Quorum Cyber

Threat Intelligence
REMCOS
RAT

TLP Status: CLEAR

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	31/05/2023	Initial Report Drafted
1.1	04/07/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
	dd/mm/yyyy	

REMCOS RAT

Overview

REMCOS RAT is a remote access trojan that has been widely used in cybercriminal and espionage campaigns. It is known for its ability to hijack computers, collect keystrokes, audio, video, screenshots, and system data, as well as deliver additional malware payloads. The malware is often delivered through phishing emails with malicious attachments or links that lead to the installation of the RAT. REMCOS has also been observed being delivered through the DBatLoader malware loader and GuLoader. The malware is sold commercially by Breaking Security but has been used for malicious purposes since the mid-2010s.

It has been observed in various parts of the world and is known for its stealthy behaviour, including the use of public cloud infrastructure and anti-analysis techniques. The most recent events involving REMCOS RAT include a phishing campaign targeting Eastern European institutions and businesses with DbatLoader and REMCOS RAT malware in March 2023, and a new campaign targeting US accounting and tax return preparation firms ahead of Tax Day in April 2023. In recent months, there have also been several reports of REMCOS being used in campaigns targeting Ukrainian government entities and organisations in Eastern Europe.

REMCOS works by initially using brute force attacks on insecure servers then gaining access, taking control of the PowerShell utility, downloading, and installing an obfuscated Visual Basic script file which is then executed. After the malware has executed, a wide range of tools can be used such as screen capture, key logging and many more.

Impact

If the REMCOS is successfully executed, it will lead to full control and surveillance of the target system which will allow threat actors to exfiltrate sensitive data over a potentially long period of time, if undetected. Use of this sensitive data, depending on the target, could lead to victims being blackmailed, loss of employment if company data is involved and stolen organisational data which could be used to launch a large-scale sophisticated attack. It is likely that this would lead to irreparable damage to organisations or individuals' livelihoods.

Incident Detection

A comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against ransomware threats such as REMCOS. EDRs can alert system users of potential breaches and prevent further progress, prior to the malware being able to implement significant damage.

Targeted Products

Microsoft SQL servers.

Containment, Mitigations & Remediations

As mentioned previously, it is recommended that a EDR solution is implemented which will allow for the prevention or mitigation of potential attacks from a wide range of threats in real time.

All devices should implement the most recent vendor updates available as these will contain updates to their security features to help prevent exploitation from known threats.

Any credentials used on critical SQL servers should be secure in combination with firewalls and other implementations to prevent the initial launching of REMCOS-related attacks.

Indicators of Compromise

REMCOS Associated File Hashes (SHA256):

- 028006e9aa7b660b8afc0f52c3cddc47dc9c755beb27b007245c24c649f011d9
- 24668000291c63d17497280863b4abb8001268e80cd185f2e9185e50115aafcc
- 39c927965e14fb38c14b82c66c398f9cac1343d450db26e43c763b08a764b04b
- f49241aa75f09d249166d8c66a4cd6d279935df2fee508efdf4105c2fc8f330a
- 4e24f18c609d04ba55264362e311e7536eda95872bf42a3327b7970f2b8eaacb
- 5baaa1bb5e6b51d0f7cad61124d33048c61376a2194ee68f7b0ee57697cd53a4
- 89adcb90dcc56d8e5b6cab4fce35a7ea8619ed9d47a5a947aaf4f34cb42c5021
- e7a7431b7c5f7d73f80f8474e5d62a3620a639c762ea78b0266ff867c048a153
- f74adb5022803397214f21afffa91f0e5579bdd80b0fd0de0ca62f9b920b994d
- fadbc6f814008e75bff67f36923f9e2fa2faf5312ac8243e80236f57a17e12c1
- cd1f8f6b9caa62dbb054f08c08054395da2a1718ac352cb2398955f4587c497c
- 0f611b87697a816d5b37f745fa94c89315327ba3458c190fe41efd891ccd5196
- 4f95967b9b1f5532cb570bb1f762328d07ea16c20b6fcf1c4cfde82d06906630
- 6b4876ee9375a56d9e126297304cafd25639be66cdd3947e36256edbd9847e9f
- 9d631f6dbf464b2cd73809ebbc09805e8ccc0fdb485b3c06fbbe6ea34a8305c0
- f39ab4435d56184a143a55aaf080d672d3695f101e4516a31b89b465906e3fb0
- 12e76c5c297106f2a3e5fe0ef2bad750d78680aaafcdfad988b53c8731c44ffb
- 14c4a990c5cecb32bba5599c76cb5376f99e746334df3e5b154b23607e4fed40
- 2149cec22f889cc1eed0485be3a4670b2f5b20a2f40eaa24633ed54b3b795da2
- 4b50be772774494835e29d063b372a3e56192a8e2a09f1e7ec742d57603ee75f

REMCOS Associated IP Addresses:

- 79[.]110[.]63[.]178

- 79[.]134[.]225[.]27
- 193[.]239[.]84[.]153
- 194[.]59[.]218[.]165
- 81[.]161[.]229[.]110
- 146[.]70[.]158[.]105
- 91[.]192[.]100[.]10
- 188[.]72[.]124[.]143
- 45[.]141[.]152[.]68
- 45[.]81[.]243[.]246
- 91[.]245[.]253[.]46
- 81[.]161[.]229[.]156
- 194[.]87[.]151[.]52
- 192[.]227[.]132[.]34
- 37[.]139[.]129[.]142
- 95[.]214[.]24[.]120
- 23[.]95[.]122[.]90
- 164[.]68[.]101[.]51
- 198[.]12[.]89[.]173

REMCOS Associated Domains:

- gdyhjjdhbvxgsfe[.]gotdns[.]ch
- hasperion[.]kozow[.]com
- plunder[.]duckdns[.]org
- colukas37[.]ddns[.]net
- fortuna777[.]duckdns[.]org
- remcoss[.]onmypc[.]org
- plunder[.]dedyn[.]io
- plunder[.]dynnamn[.]ru
- plunder[.]jumpingcrab[.]com
- www[.]rmagent[.]biz
- fgfdbdgnghbgdd[.]con-ip[.]com
- groceria[.]con-ip[.]com
- jhcdiucishcisdfs[.]con-ip[.]com
- olkmnbftyujbvfd[.]con-ip[.]com

- sofiavergarate72[.]con-ip[.]com

REMCOS Associated URLs:

- hxxp[://]192[.]227[.]132[.]34/23/vbc[.]exe
- hxxp[://]23[.]95[.]122[.]90/176/vbc[.]exe
- hxxp[://]192[.]227[.]132[.]34/57/vbc[.]exe
- hxxp[://]198[.]12[.]89[.]173/191/vbc[.]exe
- hxxp[://]198[.]12[.]89[.]173/42/vbc[.]exe
- hxxp[://]37[.]139[.]129[.]142/htdocs/BwBsEPWWqtKSTHp[.]exe
- hxxp[://]37[.]139[.]129[.]142/htdocs/MyPRKcYpZgJEQQs[.]exe
- hxxp[://]37[.]139[.]129[.]142/htdocs/eGKBfFwQLEHtFdW[.]exe
- hxxp[://]81[.]161[.]229[.]110/htdocs/CjYrWNZyEcMBBMa[.]exe
- hxxp[://]81[.]161[.]229[.]110/htdocs/DrZpWMExDLTwCgS[.]exe
- hxxp[://]81[.]161[.]229[.]110/htdocs/WtSWKiEcEdFQMgT[.]exe
- hxxp[://]81[.]161[.]229[.]110/htdocs/ZtJEHbBnGzCABCs[.]exe
- hxxp[://]81[.]161[.]229[.]110/htdocs/dNHAwSjJLKWpyEZ[.]exe
- hxxp[://]81[.]161[.]229[.]156/MMY[.]exe
- hxxp[://]95[.]214[.]24[.]120/vect/BGTHPNHv[.]exe
- hxxp[://]95[.]214[.]24[.]120/vect/VXGFHDHHFG[.]exe
- hxxp[://]95[.]214[.]24[.]120/vect/WTRGHXBHJX[.]exe

Threat Group

REMCOS has been associated with the threat groups tracked as 'Gorgon Group' and 'LazyScripter', both of which have been known to target the government and critical national infrastructure (CNI). Gorgon Group is suspected to be a Pakistan-based group targeting western governments and was first seen in 2018. LazyScripter is a group with an unknown country of origin that has been known to predominantly target the airline industry and were first seen in 2018.

Threat Landscape

Critical SQL servers have long been a target of attacks due to their use in storing various sensitive information. These most recent attacks target SQL servers as they contain PowerShell utilities for management that can be used to deploy the malware onto the system.

REMCOS malware is one of many new methods involved in the prominent threat to key national infrastructure. The increase in threats to national infrastructure and use of malware targeting the various industries is due to the increasing geopolitical tension between nations leading to the increase of state-sponsored active persistent threat (APT) groups.

Mitre Methodologies

Execution

T1059.006 - Command and Scripting Interpreter: Python[1]

T1059.003 - Command and Scripting Interpreter: Windows Command Shell[2]

Persistence

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder[3]

Privilege Escalation

T1055 - Process Injection[4]

T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control[5]

Defence Evasion

T1497.001 - Virtualization/Sandbox Evasion: System Checks[6]

T1112 - Modify Registry[7]

T1027 - Obfuscated Files or Information[8]

Credential Access

T1056.001 - Input Capture: Keylogging[9]

Discovery

T1083 - File and Directory Discovery[10]

Collection

T1125 - Video Capture[11]

T1113 - Screen Capture[12]

---

[1] Command and Scripting Interpreter: Python, Sub-technique T1059.006 - Enterprise | MITRE ATT&CK®
[2] Command and Scripting Interpreter: Windows Command Shell, Sub-technique T1059.003 - Enterprise | MITRE ATT&CK®
[3] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®
[4] Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®
[5] Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®
[6] Virtualization/Sandbox Evasion: System Checks, Sub-technique T1497.001 - Enterprise | MITRE ATT&CK®
[7] Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®
[8] Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®
[9] Input Capture: Keylogging, Sub-technique T1056.001 - Enterprise | MITRE ATT&CK®
[10] File and Directory Discovery, Technique T1083 - Enterprise | MITRE ATT&CK®
[11] Video Capture, Technique T1125 - Enterprise | MITRE ATT&CK®
[12] Screen Capture, Technique T1113 - Enterprise | MITRE ATT&CK®

T1115 - Clipboard Data[13]

T1123 - Audio Capture[14]

Command and Control

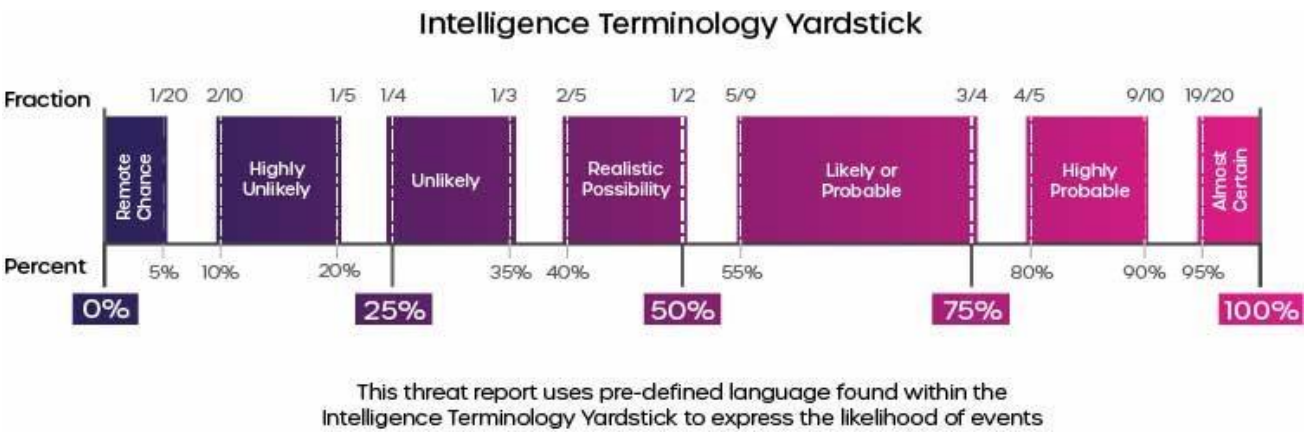
T1105 - Ingress Tool Transfer[15]

T1090 - Proxy[16]

Further Information

- AhnLab Report

Intelligence Cut-off Date (ICoD): 04/07/2023 10:00 UTC



[13] Clipboard Data, Technique T1115 - Enterprise | MITRE ATT&CK®
[14] Audio Capture, Technique T1123 - Enterprise | MITRE ATT&CK®
[15] Ingress Tool Transfer, Technique T1105 - Enterprise | MITRE ATT&CK®
[16] Proxy, Technique T1090 - Enterprise | MITRE ATT&CK®