STORMSHIELD

Bedrohungswarnung

Stormshield Endpoint Security Evolution

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

LockBit 2.0

EXFILTRATION UND VERSCHLÜSSELUNG VON DATEN AUF INFIZIERTEN RECHNERN

Bei LockBit handelt es sich um eine Gruppe von Cyberangreifern, die anderen Organisationen oder Einzelpersonen ein Ransomware-as-a-Service-Produkt (RaaS) anbietet, das diese im Rahmen eines Affiliate-Modells nutzen können – ähnlich einer schlüsselfertigen Lösung.

LockBit ist vermutlich die aktivste Ransomware-Gruppe mit einer beeindruckenden Liste von 203 Opfern allein im 3. Quartal 2021.

Erstzugriff
Erlangen hoher Privilegien mittels Social Engineering, um Dateien zu verschlüsseln und ein Lösegeld zu fordern.

Ziel
Unternehmen jeder Größe ohne wirksamen Schutz vor Ransomware. Insbesondere in den USA, Kanada und Europa.

Risiken
Verschlüsselung von Daten (Auswirkungen auf die Integrität), Diebstahl sensibler Informationen (Auswirkungen auf die Vertraulichkeit), Produktivitätsverlust (Auswirkungen auf die Verfügbarkeit) usw.

Lernen Sie unsere Lösung zum Schutz vor Ransomware kennen

LOCKBIT 2

#1

Erstinfektion

Phase 1

Die Cyber-Angreifer **erhalten entweder durch den Kauf** von einer anderen Gruppe oder durch einen von ihnen durchgeführten Phishing-Angriff Zugang zum Zielunternehmen.

Stormshield Endpoint Security Evolution **schützt Sie effektiv vor verschiedenen Angriffstechniken** *(Buffer Overflow, Packed Malware oder auch Process Hollowing).*

#2

Lateralisierung und Suche nach wertvollen Daten (Expansion)

Phase 2

Die Cyber-Angreifer **dringen tief in das Netzwerk ein**, um es im Detail zu analysieren. Anschließend weiten sie ihren Angriff lateral aus, um Rechner mit wertvollen Informationen zu identifizieren.

Stormshield Endpoint Security Evolution ***erkennt und neutralisiert Analyseoperationen*** *(z. B. das Starten von Befehlen, um IP-Adressen, Benutzerkonten, DNS-Server, Netzwerkfreigaben usw. in Erfahrung zu bringen).*

#3

Auswirkungen

Phase 3

Exfiltration von Daten in die Infrastruktur der LockBit-Gruppe

Stormshield Endpoint Security Evolution ***blockiert den Zugriff auf vertrauliche Dateien****, wie Passwörter, private Schlüssel, Tresore, Anmeldedaten usw.*

Verschlüsselung von Dateien und Stellen von Lösegeldforderungen

Dieser Schritt bleibt aus. *Stormshield Endpoint Security Evolution neutralisiert Malware, die wie Ransomware agiert und verhindert somit die Verschlüsselung von Daten.*

Zerstörung der Wiederherstellungspunkte von Shadow Copies

Stormshield Endpoint Security Evolution ***erkennt Versuche zur Manipulation*** *von Shadow Copies, wehrt diese ab und stoppt die Ausführung von Ransomware.*