Systems Affected

Microsoft Windows NT, 2000, XP, Vista, and 7

Overview

On November 24, 2014, Symantec released a report on Regin, a sophisticated backdoor Trojan used to conduct intelligence-gathering campaigns. At this time, the Regin campaign has not been identified targeting any organizations.

Description

Regin is a multi-staged, modular threat—meaning it has a number of components, each dependent on others to perform an attack. Each of the five stages is hidden and encrypted, with the exception of the first stage. The modular design poses difficulties to analysis, as all components must be available in order to fully understand the Trojan.

Impact

Regin is a remote access Trojan (RAT), able to take control of input devices, capture credentials, monitor network traffic, and gather information on processes and memory utilization. The complex design provides flexibility to actors, as they can load custom features tailored to individual targets. [1(link is external)]

Solution

Users and administrators are recommended to take the following preventive measures to protect their computer networks:

- *Use and maintain anti-virus software* – Anti-virus software recognizes and protects your computer against most known viruses. It is important to keep your anti-virus software up-to-date (see Understanding Anti-Virus Software for more information). [2(link is external)]
- *Keep your operating system and application software up-to-date* – Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it (see Understanding Patches for more information).

The following is a list of the Indicators of Compromise (IOCs) that can be added to network security solutions to determine whether they are present on a network.

MD5s: [1(link is external)]
Stage 1 files, 32 bit:

06665b96e293b23acc80451abb413e50

187044596bc1328efa0ed636d8aa4a5c

1c024e599ac055312a4ab75b3950040a

2c8b9d2885543d7ade3cae98225e263b

4b6b86c7fec1c574706cecedf44abded

6662c390b2bbbd291ec7987388fc75d7

b269894f434657db2b15949641a67532

b29ca4f22ae7b7b25f79c1d4a421139d

b505d65721bb2453d5039a389113b566

26297dc3cd0b688de3b846983c5385e5

ba7bb65634ce1e30c1e5415be3d1db1d

bfbe8c3ee78750c3a520480700e440f8

d240f06e98c8d3e647cbf4d442d79475

ffb0b9b5b610191051a7bdf0806e1e47

Unusual stage 1 files apparently compiled from various public source codes merged with malicious code:

01c2f321b6bfdb9473c079b0797567ba

47d0e8f9d7a6429920329207a32ecc2e

744c07e886497f7b68f6f7fe57b7ab54

db405ad775ac887a337b02ea8b07fddc

Stage 1, 64-bit system infection:

bddf5afbea2d0eed77f2ad4e9a4f044d

c053a0a3f1edcbbfc9b51bc640e808ce

e63422e458afdfe111bd0b87c1e9772c

Stage 2, 32 bit:

18d4898d82fcb290dfed2a9f70d66833

b9e4f9d32ce59e7c4daf6b237c330e25

Stage 2, 64 bit:

d446b1ed24dad48311f287f3c65aeb80

Stage 3, 32 bit:

8486ec3112e322f9f468bdea3005d7b5

da03648948475b2d0e3e2345d7a9bbbb

Stage 4, 32 bit:

1e4076caa08e41a5befc52efd74819ea

68297fde98e9c0c29cecc0ebf38bde95

6cf5dc32e1f6959e7354e85101ec219a

885dcd517faf9fac655b8da66315462d

a1d727340158ec0af81a845abd3963c1

Stage 4, 64 bit:

de3547375fbf5f4cb4b14d53f413c503

Note: Stages 2, 3, and 4 do not appear on infected systems as real files on disk. Hashes are provided for research purposes only.

Registry branches used to store malware stages 2 and 3:

\REGISTRY\Machine\System\CurrentControlSet\Control\RestoreList

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{39399744-44FC-AD65-474B-E4DDF-8C7FB97}

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{3F90B1B4-58E2-251E-6FFE-4D38C5631A04}

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{9B9A8ADB-8864-4BC4-8AD5-B17DFDBB9F58}

IP IOCs [3(link is external)]:

61.67.114.73

202.71.144.113

203.199.89.80

194.183.237.145

References

- [1] Symantec "Regin: Top-tier espionage tool enables stealthy surveillance"(link is external)
- [2] VirusTotal Analysis of a Regin Binary(link is external)
- [3] Kaspersky "The Regin Platform Nation-State Ownage of GSM Networks"(link is external)

Revisions

- November 25, 2014: Initial Release