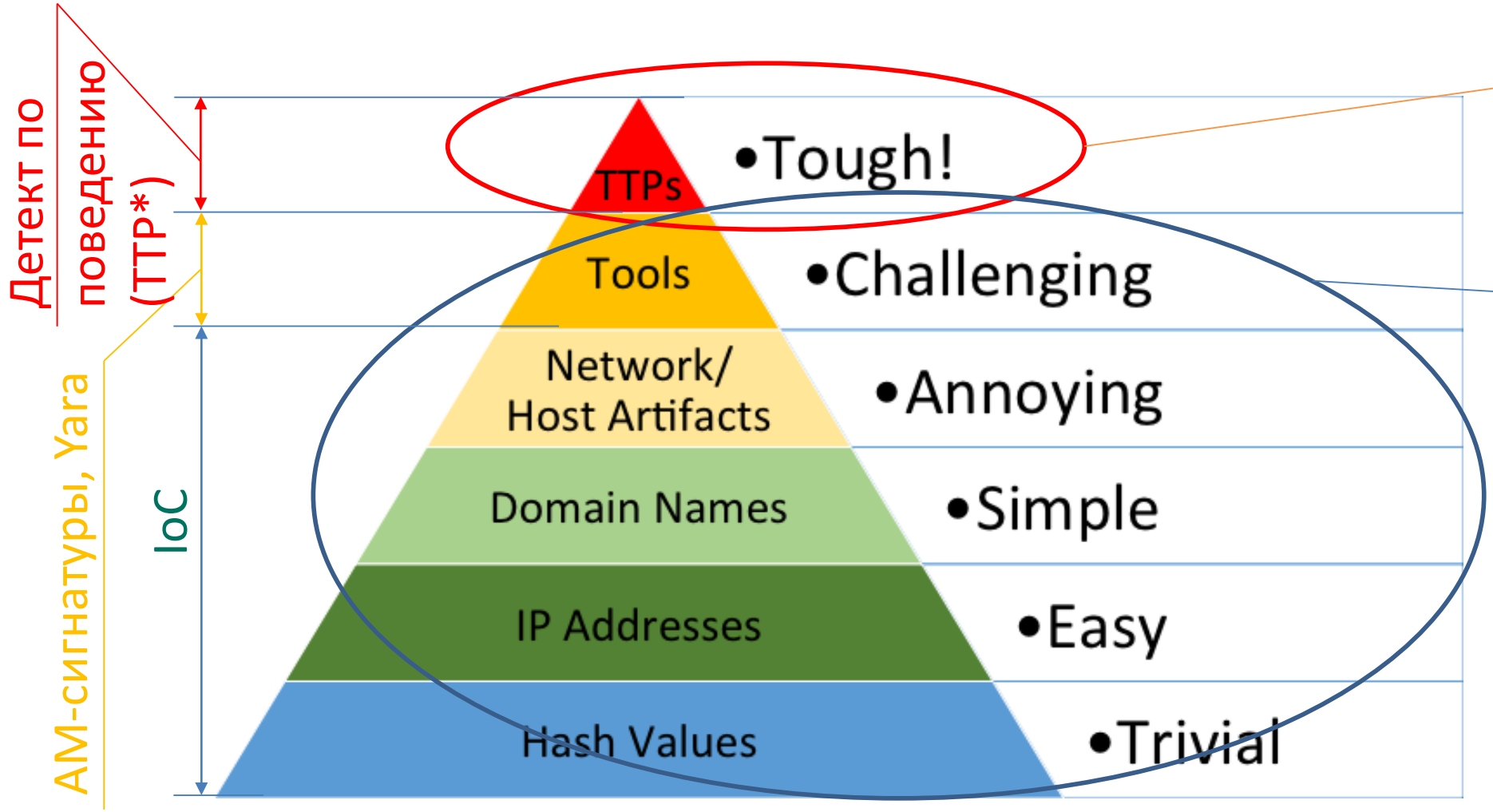
KASPERSKY lab

MITRE ATT&CK для операционной Безопасности

Сергей Солдатов
Руководитель Центра мониторинга

Уровни детекта: Пирамида боли Давида Бианко



Требуется аналитик

Возможности типовых детектирующих и превентивных инструментов (может быть сделано автоматически)

http://detect-respond.blogspot.ru/2013/03/the-pyramid-of-pain.html

* TTP – tactics, techniques and procedures (тактики, техники и процедуры)

Различные подходы к детектированию

Возможные действия атакующего	Детектирование на основе IOC-ов	Детектирование по артефактам инструментов	Детектирование по техникам (поведению)
Использование Mimikatz для дампа учётных данных (пароли/хеши) из памяти	Поиск по хешам (MD5/SHA1/SHA256) бинарных файлов утилит дампа учётных данных	Поиск файлов с расширениями или именами, характерными для различных утилит дампа учётных данных. Например, Mimikatz экспортирует билеты Kerberos в файлы с расширением *.kirbi*, а утилиты WCE создаёт на диске DLL с именем wceaux.dll	Выявление процессов, осуществляющих доступ к памяти процесса Lsass Поиск неподписанных DLL-библиотек, загружаемых в процесс Lsass
Использование легитимных утилит удалённого администрирования типа PsExec	Поиск по хешам (MD5/SHA1/SHA256) бинарных файлов утилит удалённого администрирования	Поиск установок сервисов с именами, характерными для утилит удалённого администрирования (например, PsExec устанавливает сервис с именем PSEXESVC)	Детектирование установки нового сервиса по сети с последующим запуском данным сервисом дочернего процесса
Взаимодействие с командным центром	Поиск взаимодействий с известными адресами командных центров ВПО (по IP/FQDN/URL)	Поиск User-Agent, специфичных для определённых утилит или ВПО Поиск взаимодействия с URL-ами, сгенерированными по алгоритму, характерному для определённой утилиты/ВПО	Поиск периодических сетевых соединений Поиск взаимодействий со случайно сгенерированными доменами Поиск взаимодействий с недавно зарегистрированными доменами

Тактики, Техники и Процедуры

- **Тактика** – промежуточная цель, этап Kill Chain.
- **Техника** – путь, с помощью которого достигаются цели Тактики
- **Процедура** – конкретная реализация Техники или/и используемые инструменты (ПО)

ATT&CK – Adversarial Tactics Techniques and Common Knowledge

Тактики

Техники

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption

https://attack.mitre.org/matrices/enterprise/

Техника

ENTERPRISE

TECHNIQUES

All
Initial Access +
Execution +
Persistence -
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor

Home > Techniques > Enterprise > Registry Run Keys / Startup Folder

Registry Run Keys / Startup Folder

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. [1] These programs will be executed under the context of the user and will have the account's associated permissions level.

The following run keys are created by default on Windows systems: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce` `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Visa and newer. Registry run key entries can reference programs directly or list them as a dependency. [2] For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"` [3]

The following Registry keys can be used to set startup folder items for persistence:

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`
`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use Masquerading to make the Registry entries look as if they are associated with legitimate programs.

ID: T1060
Tactic: Persis
Platform: W
Permissions
Data Source
CAPEC ID:
Contributors
Version: 1.0

Examples

Name	Description
ADVSTORESHELL	ADVSTORESHELL achieves persistence by adding itself to the `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Ru`
APT19	An APT19 HTTP malware variant establishes persistence by setting the Registry key `HKCU\Software\Microsoft\Windo`
APT29	APT29 added Registry Run keys to establish persistence.[8]

Mitigation

Identify and block potentially malicious software that may be executed through run key or startup folder persistence using whitelisting [102] tools like AppLocker [103] [104] or Software Restriction Policies [105] where appropriate. [106]

Detection

Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. [107] Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.

Changes to these locations typically happen under normal conditions when legitimate software is installed. To increase confidence of malicious activity, data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

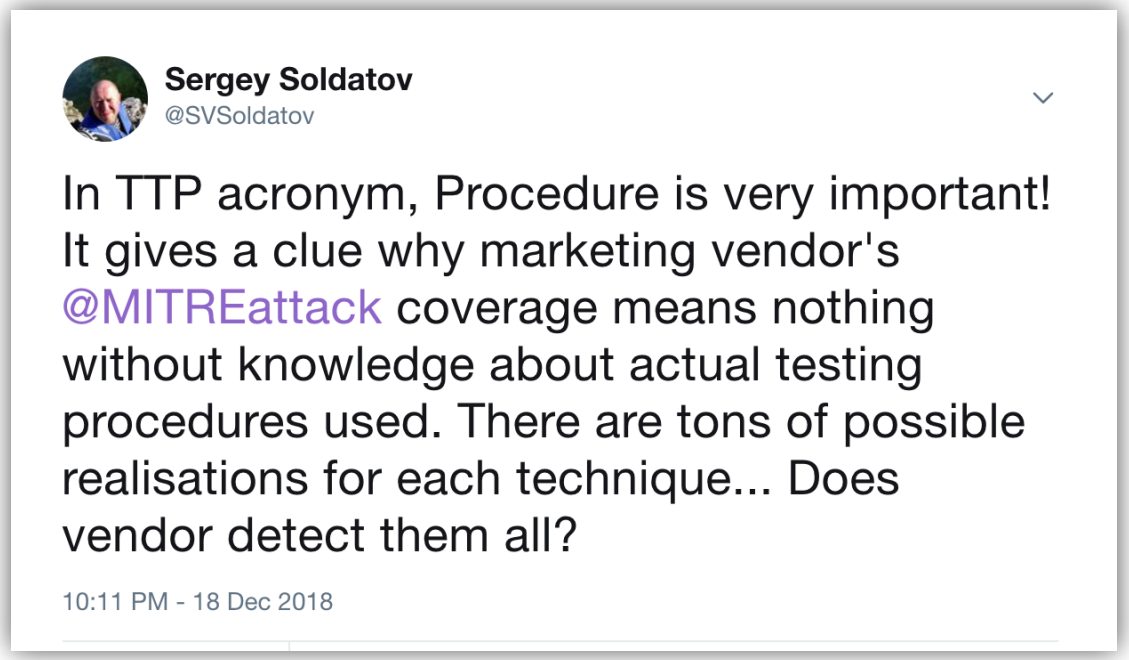
References

1. Microsoft. (n.d.). Run and RunOnce Registry Keys. Retrieved November 12, 2014.
2. Microsoft. (2018, August 20). Description of the RunOnceEx Registry Key. Retrieved June 29, 2018.
3. Moe, O. (2018, March 21). Persistence using RunOnceEx - Hidden from Autoruns.exe. Retrieved June 29, 2018.
4. Kaspersky Lab's Global Research and Analysis Team. (2015, December 4). Sofacy APT hits high profile targets with updated toolset. Retrieved December 10, 2015.
55. Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Remote Administration Tools & Content Staging Malware Report. Retrieved March 16, 2016.
56. Sherstobitoff, R. (2018, February 12). Lazarus Resurfaces, Targets Global Banks and Bitcoin Users. Retrieved February 19, 2018.
57. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.

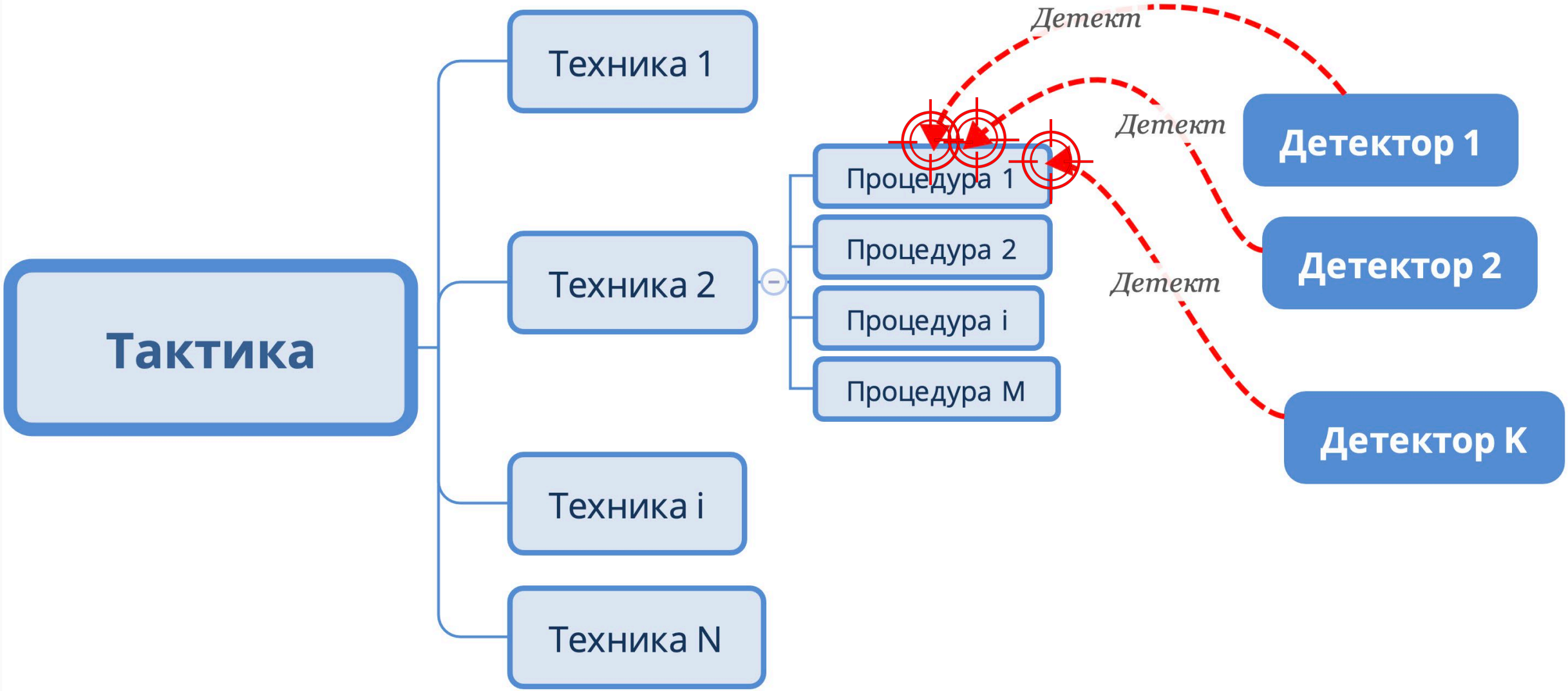
https://attack.mitre.org/techniques/T1060/

Важность Процедуры

- Для каждой Техники много Процедур может быть предложено
- Возможно наличие процедур, которые не могут быть обнаружены из-за технологических ограничений
- **Не все процедуры на данный момент известны**



Что мы обнаруживаем? Процедуру!



Где в ATT&CK указаны Процедуры?

Password Filter DLL

Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as dynamic link libraries (DLLs) containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts.

Before registering new passwords in the Security Accounts Manager (SAM), the Local Security Authority (LSA) requests validation from each registered filter. Any potential changes cannot take effect until every registered filter acknowledges validation.

Adversaries can register malicious password filters to harvest credentials from local computers and/or entire domains. To perform proper validation, filters must receive plain-text credentials from the LSA. A malicious password filter would receive these plain-text credentials every time a password request is made. [1]

ID: T1174

Tactic: Credential Access

Platform: Windows

Permissions Required: Administrator, SYSTEM

Data Sources: DLL monitoring, Process monitoring, Windows Registry

Contributors: Vincent Le Toux

Version: 1.0

Examples

Name	Description
Remsec	Remsec harvests plain-text credentials as a password filter registered on domain controllers.[2]

Mitigation

Ensure only valid password filters are registered. Filter DLLs must be present in Windows installation directory (`C:\Windows\System32\` by default) of a domain controller and/or local computer with a corresponding entry in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages`. [3]

Detection

Monitor for change notifications to and from unfamiliar password filters.

Newly installed password filters will not take effect until after a system reboot.

Password filters will show up as an autorun and loaded DLL in lsass.exe. [4]

References

1. Fuller, R. (2013, September 11). Stealing passwords every time they change. Retrieved November 21, 2017.
2. Kaspersky Lab's Global Research & Analysis Team. (2016, August 9). The ProjectSauron APT. Retrieved August 17, 2016.
3. Microsoft. (n.d.). Installing and Registering a Password Filter DLL. Retrieved November 21, 2017.
4. Bialek, J. (2013, September 15). Intercepting Password Changes With Function Hooking. Retrieved November 21, 2017.

Хорошие доклады в Сети

Hunting for Credentials Dumping in Windows Environment

Teymur Kheirhabarov

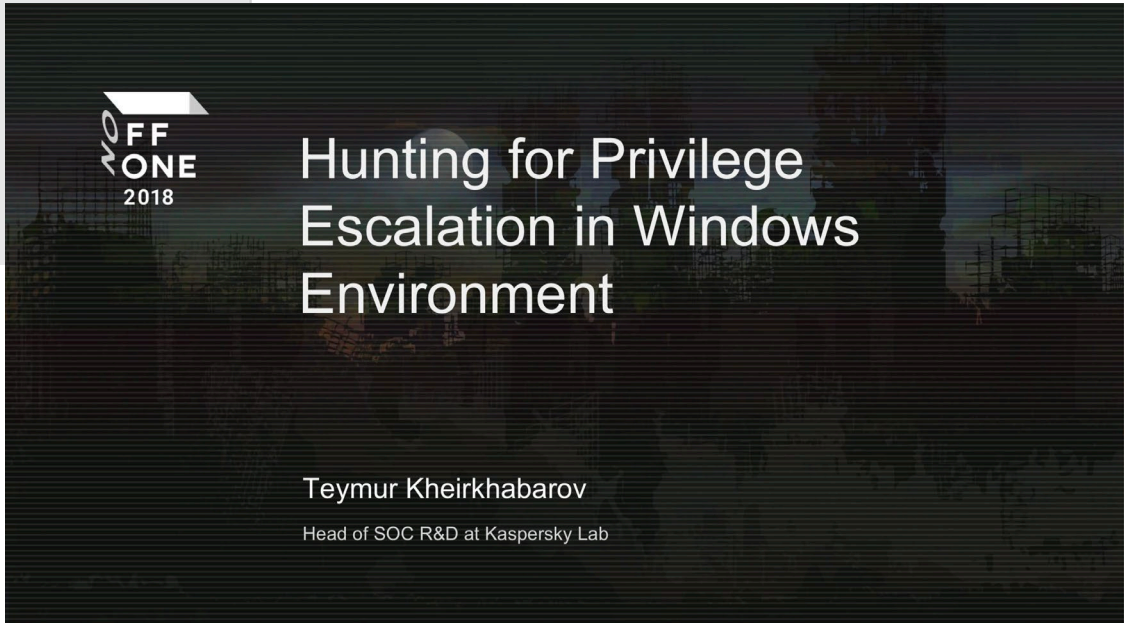
https://2017.zeronights.ru/report/hunting-for-credentials-dumping-in-windows-environment/

phd Positive Hack Days

Hunting Lateral Movement in Windows Infrastructure

Teymur Kheirkhabarov

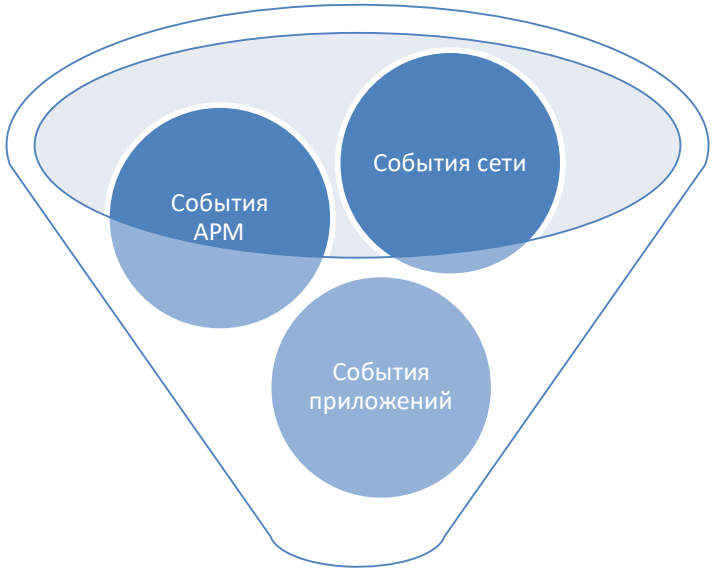
https://www.slideshare.net/heirhabarov/kheirkhabarov24052017phdays7



https://offzone.moscow/speakers/teymur-heirhabarov/

KASPERSKY lab

Мониторинг и Активный поиск угроз

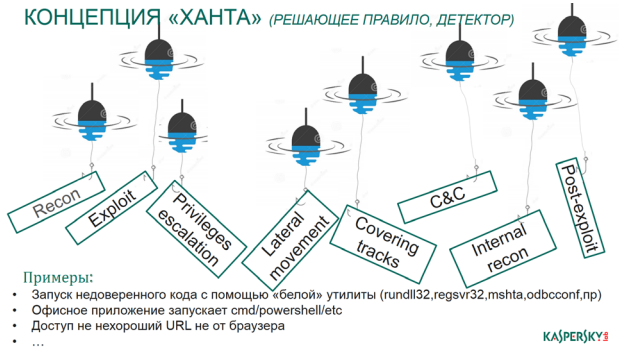


Магия

(Разметка)

Другая Магия

(Агрегация)



Зацепки

Аналитик

FP

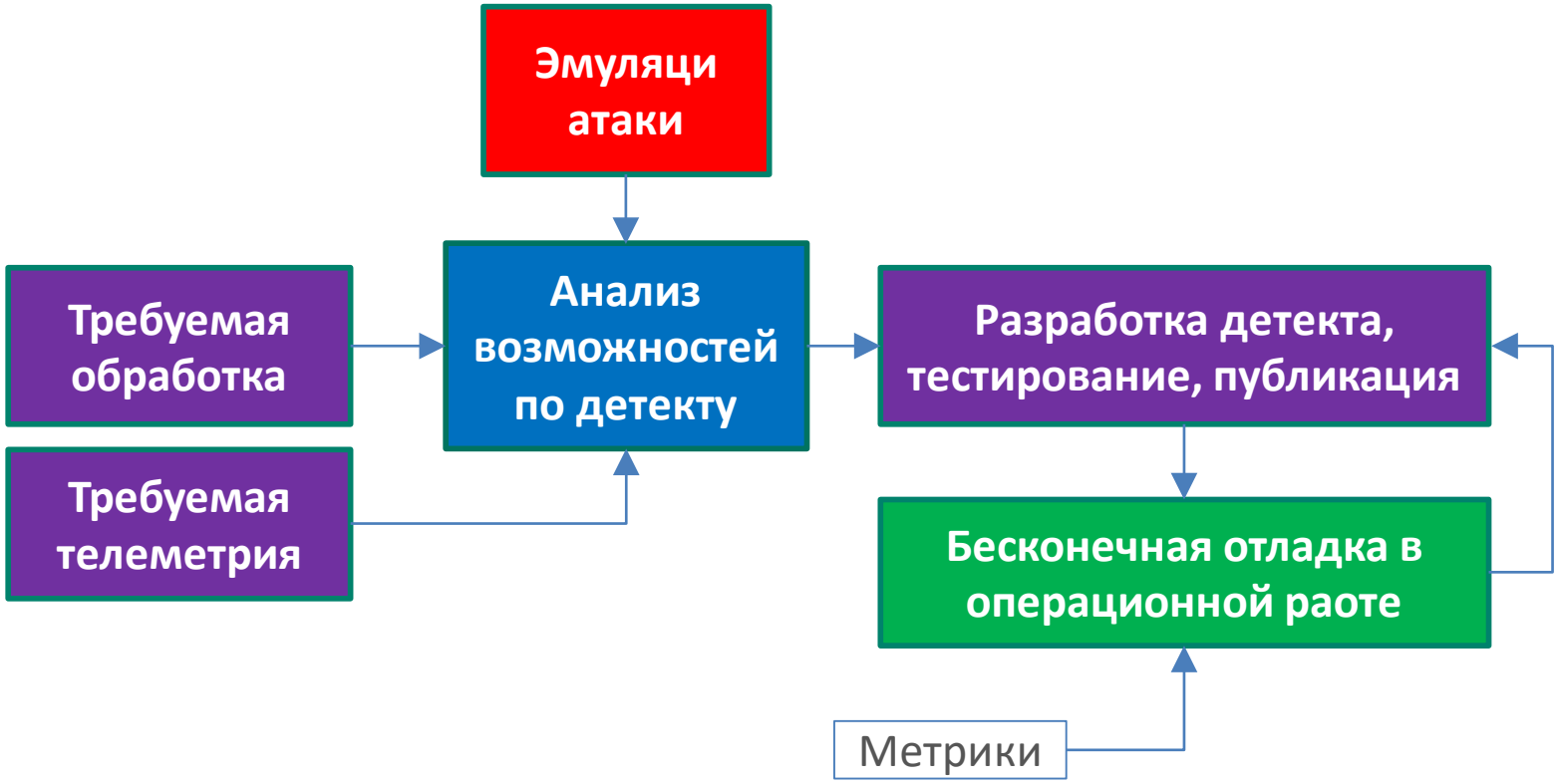
Правим Магию

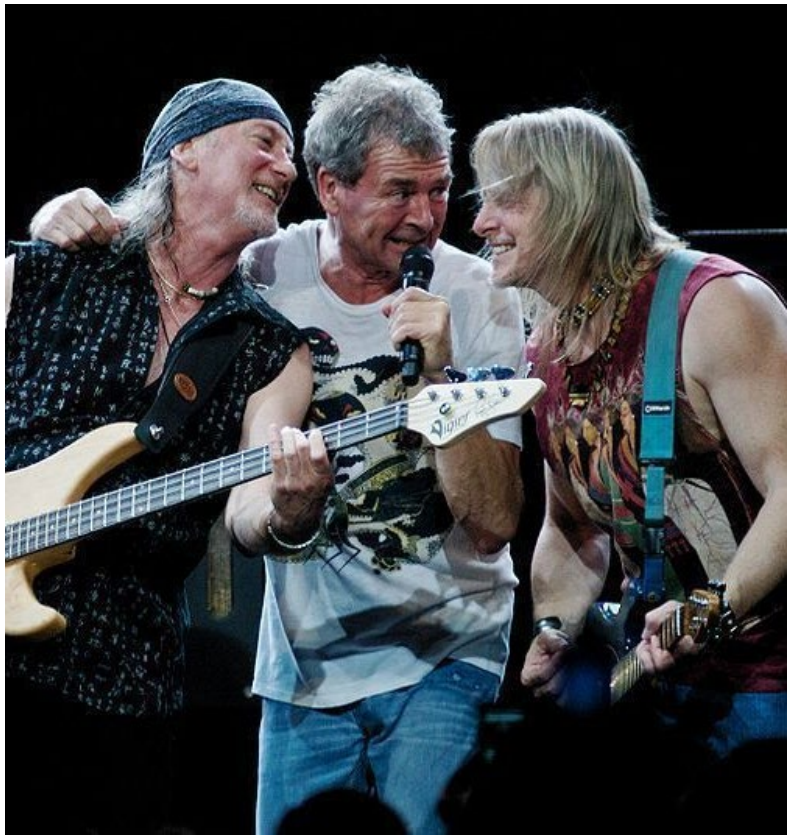
TP

Реагирование

Сценарий #1: Разработка детекторов

- ATT&CK – **хороший источник идей**

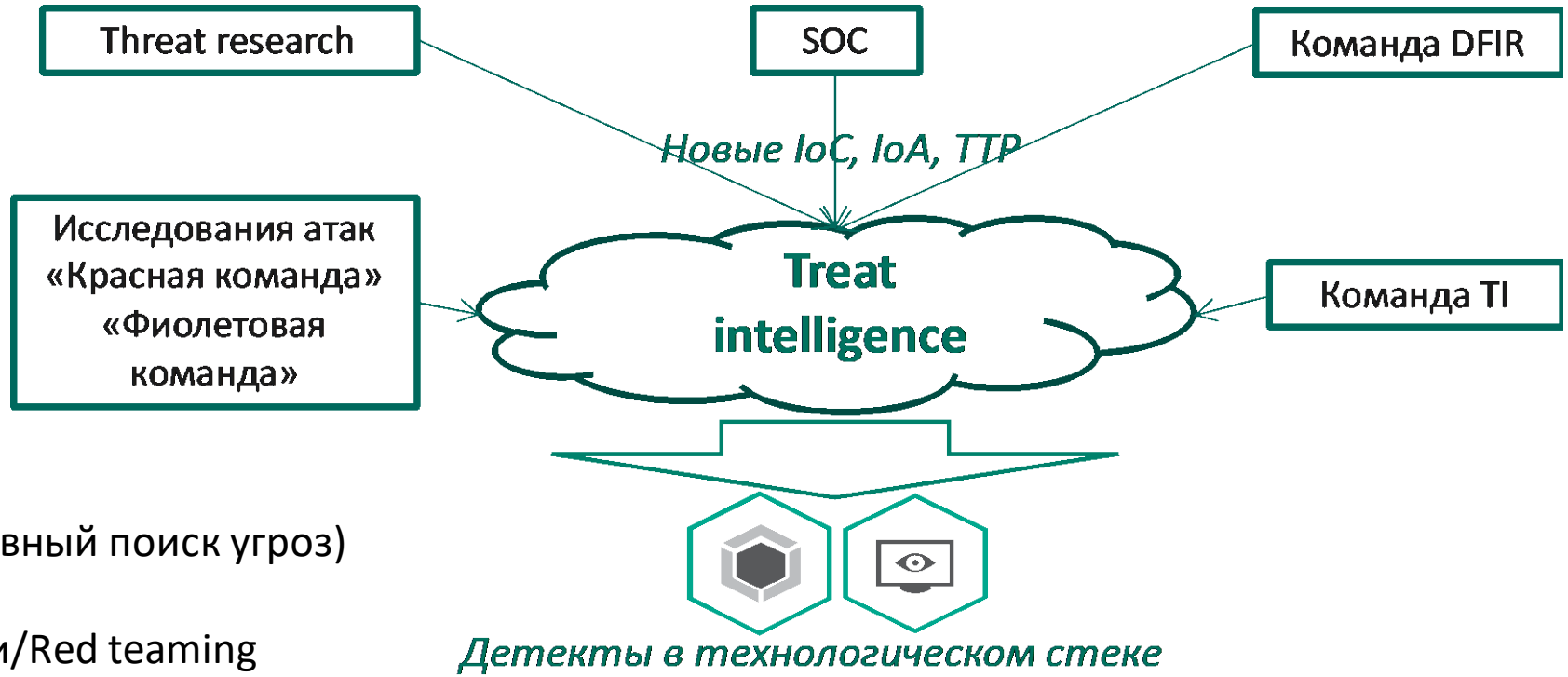




Важный источник идей для детекторов – TI из операционной практики

- Открытые источники
  - Twitter, блоги, конфы, т.п.
  - Тесты*
- Непубличные
  - Отчеты об угрозах
  - **Операционная практика**

    Threat hunting** (активный поиск угроз)
    DFIRMA***
    Анализ защищенности/Red teaming



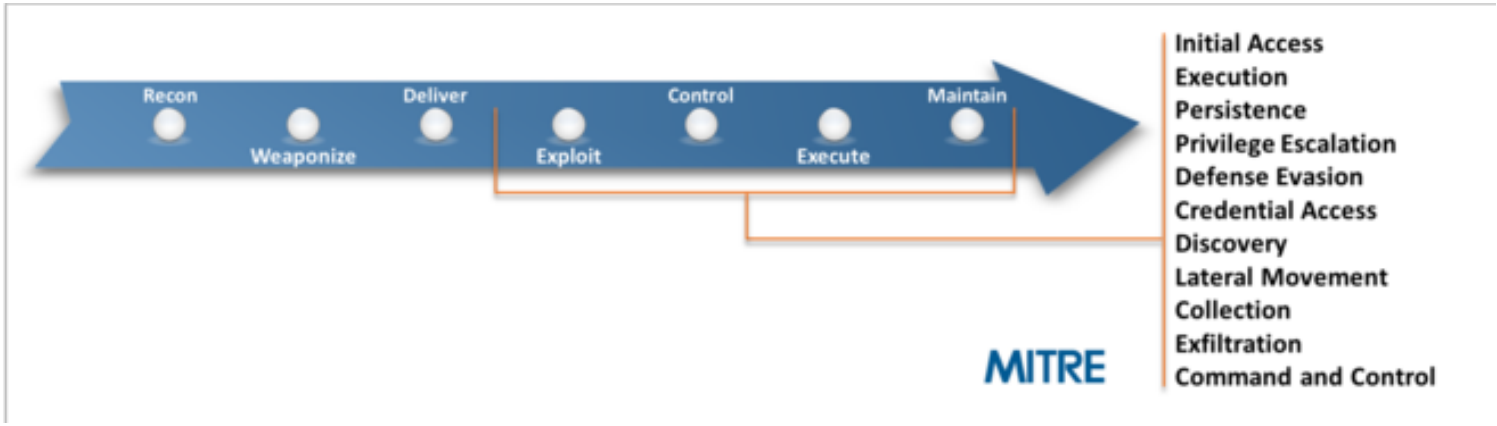
* https://attackevals.mitre.org/evaluations.html , например

** практика **итеративного поиска** с целью обнаружить угрозы, которые **уже не были обнаружены** полностью автоматическими средствами

*** Digital forensics, Incident response, Malware analysis

Сценарий #1’: Приоритеты разработки детекторов (post-breach)

- Приоритеты тактик:
  - Persistence
  - Privilege escalation
  - Defense evasion
  - Credential access
  - Lateral movement
  - Execution
  - …

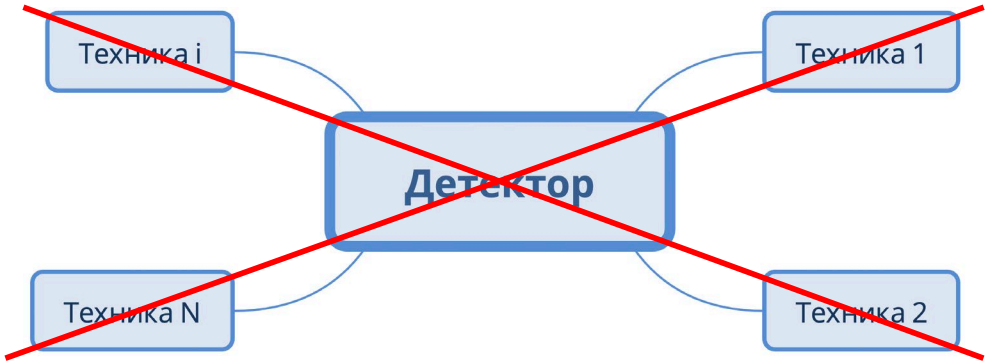


- Приоритеты техник
  - Доступная телеметрия
  - Каким APT использовалось и насколько это релевантно для вас?
  - Необходимые инвестиции (~ оценка риска)

http://reply-to-all.blogspot.com/2019/01/mitre-att.html

Сценарий #2: Классификация детекторов

- Управление детекторами
  - Понимание текущего покрытия
    - Что у нас есть для каждой техники*?
      - Анализ слабых мест
  - Увеличение покрытия
    - Создать новые детекторы?
    - Скорректировать существующие?
- Упрощение работы команды исследователей



* Посредством соответствующих процедур

Соответствие детекторов Техникам MITRE ATT&CK

Time	eventtype	parentprocessfilepath	processfilepath	filecmdline	aps_hunts	attack_ttps
2018-04-24 15:11:21	11	C:\Windows\System32\cmd.exe	-	-	dump_sensitive_registry_hives_locally_detects	T1003: Credential Dumping
2018-04-24 15:11:21	2	C:\Windows\System32\rundll32.exe	c:\windows\system32\cmd.exe	reg.exe save hklm\sam C:\sam.save	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:21	11	C:\Windows\System32\rundll32.exe	-	-	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:21	11	C:\Windows\System32\rundll32.exe	-	-	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:38	11	C:\Windows\System32\rundll32.exe	-	-	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:38	11	C:\Windows\System32\rundll32.exe	-	-	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:38	2	C:\Windows\System32\rundll32.exe	c:\windows\system32\cmd.exe	reg.exe save hklm\system C:\system.save	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:38	11	C:\Windows\System32\cmd.exe	-	-	dump_sensitive_registry_hives_locally_detects	T1003: Credential Dumping
2018-04-24 15:11:59	11	C:\Windows\System32\rundll32.exe	-	-	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:59	11	C:\Windows\System32\cmd.exe	-	-	dump_sensitive_registry_hives_locally_detects	T1003: Credential Dumping
2018-04-24 15:11:59	11	C:\Windows\System32\rundll32.exe	-	-	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry
2018-04-24 15:11:59	2	C:\Windows\System32\rundll32.exe	c:\windows\system32\cmd.exe	reg.exe save hklm\security C:\security.save	dump_sensitive_registry_hives_using_reg	T1214: Credentials in Registry

Сценарий #3 База знаний аналитика

- Attack kill chain (Тактики)
- **Описание актуальных Техник проведения атак**
- Публичные отчеты об актуальных целевых кампаниях (APT) и соответствующие техники атак
- Рекомендации по обнаружению и предотвращению

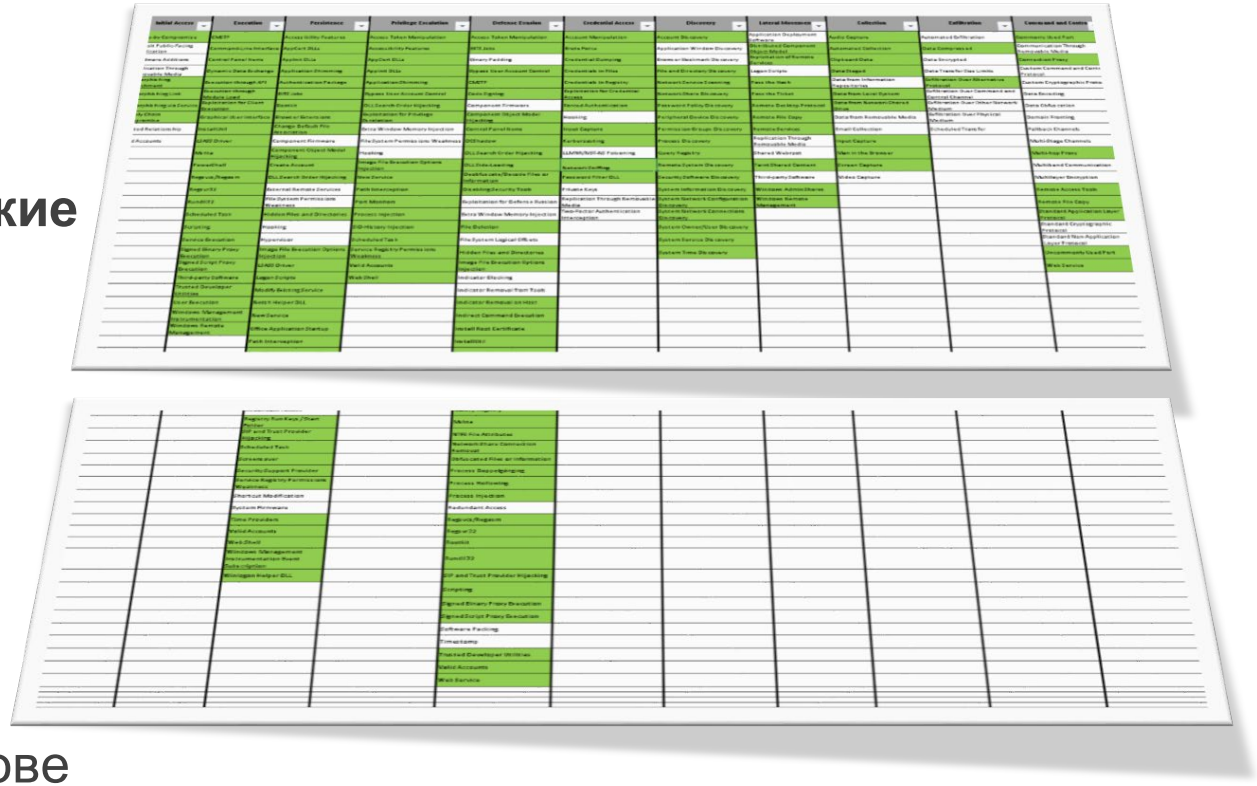
Дополнительно:

- Архитектура современных операционных систем
- Актуальные инструменты атакующих
- **Не гипотетически атаки, но взятые из конкретной практики***

* https://reply-to-all.blogspot.com/2013/01/blog-post.html

Сценарий #4: Оценка качества обнаружения на базе покрытия ATT&CK

- Выберите сценарий тестирования (последовательность конкретных процедур)*
- **Выполняйте тест на стендах и смотрите какие детекторы сработали**
- Оцените на основе типов детекторов**:
  - Телеметрия
  - Обогащение
  - Обнаружение поведения (TTP-based)
- Теперь результаты можно сравнить***
- Может ли Техника считаться покрытой на основе теста – вопрос открытый, **зависит от конкретных процедур, используемых в тестах**



* https://attackevals.mitre.org/
** https://attackevals.mitre.org/methodology/detection-categorization.html
*** https://reply-to-all.blogspot.com/2018/12/mitre-edr.html

Тесты MITRE ATT&CK

- **Конкретные процедуры**:
  - APT3: 56 Техник, 10 Тактик
  - Подход “Living off the land”*
  - Фокус на «Первичные» Техники**, на поведение, а не на конкретные инструменты и артефакты (IoCs)
  - 2 Сценария: 10 шагов с Cobalt Strike + 10 шагов с Empire***
- **Одинаковые стенды для всех вендоров**
- **Категории детекторов**
  - Основные типы:
    - Ничего (None)
    - Телеметрия (Telemery)
    - Артефакт (IoC)
    - Обогащение (Enrichment)
    - Общий поведенческий (General behavior)
    - Конкретный поведенческий (Specific behavior)
  - Опции:
    - Отложенный (Delayed)
    - Зависимый (Tained)
    - При изменении конфигурации (Configuration change)

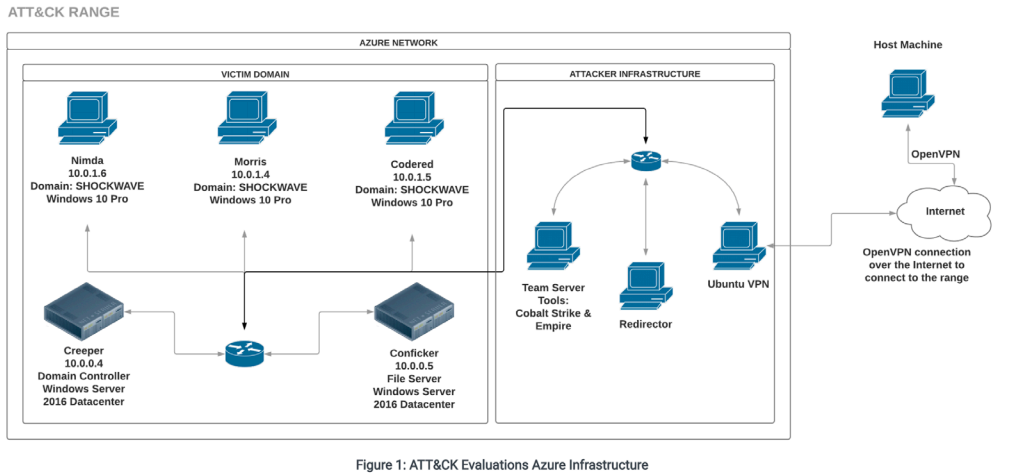
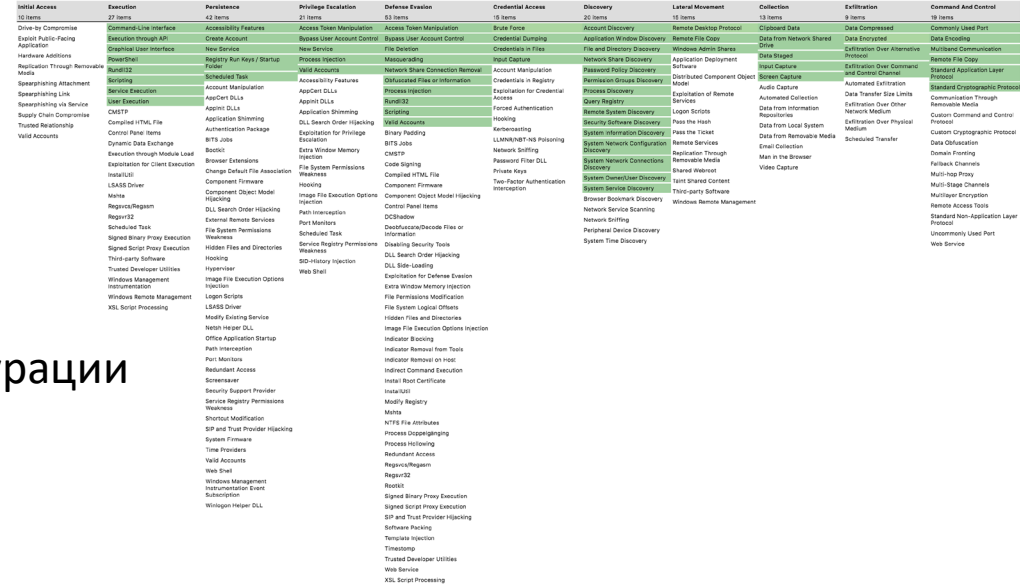


Figure 1: ATT&CK Evaluations Azure Infrastructure



* https://www.youtube.com/watch?v=j-r6UonEkUw

** Differentiate “Primary” and “Enabling” techniques. “Enabling” - many of the techniques required Command-Line Interface, Execution through API, and PowerShell. In assessment MITRE focused on the Primary technique that was performed, rather than the mechanism of execution (which was considered the Enabling technique)

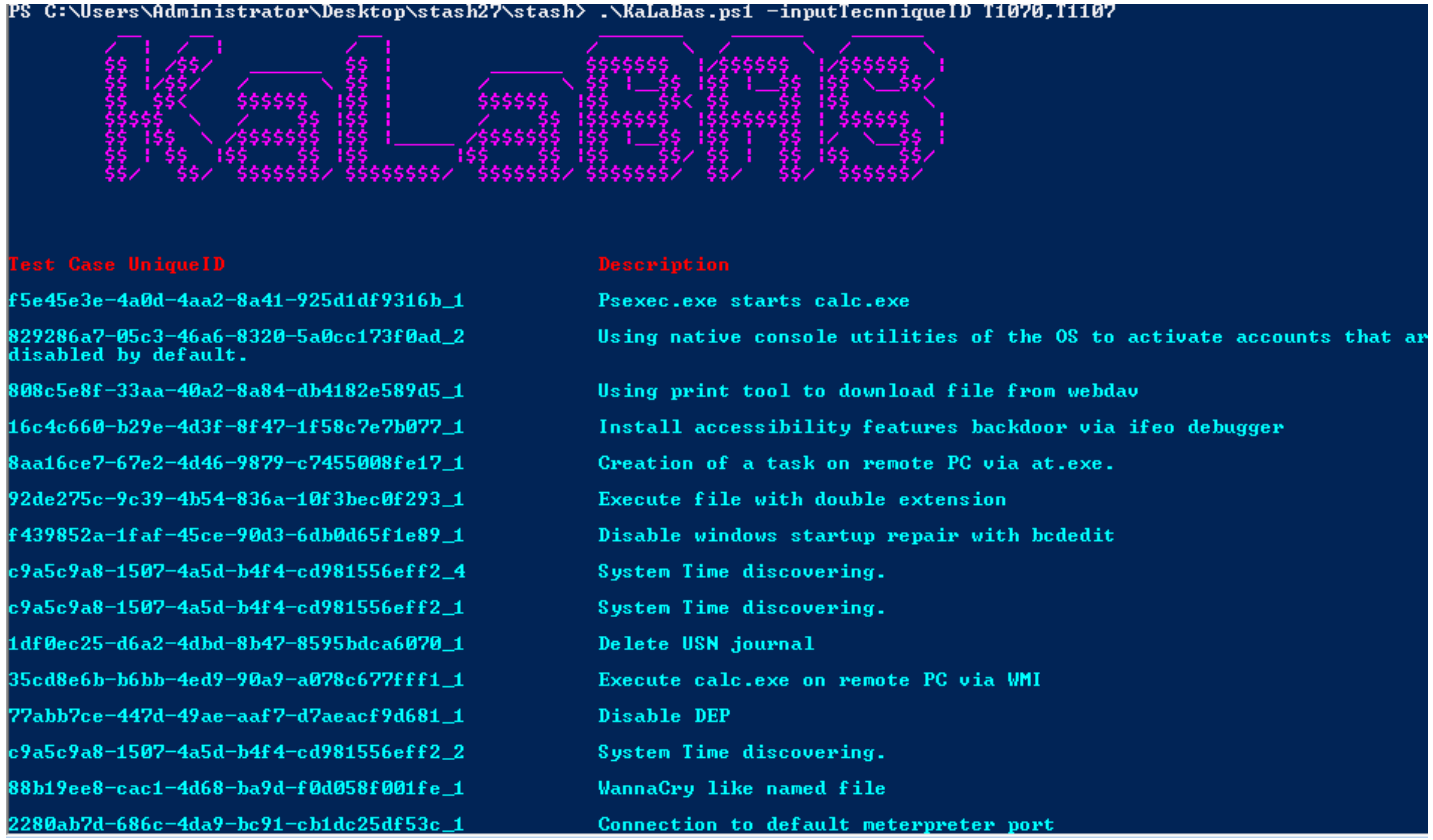
*** https://www.cobaltstrike.com/ ; https://github.com/EmpireProject/Empire

BAS: Breach and Attack Simulation

- METTA
  - https://github.com/uber-common/metta
- Caldera
  - https://github.com/mitre/caldera
- Unfetter
  - https://mitre.github.io/unfetter/
- Endgame
  - https://github.com/endgameinc/RTA
- Red Canary - Atomic read team
  - https://github.com/redcanaryco/atomic-red-team
- Microsoft
  - https://blogs.technet.microsoft.com/motiba/2018/04/09/invoke-adversary-simulating-adversary-operations/

KaLaBAS?

- Готовые – заточены под конкретного вендора
- Недостаточно тестов
  - Как покрытие вообще
  - Так и конкретные опции
- Есть задача интеграции в существующую инфраструктур автоматического тестирования



Сценарий #5: Симуляция атаки, red teaming

- Общий фреймворк для взаимодействия Красных, Голубых и Фиолетовых команд
- Создание сценариев эмуляции атак: выбор релевантных TTP
- Планирование работы Красных команд: выбор TTP, которые могли бы пропустить Голубые
- Анализ слабых мест системе безопасности – приоритезация будущих инвестиций
- Оценка операционной эффективности (зрелости) SOC

How To Test Your MSSP/MDR?

by **Anton Chuvakin** | October 11, 2017 | Submit a Comment

As customary in our beloved domain of "cyber", I will start with a depressing quote:

> *"If you really knew how to test an MSSP properly, you likely didn't need an MSSP."* (source: in this thread somewhere, if the author reads this, I am happy to ack by name)

On a more serious note, *clients must test* their Managed Security Services (MSS) or Managed Detection and Response (MDR) provider! In fact, there are two different things to discuss:

- **TEST BEFORE CONTRACT SIGNING** in order to pick the partner with the quality of security you a/ need and b/ are willing to pay for.
- **TEST DURING ONGOING OPERATION** in order to *…and this is tricky!…* test for ongoing value, check for degradation of service effectiveness, and even check to remind the MSSP that you care about the quality of delivery.

Before we talk more, we need to get this out of the way: we all know that some clients who sign up with an MSSP do NOT want quality. They need a checkbox, a party to scream at (and possible to sue) when they are hacked. We are not going to discuss this case…today.

While we want a framework to emerge eventually, here are some ideas, from heavy/deep to light/shallow tests:

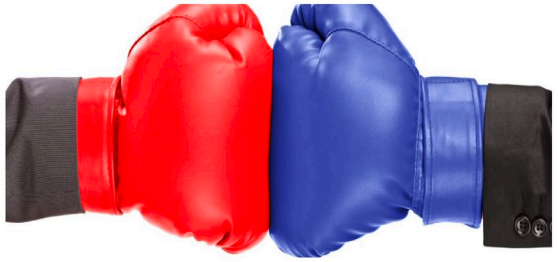
- **HEAVY** (and expensive): A full red team test or a quality pentest [without telling the MSSP/MDR]; your partner should catch them reliably and early in their process.
- **MEDIUM**: some people reported using *threat simulation tools* that generate [hopefully] realistic attack or exfiltration traffic and other "bad-looking" activities; you can probably just vuln scan a box too…
- **LIGHT**: A basic test can be as easy as unplugging an MSSP hardware sensor or blocking its network access (or log flow) and checking how fast they notice 😊

Pentesting and Red Teams

by **Augusto Barros** | March 31, 2017 | 3 Comments

A red team should be a continuous operation to keep the blue team on its toes. With continuous operations the red team can pick opportunities and scenarios that best fit the threat landscape of the organization at each moment and also work together with the blue team to force it into a continuous improvement mode. This also answers a common question about when to implement a red team: continuous improvement is often a defining factor of the highest maturity level in any maturity scale. So, it makes sense to assemble a red team (a continuous one, not a single "red team exercise", which is just another pentest) when you already on a reasonably high maturity and wants to move into the continuous improvement territory.

https://blogs.gartner.com/augusto-barros/2017/03/31/pentesting-and-red-teams/



https://blogs.gartner.com/anton-chuvakin/2017/10/11/how-to-test-your-msspmdr/

Поговорим?

Сергей Солдатов, CISA, CISSP
Руководитель SOC

KASPERSKY lab