SOC FORUM 2023

АВТОМАТИЗАЦИЯ LIVE INCIDENT RESPONSE С ПОМОЩЬЮ KAPE

Баландин Алексей

Эксперт

Security Vision

МОСКВА 2023

Категории forensics артефактов

SOC FORUM 2023

- System Information
- Application Execution
- File and Folder Opening
- Browser Activity
- Account Usage
- Deleted Items and File Existence
- Cloud Storage
- Network Activity and Physical Location
- External Device/USB Usage

Огромное разнообразие forensics артефактов

SOC FORUM 2023

Application Execution

- Shimcache
- Amcache
- Jump Lists
- Prefetch
- UserAssits
- Last Visited MRU
- SRUM
- Windows 10 Timeline
- Task Bar Feature Usage
- CapabilityAccess Manager

System Information

- Operation System Version
- Computer Name
- System Boot Programs
- Autostart Programs
- System Last Shutdown Time

File and Folder Opening

- Open/Save MRU
- Recent Files
- Last Visited MRU
- Shortcut (LNK) Files
- Shell Bags
- Office OALerts
- Jump Lists
- Office Recent Files
- MS Word Reading Location
- Office Trust Records

Огромное разнообразие forensics артефактов

SOC FORUM 2023

Browser Activity

- Browser History
- Download History
- Media History
- Bookmarks
- Stored Credentials
- Cache
- Cookies
- Browser Preferences
- Extensions
- HTML5 Web Storage

Account Usage

- Last Login and Password Change
- Authentication Events
- Successful / Failed Logons
- Logon Event Types
- RDP Usage
- Create / Delete Account
- Account Group Membership
- Cloud Account Details

Огромное разнообразие forensics инструментов

SOC FORUM 2023

ПРОБЛЕМАТИКА

- Sysinternals
- Eric Zimmerman tools
- NirSoft
- FTK
- Volatility
- PowerForensics
- ...

- У каждого инструмента свой интерфейс, свои параметры

- Запуск по отдельности занимает очень много времени (хранение, классификация результатов)

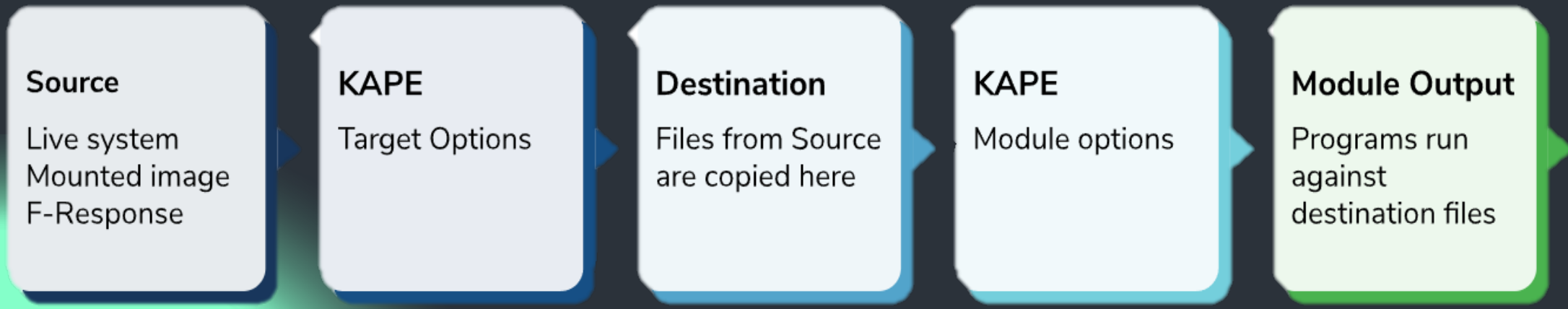
Каре — инструмент автоматизации сбора и анализа цифровых свидетельств

SOC FORUM 2023

- Модульная архитектура
- Удобный интерфейс
- Гибкое добавление новых инструментов
- Предустановленный набор модулей
- Высокая производительность
- Возможность разработки собственных модулей
- Бесплатный

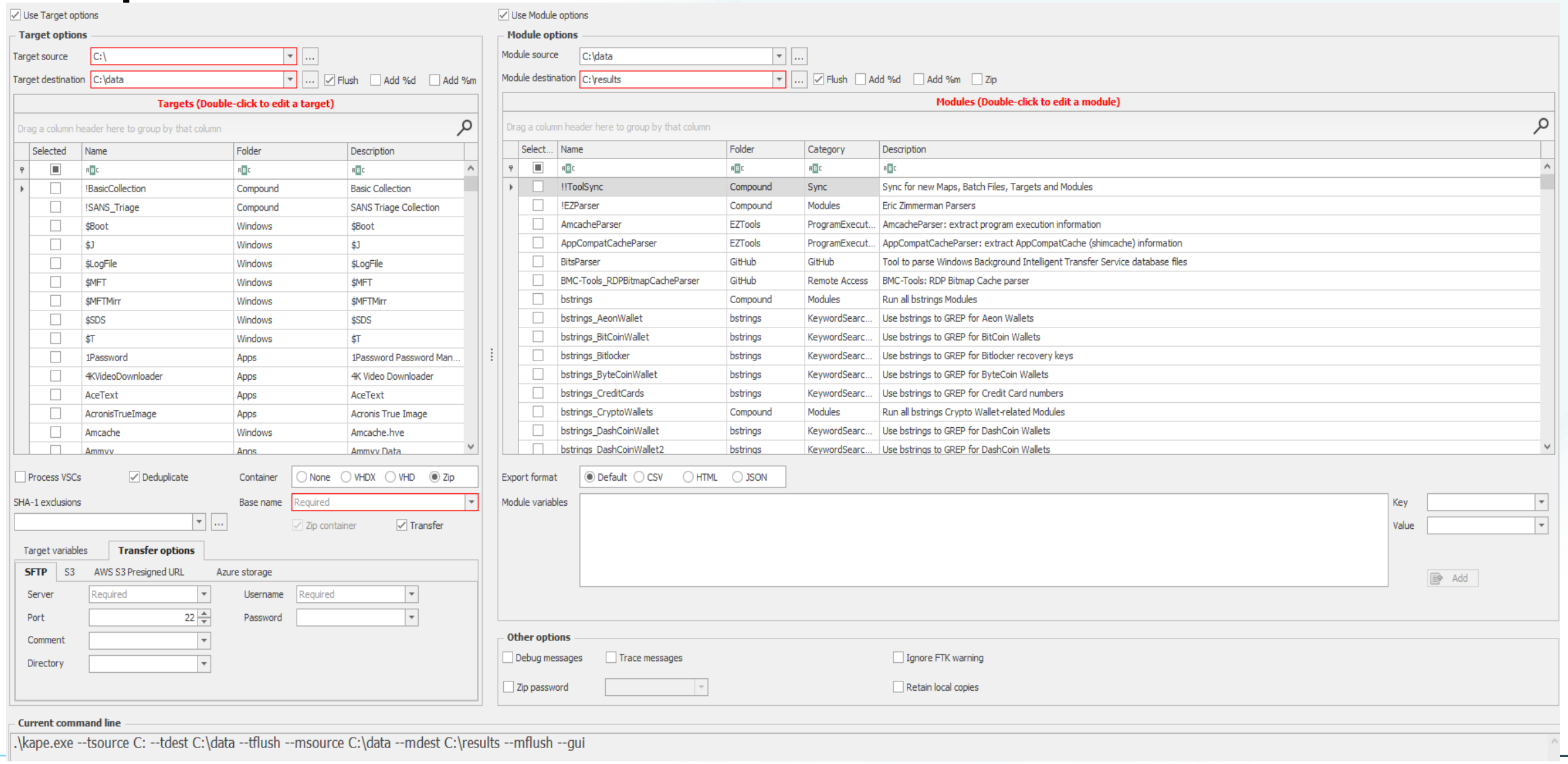
SOC FORUM 2023

Алгоритм работы KAPE



Kape GUI

SOC FORUM 2023



Kape targets

SOC FORUM 2023

```
Description: SANS Triage Collection
Author: Mark Hallman
Version: 1.3
Id: 1bfbd59d-6c58-4eeb-9da7-1d9612b79964
RecreateDirectories: true
Targets:
    -
        Name: Antivirus
        Category: Antivirus
        Path: Antivirus.tkape
    -
        Name: CloudStorage_Metadata
        Category: Apps
        Path: CloudStorage_Metadata.tkape
    -
        Name: CombinedLogs
        Category: WindowsLogs
        Path: CombinedLogs.tkape
    -
        Name: EvidenceOfExecution
        Category: EvidenceOfExecution
        Path: EvidenceOfExecution.tkape
    -
        Name: FileSystem
        Category: FileSystem
        Path: FileSystem.tkape
    -
        Name: LNKFilesAndJumpLists
        Category: LNKFiles
        Path: LNKFilesAndJumpLists.tkape
    -
        Name: MessagingClients
        Category: MessagingClients
        Path: MessagingClients.tkape
    -
```

```
Description: LNK Files and jump lists
Author: Eric Zimmerman, Andrew Rathbun, Yogesh Khatri
Version: 1.3
Id: 2e354bdc-e418-438e-8439-c21c83c64e90
RecreateDirectories: true
Targets:
    -
        Name: LNK Files from Recent
        Category: LNKFiles
        Path: C:\Users\%user%\AppData\Roaming\Microsoft\Windows\Recent\
        Recursive: true
        Comment: Also includes automatic and custom jumplist directories
    -
        Name: LNK Files from Microsoft Office Recent
        Category: LNKFiles
        Path: C:\Users\%user%\AppData\Roaming\Microsoft\Office\Recent\
        Recursive: true
    -
        Name: Start Menu LNK Files
        Category: LNKFiles
        Path: C:\Users\%user%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
        FileMask: '*.LNK'
    -
        Name: LNK Files from Recent (XP)
        Category: LNKFiles
        Path: C:\Documents and Settings\%user%\Recent\
        Recursive: true
    -
        Name: Desktop LNK Files XP
        Category: LNKFiles
        Path: C:\Documents and Settings\%user%\Desktop\
        FileMask: '*.LNK'
    -
```

Kape modules

SOC FORUM 2023

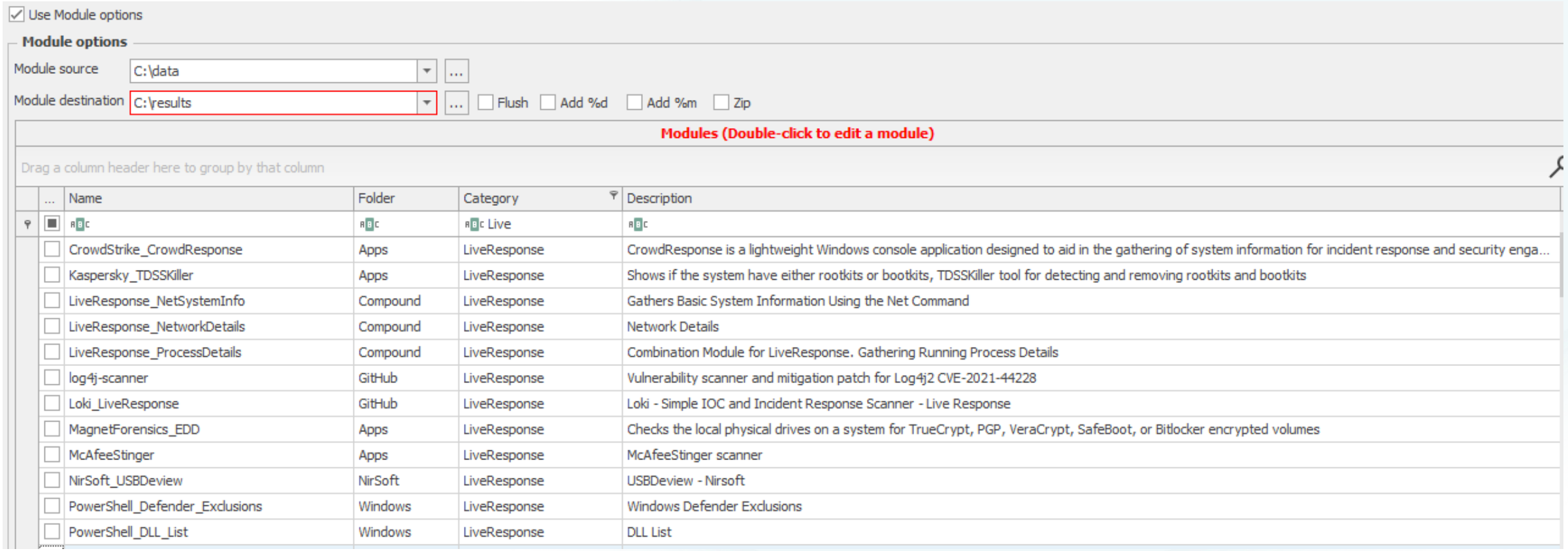
```
Description: Eric Zimmerman Parsers
Category: Modules
Author: Phill Moore
Version: 1.4
Id: f531e7cc-c9f3-4d04-881b-dbc89d1e7f38
BinaryUrl: https://ericzimmerman.github.io/
ExportFormat: csv
Processors:
    -
        Executable: AmcacheParser.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: AppCompatCacheParser.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: EvtxECmd.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: JLECmd.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: LECmd.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: MFTECmd.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: PECmd.mkape
        CommandLine: ""
        ExportFormat: ""
    -
```

```
Description: 'AmcacheParser: extract program execution information'
Category: ProgramExecution
Author: Eric Zimmerman
Version: 1.1
Id: 4190c518-524f-4623-8038-a014784c018c
BinaryUrl: https://f001.backblazeb2.com/file/EricZimmermanTools/AmcacheParser.zip
ExportFormat: csv
FileMask: Amcache.hve
Processors:
    -
        Executable: AmcacheParser.exe
        CommandLine: -f %sourceFile% --csv %destinationDirectory% -i --mp
        ExportFormat: csv

# Documentation
# https://github.com/EricZimmerman/AmcacheParser
# https://binaryforay.blogspot.com/2015/07/amcacheparser-reducing-noise-finding.html
# https://www.youtube.com/watch?v=ZKlyu-HOvxY
# https://www.youtube.com/watch?v=GhCZfCzn210
```

Kape Live Incident Response

SOC FORUM 2023



Use Module options

Module options

Module source: C:\data

Module destination: C:\results

Flush | Add %d | Add %m | Zip

Modules (Double-click to edit a module)

Drag a column header here to group by that column

...	Name	Folder	Category	Description
			Live	
	CrowdStrike_CrowdResponse	Apps	LiveResponse	CrowdResponse is a lightweight Windows console application designed to aid in the gathering of system information for incident response and security enga...
	Kaspersky_TDSSKiller	Apps	LiveResponse	Shows if the system have either rootkits or bootkits, TDSSKiller tool for detecting and removing rootkits and bootkits
	LiveResponse_NetSystemInfo	Compound	LiveResponse	Gathers Basic System Information Using the Net Command
	LiveResponse_NetworkDetails	Compound	LiveResponse	Network Details
	LiveResponse_ProcessDetails	Compound	LiveResponse	Combination Module for LiveResponse. Gathering Running Process Details
	log4j-scanner	GitHub	LiveResponse	Vulnerability scanner and mitigation patch for Log4j2 CVE-2021-44228
	Loki_LiveResponse	GitHub	LiveResponse	Loki - Simple IOC and Incident Response Scanner - Live Response
	MagnetForensics_EDD	Apps	LiveResponse	Checks the local physical drives on a system for TrueCrypt, PGP, VeraCrypt, SafeBoot, or Bitlocker encrypted volumes
	McAfeeStinger	Apps	LiveResponse	McAfeeStinger scanner
	NirSoft_USBDeview	NirSoft	LiveResponse	USBDeview - Nirsoft
	PowerShell_Defender_Exclusions	Windows	LiveResponse	Windows Defender Exclusions
	PowerShell_DLL_List	Windows	LiveResponse	DLL List

Собственный модуль LiveResponseAll

SOC FORUM 2023

Хостовая телеметрия (powershell скрипт)

(процессы, службы, драйвера, задачи планировщика, logon сессии, сетевые соединения, сетевые настройки, установленные обновления/ПО,...)

Сканеры памяти (IoC/IoA, yara)

Moneta, PE-Sieve, Get-InjectedThread, Hollows_hunter, YaraMemoryScanner

Сканеры хоста (yara, sigma)

Loki, Chainsaw, Hayabusa

Артефакты хоста (автозагрузка)

Autoruns (powershell), Kansa

Удаленный запуск модуля LiveResponse

SOC FORUM 2023

Kape и все необходимые модули расположены на отдельном сервере

Сервер доступен по SMB UNC

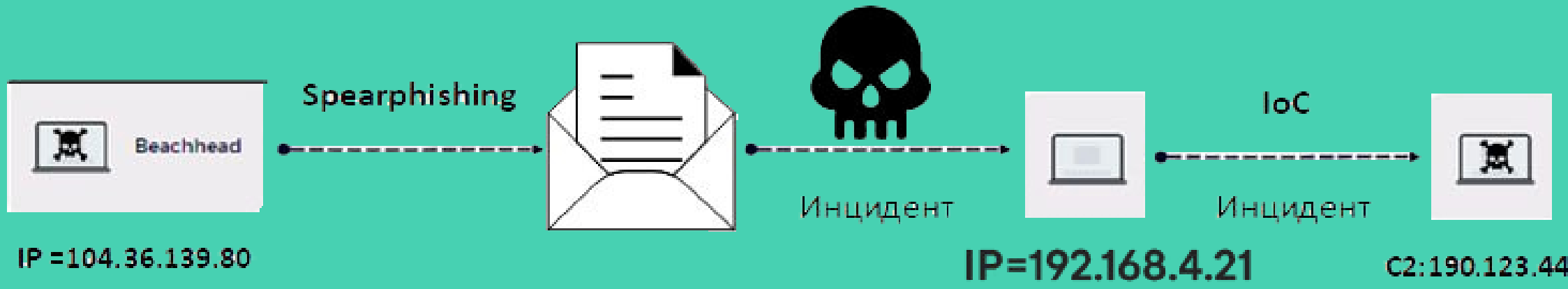
На сервере хранится PS скрипт, запускающий kape на удаленных хостах

Результаты по каждому хосту хранятся на выделенном сервере

Launches script for list of targets	$Session = New-PSSession - ComputerName (Get-Content computers.txt)
Stars of Job on Remote Target	Invoke-Command -Session $Session -ScriptBlock {
Runs KAPE	Start-Job - scriptblock { \\Server-A\KAPE\kape.exe }}

Сценарий вредоносного заражения

SOC FORUM 2023



Задетектированы инциденты:

- Фишинговая рассылка на сотрудников компании
- Обращение к вредоносному C2 домену (критичность = высокая)

Настройки модуля KAPE

SOC FORUM 2023

Командная строка для запуска: .\kape.exe --scs 89.214.32.45 --scp 22 --scu user --scpw P@ssw0rd --msource C:\ --mdest C:\results --module LiveResponseAll

- Скомпрометированный хост: 192.168.4.21
- Типы артефактов:
  - Хостовая телеметрия (запущенные процессы,сетевые соединения ...)
  - Индикаторы атаки на хосте (файловая система, Eventlog)
  - Индикаторы атаки в памяти

Собственный модуль LiveResponse

SOC FORUM 2023

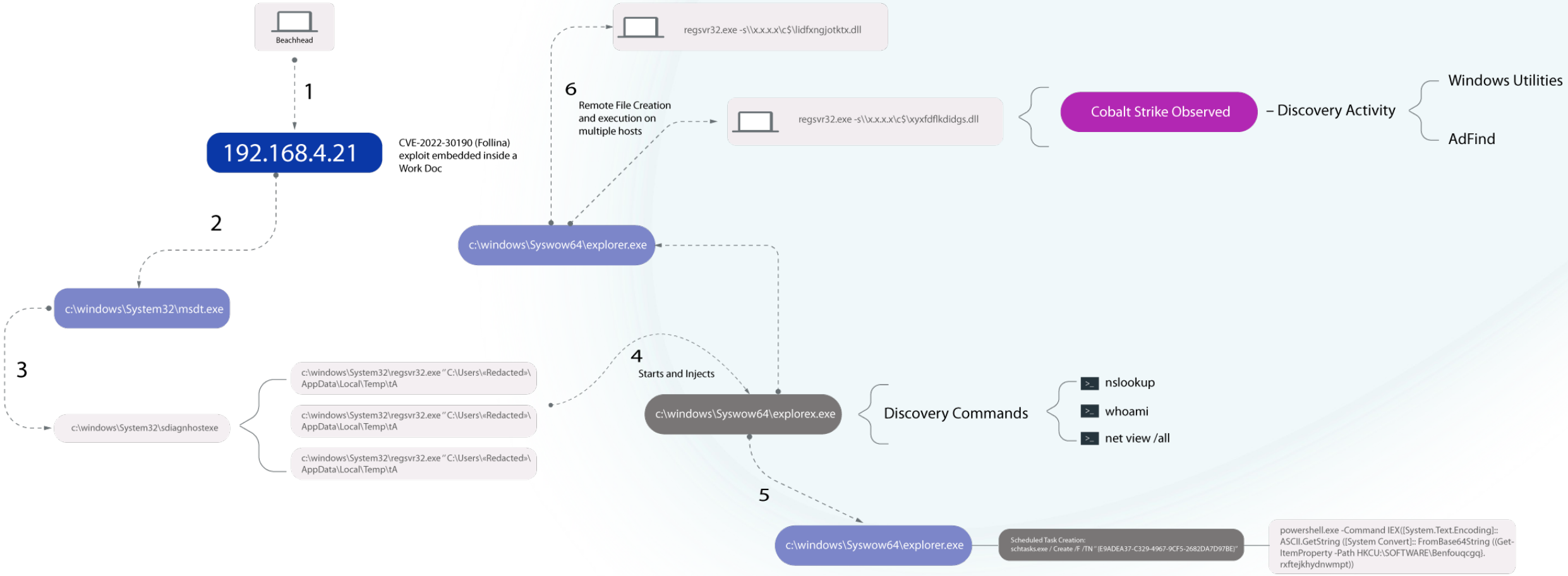
```
Description: LiveResponse modules
Category: Modules
Author: Security Vision
Version: 0.9
Id: d97624f2-d942-4c08-9ef4-8206087037b3
BinaryUrl:
ExportFormat: csv
Processors:
    -
        Executable: Get-Artifacts.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: YaraMemoryScanner.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: MonetaScanner.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: Get-InjectedThread.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: PE-Sieve.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: Chainsaw.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: Hayabusa.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: Loki.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable:  Autoruns.mkape
        CommandLine: ""
        ExportFormat: ""
```

```
Description: Powershell модуль, собирающий телеметрию с хоста
Category: LiveResponse
Author: Security Vision
Version: 0.9
Id: 32a4d8a5-e3ee-40d2-a242-afb158efa493
BinaryUrl:
ExportFormat: json
Processors:
    -
        Executable: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
        CommandLine: "& '%kapeDirectory%\\Modules\\bin\\Get-Artifacts.ps1' -all"
        ExportFormat: json

# Documentation
# Powershell модуль, собирающий телеметрию с хоста
(процессы, службы, драйвера, задачи планировщика, logon сессии, сетевые соединения,
сетевые настройки, установленные обновления/ПО,...)
```

Цепочка заражения тестового сценария

SOC FORUM 2023



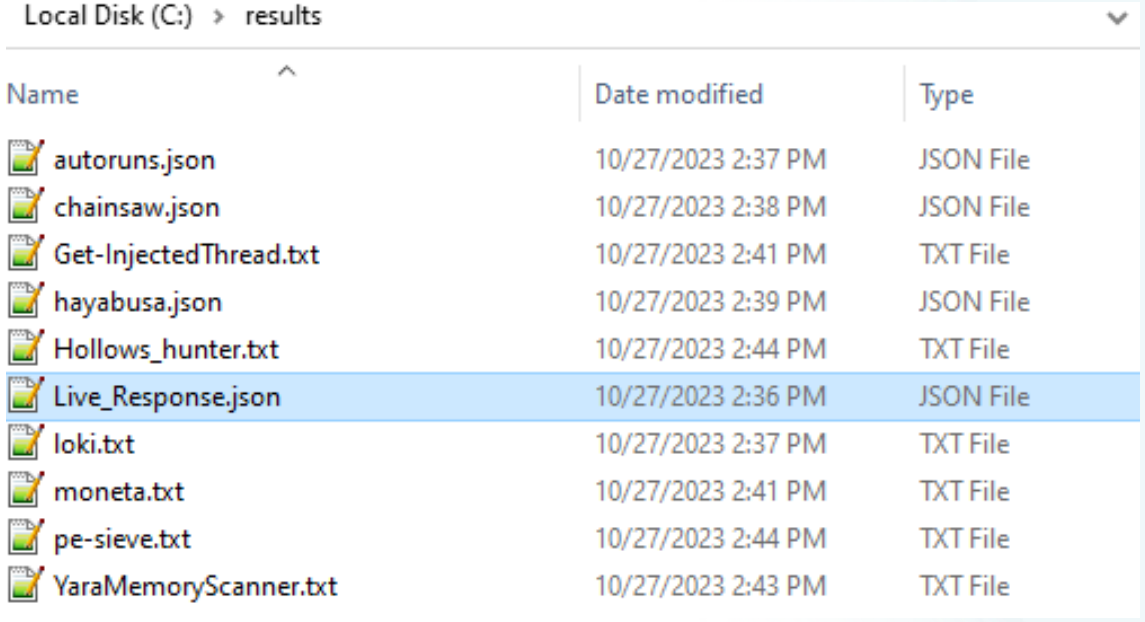
Собранные артефакты Kape

SOC FORUM 2023

Этап	Артефакт	Модуль	Источник
0	Сетевые соединения, запущенные процессы, установленные обновления ОС	LiveResponse.ps1, Kansa	Файловая система
1.	Вредоносный docx, Follina	Loki	Файловая система
2.	Цепочка Winword - msdt	Chainsaw, Hayabusa	Eventlog
	Powershell encoded		
3.	Запуск regsvr32 с dll в каталоге Temp	Chainsaw, Hayabusa	
4.	Запуск Explorer, используя технику Process Hollowing	Moneta, Hollows_Hunter	Память
	Инжектирование Cobalt Strike	Moneta, Get-InjectedThread, YaraMemoryScanner	
	Запуск команд сбора данных (net, whoami, nslookup, adfind)	Chainsaw, Hayabusa	Eventlog
	Компрометация УЗ	Chainsaw, Hayabusa	Sysmon logs
5.	Создание задачи планировщика	LiveResponse.ps1, autoruns.ps1	Файловая система
6.	Запуск regsvr32 с dll в сетевой шаре на хостах	Chainsaw, Hayabusa	Eventlog

Результаты работы модуля Kape (LiveResponse.ps1)

SOC FORUM 2023




```
"NETSTAT":  [
        {
            "Protocol":  "TCP",
            "LocalAddress":  "0.0.0.0",
            "LocalPort":  "22",
            "RemoteAddress":  "0.0.0.0",
            "RemotePort":  "0",
            "State":  "LISTENING",
            "ProcessName":  "sshd",
            "PID":  "4168",
            "Path":  "C:\\Program Files\\OpenSSH\\sshd.exe"
        },
        {
            "Protocol":  "TCP",
            "LocalAddress":  "0.0.0.0",
            "LocalPort":  "135",
            "RemoteAddress":  "0.0.0.0",
            "RemotePort":  "0",
            "State":  "LISTENING",
            "ProcessName":  "svchost",
            "PID":  "1128",
            "Path":  "C:\\WINDOWS\\system32\\svchost.exe"
        },
        {
            "Protocol":  "TCP",
            "LocalAddress":  "192.168.4.21",
            "LocalPort":  "35922",
            "RemoteAddress":  "190.123.44.126",
            "RemotePort":  "443",
            "State":  "ESTABLISHED",
            "ProcessName":  "Regsvr32.exe",
            "PID":  "11640",
            "Path":  "C:\\WINDOWS\\system32\\Regsvr32.exe"
        },
```

Результаты работы модуля Kape (LiveResponse.ps1)

SOC FORUM 2023


```
"SCHED_TASKS":  [
                    {
                        "task":  "{E9ADEA37-C329-4967-9CF5-2682DA7D97BE}",
                        "task_path":  "powershell -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\SOFTWARE\Benfouqcgq\rxftejkhydnwmpt))",
                        "status":  "Ready",
                        "user":  "SYSTEM"
                    },
                    {
                        "task":  "\\MicrosoftEdgeUpdateTaskMachineCore",
                        "task_path":  "C:\\Program Files (x86)\\Microsoft\\EdgeUpdate\\MicrosoftEdgeUpdate.exe /c",
                        "status":  "Ready",
                        "user":  "SYSTEM"
                    },
                    {
                        "task":  "\\Adobe Acrobat Update Task",
                        "task_path":  "C:\\Program Files (x86)\\Common Files\\Adobe\\ARM\\1.0\\AdobeARM.exe ",
                        "status":  "Ready",
                        "user":  "INTERACTIVE"
                    },
                    {
                        "task":  "\\GoogleUpdateTaskMachineCore{C31B1408-A566-4AC7-B1E5-08974C581461}",
                        "task_path":  "C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe\" /c\"",
                        "status":  "Ready",
                        "user":  "SYSTEM"
                    },
                    {
```

Результаты работы модуля Kape (Chainsaw)

SOC FORUM 2023


```
{
    "group": "Sigma",
    "kind": "individual",
    "document": {
        "kind": "evtx",
        "data": {
            "Event": {
                "EventData": {
                    "CommandLine": "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotLi
                    "[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyX
                    "raWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCYmZm9y
                    "UFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRlY29kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw==='+[char]34+'))'))))i/../../../../../../../
                    "Image": "C:\WINDOWS\system32\msdt.exe",
                    "IntegrityLevel": "Medium",
                    "LogonId": "0x13531",
                    "ParentImage": "C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE",
                    "User": "WIN10\\test",
                    "UtcTime": "2023-10-18 17:51:13"
                },
                "System": {
                    "Channel": "Security",
                    "Computer": "WIN10",
                    "EventID": 4688,
                    "EventRecordID": 18851,
        }
    },
    "name": "Potential Arbitrary Command Execution Using Msdt.EXE",
    "timestamp": "2022-05-18T12:10:10",
    "authors": [
        "Florian Roth (Nextron Systems)"
    ],
    "level": "medium",
    "source": "sigma",
    "status": "experimental",
    "id": "b236190c-1c61-41e9-84b3-3fe03f6d76b0",
    "logsource": {
        "category": "process_creation",
        "product": "windows"
    },
    "references": [
        "https://app.any.run/tasks/713f05d2-fe78-4b9d-a744-f7c133e3fafb/"
    ],
    "tags": [
        "attack.defense_evasion",
        "attack.t1202"
    ]
},
```

```
{
    "group": "Sigma",
    "kind": "individual",
    "document": {
        "kind": "evtx",
        "data": {
            "Event": {
                "EventData": {
                    "CommandLine": "C:\\Users\\test\AppData\\Local\\Temp\\t.A",
                    "Image": "C:\\Windows\\System32\\regsvr32.exe",
                    "IntegrityLevel": "Medium",
                    "LogonId": "0x13531",
                    "ParentImage": "C:\\Windows\\System32\\sdiagnhost.exe",
                    "User": "WIN10\\test",
                    "UtcTime": "2023-10-18 17:51:14.254"
                },
                "System": {
                    "Channel": "Security",
                    "Computer": "WIN10",
                    "EventID": 4688,
                    "EventRecordID": 18851,
        }
    },
    "name": "Regsvr32 Execution From Potential Suspicious Location",
    "timestamp": "2019-05-18T17:51:14.254967+00:00",
    "authors": [
        "Florian Roth (Nextron Systems)"
    ],
    "level": "medium",
    "source": "sigma",
    "status": "experimental",
    "id": "b236190c-1c61-41e9-84b3-3fe03f6d76b0",
    "logsource": {
        "category": "process_creation",
        "product": "windows"
    },
    "references": [
        "https://app.any.run/tasks/34221348-072d-4b70-93f3-aa71f6ebecad/"
    ],
    "tags": [
        "attack.defense_evasion",
        "attack.t1218.010"
    ]
},
```

Результаты работы модуля Kape (hollows_hunter, Get-InjectedThreads)

SOC FORUM 2023


```
{
 "scan_date_time" : "10/27/23 09:27:29",
 "scan_timestamp" : 1698424049,
 "scan_time_ms" : 23000,
 "scanned_count" : 167,
 "suspicious_count" : 2,
 "suspicious" : [
  {
   "pid" : 5780,
   "is_managed" : 0,
   "name" : "explorer.exe",
   "replaced" : 0,
   "hdr_modified" : 0,
   "implanted_pe" : 4,
   "implanted_shc" : 0,
   "unreachable_file" : 0,
   "other" : 0
  },
  {
   "pid" : 4824,
   "is_managed" : 0,
   "name" : "regsvr32.exe",
   "replaced" : 0,
   "hdr_modified" : 0,
   "implanted_pe" : 4,
   "implanted_shc" : 0,
   "unreachable_file" : 0,
   "other" : 0
  }
 ]
}
```

```
{
    "ProcessName": "explorer.exe",
    "ProcessId": 5780,
    "Path": "C:\\WINDOWS\\Explorer.EXE",
    "KernelPath": "C:\\Windows\\explorer.exe",
    "CommandLine": "C:\\WINDOWS\\Explorer.EXE",
    "PathMismatch": false,
    "ThreadId": 2200,
    "ThreadStartTime": "/Date(1698423328116)/",
    "AllocatedMemoryProtection": 64,
    "MemoryProtection": 64,
    "MemoryState": 4096,
    "MemoryType": 131072,
    "BasePriority": 8,
    "IsUniqueThreadToken": false,
    "Integrity": "MEDIUM_MANDATORY_LEVEL",
    "Privilege": "SeChangeNotifyPrivilege",
    "LogonId": "999",
    "SecurityIdentifier": "S-1-5-21-3163525606-1107823640-3692433694-1001",
    "UserName": "DESKTOP-9MVDBS5\\SYSTEM",
    "LogonSessionStartTime": {
        "value": "/Date(1698336465820)/",
        "DateTime": "Thursday, October 26, 2023 9:07:45 AM"
    },
    "LogonType": "System",
    "AuthenticationPackage": "NTLM",
    "BaseAddress": 485949440,
    "Size": 204800,
    "Bytes": [252, 72, 137, 206,]
}
```

Преимущества собственного модуля LiveResponseAll

SOC FORUM 2023

- Поддержка json output всеми командами в отличие от команд ОС (net,netstat,nslookup,wmic,…)
- Добавлены новые forensics инструменты (сканеры памяти, сканеры IoC/IoA, данные по ОС)
- Часть модулей переписаны на powershell (autorunsc)
- Автоматическая загрузка недостающих модулей
- Автоматический удаленный запуск

SOC FORUM 2023

Вопросы?