win764\_Cridex Report

## Case Overview

## Case Acquisition

## Case Findings

## Case Conclusion

## 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: Possibly malicious  
 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 (Possibly malicious)  
 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 (Possibly malicious)  
 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 (Possibly malicious)  
 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 (Possibly malicious)  
 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 (Possibly malicious)  
 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 (Possibly malicious)  
 object\_id: 32154  
 pid: 2532  
 physical\_offset: 2106252992  
 marked: disabled  
 foreign\_address:   
 protocol\_version: UDPv6  
 local\_address: 0:0:0:0:0:0  
 owner\_process: First Data Cor  
 port: 0

comment: Network connection related to malicious process (Possibly malicious)  
 object\_id: 32156  
 pid: 2532  
 physical\_offset: 2106561360  
 marked: disabled  
 foreign\_address: 104.96.239.24:0  
 protocol\_version: TCPv4  
 local\_address: 120.96.239.24:0  
 owner\_process: First Data Cor  
 port: 0

comment: Network connection related to malicious process (Possibly malicious)  
 object\_id: 32163  
 pid: 2532  
 physical\_offset: 2108576576  
 marked: disabled  
 foreign\_address: 104.96.239.24:0  
 protocol\_version: TCPv4  
 local\_address: 120.96.239.24:0  
 owner\_process: First Data Cor  
 port: 0

comment: Network connection related to malicious process (Avira: TR/Crypt.XPACK.Gen5 - VBA32: BScope.Trojan.Reconyc - CrowdStrike: malicious\_confidence\_100% (D) - )  
 object\_id: 32241  
 pid: 2876  
 physical\_offset: 2142774784  
 marked: disabled  
 foreign\_address: 172.217.166.46:47873  
 protocol\_version: TCPv4  
 local\_address: 0.0.0.0:5056  
 owner\_process: GoogleUpdate.e  
 port: 5056

comment: Network connection related to malicious process (Possibly malicious)  
 object\_id: 32246  
 pid: 2532  
 physical\_offset: 2144325648  
 marked: disabled  
 foreign\_address: 185.217.94.124:20480  
 protocol\_version: TCPv4  
 local\_address: 0.0.0.0:4032  
 owner\_process: First Data Cor  
 port: 4032

comment: Network connection related to malicious process (Possibly malicious)  
 object\_id: 32247  
 pid: 2532  
 physical\_offset: 2144650304  
 marked: disabled  
 foreign\_address:   
 protocol\_version: UDPv4  
 local\_address: 0.0.0.0  
 owner\_process: First Data Cor  
 port: 0

comment: Network connection related to malicious process (Possibly malicious)  
 object\_id: 32248  
 pid: 2532  
 physical\_offset: 2144767680  
 marked: disabled  
 foreign\_address:   
 protocol\_version: UDPv4  
 local\_address: 0.0.0.0  
 owner\_process: First Data Cor  
 port: 0

comment: Network connection related to malicious process (Possibly malicious)  
 object\_id: 32249  
 pid: 2532  
 physical\_offset: 2144783056  
 marked: disabled  
 foreign\_address:   
 protocol\_version: UDPv6  
 local\_address: 0:0:0:0:0:0  
 owner\_process: First Data Cor  
 port: 0