

Project TajMahal – a sophisticated new APT framework

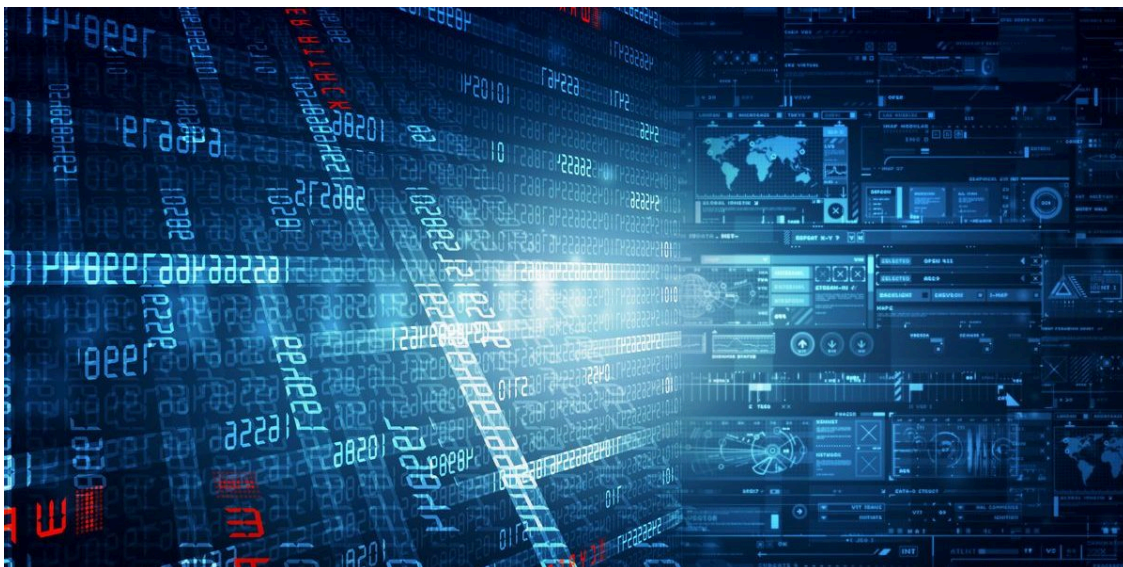
By AMR

Published: 2019-04-10 · Archived: 2026-04-05 14:43:49 UTC



10 Apr 2019

5 minute read



Executive summary

‘TajMahal’ is a previously unknown and technically sophisticated APT framework discovered by Kaspersky Lab in the autumn of 2018. This full-blown spying framework consists of two packages named ‘Tokyo’ and ‘Yokohama’. It includes backdoors, loaders, orchestrators, C2 communicators, audio recorders, keyloggers, screen and webcam grabbers, documents and cryptography key stealers, and even its own file indexer for the victim’s machine. We discovered up to 80 malicious modules stored in its encrypted Virtual File System, one of the highest numbers of plugins we’ve ever seen for an APT toolset.

Just to highlight its capabilities, TajMahal is able to steal data from a CD burnt by a victim as well as from the printer queue. It can also request to steal a particular file from a previously seen USB stick; next time the USB is connected to the computer, the file will be stolen.

TajMahal has been developed and used for at least the past five years. The first known ‘legit’ sample timestamp is from August 2013, and the last one is from April 2018. The first confirmed date when TajMahal samples were seen on a victim’s machine is August 2014.

More details about TajMahal are available to customers of the Kaspersky Intelligence Reporting service (contact intelreports@kaspersky.com).

Technical details

We have discovered two different types of TajMahal packages, self-named Tokyo and Yokohama. The targeted systems found by Kaspersky Lab were infected with both packages. This suggests that Tokyo was used as first stage infection, deploying the fully-functional Yokohama package on interesting victims, and then left in for backup purposes. The packages share the same code base, we identified the following interesting features:

- Capable of stealing documents sent to the printer queue.
- Data gathered for victim recon includes the backup list for Apple mobile devices.
- Takes screenshots when recording VoiceIP app audio.
- Steals written CD images.

- Capable of stealing files previously seen on removable drives once they are available again.
- Steals Internet Explorer, Netscape Navigator, FireFox and RealNetworks cookies.
- If deleted from Frontend file or related registry values, it will reappear after reboot with a new name and startup type.

Victims

So far we have detected a single victim based on our telemetry – a diplomatic entity from a country in Central Asia.

Conclusion

The TajMahal framework is an intriguing discovery that's of great interest, not least for its high level of technical sophistication, which is beyond any doubt. The huge amount of plugins that implement a number of features is something we have never before seen in any other APT activity. For example, it has its own indexer, emergency C2s, is capable of stealing specific files from external drives when they become available again, etc.

The question is, why go to all that trouble for just one victim? A likely hypothesis is that there are other victims we haven't found yet. This theory is reinforced by the fact that we couldn't see how one of the files in the VFS was used by the malware, opening the door to the possibility of additional versions of the malware that have yet to be detected.

Kaspersky Lab products detect the TajMahal APT samples as HEUR:Trojan.Multi.Chaperone.gen

Appendix I – Indicators of compromise

A full set of IOCs and Yara rules is available to customers of Kaspersky Intelligence Reporting service – contact intelreports@kaspersky.com

Domains and IPs

104.200.30.125

50.56.240.153

rahasn.webhop.org

rahasn.akamake.net

rahasn.homewealth.biz

File Hashes

22d142f11cf2a30ea4953e1fffb0fa7e

2317d65da4639f4246de200650a70753

27612cb03c89158225ca201721ea1aad

412956675fbc3f8c51f438c1abc100eb

490a140093b5870a47edc29f33542fd2

51a7068640af42c3a7c1b94f1c11ab9d

533340c54bd25256873b3dca34d7f74e

684eca6b62d69ce899a3ec3bb04d0a5b

69a19abf5ba56ee07cdd3425b07cf8bf
6cfd131fef548fcd60fbcdb59317df8e
72dc98449b45a7f1ccdef27d51e31e91
7c733607a0932b1b9a9e27cd6ab55fe0
7d5265e814843b24fcb3787768129040
80c37e062aa4c94697f287352acf2e9d
815f1f8a7bc1e6f94cb5c416e381a110
a43d3b31575846fa4c3992b4143a06da
08e82dc7bae524884b7dc2134942aad
7bcd736a2394fc49f3e27b3987cce640
57314359df11ffdf476f809671ec0275
b72737b464e50aa3664321e8e001ff32
ce8ce92fb6565181572dce00d69c24f8
5985087678414143d33ffc6e8863b887
84730a6e426fbd3cf6b821c59674c8a0
d5377dc1821c935302c065ad8432c0d2
d8f1356bebda9e77f480a6a60eab36bb
92f8e3f0f1f7cc49fad797a62a169acd
9003cfaac523e94d5479dc6a10575e60
df91b86189adb0a11c47ce2405878fa1
e17bd40f5b5005f4a0c61f9e79a9d8c2
c1e7850da5604e081b9647b58248d7e8
99828721ac1a0e32e4582c3f615d6e57
f559c87b4a14a4be1bd84df6553aaf56
b9c208ea8115232bfd9ec2c62f32d6b8
061089d8cb0ca58e660ce2e433a689b3
0e9afd3a870906ebf34a0b66d8b07435
9c115e9a81d25f9d88e7aaa4313d9a8f
520ee02668a1c7b7c262708e12b1ba6b
7bfba2c69bed6b160261bdbf2b826401
77a745b07d9c453650dd7f683b02b3ed
3a771efb7ba2cd0df247ab570e1408b2
0969b2b399a8d4cd2d751824d0d842b4
fc53f2cd780cd3a01a4299b8445f8511
4e39620afca6f60bb30e031ddc5a4330
bfe3f6a79cad5b9c642bb56f8037c43b
3dfebce4703f30eed713d795b90538b5
9793afcea43110610757bd3b800de517
36db24006e2b492cafb75f2663f241b2
21feb6aa15e02bb0cddb544605aabad
21feb6aa15e02bb0cddb544605aabad
649ef1dd4a5411d3afcf108d57ff87af

320b2f1d9551b5d1df4fb19bd9ab253a
 3d75c72144d873b3c1c4977fbafe9184
 b9cf4301b7b186a75e82a04e87b30fe4
 b4e67706103c3b8ee148394ebee3f268
 7bfb72441e1f2ed48fbc0f33be00f24
 cdb303f61a47720c7a8c5086e6b2a743
 2a6f7ec77ab6bd4297e7b15ae06e2e61
 8403a28e0bffa9cc085e7b662d0d5412
 3ffd2915d285ad748202469d4a04e1f5
 04078ef95a70a04e95bda06cc7bec3fa
 235d427f94630575a4ea4bff180ecf5d
 8035a8a143765551ca7db4bc5efb5dfd
 cacia3bf3b2801956318251db5e90f3c
 1aadf739782afcae6d1c3e4d1f315cbd
 c3e255888211d74cc6e3fb66b69bbffb
 d9e9f22988d43d73d79db6ee178d70a4
 16ab79fb2fd92db0b1f38bedb2f02ed8
 8da15a97eaf69ff7ee184fc446f19cf1
 ffc7305cb24c1955f9625e525d58aeec
 c0e72eb4c9f897410c795c1b360090ef
 9ad6fa6fdedb2df8055b3d30bd6f64f1
 44619a88a6cff63523163c6a4cf375dd
 a571660c9cf1696a2f4689b2007a12c7
 81229c1e272218eeda14892fa8425883
 0ac48cfa2ff8351365e99c1d26e082ad

Appendix II – Additional technical details

The following table provides the full list of files stored in the VFS with a short description describing what the plugins do:

| nn | Name | Short description |
|----------|----------------------|--|
| 00 01 | cs64.dll cs32.dll | C2 communication and command processing. WatchPoints document stealer. |
| 02 03 | li64.dll li32.dll | LocalInfo. Collects a large amount of information, titled “TAJ MAHAL” |
| 04 06 | ad64.dll ad32.dll | AudioRecorder. Microphone, Voice IP applications. |
| 07 08 | le64.dll le32.dll | Open source-based LAME mp3 encoder (“Mar 27 2014”) used by AudioRecorder plugins (adXX.dll). |

| | | |
|----|---------------|--|
| 09 | dd.m | MP3 file is sent by AudioRecorder (adXX.dll) when cache is cleared. |
| 10 | me64.dll | AudioRecorder for Windows Metro applications. |
| 11 | me32.dll | Injects ma32.dll into “wwahost.exe” or “audacity.exe”. |
| 12 | ma32.dll | AudioRecorder for Windows COM. Hooks IAudioClient, IAudioRenderClient, IMMDevice. |
| 13 | ams_api64.dll | Handy wrapper around API of exXX.dll, pdXX.dll, sgXX.dll. |
| 14 | ams_api32.dll | |
| 15 | ex64.dll | Orchestrator. Update/install/uninstall, selects target processes and loads plugins. |
| 16 | ex32.dll | |
| 17 | fe64.dll | Template of “Yokohama” Frontend module; is used for reinstalling. |
| 18 | fe32.dll | |
| 19 | pd64.dll | Provides API to access configuration settings, working files, egress queue. |
| 20 | pd32.dll | |
| 21 | libpng64.dll | Open source “libpng” library version 1.5.8 (February 1, 2012). Used by Screenshoter plugin (ssXX.dll). |
| 22 | libpng32.dll | |
| 23 | rs64.dll | Reinstaller/Injector. |
| 24 | rs32.dll | |
| 25 | ix32.dll | LoadLibrary call template dll is used by Reinstaller/Injector plugin (rsXX.dll) for injecting LoadLibrary call into running processes. |
| 26 | ix64.dll | |
| 05 | obj32.bin | Shellcode template is used by Reinstaller/Injector (rsXX.dll) and AudioRecorder4MetroApp (meXX.dll) for injecting into running processes. Both versions of “obj32.bin” are the same; it seems to be stored twice by mistake. |
| 27 | obj32.bin | |
| 28 | obj64.bin | |
| 29 | sc64.dll | Utility library. Provides API for cryptography, file, registry, memory management operations and so on. |
| 30 | sc32.dll | |
| 31 | sg64.dll | Library for managing egress queue (files and messages prepared to send to CC). |
| 32 | sg32.dll | |
| 33 | st64.dll | SuicideWatcher. Watches uninstall time, checks time diff (local time vs internet time). |
| 34 | st32.dll | |
| 35 | zip64.dll | Open source “XZip/XUnzip” library by Info-Zip + Lucian Wischik + Hans Dietrich. Is used by Indexer (inXX.dll) and C2 communication (csXX.dll) plugins. |
| 36 | zip32.dll | |

| | | | |
|----|----------------------|--|--|
| 37 | zlib64.dll | Open source “zlib” version 1.2.3 used by libpngXX.dll for compressing screenshots (ssXX.dll). | |
| 38 | zlib32.dll | | |
| 39 | il32.dll | IM-Stealer. Steals conversation content from chat windows of instant messaging applications. | |
| 40 | in32.dll | Indexer. Indexes files on victim drives, user profiles, removable drives. Built index files are zipped (by zipXX.dll) and put in send queue. | |
| 55 | in64.dll | | |
| 41 | isys9core_64.dll | Proprietary “ISYS Search Software” components are used by Indexer plugin. Licensee_ID1 “Q5GXU H5W67 23B4W SCQFD 4G7HV 9GSLW” Licensee_ID2 “objectviewer.exe” | |
| 42 | isyspdf6_64.dll | | |
| 43 | isyspdf1_64.dll | | |
| 44 | isysdc_64.dll | | |
| 46 | isys9.key | | |
| 47 | isys.cwd | | |
| 48 | isys.elx | | |
| 49 | isys9_32.dll | | |
| 50 | isys9core_32.dll | | |
| 51 | isyspdf6_32.dll | | |
| 52 | isyspdf1_32.dll | | |
| 53 | isysdc_32.dll | | |
| 56 | isys9_64.dll | | |
| 45 | sqlite3_64.dll | | Open source “sqlite” library. Used by “ISYS Search”. |
| 54 | sqlite3_32.dll | | |
| 57 | tn32.dll | | Thumbnailer. Makes and prepares to send thumbnails of found picture files. |
| 58 | tn64.dll | | |
| 59 | freeimage_32.dll | FreeImage open source library supports popular graphics image formats (ver 3.15.4 2012-10-27) (http://freeimage.sourceforge.net). Is used by Thumbnailer (tnXX.dll) plugin. | |
| 60 | freeimageplus_32.dll | | |
| 61 | freeimage_64.dll | | |
| 62 | freeimageplus_64.dll | | |
| 63 | ku64.dll | Keylogger & clipboard monitor. | |
| 64 | ku32.dll | | |
| 65 | pm64.dll | Steals printed documents from spooler queue. This is done by enabling the “KeepPrintedJobs” attribute for each configured printer stored in Windows Registry: key: “SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers” value: “Attributes” | |
| 66 | pm32.dll | | |
| 67 | rc64.dll | EgressSender. Sends files from output queue to C2. | |
| 68 | rc32.dll | | |

| | | |
|----|-------------|---|
| 69 | rn64.dll | Daily "ClientRecon" (ComputerName, OS information, MacAddress, WirelessNetwork keys, connected Apple devices, Apple mobile devices backups list, IE version, SecurityCenterInfo (AV, Firewalls and AntiSpyware products), Hardware info, Installed soft including Metro Apps, Users, Autoruns). Check and send to C2 if something changed. |
| 70 | rn32.dll | |
| 71 | ss64.dll | Screenshooter. Periodic low resolution screenshots. High resolution screenshots of specified process windows and when recording VoiceIP application audio. See "ss_pr" & "ss_wt_nm" cfg vars. |
| 72 | ss32.dll | |
| 73 | vm32.dll | Steal documents from fixed and removable drives. Watch CDBurnArea and steals written CD images. |
| 74 | vm64.dll | |
| 75 | wc64.dll | Periodically makes webcam camera snapshots. |
| 76 | wc32.dll | |
| 77 | default.cfg | Default configuration settings file. |
| 78 | runin.bin | List of processes names and associated plugins should be run inside these processes. |
| 79 | morph.dat | Configuration file stores path of work folders and registry keys. |



Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.

Source: <https://securelist.com/project-tajmahal/90240/>