



Emotet Malware Resurgence

First wave of the year 2023

<https://en.wikipedia.org/wiki/Emotet>

Emotet, a Trojan that is distributed via spam emails, has been prevalent since its first appearance in 2014. With a network made up of multiple botnets, Emotet has continuously sent out spam emails in campaigns designed to infect users via phishing attacks.

Background

The EuroPol has considered Emotet as one of the world's most dangerous malware. It was first discovered on year 2014 as a Banking Trojan. This report focusses specifically on the Emotet malware protection and IOC detections by the Security Fabric products.

Announced

March 7, 2023: After several months of inactivity, the Emotet botnet resumed email activity and was seen adopting new methods of evasion by using Microsoft OneNote attachments and archive bombs.

<https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/>

Latest Developments

November 16, 2021: Hundreds of Malware samples were flagged as VB/Dloader.BLG!tr.

March 23, 2022: FortiGuard Labs released threat research on Emotet. "MS Office Files Involved Again in Recent Emotet Trojan Campaign – Part II"

<https://www.fortinet.com/blog/threat-research/ms-office-files-involved-again-in-recent-emotet-trojan-campaign-part-ii>

April 18, 2022: FortiGuard Labs research on "Trends in the Recent Emotet Maldoc Outbreak"

<https://www.fortinet.com/blog/threat-research/Trends-in-the-recent-emotet-maldoc-outbreak>

March 20, 2023: Alert on resurgence of Emotet malware updated by JPCERT

<https://www.jpcert.or.jp/at/2022/at220006.html>

PROTECT

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

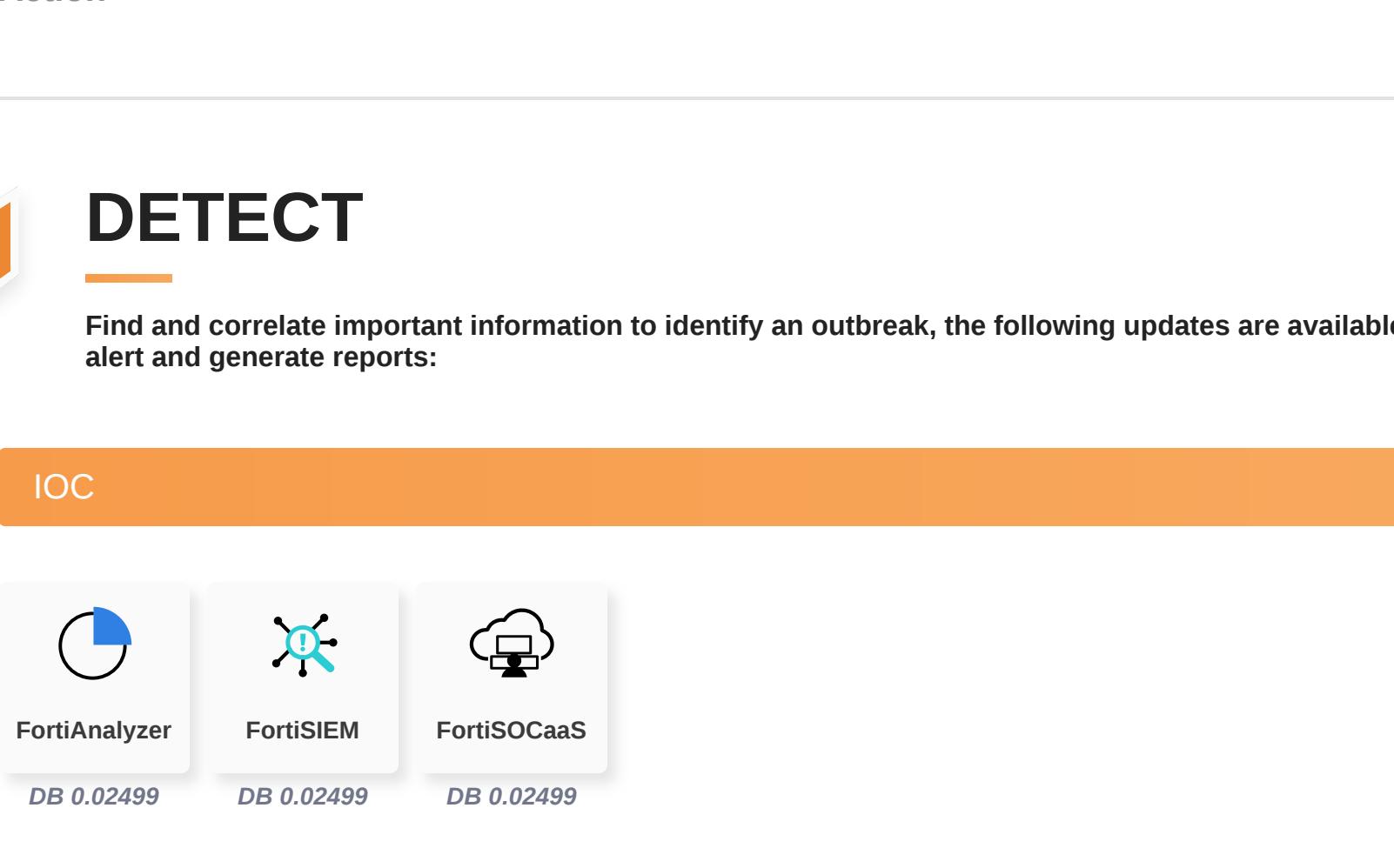
Reconnaissance

Weaponization

Delivery

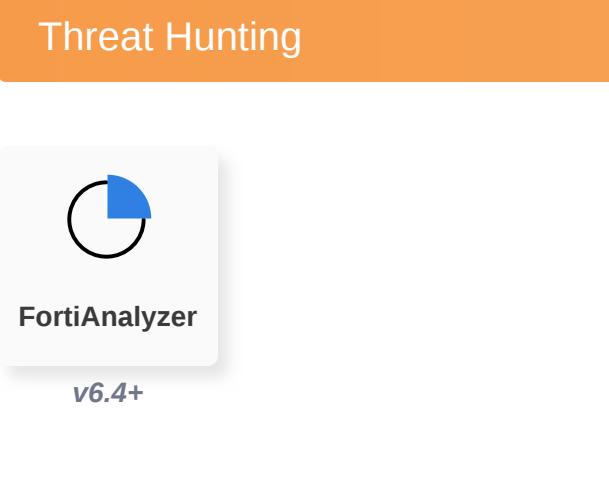
AV

Detects and blocks the Emotet payload



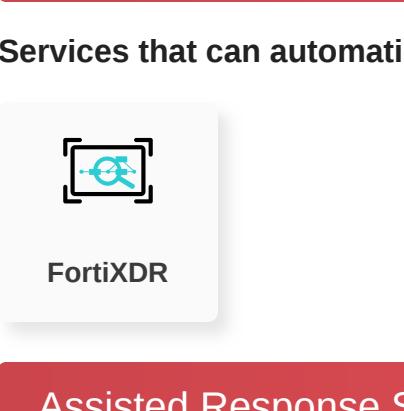
AV (Pre-filter)

Detects and blocks the Emotet payload



Behavior Detection

Behavior Detection Engine detects Emotet Malware as High risk and blocks 0day threats



Anti-spam

Detects and filters Spam from the Mailbox



Exploitation

Installation

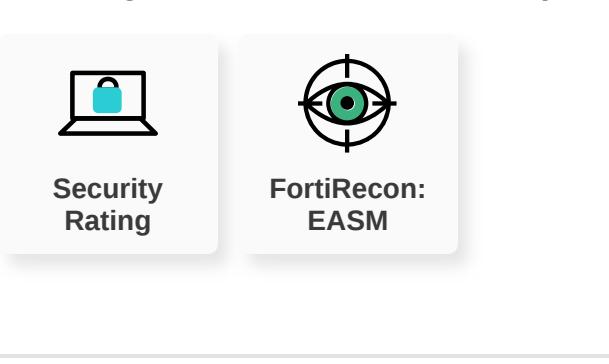
C2

Action

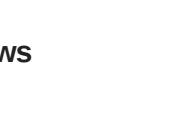
DETECT

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

IOC



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:

Incident Response

FortiRecon: ACI

RECOVER

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

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

FortiPhish

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating

FortiRecon: EASM

Additional Resources

CoFense

<https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus/>

The Hacker News

<https://thehackernews.com/2021/11/notorious-emotet-botnet-makes-comeback.html>

Dark Reading

<https://www.darkreading.com/threat-intelligence/emotet-returns>

Security Week

<https://www.securityweek.com/emotet-using-trickbot-get-back-game>

Security Week

<https://www.securityweek.com/malware-trends-whats-old-is-still-new/>

Bleeping Computer

<https://www.bleepingcomputer.com/news/security/emotet-malware-distributed-as-fake-w-9-tax-forms-from-the-irs/>

Learn more about [FortiGuard Outbreak Alerts](#)

