OPENIOC

como identificar e descrever os artefatos para distribuição entre ferramentas e times

Análise de comprometimento

Muito material sobre ferramentas e técnicas de análise.

Pouca troca automatizada de informação na fase de relatório.

Adotar estrutura comum de reporte possibilita a automação de detecção e resposta.

Passos de gerenciamento de incidente

1. Preparação
2. Identificação
3. Contenção
4. Erradicação
5. Recuperação
6. Aprendizado e prevenção << baixo índice de automação e compartilhamento

OpenIOC

Desenvolvido pela Mandiant

Framework de código aberto

Pode ser escrito à mão, mas tem o OpenIOC Editor.

Baseado em XML

Vantagem de ser lido por humanos e máquinas

Usado para reportar artefatos

Baseado em metadados

OpenIOC X STIX

A structured language for cyber threat intelligence

A transport mechanism for sharing cyber threat intelligence

- Criado e mantido pela OASIS Cyber Threat Intelligence Technical Committee
- Suporte a TLP
- Reporta a ameaça em alto nível (inclusive artefatos)
- Baseado e domínios e relacionamentos (SDO - 18 atualmente e SRO - 2 atualmente)
- JSON (a versão 1 era XML)

MISP para ambientes heterogêneos

- Opensource
- Capacidade de organizar estruturas complexas
- Exporta para todo tipo de padrão: IDS (Suricata, Snort, Bro), OpenIOC, STIX, plain text, CSV, MISP XML, JSON

misp-project.org

Coleta de atividades e metadados

REMnux - MS Sysinternals / PEiD / xPELister / **RegShot**

Áreas para coleta:

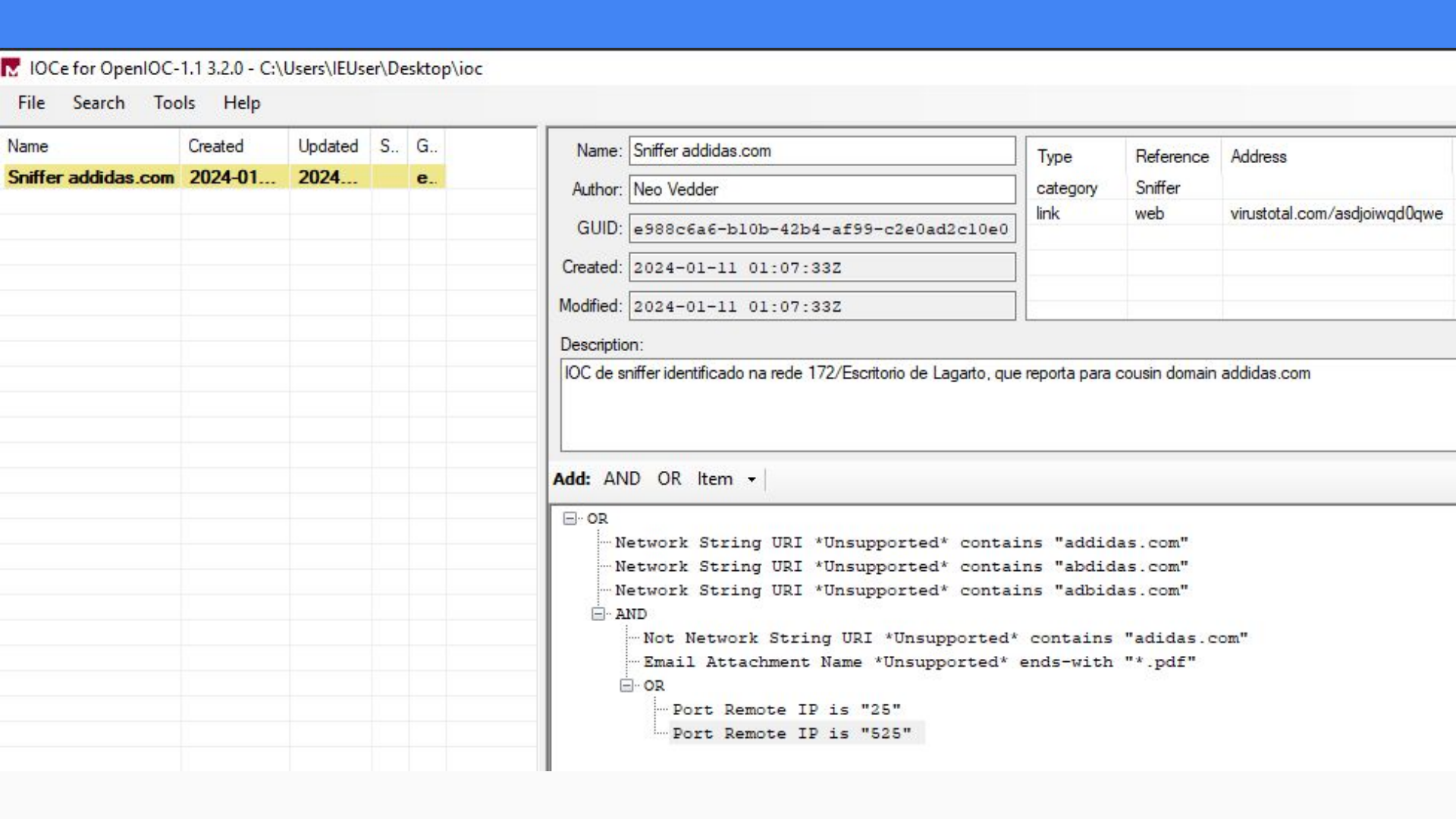
- Metadados de armazenamento
- Processos
- Registros
- Chamadas de API
- Atividade de rede (URLs e beacons são os principais)
- Rastros no FS e no sistema

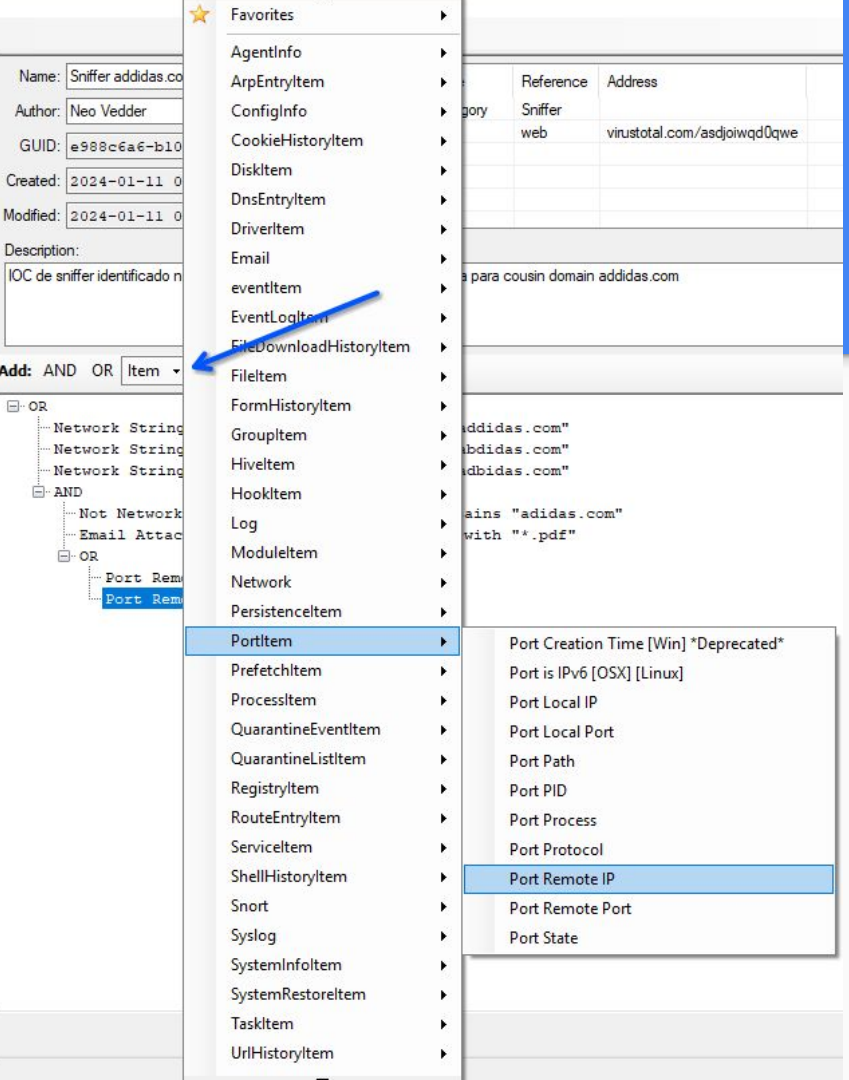
Metadados em destaque

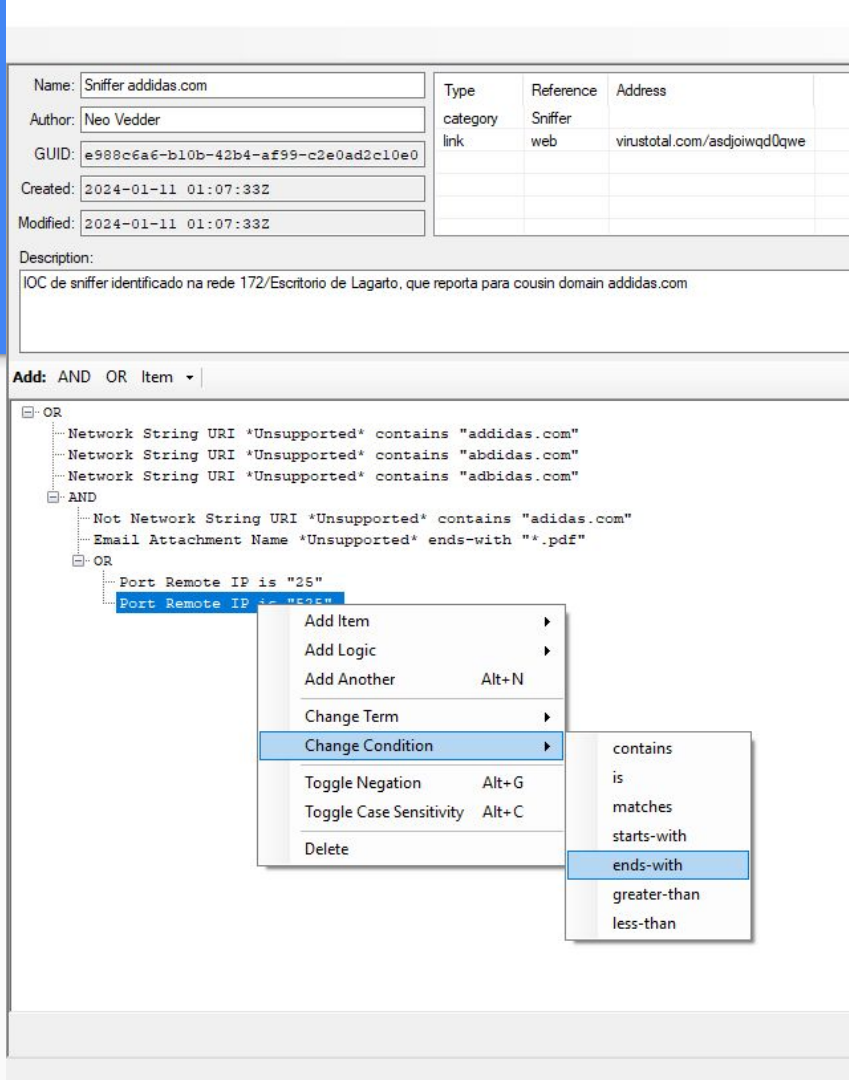
Sempre use hashes em OR por conta da mutabilidade do malware

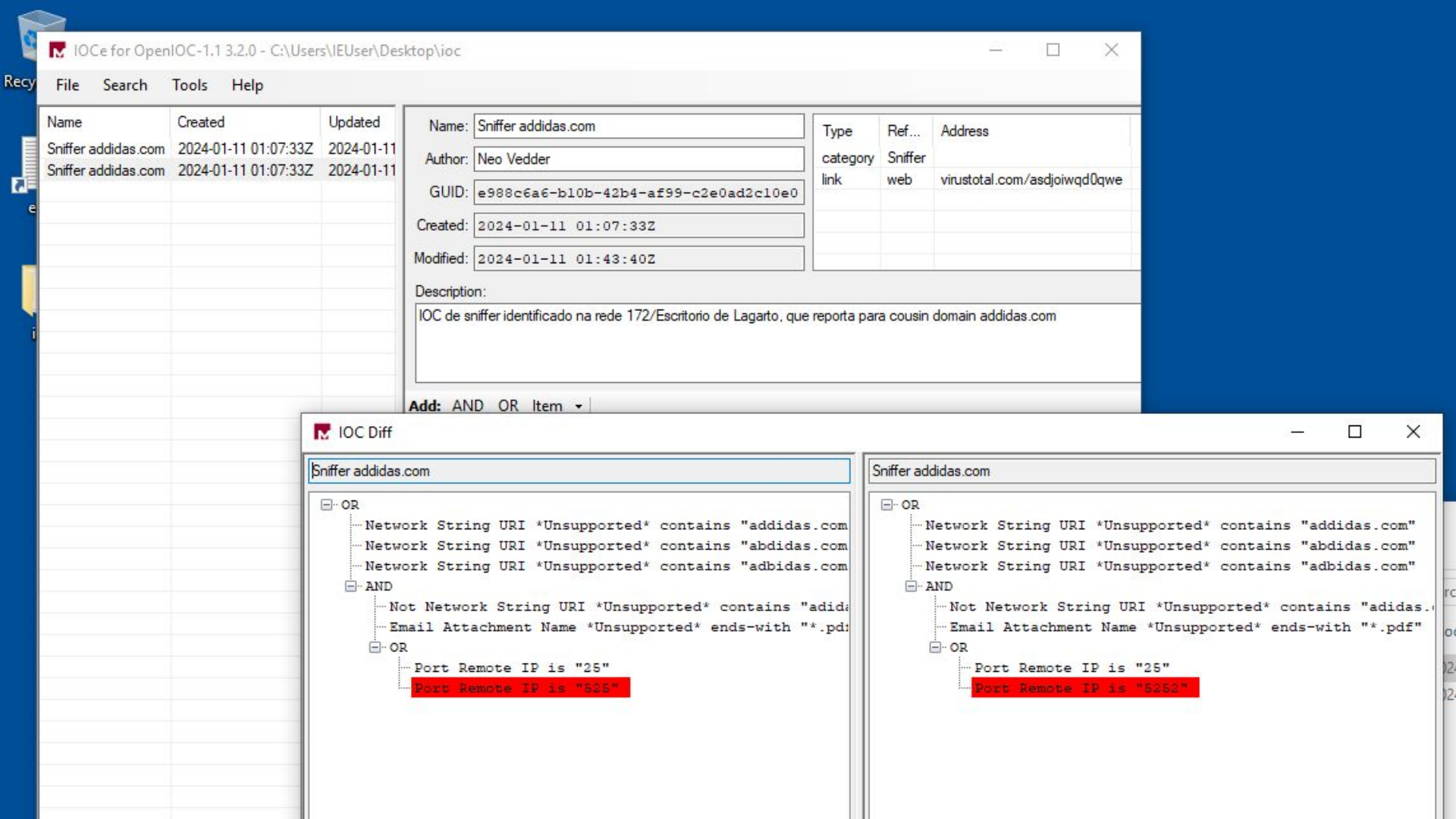
Foque mais nos rastros produzidos e nos padrões de atividades (intervalos de tempo, arquivos manipulados, APIs invocadas, padrões de URLs). Ou seja, veja mais os efeitos do que o artefato em si!

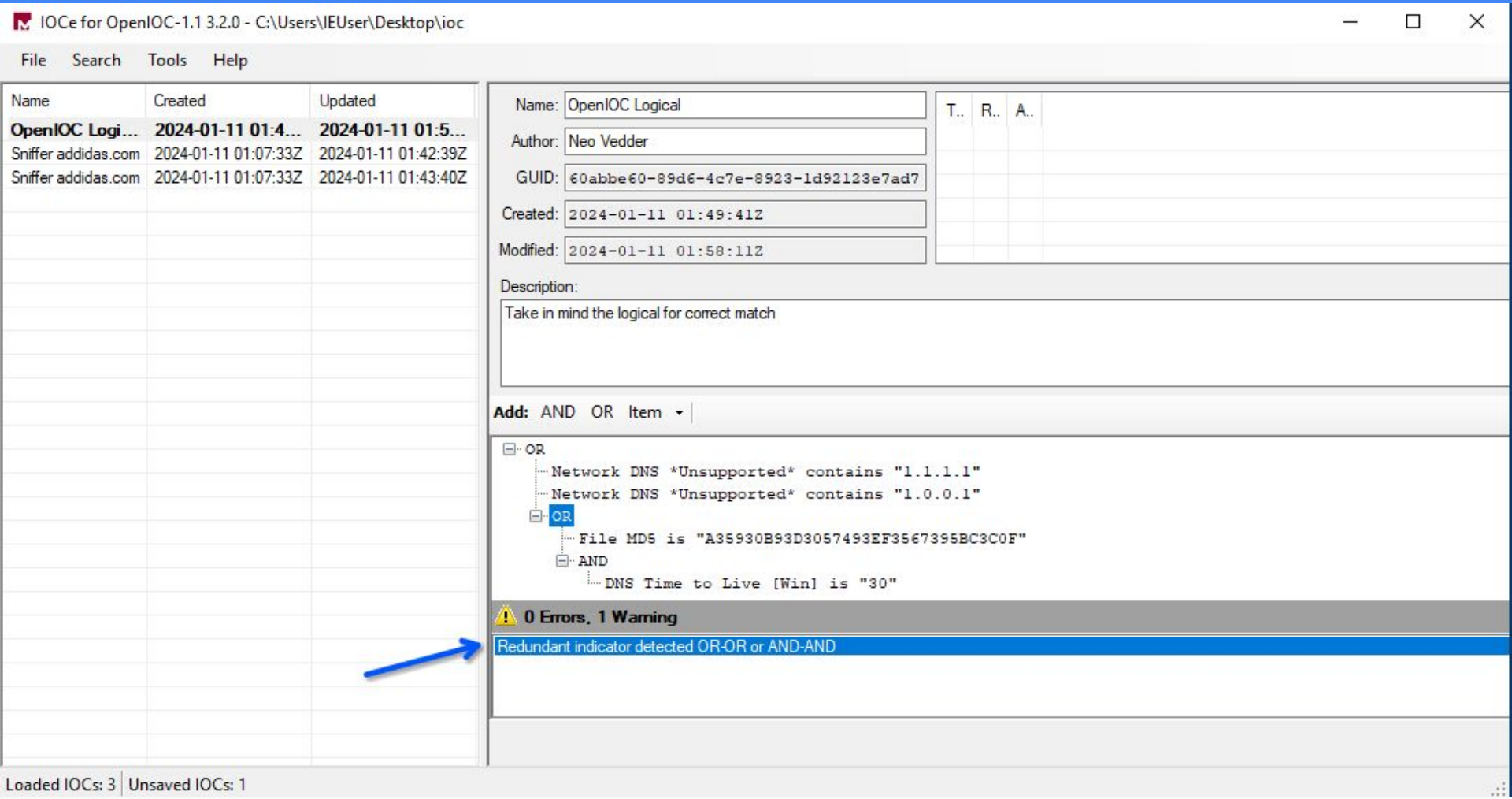
OpenIOC consegue dar um bom suporte na descrição de efeitos.

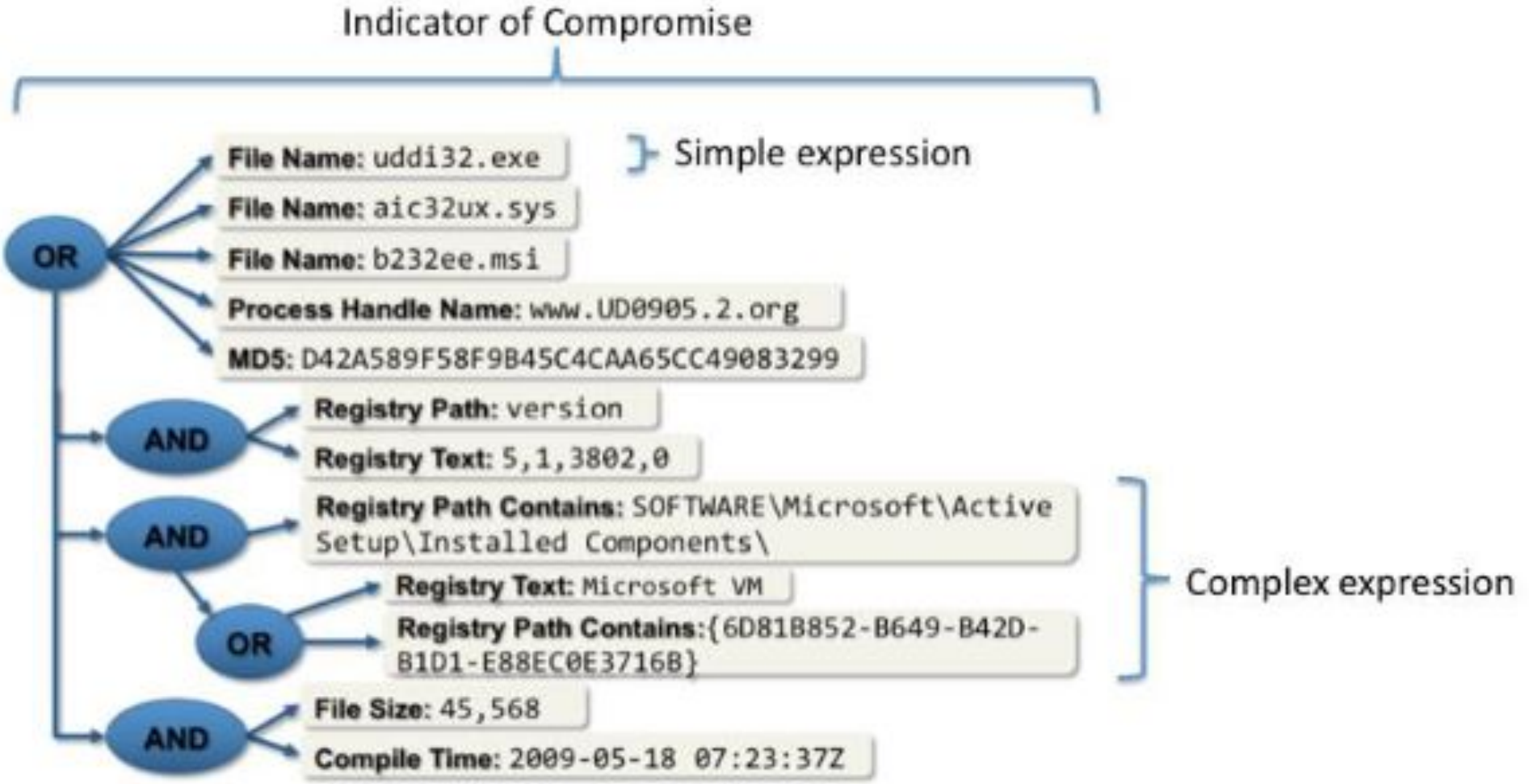

IOCe for OpenIOC-1.1 3.2.0 - C:\Users\IEUser\Desktop\ioc
File
Search
Tools
Help
Name
Created
Updated
S..
G..
Sniffer addidas.com
2024-01...
2024...
e..
Name: Sniffer addidas.com
Author: Neo Vedder
GUID: e988c6a6-b10b-42b4-af99-c2e0ad2c10e0
Created: 2024-01-11 01:07:33Z
Modified: 2024-01-11 01:07:33Z
Type
Reference
Address
category
Sniffer
link
web
virustotal.com/asdjoiwqd0qwe
Description:
IOC de sniffer identificado na rede 172/Escritorio de Lagarto, que reporta para cousin domain addidas.com
Add: AND OR Item
OR
Network String URI *Unsupported* contains "addidas.com"
Network String URI *Unsupported* contains "abdidas.com"
Network String URI *Unsupported* contains "adbidas.com"
AND
Not Network String URI *Unsupported* contains "adidas.com"
Email Attachment Name *Unsupported* ends-with "*.pdf"
OR
Port Remote IP is "25"
Port Remote IP is "525"


Favorites
AgentInfo
ArpEntryItem
ConfigInfo
CookieHistoryItem
DiskItem
DnsEntryItem
DriverItem
Email
eventItem
EventLogItem
FileDownloadHistoryItem
FileItem
FormHistoryItem
GroupItem
HiveItem
HookItem
Log
ModuleItem
Network
PersistenceItem
PortItem
PrefetchItem
ProcessItem
QuarantineEventItem
QuarantineListItem
RegistryItem
RouteEntryItem
ServiceItem
ShellHistoryItem
Snort
Syslog
SystemInfoItem
SystemRestoreItem
TaskItem
UrlHistoryItem
Port Creation Time [Win] *Deprecated*
Port is IPv6 [OSX] [Linux]
Port Local IP
Port Local Port
Port Path
Port PID
Port Process
Port Protocol
Port Remote IP
Port Remote Port
Port State
Name: Sniffer addidas.co
Author: Neo Vedder
GUID: e988c6a6-b10
Created: 2024-01-11 0
Modified: 2024-01-11 0
Description:
IOC de sniffer identificado n
Add: AND OR Item
OR
Network String
Network String
Network String
AND
Not Network
Email Attac
OR
Port Rem
Port Rem
Reference
Address
Sniffer
web
virustotal.com/asdjoiwqd0qwe
a para cousin domain addidas.com
addidas.com"
abdidas.com"
adbidas.com"
ains "adidas.com"
with "*.pdf"


Name: Sniffer addidas.com
Author: Neo Vedder
GUID: e988c6a6-b10b-42b4-af99-c2e0ad2c10e0
Created: 2024-01-11 01:07:33Z
Modified: 2024-01-11 01:07:33Z
Type
Reference
Address
category
Sniffer
link
web
virustotal.com/asdjoiwqd0qwe
Description:
IOC de sniffer identificado na rede 172/Escritorio de Lagarto, que reporta para cousin domain addidas.com
Add: AND OR Item
OR
Network String URI *Unsupported* contains "addidas.com"
Network String URI *Unsupported* contains "abdidas.com"
Network String URI *Unsupported* contains "adbidas.com"
AND
Not Network String URI *Unsupported* contains "adidas.com"
Email Attachment Name *Unsupported* ends-with "*.pdf"
OR
Port Remote IP is "25"
Add Item
Add Logic
Add Another Alt+N
Change Term
Change Condition
Toggle Negation Alt+G
Toggle Case Sensitivity Alt+C
Delete
contains
is
matches
starts-with
ends-with
greater-than
less-than


IOCe for OpenIOC-1.1 3.2.0 - C:\Users\IEUser\Desktop\ioc
File
Search
Tools
Help
Name
Created
Updated
Sniffer addidas.com
2024-01-11 01:07:33Z
2024-01-11
Sniffer addidas.com
2024-01-11 01:07:33Z
2024-01-11
Name: Sniffer addidas.com
Author: Neo Vedder
GUID: e988c6a6-bl0b-42b4-af99-c2e0ad2cl0e0
Created: 2024-01-11 01:07:33Z
Modified: 2024-01-11 01:43:40Z
Type
Ref...
Address
category
Sniffer
link
web
virustotal.com/asdjoiwqd0qwe
Description:
IOC de sniffer identificado na rede 172/Escritorio de Lagarto, que reporta para cousin domain addidas.com
Add: AND OR Item
IOC Diff
Sniffer addidas.com
OR
Network String URI *Unsupported* contains "addidas.com
Network String URI *Unsupported* contains "abdidas.com
Network String URI *Unsupported* contains "adbidas.com
AND
Not Network String URI *Unsupported* contains "adida
Email Attachment Name *Unsupported* ends-with "*.pd
OR
Port Remote IP is "25"
Port Remote IP is "525"
Sniffer addidas.com
OR
Network String URI *Unsupported* contains "addidas.com"
Network String URI *Unsupported* contains "abdidas.com"
Network String URI *Unsupported* contains "adbidas.com"
AND
Not Network String URI *Unsupported* contains "adidas.
Email Attachment Name *Unsupported* ends-with "*.pdf"
OR
Port Remote IP is "25"
Port Remote IP is "5252"


IOCe for OpenIOC-1.1 3.2.0 - C:\Users\IEUser\Desktop\ioc
File
Search
Tools
Help
Name
Created
Updated
OpenIOC Logi...
2024-01-11 01:4...
2024-01-11 01:5...
Sniffer addidas.com
2024-01-11 01:07:33Z
2024-01-11 01:42:39Z
Sniffer addidas.com
2024-01-11 01:07:33Z
2024-01-11 01:43:40Z
Name: OpenIOC Logical
Author: Neo Vedder
GUID: 60abbe60-89d6-4c7e-8923-1d92123e7ad7
Created: 2024-01-11 01:49:41Z
Modified: 2024-01-11 01:58:11Z
T..
R..
A..
Description:
Take in mind the logical for correct match
Add: AND OR Item
OR
Network DNS *Unsupported* contains "1.1.1.1"
Network DNS *Unsupported* contains "1.0.0.1"
OR
File MD5 is "A35930B93D3057493EF3567395BC3C0F"
AND
DNS Time to Live [Win] is "30"
0 Errors, 1 Warning
Redundant indicator detected OR-OR or AND-AND
Loaded IOCs: 3
Unsaved IOCs: 1


Indicator of Compromise
File Name: uddi32.exe
File Name: aic32ux.sys
File Name: b232ee.msi
Process Handle Name: www.UD0905.2.org
MD5: D42A589F58F9B45C4CAA65CC49083299
Simple expression
OR
AND
Registry Path: version
Registry Text: 5,1,3802,0
AND
Registry Path Contains: SOFTWARE\Microsoft\Active Setup\Installed Components\
Registry Text: Microsoft VM
OR
Registry Path Contains:{6D81B852-B649-B42D-81D1-E88EC0E3716B}
Complex expression
AND
File Size: 45,568
Compile Time: 2009-05-18 07:23:37Z