VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: SHablon_avtootveta_na_vremya_otpuska.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 81e6b7f47a69eccc488e65459feeefe90ef2643d
MD5: 7139808eeee4c7bee372ab42f370c73f
First Seen Date: 2017-08-18 01:22:15 UTC
Number of Clients Seen: 3
Last Analysis Date: 2017-08-18 01:22:15 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-08-18 01:22:15 UTC	Malware
Static Analysis Overall Verdict	2017-08-18 01:22:15 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2017-08-18 01:22:15 UTC	No Threat Found
Precise Detectors Overall Verdict	2017-08-18 01:22:15 UTC	No Match
File Certificate Validation		Vendor is Gray Listed

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Suspicious
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Clean
Timestamp value suspicious	Clean
Header Checksum is zero!	Clean
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Clean
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Creates a child process	!
Reads memory of another process	!
Writes to address space of another process	!
Uses a function clandestinely	!
Downloads data from internet	!
Modifies Windows policies	!
Opens a file in a system directory	!
Has no visible windows	!

Behavioral Information

QueryFilePath

C:\SHablon_avtootveta_na_vremya_otpuska.exe
C:\SHablon_avtootveta_na_vremya
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

CreateRegisteryKey

{"h_key": "80000001", "samDesired": "2001f", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "2b5e468", "dwOptions": "0", "lpClass": "<NULL>", "phkResult": "2b5e46c", "lpSubKey": "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"}
{"h_key": "80000001", "samDesired": "2001f", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "<NULL>", "phkResult": "368fc08", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad"}
{"h_key": "318", "samDesired": "e", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "3bcfbfc", "dwOptions": "0", "lpClass": "<NULL>", "phkResult": "3bcfc00", "lpSubKey": "{35B2A6E5-E669-426E-AFB6-1C7A607735EF}"}
{"h_key": "80000001", "samDesired": "2001f", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "<NULL>", "phkResult": "3e6fc08", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad"}
{"h_key": "80000001", "samDesired": "1", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "", "phkResult": "2b5e2e4", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections"}
{"h_key": "80000001", "samDesired": "1", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "", "phkResult": "2b5e404", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections"}
{"h_key": "80000001", "samDesired": "20006", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "", "phkResult": "2b5e404", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"}
{"h_key": "80000001", "samDesired": "2", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "", "phkResult": "2b5e3a4", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections"}
{"h_key": "80000001", "samDesired": "1", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "", "phkResult": "2b5e3e8", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections"}
{"h_key": "80000001", "samDesired": "1", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "", "phkResult": "2b5e1cc", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections"}
{"h_key": "80000001", "samDesired": "2001f", "Reserved": "0", "lpSecurityAttributes": "0", "lpdwDisposition": "0", "dwOptions": "0", "lpClass": "<NULL>", "phkResult": "3bcfc08", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad"}

RegCloseKey

26c
214
318
190
218
192
1e0
118
3a4
368
328
330
380
244
260
21c

1d0
264
220
32c
1f8
36c

LoadLibrary

API-MS-Win-Core-LocalRegistry-L1-1-0.dll
apphelp.dll
atl.dll
WININET.dll
KERNEL32.dll
USER32.dll
GDI32.dll
COMDLG32.dll
WINSPOOL.DRV
ADVAPI32.dll
SHELL32.dll
COMCTL32.dll
SHLWAPI.dll
ole32.dll
OLEAUT32.dll
oledlg.dll
gdiplus.dll
OLEACC.dll
OLEACCRC.DLL
API-MS-Win-Security-LSALookup-L1-1-0.dll
C:\SHablon_avtootveta_na_vremya_otpuskaENU.dll
C:\SHablon_avtootveta_na_vremya_otpuskaLOC.dll
SspiCli.dll
Iphlpapi.dll
Comctl32.dll
comctl32.dll
UxTheme.dll
C:\Windows\system32\ole32.dll
Secur32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
IPHLPAPI.DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll
DNSAPI.dll
dhcpcsvc.DLL
CRYPTBASE.dll
urlmon.dll
imageres.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL

ReadRegisteryKey

DnsCacheEntries
DisableKeepAlive
CacheMode
ProxyHttp1.1
NoDrives
DisableBasicOverClearChannel
DisableBranchCache
ScavengeCacheLowerBound
CertCacheNoValidate
IdnEnabled
LeashLegacyCookies
EnablePunycode
Plane16
MaxConnectionsPer1_0Server
Plane14
Plane15
Plane12
Plane13
Plane10

Plane11
MaxConnectionsPerProxy
DnsCacheTimeout
UseFirstAvailable
FrameMerging
SendTimeOut
DefaultConnectionSettings
WpadSearchAllDomains
ProxyOverride
Plane4
Plane5
Plane6
Plane7
BadProxyExpiresTime
Plane2
Plane3
HttpDefaultExpiryTimeSecs
FromCacheTimeout
Plane8
Plane9
ProxyEnable
WpadDhcp
SendExtraCRLF
DisableNTLMPreAuth
ShareCredsWithWinHttp
SocketSendBufferLength
ReceiveTimeOut
WarnOnPost
EnforceP3PValidity
WpadDecisionReason
ServerInfoTimeout
NoClose
ConnectTimeOut
AlwaysDrainOnRedirect
WarnOnZoneCrossing
DontUseDNSLoadBalancing
EnableSpdyDebugAsserts
SecureProtocols
WarnAlwaysOnPost
AutoConfigURL
WpadOverride
PreConnectLimit
SavedLegacySettings
WpadDecisionTime
MaxConnectionsPerServer
TcpAutotuning
TabProcGrowth
CreateUriCacheSize
EnableNegotiate
WarnOnBadCertRecving
EnableHttp1_1
SocketReceiveBufferLength
ClientAuthBuiltInUI
FtpDefaultExpiryTimeSecs
ScavengeCacheFileLimit
SyncMode5
CombineFalseStartData
Plane1
DnsCacheEnabled
DisableReadRange
DisableFalseStartBlocklist
ConnectRetries
SqmHttpStreamRandomUploadPoolSize
WpadDecision
WarnOnPostRedirect
WpadDetectedUrl
WpadExpirationDays
WpadDns
DisableSecuritySettingsCheck
svcVersion
Disable
RestrictRun
FrameTabWindow
MaxHttpRedirects
DataFilePath
NoRecentDocsHistory
AutoDetect

SystemSetupInProgress
AutoProxyDetectType
NoNetConnectDisconnect
SessionMerging
NoRun
ScavengeCacheFileLifeTime
FEATURE_CLIENTAUTHCERTFILTER
KeepAliveTimeout
WarnOnHTTPSToHTTPRedirect
PreResolveLimit
ProxyServer
DuoProtocols
AdminTabProcs

RegSetValue

{"Reserved": "0", "hKey": "36c", "lpData": "88c42c", "dwType": "1", "lpValueName": "WpadNetworkName", "cbData": "2a"}
{"Reserved": "0", "hKey": "368", "lpData": "760c48bc", "dwType": "1", "lpValueName": "CachePrefix", "cbData": "12"}
{"Reserved": "0", "hKey": "36c", "lpData": "3bcfcf8", "dwType": "3", "lpValueName": "WpadDecisionTime", "cbData": "8"}
{"Reserved": "0", "hKey": "260", "lpData": "2b5e400", "dwType": "4", "lpValueName": "ProxyEnable", "cbData": "4"}
{"Reserved": "0", "hKey": "368", "lpData": "76089c98", "dwType": "1", "lpValueName": "CachePrefix", "cbData": "10"}
{"Reserved": "0", "hKey": "36c", "lpData": "3bcfcf0", "dwType": "4", "lpValueName": "WpadDecision", "cbData": "4"}
{"Reserved": "0", "hKey": "36c", "lpData": "3bcfcf4", "dwType": "4", "lpValueName": "WpadDecisionReason", "cbData": "4"}
{"Reserved": "0", "hKey": "264", "lpData": "8649c8", "dwType": "3", "lpValueName": "SavedLegacySettings", "cbData": "b8"}
{"Reserved": "0", "hKey": "368", "lpData": "76086a44", "dwType": "1", "lpValueName": "CachePrefix", "cbData": "2"}

InternetDownload

0

CreateFile

{"dwCreationDisposition": "3", "path": "\\\\.\\PhysicalDrive4", "dwDesiredAccess": "0", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "\\\\.\\PhysicalDrive2", "dwDesiredAccess": "0", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "C:\\Windows\\system32\\rsaenh.dll", "dwDesiredAccess": "80000000", "dwShareMode": "1"}
{"dwCreationDisposition": "3", "path": "\\\\.\\PhysicalDrive1", "dwDesiredAccess": "0", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "\\\\.\\PhysicalDrive3", "dwDesiredAccess": "0", "dwShareMode": "3"}
{"dwCreationDisposition": "4", "path": "C:\\Users\\win7\\AppData\\Local\\Microsoft\\Windows\\Temporary Internet Files\\counters.dat", "dwDesiredAccess": "c0000000", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "\\\\.\\Nsi", "dwDesiredAccess": "0", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "\\\\.\\PhysicalDrive0", "dwDesiredAccess": "0", "dwShareMode": "3"}
{"dwCreationDisposition": "3", "path": "C:\\Windows\\Fonts\\staticcache.dat", "dwDesiredAccess": "80000000", "dwShareMode": "5"}

OpenRegisteryKey

{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_IGNORE_MAPPINGS_FOR_CREDPOLICY"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Comdlg32"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_INCLUDE_PORT_IN_SPN_KB908209"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Internet Explorer"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "RETRY_HEADERONLYPOST_ONCONNECTIONRESET"}
{"hKey": "364", "phkResult": "0", "lpSubKey": "Cookies"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\Shell\\Associations\\UrlAssociations\\http\\UserChoice"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562"}
{"hKey": "364", "phkResult": "0", "lpSubKey": "History"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Internet Explorer\\Main"}
{"hKey": "318", "phkResult": "0", "lpSubKey": "{35B2A6E5-E669-426E-AFB6-1C7A607735EF}"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\LanguagePack\\DataStore_V1.0"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Internet Explorer\\Main"}
{"hKey": "37c", "phkResult": "0", "lpSubKey": "{35B2A6E5-E669-426E-AFB6-1C7A607735EF}"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Internet Explorer"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_MIME_HANDLING"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Network"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Internet Explorer\\Main"}
{"hKey": "364", "phkResult": "0", "lpSubKey": "Content"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Policies"}

{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_USE_CNAME_FOR_SPN_KB911149"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Internet Explorer\\Main"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_HTTP_USERNAME_PASSWORD_DISABLE"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap"}
{"hKey": "20c", "phkResult": "0", "lpSubKey": "Microsoft\\Internet Explorer\\Security"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_LOCALMACHINE_LOCKDOWN"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\5.0\\Cache"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Wine"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_SCH_SEND_AUX_RECORD_KB_2618444"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Internet Explorer\\Main\\FeatureControl"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_DIGEST_NO_EXTRAS_IN_URI"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"}
{"hKey": "210", "phkResult": "0", "lpSubKey": "Microsoft\\Internet Explorer\\Security"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Policies"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Internet Explorer"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Policies\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\5.0\\Cache"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\5.0\\Cache"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915"}
{"hKey": "80000000", "phkResult": "0", "lpSubKey": "http\\shell\\open\\command"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "System\\Setup"}
{"hKey": "3a0", "phkResult": "0", "lpSubKey": "{35B2A6E5-E669-426E-AFB6-1C7A607735EF}"}
{"hKey": "35c", "phkResult": "0", "lpSubKey": "{35B2A6E5-E669-426E-AFB6-1C7A607735EF}"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_BUFFERBREAKING_818408"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\Internet Explorer\\Main\\FeatureControl"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\LanguagePack\\SurrogateFallback"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Wpad"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Wine"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "SOFTWARE\\Policies\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\5.0\\Cache"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Internet Explorer\\Main\\FeatureControl"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\5.0\\Cache"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Policies\\Microsoft\\PeerDist\\Service"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\5.0\\Cache"}
{"hKey": "80000001", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Zones\\"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\FontLink\\SystemLink"}
{"hKey": "80000002", "phkResult": "0", "lpSubKey": "Software\\Microsoft\\Windows NT\\CurrentVersion\\PeerDist\\Service"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274"}
{"hKey": "1f4", "phkResult": "0", "lpSubKey": "FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543"}
{"hKey": "1e0", "phkResult": "0", "lpSubKey": "MS Shell Dlg 2"}

CreateMutex

<NULL>
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

OpenMutex

Local\MSCTF.Asm.MutexDefault1

CreateProcess

cmd.exe /C timeout 3 > Nul & Del "C:\SHablon_avtootveta_na_vremya_otpuska.exe"

SetFilePointer

{"lDistanceToMove": "fffffc00", "dwMoveMethod": "2", "lpDistanceToMoveHigh": "0", "hFile": "3d0"}

QueryProcessAddress

SetWindowsHookExW
OpenProcess
ReadProcessMemory
CreateProcessW
InternetReadFile
ShellExecuteExW
ShellExecuteW
IsDebuggerPresent

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise Adware Prepscram 1	2017-08-18 01:20:52 UTC	No Match	No match.
Static Precise Trojan Cryptor Detector 1	2017-08-18 01:20:52 UTC	No Match	No match.
Yara Rule Static Malware Detector	2017-08-18 01:20:52 UTC	No Match	No match.
Static Precise PUA Detector 1	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise Virus Detector	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise Trojan Detector	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2017-08-18 01:20:52 UTC	No Match	No match.
Static Precise PUA Detector 3	2017-08-18 01:20:52 UTC	No Match	No match.
Static Precise Virus Hezhi Detector	2017-08-18 01:20:52 UTC	No Match	No match.
Ransomware Chunk Detector	2017-08-18 01:21:03 UTC	No Match	No match.
Static Precise Virus Detector 2	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise Trojan Detector 2	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise Adware InstallCore Detector 1	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise Trojan Generic Cryptor Detector 1	2017-08-18 01:20:52 UTC	No Match	NotDetected
Static Precise MD5 Detector	2017-08-18 01:20:53 UTC	No Match	No match.
Malicious Url Detector	2017-08-18 01:22:15 UTC	No Match	No match.

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Gray Listed

[+] OOO_MASTERKOD

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] OOO_MASTERKOD

Status	NoError ✔
Start Date	2017-07-19 00:00:00+00:00
End Date	2017-08-19 23:59:59+00:00
Sha256	c14b31ca402786ba776bc608b5b3ff32732eb9f1e7b9d2537ef261c7897102a8
Serial	00F30C4A141F0F7395181AA2D9286883D4
Subject Name	OOO_MASTERKOD
Subject Key Identifier	f4 05 50 33 4a ac e4 a0 e7 38 d3 df 94 41 08 19 a0 5a 97 f1
Subject Organization	OOO_MASTERKOD
Subject Locality	Brjansk
Subject State	RU
Subject Country	RU
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Code Signing CA

Status	NoError ✔
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Name	COMODO RSA Code Signing CA
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Subject Organization	COMODO CA Limited
Subject Locality	Salford
Subject State	Greater Manchester
Subject Country	GB
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Certification Authority

Status	NoError ✔
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Name	COMODO RSA Certification Authority
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Subject Organization	COMODO CA Limited
Subject Locality	Salford
Subject State	Greater Manchester
Subject Country	GB
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Issuer Organization	COMODO CA Limited
Issuer Locality	Salford
Issuer State	Greater Manchester
Issuer Country	GB
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x57B15134 [Mon Aug 15 05:20:52 2016 UTC]
Entry Point	0x5c39b6 (.text)
File Size	2261952
File Type Enum	6
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	f51fa35e944db63d7d588d4e48c0664804534db15b0345d7c71451aaa3771668

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1c523e	0x1c6000	4.75090997643	e175af89560b33469d20765fde084e28
.data	0x1c7000	0x326ce	0x33000	0.287295651761	30db0ddb50fc141a2c62f56eeb908644
f54ed	0x1fa000	0x8	0x1000	0.0	620f0b67a91f7f74151bc5be745b7110
.rsrc	0x1fb000	0x2c000	0x2c000	5.43317938745	2c6bda0fdd87e8d2b53ba831222b6b34