win764_Cridex Report

Case Overview

Victim System was infected

Case Acquisition

Test Message

Case Findings

It was confirmed that the system was attacked, claim is supported by the artifacts found

Case Conclusion

System is infected with Trojan

Artifacts

process_list

---

comment: --MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --

name: KB00510801.exe
physical_offset: 2106657392
pid: 1820
marked: disabled
object_id: 19
unlinked: No
ppid: 1188

---

comment: --Avira: TR/Crypt.XPACK.Gen5 -- VBA32: BScope.Trojan.Reconyc -- CrowdStrike: malicious_confidence_100% (D) --

name: GoogleUpdate.e
physical_offset: 2141301552
pid: 2876
marked: disabled
object_id: 47
unlinked: No
ppid: 2016
---

comment: --Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9590 -- CrowdStrike: malicious_confidence_90% (W) --

name: powershell.exe
physical_offset: 2141608752
pid: 1888
marked: disabled
object_id: 53
unlinked: No
ppid: 1164
---

comment: --Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --

name: sppsvc.exe
physical_offset: 2142500656
pid: 2416
marked: disabled
object_id: 55
unlinked: No
ppid: 472
---

comment: Possible Threat

name: First Data Cor
physical_offset: 2144391264
pid: 2532
marked: disabled
object_id: 59
unlinked: No
ppid: 1848
---

dll_object_list

---

comment: DLLs linked to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: KB00510801.exe
physical_offset: 1890404112
pid: 1820
marked: disabled
object_id: 220
load_count: 65535
dll_base: 16715776
size_of_image: 184320
full_dll_name: C:/Users/Ryuzaki/AppData/Roaming/KB00510801.exe

---

comment: DLLs linked to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: ntdll.dll
physical_offset: 1890404352
pid: 1820
marked: disabled
object_id: 221
load_count: 65535
dll_base: 713023488
size_of_image: 1740800
full_dll_name: C:/Windows/SYSTEM32/ntdll.dll

---

comment: DLLs linked to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike:

malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: wow64.dll
physical_offset: 1890405808
pid: 1820
marked: disabled
object_id: 222
load_count: 3
dll_base: 172462080
size_of_image: 258048
full_dll_name: C:/Windows/SYSTEM32/wow64.dll
---

comment: DLLs linked to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: wow64win.dll
physical_offset: 1890406256
pid: 1820
marked: disabled
object_id: 223
load_count: 1
dll_base: 1956696064
size_of_image: 376832
full_dll_name: C:/Windows/SYSTEM32/wow64win.dll
---

comment: DLLs linked to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: wow64cpu.dll

physical_offset: 1890405424
pid: 1820
marked: disabled
object_id: 224
load_count: 1
dll_base: 1955196928
size_of_image: 32768
full_dll_name: C:/Windows/SYSTEM32/wow64cpu.dll
---

comment: DLLs linked to malicious process (--Avira: TR/Crypt.XPACK.Gen5 -- VBA32: BScope.Trojan.Reconyc -- CrowdStrike: malicious_confidence_100% (D) --)

name: GoogleUpdate.exe
physical_offset: 1582106352
pid: 2876
marked: disabled
object_id: 1504
load_count: 65535
dll_base: 248508416
size_of_image: 163840
full_dll_name: C:/Program Files (x86)/Google/Update/GoogleUpdate.exe
---

comment: DLLs linked to malicious process (--Avira: TR/Crypt.XPACK.Gen5 -- VBA32: BScope.Trojan.Reconyc -- CrowdStrike: malicious_confidence_100% (D) --)

name: ntdll.dll
physical_offset: 1582106592
pid: 2876
marked: disabled
object_id: 1505
load_count: 65535
dll_base: 713023488
size_of_image: 1740800
full_dll_name: C:/Windows/SYSTEM32/ntdll.dll
---

comment: DLLs linked to malicious process (--Avira: TR/Crypt.XPACK.Gen5 -- VBA32: BScope.Trojan.Reconyc -- CrowdStrike: malicious_confidence_100% (D) --)

name: wow64.dll
physical_offset: 1582108048
pid: 2876

marked: disabled
object_id: 1506
load_count: 3
dll_base: 172462080
size_of_image: 258048
full_dll_name: C:/Windows/SYSTEM32/wow64.dll
---

comment: DLLs linked to malicious process (--Avira: TR/Crypt.XPACK.Gen5 -- VBA32: BScope.Trojan.Reconyc -- CrowdStrike: malicious_confidence_100% (D) --)

name: wow64win.dll
physical_offset: 1582108496
pid: 2876
marked: disabled
object_id: 1507
load_count: 1
dll_base: 1956696064
size_of_image: 376832
full_dll_name: C:/Windows/SYSTEM32/wow64win.dll
---

comment: DLLs linked to malicious process (--Avira: TR/Crypt.XPACK.Gen5 -- VBA32: BScope.Trojan.Reconyc -- CrowdStrike: malicious_confidence_100% (D) --)

name: wow64cpu.dll
physical_offset: 1582107664
pid: 2876
marked: disabled
object_id: 1508
load_count: 1
dll_base: 1955196928
size_of_image: 32768
full_dll_name: C:/Windows/SYSTEM32/wow64cpu.dll
---

comment: DLLs linked to malicious process (--Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9590 -- CrowdStrike: malicious_confidence_90% (W) --)

name: powershell.exe
physical_offset: 1770682624
pid: 1888
marked: disabled

object_id: 1685
load_count: 65535
dll_base: 1594425344
size_of_image: 466944
full_dll_name: C:/Windows/SysWow64/WindowsPowerShell/v1.0/powershell.exe
---

comment: DLLs linked to malicious process (--Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9590 -- CrowdStrike: malicious_confidence_90% (W) --)

name: ntdll.dll
physical_offset: 1770682864
pid: 1888
marked: disabled
object_id: 1686
load_count: 65535
dll_base: 713023488
size_of_image: 1740800
full_dll_name: C:/Windows/SYSTEM32/ntdll.dll
---

comment: DLLs linked to malicious process (--Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9590 -- CrowdStrike: malicious_confidence_90% (W) --)

name: HD+'$
physical_offset: 1770684320
pid: 1888
marked: disabled
object_id: 1687
load_count: 24936
dll_base: 172462080
size_of_image: 258048
full_dll_name: C:/Windows/SYSTEM32/wow64.dll
---

comment: DLLs linked to malicious process (--Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9590 -- CrowdStrike: malicious_confidence_90% (W) --)

name: wow64win.dll
physical_offset: 1770683888
pid: 1888

marked: disabled
object_id: 1688
load_count: 1
dll_base: 1956696064
size_of_image: 376832
full_dll_name: C:/Windows/SYSTEM32/wow64win.dll
---

comment: DLLs linked to malicious process (--Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9590 -- CrowdStrike: malicious_confidence_90% (W) --)

name: wow64cpu.dll
physical_offset: 1768596320
pid: 1888
marked: disabled
object_id: 1689
load_count: 1
dll_base: 1955196928
size_of_image: 32768
full_dll_name: C:/Windows/SYSTEM32/wow64cpu.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: sppsvc.exe
physical_offset: 1491261008
pid: 2416
marked: disabled
object_id: 1740
load_count: 65535
dll_base: 1510887424
size_of_image: 3534848
full_dll_name: C:/Windows/system32/sppsvc.exe
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: ntdll.dll
physical_offset: 1491261248
pid: 2416
marked: disabled

object_id: 1741
load_count: 65535
dll_base: 713023488
size_of_image: 1740800
full_dll_name: C:/Windows/SYSTEM32/ntdll.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: kernel32.dll
physical_offset: 1491262144
pid: 2416
marked: disabled
object_id: 1742
load_count: 65535
dll_base: 590532608
size_of_image: 1175552
full_dll_name: C:/Windows/system32/kernel32.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: KERNELBASE.dll
physical_offset: 1491262512
pid: 2416
marked: disabled
object_id: 1743
load_count: 65535
dll_base: 591392768
size_of_image: 438272
full_dll_name: C:/Windows/system32/KERNELBASE.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: ADVAPI32.dll
physical_offset: 1510197600
pid: 2416
marked: disabled
object_id: 1744
load_count: 65535

dll_base: 583405568
size_of_image: 897024
full_dll_name: C:/Windows/system32/ADVAPI32.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: msvcrt.dll
physical_offset: 1510197920
pid: 2416
marked: disabled
object_id: 1745
load_count: 65535
dll_base: 593715200
size_of_image: 651264
full_dll_name: C:/Windows/system32/msvcrt.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: sechost.dll
physical_offset: 1510199088
pid: 2416
marked: disabled
object_id: 1746
load_count: 65535
dll_base: 592363520
size_of_image: 126976
full_dll_name: C:/Windows/SYSTEM32/sechost.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: RPCRT4.dll
physical_offset: 1295790112
pid: 2416
marked: disabled
object_id: 1747
load_count: 65535
dll_base: 540835840
size_of_image: 1232896

full_dll_name: C:/Windows/system32/RPCRT4.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: ole32.dll
physical_offset: 1304791664
pid: 2416
marked: disabled
object_id: 1748
load_count: 65535
dll_base: 591908864
size_of_image: 2109440
full_dll_name: C:/Windows/system32/ole32.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: GDI32.dll
physical_offset: 1304791984
pid: 2416
marked: disabled
object_id: 1749
load_count: 65535
dll_base: 588156928
size_of_image: 421888
full_dll_name: C:/Windows/system32/GDI32.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: USER32.dll
physical_offset: 1304792304
pid: 2416
marked: disabled
object_id: 1750
load_count: 65535
dll_base: 541601792
size_of_image: 1024000
full_dll_name: C:/Windows/system32/USER32.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: LPK.dll
physical_offset: 1304792544
pid: 2416
marked: disabled
object_id: 1751
load_count: 65535
dll_base: 554225664
size_of_image: 57344
full_dll_name: C:/Windows/system32/LPK.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: USP10.dll
physical_offset: 1304792864
pid: 2416
marked: disabled
object_id: 1752
load_count: 65535
dll_base: 538746880
size_of_image: 823296
full_dll_name: C:/Windows/system32/USP10.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: IMM32.DLL
physical_offset: 1299979392
pid: 2416
marked: disabled
object_id: 1753
load_count: 2
dll_base: 538529792
size_of_image: 188416
full_dll_name: C:/Windows/system32/IMM32.DLL
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: MSCTF.dll
physical_offset: 1299978832
pid: 2416
marked: disabled
object_id: 1754
load_count: 1
dll_base: 540389376
size_of_image: 1085440
full_dll_name: C:/Windows/system32/MSCTF.dll
---

comment: DLLs linked to malicious process (--Cylance: Unsafe -- CrowdStrike: malicious_confidence_60% (W) --)

name: CRYPTBASE.dll
physical_offset: 1514620032
pid: 2416
marked: disabled
object_id: 1755
load_count: 1
dll_base: 468566016
size_of_image: 61440
full_dll_name: C:/Windows/syste
---

comment: DLLs linked to malicious process (Possible Threat)

name: First Data Corp.exe
physical_offset: 2013997072
pid: 2532
marked: disabled
object_id: 1985
load_count: 65535
dll_base: 120180736
size_of_image: 253952
full_dll_name: C:/Users/Ryuzaki/AppData/Local/Temp/First Data Corp/First Data Corp.exe
---

comment: DLLs linked to malicious process (Possible Threat)

name: ntdll.dll
physical_offset: 2013997312
pid: 2532

marked: disabled
object_id: 1986
load_count: 65535
dll_base: 713023488
size_of_image: 1740800
full_dll_name: C:/Windows/SYSTEM32/ntdll.dll
---

comment: DLLs linked to malicious process (Possible Threat)

name: wow64.dll
physical_offset: 2013998768
pid: 2532
marked: disabled
object_id: 1987
load_count: 3
dll_base: 172462080
size_of_image: 258048
full_dll_name: C:/Windows/SYSTEM32/wow64.dll
---

comment: DLLs linked to malicious process (Possible Threat)

name: wow64win.dll
physical_offset: 2013998288
pid: 2532
marked: disabled
object_id: 1988
load_count: 1
dll_base: 1956696064
size_of_image: 376832
full_dll_name: C:/Windows/SYSTEM32/wow64win.dll
---

comment: DLLs linked to malicious process (Possible Threat)

name: wow64cpu.dll
physical_offset: 2019783328
pid: 2532
marked: disabled
object_id: 1989
load_count: 1
dll_base: 1955196928
size_of_image: 32768

full_dll_name: C:/Windows/SYSTEM32/wow64cpu.dll
---

phandle_list

---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: N.A.
pid: 1820
physical_offset: 2111456848
marked: disabled
object_id: 17239
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: M0000071C
pid: 1820
physical_offset: 2106317472
marked: disabled
object_id: 17273
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus:

Trojan.Win32.Necurs.euhjay --)

name: I0000071C
pid: 1820
physical_offset: 2106317664
marked: disabled
object_id: 17274
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: _!MSFTHISTORY!_
pid: 1820
physical_offset: 2122554896
marked: disabled
object_id: 17317
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: c:!users!ryuzaki!appdata!local!microsoft!windows!temporary internet files!content.ie5!
pid: 1820
physical_offset: 2122555088
marked: disabled
object_id: 17318
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: M0000071C
pid: 1820
physical_offset: 2106317472
marked: disabled
object_id: 17333
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: I0000071C
pid: 1820
physical_offset: 2106317664
marked: disabled
object_id: 17334
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: c:!users!ryuzaki!appdata!roaming!microsoft!windows!cookies!
pid: 1820
physical_offset: 2124251024
marked: disabled

object_id: 17338
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: c:!users!ryuzaki!appdata!local!microsoft!windows!history!history.ie5!
pid: 1820
physical_offset: 2107020784
marked: disabled
object_id: 17341
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: WininetStartupMutex
pid: 1820
physical_offset: 2107020976
marked: disabled
object_id: 17346
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: WininetConnectionMutex
pid: 1820
physical_offset: 2106926176
marked: disabled
object_id: 17358
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: WininetProxyRegistryMutex
pid: 1820
physical_offset: 2106316272
marked: disabled
object_id: 17359
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: RasPbFile
pid: 1820
physical_offset: 2106316080
marked: disabled
object_id: 17361
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus:

P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: N.A.
pid: 1820
physical_offset: 2106074448
marked: disabled
object_id: 17399
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: N.A.
pid: 1820
physical_offset: 2106921008
marked: disabled
object_id: 17401
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: ZonesCounterMutex
pid: 1820
physical_offset: 2108913504
marked: disabled
object_id: 17453
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: ZoneAttributeCacheCounterMutex
pid: 1820
physical_offset: 2108913056
marked: disabled
object_id: 17461
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: ZonesCacheCounterMutex
pid: 1820
physical_offset: 2109822784
marked: disabled
object_id: 17463
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: ZoneAttributeCacheCounterMutex
pid: 1820
physical_offset: 2108913056
marked: disabled

object_id: 17464
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: ZonesLockedCacheCounterMutex
pid: 1820
physical_offset: 2109822592
marked: disabled
object_id: 17467
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: !IETld!Mutex
pid: 1820
physical_offset: 2112910528
marked: disabled
object_id: 17468
type: Mutant
---

comment: Handles (Mutants) related to malicious process (--MicroWorld-eScan: Gen:Trojan.Heur.GZ.dqW@b0MCmAj -- CAT-QuickHeal: Trojan.Dapato.13729 -- McAfee: GenericRXBV-NG!E00B2ABB7DEB -- Cylance: Unsafe -- CrowdStrike: malicious_confidence_100% (W) -- K7GW: P2PWorm (002e17181) -- K7AntiVirus: P2PWorm (002e17181) -- Invincea: heuristic -- Baidu: Win32.Trojan.WisdomEyes.16070401.9500.9997 -- NANO-Antivirus: Trojan.Win32.Necurs.euhjay --)

name: c:!users!ryuzaki!appdata!roaming!microsoft!windows!ietldcache!
pid: 1820
physical_offset: 2111773728
marked: disabled
object_id: 17469
type: Mutant
---

service_list

---

registry_list

---

kernel_list

---

network_list

---

comment: Network connection related to malicious process (Possible Threat)

foreign_domain:
pid: 2532
physical_offset: 2106252992
marked: disabled
object_id: 32154
local_address: 0:0:0:0:0:0
protocol_version: UDPv6
owner_process: First Data Cor
foreign_address:
port: 0
---

comment: Network connection related to malicious process (Possible Threat)

foreign_domain: a104-96-239-24.deploy.static.akamaitechnologies.com
pid: 2532
physical_offset: 2106561360
marked: disabled
object_id: 32156
local_address: 120.96.239.24:0
protocol_version: TCPv4
owner_process: First Data Cor

foreign_address: 104.96.239.24:0
port: 0
---

comment: Network connection related to malicious process (Possible Threat)

foreign_domain: a104-96-239-24.deploy.static.akamaitechnologies.com
pid: 2532
physical_offset: 2108576576
marked: disabled
object_id: 32163
local_address: 120.96.239.24:0
protocol_version: TCPv4
owner_process: First Data Cor
foreign_address: 104.96.239.24:0
port: 0
---

comment: Network connection related to malicious process (--Avira: TR/Crypt.XPACK.Gen5 -- VBA32: BScope.Trojan.Reconyc -- CrowdStrike: malicious_confidence_100% (D) --)

foreign_domain: bom07s18-in-f14.1e100.net
pid: 2876
physical_offset: 2142774784
marked: disabled
object_id: 32241
local_address: 0.0.0.0:5056
protocol_version: TCPv4
owner_process: GoogleUpdate.e
foreign_address: 172.217.166.46:47873
port: 5056
---

comment: Network connection related to malicious process (Possible Threat)

foreign_domain: abelohost-124.94.217.185.dedicated-ip.abelons.com
pid: 2532
physical_offset: 2144325648
marked: disabled
object_id: 32246
local_address: 0.0.0.0:4032
protocol_version: TCPv4
owner_process: First Data Cor
foreign_address: 185.217.94.124:20480

port: 4032
---

comment: Network connection related to malicious process (Possible Threat)

foreign_domain:
pid: 2532
physical_offset: 2144650304
marked: disabled
object_id: 32247
local_address: 0.0.0.0
protocol_version: UDPv4
owner_process: First Data Cor
foreign_address:
port: 0
---

comment: Network connection related to malicious process (Possible Threat)

foreign_domain:
pid: 2532
physical_offset: 2144767680
marked: disabled
object_id: 32248
local_address: 0.0.0.0
protocol_version: UDPv4
owner_process: First Data Cor
foreign_address:
port: 0
---

comment: Network connection related to malicious process (Possible Threat)

foreign_domain:
pid: 2532
physical_offset: 2144783056
marked: disabled
object_id: 32249
local_address: 0:0:0:0:0:0
protocol_version: UDPv6
owner_process: First Data Cor
foreign_address:
port: 0
