KPMG

KPMG Cyber Threat Intelligence Platform

EggStreme Malware – Fileless Espionage Targeting Southeast Asia

TLP : Clear

KPMG. Make the Difference.

EggStreme is a newly identified fileless malware framework attributed to a Chinese APT group, discovered in 2025 following a breach of a Philippine military entity. Their advanced toolset enables persistent, stealthy access via in-memory code injection, leaving minimal forensic evidence. Its advanced techniques indicate a long-term espionage focus on Southeast Asia, with the Philippines as a primary target due to its geopolitical importance.

Initial access occurs via a logon script from an exposed SMB share, deploying a legitimate Windows binary and a malicious DLL to the user's AppData or a similar directory. The binary uses DLL sideloading to load the DLL as a first-stage loader called EggStremeFuel, which fingerprints the system, opens a reverse shell via cmd.exe, and contacts a command-and-control (C2) server. Persistence is achieved by installing EggStremeLoader as a service, modifying the ServiceDLL registry key, or replacing service binaries to survive reboots. EggStremeLoader decrypts an on-disk payload containing a reflective loader and the core implant EggStremeAgent, both decrypted only in memory. EggStremeAgent is reflectively injected into trusted or elevated processes, avoiding disk writes and enhancing stealth. During each user session, EggStremeKeylogger is injected into explorer.exe to capture keystrokes, clipboard data, window titles, and other sensitive information. EggStremeAgent establishes a gRPC channel secured with mutual TLS, authenticating with certificates issued by a malicious certificate authority. It supports commands for file and registry manipulation, process injection, lateral movement using RPC and WMIC, and data exfiltration. A secondary backdoor, EggStremeWizard, enables fallback file transfer and alternate C2 access.

EggStreme's modular and fileless architecture highlights stealthy multi-stage intrusions, underscoring the need for defense-in-depth via behavioral monitoring and control over trusted binaries.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper the OEM and secure it with multi-factor authentication.
- 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:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

EggStreme Malware – Fileless Espionage Targeting Southeast Asia

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
103.103.0[.]225	103.169.90[.]164
103.131.95[.]114	103.78.242[.]128

Indicators of Compromise: Domains	
fetraa[.]com	traveldog[.]org
theuklg[.]com	fionamcleod[.]net
sinhluc[.]net	sealtribute[.]org
safiasol[.]com	powerontheroad[.]org

Indicators of Compromise: Hashes
0f37cd2f6b40649b82ba4f1921cd504b
5e3b763a9ba153edade783e8a0303177
df29898c0742f6b0175e4e34b5f0755d
16c95842bedc3c4d1df053ea9ae188d7
2a2900a9792f8020a9deda0d676fe989
7de52573ebe4073fa97fc72d9b6a9b7a
bf89b83267a9debc7b61ccb04cd329a5
e59eaab989c5a8433852e77fb9dd7986
a69908de2c1903afb41f0c7fb14162fd
0f45e73eccdb485e662c49fbd4821324
7392c09e0ac355e15b2d1236e62b6a57
537299a4e6c0f286c8a33fb444846a85
792005181a433afc9f7a8c230dcf4dfa
df2e68fe6be163d40a21b4199033b434
97bef0d9a2ad4249db2214fd43b5353a

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

EggStreme Malware – Fileless Espionage Targeting Southeast Asia

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
b9bd98484c186f47999bf328bb34794c
03ab706b45b1190c1f14059a2b443b13
a5fcd07b4cfba212af7e76fe88212ad7
c180e98725a466c3208e2c8874abc1ed
eb4948c42f418325c1b8b2b79af7ef08
8232e0c75f4ddc01cf846646f484ab43
3ca1b4542c44834839149e080e5c0498
63a4fbb304ce66ba2b8e87fae96ab35a
a43b957ef22072fc0b213989ab15560d
bae6b54f98bb23ddbb69487f8abfcd8c
7ec144401e983edbb5196699773c3660
a39d496e84f74c2ef5437389358f1521
95472a444f9b1120b7f31945202010c0
b7926de548c9c139dada2cff62cf3711
c1fdabb61c941053c2272c8c147670d1
e3d8fbf45fac3793aac87568a1919cf7
8843ff02ebc51afb3c3873d97c0b9846
aec8a3511907d8a27aa8082869ae80c4