

## Microsoft Signed Driver Malware

### Ransomware attackers leverage Microsoft-Signed Drivers

<https://msrc.microsoft.com/update-guide/vulnerability/ADV220005>  
 CVEs: TBA

Microsoft disclosed on Tuesday (Dec 13, 2022) that drivers certified by Microsoft's Windows Hardware Developer Program were being used maliciously in post-exploitation activity and Microsoft Threat Intelligence Center (MSTIC) ongoing analysis indicates that the signed malicious drivers were likely used to facilitate post-exploitation intrusion activity such as the deployment of ransomware.

**Background** Since the malware drivers are signed by Microsoft, trust associated with signed drivers can be exploited by threat actors to facilitate large-scale software supply chain attacks. Previously, we have seen many instances of signed software/drivers been taken advantage of. Last year in 2021, the driver, called "Netfilter," signed by Microsoft was used by attackers to plant rootkit and in Dec 2020, another notable supply chain incident occurred after attackers planted a vulnerability on popular SolarWinds Orion platform. Full read at: <https://fortiguard.fortinet.com/outbreak-alert/solarwinds>

**Announced** Dec 13, 2022: Microsoft released security advisory <https://msrc.microsoft.com/update-guide/vulnerability/ADV220005>

**Latest Developments** Dec 14, 2022: FortiGuard Labs has released AV protections against "BURNTCIGAR" malware and its variants and recommends all customers to install the latest Windows updates and to ensure that anti-virus and endpoint detection engines are up to date with the latest signatures to prevent these attacks. Apart from virus detections, behavioral based detections are in place to alert on suspicious or malware like activities and overcome the implicit trust granted to Microsoft-signed binaries.

## PROTECT

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

### Reconnaissance

#### Decoy VM

Detects activities of Ransomware Malware related to Microsoft Signed Driver












**FortiDeceptor**  
v3.3+

### Weaponization

### Delivery




#### AV

Detects and block BURNTCIGAR Malware and its variants related to Microsoft Signed Driver

 <b>FortiGate</b> DB 90.08790	 <b>FortiWeb</b> DB 90.08790	 <b>FortiClient</b> DB 90.08790	 <b>FortiSASE</b> DB 90.08790	 <b>FortiMail</b> DB 90.08790	 <b>FortiCASB</b> DB 90.08790	 <b>FortiCWP</b> DB 90.08790
 <b>FortiADC</b> DB 90.08790	 <b>FortiProxy</b> DB 90.08790					


#### AV (Pre-filter)

Detects and block BURNTCIGAR Malware and its variants related to Microsoft Signed Driver

 <b>FortiEDR</b> DB 90.08790	 <b>FortiSandbox</b> DB 90.08790	 <b>FortiNDR</b> DB 90.08790
---	---	---

#### Behavior Detection

Behavior detection engine rates BURNTCIGAR Malware as Medium risk



**FortiSandbox**  
v4.0+

### 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

 <b>FortiAnalyzer</b> DB 0.02410	 <b>FortiSIEM</b> DB 0.02410	 <b>FortiSOCaaS</b> DB 0.02410
---	---	---

#### Outbreak Detection




**FortiAnalyzer**  
DB 1.00080

#### Threat Hunting

 <b>FortiAnalyzer</b> v6.4+	 <b>FortiSIEM</b> v6.6+
--	--

#### Content Update



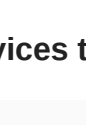
**FortiSIEM**  
DB 402

## RESPOND

Develop containment techniques to mitigate impacts of security events:

#### Automated Response


Services that can automatically respond to this outbreak.



**FortiClient Forensics**

#### 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

- Microsoft** <https://msrc.microsoft.com/update-guide/vulnerability/ADV220005>
- Microsoft Driver Blocklist** <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules>
- The Hacker News** <https://thehackernews.com/2022/12/ransomware-attackers-use-microsoft.html>
- Security Week** <https://www.securityweek.com/security-firms-warn-microsoft-signed-drivers-used-kill-edr-av-processes>
- Bleeping Computer** <https://www.bleepingcomputer.com/news/microsoft/microsoft-signed-malicious-windows-drivers-used-in-ransomware-attacks/>

Learn more about [FortiGuard Outbreak Alerts](#)