Conti Ransomware
(CSB21-11)
September 24, 2021

Conti Ransomware, first observed on May 2020, is a private Ransomware-as-a-Service (RaaS) operation believed to be controlled by a Russian-based cybercrime group named as Wizard Spider. Conti ransomware has been identified to attack US healthcare, law enforcement agencies, emergency medical services, and 9-1-1 dispatch centers within 2020.

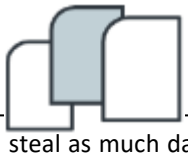
Like most ransomware variants, Conti Ransomware threat actors use the same methods of access found in many ransomware attacks, such as phishing emails with malicious links or attachments, stolen Remote Desktop Protocol (RDP) credentials, and exploiting unprotected internet-facing applications. These threat actors steal their victims' files and encrypts the servers and workstations in effort to force a ransom payment from their victims.

Conti's threat actors are observed inside their victims' network between four days and three weeks on average before deploying Conti ransomware, primarily using dynamic-link libraries (DLLs) for delivery. Threat actors fist use tools already available on the network and in case where additional resources are needed, these actors also use Trickbot. Once Conti actors deploy the ransomware, they may stay in the network and beacon out using Anchor DNS.

HOW IT WORKS

1. Threat actor either sends phishing email with malicious links or attachment or exploit vulnerable firewalls or any internet-facing RDP servers to gain access

2. Once the attacker has gained access to the network, they will try to gain access to a domain admin account, which will enable them to execute the ransomware code. They will also try to access any privileged accounts that will enable them to steal sensitive data.



3. The attackers will steal as much data as possible before executing the ransomware code. Threat actors either upload the files to their own server, to anonymous cloud servers, or send then via email.

4. Once threat actors have exfiltrated as much data as possible, deleted/encrypted backups, disabled relevant security features, they will initiate the ransomware attack and locks the computer from its user leaving a ransom note.

ITMS ISSD Computer Security Incident Response Team
2nd Floor ITMS Bldg Camp Crame, Quezon City
723-0401 loc 6546

www.itms.pnp.gov.ph
issd.itms@pnp.gov.ph

IMPACT

- Temporary or permanent loss of data.
- Interfere with the normal functioning of the computer system or prevent its utilization.
- Potential harm to the organization's reputation.

MITIGATIONS

- Do not pay the ransom.
- Remove infected computer within the network.
- Coordinate with IT Project Officer assigned in your office/unit.
- Perform a full system scan in safe mode to remove any infections.
- Implement network segmentation and filter traffic.
- Scan for vulnerabilities and keep software updated.
- Remove unnecessary applications and apply controls.
- Implement endpoint and detection response tools.
- Limit access to resources over the network, especially by restricting RDP.
- Ensure critical data are backed up, with backups stored offline and tested to ensure file recovery is possible.

PREVENTION

- Back up your files.
- Regularly update system, software, and applications.
- Block malicious executable, spam, phishing emails and other methods ransomware is known to use.
- Use Intrusion Detection/Prevention System (IDS/IPS).
- Add acceptable software and applications in whitelist and block unauthorized programs from running.
- Conduct trainings on how to identify and avoid common ransomware pitfalls or other related cybersecurity-related topics.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa21-265a