Rule Name	Average number of AV engines that flagged the matched samples	Number of Matches (last 21 days)	Category
SUSP_HKTL_FRP_Config_Nov21_1	0,00	13	Dual Use Tool
HKTL_DNSCrypt_Proxy_ServiceInstall	0,00	18	Hacktool
SUSP_PUA_RustDesk_Apr23_1	0,00	18	Dual Use Tool
APT_MAL_ME_Loader_May20_2	0,00	12	Malware
Casing_Anomaly_Schtasks	0,00	41	Obfuscation
SUSP_Scheduled_Task_Suspicious_Folder_Nov	0,00	248	Anomaly
HKTL_PUA_WinTun_Jan22	0,00	14	Dual Use Tool
Shellcode_ClearText	0,00	42	Malicious Script
SUSP_OBFUSC_Casing_Anomaly_Schtasks_Exe	0,00	42	Obfuscation
MAL_CN_Campaign_Dropped_Dir_Listing_Aug1	0,00	81	Forensic Artefact
APT_MalDoc_RU_Gamaredon_Mar22_1	0,00	17	Malicious Document
OWASP_ZSC_JS_Code	0,00	12	Malicious Script
SUSP_PUA_LNX_macOS_AnyDesk_Feb22_1	0,00	58	Dual Use Tool
SUSP_BAT_Aux_Jan20_1	0,00	1065	Malicious Script
URL_File_Local_EXE	0,06	18	Anomaly
SUSP_Webshell_PHPUnderscoreObfuscation_A	0,08	64	Webshell
PUA_Shadowsocks_Oct24	0,08	155	Dual Use Tool
SUSP_ISO_In_ZIP_Small_May22_1	0,10	62	Phishing Attachment
SUSP_Dropper_Characteristics_May24_1	0,13	48	Obfuscation
SUSP_URL_SHORTCUT_Mar25	0,16	32	Anomaly
SUSP_PE_OK_RU_URL_Jun23	0,17	35	Anomaly
SUSP_CreateMutex_Script_Apr20	0,21	14	Anomaly
SUSP_NET_MSIL_OBFUSC_VirtualGuard	0,32	19	Anomaly
HKTL_GetGPP_Password	0,33	15	Hacktool
SUSP_Odd_SC_Stop_Aug24	0,38	21	Anomaly
SUSP_VBA_User32_Import_Indicators_Oct20_1	0,38	122	Malicious Script
SUSP_LNX_Crontab_Wget_Oct21_1	0,43	14	Config Backdoor
SUSP_EXPL_POC_PY_Indicators_Oct23	0,46	13	Hacktool
SUSP_POC_Indicator_AndyNguyen_Mar22	0,46	37	Hacktool
SUSP_PS1_Indicators_Loader_Gen_Dec21_2	0,47	78	Malicious Script
SUSP_Wget_IPLogger_Reference_Oct21_1	0,47	45	Malicious Script
WEBSHELL_PHP_BeginsWith_eval_Sep21	0,48	164	Webshell
SUSP_LNX_Crontab_Curl_Oct21_1	0,50	12	Config Backdoor
SUSP_OBFUSC_PY_Loader_Jun23_1	0,58	125	Obfuscation
SUSP_PS1_Invoke_Expression_May22_1	0,63	65	Malicious Script
SUSP_PY_Payload_May24_1	0,64	39	Malicious Script
SUSP_LNK_NO_META	0,64	25	Anomaly
SUSP_JS_OBFUSC_Feb23_2	0,72	653	Obfuscation
SUSP_Python_Base64_Encoded_Sep21	0,86	29	Obfuscation
SUSP_CreateObject_RegWrite_Combo	0,92	24	Anomaly
HKTL_Gen_Pattern_Rust_Feb25	0,95	42	Hacktool
SUSP_OBFUSC_Python_Zlib_Base64_Apr25	0,97	31	Obfuscation
WiltedTulip_Tools_clrlg	1,00	12	Malicious Script
EXPL_SUSP_MalDoc_TemplateInjection_Dec21	1,00	78	Malicious Document
SUSP_VBA_Macro_AccessVBOM_Oct22	1,00	16	Malicious Script

SUSP_VBA_Kernel32_Imports_Jun22_1	1,01	1012	Malicious Script
SUSP_Encoded_ScriptHeader_Feb19	1,04	80	Obfuscation
SUSP_VBA_Macro_WScript_KernelDLL_May19_1	1,04	27	Malicious Script
HKTL_Evil_Winrm_Jul19	1,09	11	Hacktool
SUSP_ELF_Loader_Indicators_Jul24	1,13	16	Malware
SUSP_Hex_Encoded_WScript_Shell	1,18	93	Obfuscation
SUSP_PS1_OBFUSC_Nov23_6	1,19	32	Obfuscation
SUSP_Obfuscation_ChrW_Feb19_1	1,21	282	Obfuscation
Disclosed_0day_POCs_payload_MSI	1,24	38	Malicious Script
PHP_Webshell_1_Feb17	1,28	18	Webshell
WScriptShell_Case_Anomaly	1,29	232	Obfuscation
SUSP_PY_OBFUSC_Berserker_Indicators_Dec22	1,33	18	Obfuscation
SUSP_PS1_Encoded_Downloader_Pattern_Mar2	1,41	27	Malicious Script
SUSP_Tiny_PowerShell_Execution_File	1,44	55	Malicious Script
SUSP_BAT_PS1_Combo_Jan23_2	1,45	91	Malicious Script
SUSP_Tiny_WScriptShell_Invoke	1,52	58	Malicious Script
Rundll32_Susp_Invocation	1,54	24	Anomaly
PUA_NetSupport_Apr22	1,59	625	Dual Use Tool
SUSP_OBFUSC_PS1_Gen_Apr23_1	1,63	16	Obfuscation
SUSP_Base64_Encoded_ELF_Binary_Feb19	1,65	269	Obfuscation
SUSP_DOC_Base64_Properties_Feb20	1,66	134	Obfuscation
SUSP_RAR_With_File_MacroEnabled_MsOffice_(	1,72	18	Anomaly
SUSP_PS1_InvokeExpression_Casing_Anomaly	1,78	117	Obfuscation
SUSP_Driver_Characteristics_Jun21_1	1,81	16	Anomaly
SUSP_Base64_Encoded_GithubUserContent_U	1,88	33	Obfuscation
SUSP_RANSOM_Note_Aug22	1,95	314	Malware
SUSP_Tiny_RAR_Suspicious_Extensions_Mar21	1,97	67	Anomaly
SUSP_Javascript_Obfuscation_NonAscii_Apr25	1,97	6089	Obfuscation
SUSP_LSA_Registry_Script_Indicators_Jan24_1	2,00	20	Malicious Script
MAL_ELF_Systembc_Jan25	2,03	65	Malware
SUSP_LNX_NetCat_Flags_Feb22_1	2,08	12	Hacktool
MAL_VBS_Executing_BAT_Nov23	2,09	43	Malicious Script
SUSP_RMM_NAble_Monitoring_Agent	2,12	41	Dual Use Tool
HKTL_PY_Bypass_Tool_Aug21_2	2,13	140	Hacktool
SUSP_CobaltStrike_Keywords_JAR_Classes_May	2,16	37	Hacktool
SUSP_Obfuscator_Generated_Content_May25	2,17	18	Obfuscation
HKTL_PY_Loader_Feb21_2	2,29	56	Hacktool
Casing_Anomaly_PS1_Invoke_Expression	2,32	90	Obfuscation
SUSP_Registry_Export_SAM_Mar21_1	2,33	15	Hacktool
SUSP_Odd_Net_Stop_Aug24	2,35	34	Malicious Script
HKTL_LNX_Gen_Detection_Jan21	2,40	15	Hacktool
SUSP_BAT_to_EXE_Converter_Jul21_1	2,40	101	Anomaly
HKTL_Unknown_Feb19_1	2,45	11	Hacktool
SUSP_PY_Reverse_Shell_Indicators_Jan23_1	2,48	33	Hacktool
SUSP_ELF_LNX_UPX_Compressed_File_DeepEv	2,49	241	Anomaly
SUSP_LNX_SH_Cron_Wget_Apr21_1	2,53	17	Config Backdoor
SUSP_VBS_Patterns_Jul21_1	2,54	13	Malicious Script
HKTL_PS1_NetScan_Oct22_1	2,55	11	Hacktool
Casing_Anomaly_PS1_StringChar	2,55	127	Obfuscation

SUSP_MSHTA_Invocation_Dec21_1	2,56	16	Malicious Script
SUSP_PY_Malware_Indicators_Mar25	2,60	50	Malware
SUSP_Odd_Sc_Config_Aug24	2,61	49	Malicious Script
APT_RU_MalDoc_Feb22_1	2,63	16	Malicious Document
APT_UA_Hermetic_Wiper_Artefacts_Feb22_1	2,71	24	Malware
SUSP_HKTL_Defender_Bypass_Patterns_Jan22_	2,71	21	Hacktool
SUSP_Find_Password_CommandLine_Feb19	2,71	17	Hacktool
Casing_Anomaly_Replace	2,72	134	Obfuscation
SUSP_OBFUSC_PY_RevShell_Jun23_1	2,74	57	Obfuscation
SUSP_LNX_SH_CryptoMiner_Indicators_Dec20_	2,75	20	Malware
SUSP_Linux_Crontab_Entry_Oct21_2	2,78	23	Config Backdoor
SUSP_LNX_Back_Connect_Shell_Indicator_Jun2	2,78	37	Hacktool
APT_MAL_Chimera_ForensicArtefacts_Jan21_1	2,79	33	Malware
Casing_Anomaly_StringChar	2,81	128	Obfuscation
HKTL_Metasploit_OfficeMacro_Apr20_1	2,85	13	Hacktool
SUSP_ISO_PhishAttachment_Password_In_Bod	2,93	29	Phishing Attachment
SUSP_WEvtUtil_ClearLogs_Sep22_1	2,95	59	Malicious Script
HKTL_Meterpreter_InMemory_Rule	2,95	20	Hacktool
ipscan24	2,96	108	Dual Use Tool
HKTL_EDRSandblast_CommandLine_Dec21_1	3,00	24	Hacktool
SUSP_Script_PS1_PE_Injection_Indicators_Mar2	3,00	14	Malicious Script
Casing_Anomaly_Public	3,00	22	Obfuscation
HKTL_Procdump_BAT_Jan13	3,02	57	Hacktool
SUSP_Linux_Crontab_Entry_Oct21_1	3,05	21	Config Backdoor
SUSP_OBF_BAT_Mar25	3,06	130	Malicious Script
SUSP_Ncat_Indicators_Apr23_1	3,06	17	Hacktool
SUSP_LNX_Rev_Shell_Indicator_Jan23_1	3,12	30143	Malicious Script
SUSP_LNX_SH_Cron_Curl_Apr21_1	3,13	15	Config Backdoor
MAL_Encrypted_IDAT_Payload_Mar24	3,14	131	Malware
OEBuilder_Nov17	3,17	76	Malware
ipscan24_Scan	3,19	109	Dual Use Tool
SUSP_Product_Uninstall_Aug24	3,21	14	Malicious Script
SUSP_BAT_OBFUSC_Jan23_3	3,24	17	Obfuscation
APT_MAL_CN_Chimera_Keywords_Apr20_1	3,25	36	Malware
SUSP_PS1_PowerShell_File_From_Network_Sha	3,29	14	Malicious Script
Casing_Anomaly_CommonProgram	3,32	22	Obfuscation
SUSP_ComSvcs_MiniDump_Indicators_Jun24	3,33	12	Malicious Script
SUSP_WEBSHELL_JPEG_PHP_Code_Dec20_1	3,34	32	Webshell
PUA_HRSword_Apr25	3,35	23	Dual Use Tool
APT_MuddyWater_VBA_Jun21_1	3,38	13	Malware
SUSP_LNX_Cat_Shadow_Jun22_1	3,38	32	Malicious Script
SUSP_OBFUSC_Casing_Anomaly_Runas_Exe	3,38	16	Obfuscation
SUSP_PS1_Decrypt_Load_Jul23_1	3,39	92	Obfuscation
empty_LM_hash	3,47	15	Anomaly
SUSP_InjectRunning_Mavinject_May21_1	3,50	24	Malicious Script
SUSP_PUA_SoftEther_VPNGate_Sftware_Dec21_	3,60	47	Dual Use Tool
SUSP_Encoded_StartSleep	3,65	164	Obfuscation
SUSP_OBFUSC_PowerShell_Format_String_Jan2	3,65	17	Obfuscation
SUSP_PY_Exploit_BackDoor_Indicators_Mar22_	3,67	27	Malicious Script

Mimikatz_Commands	3,67	15	Hacktool
SUSP_LNX_RevShell_Indicators_Mar23_3	3,67	20450	Malicious Script
SUSP_VBS_Jul21_1	3,68	19	Malicious Script
SUSP_SVG_Embedded_JS_Apr25	3,69	636	Malicious Script
SUSP_PS1_Obfuscation_Char_Sep22	3,73	26	Obfuscation
SUSP_BAT_OBFUSC_Indicators_Sep23	3,74	47	Obfuscation
SUSP_BAT_Obfuscation_Nov19_1	3,84	38	Obfuscation
HKTL_Ladpdomaindump_Bloodhound_Feb19	3,85	33	Hacktool
SUSP_PY_Pattern_Dec21_1	3,89	127	Malicious Script
EXPL_Log4j_CallBackDomain_IOCs_Dec21_1	3,91	11	Malicious Script
AppLocker_Rundll32_Bypass_Method	4,00	15	Malicious Script
SUSP_Comsvcs_DLL_MiniDump_Dec21_1	4,04	26	Malicious Script
SUSP_MSF_MSFVenom_Indicator_Jan23_1	4,05	97	Hacktool
SUSP_OfficeDoc_Macro_Indicator_SubAutoOpe	4,06	2305	Malicious Document
SUSP_BAT_OBFUSC_ENV_Obfuscation_Apr21_	4,07	86	Obfuscation
Char_Casing_Anomaly	4,17	132	Obfuscation
SUSP_PS1_Obfusc_Combo_Base64_Character(	4,17	18	Obfuscation
SUSP_MAL_RANSOM_Go_Indicators_Jun26_2	4,19	37	Malware
SUSP_JS_Reversed_Http_Aug23	4,21	24	Malicious Script
SUSP_CertUtil_Encode_Feb22_1	4,21	29	Obfuscation
EXPL_JNDI_Exploit_Patterns_Dec21_1	4,27	11	Hacktool
SUSP_MAL_Bot_Indicators_Nov21_1	4,27	22	Malware
EXPL_Log4j_CVE_2021_44228_Pattern_Dec21	4,33	12	Hacktool
SUSP_FilePath_PerfLogs_Oct21_1	4,33	12	Anomaly
SUSP_Registry_Save_SAM	4,46	35	Malicious Script
MAL_RAT_MALSPAM_PE_Sep19	4,51	79	Malware
MAL_BAT_OBFUSC_BOM_Override_Apr25	4,58	342	Obfuscation
SUSP_BAT_PS1_Contents_Jan23_1	4,61	28	Malicious Script
Certutil_Decode_Suspicious	4,62	42	Obfuscation
SUSP_PHP_OBFUSC_Indicators_May25	4,62	50	Obfuscation
SUSP_PyInstaller_ReflectiveLoad_Apr25	4,63	123	Malicious Script
SUSP_BAT_OBFUSC_Dec24	4,73	11	Obfuscation
PUA_RMM_GetScreen_Dec24	4,76	34	Dual Use Tool
SUSP_AMSI_Manipulation_Indicator_Mar23_1	4,77	13	Malicious Script
SUSP_OBFUSC_Base64_Hex_Encoded_Apr19	4,77	818	Obfuscation
SUSP_OBFUSC_PY_PYInstaller_Obfuscator_Dec	4,80	15	Obfuscation
SUSP_Encoded_Net_ServicePointManager	4,81	31	Obfuscation
SUSP_LNX_SH_Code_Indicator_Payload_Nov21	4,86	21	Malicious Script
EXPL_SUSP_Yoserial_Payloads_Jan21_3	4,86	14	Hacktool
SUSP_BAT_Registry_DisableRealtimeMonitoring_	4,92	26	Malicious Script
SUSP_Registry_SecurityDisable_Jun21	4,92	24	Malicious Script
MAL_PY_Compressed_B64_May24	4,97	89	Obfuscation
SUSP_MalDoc_Nov18_1	5,00	26	Malicious Document
APT_HEXANE_OfficeDropper_Aug19_1	5,00	28	Anomaly
SUSP_Script_PS1_Indicators_Mar21_1	5,13	45	Malicious Script
SUSP_Doc_StartMenu_Startup_Reference	5,18	11	Malicious Script
SUSP_LNX_BASH_Reverse_Shell_Indicators_Jan	5,28	18	Malicious Script
SUSP_LNX_Reverse_Shell_Indicator_Others_Jun	5,29	21	Malicious Script
SUSP_Encoded_SystemReflection_Assemly_Lo	5,33	61	Obfuscation

SUSP_PY_Exec_Import_Aug22_1	5,38	13	Anomaly
SUSP_PHP_OBFUSC_Encoded_Eval_May25	5,44	72	Obfuscation
HKTL_Reverse_Shell_Patterns_Jan23_1	5,45	20	Hacktool
SUSP_OBFUSC_PowerShell_True_Jun20_1	5,47	15	Obfuscation
SUSP_PY_PTY_Spawn_Jun21_1	5,50	14	Malicious Script
Exec_master_xp_cmdshell_exection	5,53	19	Anomaly
SUSP_OBFUSC_Aug22_1	5,57	505	Obfuscation
NTLM_Dump_Output	5,58	19	Anomaly
SUSP_ProcDumping_Indicators_Oct21_1	5,58	12	Hacktool
WEBSHELL_CloakedAsPic_Feb20	5,63	41	Webshell
SUSP_LNX_Reverse_Shell_Indicators_Jul22	5,64	22	Malicious Script
SUSP_SC_STOP_Windows_Defender_Jan22	5,66	64	Malicious Script
Mimikatz_Memory_Rule_1	5,69	68	Hacktool
SUSP_VBA_Macro_Import_DLL_Oct22	5,71	544	Malicious Document
SUSP_MalDoc_Emotet_Char_OBFUSC_May22	5,72	47	Malicious Document
SUSP_PS1_Kernel32_User32_Imports_May21_	5,73	44	Malicious Script
SUSP_CryptoCoin_Miner_URIScheme_Stratum_	5,73	30	Dual Use Tool
LM_hash_empty_String	5,75	16	Anomaly
SUSP_Base64_Encoded_WScriptShell	5,75	16	Malicious Script
HKTL_JS_PowerShell_Token_Grabber_JavaScript	5,75	99	Malicious Script
SUSP_FromBase64_StartProcess_Combo_Mar2	5,77	95	Obfuscation
SUSP_Github_Repo_Name_Mar25	5,78	456	Hacktool
EXPL_Office_TemplateInjection_Aug19	5,79	71	Malicious Document
WEBSHELL_JSP_Nov21_1	5,80	15	Webshell
SUSP_VBA_Jan25_3	5,86	22	Malicious Document
SUSP_PY_OBFUSC_Hyperion_Aug22_1	5,87	15	Obfuscation
SUSP_OBFUSC_Bat_May25	5,88	26	Obfuscation
HKTL_Meterpreter_PY_Pattern_Dec21_1	5,88	101	Hacktool
SUSP_Combo_JS_PS_SchTasks	5,94	124	Obfuscation
Casing_Anomaly_String_Statement	5,96	165	Obfuscation
SUSP_PS1_Loader_Indicators_Jul22_6	5,96	23	Obfuscation
SUSP_OBFUSC_JS_May22_1	6,00	45	Obfuscation
SUSP_Encoded_User_Public_Nov21	6,01	112	Malicious Script
MAL_RANSOM_LockBit_Apr23_1	6,05	19	Malware
SUSP_Python_Import_Function_Combo_Jul21_	6,06	18	Malicious Script
SUSP_PS1_FunctionImports_Jul22_1	6,07	14	Malicious Script
Webshell_Cloaked	6,07	14	Webshell
SUSP_Base64_Encoded_AppData	6,14	508	Obfuscation
SUSP_PUA_MitmProxy_Feb25	6,15	13	Dual Use Tool
SUSP_LOLBAS_2	6,15	26	Malicious Script
SUSP_MAL_WASP_Stealer_Indicators_Jun24_1	6,17	12	Malware
SUSP_VBS_Loader_Oct24_1	6,21	14	Malicious Script
SUSP_PS1_Loader_Indicators_Dec22_2	6,21	560	Malicious Script
SUSP_Encoded_PS_DownloadString	6,22	106	Obfuscation
SUSP_PS1_Loader_Indicators_Oct23_1	6,25	12	Malicious Script
HKTL_PS1_Hacktool_Indicator_Feb20_1	6,27	15	Hacktool
SUSP_Injector_Keywords_Dec19_1	6,31	13	Malicious Script
Casing_Anomaly_WindowStyle_Hidden	6,35	17	Obfuscation
SUSP_MAL_PY_Python_Pattern_Aug22_2	6,36	22	Malicious Script

SUSP_OBFUSC_Ampersand_Excel_Jun22_2	6,38	52	Obfuscation
Impacket_Python_Library	6,40	105	Hacktool
Webshell_templatr	6,43	54	Webshell
SUSP_EXPL_CVE_2019_16098_PPL_Killer_Too	6,44	18	Malicious Script
HKTL_LSASS_Dumper_CmdLines_May23_1	6,45	69	Hacktool
SUSP_MAL_PY_Python_Pattern_Aug22_1	6,47	17	Malicious Script
SUSP_Go_Binary_IP_Lookup_Indicators_Jan22_	6,49	445	Anomaly
SUSP_VBA_System32Access_Dec21	6,52	29	Malicious Document
SUSP_PY_OBFUSC_RevShell_Indicators_Mar23	6,52	99	Obfuscation
SUSP_Office_Macro_VBA_AutoExec_Combo_OB	6,53	36	Obfuscation
SUSP_Download_RawGithubUsercontent	6,53	17	Anomaly
SUSP_Encoded_PowerShell_Class	6,53	66	Obfuscation
SUSP_PY_OBFUSC_RevShell_Indicators_Mar23	6,55	95	Obfuscation
SUSP_MkFifo_Tmp_Jul22	6,59	27	Anomaly
SUSP_LNK_BatchScripting_Apr22_2	6,61	187	Malicious Script
SUSP_PS1_Loader_Dec21_1	6,62	13	Malicious Script
SUSP_PS1_Dropper_Indicators_Oct23	6,63	48	Anomaly
SUSP_BAT_Big_Jul23_1	6,63	57	Malicious Script
SUSP_Linux_Commands_Sep18_1	6,64	11	Malicious Script
SUSP_OfficeDoc_Bin_Base64_Indicator_Jun22	6,66	192	Malicious Document
SUSP_PHP_Obfuscation_GZ_Base64	6,77	57	Obfuscation
SUSP_Suspicious_PowerShell_Indicator_Oct21	6,77	13	Malicious Script
SUSP_Encoded_PS1_Reflection_Assembly_Jul2	6,79	162	Obfuscation
WEBSHELL_O0_obfuscation_Feb20	6,82	17	Obfuscation
SUSP_OBFUSC_Casing_Anomaly_Comobject	6,82	11	Obfuscation
SUSP_PS1_PowerShell_Loader_May21_1	6,82	57	Malicious Script
SUSP_Encoded_IO_Decompress	6,83	668	Obfuscation
SUSP_CryptoMiner_Config_Indicator_Dec21_1	6,84	49	Dual Use Tool
SUSP_PS1_PowerShell_Ipify_Mar23_1	6,85	20	Anomaly
SUSP_OBFUSC_obfs4_May22	6,86	14	Obfuscation
SUSP_Combo_DOMDocument_Base64Data_Ma	6,87	189	Obfuscation
MAL_NET_MeterPreter_Payload_2	6,91	11	Hacktool
MAL_Tiny_Utility_Module_May24	6,91	241	Hacktool
SUSP_PS1_FromBase64_IEX_Combo_Jul21_1	6,93	15	Obfuscation
HKTL_VBA_Shellcode_Runner_Dec22_1	6,97	32	Malicious Script
SUSP_Hex_Encoded_WScript_Shell_1	7,00	13	Malicious Script
SUSP_Go_OBFUSC_Pattern_Jan23_2	7,01	170	Obfuscation
HKTL_LNX_GenShell_Feb21_1	7,10	51	Hacktool
SUSP_JS_Exfiltrating_Info_Dec23_3	7,19	67	Malicious Script
SUSP_NCat_Flags_Dec22_1	7,21	39	Hacktool
SUSP_OBFUSC_HTTPS_Split_Apr25_3	7,22	27	Obfuscation
SUSP_Small_Powershell_Download_Execute_M	7,23	26	Anomaly
SUSP_Eval_Base64_Indicators_Feb22_1	7,23	173	Obfuscation
SUSP_OBFUSC_BAT_Jan23_2	7,26	23	Obfuscation
SUSP_LNX_Reverse_Shell_Indicator_PHP_Jun21	7,28	18	Malicious Script
SUSP_RANSOM_ESX_Indicators_Feb23_1	7,33	12	Malware
HKTL_PS1_Villain_C2_Implant_Apr23_1	7,33	15	Hacktool
SUSP_Recon_Suspicious_Dirs_Sep21_1	7,33	21	Malicious Script
SUSP_Wide_Base64_Convert_FromBase64Strin	7,36	539	Obfuscation

SUSP_MPClient_ANOMALY_Aug22_2	7,42	24	Anomaly
SUSP_Base64_ReflectionAssembly	7,42	115	Obfuscation
SUSP_JS_OBFUSC_Base64_Combo_Jul22_1	7,45	40	Obfuscation
SUSP_OffSec_Authors_Indicator_Jun21	7,46	13	Hacktool
SUSP_InvokeDosfucation_Gen_1	7,50	12	Obfuscation
WMIC_Remote_Process_and_RAR	7,53	15	Anomaly
SUSP_PS1_OFBUSC_XOR_Encryption_Aug23	7,54	56	Obfuscation
SUSP_LNX_Reverse_Shell_Indicator_Jun21_2	7,55	29	Malicious Script
SUSP_PY_Stealer_Characteristics_Sep24	7,56	138	Malware
Casing_Anomaly_Certutil_Urlcache	7,58	12	Obfuscation
SUSP_LNX_Malware_Indicators_Aug21_1	7,58	12	Malware
MAL_Valak_VBA_Indicators_Jul20_1	7,64	14	Malicious Document
SUSP_Encoded_PS1_IntPtr_Zero_Jul21_1	7,65	17	Obfuscation
SUSP_Hacktool_Output_Strings_Feb16	7,66	56	Hacktool
SUSP_JS_IN_LNK_Mar25	7,68	130	Malicious Script
SUSP_CharCode_Obfuscation	7,73	48	Obfuscation
SUSP_JS_Document_Write_Unescape_Indicator	7,80	352	Malicious Script
SUSP_shellpop_Bash	7,81	110	Malicious Script
SUSP_Download_Githubcontent_Shell	7,85	20	Malicious Script
WEBSHELL_PHP_NeoReGeorg_Tunnel_Sep23	7,86	14	Webshell
MAL_SUSP_RANSOM_LockBit_RansomNote_Fe	7,92	12	Malware
Casing_Anomaly_ToString	7,92	13	Obfuscation
SUSP_PS1_Loader_Indicators_Nov21_1	7,93	2011	Malicious Script
SUSP_LNX_ShellCode_Loader_Jun21_1	7,93	15	Malicious Script
SUSP_Encoded_IWR_Jun22	7,93	178	Obfuscation
SUSP_OBFUSC_JS_Atob_Split_Feb23	7,97	101	Obfuscation
SUSP_PHP_Obfuscation_ROT13_GZ_Base64	8,00	12	Obfuscation
WEBSHELL_Gen_NeoRegeorg_Tunnel_Feb21	8,00	22	Webshell
SUSP_CVE_Program_Indicator_Oct21_1	8,04	57	Hacktool
HKTL_PS1_Hack_Tools_Jul23_1	8,05	22	Hacktool
SUSP_PostExploitation_Cmds_Aug19_1	8,09	34	Hacktool
SUSP_OBFUSC_Reversed_Encoded_Executable	8,11	212	Obfuscation
SUSP_Encoded_ShellCode	8,14	85	Malicious Script
SUSP_PS1_IEX_Pattern_Feb22_1	8,16	25	Malicious Script
SUSP_LNX_ReverseShells_Jun21_1	8,17	23	Malicious Script
SUSP_Base64_Encoded_PS1_TCPClient_Jan22	8,21	38	Obfuscation
SUSP_HKTL_CodeGangsta_Inject_Lib_May21	8,21	14	Hacktool
SUSP_Download_Cradles_Oct22_1	8,21	14	Malicious Script
HKTL_Nightmangle_Indicators_Sep23	8,21	29	Hacktool
SUSP_PS1_Base64_Encoded_Pattern_Feb22_1	8,21	34	Obfuscation
HKTL_SharpMonoInjector_Mar22_1	8,21	34	Hacktool
SUSP_AdobePDF_Bitmap_Executable	8,23	13	Malicious Document
SUSP_WIN_AD_Evaluations_Nov24	8,30	23	Malicious Script
SUSP_PS1_OBFUSC_String_Obfuscation_Mar25	8,31	39	Obfuscation
SUSP_Dir_Ref_in_File_Perflogs	8,32	41	Anomaly
SUSP_LNX_Reverse_Shell_Indicator_Ruby_Jun2	8,35	20	Malicious Script
SUSP_Defense_Evasion_Virtualization_Artifacts_	8,36	11	Dual Use Tool
SUSP_PS1_Shellcode_Runner_Indicators_Dec2	8,38	16	Malicious Script
SUSP_HKTL_LNX_CheatSheet_Commands	8,41	41	Hacktool

HKTL_CobaltStrike_Beacon_BOF_Indicators	8,44	25	Hacktool
SUSP_ZIP_LNK_Small_Apr22_1	8,45	104	Anomaly
SUSP_EXPL_Script_MultipleAs_May21_1	8,45	11	Malicious Script
WEBSHELL_phpWhitespace_Feb20	8,50	12	Webshell
SUSP_Hex_Encoded_RegistryKey	8,52	33	Obfuscation
SUSP_ZIP_LNK_PhishAttachment_Pattern_Jun2	8,53	124	Anomaly
SUSP_VBS_Combo_Jul22_2	8,56	25	Malicious Script
SUSP_TINY_ISO_Feb22_1	8,60	45	Phishing Attachment
SUSP_HKTL_ShellCode_Loader_Jan21_3	8,63	38	Malicious Script
SUSP_Base64_Encoded_Metasploit_Payload	8,64	36	Obfuscation
SUSP_PS1_Kernel32_Reference_Aug22	8,67	18	Malicious Script
SUSP_CobaltStrike_Beacon_BOF_Indicators_Fe	8,70	30	Hacktool
SUSP_Reversed_PowerShell_Code	8,71	21	Malicious Script
PUA_HKTL_SoftPerfect_Netscan_Nov24	8,75	20	Hacktool
SUSP_OBFUSC_BAT_Mar25	8,75	48	Obfuscation
SUSP_HKTL_CobaltStrike_PS1_Loader_Indicato	8,80	130	Hacktool
SUSP_CryptoMiner_Indicator_Dec21_1	8,81	47	Dual Use Tool
SUSP_PS1_IWR_Uri_Feb22	8,82	22	Malicious Script
MAL_Webshell_Mini_PHP	8,82	11	Webshell
SUSP_PS1_PowerShell_Script_Indicators_Jul21	8,83	18	Malicious Script
SUSP_Hacktool_Authors_Mar21_1	8,90	30	Hacktool
SUSP_Go_OBUFSC_Nov22_1	8,90	21	Obfuscation
SUSP_PHP_Base64_File_Download_Aug23	8,91	11	Anomaly
SUSP_Env_Var_Obfuscation	8,95	126	Obfuscation
SUSP_Reversed_Base64_Encoded_EXE	8,99	169	Anomaly
Generic_Exploit_Strings_Apr18	9,05	57	Hacktool
SUSP_PS1_Indicators_OBFUSC_Dec21_6	9,06	1368	Obfuscation
SUSP_PS1_OBFUSC_Patterns_Nov21_1	9,09	11	Obfuscation
SUSP_Script_PS1_PE_Injection_Indicators_Mar2	9,11	1518	Malicious Script
SUSP_HKTL_PS1_Loader_May23_3	9,12	2692	Hacktool
SUSP_PS1_Keywords_Mar21_1	9,15	13	Malicious Script
SUSP_PowerShell_Content_JAB	9,16	44	Obfuscation
SUSP_WEBSHELL_ASP_Indicators_Jan21_2	9,17	12	Webshell
SUSP_PS1_OBFUSC_Nov23_1	9,18	11	Obfuscation
SUSP_LNX_Back_Connect_Shell_Indicator_Jun2	9,18	66	Malicious Script
Webshell_like_System_Shell_Exec	9,21	73	Anomaly
HKTL_AntiAV_Indicators_Jul21_1	9,24	17	Hacktool
SUSP_Env_Variable_Substring_Obfuscation_Se	9,27	44	Obfuscation
SUSP_SCRIPT_Hacktool_Indicator_May25	9,32	152	Malicious Script
MAL_CobaltStrike_Apr18_1_CSharp_Powershel	9,33	15	Hacktool
SUSP_HKTL_Encoded_Hacktool_Strings_Oct21	9,34	29	Hacktool
SUSP_ShellCode_Indicators_Feb23_1	9,41	17	Malicious Script
HKTL_PS1_Loader_Mar21_1	9,55	29	Hacktool
HKTL_Chrome_App_Bound_Encryption_Decryp	9,55	11	Hacktool
SUSP_Keywords_EDR_Fingerprinting_Feb22_1	9,63	16	Malicious Script
SUSP_SC_Service_Delete_Jul21_1	9,63	19	Malicious Script
Casing_Anomaly_Split	9,72	18	Obfuscation
MAL_Enemybot_Botnet_Apr22	9,73	97	Malware
SUSP_PS1_Small_Base64Decode_Jun22_1	9,76	1520	Obfuscation

SUSP_PS1_OBFUSC_Carret_Function_Obfuscat	9,79	14	Obfuscation
SUSP_Encoded_PowerShell_Policies_Sep21_1	9,79	28	Malicious Script
SUSP_WScript_Shell_Cut	9,80	41	Malicious Script
SUSP_WriteLdSoPreload_Sep21	9,83	12	Malicious Script
SUSP_Defense_Evasion_Known_MAC_Addresse	9,92	26	Malicious Script
SUSP_Beacon_BOF_Loader_Indicators_Mar23_1	9,94	31	Hacktool
SUSP_PS1_Telegram_Bot_Indicators_Jan23_1	10,00	15	Malware
SUSP_WMI_TimerEvent_Eval_Jun21_1	10,00	25	Malicious Script
SUSP_HKTL_PY_Impacket_Feb24	10,05	63	Hacktool
SUSP_PS1_Obfuscated_Payload_Feb19_1	10,08	25	Obfuscation
SUSP_B64_Atob_Aug23	10,09	2334	Obfuscation
SUSP_PowerShell_Command_JAB	10,17	52	Obfuscation
SUSP_SMALL_Loader_Indicators_Feb24_1	10,17	24	Malicious Script
WEBSHELL_PHP_Gen_Sep24_1	10,20	131	Webshell
SUSP_PS1_OBFUS_Loader_Feb24_4	10,23	48	Obfuscation
SUSP_Decimal_Encoded_MSDOS_Stub_Nov21	10,31	13	Obfuscation
SUSP_PS1_Loader_Indicator_Nov21_1	10,32	28	Malicious Script
SUSP_PS1_OBFUSC_Xor_Mar25	10,33	15	Obfuscation
SUSP_PS1_Loader_Indicators_Aug23	10,36	886	Malicious Script
SUSP_Bitsadmin_Transfer_Github_Jun22	10,38	40	Malicious Script
SUSP_EXPL_Shellcode_Keywords_Oct21	10,44	18	Malicious Script
SUSP_PS1_SCRIPT_Defender_Exlusions_Interp	10,47	15	Malicious Script
SUSP_PS1_CaseAnomaly_Chrw_Aug22_1	10,55	140	Obfuscation
SUSP_HKTL_Go_Rev_Shell_Indicators_Jan23_3	10,56	18	Hacktool
Webshell_GIF_Cloaked_PHP_Webshell	10,57	14	Webshell
Webshell_DTool_Pro_php	10,57	14	Webshell
WEBSHELL_suspEval_Mar20	10,59	311	Webshell
SUSP_SVG_JS_Payload_Mar25	10,59	17	Malicious Script
SUSP_VBA_Downloading_File_Using_Powershe	10,60	30	Malicious Document
SUSP_LNK_SuspiciousCommands_Jan23_1	10,64	25	Malicious Script
SUSP_VBS_Run_PowerShell_Jan22_1	10,66	199	Malicious Script
SUSP_BAT_UrlCache_Split	10,69	77	Malicious Script
SUSP_Encoded_NewObject_NetWebclient_2	10,70	27	Obfuscation
SUSP_PS1_OBFUSC_Nov23_5	10,72	25	Obfuscation
SUSP_Encoded_DownloadData	10,75	59	Obfuscation
SUSP_Encoded_WhereObject_GlobalAssembly	10,76	25	Obfuscation
SUSP_Webshell_slopShell_Jun21_1	10,77	13	Webshell
SUSP_GIF_Anomalies	10,82	33	Anomaly
EXPL_POC_SpringCore_0day_Indicators_Mar22	10,86	35	Hacktool
SUSP_OLE_Embedded_EXE_Oct23	10,89	439	Anomaly
SUSP_WEBSHELL_Tiny_Eval_Oct20	10,90	39	Webshell
SUSP_Base64_Encoded_C_Powershell	10,90	61	Obfuscation
HKTL_SecretsDump_Indicator_Jun21_1	10,92	12	Hacktool
Webshell_STNC_php_php	10,93	14	Webshell
SUSP_InvokeDosfucation_Set_Caret_Gen	10,97	33	Malicious Script
SUSP_SMALL_ISO_Script_Feb22_1	11,00	17	Malicious Script
PsExec_RemComService_PY	11,07	14	Anomaly
SUSP_Doc_with_PowerShell_Download	11,07	41	Malicious Document
SUSP_Obfuscated_Batch_Script_Apr25	11,08	26	Obfuscation

SUSP_LNK_Curl_Download_Jul22_2	11,11	27	Malicious Script
SUSP_PS1_Base64_Encoded_Shells_Indicators	11,14	21	Obfuscation
WEBSHELL_PHP_Obfuscation_Functions_Sep2	11,15	79	Obfuscation
SUSP_HKTL_ShellCode_Loader_Jan21_1	11,18	51	Malicious Script
HKTL_CN_Archive_KHS_Mar15	11,20	20	Hacktool
SUSP_NtOpenProcess_Indicator_Jul21_1	11,20	15	Malicious Script
SUSP_PY_ShellCode_Loader_Jan23_1	11,21	14	Malicious Script
SUSP_PS1_Tiny_Download_Cradle_Jan23_1	11,27	11	Malicious Script
SUSP_PS1_PowerShell_Loader_Indicators_Mar2	11,30	33	Malicious Script
WEBSHELL_ChinaChopper_Generic_Mar15	11,33	43	Webshell
Webshell_lamashell_php	11,38	13	Webshell
SUSP_PS1_CommandLine_Flag_Combo_Feb22	11,38	50	Malicious Script
HKTL_BeefXSSFramework_Dec19	11,40	35	Hacktool
SUSP_JS_Base64_WASM_Loader_Aug23	11,41	17	Malicious Script
SUSP_RevShell_CmdLine_Code	11,42	50	Malicious Script
SUSP_Certificate_Encoded_PE_Nov21_1	11,45	11	Malicious Script
SUSP_JS_OBFUSC_WebAssembly_Aug23	11,48	21	Obfuscation
WEBSHELL_JSP_Runtime_Exec_Oct20	11,50	12	Anomaly
Generic_Exploit_Strings_Oct18	11,58	154	Hacktool
MAL_GO_Shellcode_Loader_Jan24	11,59	56	Malicious Script
EXPL_CVE_2020_0796_Keywords	11,63	16	Hacktool
SUSP_PS1_Base64_Encoded_SingleLiner_Jun2	11,64	83	Obfuscation
SUSP_ExcelDNA_Apr22	11,66	59	Malicious Document
SUSP_PS1_IEX_IWR_Indicator_Feb22_1	11,67	15	Malicious Script
HKTL_PS1_Base64_Encoded_Shell_Indicators_	11,69	29	Hacktool
SUSP_PS1_Downloader_ProcInject_Sep21_2	11,69	13	Malicious Script
SUSP_PS1_OBFUSC_Nov23_2	11,71	14	Obfuscation
HKTL_SilentTrinity_Dev_Aug19	11,72	18	Hacktool
SUSP_Base64_Encoded_ShellCode_Mar22_1	11,73	15	Malicious Script
SUSP_MalDev_Indicators_Feb24_1	11,74	19	Malware
SUSP_BAT_Start_Min_Combo_PowerShell_Jul2	11,78	77	Malicious Script
SUSP_PS1_IEX_Indicator_Feb22_1	11,79	39	Malicious Script
SUSP_EnableContent_String_Gen	11,82	77	Malicious Script
WEBSHELL_Godzilla_Indicators_Jun22_1	11,83	18	Webshell
SUSP_FromBase64String_PAYLOAD_Combo	11,84	119	Obfuscation
SUSP_JS_May23	11,88	25	Malicious Script
SUSP_Encoded_Mingw_64_PE_Dec20_1	11,89	54	Obfuscation
Suspicious_Javascript_Running_Interpreter	11,93	162	Malicious Script
SUSP_InnoSetup_IDP_May25	11,93	542	Anomaly
SUSP_Linux_PrivEsc_Commands	11,95	20	Malicious Script
MAL_Discord_Token_Grabber_V2_Jun23	11,96	27	Malware
SUSP_PS1_Loader_Jan22_5	11,97	31	Malicious Script
SUSP_PS1_FromBase64String_Content_Indicat	11,97	115	Obfuscation
SUSP_OBFUSC_May21_1	12,00	32	Obfuscation
SUSP_ShellCode_Indicators_Jan24_1	12,04	46	Malicious Script
SUSP_Base64_UserAgent_Definition_Mar25	12,07	14	Obfuscation
SUSP_JS_Loader_Indicators_Jul23_1	12,07	27	Malicious Script
SUSP_Encoded_PE_Code_Jul21_1	12,08	13	Obfuscation
HKTL_ProcessInjection_Strings_PS1_Feb19_1	12,09	22	Hacktool

SUSP_Go_Keylogger_Indicators_May22_1	12,10	30	Hacktool
SUSP_BAT_Indicators_Aug24_1	12,16	77	Malicious Script
SUSP_ZIP_LNK_PhishAttachment_Pattern_Jun2	12,16	25	Phishing Attachment
SUSP_Netsh_PortProxy_Command_Apr19	12,20	15	Hacktool
EXPL_PaloAlto_CVE_2024_3400_Apr24_1	12,20	35	Hacktool
SUSP_ShellCode_Loader_OpCodes_Jun22_1	12,23	47	Malicious Script
SUSP_Office_Dropper_Strings	12,26	69	Anomaly
SUSP_WEBSHELL_PHP_Indicators_Apr25_1	12,27	15	Webshell
Casing_Anomaly_ForEach	12,27	22	Obfuscation
SUSP_ShellCode_Injector_Indicators_Jun22_1	12,28	53	Malicious Script
HKTL_Gost_Tunnel_May22	12,30	37	Hacktool
SUSP_OBFUSC_JS_Oct23_4	12,31	6567	Obfuscation
HKTL_SilentTrinity_PS1_Posh_Stager	12,31	13	Hacktool