

Rewterz Threat Intel – IndigoZebra APT Group Targeting Central Asia – Active IOCs

 rewterz.com/rewterz-news/rewterz-threat-intel-indigozebra-apt-group-targeting-central-asia-active-iocs

July 2, 2021

- [Solutions](#)

- [Resources](#)

Resources

January 7, 2024



January 7, 2024

[Rewterz Threat Advisory – CVE-2023-6690 – GitHub Enterprise Server Vulnerability](#)

Severity Low Analysis Summary CVE-2023-6690 GitHub Enterprise Server could allow a remote authenticated attacker to gain elevated privileges on the system, caused by a race condition. [...]

January 7, 2024



January 7, 2024

[Rewterz Threat Advisory – CVE-2023-51441 – Apache Axis Vulnerability](#)

Severity High Analysis Summary CVE-2023-51441 Apache Axis is vulnerable to server-side request forgery, caused by a improper input validation by the service admin HTTP API. By [...]

January 6, 2024



January 6, 2024

[Rewterz Threat Update – 4.5 Million Patients Impacted Due to Healthcare Tech Company Data Breach](#)

Severity High Analysis Summary A health management solutions provider, HealthEC LLC, recently suffered a data breach that has impacted almost 4.5 million patients who received healthcare [...]

Get in Touch

- [Solutions](#)

- [Resources](#)

Resources

January 7, 2024



January 7, 2024

[Rewterz Threat Advisory – CVE-2023-6690 – GitHub Enterprise Server Vulnerability](#)

Severity Low Analysis Summary CVE-2023-6690 GitHub Enterprise Server could allow a remote authenticated attacker to gain elevated privileges on the system, caused by a race condition. [...]

January 7, 2024



January 7, 2024

[Rewterz Threat Advisory – CVE-2023-51441 – Apache Axis Vulnerability](#)

Severity High Analysis Summary CVE-2023-51441 Apache Axis is vulnerable to server-side request forgery, caused by a improper input validation by the service admin HTTP API. By [...]

January 6, 2024



January 6, 2024

[Rewterz Threat Update – 4.5 Million Patients Impacted Due to Healthcare Tech Company Data Breach](#)

Severity High Analysis Summary A health management solutions provider, HealthEC LLC, recently suffered a data breach that has impacted almost 4.5 million patients who received healthcare [...]

[Get in Touch](#)



[Rewterz Threat Advisory –ICS: Sensormatic Electronics C-CURE 9000](#)

[July 2, 2021](#)



Rewterz Threat Advisory – CVE-2021-34527 – Microsoft Windows Code Execution

July 3, 2021



Rewterz Threat Advisory –ICS: Sensormatic Electronics C-CURE 9000

July 2, 2021



Rewterz Threat Advisory – CVE-2021-34527 – Microsoft Windows Code Execution

July 3, 2021

Severity

High

Analysis Summary

Recently discovered an ongoing spear-phishing campaign targeting the Afghan government. Further investigation revealed this campaign was a part of a long-running activity targeting other Central-Asia countries, including Kyrgyzstan and Uzbekistan, since at least 2014. The actor suspected of this cyber-espionage operation is an APT group dubbed “IndigoZebra“, previously attributed by researchers to China. The technical details of the operation were not publicly disclosed before. It discusses the tools, TTPs, and infrastructure used by the attacker during the years of its activity. We will also provide technical analysis of the two

different strains of the previously publicly undescribed backdoor xCaon, including its latest version we dubbed BoxCaon which uses the legitimate cloud-storage service Dropbox to act as its Command and Control server.

Impact

- Credential theft
- Financial loss
- Exposure of sensitive data

Indicators of Compromise

MD5

- b9973b6f9f15e6b20ba1c923540a3c9b
- 974201f7895967bff0b018b95d5f5f4b
- 3ecfc67294923acdf6bd018a73f6c590
- 35caae29c47dfb570773f6d5fd37e625
- 3562bf97997c54d74f58d4c1ad84fcea
- c00f6268075e3af85176bf0b00c66c13
- 85ea346e74c120c83db7a89531f9d9a1
- 5a8783783472be67c09926cc139d5b27
- b3d11e570da4a66f4b8520bc6107283b
- fdcae752f64245c159ab0f4d585c5bf8
- bb521918d08a4480699e673554d7072c
- c5406e7e161c758e863eb63001861bb1
- 4d6e93d2416898ea3a4f419aa3a438e3
- 6dfd06f91060e421320b6ebd63c957f0
- 0b10ac9bf6d2d31cbce06b09f9b0ae75
- b831a48e96e2f033d09d7ad5edd1dc67
- a875112c66da104c35d0eb43385d7094
- 1a28c673b2b481ba53e31f77a27669e7
- ef3383809fdf5a895b42e02bf06f5aa3
- aa107be86814d9c86911a2a7874d38a0
- 45d8cfe3450562564a1eb00a1aa0db83
- cdd7bfa36c6e47730fad94113aba7070
- 06d72a4d99fcd76a3502432657f3c999
- 5a91ccabd2b12ac56ba5170cf9ff8343
- 33f42e9678ee91369d11ef344bbd5a0d
- 84575619a690d3ef1209b7e3a7e79935
- 16e61624827d7785740b17c771a052e6
- ccc7f88b72c286fd756e76309022e9f8

- e98031cf43bfed73db0bce43918a608c
- 5ea42089cf91464b9c0c42292c18ba4c
- cff6d9f5d214e3366d6b4ae31c413adc
- c74711de8aa68e7d97f501eda328d032

SHA-256

- 8be3b10406f690ae5cf46c1dba18cb9a1c75bf646defcc9cab81d40fe0e0cc1b
- d0b88ab321a05fc94505620c9d02baec4cb1de7bb3b0067de4f8c0d3ba8548b2
- 489fca69a622195328302e64e29b6183feac90826dce198432d603202ca4d216
- 6395c4a8495d3bff293a8a55ca3c5ebf68a616ee212b2a7284610b0a3f7bb5d4
- 6ffe81c2883c298a65477ba2bc7ba1063315ad6b26f0188e3361d0fa924575ae
- e9013f35ce11fc4c5eb2c21827bdc459202d362365d6ea5b724dee4fe0088bd1
- 42e781f5e9c00d09cb5f7697a7b2fc9b04d77cc7978dcca8098f77d57693ca6c
- 15633871c3630a559dd4e2c7a9b93b02d17dd64ee60a2d7ba340ebd14d13ffac
- 05f3293dc1f22b1a4b15b8cacce8d4205dec8615627d11f1301ff3871e64015
- f5ba2676ddb81f29c69867556fa261563d68a5905252bb94090e0db05b048cc8
- adb2cf3550ff3c3ed841f672e8b6f7f01ec502c563e0a3a0472ce2be0995f4d8
- aaacaff803623414b7ee1ee6130b08380722752d97d1659f67fe6763f208f315
- 16c5bfcd1c454de1d0d55e41d1a8c35f78bab94acff4d09ecaa8faff9770a373
- d31e440e0d6f98209a9c9c7b4e332f417e41030a4bf4a4ae99d326cec24807af
- 0180d1ef09fcd684e0f496ecca21b11bc5142fe068f10ad5699027fbd7688103
- 39ec0cab03888c8f77dc5b989abe26b1997ad8e87849b9c1374902b908e78b6a
- 4122bb06352410a9b4bef4bc2bcf249265c14f1332df4fe1256a1281bd53bf22
- 984041fcf46bf0d275bf5f7eed649b3e2968e005e6a59829e4b9a51b875c7ef9
- 7bd75383dfab3948ce06a7f533870946934c87fb1c7b8035b69b4f2a166bd5b0
- 295b987c8926399c063ff20d2484477fe31cd2188b604a919dbfa11d9c34b988
- 86a0761fa0f6b15d9d5342882e09992270358766d5c11ef1b8d848c7f4075c79
- 935051367363838fcadd8856e08575e740bdf8af0d2271b81e6ba4d231b3a531
- 27312973aefcfa2511573a28ff42ef12ecbfcf56db42bf4d1371b0a1f1f2732c
- 78e7c41458e1ddf336f0d2e9625abbdc0b3e86db18aee7377af5711bc927da35
- 52a53e7e250fa9faa823d26421ca8af42ac40c27bac1d5af65b452c8987cda72
- ab1983217880dad9c0481aab5b06e1fe4b9caaf8d56d8a03bf794aca18f2e4c6
- fc3cdc3932d69c05c735040245f94fafa22b79cd865bb7d23c4364a3f4e8c774
- e683c86fd40eac23bc6435f479518ea5d80f90da294d5ad21d024dd7acc8a6ac
- c82e0a487203457026e61b77d1becb97e8e0d2d8a30ee17d1d8827f9ece87607
- 784cf7d224974f7e2c43cf10580c42a2521556608a5dd4a11247d09a77f5c8df
- c0082f8f1e49c0805c4eaacf5cf5b99ae30eeea585fd77cbd50904927052a18c
- f6942682162769091569d0129f0b77dd7176672b0e978a29416efe3d3859d0f9

SHA-1

- 22e327a5e2beba5b52358dbe9cd11727a7ddde91

- 5c027de1a7883f78e508ebf85847d0b32bf3c9a0
- 3557d162828baab78f2a7af36651a3f46d16c1cb
- 6519a71c64aa216673f3582da1338e22c4ad78a8
- 5a08e5bce797142c6d46675a6c070e503e987dd7
- a3343f4cd3eb8415d3b787ff442074180d108d3a
- df8201f67be99d7c6094e9d67f3a54c94809dda
- 4ea195fd2af0a4fa0ce2a9b052ca380206ad6fe6
- d14b84a15a4673c24c666d938a34232676e69df6
- d280f33f6d6e748313d3b637591525383ea749fe
- d71c7966d2c4ae8beb742c0f9152f1699703a601
- 3c6a4db19321a10f563e5c2a018e3a72b243a276
- d367676de8f100ea9592021a7997a08d07a0dd0f
- 10d3f7e7376c88429d829ed084974966462ecbfc
- 0c061ec90fbc61a868c2ce7aaac4fe79b42cc6c0
- 730c4d0cde7316c0b5cde69254c8b1cbe8af9a91
- e5cafc60a76cb8cd738d6133ff562f735712542e
- 9c9f1dfa79575a212023233ef5a3db4e7a250278
- 42bab3bc85c72864592a8ca3ae2351399e0efde1
- 8cfd45f1364f569522399d1e246039cffbde6d82
- 6bbdc51640ea88fdd15e58e60c1e7e4a27fcc5f0
- 245259780d59c3f4eb2d873f05ad86673c88815d
- 9976e5121c264a2b0dcf09ddd6c8cb53fdd964f8
- 24ffb24a73e68e6f5c23ab090f9ce5ac5dd41a8e
- 8b8a5ed2f2921d355d82e342595b1e73f5ed2560
- f2ee686c24eddea9ca495cfbb790798e6b6d451b
- 3fa8f0de425317407a540c359dfcb5e87fc02abf
- 4f2ba5c8848ec94835f4070acb92dcad46769995
- de83c07a3311b5ecb908b7ae8c78766da383d1da
- 88927e4d9a6a1ce5e656c599c0b0f462af97ba57
- 6305784544936d4b1b2f7ede4028c33094ddcea2
- e5608c6d7436e5697feef61ba4cddd9be0a37b96

Remediation

- Block all threat indicators at their respective controls.
- Look for IOCs in your environment.