Покоряя пирамиду боли

Совершенствуем стратегию обнаружения индикаторов киберугроз

БОЛЬШОЙ МОСКОВСКИЙ ТЕХНО infotecs ФЕСТ

Александр Дёмочкин
Специалист по исследованию киберугроз
«Перспективный мониторинг»

«Весь смысл обнаружения индикаторов заключается в том, чтобы реагировать на них.

Как только вы научитесь реагировать достаточно быстро, вы лишите противника возможности использовать эти индикаторы при атаке.

Однако не все индикаторы одинаковы, и некоторые из них гораздо ценнее других»,

— Дэвид Бьянко, автор модели «Пирамида боли»

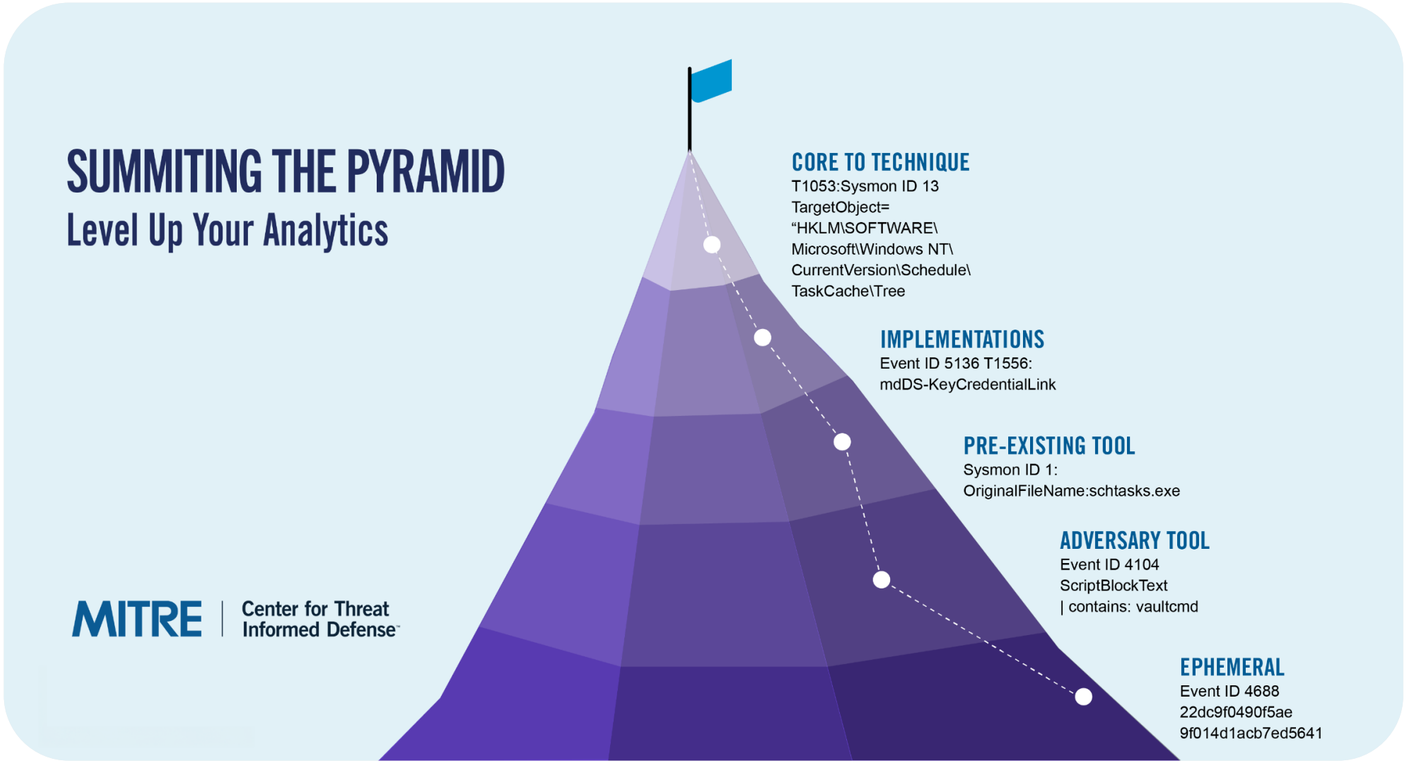
Модель «Пирамида боли»

«Пирамида боли» — диаграмма классификации IoC, а также сложности обхода защитных мер при их обнаружении

Актуальность

Модель «Summiting the Pyramid»

Надежность обнаружения — это выявление вредоносной активности с высокой точностью и устойчивое с течением времени



Уровни модели
«Summiting the Pyramid»

Поведение злоумышленников в ходе проведения атак

Инструменты, используемые злоумышленниками во время атаки

Кратковременные значения, которые злоумышленники можно легко изменить

Тактики и техники

Тактики и техники с низкой дисперсией

LOLBAS инструменты

Внешние инструменты

Кратковременные (эфемерные) значения

Уровни модели
«Summiting the Pyramid»

Поведение злоумышленников в ходе проведения атак

Инструменты, используемые злоумышленниками во время атаки

Кратковременные значения, которые злоумышленники можно легко изменить

Тактики и техники

Тактики и техники с низкой дисперсией

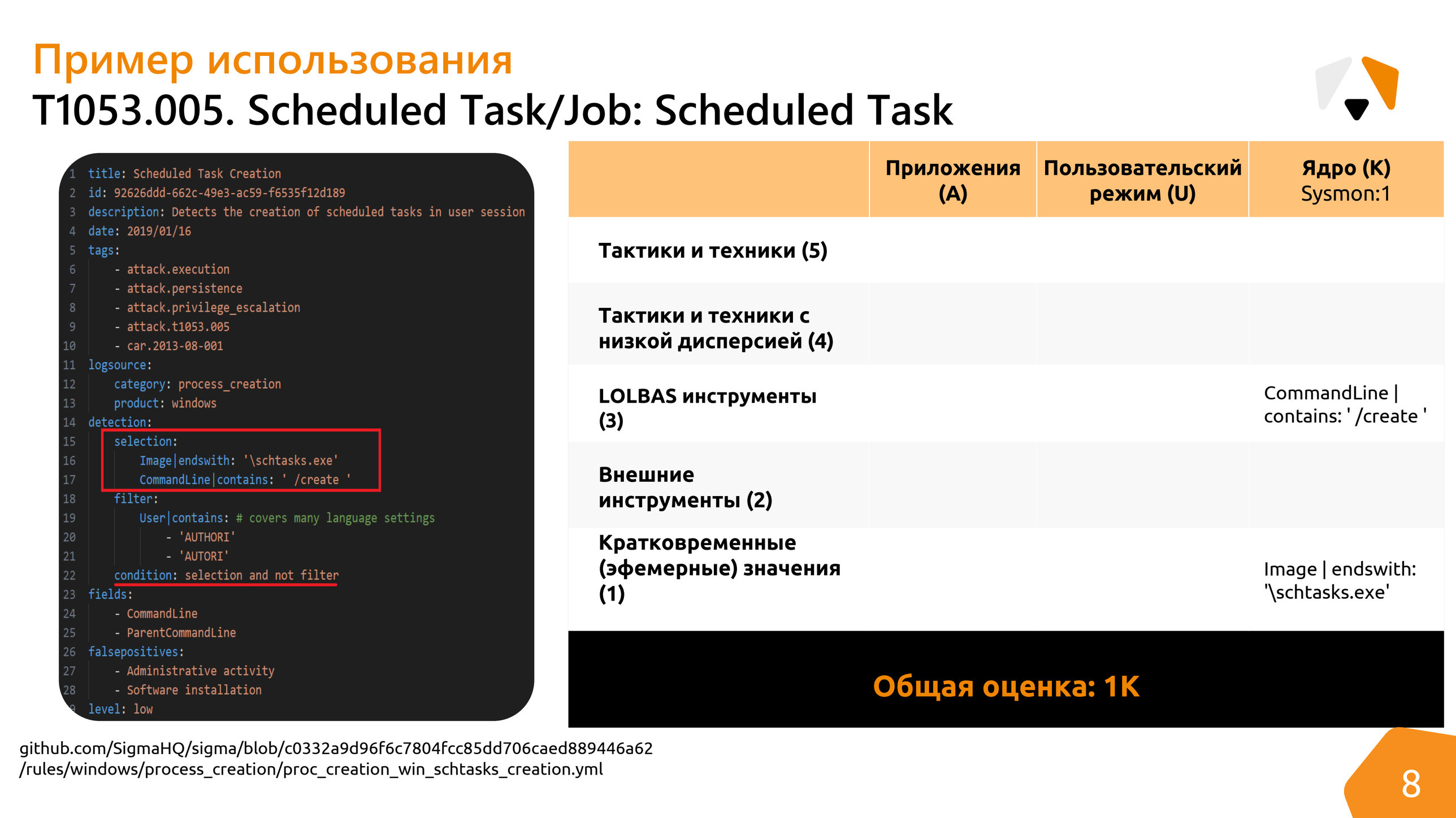
LOLBAS-инструменты

Внешние инструменты

Кратковременные (эфемерные) значения

Пример использования

T1053.005. Scheduled Task/Job: Scheduled Task



```yaml
title: Scheduled Task Creation
id: 92626ddd-662c-49e3-ac59-f6535f12d189
description: Detects the creation of scheduled tasks in user session
date: 2019/01/16
tags:
    - attack.execution
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1053.005
    - car.2013-08-001
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith: '\schtasks.exe'
        CommandLine|contains: ' /create '
    filter:
        User|contains: # covers many language settings
            - 'AUTHORI'
            - 'AUTORI'
    condition: selection and not filter
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Administrative activity
    - Software installation
level: low
```

	Приложения (A)	Пользовательский режим (U)	Ядро (K) Sysmon:1
Тактики и техники (5)			
Тактики и техники с низкой дисперсией (4)			
LOLBAS инструменты (3)			CommandLine | contains: ' /create '
Внешние инструменты (2)			
Кратковременные (эфемерные) значения (1)			Image | endswith: '\schtasks.exe'

Общая оценка: 1K

github.com/SigmaHQ/sigma/blob/c0332a9d96f6c7804fcc85dd706caed889446a62/rules/windows/process_creation/proc_creation_win_schtasks_creation.yml

Как можно
улучшить аналитику

Возможности

T1053. Scheduled Task/Job

T1053 – Scheduled Tasks					
Tools	**schtasks.exe**	**Task Scheduler (GUI)**	**Remote Registry**	**At** (Deprecated in Win8)	**Powershell Register-ScheduledTask**
COM Method	**ITaskFolder::RegisterTask**				**ITaskFolder::RegisterTask**
Win32 API	**CreateFile/RegCreateKey**			**NetScheduleJobAdd** **CreateFile/RegCreateKey**	
Registry	**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree OR HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks**				
File	**C:\Windows\System32\Tasks OR C:\Windows\Tasks OR C:\Windows\SYSWOW64\Tasks**				
RPC Server Code/RPC Server Application	**schedsvc.dll**		**regsvc.dll**	**taskcomp.dll**	
RPC Interface	**ITaskSchedulerServices** (86D35949-83C9-4044-B424-DB363231FD0C)		**[MS-RRP]** {338CD001-2244-31F1-AAAA-900038001003}	**[ATSvc]** {1FF70682-0A51-30E8-076D-740BE8CEE98B}	
RPC Method	**SchRpcRegisterTask, SchRpcEnumTasks**		**BaseRegCreateKey, BaseRegQueryInfoKey**	**NetrJobAdd***	
Network Protocol	**ITaskSchedulerServices**		**winreg Endpoint: \pipe\winreg**	**atsvc Endpoint: \pipe\atsvc**	**WS-Management TCP/5985/5986/Custom Port**

posts.specterops.io/abstracting-scheduled-tasks-3b6451f6a1c5

Level:1

	Приложения (A)	**Пользовательский режим (U)**	**Ядро (K)** Событие Sysmon: ID 1
Тактики и техники (5)			
Тактики и техники с низкой дисперсией (4)			
LOLBAS-инструменты (3)			CommandLine | contains: ‘ /create’ AND OriginalFileName “schtasks”
Внешние инструменты (2)			
Кратковременные (эфемерные) значения (1)			

Общая оценка: 3K

Level:2

	Приложения (A) Событие Windows: ID 4698	**Пользовательский режим (U)**	**Ядро (K)**
Тактики и техники (5)			
Тактики и техники с низкой дисперсией (4)	Task Created/Scheduled		
LOLBAS-инструменты (3)			
Внешние инструменты (2)			
Кратковременные (эфемерные) значения (1)			

Общая оценка: 4A

Level:3

	Приложения (A)	Пользовательский режим (U)	**Ядро (K)** Событие Sysmon: ID 12,13,14
Тактики и техники (5)			“HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\” “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\”
Тактики и техники с низкой дисперсией (4)			
LOLBAS-инструменты (3)			
Внешние инструменты (2)			
Кратковременные (эфемерные) значения (1)			

Общая оценка: 5K

Пример: Sigma

```yaml
title: Scheduled Task/Job
id: 02f7c9c1-1ae8-4c6a-8add-04693807f92f
description: Detects the scheduled tasks/job
references:
    - https://center-for-threat-informed-defense.github.io/summiting-the-pyramid/analytics/task_scheduling/
date: 2025/09/09
tags:
    - attack.execution
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1053.005
logsource:
    product: windows
    service: sysmon
detection:
    selection:
        EventID:
            - 12
            - 13
            - 14
        TargetObject|contains:
            - "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\"
            - "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\"
    condition: selection
falsepositives:
    - Administrative activity
    - Software installation
level: medium
```

Пример: OSSEC

```
<rule id="400122" level="2">
    <decoded_as>eventlog</decoded_as>
    <id>^12$|^13$|^14$</id>
    <regex ignorecase="true">TargetObject.{2}HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\TaskCache\\(Tree|Tasks)</regex>
    <description>Обнаружена попытка манипуляции с запланированной задачей</description>
    <info>
        <link>attack.mitre.org/techniques/T1053/005</link>
        <techniques>T1053.005</techniques>
        <capec></capec>
        <cwe></cwe>
        <cve></cve>
    </info>
    <category>persistent</category>
</rule>
```

Какой итог?

- Обнаружение и покрытие угроз становится более точным
- Учитывается устойчивость с течением времени
- Возможность выстраивать приоритеты по всем IOC’s
- Демонстрация критичности каждого индикатора

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Дёмочкин Александр
Специалист
по исследованию киберугроз

t.me/pm_public

amonitoring.ru

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС