Detect, Respond, and Recover: The Most Critical Challenge to Cybersecurity T&E

Presented at the 32nd Annual International Test and Evaluation Symposium

John Schab

CISSP, GSEC, GCED, Security+

Systems Engineering Lead

MITRE Corporation

20 Aug 2015

MITRE

Terminology

- **Note for this presentation, the word "detect" means finding an unauthorized user/adversary on a system who has already successfully bypassed some/all defenses or finding unauthorized/malicious activity running on a system.**

- **In other words, "detect" is meant to mean discovering compromised system……not discovering an attacker who is attempting to compromise the system.**

- **In the NIST framework, the "detect" function is defined as identifying the occurrence of a cybersecurity event.**

BLUF

- **ALL systems have been, will be, and can be comprised by a determined attacker.**
- **Cybersecurity is a risk management exercise which is only partially about prevention.**
- **On average, the time it takes to detect, respond, and recover from a breach is unacceptable.**
- **Current T&E efforts are not resulting in systems with acceptable levels of cybersecurity risk.**
- **The greatest opportunity to reduce cybersecurity risk can be found in detect, respond, and recover.**
- **Current T&E efforts focus mainly on discovering and preventing an attack in process (attack – defend).**
- **By working with developers and defenders, T&E can reduce cybersecurity risk through improving detection, response, and recovery capabilities of a system.**

Breaches Happen!

- **"All the data is stolen. At least twice." – Eugene Kaspersky**
- **FireEye estimates that 96% of organizations have been breached despite an annual global investment of $67 billion in cybersecurity defense.**
- **Two kinds of organizations: the ones that have been compromised and are aware, and those that have been compromised and are unaware.**
  - Mike McConnell, former director of national intelligence and the National Security Agency (NSA), and James Comey, director of the FBI
- **Therefore, we need to start accepting every system will be or has been compromised at some point.**

Learning From Breaches: What's the Takeaway?

- **Home Depot**
  - Currently with nearly 56 million cards available the price has plummeted to $9 from $100 on the black market.
- **Target**
  - Penn.-based provider of refrigeration and HVAC systems was given access to a Target database so the company could remotely login.
- **Kaspersky Lab**
  - "Knowing better" doesn't help.
- **Nasdaq (Oct 2010)**
  - "We've seen a nation-state gain access to at least one of our stock exchanges" says House Intelligence Committee Chairman Mike Rogers.
  - Attack code was designed to cause damage.
- **Banks**
  - Hacking ring stole $1 billion from more than 100 banks in 30 countries.

Learning From Breaches: What's the Takeaway?

- **White House**
  - U.S. officials were alerted by an ally to the White House email breach.
- **State Department**
  - An employee clicked on a bogus link in an email.
  - The government will likely never know for certain has much information was viewed or stolen.
  - The clean-up process took around 6 months, and systems were taken down twice.
- **Navy**
  - Iranian attack took 4 months to clean up.
- **OPM**
  - Went Undetected For More Than A Year, Sources Say.
  - Discovered in April, it was not until early May that investigators determined that employees' personal data probably was taken.
  - Accidental discovery….CyTech Services sales demo discovered malware.

What Has Current Cybersecurity T&E Produced?

- **Breach after Breach after Breach! Even the best defense can't stop a user from being stupid or an insider.**
- **Systems that allow attackers to compromise systems for months to years before being detected allowing massive data theft.**
- **Systems that have compromises mainly detected by the FBI after the data is put on the black market or by accidental discovery.**
- **Systems that make it difficult to impossible for organizations to determine what was stolen or accessed.**
- **Systems where it takes months for organizations to remove attackers after detection, and in some cases, multiple attempts.**

Cyber Security T&E Critical Failure

- **Testing the ability to Detect, Respond, and Recover**
  - Attackers on average were on breached environments for 205 days before being detected.
  - 69% of organizations learned of the breach from an outside entity.
  - Organizations are unable to identify what an attacker stole, accessed, or modified.
    - Bogus entries in OPM database?
  - Organizations generally need months to evict attackers and recover their systems.

NIST Cybersecurity Framework

- **In February 2014, NIST released a Cybersecurity Framework which is a risk-based approach to managing cybersecurity risk.**
- **The framework core consists of five concurrent and continuous functions – Identify, Protect, Detect, Respond, and Recover.**
- **However, organizations including the DoD have overwhelmingly focused on the protection function of this framework.**
- **Since it is impossible to guarantee full protection, the functions of detect, respond, and recovery have to be viewed equally as important.**
- **"Protection is ideal, but detection is a must."**
  - Dr. Eric Cole, SANS

Focus on the Entire Framework

- **The game is not over if an attacker successfully makes it through the layers of defense.**
  - Typical the attacker isn't where he ideally wants to go.
  - Typically the attacker doesn't have the privileges he needs to execute his attack.
  - It takes time for an attacker to gain privileges and find the files he wants to steal.
  - Typically the attacker needs to change critical files to survive a reboot and/or install additionally files on the system.
  - The most skilled attackers can be nearly invisible, but they always leave a footprint.
    - Malware can hide, but it must run.
      - If malware is running, it will show up in live memory.

Focus of Cyber Security: Managing Risk

- **Cyber security should focus on managing risk to your critical assets.**
  - Note: goal cannot be 100% prevention.
  - 100% security is only achieved with 0% functionality.
- **Preventing a threat from exploiting a vulnerability is one way to reduce cybersecurity risk.**
  - Reduce vulnerabilities
  - Limited success as reducing vulnerabilities by 90% does not necessarily mean you reduce your risk by 90%.

- **Another way to deal with risk is to minimize/reduce the damage that occurs when a threat exploits a vulnerability.**

Prevent Defense Concept

- **Think the Prevent Defense Approach in football.**
  - For most of the game, the defense competes directly against the offense.
  - Every yard and every point is hardly fought for.
  - At the end of the game, the winning team implements a prevent defense.
  - The defense is now competing against the clock.
    - Goal is to have time run out before the offense can score enough points to win.
- **In cybersecurity, the game can still be won even when breached if the attacker can be detected and stopped before they can cause damage.**

Evolving Cybersecurity T&E

- **Below metrics need to be abolished as they are misleading.**
  - "Number of Attacks Attempted"
  - "Number of Successful Attacks"
  - "Number of Attacks Detected"
  - "Number of Attacks Prevented"
- **The fundamental difference between real threats and a pen test: Real threats only need to be successful once.**
- **Cybersecurity T&E's goal:**
  - Determine and minimize the amount of cybersecurity risk of a system.
  - It's not to measure and achieve a certain level of protection.
    - Misleading: 99% of attacks were detected and prevented.

Evolving Cybersecurity T&E

- **Better metrics to incorporate:**
  - Mean time to detect attacker after compromise.
  - Mean time to react (stop attacker activities).
  - Mean time to recovery (clean system to original state).
- **To improve determining level of cybersecurity risk of a system:**
  - Measure/rank complexity of attacks needed to compromise.
  - Identify and demonstrate impact of compromise.
  - Provide data to answer: Is the system built so operators can detect, react, and restore within a mission timeframe?

Evolving Cybersecurity T&E

- **Continue to test and verify best practices are being followed for prevention.**
- **Shift focus from preventative (attack-defend) T&E to detect, respond, recover T&E.**
  - Risk can be lowered through detect, respond, recover.
  - Conduct testing events with attackers already inside the system.
    - To identify level of cybersecurity risk, T&E needs to answer:
      - Actions attackers are capable and likely to perform once inside a system.
      - Damage attackers will likely cause once inside a system.
      - How/when defenders will be able to detect attackers.
      - The amount of damage that an attacker can likely cause before detection and removal.

List of Detect, Respond, Recover T&E Recommendations

- Improve cyber-attack surface analysis.
- Produce accurate activity baselines from testing.
- Use baselines to implement statistical-based intrusion detection and test abnormal activity detection.
- Produce user activity baselines from testing and test attack detection through User Behavioral Analytics (UBA).
- Test detection of an attacker executing techniques for each post-exploit phase of an attack.
- Test Host-based sensing and analytics capabilities.

Detect, Respond, Recover T&E Recommendations

- **Increase thoroughness of Cyber-Attack Surface Analysis**
  - You have to know, I mean REALLY KNOW, what you have and why you have it – eliminate everything you don't need.
  - Typically becomes a checklist exercise rather than a system understanding process.
    - Example: Who can access the command prompt? What can they run?
    - Understand all processes, services, protocols, utilities (whitelist over blacklist).
      - Understand how attackers will use legitimate processes, services, protocols, utilities in hiding and executing their attacks.
- **Vulnerability Assessments are critical but have a severe limitation.**
  - The most advanced attackers will likely exploit an unknown vulnerability.
  - We can't fix a hole we didn't know existed.

Detect, Respond, Recover T&E Recommendations

- **Testing needs to produce an accurate & detailed picture of normal activity which can serve as a baseline.**
  - Signature-based intrusion detection will have limited success.
    - Even novice attackers have tools to obfuscate well-know malware to bypass signature detection.
    - 70 to 90% of malware are unique to a single organization–Verizon 2015.
  - Statistical-based intrusion detection offers benefits over signature-based.
    - Determine "normal" activity (use a cyber range!) and then test to see if traffic that falls outside the scope of normal is detected.
- **Don’t forget the memory.**
  - The memory is the best way to determine what a system is doing.

Detect, Respond, Recover T&E Recommendations

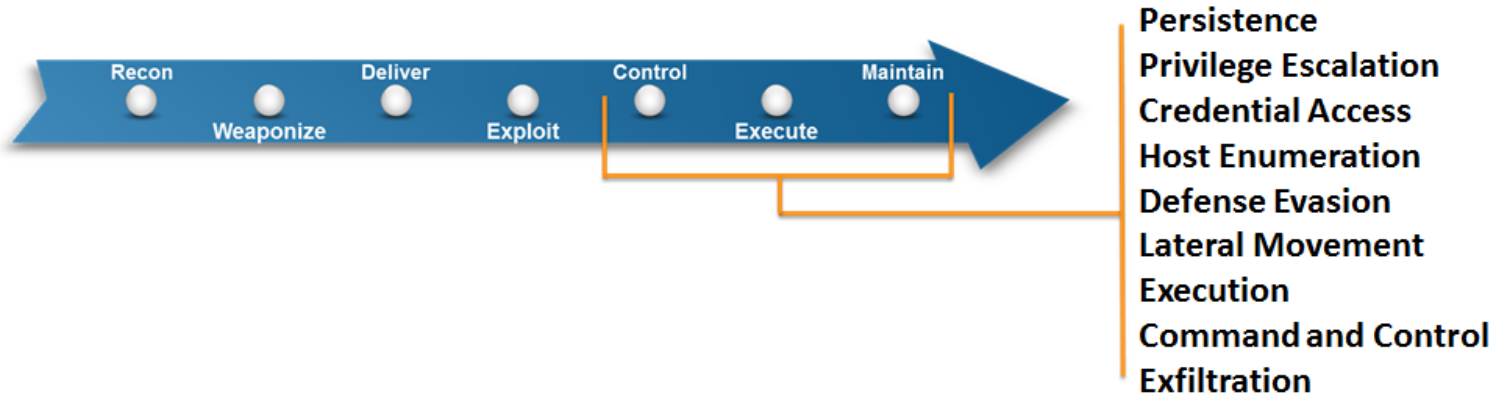
- **Even implementing the previous recommendations will only get so far against the stealthiest adversaries.**
- **The problem: Cyber adversaries blend in.**
  - Adversaries, post-exploit, can look very similar to normal users.
  - Adversaries use legitimate means of communication through the infrastructure for command and control.
  - Adversaries hide or masquerade their tools to blend into the operating environment.

Detect, Respond, Recover T&E Recommendations

- **User Behavioral Analytics (UBA)**
  - Testing needs to produce data for user profile baselines (cyber range opportunity).
    - Goal is to detect an attacker or insider using valid credentials.
    - UBA can detect a normal legitimate user acting in an anomalous and illegitimate way.
- **Once profile baselines are created for each user account type, test capability to detect anomalous user behavior (which may be viewed as normal without comparing to a user profile) such as log in attempts at atypical hours, access to databases and files outside of job function….**
  - Examples: second shift user logging in at the same time as a first shift user, a user touching a file they never touched.

Detect, Respond, Recover T&E Recommendations

- **Test detection of an attacker moving through the system.**
  - In order to accomplish his objective, an attacker will likely have to execute other actions once inside a system.
  - Known post-access techniques give insight into the actions that may be seen during an intrusion.
  - Conduct tests with an attacker executing techniques available for each post-exploit phase of an attack.



MITRE

Detect, Respond, Recover T&E Recommendations

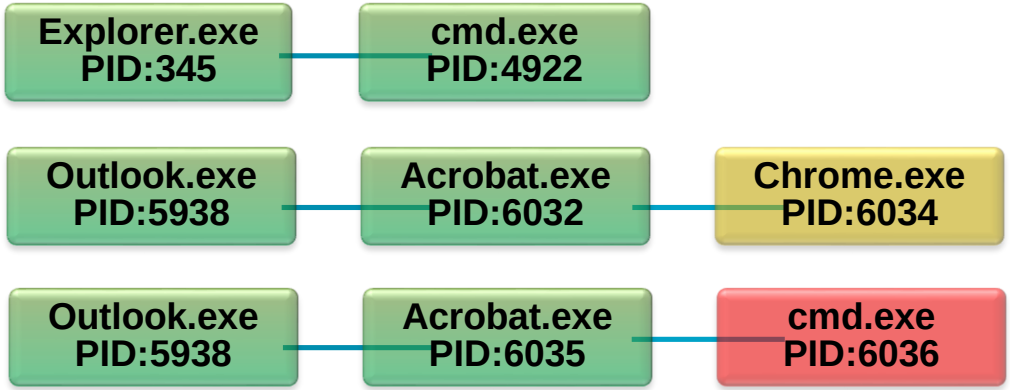
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials		Binary Padding	Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		DLL Side-Loading	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		Disabling Security Tools	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		File System Logical Offsets	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		Process Hollowing		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Indicator blocking on host		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception		Indicator removal from tools		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task		Indicator removal from host		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness		Masquerad-ing		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification		NTFS Extended Attributes		Service enumeration	Remote Services		Standard app layer protocol	From local system
BIOS	Bypass UAC	Obfuscated Payload		Window enumeration	Replication through removable media		Standard non-app layer protocol	From network resource
Hypervisor Rootkit	DLL Injection	Rootkit			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts	Exploitation of Vulnerability	Rundll32			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		Scripting			Windows admin shares			
Mod. Exist'g Service		Software Packing						
Registry Run Keys								
Serv. Reg. Perm. Weakness								
Windows Mgmt Instr. Event Subsc.								
Winlogon Helper DLL								

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

MITRE

Detect, Respond, Recover T&E Recommendations

- **Host-based sensing provides visibility into behaviors..**
  - Monitor Process Chains



- **Analytics leverage observation that adversaries engage in similar behaviors as they execute their missions**
  - Monitor c:\windows\system32\lsass.exe to see which programs are “touching” it (remember Duqu which ran inside the lsass.exe process?).

MITRE

Detect, Respond, Recover T&E Recommendations

- **Test systems by executing actions that are highly indicative of adversary activity to evaluate detection capability.**
- **Host-based sensing and robust analytics can find the attacker operating "right-of-exploit".**
  - Can significantly reduce detection times.
- **Host-based analytics can assist in reverse engineering attacker activities.**
  - Can greatly reduce recovery time.

Bottom Line At Bottom (BLAB)

- ALL systems have been, will be, and can be comprised by a determined attacker.
- Cybersecurity is a risk management exercise which is only partially about prevention.
- On average, the time it takes to detect, respond, and recover from a breach is unacceptable.
- Current T&E efforts are not resulting in systems with acceptable levels of cybersecurity risk.
- The greatest opportunity to reduce cybersecurity risk can be found in detect, respond, and recover.
- Current T&E efforts focus mainly on discovering and preventing an attack in process.
- By working with developers and defenders, T&E can reduce cybersecurity risk through improving detection, response, and recovery capabilities of a system.

Questions/Discussion

POC Information:

John Schab

MITRE Corporation

jschab@mitre.org