KPMG Cyber Threat Intelligence Platform

NightSpire : Emerging Ransomware Targeting Manufacturing Firms

TLP : Clear

KPMG. Make the Difference.

NightSpire, a financially motivated ransomware group, emerged in early 2025, targeting organizations across various sectors, with a notable focus on manufacturing. The group primarily targets small to medium-sized businesses, exploiting them opportunistically. Initially focused on data exfiltration and extortion, NightSpire has transitioned to a double extortion model, encrypting victim data post-exfiltration, as observed in recent attacks. Operating a dark web leak site since 12 March 2025, NightSpire threatens to publish stolen sensitive information. On 10 April 2025, NightSpire compromised Nippon Ceramic, further underscoring its active targeting of manufacturing firms.

NightSpire gains initial access by exploiting vulnerable external services, such as firewalls and VPNs, notably leveraging CVE-2024-55591, a FortiOS zero-day discovered in late 2024. This vulnerability grants unauthorized super-admin access to FortiGate firewalls, enabling configuration changes that facilitate network access and lateral movement. To evade detection, NightSpire combines external tools, including living-off-the-land binaries (LOLBins) like network scanners and FTP clients, with legitimate processes within victim environments. For data exfiltration, the group utilizes legitimate tools such as WinSCP and MEGACmd to steal sensitive information. Additionally, NightSpire encrypts systems to enforce double extortion, locking data to disrupt operations. The group then posts victim data on its dark web leak site and intensifies pressure using tactics such as two-day payment deadlines and data sales to third parties.

NightSpire's aggressive exploitation of zero-days and adaptive double extortion tactics underscore the dynamic ransomware threat landscape, highlighting the critical need for heightened vigilance and robust defenses.

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.

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

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

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

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

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

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG Cyber Threat Intelligence Platform

NightSpire : Emerging Ransomware Targeting Manufacturing Firms

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes

0170601e27117e9639851a969240b959
7a4aee1910b84c6715c465277229740dfc73fa39
35cefe4bc4a98ad73dda4444c700aac9f749efde8f9de6a643a57a5b605bd4e7

Indicators of Compromise: Domain

a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion