MAR-10296782-3.v1 – WELLMAIL | CISA

Published: 2020-07-16 · Archived: 2026-04-05 13:54:09 UTC

Notification

Summary

Description

The Malware Analysis Report (MAR) is the result of analytic efforts by the Cybersecurity and Infrastructure Security Agency (CISA). This malware has been identified as WELLMAIL. Advanced persistent threat (APT) groups have been identified using this malware. For more information regarding this malware, please visit: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

This report analyzes two unique files. The files are a variant of the WellMail implant. The malware provides remote operator encrypted C2 sessions and the ability to dynamically run executable scripts on infected systems.

For a downloadable copy of IOCs, see MAR-10296782-3.v1.stix.

Submitted Files (2)

0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494 (0c5ad1e8fe43583e279201cdb1046a...)

83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18 (83014ab5b3f63b0253cdab6d715f59...)

IPs (1)

119.81.184.11

Findings

0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494

Tags

trojan

Details

Name	0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494
Size	6366794 bytes
Type	ELF 64-bit LSB executable, x86-64, version 1 (SYSV)
MD5	01d322dcac438d2bb6bce2bae8d613cb
SHA1	8830e9d90c508adf9053e9803c64375bc9b5161a
SHA256	0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494
SHA512	3705b5ceb4ea06370da2a0d73b60e776c9528545704442d0872b75d8593966905eb2ad6a4edddec42bed2115bcd22a37154079c73c26d0a
ssdeep	49152:RXKUBXE/J9KhwyXGHjKRwpEcWDm4grE/jwgQbl+8cUiFNj8hqTQqc5Y4lZT3iDS7:ZK34fLjLU0xQq2YRQD
Entropy	6.084206

Antivirus

No matches found.

YARA Rules

- rule CISA_10296782_01 : trojan WELLMESS
  {
  meta:
    Author = "CISA Code & Media Analysis"
    Date= "2020-07-06"
    Last_Modified="20200706_1017"
    Actor="n/a"
    Category="Trojan"
    Family="WellMess"
    Description = "Detects WellMess implant and SangFor Exploit"
    MD5_1 = "4d38ac3319b167f6c8acb16b70297111"
    SHA256_1 = "7c39841ba409bce4c2c35437ecf043f22910984325c70b9530edf15d826147ee"
    MD5_2 = "a32e1202257a2945bf0f878c58490af8"
    SHA256_2 = "a4b790ddffb3d2e6691dcacae08fb0bfa1ae56b6c73d70688b097ffa831af064"
    MD5_3 = "861879f402fe3080ab058c0c88536be4"
    SHA256_3 = "14e9b5e214572cb13ff87727d680633f5ee238259043357c94302654c546cad2"
    MD5_4 = "2f9f4f2a9d438cdc944f79bdf44a18f8"
    SHA256_4 = "e329607379a01483fc914a47c0062d5a3a8d8d65f777fbad2c5a841a90a0af09"
    MD5_5 = "ae7a46529a0f74fb83beeb1ab2c68c5c"
    SHA256_5 = "fd3969d32398bbe3709e9da5f8326935dde664bbc36753bd41a0b111712c0950"
    MD5_6 = "f18ced8772e9d1a640b8b4a731dfb6e0"
    SHA256_6 = "953b5fc9977e2d50f3f72c6ce85e89428937117830c0ed67d468e2d93aa7ec9a"
    MD5_7 = "3a9cdd8a5cbc3ab10ad64c4bb641b41f"
    SHA256_7 = "5ca4a9f6553fea64ad2c724bf71d0fac2b372f9e7ce2200814c98aac647172fb"
    MD5_8 = "967fcf185634def5177f74b0f703bdc0"
    SHA256_8 = "58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
    MD5_9 = "c5d5cb99291fa4b2a68b5ea3ff9d9f9a"
    SHA256_9 = "65495d173e305625696051944a36a031ea94bb3a4f13034d8be740982bc4ab75"
    MD5_10 = "01d322dcac438d2bb6bce2bae8d613cb"
    SHA256_10 = "0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494"
    MD5_11 = "8777a9796565effa01b03cf1cea9d24d"
    SHA256_11 = "83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18"
    MD5_12 = "507bb551bd7073f846760d8b357b7aa9"
    SHA256_12 = "47cdb87c27c4e30ea3e2de620bed380d5aed591bc50c49b55fd43e106f294854"
  strings:
    $0 = "/home/ubuntu/GoProject/src/bot/botlib/chat.go"
    $1 = "/home/ubuntu/GoProject/src/bot/botlib.Post"
    $2 = "GoProject/src/bot/botlib.deleteFile"
    $3 = "ubuntu/GoProject/src/bot/botlib.generateRandomString"
    $4 = "GoProject/src/bot/botlib.AES_Decrypt"
    $5 = { 53 00 63 00 72 00 69 00 70 00 74 00 00 0F 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 00 07 2F 00 63 }
    $6 = { 3C 00 6E 00 77 00 3E 00 2E 00 2A 00 29 00 00 0B 24 00 7B 00 66 00 6E 00 7D }
    $7 = { 7B 00 61 00 72 00 67 00 7D 00 00 0B 24 00 7B 00 6E 00 77 00 7D }
    $8 = { 52 61 6E 64 6F 6D 53 74 72 69 6E 67 00 44 65 6C 65 74 65 46 69 6C 65 }
    $9 = "get_keyRC6"
    $10 = { 7D A3 26 77 1D 63 3D 5A 32 B4 6F 1F 55 49 44 25 }
    $11 = { 47 C2 2F 35 93 41 2F 55 73 0B C2 60 AB E1 2B 42 }
    $12 = { 53 58 9B 17 1F 45 BD 72 EC 01 30 6C 4F CA 93 1D }
    $13 = { 48 81 21 81 5F 53 3A 64 E0 ED FF 21 23 E5 00 12 }
    $14 = "GoProject/src/bot/botlib.wellMess"
    $15 = { 62 6F 74 6C 69 62 2E 4A 6F 69 6E 44 6E 73 43 68 75 6E 6B 73 }
    $16 = { 62 6F 74 6C 69 62 2E 45 78 65 63 }
    $17 = { 62 6F 74 6C 69 62 2E 47 65 74 52 61 6E 64 6F 6D 42 79 74 65 73 }
    $18 = { 62 6F 74 6C 69 62 2E 4B 65 79 }
    $19 = { 7F 16 21 9D 7B 03 CB D9 17 3B 9F 27 B3 DC 88 0F }
    $20 = { D9 BD 0A 0E 90 10 B1 39 D0 C8 56 58 69 74 15 8B }

```
    $21 = { 44 00 59 00 4A 00 20 00 36 00 47 00 73 00 62 00 59 00 31 00 2E }
    $22 = { 6E 00 20 00 46 00 75 00 7A 00 2C 00 4B 00 5A 00 20 00 33 00 31 00 69 00 6A 00 75 }
    $23 = { 43 00 31 00 69 00 76 00 66 00 39 00 32 00 20 00 56 00 37 00 6C 00 4F 00 48 }
    $24 = { 66 69 6C 65 4E 61 6D 65 3A 28 3F 50 3C 66 6E 3E 2E 2A 3F 29 5C 73 61 72 67 73 3A 28 3F 50 3C 61
72 67 3E 2E 2A 3F }
    $25 = { 5C 00 2E 00 53 00 61 00 6E 00 67 00 66 00 6F 00 72 00 55 00 44 00 2E 00 73 00 75 00 6D }
    $26 = { 66 6F 72 6D 2D 64 61 74 61 3B 20 6E 61 6D 65 3D 22 5F 67 61 22 3B 20 66 69 6C 65 6E 61 6D 65 3D }
    $27 = { 40 5B 5E 5C 73 5D 2B 3F 5C 73 28 3F 50 3C 74 61 72 3E 2E 2A 3F 29 5C 73 27 }
condition:
  ($0 and $1 and $2 and $3 and $4) or ($5 and $6 and $7 and $8 and $9) or ($10 and $11) or ($12 and $13) or ($14)
or ($15 and $16 and $17 and $18) or ($19 and $20) or ($21 and $22 and $23) or ($24) or ($25 and $26) or ($27)
}
```

ssdeep Matches

No matches found.

Relationships

0c5ad1e8fe...	Connected_To	119.81.184.11

Description

This artifact is an ELF 64-bit file written in Go. This file has been identified as a variant of the malware family known as WellMail.

When executed, it attempts to collect the following data from the victim's system:

—Begin Data Collected —
IP address of the victim system
Current username
—End Data Collected—

The data is stored in the following format:

—Begin format—
"200.200.200.150|root|50d3a7116bf847c869f71ecc08eb124a"
—End format—

It will attempt to send the above data to its C2 server at the IP address, 119.81.184.11:25 over TCP port 25 with the User-Agent string "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 Safari/537.36".

The following key and certificates are used to create the secure connection:

—Begin Key and Certificates—

—Begin Certificate—
MIIDHzCCAgegAwIBAgICBnowDQYJKoZIhvcNAQELBQAwNzELMAkGA1UEBhMCVVMx
HDAaBgNVBAoTE0dNTyBHbG9iYWxTaWduLCBJbmMxCjAIBgNVBAMTASowHhcNMTgw
NTExMjE1OTEzWhcNMjgxMjExMjI1OTEzWjArMQswCQYDVQQGEwJVUzEcMBoGA1UE
ChMTR01PIEdsb2JhbFNpZ24sIEluYzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANf06onDYhHc7h5msEdruHffSx78EyNhAR08MrF8Zvlyq6BtsRfxscJ6
dcYxV18o5Nd5SXEu80wAz0+GBk+jN90mCz/54MtSMii4CnbCCxFd2Rs7ibMsnd/w
OiZRyiWTpAQ0dc+Kp2YIT0icEIJQ5bXauqRPHKyYfcJcJNSPxkMswnfaYYOIyGqJ
xGmBepBOyl8AVP7EizeaAL+4WoejHAW37hSeTJmmwpqojGeGEgTl5IU/QUNlTnDE
a8VlnJ6H3fCU6irCRp5RZeE87fHt10rOiIlqMg8DDz8RHytLGlaO3SCXXzoJvzD8
zaHaD3nWnFkeKhYxg0LJUYM9rl7LkNkCAwEAAaNBMD8wDgYDVR0PAQH/BAQDAgeA
MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ4EBwQFAQIDBAYw
DQYJKoZIhvcNAQELBQADggEBANTxGwoIup6pfoABqlS8VOSz8qPDSAaTMZSawmyc
f5MgN9IdI+9vtl391qSxPYE21fRM0qAW620YVIM1Io42fEx+Ncou+35T/dAmbcUG
wmT2b5ipg079lBwR2MeV+2DgS/Es7ICfKyXN5Y3aRfZo3gN/MGJ+1HIjvLK9b7dl
J0HLvcViFuCHlikw+woGl9WZIAzu2Za6P87tf9kSlBhfpOGvHG5p/lnw+rRRvsoW
N8HqZsAELwK9YqKohHoQ4K8VpoocmtnOpJ4bXIGwd0trM0ha6zKgcUWiHFOPTgdB

9gheCTIR7uhsXkw/gsG/Qn4FO/bY13ptI/0lQe3FZEVivTU=
—End Certificate—

—Begin Certificate—
MIIDLDCCAhSgAwIBAgICBnUwDQYJKoZIhvcNAQELBQAwNzELMAkGA1UEBhMCVVMx
HDAaBgNVBAoTE0dNTyBHbG9iYWxTaWduLCBJbmMxCjAIBgNVBAMTASowHhcNMTgx
MjAxMjI1ODAyWhcNMjgxMjExMjI1ODAyWjA3MQswCQYDVQQGEwJVUzEcMBoGA1UE
ChMTR01PIEdsb2JhbFNpZ24sIEluYzEKMAgGA1UEAxMBKjCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAPEgxGDxc/86bPDopIUb79TW6IJct4xJ9oK+ebSV
kEa2E0dIqg/nw3i+zbU0cQW+MMTVrSD9K9h6lkqhuXtXTyev+ewVNFJHTBpPY2rp
zDE/oYwqp1zuFxjL5yvCJIMKrvBwvZkpzO4jxGGm4XllRMugzPGJ48HBDYkNJvyF
mkABtgAfR+FF8ecQx5Hy250ELgHnvBL9YwD7sd+5/gSCgWMfTju1TazC1qS6xoFO
Xb9Dgp9ax8+UFVsL2lQkkt0O2GQ1rYvanc4ccsJmd4H0VtOm5C6VBQP8o1MVkOKA
v4dop+Tu694Wbv6M55VrgAtz/XPjTvzrCewl0QLIwHmevm8CAwEAAaNCMEAwDgYD
VR0PAQH/BAQDAgKEMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAPBgNV
HRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBLrN+wxjxk4YsqPQ7YUSWd
VpSQHp2WN6m6R4hfsjPoGSy5U36xygHq7fVkqh+nrOQfGjTps/7rFRLGAIoSjTWH
LisO1rEhpIduahWOdT4NxgeWBKUGCzwX2f7DcJ08uJwupGpzqxZh73LD+ox+6suL
YZP5g00kM0yPfTcDSKLkdFcPCRGCxtCBB9oW+dSzDEaVCSY5RjEHsbRLn4GRYv+V
96H9rbFHb80wofJvUYAdrFl6dRNty1QgCp1s9rZEFxdIzTQsuaVsi2zN/xARPP30
S+I+9FfdRr0zJdks7eEXQNKBijzRQPVahfBwUEkjbapUOAQIX3xR2a50d88BZybm
—End Certificate—

—Begin RSA Private Key—
MIIEowIBAAKCAQEA1/TqicNiEdzuHmawR2u4d99LHvwTI2EBHTwysXxm+XKroG2x
F/Gxwnp1xjFXXyjk13lJcS7zTADPT4YGT6M33SYLP/ngy1IyKLgKdsILEV3ZGzuJ
syyd3/A6JlHKJZOkBDR1z4qnZghPSJwQglDltdq6pE8crJh9wlwk1I/GQyzCd9ph
g4jIaonEaYF6kE7KXwBU/sSLN5oAv7hah6McBbfuFJ5MmabCmqiMZ4YSBOXkhT9B
Q2VOcMRrxWWcnofd8JTqKsJGnlFl4Tzt8e3XSs6IiWoyDwMPPxEfK0saVo7dIJdf
Ogm/MPzNodoPedacWR4qFjGDQslRgz2uXsuQ2QIDAQABAoIBAGwOSCyWbsOxYBQm
HZ4e8DZKrDPcvVa+eug97r+QF5ZJIkcrm6j3bpJ44+U/WxBqTdbjATR44ZPt880+
qnm+mX02Q/rG9QvHHQHy1ImHnjIaWz+dEtFsSbJ7aR0zX4pdzXutJCWsowYSslkK
fdg20jmkMC92xko2IvbVVDhnmDSTjYJv3t8ErUgQqGTWnIluIsVJtUfdtZE62Wqj
ETW7N09mgFZ6DkAWwi6GqM6R0h5assf9an+IRjdEvh0yAdgdeeGYugyxg4QsQaBP
z/8Nc+0MsljNOJ3l9mGvv5Le9lrkdQo4/LEinuq5EQCasDnhUAEa3ure8+iNwv7C
BjGQqYECgYEA78II0db0DrMjKK+lqvTRaWgjlGMUyc93datTipiCR2LCulipv2OE
Q7D9thg2dBvY+87mSoFFgJyhGl1nEtj23IsnJSfg8wrrOPGbHGROa3Hh7Yr/S1vk
codyakjfQ2+ShiiqEZHNfxyxV26A0dLFcKxI8e8HBI1oadJo5teh1MUCgYEA5pYc
vvXv4Aa72tMJFF6Dd2vN3kL6aIrrMCp3tLKjUhYz+H0bjHH9QVqj+O5cihxppQ2o
MuzyOuCbEDBYusgh4j0gHEetTOlGh0WO1H9XM25/ULFaNv3TckBI0neiyiWq9lyu
W6Fe6XnYdFBca2VaaixHkqq2FvnQu6AN4urZVQUCgYEAhuX7pGV3SFYOcDPz2K6K
rO4FJtZgufPbWP+er5qDorq0qbh9Ocw6fQO2nKAe81E/0t5kwILfoi9+jaED/5zH
uOsqiUNY1CbOlmmKRn1Bij63SbotTi9T6ATBoX+C7yR1orp6hgwtPVndhj4MiQI4
SN8G4+kDX9JYb0IN9+RXj6kCgYByhVlviiwBoraH/soCoNJAbH1JhxBg/aXDPURI
rXQp37ceEdytyytR2xeXGaNCQMxDWl4QNNg1X7oDt09KLP2PJHafNQYgLbeGlYhT
h48ijx2SURMSPsxWcRD53ssuBLk9NFiwT5wY7xgO5J6SBDt8gdNmR3y6OoZtuRdM
fQFFlQKBgCQ6qBuKHdNdriG1t7yo6kXBTGvNxhpq+MczIcHIr1g6u9SC2nrrEE+n
LF9EaHQT98PKqsO/8AFUkpwPpTftg6v4E2fKtU3WAvTOz3rydWvc00qSfTeBRQ2/
ypF1hXBXYRIil4qsX1xQRw2k+K+Mw+/I5CErVVNQ9aAvxNLwEKc7
—End RSA Private Key—

—End Key and Certificates—

Screenshots

Figure 1 - This WellMail implant contains a structure similar to the Work function contained within the WellMess implant (47cdb87c27c4e30ea3e2de620bed380d5aed591bc50c49b55fd43e106f294854), detailed within MAR-10296782.r2.v1.WHITE. This structure parses out executable scripts from data provided via a remote operator. In this case, the REGEX value indicates this implant will receive scripts compressed (tar files). The malware will then decompress them before executing the embedded script. Analysis indicates the WellMail implant is similar in design and structure to the WellMess implant -- and both accept and execute shell scripts from a remote operator.

119.81.184.11

Tags

command-and-control

Ports

- 25 TCP

Whois

Queried whois.apnic.net with "119.81.184.11"...

% Information related to '119.81.184.0 - 119.81.184.31'

% Abuse contact for '119.81.184.0 - 119.81.184.31' is 'abuse@softlayer.com'

inetnum: 119.81.184.0 - 119.81.184.31
netname: NETBLK-SOFTLAYER-APNIC-CUST-AW717-AP
descr: Sharenet Limited
country: NZ
admin-c: AW717-AP
tech-c: AW717-AP
status: ASSIGNED NON-PORTABLE
mnt-by: MAINT-SOFTLAYER-AP
mnt-irt: IRT-SOFTLAYER-AP
last-modified: 2015-01-12T14:07:06Z
source: APNIC

irt: IRT-SOFTLAYER-AP
address: Keplerstaat 34, 1171CD Badhoevedorp
e-mail: abuse@softlayer.com
abuse-mailbox: abuse@softlayer.com
admin-c: SDHB1-AP
tech-c: SDHB1-AP
auth: # Filtered
remarks: abuse@softlayer.com was validated on 2020-01-29
mnt-by: MAINT-SOFTLAYER-AP
last-modified: 2020-01-29T23:08:58Z
source: APNIC

person: Anthony Walker
address: Unit 1246,
24B Moorefield Rd Wellington 6037 NZ
country: NZ
phone: +1.866.398.7638
e-mail: anthony@sharenet.co.nz
mnt-by: MAINT-SOFTLAYER-AP
nic-hdl: AW717-AP
abuse-mailbox: anthony@sharenet.co.nz
last-modified: 2015-01-12T14:06:59Z
source: APNIC

% This query was served by the APNIC Whois Service version 1.88.15-SNAPSHOT (WHOIS-US3)

Relationships

119.81.184.11	Connected_From	83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18
119.81.184.11	Connected_From	0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494

Description

83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18 and 0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494 attempt to connect to the IP address.

83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18

Tags

trojan

Details

Name	83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18
Size	2214184 bytes
Type	ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux)
MD5	8777a9796565effa01b03cf1cea9d24d
SHA1	53098b025a3f469ebc3e522f7b0999011cafb943
SHA256	83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18
SHA512	e9c2bdcd2b298456726f0fc15ecf3cbfd667a7f0196bd42ecde1058dbfe33aeccb1626a462797cdaf1f32e2515ce08f0fa2d46e34833e0ac098(
ssdeep	49152:xtt6IZ6yPcb6MSsGN4aftKLK8Fa0Bpmy8TxQbjtHpbJ4E:xttn7Pc/Sjb5GpmyWxQVJbJ4E
Entropy	7.892960

Antivirus

No matches found.

YARA Rules

- rule CISA_10296782_01 : trojan WELLMESS
  {
  meta:
    Author = "CISA Code & Media Analysis"
    Date= "2020-07-06"
    Last_Modified="20200706_1017"
    Actor="n/a"
    Category="Trojan"
    Family="WellMess"
    Description = "Detects WellMess implant and SangFor Exploit"
    MD5_1 = "4d38ac3319b167f6c8acb16b70297111"
    SHA256_1 = "7c39841ba409bce4c2c35437ecf043f22910984325c70b9530edf15d826147ee"
    MD5_2 = "a32e1202257a2945bf0f878c58490af8"
    SHA256_2 = "a4b790ddffb3d2e6691dcacae08fb0bfa1ae56b6c73d70688b097ffa831af064"
    MD5_3 = "861879f402fe3080ab058c0c88536be4"
    SHA256_3 = "14e9b5e214572cb13ff87727d680633f5ee238259043357c94302654c546cad2"
    MD5_4 = "2f9f4f2a9d438cdc944f79bdf44a18f8"
    SHA256_4 = "e329607379a01483fc914a47c0062d5a3a8d8d65f777fbad2c5a841a90a0af09"
    MD5_5 = "ae7a46529a0f74fb83beeb1ab2c68c5c"
    SHA256_5 = "fd3969d32398bbe3709e9da5f8326935dde664bbc36753bd41a0b111712c0950"
    MD5_6 = "f18ced8772e9d1a640b8b4a731dfb6e0"
    SHA256_6 = "953b5fc9977e2d50f3f72c6ce85e89428937117830c0ed67d468e2d93aa7ec9a"
    MD5_7 = "3a9cdd8a5cbc3ab10ad64c4bb641b41f"
    SHA256_7 = "5ca4a9f6553fea64ad2c724bf71d0fac2b372f9e7ce2200814c98aac647172fb"
    MD5_8 = "967fcf185634def5177f74b0f703bdc0"
    SHA256_8 = "58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
    MD5_9 = "c5d5cb99291fa4b2a68b5ea3ff9d9f9a"
    SHA256_9 = "65495d173e305625696051944a36a031ea94bb3a4f13034d8be740982bc4ab75"
    MD5_10 = "01d322dcac438d2bb6bce2bae8d613cb"
    SHA256_10 = "0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494"
    MD5_11 = "8777a9796565effa01b03cf1cea9d24d"
    SHA256_11 = "83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18"
    MD5_12 = "507bb551bd7073f846760d8b357b7aa9"
    SHA256_12 = "47cdb87c27c4e30ea3e2de620bed380d5aed591bc50c49b55fd43e106f294854"
  strings:
    $0 = "/home/ubuntu/GoProject/src/bot/botlib/chat.go"

```
    $1 = "/home/ubuntu/GoProject/src/bot/botlib.Post"
    $2 = "GoProject/src/bot/botlib.deleteFile"
    $3 = "ubuntu/GoProject/src/bot/botlib.generateRandomString"
    $4 = "GoProject/src/bot/botlib.AES_Decrypt"
    $5 = { 53 00 63 00 72 00 69 00 70 00 74 00 00 0F 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 00 07 2F 00 63 }
    $6 = { 3C 00 6E 00 77 00 3E 00 2E 00 2A 00 29 00 00 0B 24 00 7B 00 66 00 6E 00 7D }
    $7 = { 7B 00 61 00 72 00 67 00 7D 00 00 0B 24 00 7B 00 6E 00 77 00 7D }
    $8 = { 52 61 6E 64 6F 6D 53 74 72 69 6E 67 00 44 65 6C 65 74 65 46 69 6C 65 }
    $9 = "get_keyRC6"
    $10 = { 7D A3 26 77 1D 63 3D 5A 32 B4 6F 1F 55 49 44 25 }
    $11 = { 47 C2 2F 35 93 41 2F 55 73 0B C2 60 AB E1 2B 42 }
    $12 = { 53 58 9B 17 1F 45 BD 72 EC 01 30 6C 4F CA 93 1D }
    $13 = { 48 81 21 81 5F 53 3A 64 E0 ED FF 21 23 E5 00 12 }
    $14 = "GoProject/src/bot/botlib.wellMess"
    $15 = { 62 6F 74 6C 69 62 2E 4A 6F 69 6E 44 6E 73 43 68 75 6E 6B 73 }
    $16 = { 62 6F 74 6C 69 62 2E 45 78 65 63 }
    $17 = { 62 6F 74 6C 69 62 2E 47 65 74 52 61 6E 64 6F 6D 42 79 74 65 73 }
    $18 = { 62 6F 74 6C 69 62 2E 4B 65 79 }
    $19 = { 7F 16 21 9D 7B 03 CB D9 17 3B 9F 27 B3 DC 88 0F }
    $20 = { D9 BD 0A 0E 90 10 B1 39 D0 C8 56 58 69 74 15 8B }
    $21 = { 44 00 59 00 4A 00 20 00 36 00 47 00 73 00 62 00 59 00 31 00 2E }
    $22 = { 6E 00 20 00 46 00 75 00 7A 00 2C 00 4B 00 5A 00 20 00 33 00 31 00 69 00 6A 00 75 }
    $23 = { 43 00 31 00 69 00 76 00 66 00 39 00 32 00 20 00 56 00 37 00 6C 00 4F 00 48 }
    $24 = { 66 69 6C 65 4E 61 6D 65 3A 28 3F 50 3C 66 6E 3E 2E 2A 3F 29 5C 73 61 72 67 73 3A 28 3F 50 3C 61
72 67 3E 2E 2A 3F }
    $25 = { 5C 00 2E 00 53 00 61 00 6E 00 67 00 66 00 6F 00 72 00 55 00 44 00 2E 00 73 00 75 00 6D }
    $26 = { 66 6F 72 6D 2D 64 61 74 61 3B 20 6E 61 6D 65 3D 22 5F 67 61 22 3B 20 66 69 6C 65 6E 61 6D 65 3D }
    $27 = { 40 5B 5E 5C 73 5D 2B 3F 5C 73 28 3F 50 3C 74 61 72 3E 2E 2A 3F 29 5C 73 27 }
  condition:
    ($0 and $1 and $2 and $3 and $4) or ($5 and $6 and $7 and $8 and $9) or ($10 and $11) or ($12 and $13) or ($14)
  or ($15 and $16 and $17 and $18) or ($19 and $20) or ($21 and $22 and $23) or ($24) or ($25 and $26) or ($27)
  }
```

ssdeep Matches

No matches found.

Relationships

83014ab5b3...	Connected_To	119.81.184.11

Description

This artifact is an ELF 64-bit file written in GO language. This file has been identified as a variant of the WellMail malware family. The program is capable of archiving files and sending and receiving files and messages. It is also capable of receiving and executing shell scripts on target systems. The following is a list of the malware's capabilities:

—Begin Malware Capabilities—
main.zipit
main.buildFileName
main.getIP
main.setParameters
main.GetRandomBytes
main.transport
main.send
main.receieve
main.hello
main.scheduler
main.runscript
main.main
main.zipit.func1

main.init
—End Malware Capabilities—

When the program is executed, it will attempt to contact its C2 at the IP address, 119.81.184.11 over TCP port 25.

Note: TCP port 25 is commonly used for email (SMTP), however, the malware is only using the port for secure communications, because of the likelihood that the port will be open on the router.

When the C2 is first contacted, the program collects the IP address of the victim machine and the current user and appends this data with a unique 128-bit hash. The following is an example of the string format:

—Begin String Format—
200.200.200.251|user|ec30305f04f4552c452c3596c88a8f2f
—End String Format—

Communication session are initiated with a hello packet with a payload formatted in the following manner:

—Begin Hello Packet—
cookie first = HgQdbx4qRNv/7c6750dc5f21bb24f2c5d1d734fc2eca
—End Hello Packet—

The following key and certificates are used for secure communications with the C2:

—Begin Key and Certificates—

—Begin Certificate—
MIIDHzCCAgegAwIBAgICBnowDQYJKoZIhvcNAQELBQAwNzELMAkGA1UEBhMCVVMx
HDAaBgNVBAoTE0dNTyBHbG9iYWxTaWduLCBJbmMxCjAIBgNVBAMTASowHhcNMTgw
NTExMjE1OTEzWhcNMjgxMjExMjI1OTEzWjArMQswCQYDVQQGEwJVUzEcMBoGA1UE
ChMTR01PIEdsb2JhbFNpZ24sIEluYzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANf06onDYhHc7h5msEdruHffSx78EyNhAR08MrF8Zvlyq6BtsRfxscJ6
dcYxV18o5Nd5SXEu80wAz0+GBk+jN90mCz/54MtSMii4CnbCCxFd2Rs7ibMsnd/w
OiZRyiWTpAQ0dc+Kp2YIT0icEIJQ5bXauqRPHKyYfcJcJNSPxkMswnfaYYOIyGqJ
xGmBepBOyl8AVP7EizeaAL+4WoejHAW37hSeTJmmwpqojGeGEgTl5IU/QUNlTnDE
a8VlnJ6H3fCU6irCRp5RZeE87fHt10rOiIlqMg8DDz8RHytLGlaO3SCXXzoJvzD8
zaHaD3nWnFkeKhYxg0LJUYM9rl7LkNkCAwEAAaNBMD8wDgYDVR0PAQH/BAQDAgeA
MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAOBgNVHQ4EBwQFAQIDBAYw
DQYJKoZIhvcNAQELBQADggEBANTxGwoIup6pfoABqlS8VOSz8qPDSAaTMZSawmyc
f5MgN9IdI+9vtl391qSxPYE21fRM0qAW620YVIM1Io42fEx+Ncou+35T/dAmbcUG
wmT2b5ipg079lBwR2MeV+2DgS/Es7ICfKyXN5Y3aRfZo3gN/MGJ+1HIjvLK9b7dl
J0HLvcViFuCHlikw+woGl9WZIAzu2Za6P87tf9kSlBhfpOGvHG5p/lnw+rRRvsoW
N8HqZsAELwK9YqKohHoQ4K8VpoocmtnOpJ4bXIGwd0trM0ha6zKgcUWiHFOPTgdB
9gheCTIR7uhsXkw/gsG/Qn4FO/bY13ptI/0lQe3FZEVivTU=
—End Certificate—

—Begin Certificate—
MIIDLDCCAhSgAwIBAgICBnUwDQYJKoZIhvcNAQELBQAwNzELMAkGA1UEBhMCVVMx
HDAaBgNVBAoTE0dNTyBHbG9iYWxTaWduLCBJbmMxCjAIBgNVBAMTASowHhcNMTgx
MjAxMjI1ODAyWhcNMjgxMjExMjI1ODAyWjA3MQswCQYDVQQGEwJVUzEcMBoGA1UE
ChMTR01PIEdsb2JhbFNpZ24sIEluYzEKMAgGA1UEAxMBKjCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAPEgxGDxc/86bPDopIUb79TW6IJct4xJ9oK+ebSV
kEa2E0dIqg/nw3i+zbU0cQW+MMTVrSD9K9h6lkqhuXtXTyev+ewVNFJHTBpPY2rp
zDE/oYwqp1zuFxjL5yvCJIMKrvBwvZkpzO4jxGGm4XllRMugzPGJ48HBDYkNJvyF
mkABtgAfR+FF8ecQx5Hy250ELgHnvBL9YwD7sd+5/gSCgWMfTju1TazC1qS6xoFO
Xb9Dgp9ax8+UFVsL2lQkkt0O2GQ1rYvanc4ccsJmd4H0VtOm5C6VBQP8o1MVkOKA
v4dop+Tu694Wbv6M55VrgAtz/XPjTvzrCewl0QLIwHmevm8CAwEAAaNCMEAwDgYD
VR0PAQH/BAQDAgKEMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAPBgNV
HRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBLrN+wxjxk4YsqPQ7YUSWd
VpSQHp2WN6m6R4hfsjPoGSy5U36xygHq7fVkqh+nrOQfGjTps/7rFRLGAIoSjTWH
LisO1rEhpIduahWOdT4NxgeWBKUGCzwX2f7DcJ08uJwupGpzqxZh73LD+ox+6suL
YZP5g00kM0yPfTcDSKLkdFcPCRGCxtCBB9oW+dSzDEaVCSY5RjEHsbRLn4GRYv+V
96H9rbFHb80wofJvUYAdrFl6dRNty1QgCp1s9rZEFxdIzTQsuaVsi2zN/xARPP30
S+I+9FfdRr0zJdks7eEXQNKBijzRQPVahfBwUEkjbapUOAQIX3xR2a50d88BZybm
—End Certificate—

—Begin RSA Private Key—
MIIEowIBAAKCAQEA1/TqicNiEdzuHmawR2u4d99LHvwTI2EBHTwysXxm+XKroG2x
F/Gxwnp1xjFXXyjk13lJcS7zTADPT4YGT6M33SYLP/ngy1IyKLgKdsILEV3ZGzuJ
syyd3/A6JlHKJZOkBDR1z4qnZghPSJwQglDltdq6pE8crJh9wlwk1I/GQyzCd9ph
g4jIaonEaYF6kE7KXwBU/sSLN5oAv7hah6McBbfuFJ5MmabCmqiMZ4YSBOXkhT9B
Q2VOcMRrxWWcnofd8JTqKsJGnlFl4Tzt8e3XSs6IiWoyDwMPPxEfK0saVo7dIJdf
Ogm/MPzNodoPedacWR4qFjGDQslRgz2uXsuQ2QIDAQABAoIBAGwOSCyWbsOxYBQm
HZ4e8DZKrDPcvVa+eug97r+QF5ZJIkcrm6j3bpJ44+U/WxBqTdbjATR44ZPt880+
qnm+mX02Q/rG9QvHHQHy1ImHnjIaWz+dEtFsSbJ7aR0zX4pdzXutJCWsowYSslkK
fdg20jmkMC92xko2IvbVVDhnmDSTjYJv3t8ErUgQqGTWnIluIsVJtUfdtZE62Wqj
ETW7N09mgFZ6DkAWwi6GqM6R0h5assf9an+IRjdEvh0yAdgdeeGYugyxg4QsQaBP
z/8Nc+0MsljNOJ3l9mGvv5Le9lrkdQo4/LEinuq5EQCasDnhUAEa3ure8+iNwv7C
BjGQqYECgYEA78II0db0DrMjKK+lqvTRaWgjlGMUyc93datTipiCR2LCulipv2OE
Q7D9thg2dBvY+87mSoFFgJyhGl1nEtj23IsnJSfg8wrrOPGbHGROa3Hh7Yr/S1vk
codyakjfQ2+ShiiqEZHNfxyxV26A0dLFcKxI8e8HBI1oadJo5teh1MUCgYEA5pYc
vvXv4Aa72tMJFF6Dd2vN3kL6aIrrMCp3tLKjUhYz+H0bjHH9QVqj+O5cihxppQ2o
MuzyOuCbEDBYusgh4j0gHEetTOlGh0WO1H9XM25/ULFaNv3TckBI0neiyiWq9lyu
W6Fe6XnYdFBca2VaaixHkqq2FvnQu6AN4urZVQUCgYEAhuX7pGV3SFYOcDPz2K6K
rO4FJtZgufPbWP+er5qDorq0qbh9Ocw6fQO2nKAe81E/0t5kwILfoi9+jaED/5zH
uOsqiUNY1CbOlmmKRn1Bij63SbotTi9T6ATBoX+C7yR1orp6hgwtPVndhj4MiQI4
SN8G4+kDX9JYb0IN9+RXj6kCgYByhVlviiwBoraH/soCoNJAbH1JhxBg/aXDPURI
rXQp37ceEdytyytR2xeXGaNCQMxDWl4QNNg1X7oDt09KLP2PJHafNQYgLbeGlYhT
h48ijx2SURMSPsxWcRD53ssuBLk9NFiwT5wY7xgO5J6SBDt8gdNmR3y6OoZtuRdM
fQFFlQKBgCQ6qBuKHdNdriG1t7yo6kXBTGvNxhpq+MczIcHIr1g6u9SC2nrrEE+n
LF9EaHQT98PKqsO/8AFUkpwPpTftg6v4E2fKtU3WAvTOz3rydWvc00qSfTeBRQ2/
ypF1hXBXYRIil4qsX1xQRw2k+K+Mw+/I5CErVVNQ9aAvxNLwEKc7
—End RSA Private Key—

—End Key and Certificates—

Relationship Summary

0c5ad1e8fe...	Connected_To	119.81.184.11
119.81.184.11	Connected_From	83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18
119.81.184.11	Connected_From	0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494
83014ab5b3...	Connected_To	119.81.184.11

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-844-Say-CISA or SayCISA@cisa.dhs.gov.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.

Revisions

July 16, 2020: Initial Version
