MALICIOUS

Classifications: Downloader

Threat Names: Emotet | Mal/Generic-S | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**bmxixqaylqt.xls**
ID	#3264575
MD5	20759385064298185538fe8560b6dd18
SHA1	50ca3dc590956809332b5b878c0ff213d81440a1
SHA256	7443d5335a207cca176825bd774a412e72882c815206c7f59ace1feb111bb4e9
File Size	113.00 KB
Report Created	2022-01-11 14:32 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (16 rules, 234 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	4	Downloader
	• Rule "EmotetEccDecryption" from ruleset "Emotet" has matched on a memory dump for (process #2) rundll32.exe. • Rule "EmotetEccDecryption" from ruleset "Emotet" has matched on a memory dump for (process #3) rundll32.exe. • Rule "EmotetEccDecryption" from ruleset "Emotet" has matched on a memory dump for (process #6) rundll32.exe. • Rule "EmotetFunctionStrings" from ruleset "Emotet" has matched on the function strings for (process #6) rundll32.exe.			
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #3) rundll32.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr".			
4/5	Network Connection	Downloads executable	1	Downloader
	• (Process #1) excel.exe downloads executable via http from http://gaidov.bg/wp-includes/Ug/.			
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #1) excel.exe connects to "http://gaidov.bg/wp-includes/Ug/".			
4/5	Network Connection	Attempts to connect through HTTPS	40	-

Score	Category	Operation	Count	Classification
		• (Process #6) rundll32.exe connects to "131.100.24.231/sZuPkhFvxiruZGnkWSvBZJFMHwMYVGejYGd".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/cbdEcXhDUxjTynjcAbsoCaeAOPEKG".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/RShuHPCsvcntVeVPloUCMqSKmqNYvSQbjTDURzDELiTxnpAroacVpj".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/NSqcpi".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/PUxFVbubbsRiyeVOkylFLvjttHGxWuLZOTznFZDJDRCzjBXsCm".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/byuxizdZiMBRMMyvTrfAhSUmno".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/ovZMsGwuDvkCTVAuyUErEnviJRjFoYdxqzHAHCmEFowVipOJxPzHxegcyB".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/KCickUNfNVdluezRJQVzrSVrPGCcfHpSXQkeXolVLkiGTdBPKaPPgeHI".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/UUjGUHzEthTahLxeYVthAdNitVdOehJweJVinGsldtKfFTIagXDeKlobzUPVWUT".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/kIveWRCGbQlVsKDQuCjbRbxbpDmUTLRXQzstFZzYzrszPLCEuLPYdLC".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/TxNbeAQdUfkbUXFUXVRqjVQtoKYHhMYdO".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/yBEEnKhBylvRxCnDmpAEUlWSNelXgbrnpn".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/EbNOMLpVejdDyVULeZGbPrCFGbVbsTOPkiZZgYBbxeXXphaLsDMbQSSB".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/zMyKgMZsAUAz".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/rbSYzmWbHkrHWqqeRSGSjBKgtutkPBcboXUUeGsfTKBsLvroB".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/grco".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/TstxALIFdZSCBbRVhJ".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/xdohqFznFrXzjvxKGDoJkJqvmiXGarZxxdHusoAojxyf".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/XUTJxlmFENzNsUqZvdcBnfTMraHDnrhQTVonROhDRzsJXlWfuBdHAGRSxkZD".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/hmoSo".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/MgpAtRGHvDYHHuqMjChsaHiLoRULfkGcPRoPgy".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/tKcWvnBRzZcTf".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/nogGHxUlWIbDIgLssUyF".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/mhpTspdGiezEmAKcdgBlJoesESjzILqnQX".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/rFlVerNgyrSmXUggWdlremBTWYZCkCuRASKHzfsqJSwnaABShqhCQtgLQSSnBq".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/lyfASJCANyEeMSEnpXpaRFmYWRdzZpmrrpAhUpzOSuzKLlOpcGsaP".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/lFfVBkyXLzLxTCxJwrPPZXuAVVBHDMJjLb".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/PjNtLFourlwOKpzxahYuFVlaUiWQiNRwnyBuXSyDBtQBExDgjyWUdVZ".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/pDnfUnKnkXpXuCb".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/oBplEaBijFHajEsGgFHQALCBZzOkCROZGGW".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/XUhtMukWyxGCOUtlOamIMpz".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/NnSPrKLklQWyLpDsOBvayvHYfpr".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/klYPnZCNPtrLUyNKeydGtHtlcmHBBTEEfGqcmElywqcBshQXLJTYLMwsdqzWYx".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/SaByipWEoOu".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/snlYiBNxSZRzyhECNZCAQ".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/cafEzF".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/XkEOqreeJDfpFdyRRpleVtPAyEdT".		
		• (Process #6) rundll32.exe connects to "131.100.24.231/vRsBkRRVGMBCUOuWdZcAAAxpxQnFiBltgrIpnZYEhBJSSfFN".		
		• (Process #6) rundll32.exe connects to "209.59.138.75/uGgpKquXhAwYVUnpJNczDqWIgfQfpTUP".		
		• (Process #6) rundll32.exe connects to "209.59.138.75/OpDIaUbKbVKthFMeufGDyGNIcFlhcBgfRArWebvvHgyyNwCcPFJL".		
4/5	Network Connection	Tries to connect using an uncommon port	1	-
		• (Process #6) rundll32.exe tries to connect to TCP port 7080 at 209.59.138.75.		
4/5	Network Connection	Connects to a CMS hoster	1	-
		• (Process #1) excel.exe connects to a hosted Wordpress site at http://gaidov.bg/wp-includes/Ug/.		
4/5	Execution	Document tries to create process	1	-
		• Document creates (process #2) rundll32.exe.		

Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S". • Reputation analysis labels a file which was only downloaded to memory as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	41	-

Score	Category	Operation	Count	Classification
		• Reputation analysis labels the URL "http://gaidov.bg/wp-includes/Ug/" which was contacted by (process #1) excel.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/sZuPkhFvxiruZGnkWSvBZJFMHwMYVGejYGd" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/cbdEcXhDUxjTynjcAbsoCaeAOPEKG" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/RShuHPCsvcntVeVPloUCMqSKmqNYvSQbjTDURzDELiTxnpAroacVpj" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/NSqcpi" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/PUxFVbubbsRiyeVOkylFLvjttHGxWuLZOTznFZDJDRCzjBXsCm" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/byuxizdZiMBRMMyvTrfAhSUmno" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/ovZMsGwuDvkCTVAuyUErEnviJRjFoYdxqzHAHCmEFowVipOJxPzHxegcyB" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/KCickUNfNVdluezRJQVzrSVrPGCcfHpSXQkeXolVLkiGTdBPKaPPgeHI" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/UUjGUHzEthTahLxeYVthAdNitVdOehJweJVinGsldtKfFTlagXDeKlobzUPVWUT" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/kIveWRCGbQlVsKDQuCjbRbxbpDmUTLRXQzstFZzYzrszPLCEuLPYdLC" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/TxNbeAQdUfkbUXFUXVRqjVQtoKYHhMYdO" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/yBEEnKhBylvRxCnDmpAEUlWSNelXgbrnpn" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/EbNOMLpVejdDyVULeZGbPrCFGbVbsTOPkiZZgYBbxeXXphaLsDMbQSSB" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/zMyKgMZsAUAz" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/rbSYzmWbHkrHWqqeRSGSjBKgtutkPBcboXUUeGsfTKBsLvroB" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/grco" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/TstxALIFdZSCBbRVhJ" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/xdohqFznFrXzjvxKGDoJkJqvmiXGarZxxdHusoAojxyf" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/XUTJxImFENzNsUqZvdcBnfTMraHDnrhQTVonROhDRzsJXlWfuBdHAGRSxkZD" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/hmoSo" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/MgpAtRGHvDYHHuqMjChsaHiLoRULfkGcPRoPgy" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/tKcWvnBRzZcTf" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/nogGHxUlWIbDIgLssUyF" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/mhpTspdGiezEmAKcdgBlJoesESjzlLqnQX" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/rFlVerNgyrSmXUggWdlremBTWYZCkCuRASKHzfsqJSwnaABShqhCQtgLQSSnBq" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/IyfASJCANyEeMSEnpXpaRFmYWRdzZpmrrpAhUpzOSuzKLIOpcGsaP" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/IFfVBkyXLzLxTCxJwrPPZXuAVVBHDMJjLb" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/PjNtLFourlwOKpzxahYuFVlaUiWQiNRwnyBuXSyDBtQBExDgjyWUdVZ" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/pDnfUnKnkXpXuCb" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/oBplEaBijFHajEsGgFHQALCBZzOkCROZGGW" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/XUhtMukWyxGCOUtlOamIMpz" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/NnSPrKLklQWyLpDsOBvayvHYfpr" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/klYPnZCNPtrLUyNKeydGtHtlcmHBBTEEfGqcmElywqcBshQXLJTYLMwsdqzWYx" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/SaByipWEoOu" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/snlYiBNxSZRzyhECNZCAQ" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/cafEzF" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/XkEOqreeJDfpFdyRRpleVtPAyEdT" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://131.100.24.231/vRsBkRRVGMBCUOuWdZcAAAxpxQnFiBltgrIpnZYEhBJSSfFN" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://209.59.138.75/uGgpKquXhAwYVUnpJNczDqWIgfQfpTUP" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
		• Reputation analysis labels the URL "https://209.59.138.75/OpDIaUbKbVKthFMeufGDyGNIcFlhcBgfRArWebvvHgyyNwCcPFJL" which was contacted by (process #6) rundll32.exe as "Mal/HTMLGen-A".		
4/5	Reputation	File has embedded malicious URL	3	-

Score	Category	Operation	Count	Classification
		• Reputation analysis labels URL "http://gaidov.bg/wp-includes/Ug/" embedded in "c:\users\keecfmwgj\desktop\15eab100" as "Mal/HTMLGen-A". • Reputation analysis labels URL "http://studiokrishnaproduction.com/wp-includes/3mJ/" embedded in "c:\users\keecfmwgj\desktop\15eab100" as "Mal/HTMLGen-A". • Reputation analysis labels URL "http://goodmarketinggroup.com/live_site/Y9cEk9QNIDUeg/" embedded in "c:\users\keecfmwgj\desktop\15eab100" as "Mal/HTMLGen-A".		
4/5	Reputation	Contacts known malicious IP address	2	-
		• Reputation analysis labels the contacted IP address 131.100.24.231 as "Mal/HTMLGen-A". • Reputation analysis labels the contacted IP address 209.59.138.75 as "Mal/HTMLGen-A".		
3/5	Persistence	Installs system startup script or application	40	-

Score	Category	Operation	Count	Classification
		• (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",mZTS" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",EvGhBl" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",rFbKbpoZMr" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",ptbVmiePhYAD" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",gcDsvzmp" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",GVooMHN" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",WvmplLtp" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",agYgigWVpOAVBG" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",ytcumrnBp" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",GMmkFNztk" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",FPJFkmXYcTJq" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",wbktQowAvaiv" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",oZXKVljb" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",wPhOoGbY" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",WYJJKnx" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",qoBP" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",UsiQqsOJaBqzaZz" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",VOdWMKiEvVgxL" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",xtlmEUMiTSPmlAQ" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",oOMLQWAePTdFU" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",VervPB" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",XyxImc" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",XORWAYbbJRxFAT" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",FdBImAu" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",moHwsQoQljeAvTz" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",NkAtcmP" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",DfksXWBtMcnnbpU" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",vrWZhmXjgDni" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",SuMZv" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",Jgspcl" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",YoyG" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",deetjmuoWFdgpwS" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",gBenykfa" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",qCnOhZL" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",gbYcFjSMKXpvo" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",AAOlrBCLc" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",yGDkHmLf" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",trcbClsr" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",YPPwAbfyWPxnF" to Windows startup via registry. • (Process #6) rundll32.exe adds "C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",uPtjtXDkcbZ" to Windows startup via registry.		
2/5	Network Connection	URL indicates a CMS hoster	2	-
		• URL http://gaidov.bg/wp-includes/Ug/ embedded in document c:\users\keecfmwgj\desktop\15eab100 is hosted by Wordpress. • URL http://studiokrishnaproduction.com/wp-includes/3mJ/ embedded in document c:\users\keecfmwgj\desktop\15eab100 is hosted by Wordpress.		
1/5	Mutex	Creates mutex	93	-

- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-use_fc_key".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-sjlj_once".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-once_global_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-once_obj_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mutex_global_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_tls_once_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_tls_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mtx_pthr_locked_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mutex_global_static_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mxattr_recursive_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-pthr_root_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListCnt_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListMax_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idList_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListNextId_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-fc_key".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_lock_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_cancelling_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-cond_locked_shmem_rwlock".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-rwl_global_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_sch_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_max_shmem".
- (Process #2) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_dest_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-use_fc_key".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-sjlj_once".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-once_global_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-once_obj_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mutex_global_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_tls_once_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_tls_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mtx_pthr_locked_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mutex_global_static_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mxattr_recursive_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-pthr_root_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListCnt_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListMax_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idList_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListNextId_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-fc_key".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_lock_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_cancelling_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-cond_locked_shmem_rwlock".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-rwl_global_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_sch_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_max_shmem".
- (Process #3) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_key_dest_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-use_fc_key".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-sjlj_once".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-once_global_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-once_obj_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mutex_global_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_tls_once_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-_pthread_tls_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mtx_pthr_locked_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mutex_global_static_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-mxattr_recursive_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-pthr_root_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListCnt_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idListMax_shmem".
- (Process #5) rundll32.exe creates mutex with name "gcc-shmem-tdm2-idList_shmem".

Score	Category	Operation	Count	Classification
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a deprecated VBA macro which could not be extracted.			
-	Trusted	Known clean file	2	-
	• Embedded file "authroot.stl" is a known clean file. • File "c:\users\keecfmwgj\appdata\local\temp\~df0e8bec461e0e10fe.tmp" is a known clean file.			

Mitre ATT&CK Matrix

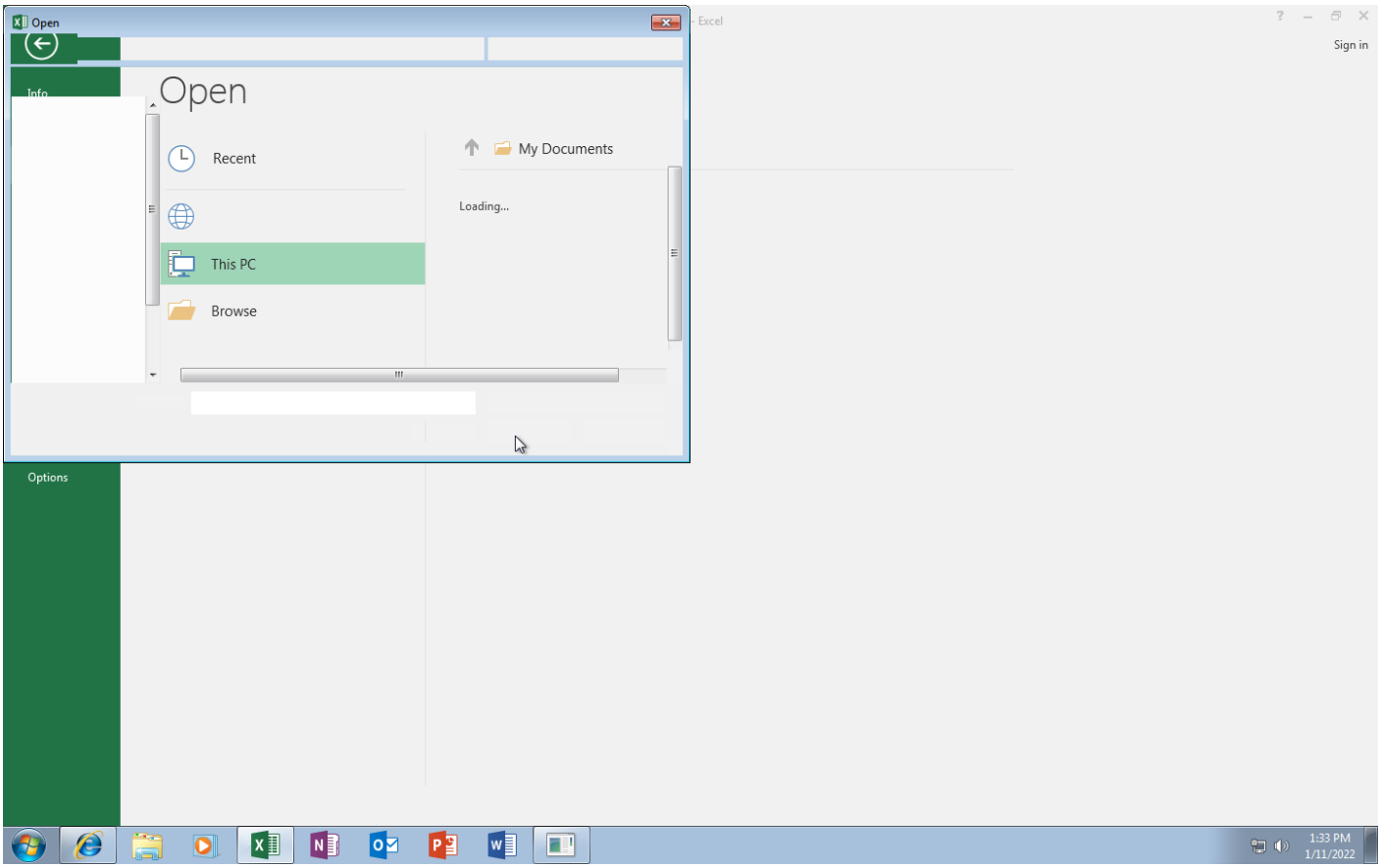
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting	#T1060 Registry Run Keys / Startup Folder		#T1096 NTFS File Attributes			#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
				#T1112 Modify Registry					#T1105 Remote File Copy		
				#T1064 Scripting					#T1032 Standard Cryptographic Protocol		
									#T1065 Uncommonly Used Port		

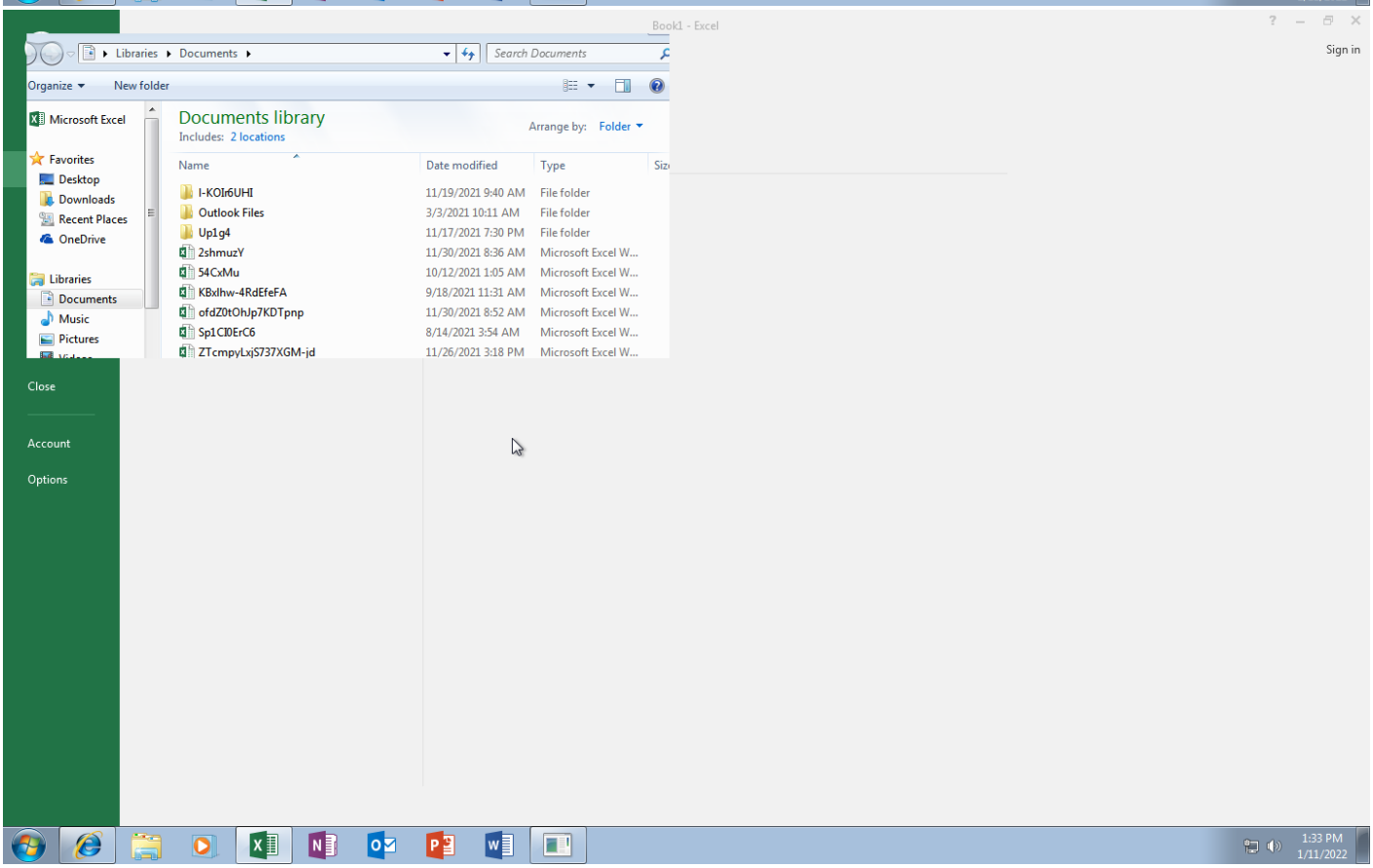
Sample Information

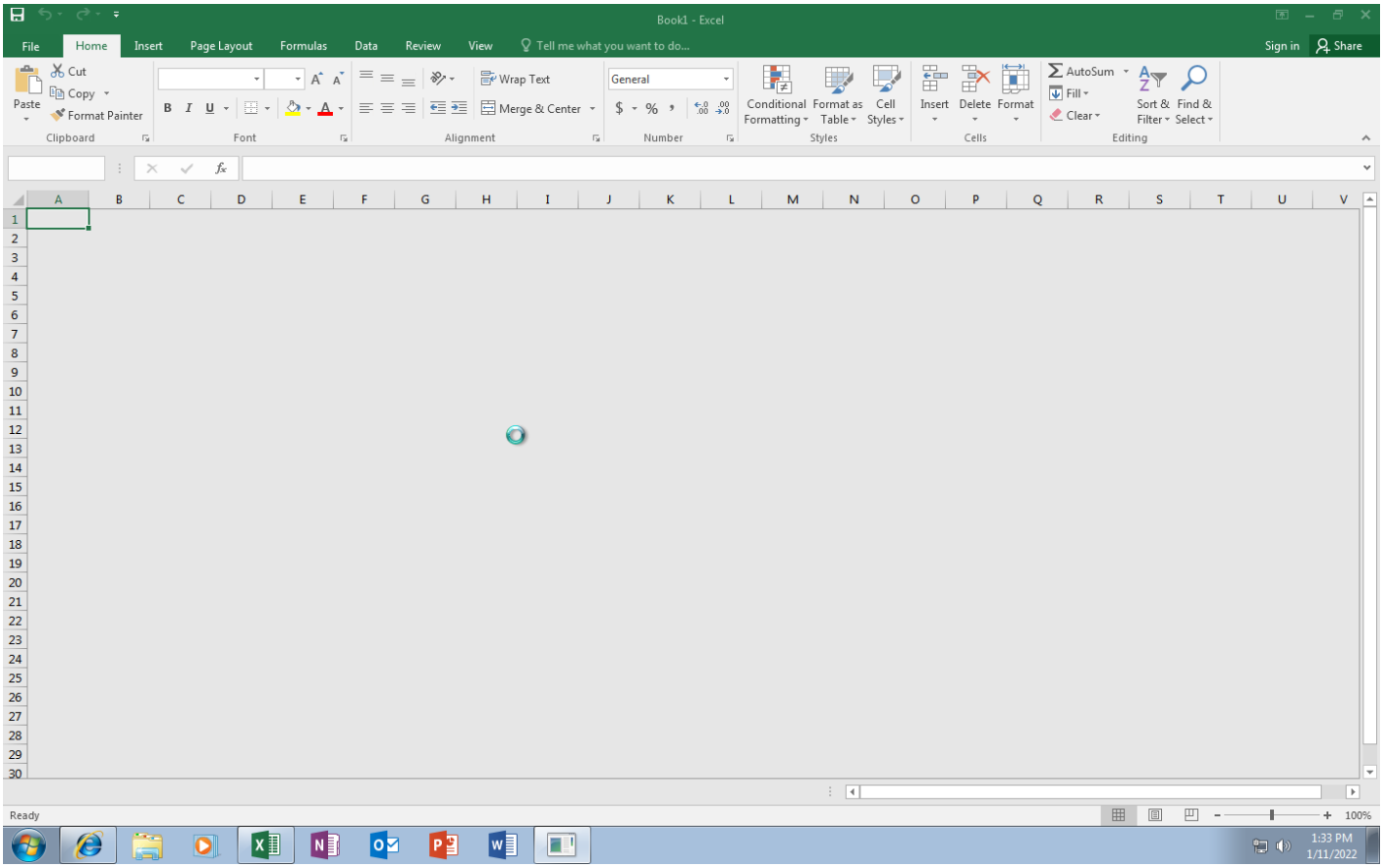
ID	#3264575
MD5	20759385064298185538fe8560b6dd18
SHA1	50ca3dc590956809332b5b878c0ff213d81440a1
SHA256	7443d5335a207cca176825bd774a412e72882c815206c7f59ace1feb111bb4e9
SSDeep	3072:yKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgQCyVEdBU6hubsll6UQjvxm:yKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgbr
File Name	bmxixqaylqt.xls
File Size	113.00 KB
Sample Type	Excel Document
Has Macros	✓

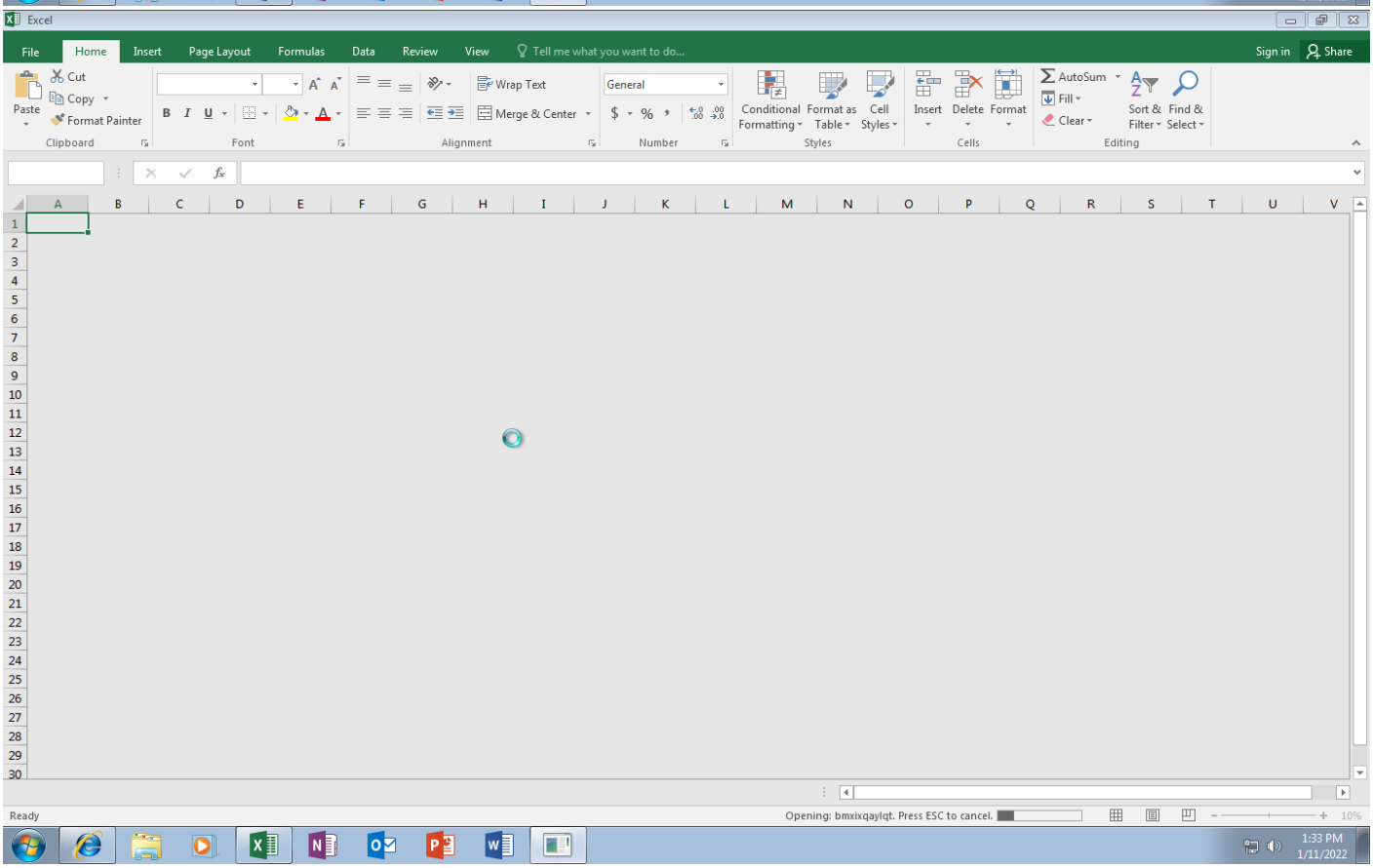
Analysis Information

Creation Time	2022-01-11 14:32 (UTC+1)
Analysis Duration	00:10:08
Termination Reason	Timeout
Number of Monitored Processes	5
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	25


Open
Info
Open
Recent
This PC
Browse
My Documents
Loading...
Options
Excel
Sign in
1:33 PM
1/11/2022


Libraries
Documents
Search Documents
Organize
New folder
Microsoft Excel
Documents library
Includes: 2 locations
Arrange by: Folder
Favorites
Desktop
Downloads
Recent Places
OneDrive
Libraries
Documents
Music
Pictures
Name
Date modified
Type
I-KOIr6UHI 11/19/2021 9:40 AM File folder
Outlook Files 3/3/2021 10:11 AM File folder
Up1g4 11/17/2021 7:30 PM File folder
2shmuzY 11/30/2021 8:36 AM Microsoft Excel W...
54CxMu 10/12/2021 1:05 AM Microsoft Excel W...
KBxlhw-4RdEfeFA 9/18/2021 11:31 AM Microsoft Excel W...
ofdZ0tOhJp7KDTpnp 11/30/2021 8:52 AM Microsoft Excel W...
Sp1Cl0ErC6 8/14/2021 3:54 AM Microsoft Excel W...
ZTcmpyLxjS737XGM-jd 11/26/2021 3:18 PM Microsoft Excel W...
Close
Account
Options
Book1 - Excel
Sign in
1:33 PM
1/11/2022





Screenshots truncated

NETWORK

General

2.66 KB total sent

431.96 KB total received

2 ports 80, 7080

3 contacted IP addresses

3 URLs extracted

2 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

41 URLs contacted, 3 servers

41 sessions, 2.66 KB sent, 431.96 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://gaidov.bg/wp-includes/Ug/	-	-		0 bytes	NA
GET	http://studiokrishnaproduction.com/wp-includes/3mJ/	-	-		0 bytes	NA
GET	http://goodmarketinggroup.com/live_site/Y9cEk9QNIDUeg/	-	-		0 bytes	NA
GET	https://131.100.24.231/sZuPkhFvxiruZGnkWSvBZJFMHwMYVGejYGd	-	-		0 bytes	NA
GET	https://131.100.24.231/cbdEcXhDUxjTynjcAbsoCaeAOPEKG	-	-		0 bytes	NA
GET	https://131.100.24.231/RShuHPCsvcntVeVPloUCMqSKmqNYvSQbjTDURzDELiTxnpAroacVpj	-	-		0 bytes	NA
GET	https://131.100.24.231/NSqcpi	-	-		0 bytes	NA
GET	https://131.100.24.231/PUxFVbubbsRiyeVOkylFLvjttHGxWuLZOTznFZDJDRCzjBXsCm	-	-		0 bytes	NA
GET	https://131.100.24.231/byuxizdZiMBRMMyvTrfAhSUmno	-	-		0 bytes	NA
GET	https://131.100.24.231/ovZMsGwuDvkCTVAuyUErEnviJRjFoYdxqzHAHCmEFowVipOJxPzHxegcyB	-	-		0 bytes	NA
GET	https://131.100.24.231/KCickUNfNVdluezRJQVzrSVrPGCcfHpSXQkeXolVLkiGTdBPKaPPgeHI	-	-		0 bytes	NA
GET	https://131.100.24.231/UUjGUHzEthTahLxeYVthAdNitVdOehJweJVinGsldtKfFTlagXDeKlobzUPVWUT	-	-		0 bytes	NA
GET	https://131.100.24.231/kIveWRCGbQlVsKDQuCjbRbxbpDmUTLRXQzstFZzYzrszPLCEuLPYdLC	-	-		0 bytes	NA
GET	https://131.100.24.231/TxNbeAQdUfkbUXFUXVRqjVQtoKYHhMYdO	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://131.100.24.231/yBEEnKhByIvRxCnDmpAEUlWSNelXgbrnpn	-	-		0 bytes	NA
GET	https://131.100.24.231/EbNOMLpVejdDyVULeZGbPrCFGbVbsTOPkiZZgYBbxeXXphaLsDMbQSSB	-	-		0 bytes	NA
GET	https://131.100.24.231/zMyKgMZsAUAz	-	-		0 bytes	NA
GET	https://131.100.24.231/rbSYzmWbHkrHWqqeRSGSjBKgtutkPBcboXUUeGsfTKBsLvroB	-	-		0 bytes	NA
GET	https://131.100.24.231/grco	-	-		0 bytes	NA
GET	https://131.100.24.231/TstxALIFdZSCBbRVhJ	-	-		0 bytes	NA
GET	https://131.100.24.231/xdohqFznFrXzjvxKGDoJkJqvmiXGarZxxdHusoAojxyf	-	-		0 bytes	NA
GET	https://131.100.24.231/XUTJxlmFENzNsUqZvdcBnfTMraHDnrhQTVonROhDRzsJXlWfuBdHAGRSxkZD	-	-		0 bytes	NA
GET	https://131.100.24.231/hmoSo	-	-		0 bytes	NA
GET	https://131.100.24.231/MgpAtRGHvDYHHuqMjChsaHiLoRULfkGcPRoPgy	-	-		0 bytes	NA
GET	https://131.100.24.231/tKcWvnBRzZcTf	-	-		0 bytes	NA
GET	https://131.100.24.231/nogGHxUlWIbDIgLssUyF	-	-		0 bytes	NA
GET	https://131.100.24.231/mhpTspdGiezEmAKcdgBlJoesESjzlLqnQX	-	-		0 bytes	NA
GET	https://131.100.24.231/rFlVerNgyrSmXUggWdlremBTWYZCkCuRASKHzfsqJSwnaABShqhCQtgLQSSnBq	-	-		0 bytes	NA
GET	https://131.100.24.231/IyfASJCANyEeMSEnpXpaRFmYWRdzZpmrrpAhUpzOSuzKLlOpcGsaP	-	-		0 bytes	NA
GET	https://131.100.24.231/IFfVBkyXLzLxTCxJwrPPZXuAVVBHDMJjLb	-	-		0 bytes	NA
GET	https://131.100.24.231/PjNtLFourlwOKpzxahYuFVlaUiWQiNRwnyBuXSyDBtQBExDgjyWUdVZ	-	-		0 bytes	NA
GET	https://131.100.24.231/pDnfUnKnkXpXuCb	-	-		0 bytes	NA
GET	https://131.100.24.231/oBplEaBijFHajEsGgFHQALCBZzOkCROZGGW	-	-		0 bytes	NA
GET	https://131.100.24.231/XUhtMukWyxGCOUtlOamIMpz	-	-		0 bytes	NA
GET	https://131.100.24.231/NnSPrKLklQWyLpDsOBvayvHYfpr	-	-		0 bytes	NA
GET	https://131.100.24.231/klYPnZCNPtrLUyNKeydGtHtlcmHBBTEEfGqcmElywqcBshQXLJTYLMwsdqzWYx	-	-		0 bytes	NA
GET	https://131.100.24.231/SaByipWEoOu	-	-		0 bytes	NA
GET	https://131.100.24.231/snlYiBNxSZRzyhECNZCAQ	-	-		0 bytes	NA
GET	https://131.100.24.231/cafEzF	-	-		0 bytes	NA
GET	https://131.100.24.231/XkEOqreeJDfpFdyRRpleVtPAyEdT	-	-		0 bytes	NA
GET	https://131.100.24.231/vRsBkRRVGMBCUOuWdZcAAAxpxQnFiBltgrlpnZYEhBJSSfFN	-	-		0 bytes	NA
GET	https://209.59.138.75/uGgpKquXhAwYVUnpJNczDqWIgfQfpTUP	-	-		0 bytes	NA
GET	https://209.59.138.75/OpDIaUbKbVKthFMeufGDyGNIcFlhcBgfRArWebvvHgyyNwCcPFJL	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	gaidov.bg	NoError	78.128.43.182		NA

BEHAVIOR

Process Graph

Process #1: excel.exe

ID	1
File Name	c:\program files (x86)\microsoft office\root\office16\excel.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64335, Reason: Analysis Target
Unmonitor End Time	End Time: 619230, Reason: Terminated
Monitor duration	554.89s
Return Code	0
PID	3132
Parent PID	912
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
..\sun.ocx	413.54 KB	a80843c86ccdbd0e03670ba1205da9a0a0acce34f78b0bf49744edf4364153db	✗
-	113.50 KB	5968b1706ddb1f6d2fa8120cd03d84f10217c0c1a71b64d3ae9bffbbbb36c4c1	✗
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
-	512 bytes	076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	✗

Host Behavior

Type	Count
File	5
Process	1

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #2: rundll32.exe

ID	2
File Name	c:\windows\syswow64\rundll32.exe
Command Line	C:\Windows\SysWow64\rundll32.exe ..\sun.ocx,D"&"l"&"lR"&"egister"&"Serve"&"r
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87931, Reason: Child Process
Unmonitor End Time	End Time: 93541, Reason: Terminated
Monitor duration	5.61s
Return Code	0
PID	3464
Parent PID	3132
Bitness	32 Bit

Host Behavior

Type	Count
System	4
Mutex	46
-	1
Module	2
Process	1

Process #3: rundll32.exe

ID	3
File Name	c:\windows\syswow64\rundll32.exe
Command Line	C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\sun.ocx",DllRegisterServer
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91464, Reason: Child Process
Unmonitor End Time	End Time: 138654, Reason: Terminated
Monitor duration	47.19s
Return Code	0
PID	3480
Parent PID	3464
Bitness	32 Bit

Host Behavior

Type	Count
System	10
Mutex	46
-	2
Module	14
-	1
File	6
Process	1

Process #5: rundll32.exe

ID	5
File Name	c:\windows\syswow64\rundll32.exe
Command Line	C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",QxrXksBkO
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120011, Reason: Child Process
Unmonitor End Time	End Time: 139998, Reason: Terminated
Monitor duration	19.99s
Return Code	0
PID	3548
Parent PID	3480
Bitness	32 Bit

Host Behavior

Type	Count
System	4
Mutex	46
-	1
Module	2
Process	1

Process #6: rundll32.exe

ID	6
File Name	c:\windows\syswow64\rundll32.exe
Command Line	C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",DllRegisterServer
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138600, Reason: Child Process
Unmonitor End Time	End Time: 674568, Reason: Terminated by Timeout
Monitor duration	535.97s
Return Code	Unknown
PID	3616
Parent PID	3548
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	59.97 KB	6b0ceccf0103afd89844761417c1d23acc41f8aebf3b7230765209b61eee5658	✗
-	157.81 KB	bdd5111162a6fa25682e18fa74e37e676d49cafcb5b7207e98e5256d1ef0d003	✗

Host Behavior

Type	Count
System	29
Mutex	48
-	22
Module	14
-	1
File	43
Registry	80

Network Behavior

Type	Count
HTTPS	40
TCP	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7443d5335a207cca176825bd774a412e72882c815206c7f59ace1feb111bb4e9	C:\Users\kEecfMwgj\Desktop\bmxixqaylqt.xls	Sample File	113.00 KB	application/vnd.ms-excel	-	MALICIOUS
5968b1706ddb1f6d2fa8120cd03d84f10217c0c1a71b64d3ae9bffbbbb36c4c1	c:\users\keecfmwgj\desktop\15eab100, c:\users\keecfmwgj\desktop\bmxixqaylqt.xls	Dropped File	113.50 KB	application/vnd.ms-excel	-	MALICIOUS
a80843c86ccdbd0e03670ba1205da9a0a0acce34f78b0bf49744edf4364153db	C:\Users\kEecfMwgj\sun.ocx, ..\sun.ocx, QKehbVshDH.dll	Downloaded File	413.54 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete	MALICIOUS
bdd5111162a6fa25682e18fa74e37e676d49cafcb5b7207e98e5256d1ef0d003	c:\users\keecfmwgj\appdata\local\temp\tar374f.tmp, authroot.stl	Embedded File	157.81 KB	application/octet-stream	-	CLEAN
076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	c:\users\keecfmwgj\appdata\local\temp\~df0e8bec461e0e10fe.tmp	Dropped File	512 bytes	application/octet-stream	-	CLEAN
6b0ceccf0103afd89844761417c1d23acc41f8aebf3b7230765209b61eee5658	c:\users\keecfmwgj\appdata\local\temp\cab374e.tmp	Downloaded File	59.97 KB	application/vnd.ms-cab-compressed	-	CLEAN
b3d17ce1ecb565498388bb5c5b19d5011a8b9034f00bd18944f01edce91049b9	0.png	Embedded File	74.02 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
..\sun.ocx	Downloaded File	Access, Create	CLEAN
C:\Users\kEecfMwgj\sun.ocx	Downloaded File	Access, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr1b36397	Accessed File	Write, Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr	Accessed File	Write, Access, Create, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://gaidov.bg/wp-includes/Ug/	-	78.128.43.182	-	GET	MALICIOUS
http://studiokrishnaproduction.com/wp-includes/3mJ/	-	-	-	GET	MALICIOUS
http://goodmarketinggroup.com/live_site/Y9cEk9QNIDUeg/	-	-	-	GET	MALICIOUS
https://131.100.24.231/sZuPkhFvxiruZGnkWSvBZJFMHwMYVGejYGd	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/cbdEcXhDUxjTynjcAbsoCaeAOPEKG	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/RShuHPCsvcntVeVPloUCMqSKmqNYvSQbjTDURzDELiTxnpAroacVpj	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/NSqcpi	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/PUxFVbubbsRiyeVOkyIFLvjttHGxWuLZOTznFZDJDRCzjBXsCm	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/byuxizdZiMBRMMyvTrfAhSUmno	-	131.100.24.231	-	GET	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://131.100.24.231/ovZMsGwuDvkCTVAuyUErEnviJRjFoYdxqzHAHCmEFowVipOJxPzHxegcyB	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/KCickUNfNVdluezRJQVzrSVrPGCcfHpSXQkeXolVLkiGTdBPKaPPgeHI	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/UUjGUHzEthTahLxeYVthAdNitVdOehJweJVinGsldtKfFTlagXDeKlobzUPVWUT	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/kIveWRCGbQlVsKDQuCjbRbxbpDmUTLRXQzstFZzYzrszPLCEuLPYdLC	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/TxNbeAQdUfkbUXFUXVRqjVQtoKYHhMYdO	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/yBEEnKhBylvRxCnDmpAEUlWSNeIXgbrnpn	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/EbNOMLpVejdDyVULeZGbPrCFGbVbsTOPkiZZgYBbxeXXphaLsDMbQSSB	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/zMyKgMZsAUAz	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/rbSYzmWbHkrHWqqeRSGSjBKgtutkPBcboXUUeGsfTKBsLvroB	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/grco	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/TstxALIFdZSCBbRVhJ	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/xdohqFznFrXzjvxKGDoJkJqvmiXGarZxxdHusoAojxyf	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/XUTJxlmFENzNsUqZvdcBnfTMraHDnrhQTVonROhDRzsJXlWfuBdHAGRSxkZD	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/hmoSo	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/MgpAtRGHvDYHHuqMjChsaHiLoRULfkGcPRoPgy	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/tKcWvnBRzZcTf	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/nogGHxUlWlbDlgLssUyF	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/mhpTspdGiezEmAKcdgBlJoesESjzILqnQX	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/rFlVerNgyrSmXUggWdlremBTWYZCkCuRASKHzfsqJSwnaABShqhCQtgLQSSnBq	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/lyfASJCANyEeMSEnpXpaRFmYWRdzZpmrrpAhUpzOSuzKLlOpcGsaP	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/IFfVBkyXLzLxTCxJwrPPZXuAVVBHDMJjLb	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/PjNtLFourlwOKpzxahYuFVlaUiWQiNRwnyBuXSyDBtQBExDgjyWUdVZ	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/pDnfUnKnkXpXuCb	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/oBplEaBijFHajEsGgFHQALCBZzOkCROZGGW	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/XUhtMukWyxGCOUtlOamIMpz	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/NnSPrKLklQWyLpDsOBvayvHYfpr	-	131.100.24.231	-	GET	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://131.100.24.231/kIYPnZCNPtrLUyNKeydGtHtlcmHBBTEEfGqcmElywqcBshQXLJTYLMwsdqzWYx	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/SaByipWEoOu	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/snlYiBNxSZRzyhECNZCAQ	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/cafEzF	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/XkEOqreeJDfpFdyRRpleVtPAyEdT	-	131.100.24.231	-	GET	MALICIOUS
https://131.100.24.231/vRsBkRRVGMBCUOuWdZcAAAxpxQnFiBltgrIpnZYEhBJSSfFN	-	131.100.24.231	-	GET	MALICIOUS
https://209.59.138.75/uGgpKquXhAwYVUnpJNczDqWIgfQfpTUP	-	209.59.138.75	-	GET	MALICIOUS
https://209.59.138.75/OpDIaUbKbVKthFMeufGDyGNIcFlhcBgfRArWebvvHgyyNwCcPFJL	-	209.59.138.75	-	GET	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
gaidov.bg	78.128.43.182	-	HTTP, DNS	CLEAN
studiokrishnaproduction.com	-	-	HTTP	CLEAN
goodmarketinggroup.com	-	-	HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
131.100.24.231	-	Brazil	TCP, TLS	MALICIOUS
209.59.138.75	-	United States	TCP, TLS	MALICIOUS
78.128.43.182	gaidov.bg	Bulgaria	TCP, HTTP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
gcc-shmem-tdm2-use_fc_key	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-sjlj_once	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-once_global_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-once_obj_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-mutex_global_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-_pthread_tls_once_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-_pthread_tls_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-mtx_pthr_locked_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-mutex_global_static_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-mxattr_recursive_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-pthr_root_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-idListCnt_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-idListMax_shmem	access	rundll32.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
gcc-shmem-tdm2-idList_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-idListNextId_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-fc_key	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-_pthread_key_lock_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-_pthread_cancelling_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-cond_locked_shmem_rwlock	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-rwl_global_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-_pthread_key_sch_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-_pthread_key_max_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-_pthread_key_dest_shmem	access	rundll32.exe	CLEAN
gcc-shmem-tdm2-pthr_last_shmem	access	rundll32.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\tfnfdhfu.kqr	write, access	rundll32.exe	SUSPICIOUS
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access, create	rundll32.exe	CLEAN

Process

Process Name	Commandline	Verdict
rundll32.exe	C:\Windows\SysWow64\rundll32.exe ..\sun.ocx,D"&"l"&"lR"&"egister"&"Serve"&"r	SUSPICIOUS
rundll32.exe	C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\sun.ocx",DllRegisterServer	SUSPICIOUS
rundll32.exe	C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",DllRegisterServer	SUSPICIOUS
excel.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE"	CLEAN
rundll32.exe	C:\Windows\SysWOW64\rundll32.exe "C:\Users\kEecfMwgj\AppData\Local\Oxeedtbi\tfnfdhfu.kqr",QxrXksBkO	CLEAN

YARA / AV

YARA (25)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetEccDecryption	Emotet ECC decryption function	Memory Dump	-	Downloader	5/5
Emotet	EmotetFunctionStrings	Emotet function strings	Function Strings	function_strings_process_6.txt	Downloader	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows