# KPMG Cyber Threat Intelligence Platform

## Earth Estries : A Cyber Espionage Revelation

Operating since 2020, Earth Estries, an APT group shares similarities in tactics, techniques, and procedures to the FamousSparrow group. Earth Estries uses various malware such as Zingdoor, TrillClient, HemiGate & demonstrates high-level resources and expertise in cyber espionage. Leverage backdoors, stealers, and port scanners to enhance intrusion vectors. Organizations in the government and technology sectors of US, Germany, South Africa, Malaysia, Taiwan, and the Philippines are targeted by this ongoing campaign. Network traffic to C&C servers in Canada and toolset detections in India and Singapore also make these regions more vulnerable to attacks.

Gains initial access to an organization's internal servers through valid accounts with administrative privileges. Leverage DLL side loading technique to deploy remote control tools such as Cobalt Strike, PlugX, or Meterpreter stagers to ensure lateral movement. To deploy backdoors and toolsets in other machines within the network, they take advantage of SMB and WMIC. The attacker uses Zingdoor to capture and enumerate system information, TrillClient to steal data from web browsers, and HemiGate to log keystrokes, take screenshots, perform file operations, and monitor processes. After each deployment, they upload PDF and DDF files to online storage repositories, AnonFiles or File.io, using curl.exe. They also use PowerShell to evade the Windows AMSI logging mechanism and hide their actual IP address by using Fastly CDN service and abusing public services such as Github, Gmail, AnonFiles, and File.io to transfer commands and data.

Utilizes a variety of sophisticated techniques and tools in order to gain access to an organization's internal servers, deploy malware, and exfiltrate sensitive information. It is important for organizations to take proactive measures to secure their networks against such attacks.

### What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The 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 |

## Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471


**Atul Gupta**
Partner, Head of Cyber Security,
KPMG in India
**T:** +91 98100 81050
**E:** atulgupta@kpmg.com

**B V, Raghavendra**
Partner, KPMG in India
**T:** +91 98455 45202
**E:** raghavendrabv@kpmg.com

**Sony Anthony**
Partner, KPMG in India
**T:** +91 98455 65222
**E:** santhony@kpmg.com

**Chandra Prakash**
Partner, KPMG in India
**T:** +91 99000 20190
**E:** chandraprakash@kpmg.com

**Manish Tembhurkar**
Associate Partner,
KPMG in India
**T:** +91 98181 99432
**E:** mtembhurkar@kpmg.com

KPMG

# KPMG Cyber Threat Intelligence Platform

## Earth Estries : A Cyber Espionage Revelation

| Indicators of Compromise: IP Addresses | |
|---|---|
| 96.44.160[.]181 | 103.159.133[.]205 |

| Indicators of Compromise: Domains | |
|---|---|
| access.trhammer[.]com | cdn-7a3d[.]vultr-dns[.]com |
| east.smartpisang[.]com | cdn-6dd0035.oxcdntech[.]com |
| nx2.microware-help[.]com | web9a78bc52.trhammer[.]com |
| ms101.cloudshappen[.]com | cdn728a66b0.smartlinkcorp[.]net |
| shinas[.]global[.]ssl[.]fastly[.]net | zmailssl3[.]global[.]ssl[.]fastly[.]net |
| cloudlibraries[.]global[.]ssl[.]fastly[.]net | |

| Indicators of Compromise: Hashes |
|---|
| 6c3045560465c27cd845b004dde11c5e |
| 3216eeb5b4881bce2e65ad51f395a4ad |
| fe6f07e1b833700562bcd48523e7595c |
| a05fbf72be2e4e7777ac1ae966642164 |
| f7366a26fcc403fa60c2c69c6255e85c |
| ac5aa40bf6483ec4bfc07a98f06df5f9 |
| c9166a880f6f92013e7714f20c2e357b |
| 1579ec612e222d16ea4491041d78531c |
| 99fb505deddd2d8b191d30f0e0db6d1e |
| c0f9813502cec3c991f5e0d75d0ec06d |
| 474ac609331dd098179fed0002af4374f850c5ab |
| ecf06c8ec81ed8f5b5802f8a6e8f21ebe5676105 |
| c043d69f9ab853472e7893411d3e31490f6571ad |
| 62670bd17f6f665efad5aa39cd202caaf48c92b8 |
| cf897c6c7bcd4a468db3499d966cff0303842d93 |
| 27a66670cc6025eabe0e0fc795c5ac9b118e809a |
| 4f1dcc7c083c3bddb2fbef1f5e96311bcef0c490 |
| 12c39258e0f1882284795da43bdf4495646379d6 |
| c5b28644be2b26c10de897bafe7a471e1ba0e645 |
| 96cc45d35c9c827db2ef05354d7671ef1e5b2811 |
| cd2b703e1b7cfd6c552406f44ec05480209003789ad4fbba4d4cffd4f104b0a0 |
| 0eaa67fe81cec0a41cd42866df1223cb7d2b5659ab295dffe64fe9c3b76720aa |

KPMG

# KPMG Cyber Threat Intelligence Platform

## Earth Estries : A Cyber Espionage Revelation

| Indicators of Compromise: Hashes |
| --- |
| e6f9756613345fd01bbcf28eba15d52705ef4d144c275b8cfe868a5d28c24140 |
| c7023183e815b9aff68d3eba6c2ca105dbe0a9b05cd209908dcee907a64ce80b |
| 1a9e0c7c88e7a8b065ec88809187f67d920e7845350d94098645e592ec5534f6 |
| efb98b8f882ac84332e7dfdc996a081d1c5e6189ad726f8f8afec5d36a20a730 |
| 8476ad68ce54b458217ab165d66a899d764eae3ad30196f35d2ff20d3f398523 |
| dff1d282e754f378ef00fb6ebe9944fee6607d9ee24ec3ca643da27f27520ac3 |
| 42d4eb7f04111631891379c5cce55480d2d9d2ef8feaf1075e1aed0c52df4bb9 |
| 45b9204ccbad92e4e5fb9e31aab683eb5221eb5f5688b1aae98d9c0f1c920227 |
| 98e250bc06de38050fdeab9b1e2ef7e4d8c401b33fd5478f3b85197112858f4e |
| b1bc10fa25a4fd5ae7948c6523eb975be8d0f52d1572c57a7ef736134b996586 |
| 49a0349dfa79b211fc2c5753a9b87f8cd2e9a42e55eca6f350f30c60de2866ce |
| 71a503b5b6ec8321346bee3f6129af0b8ad490a36092488d085085cdc0fc6b9d |
| 28109c650df5481c3997b720bf8ce09e7472d9cdb3f02dd844783fd2b1400c72 |
| a8dd0ca6151000de33335f48a832d24412de13ce05ea6f279bf4aaaa2e5aaecb |
| deaa3143814c6fe9279e8bc0706df22d63ef197af980d8feae9a8468f441efec |
| eeb3d2e87d343b2acf6bc8e4e4122d76a9ad200ae52340c61e537a80666705ed |
| 4b014891df3348a76750563ae10b70721e028381f3964930d2dd49b9597ffac3 |
| 2531891691ef674345f098ef18b274091acdf3f2808cca753674599c043ccd7d |
| c59e17806e3a58792f07662b4985119252c8221688084d20b599699bfdb272d8 |
| e1a7e5f27362aaf0d12b58b96a816ef61a2a498def9805297aa81f6f83729230 |
| ca6713bedbd19c2ad560700b41774825615b0fe80bf61751177ffbc26c77aa30 |
| cdadad8d7ced1370baa5d1ffe435bed78c2d58ed4cda364b8a7484e3c7cdac98 |
| 82f3384723b21f9a928029bb3ee116f9adbc4f7ec66d5a856e817c3dc16d149d |
| 415e0893ce227464fb29d76e0500c518935d11379d17fb14effaef82e962ff76 |
| f6223d956df81dcb6135c6ce00ee14d0efede9fb399b56d2ee95b7b0538fe12c |