KPMG

KPMG Cyber Threat Intelligence Platform

Gold Melody – Exploiting Vulnerabilities in Unpatched Servers

Gold Melody (aka UNC961 and Prophet Spider) is a financially motivated crime group that has been active since 2017. They have been exploiting vulnerabilities in unpatched internet-facing systems/applications like JBoss Messaging, Citrix ADC, Oracle WebLogic, GitLab, Citrix ShareFile Storage Zones Controller, Atlassian Confluence, Apache Log4j. Instead of state-sponsored espionage, they concentrate on opportunistic strikes for financial gain. They targets retail, healthcare, energy, finance, and high-tech sectors in various regions of North America, Northern Europe, and Western Asia. Their intrusion activities often precede Maze & Egregor ransomware distribution by other attackers, using a cost-effective approach targeting recent vulnerabilities.

Achieved initial access through unpatched vulnerabilities in publicly accessible software, including Apache Struts, Log4j, Oracle E-business, etc. Post access, they gathers system information by executing commands like 'whoami', 'ipconfig' & utilize tools like PwnTools, TxPortMap, pscan2. To ensure persistence, they use JSP web shells and the Perl-based IHS Back-Connect backdoor (bc.pl). They uses PowerShell commands to dump LSASS memory by using legitimate Windows DLL. They uses Mimikatz to dump credentials and manipulates Windows network protocols by using python script. For lateral movement, they connect to a domain controller to create an SMB connection and employ a Perl script to link two remote hosts, enabling shell access and remote command execution. For exfiltration, data was transferred from the domain controller to network's staging server, followed by the installation of the PuTTY Secure Copy Client.

To defend against threats like Gold Melody, organization should prioritize regular patch management, implement user privileges restrictions, and script whitelisting.

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

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 endeavor 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.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

Indicators of Compromise: IP Addresses	
149.28.193[.]216	23.227.203[.]214
149.28.207[.]216	209.141.61[.]225
149.28.207[.]120	195.123.240[.]183
64.190.113[.]185	104.149.170[.]183
107.181.187[.]182	107.181.187[.]184

Indicators of Compromise: Hashes
C6c1c3d7e25327a6d46039aa837491e5
B53063c59d999ff1a6b8b1fc15f58ffc
Ce76362104bd6d8c920a2a9c4cce3fe2
8addc16baeb0474d41ba2d3805665969
687157882f603897bf6d358d49a12064
711552fff3830d8e1bf99ff745b91b32
851aab4341e73f400ab0969cab29298d
Fd544bda416f0819df01b457d42888af
F7f4ca923b29964a8d081cea04db6f73
F02f4c22992830ee15fba7a4fbf9f26a
E7942dffdc98b9e32f1ec30e8e00c1f4
E787591a5ef810bfc9ecd45cb6d3d51e
B5bdeadf31fc968c9cc219e204115456
B20ba6df30bbb27ae74b2567a81aef66
A7a9a5676a1467ac8360b600e83eeae1
A3d5ead160614336a013f5de4cff65a5
9240e1744e7272e59e482f68a10f126f
8a69699df490e6c028cfe6a22340a827
64f2652fd9a907fd4cfc129a5556e97b
5cd4fd735e59f81d0c595b06ee61ad10
5adde740a47f88fceb845c8b1b236017
5286a79be3eb5a8a4a639aa9d1319f4f
4bc05be75e5c5e20e2beb58dea27127a
3e564d0ae79990368be84758e6b858a5
3e2ba059fe882ee4f8ec7ed2952ebee0
36128eefecb9fce9f4e4e9b5fb67957c
2dfe49db47d7e6ca0d7c5f3641da4911

KPMG Cyber Threat Intelligence Platform

Gold Melody – Exploiting Vulnerabilities in Unpatched Servers

Indicators of Compromise: Hashes
274edd99626cce95a06da525bb028e1f
198b1d73238a5b456f558e70b503f52e
0a3d502a5a5c8ea38124ec32dbf2247d
05d5fa365498651bcbb8a356cd580b25
F7f4ca923b29964a8d081cea04db6f732940b32b
3e564d0ae79990368be84758e6b858a5cd1cbfa4
274edd99626cce95a06da525bb028e1f0582936c
2dfe49db47d7e6ca0d7c5f3641da4911675baa25
3e2ba059fe882ee4f8ec7ed2952ebee0f014bc95
A7a9a5676a1467ac8360b600e83eeae18f91a663
5286a79be3eb5a8a4a639aa9d1319f4fdd1f45e8
Fd544bda416f0819df01b457d42888af64f2652fd9a907fd4cfc129a5556e97b
B5bdeadf31fc968c9cc219e2041154560a3d502a5a5c8ea38124ec32dbf2247d
36128eefecb9fce9f4e4e9b5fb67957c8a69699df490e6c028cfe6a22340a827
05d5fa365498651bcbb8a356cd580b255cd4fd735e59f81d0c595b06ee61ad10
A3d5ead160614336a013f5de4cff65a5198b1d73238a5b456f558e70b503f52e
F02f4c22992830ee15fba7a4fbf9f26ae7942dffdc98b9e32f1ec30e8e00c1f4
4bc05be75e5c5e20e2beb58dea27127a5adde740a47f88fceb845c8b1b236017