Orangeworm: Indicators of Compromise

Sample dropper hashes

MD5 hash	File directory	File name
0240ed7e45567f606793dafaff024acf	%WINDOWS%\SysWOW64	wmipsrvce.exe
047f70dbac6cd9a4d07abef606d89fb7	%WINDOWS%\system32	wmiapsrvce.exe
0240ed7e45567f606793dafaff024acf	%WINDOWS%\system32	WMIAPSRVUX.EXE
2ae53de1a1f65a6d57e96dab26c73cda	%WINDOWS%\system32	wmiapsrve.exe
47345640c135bd00d9f2969fabb4c9fa	%WINDOWS%\system32	WMIPSVRCE.EXE
cb9954509dc82e6bbed2aee202d88415	%WINDOWS%\system32	wmipsrvce.exe
cb9954509dc82e6bbed2aee202d88415	%WINDOWS%\system32	WMIPSVRE.EXE
b680b119643876286030c4f6134dc4e3	%WINDOWS%\system32	wmiapsrve.exe
fac94bc2dcfbef7c3b248927cb5abf6d	%WINDOWS%\system32	wmipvsre.exe
856683aee9687f6fdf00cfd4dc4c2aef	%WINDOWS%\system32	wmiapsvrce.exe
847459c8379250d8be2b2d365be877f5	%WINDOWS%\system32	wmiapsrve.exe
fac94bc2dcfbef7c3b248927cb5abf6d	%WINDOWS%\system32	WMIAPSRVE.EXE
fac94bc2dcfbef7c3b248927cb5abf6d	%WINDOWS%\system32	WMIPRVSE.EXE
cb9954509dc82e6bbed2aee202d88415	%WINDOWS%\system32	WMIPVSRE.EXE
6277e675d335fd69a3ff13a465f6b0a8	%WINDOWS%\system32	wmipsrvce.exe
847459c8379250d8be2b2d365be877f5	%WINDOWS%\system32	wmiapsvre.exe
3bedc1c4c1023c141c2f977e846c476e	%WINDOWS%\System32	wmipsvrce.exe
ce3894ee6f3c2c2c828148f7f779aafe	%WINDOWS%\system32	WMIAPVSRE.EXE
3b3a1062689ffa191e58d5507d39939d	%WINDOWS%\system32	wmiaprvse.exe
47345640c135bd00d9f2969fabb4c9fa	%WINDOWS%\system32	WMIAPSVRE.EXE
3bedc1c4c1023c141c2f977e846c476e	%WINDOWS%\system32	wmiapvsre.exe
6277e675d335fd69a3ff13a465f6b0a8	%WINDOWS%\System32	wmiapsrve.exe
856683aee9687f6fdf00cfd4dc4c2aef	%WINDOWS%\system32	wmipsvrce.exe
cb9954509dc82e6bbed2aee202d88415	%WINDOWS%\system32	wmipsvrce.exe
fac94bc2dcfbef7c3b248927cb5abf6d	%WINDOWS%\System32	wmipsrvce.exe
847459c8379250d8be2b2d365be877f5	%WINDOWS%\system32	WMIPRVSE.EXE
cb9954509dc82e6bbed2aee202d88415	%WINDOWS%\system32	wmiapsrvcx.exe
856683aee9687f6fdf00cfd4dc4c2aef	%WINDOWS%\System32	wmiapsrvce.exe
cb9954509dc82e6bbed2aee202d88415	%WINDOWS%\System32	wmiprvse.exe
7e5f76c7b5bf606b0fdc17f4ba75de03	%WINDOWS%\system32	wmiapsvrce.exe
177bece20ba6cc644134709a391c4a98	%WINDOWS%\system32	wmiapsrvex.exe
fac94bc2dcfbef7c3b248927cb5abf6d	%WINDOWS%\system32	wmiaprvse.exe
fac94bc2dcfbef7c3b248927cb5abf6d	%WINDOWS%\system32	wmipsvre.exe
3b3a1062689ffa191e58d5507d39939d	%WINDOWS%\system32	wmiapsrvex.exe
b59e4942f7c68c584a35d59e32adce3a	%WINDOWS%\system32	wmiapsrve.exe
81e61e5f44a6a476983e7a90bdac6a55	%WINDOWS%\system32	WMIAPSRVCX.EXE

Sample payload DLL hashes

MD5 hash	File directory	File name
ec968325394f3e6821bf90fda321e09b	%WINDOWS%\system32	WMIAMGMT.DLL
01cf05a07af57a7aafd0ad225a6fd300	%WINDOWS%\system32	WMIASSN.DLL
d57df638c7befd7897c9013e90b678f0	%WINDOWS%\system32	wmiamgmt.dll
5c3499acfe0ad7563b367fbf7fb2928c	%WINDOWS%\syswow64	wmipadp.dll
4b91ec8f5d4a008dd1da723748a633b6	%WINDOWS%\system32	wmipadp.dll
134846465b8c3f136ace0f2a6f15e534	%WINDOWS%\system32	wmiassn.dll
9d2cb9d8e73fd879660d9390ba7de263	%WINDOWS%\system32	WMIPDPA.DLL
939e76888bdeb628405e1b8be963273c	%WINDOWS%\system32	wmiadrv.dll
de9b01a725d4f19da1c1470cf7a948ee	%WINDOWS%\system32	wmipdpa.dll
bb939a868021db963916cc0118aab8ee	%WINDOWS%\system32	wmipadp.dll
3289c9a1b534a19925a14a8f7c39187c	%WINDOWS%\system32	wmiadrv.dll
9d3839b39d699336993df1dd4501892b	%WINDOWS%\system32	wmipdpa.dll
5c3499acfe0ad7563b367fbf7fb2928c	%WINDOWS%\system32	wmipadp.dll
fece72bd41cb0e06e05a847838fbde56	%WINDOWS%\system32	wmiassn.dll
bbd9e4204514c66c1babda178c01c213	%WINDOWS%\system32	wmiadrv.dll
ee4206cf4227661d3e7ec846f0d69a43	%WINDOWS%\system32	wmipadp.dll
290d8e8524e57783e8cc1b9a3445dfe9	%WINDOWS%\system32\	wmiamgmt.dll

Sample C&Cs

Remote IP address	URL
65.116.107.24	hxxp://65.116.107.24/login/login.php?q=kt[REDACTED_BASE64_STRING]==
13.44.61.126	hxxp://13.44.61.126/main/indexmain.php?q=KT[REDACTED_BASE64_STRING]==
56.28.111.63	hxxp://56.28.111.63/group/group/defaultmain.php?q=KT[REDACTED_BASE64_STRING]==
118.71.138.69	hxxp://118.71.138.69/new/main/default.php?q=KT[REDACTED_BASE64_STRING]==
117.32.65.101	hxxp://117.32.65.101/users/login.php?q=kt[REDACTED_BASE64_STRING]==
18.25.62.70	hxxp://18.25.62.70/groupgroup/default.php?q=kt[REDACTED_BASE64_STRING]==
92.137.43.17	hxxp://92.137.43.17/group/group/home/login/home.php?q=KT[REDACTED_BASE64_STRING]==
33.25.72.21	hxxp://33.25.72.21/group/main.asp?q=KT[REDACTED_BASE64_STRING]==
16.48.37.37	hxxp://16.48.37.37/groupusers/default.php?q=kt[REDACTED_BASE64_STRING]==
91.29.51.11	hxxp://91.29.51.11/default/main.php?q=KT[REDACTED_BASE64_STRING]==

Sample configuration file names

File path	Description
%WINDOWS%\inf\mkdiawb3.PNF	File contains a list of MD5 hashes of encoded modules downloaded by Trojan.Kwampirs
%WINDOWS%\inf\mtmndkb32.PNF	Last modified timestamp is used to control frequency in which Trojan.Kwampirs attempts to communicate with the C&C infrastructure

%WINDOWS%\inf\digirps.PNF	Contains encrypted system information (e.g. MAC address)
%WINDOWS%\inf\e11.PNF	Used to determine read/write permissions on remote machine

Yara signature

```
rule Kwampirs
{
    meta:
        copyright = "Symantec"
        family = "Kwampirs"
        description = "Kwampirs dropper and main payload components"

    strings:
        $pubkey =
        {
            06 02 00 00 00 A4 00 00 52 53 41 31 00 08 00 00
            01 00 01 00 CD 74 15 BC 47 7E 0A 5E E4 35 22 A5
            97 0C 65 BE E0 33 22 F2 94 9D F5 40 97 3C 53 F9
            E4 7E DD 67 CF 5F 0A 5E F4 AD C9 CF 27 D3 E6 31
            48 B8 00 32 1D BE 87 10 89 DA 8B 2F 21 B4 5D 0A
            CD 43 D7 B4 75 C9 19 FE CC 88 4A 7B E9 1D 8C 11
            56 A6 A7 21 D8 C6 82 94 C1 66 11 08 E6 99 2C 33
            02 E2 3A 50 EA 58 D2 A7 36 EE 5A D6 8F 5D 5D D2
            9E 04 24 4A CE 4C B6 91 C0 7A C9 5C E7 5F 51 28
            4C 72 E1 60 AB 76 73 30 66 18 BE EC F3 99 5E 4B
            4F 59 F5 56 AD 65 75 2B 8F 14 0C 0D 27 97 12 71
            6B 49 08 84 61 1D 03 BA A5 42 92 F9 13 33 57 D9
            59 B3 E4 05 F9 12 23 08 B3 50 9A DA 6E 79 02 36
            EE CE 6D F3 7F 8B C9 BE 6A 7E BE 8F 85 B8 AA 82
            C6 1E 14 C6 1A 28 29 59 C2 22 71 44 52 05 E5 E6
            FE 58 80 6E D4 95 2D 57 CB 99 34 61 E9 E9 B3 3D
            90 DC 6C 26 5D 70 B4 78 F9 5E C9 7D 59 10 61 DF
            F7 E4 0C B3
        }

        $network_xor_key =
        {
            B7 E9 F9 2D F8 3E 18 57 B9 18 2B 1F 5F D9 A5 38
            C8 E7 67 E9 C6 62 9C 50 4E 8D 00 A6 59 F8 72 E0
            91 42 FF 18 A6 D1 81 F2 2B C8 29 EB B9 87 6F 58
            C2 C9 8E 75 3F 71 ED 07 D0 AC CE 28 A1 E7 B5 68
            CD CF F1 D8 2B 26 5C 31 1E BC 52 7C 23 6C 3E 6B
            8A 24 61 0A 17 6C E2 BB 1D 11 3B 79 E0 29 75 02
            D9 25 31 5F 95 E7 28 28 26 2B 31 EC 4D B3 49 D9
            62 F0 3E D4 89 E4 CC F8 02 41 CC 25 15 6E 63 1B
            10 3B 60 32 1C 0D 5B FA 52 DA 39 DF D1 42 1E 3E
            BD BC 17 A5 96 D9 43 73 3C 09 7F D2 C6 D4 29 83
            3E 44 44 6C 97 85 9E 7B F0 EE 32 C3 11 41 A3 6B
            A9 27 F4 A3 FB 2B 27 2B B6 A6 AF 6B 39 63 2D 91
            75 AE 83 2E 1E F8 5F B5 65 ED B3 40 EA 2A 36 2C
            A6 CF 8E 4A 4A 3E 10 6C 9D 28 49 66 35 83 30 E7
            45 0E 05 ED 69 8D CF C5 40 50 B1 AA 13 74 33 0F
            DF 41 82 3B 1A 79 DC 3B 9D C3 BD EA B1 3E 04 33
        }

        $decrypt_string =
        {
            85 DB 75 09 85 F6 74 05 89 1E B0 01 C3 85 FF 74
            4F F6 C3 01 75 4A 85 F6 74 46 8B C3 D1 E8 33 C9
            40 BA 02 00 00 00 F7 E2 0F 90 C1 F7 D9 0B C8 51
            E8 12 28 00 00 89 06 8B C8 83 C4 04 33 C0 85 DB
            74 16 8B D0 83 E2 0F 8A 92 1C 33 02 10 32 14 38
            40 88 11 41 3B C3 72 EA 66 C7 01 00 00 B0 01 C3
            32 C0 C3
        }

        $init_strings =
        {
            55 8B EC 83 EC 10 33 C9 B8 0D 00 00 00 BA 02 00
            00 00 F7 E2 0F 90 C1 53 56 57 F7 D9 0B C8 51 E8
            B3 27 00 00 BF 05 00 00 00 8D 77 FE BB 4A 35 02
            10 2B DE 89 5D F4 BA 48 35 02 10 4A BB 4C 35 02
            10 83 C4 04 2B DF A3 C8 FC 03 10 C7 45 FC 00 00
            00 00 8D 4F FC 89 55 F8 89 5D F0 EB 06
        }

    condition:
        2 of them
}
```