis	HP ArcSight, IBM QRadar, LogRhythm, Splunk
	1.7	Command and Control Monitoring	Damballa, FireEye
	1.8	Threat Intelligence, Threat Aggregation	iSIGHT Partners, ThreatStream
	2	**Endpoint Security Defenses**	
Identify	2.1	Asset Discovery, Patch Management, Configuration	Microsoft, IBM BigFix, Symantec Altiris, Tanium
Protect	2.2	Anti-virus	
	2.2.1	- Standard AV (signature-based)	Symantec, Intel McAfee, Trend Micro, Sophos
	2.2.2	- Next Generation AV (machine learning)	Cylance
	2.3	White-listing, App Control, Integrity Monitoring	Bit9, Microsoft, Tripwire
	2.4	Containerization	Invincea, Bromium
	2.5	Multi-factor Authentication, PIV/CAC	RSA, CA, Symantec
	2.6	Data/disk Encryption	Intel McAfee, Symantec, Sophos
	2.7	Privilege Management	
	2.8	Secure Remote Access/VPN	Cisco, RSA
Detect	2.9	Process Monitoring/Anomaly Detection	Invincea, CrowdStrike, Cybereason, CounterTack, Microsoft EMET, Palo Alto TRAPS
	2.10	Data Loss Prevention	Vontu, Digital Guardian
	3	**Response and Recovery**	
Respond	3.1	SOC Response Orchestration	CSG Invotas
	3.2	Endpoint Breach Query & Confirmation	FireEye Mandiant, Tanium
	3.3	Endpoint Quarantine/Isolation	Invincea, FireEye Mandiant
	3.4	Endpoint Forensics Collection	RSA ECAT, Carbon Black, Guidant, EnCase
	3.5	Malware Analysis	Invincea, EnCase, Cisco ThreatGrid, Cuckoo
Recover	3.6	Endpoint Re-imaging, Remediation	Ghost, Tanium
	3.7	Endpoint Data & System Restoration	Code42

About Invincea

The company provides the most comprehensive solution to contain, identify, and control advanced attacks. Invincea protects enterprises against targeted threats, including spear-phishing and Web drive-by attacks. Combining the visibility and control of an endpoint solution with the intelligence of cloud analysis, Invincea defends against 0-day exploits, file-less malware, and previously unknown malware.

3975 University Drive, Suite 330, Fairfax, VA 22030 USA | Tel: 1-855-511-5967 | info@invincea.com | www.invincea.com

© 2015, Invincea, Inc. All rights reserved. Invincea and the Invincea Logo are trademarks of Invincea, Inc. All other product or company names may be trademarks of their respective owners. All specifications are subject to change without notice. Invincea assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document.

invincea®

Rev 1115

© Copyright 2015 Invincea, Inc. All rights reserved.