CYTRES

AntiCrypt Datenblatt

1. Übersicht und Spezifikationen

1.1. Aktuelle Situation

Die Bedrohung durch Ransomware und Cryptolocker hat in den letzten Jahren erheblich zugenommen. Diese schädliche Software verschlüsselt die Dateien ihrer Opfer und fordert ein Lösegeld für deren Entschlüsselung. Unternehmen und Einzelpersonen weltweit sind betroffen, was zu erheblichen finanziellen Verlusten und Datenverlusten führt.

CYTRES präsentiert mit AntiCrypt eine Lösung, die in Echtzeit Ransomware und Cryptolocker abwehrt und die ursprünglichen Dateien in Echtzeit wiederherstellt, wenn diese auf dem Gerät verschlüsselt oder gelöscht werden.

Dabei wird automatisch ein Backup der betroffenen Datei aus dem RAM wiederhergestellt, sodass der Systembetrieb nicht beeinflusst wird. Danach wird der Nutzer über den Angriff sofort benachrichtigt. AntiCrypt ist auch für KRITIS-Infrastrukturen geeignet und erfordert keine Internetverbindung.

1.2. Vorteile der Lösung

Effektive Erkennung und Abwehr: Die Methode ermöglicht eine schnelle und effiziente Erkennung und Wiederherstellung von Änderungen an Dateien, die durch Malware oder Ransomware verursacht wurden.

Sofortige Benachrichtigung: Der Nutzer wird im Falle eines erkannten Angriffs sofort benachrichtigt und kann bei Bedarf weitere Schritte (z.B. eine IT-Forensik) durchführen.

Einfache Implementierung: Die Methode kann relativ einfach implementiert werden und erfordert keine komplexe Infrastruktur.

Echtzeit-Wiederherstellung: Änderungen an Dateien werden in Echtzeit erkannt, wodurch AntiCrypt diese sofort wiederherstellen und damit die Verfügbarkeit der Infrastruktur schützen kann.

Keine Signaturen erforderlich: Die Methode benötigt keine Signaturen oder Updates, um neue Malware zu erkennen.

Früherkennung: Potentielle Bedrohungen können frühzeitig erkannt werden, bevor sie größeren Schaden anrichten.

Reduzierung von Fehlalarmen: Durch den Vergleich spezifischer Byte-Muster kann die Methode Fehlalarme reduzieren, die durch normale Dateiveränderungen verursacht werden.

Skalierbarkeit: Die Methode kann auf verschiedenen Systemen und Umgebungen skaliert werden, von Einzelrechnern bis zu großen Netzwerken.

Low-Level-Erkennung: Die Methode arbeitet auf niedriger Dateiebene, was es schwieriger macht, sie zu umgehen.

1.3. Limitierungen der Lösung

Speicherbedarf: Das Laden der alten Datei in den RAM kann bei großen Dateien zu hohem Speicherverbrauch führen.

Teilverschlüsselung: Wenn nur die Dateiheader verglichen werden, könnten Änderungen in späteren Teilen der Datei unbemerkt bleiben. Das ist allerdings ein Szenario, welches in der Realität eher im unteren Durchschnitt liegt (siehe "Fallstudien").

Nicht für alle Dateitypen geeignet: Bei bestimmten Dateitypen, die sich häufig ändern (z.B. Datenbanken) oder einen dynamischen Datei-Header haben, könnte die Methode Fehlalarme auslösen, weshalb diese Dateitypen von der Analyse ausgeschlossen werden (siehe "Unterstützte Dateiformate").

Speicher-Volatilität: Da RAM ein flüchtiger Speicher ist, können Daten verloren gehen, wenn das System neu gestartet oder ausgeschaltet wird.

Es geht im Grunde darum die Angriffsoberfläche zu reduzieren, wozu AntiCrypt massiv und messbar beiträgt. Alle möglichen Angriffsszenarien abzudecken wird niemals möglich sein. Für weitere Infos zur Abdeckung, siehe "Fallstudien".

1.4. Unterstützte Dateiformate

Aktuell liegt der Fokus auf typischen Dateitypen, die von Ransomware und Cryptolockern targetiert werden.

Das gezielte Monitoring auf Dateitypen reduziert die Wahrscheinlichkeit für False Positives massiv, da diese Dateitypen ein bestimmtes Header-Format vorraussetzen.

1.4.1. Vollständige Unterstützung

Dateityp	Unterstützung
doc	Vollständig
docx	Vollständig
xls	Vollständig
xlsx	Vollständig
pages	Vollständig
ppt	Vollständig
pptx	Vollständig
pdf	Vollständig
jpg	Vollständig
jpeg	Vollständig
png	Vollständig
gif	Vollständig
bmp	Vollständig
tif	Vollständig
tiff	Vollständig
psd	Vollständig
ai	Vollständig
eps	Vollständig
mp3	Vollständig
wav	Vollständig
wma	Vollständig
aac	Vollständig
ogg	Vollständig
flac	Vollständig
mp4	Vollständig
avi	Vollständig

Dateityp	Unterstützung
mov	Vollständig
wmv	Vollständig
flv	Vollständig
mkv	Vollständig
mpg	Vollständig
mpeg	Vollständig
3gp	Vollständig
zip	Vollständig
rar	Vollständig
7z	Vollständig
tar	Vollständig
gz	Vollständig
iso	Vollständig
exe	Vollständig
dll	Vollständig
sys	Vollständig
msi	Vollständig
jar	Vollständig
mdb	Vollständig
accdb	Vollständig
sqlite	Vollständig
rtf	Vollständig
wps	Vollständig
pps	Vollständig

1.4.2. Eingeschränkte Unterstützung

Die vollständigen Formate sind nur teilweise unterstützt. Um False Positives zu vermeiden, werden sie von der Analyse ausgeschlossen.

Dateityp	Unterstützung
sqlite	Teilweise
xml	Teilweise
sql	Teilweise

1.5. Fallstudien

Die nachfolgende Ransomware und die nachfolgenden Cryptolocker zählen mitunter zu den bekanntesten und weit verbreitesten Cryptolockern auf dem Markt. In der Tabelle wird dargestellt, welche Methode die jeweilige Software anwendet, und ob diese Methode durch AntiCrypt erkannt und blockiert wird.

Ransomware	Beschreibung des Schadens	Geschätzte Infektionen	Durch AntiCrypt blockiert
Locky	Verschlüsselt Dateien vollständig ohne Auslassen von Bytes.	Hunderttausende	Ja
CryptoLocker	Verschlüsselt Dateien vollständig und fordert ein Lösegeld.	Rund 500.000	Ja
TeslaCrypt	Zielt auf eine Vielzahl von Dateiformaten mit vollständiger Verschlüsselung ab.	Zehntausende	Ja
Cerber	Vollständige Dateiverschlüsselung, die auf Lösegeld abzielt.	Zehntausende	Ja
WannaCry	Verschlüsselt Dateien und nutzt eine Sicherheitslücke zur Verbreitung.	Über 200.000	Ja
Petya/NotPetya	Verschlüsselt den Master Boot Record und verhindert das	Zehntausende	Nein

Ransomware	Beschreibung des Schadens	Geschätzte Infektionen	Durch AntiCrypt blockiert
	Hochfahren des Systems.		
Bad Rabbit	Verschlüsselt Dateien und verbreitet sich durch gefälschte Adobe Flash-Updates.	Tausende	Ja
Jigsaw	Verschlüsselt Dateien und löscht sie nach und nach, bis Lösegeld gezahlt wird.	Tausende	Ja
SamSam	Zielgerichtete Angriffe auf Organisationen, Verschlüsselung kritischer Systeme.	Hunderte	Ja
Ryuk	Hochgradig zielgerichtete Ransomware, oft manuell eingesetzt.	Hunderte	Ja

1.6. Angriffsszenarien

Die nachfolgende Tabelle stellt dar, welche Angriffsszenarien durch AntiCrypt abgewehrt werden können, und welche derzeit außerhalb der Abdeckung liegen.

Szenario	Beschreibung	Durch AntiCrypt abgewehrt
Manipulation von Backup-Punkten	Ransomware deaktiviert oder löscht Schattenkopien und Backup-Dateien.	Ja
Temporäre Datei-Manipulation	Ransomware erstellt temporäre Dateien, verschlüsselt diese und tauscht sie gegen die Originaldateien aus.	Ja
Mehrschichtige Verschlüsselung	Ransomware verwendet mehrere	Ja

Szenario	Beschreibung	Durch AntiCrypt abgewehrt
	Verschlüsselungsschichten, um die Erkennung zu umgehen.	
Verschlüsselung im Speicher	Ransomware verschlüsselt Daten im Speicher und schreibt sie dann auf die Festplatte.	Ja
Datei-Löschung	Ransomware löscht Dateien nach der Verschlüsselung.	Ja
Volle Dateiverschlüsselung	Ransomware verschlüsselt die gesamte Datei, einschließlich des Headers.	Ja
Dateiumbenennung	Ransomware benennt Dateien um, nachdem sie verschlüsselt wurden.	Ja
Metadatenänderung	Ransomware ändert die Metadaten der Datei (z.B. Dateierstellungsdatum, letzte Zugriffszeit).	Ja
Teilveränderung der Datei	Ransomware verschlüsselt nur bestimmte Teile der Datei, möglicherweise nicht die ersten 20 Bytes.	Teilweise
MBR Verschlüsselung	Ransomware verschlüsselt den Master Boot Record (MBR) und verhindert das Hochfahren des Systems.	Nein
Fileless Ransomware	Ransomware agiert im Speicher des Computers und hinterlässt keine Dateien auf der Festplatte.	Nein
Ungeschützte Dateiformate	Einige Dateiformate haben flexible oder nicht standardisierte Header, die schwer zu überwachen sind.	Nein

1.7. Abgewehrte Verschlüsselungsalgorithmen

Verschlüsselungsalgorithmus	Typisch von Ransomware verwendet	Durch AntiCrypt abgewehrt
AES (Advanced Encryption Standard)	Ja	Ja
RSA (Rivest-Shamir-Adleman)	Ja	Ja
ECC (Elliptic Curve Cryptography)	Ja	Ja
Salsa20	Ja	Ja
ChaCha20	Ja	Ja
Blowfish	Ja	Ja
Twofish	Ja	Ja
Camellia	Ja	Ja
3DES (Triple Data Encryption Standard)	Ja	Ja
Serpent	Ja	Ja
CAST-128	Ja	Ja

2. Lizensierung

Die Lizensierung erfolgt über einen Lizenz-Manager, über welchen der Partner direkt gültige Lizenzen für seine Kunden erzeugen kann. Das Ablaufdatum der jeweiligen Lizenz gilt ab der Erzeugung. Das Volumen der verfügbaren Lizenzen lässt sich jederzeit erweitern.

Sobald die Gültigkeit einer Lizenz ihr Ablaufdatum erreicht hat, werden alle Sicherheitsmechanismen von AntiCrypt deaktiviert, bis der Nutzer seine Lizenz verlängert. Dazu muss der Nutzer ausschließlich die neue Lizenz in der Oberfläche eintragen und AntiCrypt ist sofort wieder mit den gespeicherten Einstellungen aktiv.

3. Installation

Die Installation erfolgt über einen lokalen Installer und erfordert keine Interaktion. Nach weniger als einer Minute wird die grafische Oberfläche von AntiCrypt geöffnet und erfordert eine Lizenzeingabe. Sobald eine gültige Lizenz

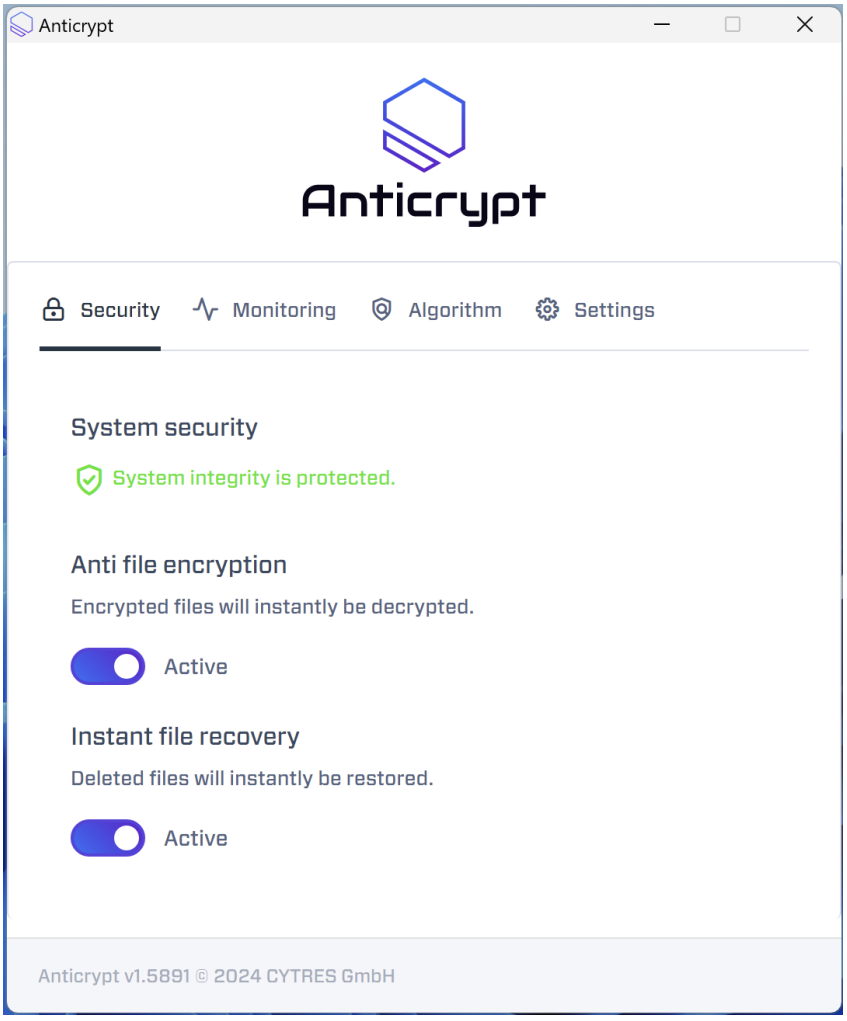
eingegeben wurde, ist die Software aktiv und bereit zur Verwendung. Auch eine Installation via UNC-Pfad ist möglich.

4. Einrichtung

Zur Einrichtung von AntiCrypt können die jeweiligen Verzeichnisse, welche geschützt werden sollen, über den Menüpunkt "monitoring" als Pfad hinterlegt werden. Danach ist das Monitoring für diese Verzeichnisse sofort aktiv.

5. Benutzeroberfläche

Die Verwaltung der Einstellungen erfolgt über eine grafische Benutzeroberfläche.



6. Einstellungen

6.1. Anti-Dateiverschlüsselung

Unter diesem Menüpunkt kann aktiviert/deaktiviert werden, ob verschlüsselte Dateien sofort wieder entschlüsselt werden sollen.

6.2. Sofortige Dateiwiederherstellung

Unter diesem Menüpunkt kann aktiviert/deaktiviert werden, ob gelöschte Dateien sofort wieder hergestellt werden sollen.