# KPMG Cyber Threat Intelligence Platform

**Bronze Sandcastle - Deploys Custom Meterpreter Backdoor**

**TLP :** Clear

**KPMG. Make the Difference.**



**Bronze Sandcastle is a China-aligned cyber-espionage threat cluster active since at least 2025. The group is known for employing DLL sideloading and encrypted payloads, and has recently deployed modified Meterpreter-based backdoors. Bronze Sandcastle primarily targets organizations across Asia and Africa, with confirmed activity in the Philippines, Taiwan, Afghanistan, Namibia, and likely South Korea.**

Initial access methods attributed to BRONZE SANDCASTLE remain unknown, but the threat actor deploys legitimate applications alongside malicious DLLs to enable DLL sideloading and execute attacker-controlled code through trusted software, including Sandboxie, Java applications, Krita, NVDA, LINE, and Sysinternals utilities. For defense evasion, sideloaded DLLs read encrypted payloads from local files and executes them directly in memory, reducing disk artifacts. The malware decrypts payloads at runtime and executes a customized Meterpreter-based backdoor via reflective in-memory loading, leveraging obfuscated control-flow mechanisms. For discovery, the backdoor collects host, user, domain, operating system, process, and network information, while operators use Windows net commands to enumerate network, users, and system. For command and control, the malware leverages attacker-controlled infrastructure and trusted online services, including GitHub, file[.]io, gofile[.]io, and Ably, to receive tasking, retrieve configurations, and exchange data. For credential access, the they create Volume Shadow Copies using vssadmin.exe and copy the NTDS.dit database to obtain Active Directory credentials and domain information. The backdoor incorporates COFFLoader-derived and Beacon Object File capabilities for data and credential theft and post-compromise activities.

BRONZE SANDCASTLE's use of DLL sideloading and in-memory execution highlights the need for robust application whitelisting, memory forensics, and network traffic analysis.

### What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Restrict execution of untrusted binaries that load non-standard DLLs outside system directories.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

### KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context.

The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

| We offer a wide-range of services, including: |
|---|
| Strategic threat intelligence report |
| Machine ingestible threat intelligence feeds |
| Threat intelligence driven pre-emptive threat hunting exercise |
| Cyber Incident Response Services |

**KPMG in India Cyber Response Hotline: 1800 2020 502**

## KPMG in India contacts:


**Srinivas Potharaju**
Partner & HoF
Cyber Security & Tech Mgmt
**T:** +91 98459 19740
**E:** srinivasbp@kpmg.com

**Sony Anthony**
Partner & SSL-HoD
Cyber Defense and IR
T: +91 98455 65222
E: santhony@kpmg.com

**Rishabh Dangwal**
Partner
Cyber Defense and IR
T: +91 99994 30277
E: rishabhd@kpmg.com

**Abhishek Dashora**
Director
Cyber Defense and IR
T: +91 88671 86493
E: abhishekdashora@kpmg.com

kpmg.com/in


**Follow us on:**
**kpmg.com/in/socialmedia**


The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

# KPMG Cyber Threat Intelligence Platform

## Bronze Sandcastle - Deploys Custom Meterpreter Backdoor

**TLP :** Clear

**KPMG. Make the Difference.**



### Indicators of Compromise: Domain

| |
|---|
| net.dpworldto[.]com |

### Indicators of Compromise: Hashes

| |
|---|
| 0a7464945e1994a7fc5ee2b86ce48c94 |
| 5ac863a8bffbcca5647284e088d401dc |
| 0ff9ecbaf18e45cd7b4943b21d5c6cf1 |
| e43a7c1169cf1d4ce8b22c1301ca100c |
| a0fa0893e1adde6b93063ab2c7369536 |
| 4cf187200a4e639e314b7f96a33f161e |
| f771159881bc82217d30a64a7716e613 |
| 32151547d912488ac5242731057170a3 |
| 2a39552543f84aa3a7a562d9bb54fc00 |
| 3addd7c803b9570fc0b1ee6899444c66 |
| 8c32bf3711b237e3c781a00b5c526695 |
| 4e916e024ea0c0eb16bd91f054d22444 |
| 5910e874fccc9b37239b00b993393994 |
| ebf221383c234ea2361ed54e6df6ddfc |
| c15c10589e671094185311e358b8903b |
| b695542718a7cc373112852d97d1811e |
| dd89cfd1f0b13addfc43cae758130b6a |
| e63ec733393e4e7e3424cbff918003a3 |
| 2f399541445cc1aade0e7a2148853fe41be57827 |
| 0ed62f00b9e7c5780c9bd05b096eee13a160480f |
| 8964de054bfb70c5560ebabe224bb45723f60b37 |
| 120d204d253293d594d6fcbe681797942fb74f7a |
| 1abe25d3255679bdc1c35c070da40e3c4572bb4a |

**Follow us on:**
**kpmg.com/in/socialmedia**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

# KPMG Cyber Threat Intelligence Platform

## Bronze Sandcastle - Deploys Custom Meterpreter Backdoor

**TLP :** Clear

**KPMG. Make the Difference.**



| Indicators of Compromise: Hashes |
|---|
| 1fc7350e215759b4d66ab6458244271b5e2cfa90 |
| 624da53bd827ca27b66d8a42a9524b0b48e882b4 |
| 24ede364f5eabe991c866e92ffa396bcb894eb14 |
| 536d6a8fa98a566079a459b16df1e29622dd8af5 |
| 56b1258c4553fb549fca9215727be1e5cd1efe4e |
| 4e6d600ce7a9cf6414e738d8f39260ae961602f0 |
| ffe58ea274af642a3fc1d50e823cb01f61dc8dae |
| ffd5cfbd5274a351315ba1e922d795f872f7ff9b |
| ab86a6b71582e16a7da14533fe9407d7a2bc525c |
| 6204c6342c5dfb67bdc29d45a524c3ac3a99aa01 |
| c2811a0fa539e4cd6633f32349fb34b0455bcba6 |
| f7db825aeee21d6326fa9c31512d090720546341 |
| cd1a262f8c2624700440b0aa464b7a2b42e23511 |
| 2411a678e4de91451e69c27369bab4329c3cd969d4ebd851ba91dcfdba7e7db2 |
| e50dc9db568c272d7b019ec8e5fb1f111dd071baa4b3a00bc3c8c885ade46fbc |
| e404b2b9f9f203dad81bdc1ef8bfcbe4f42eb616f113a89ed504202212af1c1e |
| fdef7b1f4c013d686bf5dbfc92f37191c04beb0dc8b53c608bb8019a8c678052 |
| 72259376f63116d1aca64bf2ef42a5d211c1ebdb01516ef3b53778ed1347c238 |
| 91ef27b1e83f324348ca51466ab17e2464f927b9c84758898fd7ce7ae6a6008b |
| 2332d924b1404961bc65280e782c787a4b048da7519fe73ccf4dc687b843d060 |
| 437ba4b0db084c261f7843f85329b5204a2dedecdacf29b25a53a90bcf8d7d2e |
| 548d5add2b27ab8c2d506b81623a37f3d27a0f4e22e6fa938c6a008b70775989 |
| 425177b18cb386f359796576e51666b7350489579550e564f51f8973b2f0979b |
| 592a6e74366bcd0c8a47657a88a6e81f99d2876baa6f923bb928bba4477054fc |
| dd9223c381893f493ca581e5bd35f16f778689e58fc459c1b0c39b0d33b41290 |
| c39ac4e1fe11639a9d46e026850cc3146eb809b542daf38e1a00eab11eaa1834 |

**Follow us on:**
**kpmg.com/in/socialmedia**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

KPMG

# KPMG Cyber Threat Intelligence Platform

## Bronze Sandcastle - Deploys Custom Meterpreter Backdoor



**TLP :** Clear

**KPMG. Make the Difference.**

| Indicators of Compromise: Hashes |
| --- |
| 5e2b035ae40f8eaab40792a92573171df0011c2fbed55582268a824effa7cb91 |
| c7f1c6cfd87e4c4f492a6da634ae6a264467aaee5a3eed14e89c2297a58e5d30 |
| 6c5c332428d914fd8eac0164947a70ec3d71bcd3f6cdcccb5e875dcb68ea076d |
| 7515417e523a776e371877e868536fa1d1961826d4bc478734be993985d9df03 |
| 95c6e9447585670b1a50551c36abe22154f6e010bfb23275fc467d2b20a423d9 |

**Follow us on:**
**kpmg.com/in/socialmedia**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.