F#RTINET. **OUTBREAK ALERTS**

Prestige Ransomware

Targeting organizations in Ukraine and Poland https://www.microsoft.com/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Researchers at Microsoft Threat Intelligence Center (MSTIC) have identified evidence of a novel ransomware campaign targeting organizations in

the transportation and logistics industries in Ukraine and Poland. According to the report, the new ransomware labels itself with a ransom note of "Prestige ranusomeware".

Background

leveraging AprilAxe (ArguePatch)/CaddyWiper or Foxblade (HermeticWiper).

Prestige Ransomware has similar deployment techniques as previously used in recent destructive attacks

Announced FortiGuard has Antivirus detection coverage on the malware as W32/Filecoder.OMM!tr.ransom. The ANN and Sandbox behavioural detection engine detects the malware as high risk.

October 14, 2022: Microsoft Security released a blog:

Latest Developments

https://www.microsoft.com/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-andpoland/

events:

PROTECT

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

Reconnaissance

Decoy VM

FortiSASE

DB 90.06852

FortiMail

DB 90.06852

FortiCASB

DB 90.06852

DB 90.06852

Detect activities related to a Prestige ransomware malware protecting lateral movement on the network segment



Delivery AV

Detects Prestige ransomware payloads

FortiGate

FortiADC

DB 90.06852

DB 90.06852 DB 90.06852

FortiWeb

FortiProxy

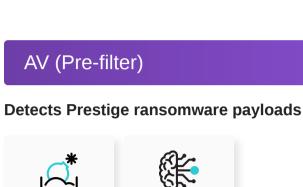
DB 90.06852

FortiNDR

DB 90.06852

FortiClient

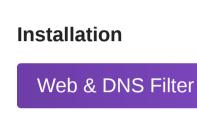
DB 90.06852



FortiSandbox

DB 90.06852

Exploitation



FortiGate

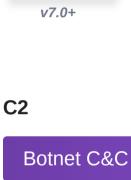
DB 26.44634

Anti-ransomware

FortiClient

Blocks suspicious process activity related to Prestige ransomware

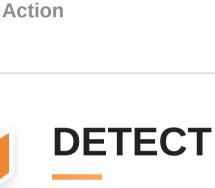
Detects known Urls, IPs and domains related to Prestige Ransomware



FortiClient

DB 3.00113

Detects traffic to known C&C domains



IOC

Outbreak Detection

alert and generate reports:

FortiAnalyzer FortiSIEM FortiSOCaaS DB 0.02355 DB 0.02355 DB 0.02355

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



v7.0+ **Content Update**

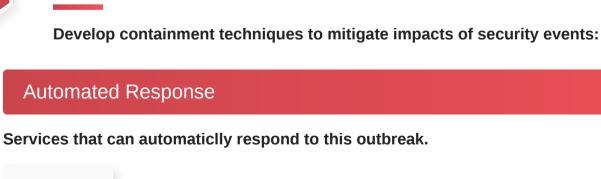
FortiSIEM

v6.4.0+

FortiEDR

FortiAnalyzer





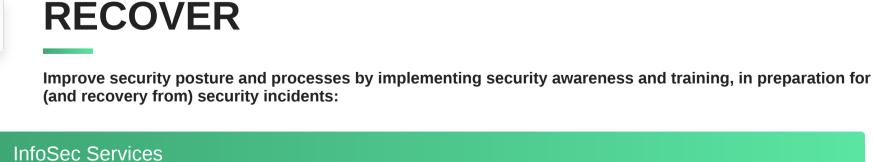
FortiXDR

Assisted Response Services

RESPOND

Incident Response

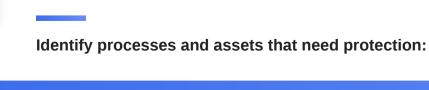
Experts to assist you with analysis, containment and response activities.



Response Readiness

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

IDENTIFY



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

Attack Surface Monitoring (Inside & Outside)

Security Rating

https://www.fortiguard.com/threat-signal-report/4808



Bleeping Computer https://www.bleepingcomputer.com/news/security/microsoft-new-prestige-ransomware-targets-orgs-in-ukraine-poland/

SecurityWeek https://www.securityweek.com/new-prestige-ransomware-targets-transportation-industry-ukraine-poland **The Hacker News** https://thehackernews.com/2022/10/new-prestige-ransomware-targeting.html

Learn more about FortiGuard Outbreak Alerts





