Threat Category: Malware ? Remote Access Trojan (RAT)

Threat Name: GlassRAT

Threat Description:

GlassRAT is a Remote Access Trojan (RAT) malware attributed to Chinese threat actors, used for persistent access into target systems. It has been deployed primarily against organizations based in China or with Chinese interests. GlassRAT binaries contain unique binary and ASCII string signatures which can be used for precise detection.

Indicators of Compromise (IoCs):

Binary patterns (hexadecimal sequences):

$bin1 = {85 C0 B3 01} ? test eax, eax followed by mov bl, 1

$bin3 = {68 4C 50 00 10} ? push offset KeyName ("2")

$bin4 = {68 48 50 00 10} ? push offset a3 ("3")

$bin5 = {68 44 50 00 10} ? push offset a4 ("4")

$hs = {CB FF 5D C9 AD 3F 5B A1 54 13 FE FB 05 C6 22} ? handshake sequence used by variants

ASCII string indicators:

$s1 = "pwlfnn10,gzg" (XOR-obfuscated form of rundll32.exe)

$s2 = "AddNum"

$s3 = "ServiceMain"

$s4 = "The Window"

$s5 = "off.dat"

Detection Mechanism:

Binary pattern matches: All bin* patterns must match.

Handshake match: The $hs pattern must match.

String matches: At least three out of five (3 of $s*) ASCII strings must match.

Strings and binary patterns are matched without encoding constraints.

Rule name should be glassRAT.

Reference:

Initial research and detection rules: RSA Research and Florian Roth

Associated report (RSA Research GlassRAT Analysis): RSA FirstWatch report

Author:

RSA RESEARCH

Modified and optimized by Florian Roth (Nextron Systems)

Rule Metadata:

description: "Detects GlassRAT by RSA (modified by Florian Roth - speed improvements)"

Info: "GlassRat"

date: "2015-11-23"

id: "7739d1f6-f16d-5599-9388-a1d89dbeb355"

Known File Hashes:

37adc72339a0c2c755e7fef346906330

59b404076e1af7d0faae4a62fa41b69f

5c17395731ec666ad0056d3c88e99c4d

e98027f502f5acbcb5eda17e67a21cdc

87a965cf75b2da112aea737220f2b5c2

22e01495b4419b564d5254d2122068d9

42b57c0c4977a890ecb0ea9449516075

b7f2020208ebd137616dadb60700b847