# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>MoonShadow</td>
<td>5</td>
</tr>
<tr>
<td>Phobos</td>
<td>6</td>
</tr>
<tr>
<td>Linda</td>
<td>7</td>
</tr>
<tr>
<td>Sheeva</td>
<td>8</td>
</tr>
<tr>
<td>Ritzer</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

Orion is an integral department in Cynet’s research team that works around the clock to track threat intelligence resources, analyze payloads, and automate labs to ensure that our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends identified in Bleeping Computer – the most up-to-date website that summarizes the newest ransomware variants – and shares how Cynet detects against these threats.
Cynet 360 AutoXDR™ VS Ransomware
MoonShadow Ransomware

- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .moonshadow
- Ransomware note: Decryption-Guide.txt | .hta
- Sample hash: ac2d92c801261e1887ad6a9dbbf52e08d9e3193976de096fb361597736a8c1ac

Cynet 360 AutoXDR™ Detections:

MoonShadow Overview

MoonShadow ransomware is supposed to rename the encrypted files with .moonshadow in the extension. Once a computer’s files have been encrypted and renamed, it drops a note as Decryption-Guide HTA.txt:

The ransomware note contains general information, warnings, and the attacker’s email address:

Orion Team
Phobos Ransomware

- Observed since: late 2017
- Ransomware encryption method: AES
- Ransomware extension: .decrypt
- Ransomware note: info.txt
- Sample hash: e63bfc04792f9f4b921ef182b83f03a5212f061a7c7d8cfe3c51f4fbc0032cba

Phobos Overview

Phobos ransomware renames the encrypted files with .decrypt in the extension:

Once a computer’s files have been encrypted and renamed, it attempts to drop the ransomware note named info.txt.

The ransomware note contains general information, warnings, and the attacker’s telegram and email:
Linda Ransomware
- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .linda
- Ransomware note: !info.hta
- Sample hash: 307e8a3de3047022e27b1178e04f2ffce51a2c5a89767290e7326283bba71e6

Once a computer's files have been encrypted and renamed, it drops a note named INFO.HTA:

The ransom note contains general information, warnings, and the attacker's email.
Sheeva Ransomware

- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .sheeva
- Ransomware note: sheeva.txt
- Sample hash: 991d018090cfd0b39d562010abf24b169ed55bea2d1bfc304622e2ade3827d7

Once a computer's files have been encrypted and renamed, it drops a note as sheeva.txt:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's contact info:

Cynet 360 AutoXDR™ Detections:
Ritzer Ransomware

- Observed since: June 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .ritzer
- Ransomware note: read_it.txt
- Sample hash: fe5b33909638954acc556be872ee86f0e2a0a92f96eda41392f23d31e9221ff10

Ritzer ransomware renames the encrypted files with .ritzer in the extension:

Once a computer's files have been encrypted and renamed, it drops a note as read_it.txt:

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains instructions and the attacker's contact information:

```
We can decrypt all your files!

1) Write an e-mail to info@orionransomware.com. In case of no answer in 24 hours check your spam folder or write us to this e-mail: orion@orionransomware.com
2) Obtain Bitcoins (You have to pay for decryption in Bitcoins. After payment we will send you the tool that will decrypt all your files.)
```