Hive Pro

THREAT ADVISORY

Pandora Ransomware Targets Multiple Plants around the Globe	TA2022058
Threat Level RED	**Publish Date –** Mar 16, 2022

Pandora ransomware is a new operation that targets business networks and obtains data for double-extortion assaults and active since March 2022. DENSO, a Japanese auto parts manufacturer's plant in Germany, and Global Wafers Japan, the world's third largest supplier of silicon wafers, both claim to have lost 1.4 TB and 1TB of data, respectively, as a result of this ransomware attack.

Attackers after gaining access to the infrastructure will do lateral movement through network to steal unencrypted files which can be further utilized in extortion demands. The ransomware will attach the '.pandora' extension to the encrypted file names. In addition to this, it will create ransom notes in every folder named 'Restore_My_Files.txt' that describes what happened to the device and provide an email address for victims to contact in order to negotiate a payment. A link to a data leak site used by the ransomware gang to execute their double-extortion activities is also included in the ransom notes. Due to code similarities and packers employed by the operation, this ransomware is suspected to be a rebrand of the Rook ransomware.

The Organizations can mitigate the risk by following the recommendations:

- Keep all operating systems and software up to date.
- Remove unnecessary access to administrative shares.
- Maintain offline backups of data and Ensure all backup data is encrypted and immutable.

The MITRE TTPs commonly used by Pandora are:

TA0040: Impact
TA0042: Resource Development
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0008: Lateral Movement
T1587: Develop Capabilities
T1587.001: Develop Capabilities: Malware
T1059: Command and Scripting Interpreter
T1055: Process Injection
T1070: Indicator Removal on Host
T1112: Modify Registry
T1027: Obfuscated Files or Information
T1027.002: Obfuscated Files or Information: Software Packing
T1021: Remote Services
T1486: Data Encrypted for Impact

Hive Pro

THREAT ADVISORY

Actor Details

Name	Target Locations	Target sectors	Motive
Pandora Ransomware Gang	Germany, Japan, USA	Automotive, Manufacturing, Technology, Finance	Ecrime, Information theft, and Financial gain

Indicators of Compromise (IoCs)

Type	Value
MD5	0c4a84b66832a08dccc42b478d9d5e1b
SHA-1	160320b920a5ef22ac17b48146152ffbef60461f
SHA-256	5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b

Recent Breaches

https://www.denso.com/global/en/
https://www.sas-globalwafers.co.jp/eng_index.html

References

https://www.securityweek.com/car-parts-giant-denso-targeted-ransomware-group
https://www.bleepingcomputer.com/news/security/automotive-giant-denso-hit-by-new-pandora-ransomware-gang/