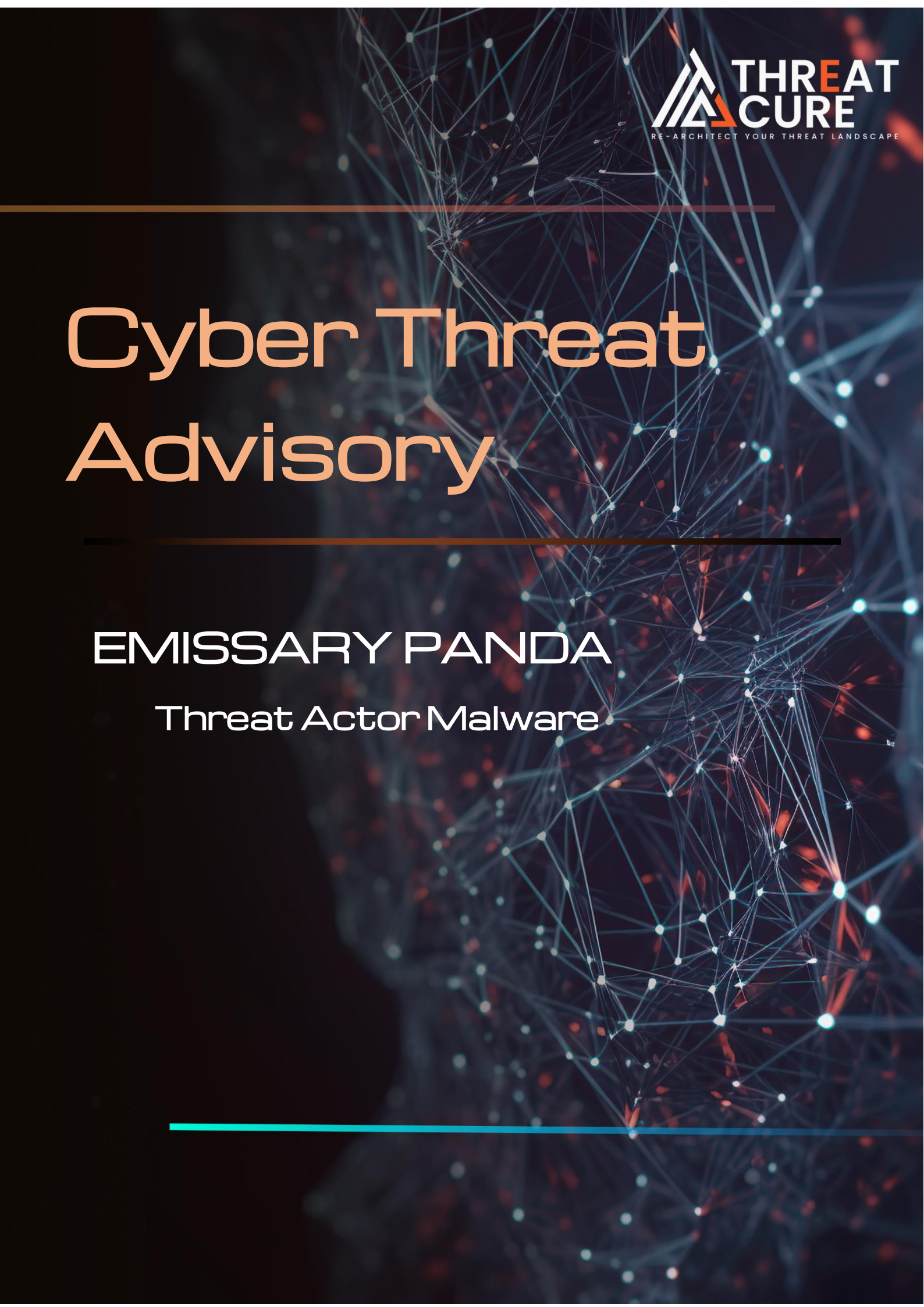

Cyber Threat Advisory

EMISSARY PANDA

Threat Actor Malware

CATEGORY

Malware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Intellectual Property Theft
- Economic Losses
- National Security Risks
- Operational Disruption
- Reputation Damage
- Increased Cybersecurity Costs
- Data Privacy Violations

Description

EMISSARY PANDA

Emissary Panda hit again almost 20 countries affected by this threat actor on this year 2024. Threat Group-3390, also known as Emissary Panda, is a China-based threat group active since at least 2010, extensively using strategic web compromises to target victims. This group focuses on collecting data from foreign embassies and targets various sectors including aerospace, government, defense, technology, energy, and manufacturing. Emissary Panda overlaps with other threat actors such as Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens, and possibly UNC215, and has collaborated with TA428 in operations like StealthyTrident.

Emissary Panda exploiting CVE-2019-0604 in Microsoft SharePoint to install webshells on government servers in two Middle Eastern countries. They used these webshells for credential dumping, network pivoting, and exploiting CVE-2017-0144 (linked to WannaCry). This aligns with alerts from Saudi Arabian and Canadian cyber security centers. The group also employed DLL sideloading and the China Chopper webshell.

Indicator of compromise

SHA-256

364400f373603c04125d7e5a5abb44a555be167ea8acecf23a833312a70dc4fa
a4a10c2ce4f2edb368c8a23e0d29deb6a1c943920da32bd0ba7a9097778145a6
14290527167110848231ed93f633d2d0a00b9736cca663894f61cfbbaaca7bd0
9be33e6cbd1226e74983c7758aa947831e016c98b2c5b7969e0e4120532e5114
dbfbae7c36e6a82711a88971fb03fc57272f465151a21f4ec97419f030e24e3e
a7394c1e0ab2ab63b421bbf4cf363a7686b8bf057ac89b3236833dff48f6dcbb
dca2ee9357ace83a06f189c757af264eec68659e298a19278ba04423fd2870c7
854f6023115212d2af6bf6303435c539b36251e0df61f5a270e057d9ee22a45e
8f25d6cbda0a9d000c30250eb626efa4a485ef57634838a41fa1c8aa08ce9ac8
b2baeb751b686b9b50046a30c1f4578222ce11f32cd2aca6a2c1974d26b7c6ad
be59ba93d17d92b2d90bd54dc20685aba3e6154c79e62ac9cb979273bbb8eb7e
44dc3f4feca316d217b1eb9f4203bfc59b9cf58d65e490ba5a544a6639947377
6772a268fe35e0ffc0e67da0c81d0e9dac0cd87f3751fe90df711a39dcbb922d
3047d5c22a245d1e4294fcd547ec5fb0f2e5ef030b764424acc74e7744fbe32e
59f4d42056bc43960c2b052fa9d615ad6e654c8aa1dfe3703342375523ba8ea5
44dc3f4feca316d217b1eb9f4203bfc59b9cf58d65e490ba5a544a6639947377
6772a268fe35e0ffc0e67da0c81d0e9dac0cd87f3751fe90df711a39dcbb922d
8f25d6cbda0a9d000c30250eb626efa4a485ef57634838a41fa1c8aa08ce9ac8
9be33e6cbd1226e74983c7758aa947831e016c98b2c5b7969e0e4120532e5114
dc7ada5c6341e98bc41182a5698527b1649c4e80924ba0405f1b94356f63ff31
e658fe6d3bd685f41eb0527432099ee01075bfdb523ef5aa3e5ebd42221c8494

6772a268fe35e0ffc0e67da0c81d0e9dac0cd87f3751fe90df711a39dcbb922d
8f25d6cbda0a9d000c30250eb626efa4a485ef57634838a41fa1c8aa08ce9ac8
9be33e6cbd1226e74983c7758aa947831e016c98b2c5b7969e0e4120532e5114
1ee0ff6d3d73df2052c8b426051d3e69da65e7f27d856de81c72c850127dced2
dc7ada5c6341e98bc41182a5698527b1649c4e80924ba0405f1b94356f63ff31
e658fe6d3bd685f41eb0527432099ee01075bfdb523ef5aa3e5ebd42221c8494
3047d5c22a245d1e4294fcd547ec5fb0f2e5ef030b764424acc74e7744fbe32e
5c3257b277f160109071e7e716040e67657341d8c42aa68d9afafe1630fcc53e
138aa7db51c362a7a58c321448b38658aef446dd742e9852ffb00ad5b2db2dc2
195673d4955533455413fdb62390ebe75bf1b752a3646adb24be57667d07c937
4085a5f9f2a98d1ece311f5efa6bd8a75b838c3d7ec75558fa2a839951b02616
46fe7689574a08991896991cec0433efd2520d479940989684046f606ae9038f
6b94aa0a43c94342d4a794f1a28db0bfca30d0d7809de3c891b1b6f022fda825
6cd90b44660b591058de76b31b8ce54a04b95fd3b6a9db4b35e44736ab8b4bb1
a552b58bfd26ce40e97acc7eefe9e1332cfc30b9b37ed339e2b15f9d2f286d43
a8f83b8bad7ae277311189a9b955d388039578f0f430200c8a807aedfaf8a7cf
c644ad27736b4f1e4b082b3be0951f4326221c40a6f43631a3d9ad9d912642d3
1e0905017edd41c2b0dd5ba722fdcf7cc08bf5c44f49b659474e834936f95145
1ee0ff6d3d73df2052c8b426051d3e69da65e7f27d856de81c72c850127dced2
40288de7a3ec34811fc9e3f95e094f7d456ada68b7be01e02a720a869e80bed3
4521379677fdc5542079a8f31a406b7c32b3ce0a8dfc5751186904143622l5d6

Indicator of compromise

SHA-256

345d665752ac390df2e0a50f5a6d034c2867eea824a56f662167cddf349d2e6d
138aa7db51c362a7a58c321448b38658aef446dd742e9852ffb00ad5b2db2dc2
195673d4955533455413fdb62390ebe75bf1b752a3646adb24be57667d07c937
470ebac11df7d2de4e2d90abbb67faadd8024579e469a401e48a23a5bdb0f5e9
56c6dfcaabe7f115b5ae3510f66067abccca6dfdae17439566c429eac5d76f08
611f66b0db562699932e6c55ff47efe5641386802ccf9c83cc1e444b3f8f7e5b
635ed79241d533433a33ef6dcc16a413a49be582722454074b5243d45f580de8
82a673f1ecf27b2f3cdee8208d34e29b4865b1f2268bf823b0150b096f275220
a552b58bfd26ce40e97acc7eefe9e1332cfc30b9b37ed339e2b15f9d2f286d43
c10f2c835c7b9aabab21022be8bef05974aa563c1ee773690d00e06c67ef28db
c151cea2cdebfbc4ca982ec6d0bed35f2d112992380d7fed3679782e8d8fba55
44dc3f4feca316d217b1eb9f4203bfc59b9cf58d65e490ba5a544a6639947377
4906acf501d299fefc4e421439b63f26e6c6be56d631a3586603f0389558ac53
5eac3c5481b0d21052e727066ac5529083e14cc732a71c6b82401a71c0a43789
96c68f304f4fe0f20f1fedadac2f741322ca0074534bad524107428e24316ea0
a2b3bb5a3c1f16b5e4aef21adcd63efa0031657a4202e1048d4f5d91a56a1bbb
284cf9bde63d704bd635279d890d5543a9e23d5a4d121fc3d4fdb82de8cffaad
ca7359a1eb60a8afa930e10890eb37b49410a56f6dbb582d9eb0489c10439c78
d4d7670275ac8f122dea944b3a391844b3844c7f9bcb3518ff73e3399938d605
cdab1c3196887d4f749d82f014786a966c87f35a7189f0f3d078558b957847bf
1a6be5ba156a951fd8a3f601d0fdc9bc698dd723b87b1e4951d89edf4a9567f2

Indicator of compromise

Domain Name

waconazure.com
tvlicenses.uk.to
skattemelding.hs.vc
s53yq.skalet.com
javastore.ignorelist.com
.chickenkiller.com
gitpi.3tec.de
mooo.com
chickenkiller.com
ecarited.strangled.net
doughouzscripts.com
chickenkiller.com
slumbo.com
youramys.com
sojda.org
discord.gg
clamav.net
bitdefender.com
aaa.com
microsoft-support.net
coursatapp.ds-deploy.online
web.danger.net
dan.danger.net
report.opennicproject.org
729t.com
729p.com
726q.com
microsoft-support.net
diankeyi.com
ds-deploy.online
twtfibra.com.br
multien.com.br
danger.net

Indicator of compromise

SHA-1

9d1ae8af9a8524c385a0aa41fb5bcdf047569f6c
33008f85428a83996083c3da92a8f00595071403
e290c6a50a5a9091ee3cb8f4d8a4059654ca73d7
b5c90950f82914442757ce192096a8f6d7927e46
82714fa4e21cff4e1c9bb4f0ecbad6073f1121e4
2a219eadb234eb09a9ede1594d68da0f294287ba
33008f85428a83996083c3da92a8f00595071403
e290c6a50a5a9091ee3cb8f4d8a4059654ca73d7
b5c90950f82914442757ce192096a8f6d7927e46
82714fa4e21cff4e1c9bb4f0ecbad6073f1121e4
49470bd1e38c6b05854dd141a49ae960a66f3d66
33008f85428a83996083c3da92a8f00595071403
e290c6a50a5a9091ee3cb8f4d8a4059654ca73d7
b5c90950f82914442757ce192096a8f6d7927e46
82714fa4e21cff4e1c9bb4f0ecbad6073f1121e4
49470bd1e38c6b05854dd141a49ae960a66f3d66

Indicator of compromise

MD5

00735e542bd4f66661c7feede2b7dba9
565ea459b6f97702f8b0ed0f0e268d80
fac1ec40eea5a4fc05f17e019328e287
764afcd2883ce9fa65be47acb8bf1451
7b312740cb1f3ccde60c8a5b3630d191
68f010c6fb4fe41401157f619fa68090
30fd67826c90600f371459578fb21e6f
41721e0f933696d50ab32d544d64dcd3
b7c999040d80e5bf87886d70d992c51e
fac1ec40eea5a4fc05f17e019328e287
764afcd2883ce9fa65be47acb8bf1451
7b312740cb1f3ccde60c8a5b3630d191
68f010c6fb4fe41401157f619fa68090
00735e542bd4f66661c7feede2b7dba9
392092eb1f915096fdf44313b56f093e
6883db983c6f6d8c4c36e15e66305c86
fac1ec40eea5a4fc05f17e019328e287
764afcd2883ce9fa65be47acb8bf1451
7b312740cb1f3ccde60c8a5b3630d191
68f010c6fb4fe41401157f619fa68090
41721e0f933696d50ab32d544d64dcd3
b7c999040d80e5bf87886d70d992c51e
803d1df4c931df4f3e50a022cda56e29
9375cff0413111d3b88a00104b2a6676

Indicator of compromise

Remediation

1. Patch Management: Regularly update software to fix vulnerabilities.
2. Network Segmentation: Limit lateral movement in case of breach.
3. User Education: Train employees to recognize threats.
4. Network Monitoring: Detect and respond to suspicious activities.
5. Incident Response Plan: Have a plan to react swiftly to breaches.
6. Application Whitelisting: Allow only approved applications.
7. Secure Remote Access: Use MFA and VPNs.
8. Threat Intelligence Sharing: Stay informed about emerging threats.
9. Security Audits: Regularly test systems for vulnerabilities.
10. Backup and Recovery: Back up data regularly and securely.
11. 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/