THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

RA World

Threat Actor Ransomware

CATEGORY

Malware | Ransomware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Data Encryption
- Financial Loss
- Operational Disruption
- Reputation Damage
- Data Exfiltration
- Network Spread
- Recovery Costs
- Legal and Regulatory Consequences

Description

RA World Ransomware

RA World, formerly known as RA Group, is a notorious ransomware group that emerged in April 2023. This group primarily targets high-value sectors such as healthcare, financial services, and manufacturing in various countries, including the United States, Germany, India, and Taiwan.

RA World's attacks typically involve several stages to maximize their impact. They begin by exploiting vulnerabilities in internet-facing servers to gain initial access. Next, they engage in credential dumping and lateral movement within the network using tools like PsExec and Impacket. Often, their attacks involve modifying Group Policy Objects (GPOs) to deploy malicious payloads across multiple machines, ensuring persistence and extensive reach within the victim's network.

Indicator of compromise

SHA-256

2a4e83ff1c48baa3d526d51d09782933cec6790d5fa8ccea07633826f378b18a

57225f38b58564cf7ec1252fbf12475abee58bd6ea9500eb7570c49f8dc6a64c

93aae0d740df62b5fd57ac69d7be75d18d16818e87b70ace5272932aa44f23e4

af4a08bbe9f698a8a9666c76c6bdac9a29b7a9572e025f85f2a6f62c293c0f5e

f1c576ed08abbb21d546a42a0857a515d617db36d2e4a49bedd9c25034ccd1e2

2d22cbe3b1d13af824d10bb55b61f350cb958046adf5509768a010df53409aa8

330730d65548d621d46ed9db939c434bc54cada516472ebef0a00422a5ed5819

9479a5dc61284ccc3f063ebb38da9f63400d8b25d8bca8d04b1832f02fac24de

31ac190b45cc32c04c2415761c7f152153e16750516df0ce0761ca28300dd6a4

74fb402bc2d7428a61f1ac03d2fb7c9ff8094129afd2ec0a65ef6a373fd31183

7c14a3908e82a0f3c679402cf060a0bcae7791bdc25715a49ee7c1fc08215c93

817b7dab5beba22a608015310e918fc79fe72fa78b44b68dd13a487341929e81

8e4f9e4c2bb563c918fbe13595de9a32b307e2ce9f1f48c06b168dbbb75b5e89

0183edb40f7900272f63f0392d10c08a3d991af41723ecfd38abdfbfdf21de0a

bb63887c03628a3f001d0e93ab60c9797d4ca3fb78a8d968b11fc19da815da2f

d0c8dc7791e9462b6741553a411a5bfa5f4a9ad4ffcf91c0d2fc3269940e48a2

d311674e5e964e7a2408b0b8816b06587b2e669221f0e100d4e0d4a914c6202c

25ba2412cf0b97353fa976f99fdd2d9ecbbe1c10c1b2a62a81d0777340ce0f0a

31105fb81a54642024ef98921a524bf70dec655905ed9a2f5e24ad503188d8ae

826f05b19cf1773076a171ef0b05613f65b3cc39a5e98913a3c9401e141d5285

36ce5b2c97892f86fd0e66d9dd6c4fbd4a46e7f91ea55cc1f51dee3a03417a3a

108a3966b001776c0cadac27dd9172e506069cb35d4233c140f2a3c467e043d0

bc2caec044efe0890496c56f29d7c73e3915740bc5fda7085bb2bb89145621e5

1066395126da32da052f39c9293069f9bcc1c8d28781eb9d44b35f05ce1fd614

b2b59f10e6bdbe4a1f8ff560dbfe0d9876cbb05c7c27540bd824b17ceb082d62

4392dcce97df199e00efb7a301e26013a44ee79d9b4175d4539fae9aed4f750b

e31f5ebff2128decd36d24af7e155c3011a9afdc36fd14480026de151e1ecee2

SHA-1

168c6d2ee0d658904f61ced17b2035530ac48b72

106ddaea421120aa6fcd09bb84dd1d4fe19000fa

f477e11d7d48e695f604467043f97ea6eb73172c

fc697f1f847b1d41ce17f7c866df0424a0df0b78

75bbd5348254b854651e747c9aa7143b4ace4820

90d31274f5a0bfc53f7b4bb7f0b9829a68e7081b

ee4fc26e3ec51ce2fc260583cdc94c40b1af3dae

0c2ba636e8ae1d9559bb3de4ab879d1c7624ab6d

e90ffe7b3d4b9b80a63ba0151ece22d5811eb3dd

b2e8a6c4f568389c50d2b25c3fee6b0cf1312a1d

ed86064d5021d003a3efa9d73f687a9cbc803862

7c7cad64b2ea60971f8f56636a16e231fbd53ae0

bb028dbcebe6751a4a807154ba88cfc82d675376

b7b31df8a36ae97c8433c62746df549f43d258ca

1e8a2f310e0e431fb83aaded9b78723d94779cfc

4b69d49e2f1f00d79f7f31c16755f4ecbdaa6fa4

d72bc8c7e23c617fd6c50484e38a4c7962c4a2be

805b17a5a93928e70577a49f98054283b489484d

e48790ebbb37d7fd074724597a98e89ffb150198

2a84933a1988c4a17cd233766a9aa2489e57fd7a

91f88ebebcf078698fba5abc82cf2005c632a7f5

1237c3ef39dfd92cf70292f1a04a8b5b837465d6

cd425c95e0d074b6baf0a339ceeb56009a0b2958

0b19f38107c7c0a9e127c04c3cac6b89fedc4481

e90fa15b6b021a061615e3a487cb8cede983d621

fb86977f8c33264421b082093409543b2793e0d4

fc64b80f521f8f28c53401584c8f3c29b456c30d

MD-5

e8d7e2878eb1c56aa5874e8620bd6955

8e8c8abf33e42753ad7d185a38870ab5

4a20817bb78ae294c4475f754f72290d

f21277781661e97e4c2e70c1b5725d90

d5f55ad3bcb083bf07c31072c0348253

7eeacfb05675f1304f0b4daf81bd56de

7844c0c39d820d373569bbc1c8dfa8ee

dcc7371a1bb7380221bc0d48b85d99b8

0d0bc6f8144b4d3f3b80654b4fd8403a

1799f830593035969952475 7cbde2381

4aa36591efdc8bfcddfe338972be9d90

5bf3dfab3aac314adaa400a317987c82

d229af68c9896935edf632c2cc1adefc

e5a972cc589109be1aae14cdb5fd6984

6ccb3ad50f52601d254f9c5b47f35e99

4e2a208090fcf8ce27d696ef15750d32

24532b52054bc1a848e47d917b4cc0a9

19c4f4e3eb499b4049c76546c99e0c10

b6c46c1bd6ea86beae25c77d05280d59

87b3f09aa41bad9d87c5cd17c1a0edfa

0f5f2290a30c8f0f33f39a4513794806

7de7717e90bb9aa2ad0e76e29994cf3f

8f84941f03bc4a9f2633a283770e780b

1177aed7c7e035e47af41a009eaaf020

d615b6a427256ebf1c132038aef19079

f59c756a517c9db12aaa35cdd0c4fbaf

Remediation

1. Regular Backups: Maintain up-to-date backups of critical data and systems. Ensure backups are stored securely and are accessible for quick recovery.
2. Network Segmentation: Segment your network to limit lateral movement for ransomware. Isolate critical systems from less secure areas.
3. Security Awareness Training: Educate employees about phishing emails, suspicious attachments, and safe online practices. Awareness helps prevent initial infection.
4. Patch Management: Keep software and operating systems updated with the latest security patches. Vulnerabilities can be exploited by ransomware.
5. Endpoint Protection: Deploy robust antivirus and anti-malware solutions on endpoints. Regularly scan for threats.
6. Access Controls: Limit user privileges to the minimum necessary. Unauthorized access can lead to ransomware spreading.
7. Incident Response Plan: Develop and test an incident response plan. Know how to respond if a ransomware attack occurs.
8. Multi-Factor Authentication (MFA): Implement MFA for critical accounts. It adds an extra layer of security.
9. Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Secure your byte world

☎ +1 (832) 271 2738

✉ info@threatcure.net

https://threatcure.net/