Ransomware: Viele Opfer, sehr wenige Lösungen

Die Neuauflage eines lukrativen Angriffs

Angriffe dieser Art sind seit langem bekannt und werden sehr häufig eingesetzt, da sie sehr lukrativ sind und sich schnell verbreiten – mit verheerenden Auswirkungen. Aktuell lässt sich wieder eine Zunahme dieser Bedrohung beobachten. Wie ANSSI berichtet, **ist die Zahl der Angriffe zwischen 2020 und 2021 um 37 % gestiegen**. Ebenso zeichnet sich ein zunehmender Trend zu Ransomware as a Service (RaaS) ab.

Bei Ransomware handelt es sich um Malware, die Daten als Geiseln nimmt.

Die erste Kategorie umfasst die klassische Ransomware, die thematisch an die Polizei angelehnt ist und **Ihren Browser einfriert** (als sogenannter Browlock) oder Ihren Computer vollständig lahmlegt.

Die zweite Kategorie beinhaltet Crypto-Ransomware oder Cryptoware. Diese Malware **verschlüsselt Dateien auf Ihrem Computer** und macht sie unlesbar ohne den Schlüssel zur Entschlüsselung, den jedoch nur die Angreifer besitzen.

Bei der letzten, neueren Kategorie **extrahieren Angreifer Daten mittels Malware** und drohen mit ihrer Veröffentlichung, sofern der Eigentümer kein Lösegeld in Form von Bitcoins zahlt.

7.000 Euro

Durchschnittliche Kosten eines Cyberangriffs

Quelle: Usine Digitale

Angriffe auf kritische Infrastrukturen zum Zweck der Sabotage bilden eine ständige Bedrohung.

LAUT DATOS101 **TRETEN RANSOMWARE-ANGRIFFE HEUTE 253 % HÄUFIGER AUF.**

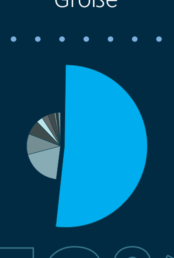
WIR SIND **ALLE IM FADENKREUZ**

Privatpersonen & Unternehmen aus allen Branchen und in jeder Größe

Gemäß eines Berichts von Hiscox **wurden fast zwei Drittel der Opfer von Ransomware mittels Phishing (65 %) geködert – weitaus mehr als bei der zweithäufigsten Methode, dem Diebstahl von Anmeldeinformationen (39 %).**

EINE AKTIVE UND VIELFÄLTIGE FAMILIE

...
GPcode (.AG, .AK)
LOCKBIT 2.0
TROJ.RANSOM.A
Archiveus
Krotten
RSA4096
Cerber
Cryzip
MayArchive
Petya
CryptoLocker
TorrentLocker
Cryptowall
TeslaCrypt
Locky Ransomware
KeRanger
CTB-Locker
WinLock
Reveton
Winwebsec
...



52 % der Opfer sind KMU.

Alle OS sind betroffen.

KERANGER
DIE ERSTE RANSOMWARE, DIE MACOSX-SYSTEME INS VISIER NAHM (2016).

CTB-LOCKER (VARIANTE)
ZIELT AUF WEBSERVER UNTER GNU/LINUX AB

HACKER-COMMUNITY
Die verschiedenen Ransomware-Kampagnen werden heute nicht mehr nur von einer einzigen Gruppe, **sondern durch mehreren Hackergruppen** durchgeführt.

ZIELGERICHTETE ANGRIFFE
Ein anschauliches Beispiel: Locky
Da Locky auf Unternehmen abzielt, erfolgt die Verbreitung über böswillige E-Mails in französischer Sprache (E-Mails mit gefälschten Rechnungen, kostenlosem Handy usw.). **Durch Personalisierung der E-Mails kann die Effizienz verdoppelt werden.**

CRYPTOWARES
Ransomwares werden immer schwieriger zu entschlüsseln, wodurch die Chancen sinken, Daten ohne Zahlung des geforderten Lösegelds wiederzuerlangen.

Innerhalb kürzester Zeit haben die Länge und Stärke der verwendeten Schlüssel erheblich zugenommen.

IMMER HÄUFIGER
Angriffe dieser Art treten immer häufiger auf (neue Angriffe oder Varianten).

EIGENE RANSOMWARE ENTWICKELN OHNE TECHNISCHE KENNTNISSE

RANSOMWARE-AS-A-SERVICE

Jetzt für jedermann verfügbar, ***denn die Generierung von Schadcode ist als Service im Dark Web verfügbar.***

WIE FUNKTIONIERT DAS?

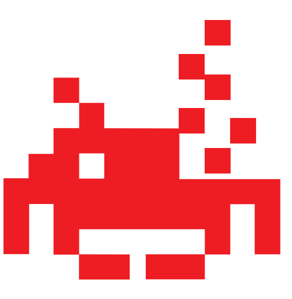
Mit sehr einfachen Schritt-für-Schritt-Tools können Hacker schnell ihre eigene Ransomware entwickeln. Sie vergüten den Anbieter dieses Service, indem sie ihm 25 % der durch die Angriffe erzielten Erlöse zahlen.

LOCKBIT 2.0

LockBit ist eine Gruppe von Cyberkriminellen, die ein Ransomware-as-a-Service-Modell (RaaS) anbietet.

Die Ransomware LockBit 2.0 entwickelt sich mit gezielten Angriffen in den USA, Kanada oder auch Europa kontinuierlich weiter.

Neuere Varianten nutzen das Modell der doppelten Erpressung: Zuerst werden Daten, lokalisiert und extrahiert, und anschließend die Systeme verschlüsselt.



Phase 1
Personalisierung

1. Die Hacker wählen **die Angriffsmethode**
   - [x] Sperre
   - [x] Verschlüsselung
   - [ ] Countdown
2. und senden **dann eine Nachricht:**
   Nachricht
   Ihre persönlichen Daten wurden verschlüsselt.
   Ihre Workstation wurde soeben gesperrt. Um Ihre Daten wiederzuerlangen, überweisen Sie 200 € an diese Adresse:
3. dann nennen sie **ihre Zahlungsdaten.**
   bitcoin

WEITERE INFORMATIONEN

Erfahren Sie, wie LockBit-Angriffe Infrastrukturen mittels **Datenextraktion und -verschlüsselung bedrohen –**

und wie Stormshield mit dem **Anti-Ransomware-Schutzbaustein seiner Lösung Endpoint Security Evolution darauf reagiert.**

Phase 2
Erstellung

4. Der Service **bereitet die Malware** je nach Wunsch vor.
5. Der Code ist **einsatzbereit.**
   </>

RANSOMWARES **WERDEN NICHT LÄNGER NUR PER E-MAIL VERBREITET.**

- eine manipulierte oder bösartige Internetseite,
- ein USB-Stick,
- die Installation von Software/Anwendungen aus einer nicht vertrauenswürdigen Quelle,
- soziale Netzwerke (die das Social Engineering erleichtern)...

COMPUTER-WURM
E-MAIL-MALWARE
FILELESS-ANGRIFF
HACKER
INFIZIERTE GERÄTE
SOFTWARE-SCHWACHSTELLEN
TROJANER

Phase 3
Verbreitung

JETZT GEHT ES LOS!
Um sich zu verbreiten, setzt die Ransomware verschiedene Methoden ein, wie z. B. „Exploit-Kits", mit denen Schwachstellen ausgenutzt werden können.

...

LÖSUNGEN GEGEN RANSOMWARE SIND VORHANDEN

STORMSHIELD
Endpoint Security Evolution

Dieser proaktive Schutz verhindert, dass Schadsoftware auf Ihrem Computer ausgeführt wird und/oder eine Schwachstelle ausnutzt (mittels einem Exploit-Kit).

Dank ihrer Technologie zur proaktiven Erkennung von böswilligem Verhalten ist **Stormshield Endpoint Security Evolution** in der Lage, Ransomware abzuwehren, bevor sie in der Cybersicherheitsbranche überhaupt bekannt wird.

Dank **Stormshield Endpoint Security Evolution** ist Ihr **Unternehmen** vor Ransomware geschützt

Weitere Informationen:
www.stormshield.com/de/produkte-und-services/produkte/schutz-von-workstations-und-servern/

EINIGE UNENTBEHRLICHE TIPPS
zum Schutz vor Ransomware

Hüten Sie sich vor verdächtigen E-Mails mit Anhängen.

Führen Sie regelmäßig Backups durch.

Aktualisieren Sie Ihre Anwendungen, Plugins und Betriebssysteme.