Die Anatomie der Ransomware: Vom allgemeinen Verständnis zur gezielten Netzwerkerkennung

Eine Analyse der Bedrohungslandschaft und eine Fallstudie zur Früherkennung in Unternehmensnetzwerken.

NotebookLM

Ransomware ist kein Nischenproblem. Es ist eine globale Wirtschaftskrise.

$20 Milliarden

Geschätzte Verluste für Organisationen durch Ransomware im Jahr 2021.

Alle 11 Sekunden

Die Frequenz, mit der eine neue Organisation von einem Ransomware-Angriff betroffen ist.

40%

Der Anteil der betroffenen Unternehmen, die das Lösegeld zahlen, ohne eine Garantie für die Wiederherstellung ihrer Daten zu haben.

Quellenangabe: Oz et al., *ACM Comput. Surv.*, 2022; Osterman Research, 2016.

NotebookLM

30 Jahre Evolution: Von einfachen Experimenten zu einem globalen kriminellen Geschäftsmodell

1989

1989: AIDS Trojan

Der erste bekannte Ransomware-Angriff, der Disketten per Post verteilte und symmetrische Verschlüsselung zur Verschlüsselung von Dateinamen verwendete.

2005

2005: GPCode

Die erste moderne kryptografische Ransomware, die über Phishing-E-Mails verbreitet wurde.

2013

2013: CryptoLocker

Ein Wendepunkt, der starke 2048-Bit-RSA-Verschlüsselung und Bitcoin für Lösegeldzahlungen einführte und damit die Anonymität der Angreifer erhöhte.

2015

2015: RaaS (Ransomware-as-a-Service)

Die Kommerzialisierung von Ransomware. Kits werden auf Untergrundmärkten verkauft, was die Eintrittsbarriere für Kriminelle drastisch senkt.

2017

2017: WannaCry

Ein globaler Ausbruch, der eine Wurm-ähnliche Verbreitung über eine SMB-Schwachstelle nutzte und über 250.000 Systeme in 150 Ländern infizierte.

2019

2019: Ryuk

Beispiel für gezielte Angriffe („Human-Operated Ransomware"), die sich ausschließlich auf große Unternehmen konzentrieren und oft über andere Malware wie TrickBot eingeschleust werden.

Die Entwicklung zeigt eine klare Professionalisierung: stärkere Verschlüsselung, anonymere Zahlungsmethoden und gezieltere Angriffe.

NotebookLM

Ein generalisiertes Angriffsmodell: Die vier Phasen eines Ransomware-Angriffs

1. Infection (Infektion)

Die Ransomware wird auf das Opfersystem geliefert. Gängige Vektoren sind bösartige E-Mails, Drive-by-Downloads oder die Ausnutzung von Software-Schwachstellen.

2. C&C Communication (C&C-Kommunikation)

Nach der Infektion kontaktiert die Malware den Command-and-Control-Server, um wichtige Informationen auszutauschen (z.B. Übermittlung von Verschlüsselungsschlüsseln, Systeminformationen des Opfers).

3. Destruction (Zerstörung)

Die eigentliche bösartige Aktion wird ausgeführt. Dies kann die Verschlüsselung von Dateien (kryptografische Ransomware) oder die Sperrung des Systemzugriffs (Locker-Ransomware) sein.

4. Extortion (Erpressung)

Dem Opfer wird eine Lösegeldforderung angezeigt, die Anweisungen für die Zahlung enthält, typischerweise in Kryptowährung.

Zusatzinformation: Einige Varianten (z.B. WannaCry) zeigen wurmartiges Verhalten und versuchen, sich selbstständig im Netzwerk zu verbreiten.

NotebookLM

Die Taxonomie der Bedrohung: Eine Klassifizierung nach Methode und Ziel.

Ransomware-Klassifizierung

Nach Methode (Malicious Action)

Kryptografische Ransomware

Verschlüsselt Opferdateien (z.B. .doc, .pdf, .zip) mit starken Algorithmen wie AES und RSA. Die Originaldateien werden gelöscht oder überschrieben. Dies ist die vorherrschende Bedrohung für PCs/Workstations.

Locker-Ransomware

Sperrt den Zugriff auf das System (z.B. Bildschirmsperre, Browsersperre), ohne die Daten selbst zu verschlüsseln. Besonders effektiv bei mobilen Geräten.

Nach Zielplattform (Target Platform)

PCs/Workstations

Das häufigste Ziel, wobei die meisten Varianten auf Windows abzielen. Beispiele existieren jedoch auch für macOS (KeRanger) und Linux (Linux.Encoder).

Mobile Geräte

Android ist aufgrund seines offenen Ökosystems ein Hauptziel. iOS ist durch Apples streng kontrolliertes System weitgehend verschont geblieben.

IoT/CPS-Geräte

Ein aufkommendes, aber noch nicht weit verbreitetes Ziel. Das Potenzial für katastrophale Auswirkungen (z.B. in medizinischen Geräten oder industriellen Kontrollsystemen) ist enorm.

NotebookLM

Angesichts dieser Komplexität, wo liegt der größte Hebel für die Verteidigung in Unternehmen?

* Endpoint-Schutz ist entscheidend, aber reaktiv und kann umgangen werden.
* Backup-Strategien sind für die Wiederherstellung unerlässlich, verhindern aber nicht den Betriebsstillstand und Datenverlust seit dem letzten Backup.
* Die Kommunikation der Ransomware mit dem C&C-Server kann getarnt oder nicht vorhanden sein.

Die Antwort: Der kritischste Moment, der beobachtet werden kann, ist die Aktion selbst: die Zerstörung von Daten. Insbesondere, wenn diese auf zentralen, für das Unternehmen überlebenswichtigen Ressourcen stattfindet.

→ Analyse des Netzwerkverkehrs zu gemeinsam genutzten Speicher-Volumes.

NotebookLM

Das Schlachtfeld: Gemeinsam genutzte Netzwerk-Volumes (NAS)

Hoher Wert für Unternehmen

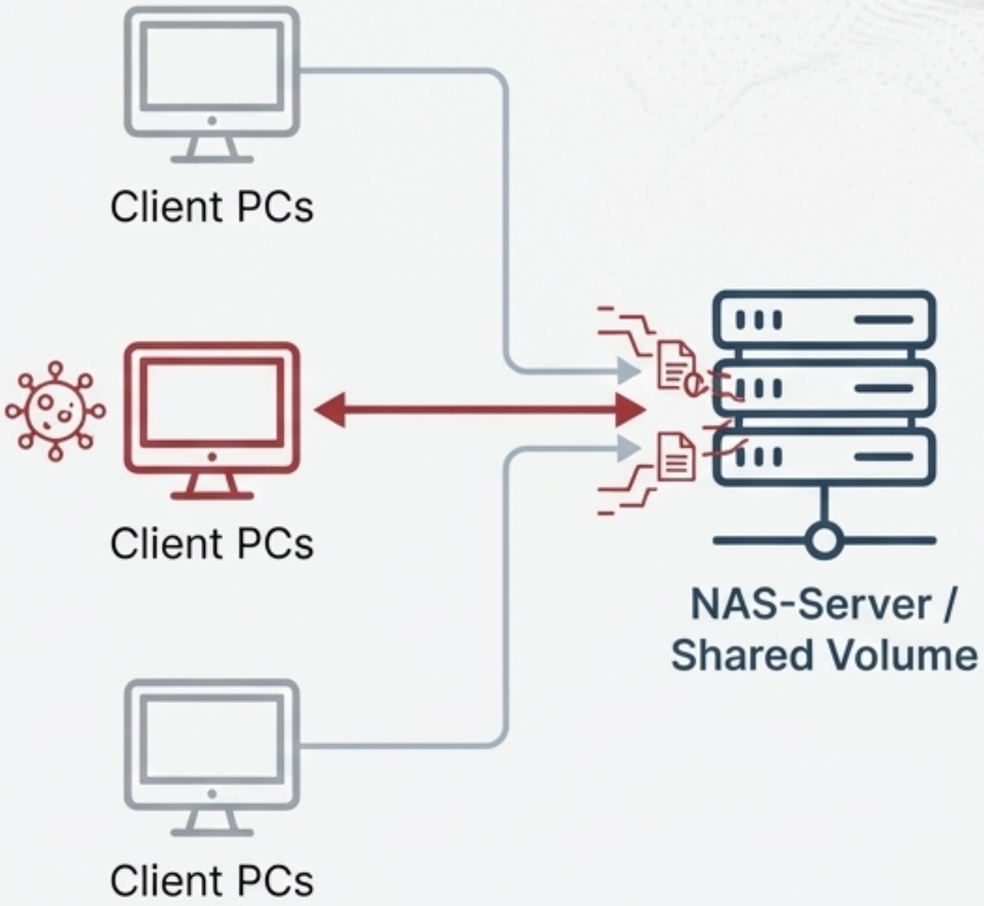
Geteilte Volumes (die über Protokolle wie SMB zugegriffen werden) sind das Rückgrat der Zusammenarbeit in Unternehmen. Sie ermöglichen zentralisierte Backups, Teamarbeit und Benutzerprofil-Mobilität.

Hohes Risiko

Ein einziger infizierter Host kann Dokumente über mehrere Abteilungen hinweg verschlüsseln und so einen globalen Einfluss auf den Geschäftsbetrieb haben. Die Wiederherstellung von nächtlichen Backups bedeutet oft den Verlust eines ganzen Arbeitstages pro Mitarbeiter.

Die Herausforderung

Herkömmliche host-basierte Erkennungstools müssen auf jedem einzelnen Computer im Unternehmen installiert und
jedem einzelnen Computer im Unternehmen installiert und
gewartet werden und können von Malware deaktiviert werden.



NotebookLM

Fallstudie: REDFISH (Ransomware Early Detection from FIle SHaring traffic)

Ein Algorithmus zur Früherkennung von Ransomware, der ausschließlich auf der Analyse des Netzwerkverkehrs (SMB-Protokoll) zu gemeinsam genutzten Volumes basiert.

Die Vorteile des Ansatzes

Keine Host-Installation: Erfordert keine Software auf den Endgeräten.

Nicht umgehbar: Da die Analyse auf einer separaten Netzwerksonde läuft, kann sie von der Malware nicht deaktiviert werden.

Keine Latenz: Die Analyse erfolgt auf einer Kopie des Traffics (z.B. über einen Switch Port Mirror) und fügt dem Benutzerverkehr keine Verzögerung hinzu.

Verhaltensbasiert: Erkennt Zero-Day-Day-Angriffe, da es auf Mustern basiert, nicht auf Signaturen.

NotebookLM

Die Logik der Erkennung: Drei einfache Regeln, um Ransomware-Verhalten zu identifizieren.

Grundannahme: Ransomware, die auf Netzwerk-Shares abzielt, muss Dateien lesen, verschlüsseln, zurückschreiben (oder überschreiben) und oft das Original löschen. Dieses Verhalten erzeugt ein einzigartiges und schnelles Muster aus Lösch-/Überschreibvorgängen und intensivem Lese-/Schreib-Traffic.

Der Algorithmus löst einen Alarm aus, wenn alle drei Bedingungen erfüllt sind:

N (Anzahl)

Eine Mindestanzahl von **N** Dateien wird gelöscht oder überschrieben.

T (Zeit)

Diese **N** Ereignisse treten innerhalb eines kurzen Zeitintervalls von **T** Sekunden auf.

V_thres (Geschwindigkeit)

Die durchschnittliche Lese- und Schreibgeschwindigkeit während dieses Zeitraums überschreitet einen Schwellenwert **V_thres**.

Konfigurierte Parameter in der Studie: N = 10 Dateien, T = 20 Sekunden, V_thres = 107 Kb/s.

NotebookLM

Die Ergebnisse: Nahezu sofortige Erkennung mit minimalem Schaden.

Getestet mit 54 Samples aus 19 verschiedenen Ransomware-Familien (u.a. Locky, Cerber, WannaCry).

100%

Erkennungsrate über alle getesteten Ransomware-Familien. Kein einziger Angriff blieb unentdeckt.

<10

Maximale Anzahl an verschlüsselten Dateien in über 99% der Erkennungsfälle, bevor der Alarm ausgelöst wurde.

<20 Sekunden

Maximale Zeit bis zur Erkennung in 99% der Fälle nach Beginn der Ransomware-Aktivität.

Zusätzlicher wichtiger Punkt: Extrem niedrige Falsch-Positiv-Rate. In einem realen Unternehmensnetzwerk mit über 4.800 Benutzern wurde über 24 Stunden nur 1 Fehlalarm pro 10 Millionen geöffneter Dateien ausgelöst.

NotebookLM

Mehr als nur Erkennung: Der Weg zur "Zero-Loss Recovery".

Das entscheidende Detail: Da die Netzwerksonde den gesamten Verkehr zum Dateiserver aufzeichnet, erfasst sie den Inhalt jeder Datei, die von der Ransomware **gelesen** wird – unmittelbar bevor sie verschlüsselt wird.

1. Erkennung

REDFISH erkennt den Angriff und löst einen Alarm aus.

2. Blockierung

Der Verkehr des infizierten Hosts wird blockiert.

3. Wiederherstellung

Die wenigen (<10) Dateien, die verschlüsselt wurden, können direkt aus dem gespeicherten SMB-READ-Verkehr auf der Sonde wiederhergestellt werden.

Das Ergebnis: Die wiederhergestellten Dateien sind nicht die veralteten Versionen aus dem nächtlichen Backup, sondern die exakte Version, die die Ransomware verschlüsselt hat. Dies ermöglicht eine echte Wiederherstellung ohne Datenverlust.

NotebookLM

Die strategische Implikation: Die Verteidigung vom Endpunkt ins Netzwerk verlagern

Zusammenfassung

- Die Ransomware-Bedrohung ist hochentwickelt und allgegenwärtig. Ein tiefes Verständnis ihrer Funktionsweise ist die Grundlage für eine effektive Verteidigung.
- Die Analyse des Netzwerkverkehrs, insbesondere zu kritischen zentralen Ressourcen wie File-Servern, bietet einen einzigartigen und robusten Aussichtspunkt für die Erkennung.
- Der REDFISH-Ansatz zeigt, dass eine verhaltensbasierte Netzwerkanalyse nicht nur möglich, sondern auch extrem effektiv ist:
  - **Umfassend**: Erkennt bekannte und unbekannte Bedrohungen.
  - **Schnell**: Stoppt Angriffe, bevor signifikanter Schaden entsteht.
  - **Widerstandsfähig**: Kann von der Malware nicht kompromittiert werden.
  - **Wiederherstellend**: Ermöglicht eine Wiederherstellung ohne Datenverlust.

Schlussfolgerung

Eine **intelligente Netzwerküberwachung** ist **keine Alternative,** sondern eine **wesentliche Ergänzung** zur **Endpoint-Sicherheit,** die den Spieß im Kampf gegen Ransomware umdrehen kann.

NotebookLM