FORTINET

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 ransomware".

Background

Prestige Ransomware has similar deployment techniques as previously used in recent destructive attacks leveraging AprilAxe (ArguePatch/CaddyWiper or Foxblade (HermeticWiper).

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.

Latest Developments

October 14, 2022: Microsoft Security released a blog: https://www.microsoft.com/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

PROTECT

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

Reconnaissance

Decoy VM

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

FortiDeceptor
v3.3+

Weaponization

Delivery

AV

Detects Prestige ransomware payloads

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 90.06852	*DB 90.06852*	*DB 90.06852*	*DB 90.06852*	*DB 90.06852*	*DB 90.06852*	*DB 90.06852*

FortiADC	FortiProxy
DB 90.06852	*DB 90.06852*

AV (Pre-filter)

Detects Prestige ransomware payloads

FortiSandbox	FortiNDR
DB 90.06852	*DB 90.06852*

Exploitation

Installation

Web & DNS Filter

Detects known Urls, IPs and domains related to Prestige Ransomware

FortiGate
DB 26.44634

Anti-ransomware

Blocks suspicious process activity related to Prestige ransomware

FortiClient
v7.0+

C2

Botnet C&C

Detects traffic to known C&C domains

FortiClient
DB 3.00113

Action

DETECT

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

IOC

FortiAnalyzer	FortiSIEM	FortiSOCaaS
DB 6.02355	*DB 6.02355*	*DB 6.02355*

Outbreak Detection

FortiAnalyzer
DB 1.00068

Threat Hunting

FortiAnalyzer	FortiSIEM	FortiEDR
v7.0+	*v6.4.0+*	

Content Update

FortiSIEM
DB 307

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

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

Incident Response

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

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

Additional Resources

FortiGuard Threat Signal	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

FORTINET