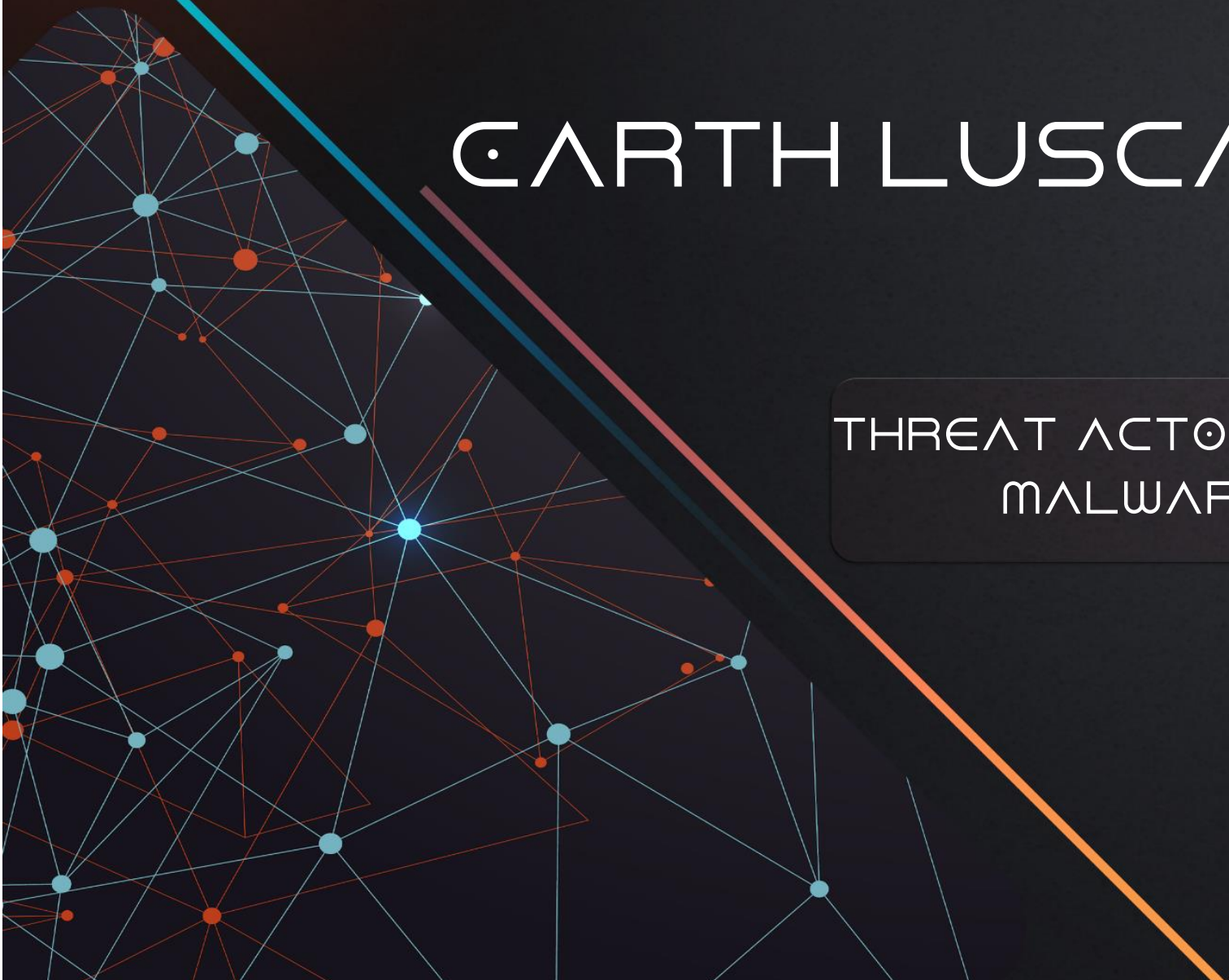
THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

CYBER THREAT ADVISORY

EARTH LUSCA

THREAT ACTOR
MALWARE



THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

CATEGORY
Malware

SEVERITY
High

PLATFORMS
Windows & Linux

IMPACT

- Loss of Sensitive Information
- Damaged Reputation
- Credentials Loss
- OS Credential Dumping: LSASS Memory

RELATED CVES:

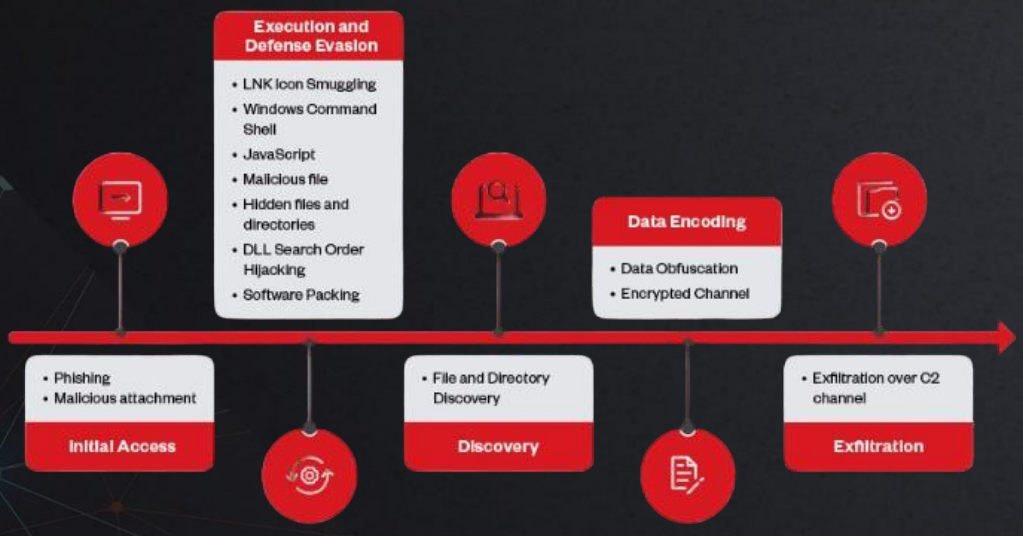
- CVE-2019-9621
- CVE-2019-9621
- CVE-2021-31207
- CVE-2021-34523
- CVE-2022-40684
- CVE-2021-37533
- CVE-2021-22205

DESCRIPTION

Earth Lusca

Earth Lusca is a threat actor from China that targets organizations of interest to the Chinese government, including academic institutions, telecommunication companies, religious organizations, and other civil society groups. Earth Lusca's tools closely resemble those used by Winnti Umbrella, but the group appears to operate separately from Winnti. Earth Lusca has also been observed targeting cryptocurrency payment platforms and cryptocurrency exchanges in what are likely financially motivated attacks.

Earth Lusca attack chain:



INDICATOR OF COMPROMISE

SHA-1

f24b0ae0864fdebdd4d12cd3b0469073d82395a3

e9f37150f4dd2d3fb0103a86185f76502b294d91

e1e416374e6b60db5a2c7da52f790d1038a46e4d

dca1c53a19afcd96d486a3b7e4683f59fef760a5

da8e863a11fb0beba48dee00829b1c16191085b5

d448fe77460682c7e00ac945c0aba0176eaa16b3

b33e7b37cf054a7d20f393cf5d1db2b1aa488ca5

b057e3e12d99605d86cdb63b789ca9f6c15ed5e0

a0267324300e453a55c727e7c9e20ba419e86260

9b57567086e7253e866c84a11256bd43e8658b07

95d751d4b380d3ca39d4db3950092ff4ec79ee35

9538e25628f854f18a26106daf1705cb4537e6d4

90da10004c8f6fafdaa2cf18922670a745564f45

7c66d3d48469eecc37257d64389e4d9571694c48

79cf19d0d5e9c9937944ae72cca806281dee692c

70c96f0f726d868975debd799d7d645f1a04426e

6dd15c03ffd3762a20b0f51faf31724d5dbf1466

5bd0690247dc1e446916800af169270f100d089b

59d89e955686799eebe8370c6eaa911bf34c6733

5044e5d2753acb450a4c3e52ecf1409700cda74d

4cc2c3ae116d8abd4ec8383b5cb2453289c7fbcf

47cdaf6c5c3fffeeff1f2c9e6c7649f99ab54932

454099b5197a74e5cc8b2957ca8e78abcb6244e6

363e32fafd2732b3cfb53dfd39bef56da1affd7f

INDICATOR OF COMPROMISE

SHA-256

16da7d6db1f419a45f43ebdcd2de988d5fcab7125ded6b113c33ddf45eac9751

95dc025a6dbd32b0493155bd15729e12c65f631c8c0061bee14941299b4edb27

4f719d67a8b414eb9b2e6d88bdf11f2ed995f9ac009daef8ef50202fb595845c

49694b9f9d0c9e2ef75ca2924f65e0442b919d86996dd50311a90ff66077e332

46bf0f1f57faee3522992a0a899b89749c0b2e7bc8c35a526019c2e855dacbe6

25e7deda66c590c7c3761b0337bcce05e8bb20506857be4834060068367a559e

10feb4b28cd467f8fcd95a067090b87a519ceb9ede1ecb99dee6f86d4da7035a

04715a91703b74d905767239506a53cb717f4cfb65ac6704eee60548bd30e162

56b79a3550334a1dc24a9ce896471a1e80d0a5c5459d53d4da4a0345faa548d7

31b3527032b5c36546cebccc6ef45faa5278dae109bbc0fcfcfb06275c78a72e

84d37e084d99c640fe59ebb6c0d4cb61b06f8782249026dad15f604fa5523220

b68919aff001d8366249403a2544fba2d833084f1ad22839b6310aadacb6a138

f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912

65b27e84d9f22b41949e42e8c0b1e4b88c75211cbf94d5fd66edc4ebe21b7359

6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc

fe2a80dee2a75d7b857626bf3d02fbbffedaf306ebc1caae2f3786c430a28667

e68fc2db08da4903b9f03972761cefd43ffd9483204c2973be18e1979c89265d

c32b84d34555d0bfac2a8059d49edefc0bf6307e5c35036f29df81d3422110b2

bf4eb6a3559f6ed39b2bb6a755358c08777efe03d82af53cf316f02db9d94566

beda49d6d0a851b220e3bb949aa217b48fe23012c96d2d0720d559a62bdbe8e5

1bad98b7600b67bb7bd1e7f97c227333a3db388d7708a961a5184f7b51e13609

be259da280486345420d56aee922585fd8b926a42f2e0cdaaf78eac26c071139

b124fa0336ce9ab3efc5a8485b066ba6c43c11772eaefcdf6cfb191ebaeb2bf9

ab2fc9037681193e4dbc7569a683a5aaac1b4a454ec81f40e7a4e6a44bd8b43d

8ce74e881727851b4427183947937854816d72704925561b9de6420cd43214ee

2bf93d6d9c2f2a8e945e6f78e16a66485c2f66469269a934f0d28657ea933805

7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe2ea177f62257a9191

9ac9dba9ac2096c72b78d693c53a59b3e348fff4007c455c7450caac0c3f8274

10f1479edcf33f3c8d60cf01748a3f38e45ecd2b894276ab19968b390395b00d

eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

CYBER THREAT ADVISORY