SecureCircle®

DATA SHEET

Mitigate Ransomware Attacks

What is Ransomware?

Ransomware is a type of malicious software that threatens companies, usually by denying access to your data or threatening to publish the victims' data. The attackers demand a ransom from the victim with the promise to restore access to the information upon payment. One of the reasons for ransomware growth is the availability of ransomware as a service and ransomware kits on the dark web that can be purchased for as low as $175 and require little to no technical knowledge to deploy.

Categories of Ransomware

- Crypto ransomware encrypts valuable files on a computer, so users cannot access them. Ransomware looks for specific file extensions and encrypts the files. Files are encrypted, and the originals are deleted. Hackers notify the victim to pay the ransom.
- Locker ransomware doesn't encrypt files but locks the victim out of the device, preventing them from using it.
- Cybertheft ransomware steals data and threatens to publish it publicly
- Combination

Impacts of Ransomware

- Company downtime to reimage and restore devices to a working state
- Temporary or permanent loss of company data
- Company reputation & loss of customers
- Ransom fee. The highest reported cost from 2020 was $10m.
- Regulatory fines for losing regulated data such as GDPR

How SecureCircle Mitigates Ransomware

- SecureCircle persistently secures data at rest, in transit, and even in use.
- SecureCircle eliminates the cyber theft threat of having data published publicly. Hackers will not be able to

access the contents of any secured files. Even if the hacker steals a copy of a secured file, the hacker would need extensive time on a supercomputer to break the encryption of a single file.

- SecureCircle can log suspicious behavior such as rename, move, delete actions on files.

Log activity that can identify ransomware activity

- Secured Application accessing secured file
- Secured Application accessing unsecured file
- Unsecured Application accessing secured file
- Unsecured Application accessing unsecured file
- File system logs (rename, delete, copy, modify)
- Location data (data accessed by remote endpoints)

Based on logs, we can create alerts for application and file system activity such as:

- Any application trying to access the contents of a secured file during non-work hours
- Any application trying to access more than # secured files per minute
- Any application trying to access specifically monitored files
- Large or constant file system operations such as copy or rename
- Alert for presencse of common ransomware file extenstions. Examples of Ransomware file extensions: .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .LeChiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .HA3, .toxcrypt, .magic, .SUPERCRYPT, .CTBL, .CTB2, .locky or 6-7 length extension consisting of random characters
- Alert of known suspicious applications (MimiKatx, Microsoft Process Explorer, Process Hacker, IOBit Uninstaller, GMER, PC Hunter, network scanning apps)

Ransomware Growth

In Q4 2020, 70% of Ransomware attacks involved the threat to leak exfiltrated data (up from 43% the previous quarter)

Other Ways to Mitigate Ransomware

- Always have backup data that is isolated from standard devices and data traffic. At least you can roll back to the last known backup.
- Keep all operating systems and applications up to date with the latest security patches. Much ransomware and malware take advantage of known security issues that are resolved in the newest software version.
- Train and remind users on cyber hygiene and essential security awareness such as not clicking suspicious links and files.

SecureCircle Best Practices

- Install SecureCircle on every device. Ransomware often utilizes SMB/Samba to scan, read, and infect other devices on the network. Don't allow unauthorized applications the freedom to try to access secured data.

About SecureCircle

SecureCircle's Data Access Security Broker (DASB) delivers a SaaS-based cybersecurity service that extends Zero Trust security to data on the endpoint. At SecureCircle, we believe frictionless data security drives business value for our customers. Instead of relying on complex reactive measures, we simply secure data persistently in transit, at rest, and even in use. End users operate without obstacles, while data is continuously secured against breaches and insider threats.

SecureCircle.com

4701 Patrick Henry Drive | Building 19, Suite B, Santa Clara, CA 95054 | 408-827-9100