THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Operation Cobalt Whisper

Threat Actor Malware

Description

Operation Cobalt Whisper

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Data Theft and Espionage
- Inhibit System Recovery

Security researchers have uncovered an ongoing cyber espionage campaign named **Operation Cobalt Whisper**, actively targeting high-value entities in Pakistan and Hong Kong. The operation has leveraged **Cobalt Strike**, a legitimate post-exploitation framework often abused by threat actors, to establish persistence and conduct surveillance.

This campaign demonstrates a high degree of sophistication, employing **obfuscated VBScript** and **malicious LNK payloads** to facilitate in-memory execution of the Cobalt Strike beacon.

THREAT OVERVIEW

- Initial Attack Vector: Delivery of malicious RAR archives via multiple platforms containing decoy files and LNK-based loaders.
- Tactics, Techniques, and Procedures (TTPs):
  - Use of malicious VBScript and LNK shortcuts
  - Execution via batch scripts that decode and launch Cobalt Strike in memory
  - Use of decoy documents to evade suspicion
  - Establishment of command-and-control (C2) via the decoded payload
- Artifacts Identified:
  - Over 30 decoy files used for social engineering
  - Malicious LNK file triggering a batch script for beacon execution

Indicator of Compromise

MD5

85144918f213e38993383f0745d7e41e
54b419c2cac1a08605936e016d460697
85144918f213e38993383f0745d7e41e

SHA-1

a6dcdfc8e97616c07549290950e78b145883e532
1b06e877c2c12d74336e7532bc0ecf761e5fa5d4
a6dcdfc8e97616c07549290950e78b145883e532

SHA-256

e6cfae572f777def856878e36bbacfaa82cb5662fc97c1492e2367a105dddbc9
d53346b5c8c6c76e7bc0407410a58328a1e214a4d359e558380963d29a35f71b
e6cfae572f777def856878e36bbacfaa82cb5662fc97c1492e2367a105dddbc9

Remediation

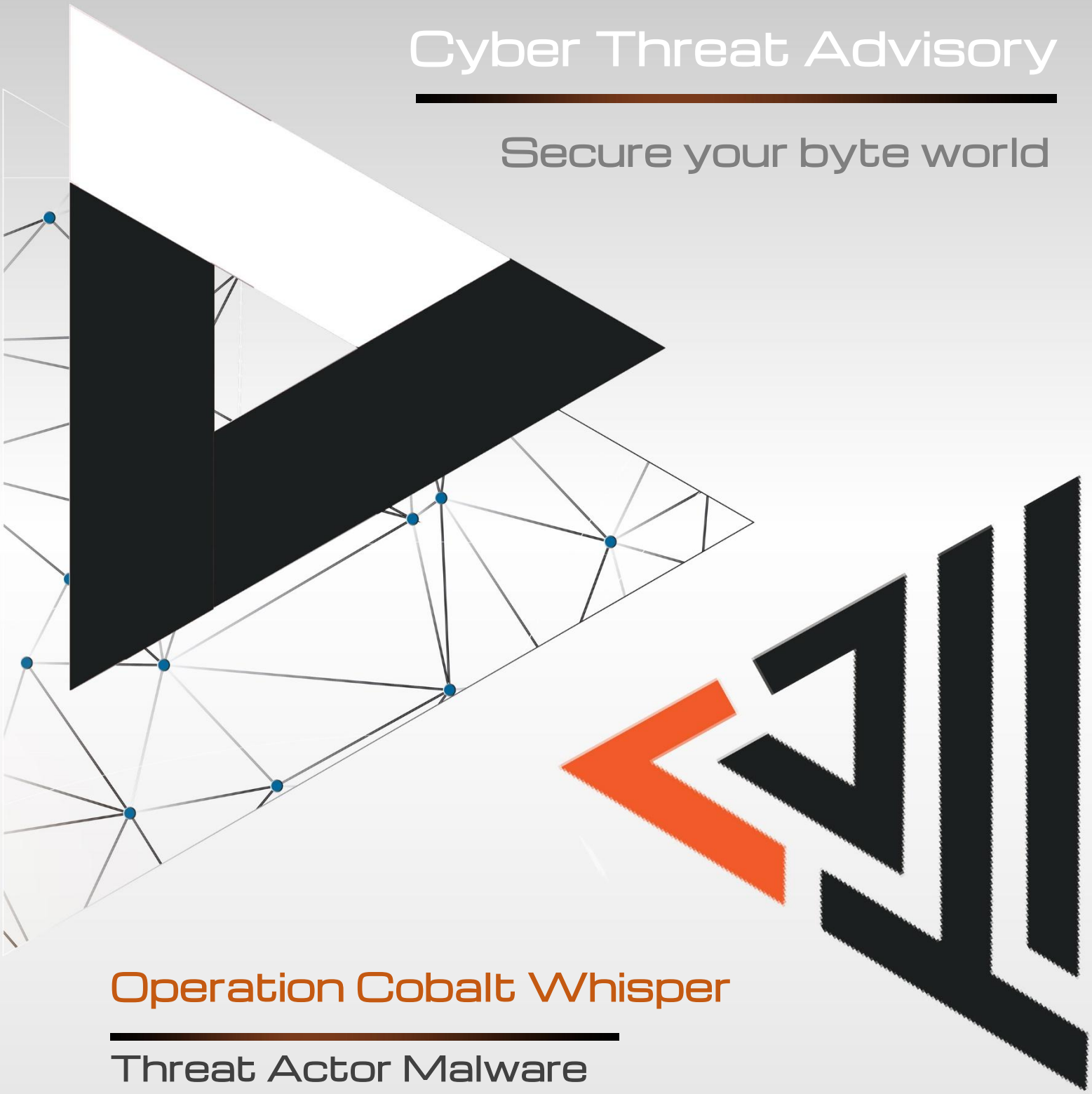
- Block Execution of Scripting Languages (VBScript, PowerShell) where not needed.
- Monitor LNK File Execution across endpoints for anomalies.
- Inspect Inbound RAR Archives and block unsolicited compressed file types.
- Threat Hunting for Cobalt Strike IOCs and memory-resident beacons.
- Educate Users on risks of opening unknown documents or shortcut files.
- Block all IOCs.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world



Operation Cobalt Whisper

Threat Actor Malware