

REPORTE DE SEGURIDAD

Generado el: 2026-02-15 12:15:28

1. Análisis de Puertos Locales

Puerto	Proceso	PID	Servicio	Estado	Recomendación
135	svchost.exe	1476	RPC	ALERTA	Restringir Firewall
135	svchost.exe	1476	RPC	ALERTA	Restringir Firewall
139	System	4	NetBIOS	ALERTA	Restringir Firewall
139	System	4	NetBIOS	ALERTA	Restringir Firewall
139	System	4	NetBIOS	ALERTA	Restringir Firewall
445	System	4	SMB	ALERTA	Restringir Firewall
445	System	4	SMB	ALERTA	Restringir Firewall
1337	RzSDKServer.exe	5212	Desconocido	OK	OK
2179	vmmms.exe	2856	Desconocido	OK	OK
2179	vmmms.exe	2856	Desconocido	OK	OK
5040	svchost.exe	10952	Desconocido	OK	OK
5357	System	4	Desconocido	OK	OK
5357	System	4	Desconocido	OK	OK
5426	System	4	Desconocido	OK	OK
5426	System	4	Desconocido	OK	OK
5829	Code.exe	5672	Desconocido	OK	OK
6463	Discord.exe	18100	Desconocido	OK	OK
7680	svchost.exe	18604	Desconocido	OK	OK
7680	svchost.exe	18604	Desconocido	OK	OK
8733	System	4	Desconocido	OK	OK
8733	System	4	Desconocido	OK	OK
9100	lghub_updater.exe	5108	Desconocido	OK	OK
9180	lghub_updater.exe	5108	Desconocido	OK	OK
13331	RzChromaConnectServer	7668	Desconocido	OK	OK
13337	RzSDKServer.exe	5212	Desconocido	OK	OK
13344	RzChromaStreamServer.exe	18812	Desconocido	OK	OK
27036	steam.exe	13968	Desconocido	OK	OK
27060	steam.exe	13968	Desconocido	OK	OK
49664	lsass.exe	1164	Desconocido	OK	OK
49664	lsass.exe	1164	Desconocido	OK	OK
49665	wininit.exe	624	Desconocido	OK	OK
49665	wininit.exe	624	Desconocido	OK	OK

Puerto	Proceso	PID	Servicio	Estado	Recomendacion
49666	svchost.exe	808	Desconocido	OK	OK
49666	svchost.exe	808	Desconocido	OK	OK
49667	svchost.exe	3012	Desconocido	OK	OK
49667	svchost.exe	3012	Desconocido	OK	OK
49668	svchost.exe	4200	Desconocido	OK	OK
49668	svchost.exe	4200	Desconocido	OK	OK
49669	spoolsv.exe	4752	Desconocido	OK	OK
49669	spoolsv.exe	4752	Desconocido	OK	OK
49670	jhi_service.exe	5036	Desconocido	OK	OK
49671	GameManagerService3.exe	4416	Desconocido	OK	OK
49671	GameManagerService3.exe	4416	Desconocido	OK	OK
49677	services.exe	1116	Desconocido	OK	OK
49677	services.exe	1116	Desconocido	OK	OK
53381	Code.exe	19008	Desconocido	OK	OK
54235	System	4	Desconocido	OK	OK
54235	System	4	Desconocido	OK	OK
55870	GitHubDesktop.exe	2512	Desconocido	OK	OK
63552	steam.exe	13968	Desconocido	OK	OK
63553	steam.exe	13968	Desconocido	OK	OK
65444	RzDiagnostic	8256	Desconocido	OK	OK

2. Análisis de Red Local

Host: 172.20.144.1

Puerto	Servicio	Descripcion
445	SMB	Servicio SMB detectado como vulnerable.

3. Análisis de Archivos Sospechosos

Archivo	Razon	Confianza	Accion
DIAGNOSTICO_AGENTE.pdf	Patrones genéricos	Bajo	Investigar
DIAGNOSTICO_COMPLETO.pdf	Patrones genéricos	Bajo	Investigar
scanner.py	Patrones genéricos	Bajo	Investigar
test_scanner.py	Keyword detectada: e	Bajo	Investigar
yara.cp311-win_amd64.pyd	Patrones genéricos	Seguro (Dev)	Investigar

Archivo	Razon	Confianza	Accion
cu2qu.cp311-win_amd64.pyd	Patrones genéricos	Seguro (Dev)	Investigar
lexer.cp311-win_amd64.pyd	Patrones genéricos	Seguro (Dev)	Investigar
bezierTools.cp311-win_amd	Patrones genéricos	Seguro (Dev)	Investigar
psLib.py	Keyword detectada: e	Seguro (Dev)	Investigar
psOperators.py	Patrones genéricos	Seguro (Dev)	Investigar
symfont.py	Patrones genéricos	Seguro (Dev)	Investigar
xmlReader.py	Keyword detectada: e	Seguro (Dev)	Investigar
momentsPen.cp311-win_amd6	Patrones genéricos	Seguro (Dev)	Investigar
qu2cu.cp311-win_amd64.pyd	Patrones genéricos	Seguro (Dev)	Investigar
__init__.py	Patrones genéricos	Seguro (Dev)	Investigar
BitmapGlyphMetrics.py	Keyword detectada: e	Seguro (Dev)	Investigar
C_O_L_R_.py	Keyword detectada: e	Seguro (Dev)	Investigar
D_S_I_G_.py	Keyword detectada: e	Seguro (Dev)	Investigar
E_B_D_T_.py	Patrones genéricos	Seguro (Dev)	Investigar
F_F_T_M_.py	Keyword detectada: e	Seguro (Dev)	Investigar
F_e_a_t.py	Keyword detectada: e	Seguro (Dev)	Investigar
G_M_A_P_.py	Keyword detectada: e	Seguro (Dev)	Investigar
G_P_K_G_.py	Keyword detectada: e	Seguro (Dev)	Investigar
G_l_a_t.py	Patrones genéricos	Seguro (Dev)	Investigar
G_l_o_c.py	Keyword detectada: e	Seguro (Dev)	Investigar
L_T_S_H_.py	Keyword detectada: e	Seguro (Dev)	Investigar
M_E_T_A_.py	Patrones genéricos	Seguro (Dev)	Investigar
otConverters.py	Keyword detectada: e	Seguro (Dev)	Investigar
O_S_2f_2.py	Keyword detectada: e	Seguro (Dev)	Investigar
sbixGlyph.py	Patrones genéricos	Seguro (Dev)	Investigar
sbixStrike.py	Patrones genéricos	Seguro (Dev)	Investigar

Archivo	Razon	Confianza	Accion
S_I_N_G_.py	Keyword detectada: e	Seguro (Dev)	Investigar
S_V_G_.py	Patrones genéricos	Seguro (Dev)	Investigar
S_i_L_f.py	Patrones genéricos	Seguro (Dev)	Investigar
S_i_L_l.py	Keyword detectada: e	Seguro (Dev)	Investigar
TupleVariation.py	Keyword detectada: e	Seguro (Dev)	Investigar
T_S_I__5.py	Keyword detectada: e	Seguro (Dev)	Investigar
V_D_M_X_.py	Patrones genéricos	Seguro (Dev)	Investigar
V_O_R_G_.py	Keyword detectada: e	Seguro (Dev)	Investigar
_a_v_a_r.py	Keyword detectada: e	Seguro (Dev)	Investigar
_c_m_a_p.py	Patrones genéricos	Seguro (Dev)	Investigar
_c_v_t.py	Keyword detectada: e	Seguro (Dev)	Investigar
_f_v_a_r.py	Patrones genéricos	Seguro (Dev)	Investigar
_g_a_s_p.py	Keyword detectada: e	Seguro (Dev)	Investigar
_g_v_a_r.py	Patrones genéricos	Seguro (Dev)	Investigar
_h_d_m_x.py	Keyword detectada: e	Seguro (Dev)	Investigar
_h_e_a_d.py	Keyword detectada: e	Seguro (Dev)	Investigar
_h_h_e_a.py	Keyword detectada: e	Seguro (Dev)	Investigar
_h_m_t_x.py	Patrones genéricos	Seguro (Dev)	Investigar
_k_e_r_n.py	Keyword detectada: e	Seguro (Dev)	Investigar
_l_t_a_g.py	Keyword detectada: e	Seguro (Dev)	Investigar
_m_a_x_p.py	Patrones genéricos	Seguro (Dev)	Investigar
_s_b_i_x.py	Keyword detectada: e	Seguro (Dev)	Investigar
_t_r_a_k.py	Keyword detectada: e	Seguro (Dev)	Investigar
_v_h_e_a.py	Keyword detectada: e	Seguro (Dev)	Investigar
iup.cp311-win_amd64.pyd	Patrones genéricos	Seguro (Dev)	Investigar

Archivo	Razon	Confianza	Accion
ast.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
encryption.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
fpdf.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
ImageMath.py	Patrones genéricos	Seguro (Dev)	Investigar
ImageShow.py	Keyword detectada: o	Seguro (Dev)	Investigar
_avif.cp311-win_amd64.pyd	Patrones genéricos	Seguro (Dev)	Investigar
_imaging.cp311-win_amd64.	Patrones genéricos	Seguro (Dev)	Investigar
_imagingcms.cp311-win_amd	Patrones genéricos	Seguro (Dev)	Investigar
_imagingft.cp311-win_amd6	Patrones genéricos	Seguro (Dev)	Investigar
_imagingmath.cp311-win_am	Patrones genéricos	Seguro (Dev)	Investigar
_imagingmorph.cp311-win_a	Patrones genéricos	Seguro (Dev)	Investigar
_imagingtk.cp311-win_amd6	Patrones genéricos	Seguro (Dev)	Investigar
_webp.cp311-win_amd64.pyd	Patrones genéricos	Seguro (Dev)	Investigar
subprocess.py	Keyword detectada: s	Seguro (Dev)	Investigar
scripts.py	Patrones genéricos	Seguro (Dev)	Investigar
t32.exe	Extensión sospechosa	Seguro (Dev)	Investigar
t64-arm.exe	Extensión sospechosa	Seguro (Dev)	Investigar
t64.exe	Extensión sospechosa	Seguro (Dev)	Investigar
w32.exe	Extensión sospechosa	Seguro (Dev)	Investigar
w64-arm.exe	Extensión sospechosa	Seguro (Dev)	Investigar
w64.exe	Extensión sospechosa	Seguro (Dev)	Investigar
_parser.py	Patrones genéricos	Seguro (Dev)	Investigar
__init__.py	Keyword detectada: e	Seguro (Dev)	Investigar

Archivo	Razon	Confianza	Accion
__init__.py	Keyword detectada: e	Seguro (Dev)	Investigar
markup.py	Patrones genéricos	Seguro (Dev)	Investigar
pyopenssl.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
pyopenssl.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
results.py	Keyword detectada: e	Seguro (Dev)	Investigar
_psaix.py	Keyword detectada: s	Seguro (Dev)	Investigar
_pssunos.py	Keyword detectada: s	Seguro (Dev)	Investigar
_psutil_windows.pyd	Patrones genéricos	Seguro (Dev)	Investigar
automaton.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
config.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
main.py	Patrones genéricos	Seguro (Dev)	Investigar
scapypipes.py	YARA: Suspicious_Net	Sospechoso (Entorno Dev)	Investigar
utils.py	YARA: Suspicious_Net	Sospechoso (Entorno Dev)	Investigar
__init__.py	Keyword detectada: s	Seguro (Dev)	Investigar
supersocket.py	Keyword detectada: e	Seguro (Dev)	Investigar
macsec.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
psp.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar

Archivo	Razon	Confianza	Accion
secoc.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
dot11.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
gssapi.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
ipsec.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
kerberos.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
ntlm.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
radius.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
smb2.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
tuntap.py	Patrones genéricos	Seguro (Dev)	Investigar
msnrpc.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
all.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
automaton_cli.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
automaton_srv.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar

Archivo	Razon	Confianza	Accion
cert.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
extensions.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
handshake.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
handshake_sslv2.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
keyexchange.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
keyexchange_tls13.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
record.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
record_tls13.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
session.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
__init__.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
all.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
ciphers.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
cipher_aead.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar

Archivo	Razon	Confianza	Accion
cipher_block.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
cipher_stream.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
groups.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
hash.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
hkdf.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
h_mac.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
pkcs1.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
prf.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
suites.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
all.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
ciphers.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
cipher_aead.cpython-311.p	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
cipher_block.cpython-311.	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar

Archivo	Razon	Confianza	Accion
cipher_stream.cpython-311	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
hash.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
hkdf.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
h_mac.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
prf.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
suites.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
all.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
automaton_cli.cpython-311	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
automaton_srv.cpython-311	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
cert.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
extensions.cpython-311.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
handshake.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
handshake_sslv2.cpython-3	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar

Archivo	Razon	Confianza	Accion
keyexchange.cpython-311.p	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
keyexchange_tls13.cpython	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
record.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
record_tls13.cpython-311.	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
session.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
gssapi.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
kerberos.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
ntlm.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
radius.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
smb2.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
extcap.py	Keyword detectada: s	Seguro (Dev)	Investigar
rfc3961.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
winpcapy.py	Keyword detectada: e	Seguro (Dev)	Investigar
rfc3961.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar

Archivo	Razon	Confianza	Accion
voip.py	Keyword detectada: s	Seguro (Dev)	Investigar
automaton.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
__init__.py	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
automaton.cpython-311.pyc	YARA: Ransomware_Ind	Sospechoso (Entorno Dev)	Investigar
isotpscanner.py	Keyword detectada: e	Seguro (Dev)	Investigar
obdscanner.py	Keyword detectada: e	Seguro (Dev)	Investigar
cli-32.exe	Extensión sospechosa	Seguro (Dev)	Investigar
cli-64.exe	Extensión sospechosa	Seguro (Dev)	Investigar
cli-arm64.exe	Extensión sospechosa	Seguro (Dev)	Investigar
cli.exe	Extensión sospechosa	Seguro (Dev)	Investigar
gui-32.exe	Extensión sospechosa	Seguro (Dev)	Investigar
gui-64.exe	Extensión sospechosa	Seguro (Dev)	Investigar
gui-arm64.exe	Extensión sospechosa	Seguro (Dev)	Investigar
gui.exe	Extensión sospechosa	Seguro (Dev)	Investigar
launch.py	Keyword detectada: e	Seguro (Dev)	Investigar
sandbox.py	Keyword detectada: e	Seguro (Dev)	Investigar
expand.py	Keyword detectada: e	Seguro (Dev)	Investigar
core.py	Patrones genéricos	Seguro (Dev)	Investigar
msvc9compiler.py	Patrones genéricos	Seguro (Dev)	Investigar
spawn.py	Keyword detectada: s	Seguro (Dev)	Investigar
results.py	Keyword detectada: e	Seguro (Dev)	Investigar
activate.bat	Extensión sospechosa	Seguro (Dev)	Investigar
Activate.ps1	Extensión sospechosa	Seguro (Dev)	Investigar

Archivo	Razon	Confianza	Accion
deactivate.bat	Extensión sospechosa	Seguro (Dev)	Investigar
fonttools.exe	Extensión sospechosa	Seguro (Dev)	Investigar
pip.exe	Extensión sospechosa	Seguro (Dev)	Investigar
pip3.11.exe	Extensión sospechosa	Seguro (Dev)	Investigar
pip3.exe	Extensión sospechosa	Seguro (Dev)	Investigar
pyftmerge.exe	Extensión sospechosa	Seguro (Dev)	Investigar
pyftsubset.exe	Extensión sospechosa	Seguro (Dev)	Investigar
python.exe	Extensión sospechosa	Seguro (Dev)	Investigar
pythonw.exe	Extensión sospechosa	Seguro (Dev)	Investigar
scapy.exe	Extensión sospechosa	Seguro (Dev)	Investigar
txt.exe	Extensión sospechosa	Seguro (Dev)	Investigar
advanced_detection.yar	YARA: Ransomware_Ind	CRITICO	ELIMINAR