

Análisis de amenazas en artefactos forenses de Windows

Laboratorio

Análisis artefactos forenses de Windows

1.Laboratorio

En este laboratorio aprenderemos cómo analizar artefactos forenses de sistemas Windows utilizando herramientas como Chainsaw, una utilidad diseñada para buscar y analizar registros de eventos, y las reglas Sigma, un lenguaje abierto y estándar para la detección de eventos. Discutiremos los fundamentos de estas herramientas, su implementación práctica en un laboratorio, y cómo se pueden combinar para identificar patrones de actividad maliciosa. Además, se incluirán ejemplos prácticos para configurar un entorno de laboratorio y ejecutar análisis efectivos.

2. Sigma Rules

Las reglas Sigma son un estándar abierto para la detección de amenazas en sistemas de información. Están diseñadas para describir patrones o indicadores de actividad sospechosa en registros de eventos (logs) de forma comprensible y flexible, similar a cómo las reglas YARA se utilizan para identificar malware en archivos.

Características principales de las reglas Sigma:

Estandarización:

Sigma proporciona un formato común para definir detecciones, independientemente de la plataforma o solución de monitoreo (como SIEMs: Splunk, Elastic, etc.).

Simplicidad:

Las reglas están escritas en un formato **legible por humanos** (usualmente YAML), lo que facilita su comprensión y modificación por analistas.

Independencia de la plataforma:

No dependen de un proveedor o herramienta específica. Una regla Sigma puede traducirse a diferentes lenguajes de consulta mediante herramientas como el **Sigma Converter**.

Estructura básica de una regla Sigma: Las reglas se organizan en secciones clave como:

- **title**: Nombre descriptivo de la regla.
- id: Identificador único (UUID) para la regla.
- description: Explicación del objetivo de la regla.



- **logsource**: Fuente de los registros (por ejemplo, Windows Event Logs, Apache Logs).
- detection: Criterios específicos de detección.
- level: Nivel de severidad (informativo, bajo, medio, alto, crítico).

Ejemplo:

title: Suspicious Process Execution id: a1b2c3d4-5678-90ab-cdef-1234567890ab description: Detecta la ejecución de procesos sospechosos. logsource: category: process_creation product: windows detection: selection: CommandLine | contains: ['powershell.exe', '-enc']

condition: selection

level: high

Uso práctico:

Ciberseguridad: Detección de actividad maliciosa como movimientos laterales, escalación de privilegios, malware, etc.

Respuesta a incidentes: Proporciona alertas específicas basadas en comportamientos definidos.

Análisis de amenazas: Ayuda a identificar patrones específicos de actores de amenazas.

Conversión:

Las reglas Sigma pueden traducirse a consultas específicas de herramientas (como Splunk SPL o Elastic Query DSL) usando herramientas como **Sigmac**.



3. Chainsaw

Chainsaw es una herramienta open-source que analiza registros de eventos de Windows utilizando técnicas avanzadas como:

- **Búsqueda basada en Sigma rules**: Sigma es un estándar de reglas genéricas para detección de amenazas que se traduce a múltiples herramientas SIEM. Chainsaw soporta estas reglas para identificar actividad sospechosa en registros.
- Análisis de patrones de ataque comunes: Chainsaw incluye heurísticas específicas para detectar actividades relacionadas con técnicas conocidas del MITRE ATT&CK.
- **Desempeño optimizado:** Diseñado para manejar grandes cantidades de registros sin sacrificar velocidad o precisión.

https://github.com/WithSecureLabs/chainsaw

Casos de uso

- Identificación de anomalías: Buscar eventos inusuales como inicios de sesión fallidos repetitivos, cambios en las políticas de auditoría o ejecuciones de scripts PowerShell con parámetros maliciosos.
- Detección de actividad lateral: Rastrear movimientos laterales en la red, como conexiones remotas sospechosas o uso de herramientas como PsExec.
- **Búsqueda de IOCs:** Analizar los registros para encontrar Indicadores de Compromiso (IPs, hashes, o cadenas específicas).
- Verificación post-intrusión: Recolectar evidencia tras un incidente para entender el alcance del ataque.

Flujo típico de trabajo con Chainsaw

Recolección de logs:

• Exportar los registros de eventos relevantes desde los sistemas Windows comprometidos o sospechosos, por ejemplo:

wevtutil epl Security logs.evtx



Ejecución de Chainsaw:

• Análisis básico: Escanear los registros con reglas Sigma predefinidas:

./chainsaw.exe hunt evtx_attack_samples/ -s sigma/ --mapping mappings/sigma-event-logs-all.yml

• Búsqueda de palabras clave: Buscar patrones específicos:

Search for the case-insensitive word 'mimikatz':

./chainsaw search mimikatz -i evtx_attack_samples/

Search for Powershell Script Block Events (EventID 4014):

./chainsaw search -t 'Event.System.EventID: =4104' evtx_attack_samples/

• Generación de resúmenes: Identificar eventos de alto interés como cuentas creadas o cambios de privilegios:

chainsaw timeline logs.evtx

Análisis de resultados:

• Los resultados se presentan en formatos estructurados y filtrados, facilitando el análisis rápido de eventos relevantes.

Toma de acción:

 Aislar máquinas comprometidas, implementar bloqueos en firewalls o ajustes en políticas de seguridad basados en los hallazgos.

Ventajas de Chainsaw

- **Portabilidad**: Funciona en sistemas locales sin necesidad de infraestructura adicional.
- Velocidad: Procesa grandes volúmenes de registros rápidamente.
- Integración con Sigma: Aprovecha una librería de reglas comunitarias y personalizables.
- Facilidad de uso: Su sintaxis es simple y amigable para analistas.



4. Laboratorio practico

Descargar las herramientas y fuentes de datos de prueba (Visor de eventos de Windows EVTX):

1. Descargar Chainsaw:

https://github.com/WithSecureLabs/chainsaw/tree/master?tab=readme -ov-file#downloading-and-running

2. Descargar reglas SIGMA:

https://github.com/SigmaHQ/sigma

3. <u>Descargar samples de logs de eventos de Windows:</u>

https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES

Para este laboratorio utilizaremos los eventos de "Credential Access".

Tareas a realizar:

1. Analizar registros de acceso y volcado a NTDS:

C:\chainsaw>chainsaw.exe search NTDS.dit -i "EVTX-ATTACK-SAMPLES-master\Credential Access"

A. Indicar hostname y dominio del equipo al que se ha accedido.

HOSTNAME: DC1

DOMINIO: insecurebank

B. Indicar username del usuario que ha accedido.

USERNAME: bob



```
---
Vert_attributes:
xmlns: http://schemas.microsoft.com/win/2004/08/events/event
Event:
System:
Provider_attributes:
    Name: ESENT
EventID_attributes:
    Qualifiers: 0
EventID: 325
Level: 4
Task: 1
Keywords: '0x80000000000'
TimeCreated_attributes:
    SystemTime: 2019-11-26T23:55:00.000000Z
EventRecordID: 1970
Channel: Application
Computer: DC1.insecurebank.local
Security: null
EventData:
    NTDS
    - '3392'
    ''
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
    '
```

2. Analizar si se ha ejecutado mimikatz sobre algún equipo.

C:\chainsaw>chainsaw.exe search mimikatz -i "EVTX-ATTACK-SAMPLES-master\Credential Access'

A. Indicar hostname del equipo:

HOSTNAME: PC04

B. Indicar username del usuario que lo ejecutó.

USERNAME: IEUser

C. Indicar la ruta en donde se ejecutó mimikatz.

RUTA: c:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe

<pre>xmlDrs: http://schemas.microsoft.com/win/2004/08/events/event Event: Vent: Vent: Provider_attributes: Name: Microsoft-Mindows-Sysmon Guid: 5770385F-C22A-43E0-BF4C-06F5698FFBD9 EventD1: 10 Version: 3 Level: 4 Task: 10 Opcode: 0 Keywords: '0×88000000000000' Keywords: '0×88000000000000' TimeCreated_attributes: SystemTime: 2019-03-17T19:37:11.661930Z EventRecords: '0×88000000000000' Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 ChannelMicrosoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserDID: 5-15-18 EventData: RuleName: '' Utcrime: 2019-03-17 19:37:11.641 SourceProcessGUID: 365A8072-AIE3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365A8072-AIE3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365A8072-AIE3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365A8072-AIE3-SC8E-0000-0010S60000 TargetProcessGUID: 365A8072-AIE3-SC8E-0000-0010S60000 TargetProcessGUID: 365A8072-AIE3-SC8E-0000-0010S60000 TargetProcessGUID: 365A8072-AIE3-SC8E-0000-0010S600000 TargetProcessGUID: 365A8072-AIE3-SC8E-0000-0010S60000 TargetProcessGUID: 365A8072-AIE3-SC8E-0000-0010S600000 TargetProcessGUID: 365A8072-AIE3-SC8E-0000-0010S600000 TargetP</pre>	Event attributes:
Event: System: Provider attributes: Name: Microsoft-Windows-Sysmon Guid: 5770385F-C22A-43E0-BF4C-06F5698FF8D9 EventID: 10 Version: 3 Level: 4 Task: 10 Opcode: 0 Keywords: '0x800000000000000 TimeCreated_attributes: Systemine: 2019-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2022 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-3-18 EventData: SourceProcessID: 365AB972-A1E3-SCBE-0000-0010CEF72200 SourceProcessID: 365AB972-A1E3-SCBE-0000-0010CEF72200 SourceProcessID: 365AB972-A1E3-SCBE-0000-0010SEF7200 SourceProcessID: 365AB972-A1E3-SCBE-0000-0010SEF7200 SourceProcessID: 365AB972-A1E3-SCBE-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF72200 SourceProcessID: 365AB972-055CBF-0000-0010SEF7200 SourceProcessID: 365AB972-055CBF-0000-0010SEF7200 SourceProcessID: 365AB972-055CBF-0000-0010SEF7200 SourceProcessID: 365AB972-055CBF-0000-0010SEF7200 SourceProcessID: 365AB972-055CBF-0000-0010SEF7200 SourceProcessID: 365AB972-055CBF-0000-0010SEF7200 SourceProcessID:	<pre>xmlns: http://schemas.microsoft.com/win/2004/08/events/event</pre>
<pre>System: Provider_attributes: Name: Microsoft-Windows-Sysmon Guid: 5770385F-C22A-43E0-BF4C-06F5600FFBD9 EventID: 10 Version: 3 Level: 4 Task: 10 Opcode: 0 Reywords: '0x80000000000000' TimeCreated_attributes: SystemTime: 2019-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessGUI: 365ABB72-A1E3-5CBE-0000-0010CEF72200 SourceProcessGI: 3548 SourceInreadId: 2272 SourceProcessGI: 354872-0886-5CBF-0000-0010CEF72200 SourceProcessGI: 3588 SourceInreadId: 2272 SourceTmage: C:Windows/System32\lsass.exe GrantedAccess: 'Wol10' TargetProcessGI: 355HB72-0886-5CBF-0000-00100EF72200 SourceProcessGI: 3548 SourceInreadId: 2272 SourceTmage: C:Windows/System32\lsass.exe GrantedAccess: 'Wol10' TargetProcessGI: 355HB72-0886-5CBF-0000-001030500000 TargetProcessGI: 355HB72-0886-5CBF-00000-001030500000 TargetProcessGI: 272 SourceTmage: C:Windows/System32\lsass.exe GrantedAccess: 'Wol10' TargetProcessGI: 476 TargetTmage: C:Windows/System32\lsass.exe GrantedAccess: 'Wol10' TargetProcessGI: 227 SourceTmage: C:Windows/System32\lsass.exe G</pre>	Event:
<pre>Provider_attributes: Name: Microsoft-Kindows-Sysmon Guid: 5770385F-C22A-43E0-BF4C-06F5696FFBD9 EventID: 10 Version: 3 Level: 4 Task: 10 Opcode: 0 Keywords: '0x8000000000000000 Opcode: 0 Keywords: '0x800000000000000 TimeCreated_attributes: SystemTime: 2010-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2010-03-17 19:37:11.641 SourceProcessGID: 365AB872-A1E3-SCBE-0000-0010CEF72200 SourceProcessGID: 365AB872-A1E3-SCBE-0000-0010CEF72200 SourceProcessGID: 365AB872-A1E3-SCBE-0000-001030560000 TargetProcessGID: 365AB872-0886-SCBF-0000-001030560000 TargetProcessGID: 365AB872-0886-SCBF-0000-00103056000 TargetProcessGID: 365AB872-0886-SCBF-0000-001030560000 TargetProcessGID: 365AB872-0886-SCBF-0000-001030560000 TargetProcessGID: 36</pre>	System:
<pre>Name: Microsoft-Windows-Sysmon Guid: 5770385r-C22A-43E0-BF4C-06F5608FFBD9 EventID: 10 Version: 3 Level: 4 Task: 10 Opcode: 0 Keywords: '0x8000000000000' TimeCreated_attributes: SystemTime: 2019-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 ChannelMicrosoft-Windows-Sysmon/Operational Computer: PC04.example.com Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessID: 365AB872-A1E3-5C8E-0000-0010CEF72200 SourceProcessId: 3588 SourceThreadId: 2272 SourceProcessId: 3588 SourceThreadId: 2272 SourceProcessId: 3588 SourceThreadId: 2272 SourceTamage: C:Windows/system32\lsass.exe GrantedAccess: 'Wol10' TargetTamage: C:Windows/SysTeM32\ndtl.dll+4595c[C:\Windows\system32\KERMELBASE.dll+8185[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz_trunk\Win32\mimikatz_trunk\Win32\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5286[C:\Users\TEUser\Desktop\mimikatz_</pre>	Provider attributes:
<pre>Guid: 5770385F-C22A-43E0-BF4C-06F5698FFBD9 EventID: 10 Version: 3 Level: 4 Task: 10 Opcode: 0 Keywords: '0x80000000000000000 TimeCreated_attributes: SystemTime: 2019-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadDD: 2032 Channel: Microsoft.windows.system0/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtCrime: 2019-03-17 19:37:11.641 SourceProcessID: 36ABB72-A1E3-SGE-0000-0010CEF72200 SourceProcessID: 36ABB72-A1E3-SGE-0000-0010CEF72200 SourceProcessID: 36ABB72-A1E3-SGE-0000-0010CEF72200 SourceProcessID: 36SABB72-A1E3-SGE-0000-0010050000 TargetProcessID: 36SABB72-A1E3-SGE-0000-001030500000 TargetProcessID: 36SABB72-ME3-SGE-0000-001030500000 TargetProcessID: 36SAB72-ME3-SGE-0000-001030500000 TargetProcessID: 36SAB72-ME3-SGE-0000-001030500000 TargetProcessID: 36SAB72-ME3-SGE-0000-001030500000 TargetProcessID: 476 TargetProcesS</pre>	Name: Microsoft-Windows-Sysmon
<pre>EventID: 10 Version: 3 Level: 4 Task: 10 Oprode: 0 Keywords: '0*800000000000000' TimeCreated_attributes: SystemTime: 2019-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 ChannelMicrosoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: S-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessGUD: 365ABB72-ALB:SCBE-0000-0010CEF72200 SourceProcessGID: 365ABB72-ALB:SCBE-0000-0010CEF72200 SourceProcessGID: 365ABB72-ALB:SCBE-0000-0010CEF72200 SourceProcessGID: 365ABB72-ALB:SCBE-0000-0010CEF72200 SourceProcessGID: 365ABB72-ALB:SCBE-0000-0010CEF72200 SourceProcessGID: 365ABB72-ALB:SCBE-0000-00100EEF72200 SourceProcessGID: 365ABB72-ALB:SCBE-0000-00100EEF72200 SourceProcessGID: 365ABB72-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365ABB72-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365ABB72-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF72200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-00100EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-001000EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-001000EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-001000EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-001000EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-001000EEF7200 SourceProcessGID: 365AB872-0886-SCB*-0000-001000EEF7200 SourceProcesGID: 365AB872-0886-SCB*-0000-001000EF7200 SourceProcesG</pre>	Guid: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
<pre>Version: 3 Level: 4 Task: 10 Opcode: 0 Keywords: '0x80000000000000000 TimeCreated_attributes: SystemTime: 2019-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 Channel: Microsoft.windows-Sysmon/Operational Computer: PC04.example.corp Security attributes: UserID: S-1-5-18 EventData: RuleWame: RuleWame: RuleWame: UserID: S-1-5-18 EventData: RuleWame: RuleWame: RuleWame: BourceInreadId: 2272 SourceInreadId: 2272</pre>	EventID: 10
Level: 4 Task: 10 Oprode: 0 Keyword: 0 Keyword: 0 Keyword: 0 Keyword: 0 Keyword: 0 SystemTime: 2019-03-1719:37:11.6619302 EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessID: 365AB872-A1E3-SCBE-0000-0010CEF72200 SourceProcessId: 3588 SourceThreadId: 2272 SourceTmage: C: VUsers\IFUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe TargetProcessId: 358AB872-0886-SCBF-0000-001030506000 TargetThrocessId: 476 TargetThrocessId: 476 TargetThroces	Version: 3
Task: 10 Opcode: 0 Keywords: '0×800000000000000 TimeCreated_attributes: systemTime: 2019-03-17119:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 Channel. Microsoft.windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleWame: RuleWame: RuleWame: RuleWame: RuleWame: SourceFrocessGID: 365AB872-A1E3-SC8E-0000-0010CEF72200 SourceFrocessGID: 365AB872-A1E3-SC8E-0000-0010CEF72200 SourceFrocessGID: 365AB872-A1E3-SC8E-0000-0010CEF72200 SourceFrocessGID: 365AB872-0886-SC8F-0000-0010SEF72200 SourceFrocessGID: 365AB872-0886-SC8F-0000-0010SEF7EFF TargetFrocesSGID: 365AB872-0886-SC8F-0000-0010SEF7EFF RuleWame: MiddawSLystem32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100wSLSYSTEM32LS8S.exe GrantedAccess: 'W100WSLSYSTEM32LS8SS.exe GrantedAccess: 'W100WSLSYSTEM32LS8SS.exe GrantedAccess: 'W100WSLSYSTEM32LS8SS.exe GrantedAccess:	Level: 4
<pre>Opcode: 0 Keywonds: '0x8000000000000' TimeCreated_attributes: SystemTime: 2010-03-17T19:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 ChannelMicrosoft.Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessID: 365ABB72-ALE3-SCBE-0000-0010CEF72200 SourceProcessId: 3588 SourceInreadId: 2272 SourceProcessId: 3588 SourceInreadId: 2272 SourceProcessId: 356ABB72-ALE3-SCBE-0000-0010CEF72200 SourceProcessId: 3588 SourceInreadId: 2272 SourceProcessId: 356ABB72-ALE3-SCBE-0000-00100EEF72200 SourceProcessId: 356ABB72-0886-SCBF-0000-001030560000 TargetProcessId: 356ABB72-0886-SCBF-0000-001030560000 TargetProcessId: 476 TargetInage: C: VUsersVIEUser/Desktop/mimikatz_trunk/Win32/mimikat2.exe GrantedAccess: 0x1010 mikatz_trunk/Win32/mimikatz.exe+5C80[C: \Users\IEUser/Desktop\mimikatz_trunk\Win32/mimikatz.exe+5C86[C: \Users\IEUser/Desktop\mimikatz_trunk\Win32/mimikatz.exe+5C86[C: \Users\IEUser\Desktop\mimikatz_trunk\Win32/mimikatz.exe+5C86[C: \Users\IEUser\Desktop\mimikatz_trunk\Win32/mimikatz.exe+5C862[C: \Users\IEUser\Desktop\mimikatz_trunk\Win32/mimikatz.exe+5C862[C: \Users\IEUser\Desktop\mimikatz_trunk\Win32/mimikatz.exe+5C862[C: \Users\IEUser\Desktop\mimikatz_trunk\Win32/mimikatz.exe+5C862[C: \Users\IEUser\Desktop\mimikatz_tr</pre>	Task: 10
<pre>keywords: '0x80000000000000' TimeCreated_attributes: SystemTime: 2019-03-17T19:37:11.661930Z EventRecordID: 4807 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2033 ChannelMicrosoft.windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-15-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessGUID: 365ABB72-AIE3-SC8E-0000-0010CEF72200 SourceProcessGID: 365ABB72-AIE3-SC8E-0000-0010CEF72200 SourceProcessGID: 365ABB72-AIE3-SC8E-0000-0010CEF72200 SourceProcessGID: 365ABB72-AIE3-SC8E-0000-00100EF72200 SourceProcessGID: 365ABB72-0886-SC8F-00000-001030500000 TargetProcessGID: 365ABB72-0886-SC8F-00000-001030500000 TargetProcessGID: 365ABB72-0886-SC8F-00000-001030500000 TargetProcessGID: 365ABB72-0886-SC8F-00000-001030500000 TargetProcessGID: 365ABB72-0886-SC8F-00000-001030506000 TargetProcessGID: 365ABB72-0886-SC8F-00000-001030506000 TargetProcessGID: 365ABB72-0885-SC8F-00000-001030506000 TargetProcessGID: 365ABB72-0886-SC8F-00000-001030506000 TargetProcessGID: 365ABB72-0886-SC8F-00000-001030506000 TargetProcessGID: 365ABB72-0886-SC8F-00000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-00000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-00000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-00000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-00000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-00000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-0000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-00000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-0000-0010305050000 TargetProcessGID: 365ABB72-0886-SC8F-0000-00103050505000 TargetProcessGID: 365ABB72-0886-SC8F-0000-0010305050000 TargetProcesSGID: 365ABB72-0886-SC8F-0000-00103050505000 TargetProcesSGID: 365ABB72-0886-SC8F-0000-00103050505000 TargetProcesSGID: 365ABB72-0886-SC8F-0000-00103050505000 TargetProcesSGID: 36</pre>	Opcode: 0
<pre>TimeCreated_attributes: SystemTem: 2019-03-1719:37:11.661930Z EventRecordID: 4807 Correlation: null Execution attributes: ProcessID: 344 ThreadD: 2032 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleKlame: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessGUT: 365ABB72-A1E3-SCBE-0000-0010CEF72200 SourceProcessGIT: 365ABB72-A1E3-SCBE-0000-0010CEF72200 SourceProcessGIT: 356ABB72-A1E3-SCBE-0000-0010CEF72200 SourceProcessGIT: 356ABB72-A1E3-SCBE-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356ABB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356AB72-0886-SCBF-0000-001030500000 TargetProcessGIT: 356AB72-0886-SCBF-0000-0010305000000 TargetProcesSIT: 356AB72-0886-SCB</pre>	Keywords: '0x8000000000000'
<pre>SystemTime: 2019-03-17T19:37:11.661930Z EventRecordID: 4809 Correlation: null Execution_attributes: ProcessID: 344 ThreadID: 2032 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security attributes: UserID: S-15-18 EventData: RuleName: '' UtcTime: 2019-08-17 19:37:11.641 SourceProcessGUID: 365ABB72-A1E3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-A1E3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-A1E3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-A1E3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-0886-SC8E-0000-0010SEF72200 SourceProcessGUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 TargetProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 TargetProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF72200 SourceProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF7200 TargetProcesSUI: 365ABB72-0886-SC8E-0000-0010SEF7EF7200 SourceProcesSUI: 365AB872-0886-SC8E-0000-0010SEF7EF7200 SourceProcesSUI: 365AB72-0886-SC8E-0000-0010SEF7EF7200 SourceProceSUI: 365AB72-0886-SC8E-0000-00100EF7200 SourcePro</pre>	TimeCreated attributes:
<pre>EventRecordID: 4807 Correlation: null Execution attributes: ProcessID: 344 ThreadID: 2032 Channel. Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessID: 365AB872-A1E3-5CBE-0000-0010CEF72200 SourceProcessID: 365AB872-A1E3-5CBE-0000-0010CEF72200 SourceProcessID: 365AB872-A1E3-5CBE-0000-0010CEF72200 SourceProcessID: 365AB872-A1E3-5CBE-0000-00100CEF7200 SourceProcessID: 365AB872-0886-5CBF-0000-001030500000 TargetProcessID: 365AB872-0886-5CBF-0000-00103050000 TargetProcessID: 365AB872-0886-5CBF-0000-0000 TargetProcessID: 365AB872-0886-5CBF-0000-0000 TargetProcessID: 365AB872-0886-5CBF-0000-0000 TargetProcessID: 365AB872-0886-5CBF-0000-0000 TargetProcessID: 365AB872-0886-5CBF-0000-0000 TargetProcessID: 365AB872-0886-5CBF-0000-0000 Targ</pre>	SystemTime: 2019-03-17T19:37:11.661930Z
Correlation: null Execution attributes: ProcessID: 344 ThreadID: 2002 ChannelMicrosoft.Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-0880-5C8P-0000-00100CEF72200 SourceProcessGUID: 365ABB72-0880-5C8P-0000-001030560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001030560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001030560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001030560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001036560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001036560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001036560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001036560000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-00103656000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-00103656000 TargetProcessGUID: 365ABB72-0880-5C8P-0000-001082-0880-5C8P-0000-001082-0880-5C8P-0000-001082-0880-5C8P-0000-001082-0880-5C8P-0000-001082-0880-5C8P-0000-001082-0880-5C8P-0000-001082-0880-5C8P-0000-001082-0880-5C8P-0000-0000-00000-000000 TargetProcesSUID: 365AB72-0880-5C8P-0000-001082-0880-5C8P-0000-00000-00000-00000-00000-0000-00	EventRecordID: 4807
Execution_attributes: ProcessID: 344 ThreadD: 2032 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtCTime: 2019-03-17 19:37:11.641 SourceProcessGID: 365AB872-A1E3-SCBE-0000-0010CEF72200 SourceProcessGID: 365AB872-A1E3-SCBE-0000-0010CEF72200 SourceProcessGID: 365AB872-0886-SCBF-0000-0010CEF72200 SourceProcessGID: 365AB872-0886-SCBF-0000-001030500000 TargetProcessGID: 365AB872-0886-SCBF-0000-00103050000 TargetProcessGID: 365AB872-0886-SCBF-0000-001000 SourceProcessGID: 365AB872-0886-SCBF-0000-0000 SourceProcessGID: 365AB872-0886-SCBF-0000-0010000 SourceProcessGID: 365AB872-0886-SCBF-0000-0000 SourceProcessGID: 365AB87-0886-SCBF-0000-0000 SourceProcesSGID: 365AB87-0886-SCBF-0000-000000 SourceProcesSGID: 365AB87	Correlation: null
ProcessID: 344 ThreadD: 2032 Channel: Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200 SourceProcessId: 3588 SourceThreadId: 2272 SourceProcessId: 3588 SourceThreadId: 2272 SourceProcessId: 356AB72-0886-5C8F-0000-0010CEF72200 SourceProcessId: 3588 SourceThreadId: 2272 SourceProcessId: 356AB72-0886-5C8F-0000-001030500000 TargetProcessId: 365AB72-0886-5C8F-0000-001030500000 TargetProcessId: 476 TargetProcessId: 476 TargetProcessId: 476 TargetProcessId: 476 CallTrac: C: \windows\System32\sas.exe GrantedAccess: '0x1010' CallTrac: C: \windows\System32\stem32\stem32\stem32 Source: C: \windows\System32\stem32 Source: C: \windows\System32\stem32 Source: C: \windows\System32\stem32 Source: C: \windows\System32 Source: C: \windows\System32 S	Execution attributes:
ThreadID: 2032 Channel: Microsoft.Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleWame: UtCTime: 2019-03-17 19:37:11.641 SourceProcessID: 365ABB72-AIE3-SCBE-0000-0010CEF72200 SourceProcessID: 365ABB72-AIE3-SCBE-0000-0010CEF72200 SourceProcessID: 365ABB72-0886-SCBF-0000-001030506000 TargetProcessID: 365AB72-0886-SCBF-0000-001030506000 TargetProcessID: 365AB72-0886-SCBF-0000-001030506000 TargetProcessID: 365AB72-0886-SCBF-0000-001030506000 TargetProcessID: 365AB72-0886-SCBF-0000-001030506000 TargetProcessID: 365AB72-0886-SCBF-0000-00100 TargetProcessID: 365AB72-0886-SCBF-0000-00103050600 TargetProcessID: 40000 SourceProcessID: 400000 SourceProcessID: 400000 Sou	ProcessID: 344
<pre>channel:-Microsoft-Windows-Sysmon/Operational Computer: PC04.example.corp Security_attributes: UserID: 5-1-5-18 EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessIG: 35888 SourceThreadId: 2272 SourceThreadId: 2372 SourceThreadId: 2372 SourceThreadId: 2372 SourceThreadId: 2372 SourceThreadId: 255AB872-0886-5C8F-0000-0010250000 TargetThrocessGUI: 355AB872-0886-5C8F-0000-00105050000 TargetThrocessGUI: 355AB872-0886-5C8F-0000-00105050000 TargetThrocessGUI: 355AB872-0886-5C8F-0000-00105050000 TargetThrocessGUI: 355AB872-0886-5C8F-0000-00105050000 TargetThrocessGUI: 355AB872-0886-5C8F-0000-00105050000 TargetThrocessGUI: 476 TargetThrocessGUI: 476 TargetThrocesSUI: 476 Target</pre>	ThreadID: 2032
Computer: PC04.example.corp security attributes UserDI: 5-1-5-18 EventData: RuleName: '' UtCrime: 2019-03-17 19:37:11.641 SourceProcessGUID: 365ABB72-AIE3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-AIE3-SC8E-0000-0010CEF72200 SourceProcessGUID: 365ABB72-0886-SC8F-00000-00103050000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-00103050000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-00103050000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-00103050000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-00103050000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-00000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-0000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-0000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcessGUID: 365ABB72-0886-SC8F-0000-0010305000 TargetProcessGUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcessGUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcessGUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcessGUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcessGUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcessGUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcesSUID: 365ABB72-0886-SC8F-0000-001030500 TargetProcesSUID: 365ABB72-0886-SC8F-0000-00103050 TargetProcesSUID: 365ABB72-0886-SC8F-0000-00103050 TargetProcesSUID: 365ABB72-0886-SC8F-0000-SV57 SourceProcesSUID: 365ABB72-0886-SC8F-0000-00103050 SourceProcesSUID: 365AB872-0886-SC8F-0000-0010050 SourceProcesSUID: 365AB872-0886-SC8F-0000-0010050 SourceProceSUID: 365AB872-0886-SC8F-0000-0010050 SourceProceSUID: 365AB872-0886-SC8F-0000-0010050 SourceProceSUID: 365AB872-0886-5C8F-0000-0010050 SourceProceSUID: 365AB872-0886-5C8F-0000-0010050 SourceProceSUID: 365AB872	_Channel: Microsoft-Windows-Sysmon/Operational
<pre>SecUnity_attributes: UserDIS_S-1-5-18 EventData: RuleName: '' RuleName: '' SourceProcessIG': 365ABB72-A1E3-5CBE-0000-0010CEF72200 SourceThreadId: 2272 SourceThreadId: 2272</pre>	Computer: PC04.example.corp
UserJD: 5-1-5-18 EventData: RLIeName: '' UtcTime: 2019-08-17 19:37:11.641 SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200 SourceInreadGi: 2271 SourceInreadGi: 2272 SourceInreadGi: 2272 SourceInreadGi: 2272 SourceInage: C:\WindowsLystem32\lsass.exe GrantedAccess: '0x1010 CallTrace: C:\WindowsLystem32\lsass.exe GrantedAccess: '0x1010 CallTrace: C:\WindowsLystem32\lsass.exe GrantedAccess: '0x1010 CallTrace: C:\WindowsLystem32\lsass.exe GrantedAccess: '0x1010 CallTrace: C:\WindowsLystem32\lsass.exe Mikatz_trunk\Win32\mimikatz.exe+5c5a9[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz.exe+5c4ff[C:\Users	Security attributes:
EventData: RuleName: '' UtcTime: 2019-03-17 19:37:11.641 SourceProcessGID: 365ABB72-A1E3-558E-0000-0010CEF72200 SourceProcessGID: 3588 SourceThreadId: 2272 SourceTmage: C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe TargetProcessGID: 365AB872-0886-558F-0000-001030560000 TargetProcessGID: 365AB872-0886-558F-0000-001030560000 TargetProcessGID: 365AB872-0886-558F-0000-001030560000 TargetTrocesSId: 476 TargetTrage: C:\Windows\system32\lsass.exe GrantedAccess: '0x1010 c:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+55a9[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+55a6C[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+55a9[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+55a6C[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\IEUser\Desktop\mimikatz_trunk\Wi	UserID: S-1-5-18
RuleName: '' Utclime: 2010-03-17 19:37:11.641 SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200 SourceInreadId: 2272 SourceInreadId: 2272 SourceInread	EventData:
<pre>Utclime: 2019-03-17 19:37:11.641 SourceProcessGUID: 365ABB72-A1E3-5CBE-0000-0010CEF72200 SourceProcessGUID: 356ABB72-A1E3-5CBE-0000-0010CEF72200 SourceThreadId: 2272 SourceThreadId: 2272 SourceThreadId: 2272 TargetProcessGUID: 365ABB72-0806-5CBF-0000-001030560000 TargetProcessGUID: 365ABB72-0806-5CBF-0000-001030560000 TargetThreadS: (:\Windows\System32\lsass.exe GrantedAccess: '0x1010 CallTrace: C:\Windows\SysTEM32\ntdll.dll+4595c]C:\Windows\system32\KERNELBASE.dll+8185 C:\Wsers\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C86c]C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C86c]C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C86c]C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f]C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimikatz_trunk\Wsin32\mimikatz.exe+5C46f[C:\Wsers\IEUser\Desktop\mimik</pre>	RuleName: ''
SourceProcessGUID: 365ABB72-AIE3-5C8E-0000-0010CEF72200 SourceInceprocessId: 3588 SourceInreadId: 2272 SourceInage: C:\USers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe TargetProcessGUID: 365AB872-0886-5C8F-0000-001030560000 TargetInage: C:\Windows\System32\lsass.exe GrantedAccess: '0x1010' CallTrac: C:\Windows\SysteM32\lsass.exe GrantedAccess: '0x1010' CallTrac: C:\Windows\SysteM32\lsass.exe Joesktop\mimikatz_trunk\Win32\mimikatz.exe+5c80C[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86C[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz_trunk\	UtcTime: 2019-03-17 19:37:11.641
SourceProcessId: 3588 SourceInreadId: 2272 SourceImage: C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe TargetProcessId: 365AB872-0886-5C8F-0000-001030500000 TargetProcessId: 476 TargetProcessId: 476 TargetProcessId: 476 CallTrace: C:\Windows\System32\lsass.exe GrantedAccess: '0x1010 CallTrace: C:\Windows\SySTEM32\ntdll.dll+4595c C:\Windows\system32\KERNELBASE.dll+8185 C:\Users\IEUser\Desktop\m mikatz_trunk\Win32\mimikatz.exe+5C80[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C86c C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5C46f[C:\Users\IEUser\Deskto	SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200
SourceThreadId: 2272 SourceThreadId: 2272 TargetProcessGUID: 365ABB72-0886-5C8F-0000-001030560000 TargetProcessId: 476 TargetProcessId: 476 CallTrace: c:\windows\System32\lsass.exe GrantedAccess: '0x1010' CallTrace: c:\windows\SYSTEM32\ntdll.dll+4595c]C:\Windows\system32\KERNELBASE.dll+8185 C:\Users\TEUser\Desktop\nmikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\Desktop\mimikatz.exe+5c8fc]C:\Users\IEUser\D	SourceProcessId: 3588
SourceImage: C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe TargetProcessGUID: 365AB872-0886-5C8F-0000-01030560000 TargetTrocessId: 476 TargetTrocessId: 476 TargetTromge: C:\Windows\System32\lsass.exe GrantedAccess: '0x1010' CallTrace: C:\Windows\SYSTEM32\ntdll.dll4595c[C:\Windows\system32\KERNELBA5E.dll+8185 C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c88c[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c88c[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c88c[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c88c[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c88c[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[C:\Users\TEUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TEUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TEUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TEUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TEUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TEUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4ff][C:\Users\TeUser\Desktop\mimikatz.exe+5c4	SourceThreadId: 2272
TargetProcessGUID: 365ABB72-0886-5C8F-0000-001030560000 TargetProcessId: 476 TargetImage: C:\Windows\system32\lsass.exe GrantedAccess: '0x1010' CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4595c C:\Windows\system32\KERNELBASE.dll+8185 C:\Users\IEUser\Desktop\m mikatz_trunk\Win32\mimikatz.exe+5c30]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c C:\Users\IEUser \Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c80[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c]C:\Users\IEUser \Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff C:\ sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+3b3d3	SourceImage: C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe
TargetProcessId: 476 TargetTmage: C:\windows\system32\lsass.exe GrantedAccess: '0x1010' CallTrace: C:\windows\SystEM32\ntdll.dll+4595c C:\Windows\system32\KERNELBASE.dll+8185 C:\Users\TEUser\Desktop\m mikatz_trunk\win32\mimikatz.exe+5c5a9 C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c8bc C:\Users\TEUser \Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff C:\Users\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff Sers\TEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5b3d3	TargetProcessGUID: 365ABB72-0886-5C8F-0000-001030560000
TargetImage: C:\Windows\System32\lsass.exe GrantedAccess: '0x1010' CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4595c C:\Windows\system32\KERNELBASE.dll+8185 C:\Users\TEUser\Desktop\m mikatz_trunk\Win32\mimikatz.exe+5c3e9 C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c C:\Users\IEUser \Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4e9 C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff C:\ sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff C:\	TargetProcessId: 476
GrantedAccess: '0x1010' CallTrace: c:\windows\SYSTEM32\ntdll.dll+4595c C:\Windows\system32\KERNELBASE.dll+8185 C:\Users\TEUser\Desktop\m mikatz_trunk\Win32\mimikatz_exe+5c3e9[c:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c[C:\Users\IEUser \Desktop\mimikatz_trunk\Win32\mimikatz.exe+5cd2]C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff C:\ sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5b3d3	TargetImage: C:\Windows\system32\lsass.exe
CallTrace: C:\Windows\SYSTEM32\htdl.dll+459sc[C:\Windows\System32\KERMELBA5E.dll+8185[C:\Users\ZTEUser\Desktop\m mikatz_trunk\Win32\mimikatz_exe+5c59 C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz_exe+5c86C[C:\Users\IEUser \Desktop\mimikatz_trunk\Win32\mimikatz_exe+5cbd2[C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz_exe+5c4f[C:\ sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz_exe+5bd3	GrantedAccess: '0x1010'
mikatz_trunk\Win32\mimikatz_exe+5c5a9[c:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz_exe+5c86c[c:\Users\IEUse \Desktop\mimikatz_trunk\Win32\mimikatz.exe+5cbd2[c:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff[c:\ sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+3b3d3	CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4595c C:\Windows\system32\KERNELBASE.dll+8185 C:\Users\IEUser\Desktop\m
\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5cbd2 C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff C:\ sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+3b3d3	mikatz_trunk\Win32\mimikatz.exe+5c5a9 C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c86c C:\Users\IEUse
sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+3b3d3	\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5cbd2 C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+5c4ff C:\
	sers\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe+3b3d3



3. Indique los dominios que se detectan en los registros analizados

C:\chainsaw>chainsaw.exe search DomainName -i "EVTX-ATTACK-SAMPLES-master\Credential Access"

DOMINIOS:

- Insecurebank:

Event_attributes:
<pre>xmlns: http://schemas.microsoft.com/win/2004/08/events/event</pre>
Event:
System:
Provider_attributes:
Name: Microsoft-Windows-Eventlog
Guid: '{fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}'
EventID: 1102
Version: 0
Level: 4
Task: 104
Opcode: 0
Keywords: '0x4020000000000000'
TimeCreated_attributes:
SystemTime: 2019-03-25T09:09:14.916619Z
EventRecordID: 198238040
Correlation: null
Execution_attributes:
ProcessID: 744
ThreadID: 2028
Channel: Security
Computer: DC1.insecurebank.local
Security: null
UserData:
LogFileCleared_attributes:
xmlns: http://manifests.microsoft.com/win/2004/08/windows/eventlog
LogFileCleared:
SubjectUserSid: S-1-5-21-738609754-2819869699-4189121830-1108
SubjectUserName: bob
SubjectDomainName: insecurebank
SubjectLogonId: '0x8d7099'

-3B - THREEBEESCO.COM:





- hqcorp:



4. Indicar si ha habido algún ataque de fuerza bruta a los servicios de bases de datos SQL:

C:\chainsaw>chainsaw.exe search SQL -i "EVTX-ATTACK-SAMPLES-master\Credential Access"

A. Indicar IP de origen que realiza el ataque.

IP: 10.0.2.17

B. Indicar hostname del equipo.

HOSTNAME: MSEDGEWIN10

A. Indicar nombre del servicio de base de datos atacado.

SERVICIO: MSSQLSERVER





5. Indicar si se ha realizado algún dump (volcado de información) a través de powershell.

:\chainsaw>chainsaw.exe hunt "EVTX-ATTACK-SAMPLES-master\Credential Access" -s sigma-master\rules\windows\powershell --mapping mappings\sigma-event-logs-all.yml --full

C:\chainsaw>chainsaw.exe search "lsass.dmp" "EVTX-ATTACK-SAMPLES-master\Credential Access"

A. Indicar Hostname del equipo donde se realizó el volcado de información.

HOSTNAME: MSEDGEWIN10

B. Indicar ruta y nombre del archivo powershell ejecutado.

RUTA: C:\Users\Public\lsass_wer_ps.ps1

C. Indicar ruta y nombre del archivo dump generado.

RUTA: C:\Users\IEUser\Desktop\lsass.dmp

+] Found 3 hits



