

DearCry Ransomware

Targeting the MS Exchange Exploit


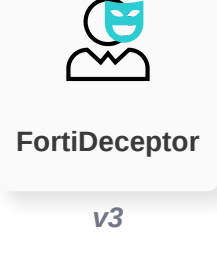
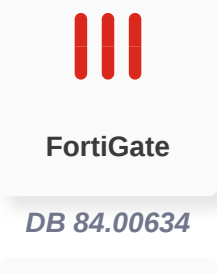
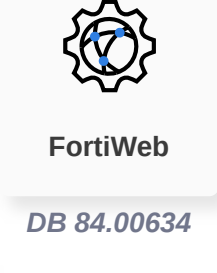
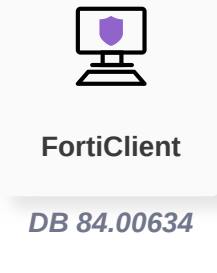

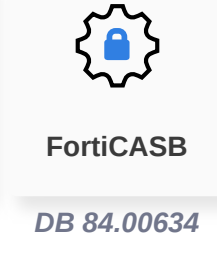
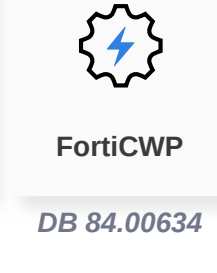
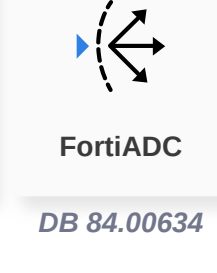
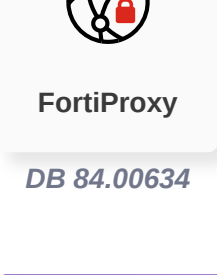
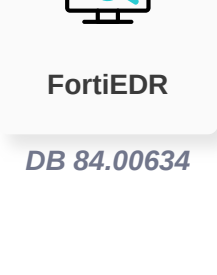
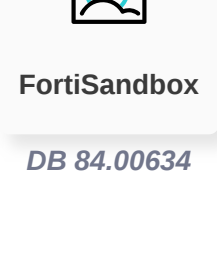
<https://twitter.com/MstfSecIntel/status/1370236539427459076>

Following initial compromise of the MS Exchange system, the attacker can execute the primary objective. From monitoring these incidents, a new family of ransomware has been detected. The threat is known as DoejoCrypt or DearCry.

- Background** Earliest detection of the MS Exchange vulnerability is covered in the MS Exchange Outbreak report.
- Announced** On March 11, Microsoft released the following announcement referring to the ransomware: <https://twitter.com/MstfSecIntel/status/1370236539427459076>
- Latest Developments** Refer to the FortiGuard Labs released the Threat Signal report: <https://www.fortiguard.com/threat-signal-report/3885/observed-in-the-wild-campaigns-leveraging-recent-microsoft-exchange-server-vulnerabilities-to-install-doejocrypt-dearcry-ransomware>

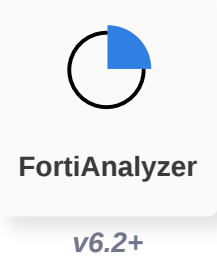

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance**
 - Lure**
A Deception Decoy that acts as a file server will detect the ransomware while encrypting the fake network drive share on the infected endpoint.

 - Decoy VM**
A Deception Decoy that acts as a file server will detect the ransomware while encrypting the fake network drive share on the infected endpoint.

- Weaponization**
- Delivery**
 - AV**
NGAV Detects & Blocks malware file transfers








 - AV (Pre-filter)**
Detected by pre-filter or scan engines, as this is a known ransomware.


- Exploitation**
- Installation**
- C2**
- Action**

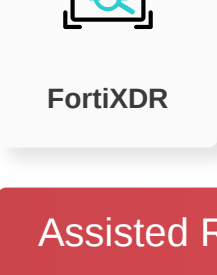
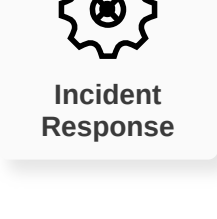
DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

- Outbreak Detection**

- Threat Hunting**


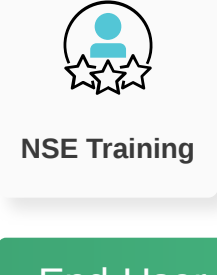
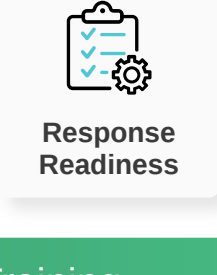

RESPOND

Develop containment techniques to mitigate impacts of security events:

- Automated Response**
Services that can automatically respond to this outbreak.

- Assisted Response Services**
Experts to assist you with analysis, containment and response activities.



RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

- NOC/SOC Training**
Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.
 
- End-User Training**
Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.


IDENTIFY

Identify processes and assets that need protection:

- Attack Surface Hardening**
Check Security Fabric devices to build actionable configuration recommendations and key indicators.


Additional Resources

Bleeping Computer <https://www.bleepingcomputer.com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/>

Learn more about [FortiGuard Outbreak Alerts](#)