6 Methoden, die Security-Profis kennen sollten, um Daten aus verschlüsselten, virtuellen Festplatten zu extrahieren

Techniken für die Cyber-Task-Force zur Informationswiedergewinnung aus gesperrten virtuellen Laufwerken

Im Falle einer Datenverschlüsselung durch Ransomware müssen „Incident Responder“ und Task-Forces schnell und effizient vorgehen, um möglichst alle Daten beispielsweise von einer verschlüsselten virtuellen Maschine zu extrahieren. Wie wichtig das Fachwissen und die richtige Vorgehensweise sind, unterstreicht einmal mehr der aktuelle Sophos-Report State of Ransomware 2024: 58 Prozent der deutschen Unternehmen waren im letzten Jahr von Ransomware betroffen und 79 Prozent der Angriffe führten dazu, dass Daten verschlüsselt wurden.
Incident Responder sollten daher über verschiedene Techniken und Tools verfügen, um die Daten aus einer verschlüsselten virtuellen Festplatte extrahieren zu können. Die Expert:innen von Sophos empfehlen sechs potenziell erfolgversprechende Tools zur Wiederherstellung von Daten, die mit Standardmethoden nicht wiederhergestellt werden können. Zwar ist ein Erfolg nicht garantiert, es gibt jedoch eine Vielzahl an positiven Erfahrungen beim Einsatz dieser Methoden, beispielsweise im Zusammenhang mit LockBit, Faust Phobos, Rhysida oder Akira.

Bitte keine Rettungsversuche mit Originaldaten
Damit eine prekäre Situation nicht zur Katastrophe wird, gilt grundsätzlich und unabhängig von den Extraktionsmethoden, alle Wiederherstellungsversuche mit Arbeitskopien und nicht mit den Originalen durchzuführen. Nur so ist garantiert, dass eine fehlgeschlagene Rettungsmethode, welche die Daten und VM-Systeme vielleicht zusätzlich geschädigt hat, Versuche mit anderen erfolgversprechenden Tools unmöglich macht.

6 bewährte Methoden
Es gibt eine Vielzahl an Methoden, die bei der Extraktion von Daten aus einer verschlüsselten Windows-VM eingesetzt werden können. Einige dieser Techniken sind sogar für Wiederherstellungsversuche unter Linux anwendbar. Sechs dieser Methoden haben sich besonders bewährt:

Methode 1: Einfaches „mounten“ des Laufwerks
Diese Methode klingt einfach, funktioniert vielfach und spart ungeheuer viel Zeit. Wenn es nicht klappt, sind nur wenige Minuten verloren. Wenn die Methode jedoch erfolgreich ist und das Laufwerk gemountet, also fester Bestandteil des Betriebssystems geworden ist, kann auf die Datei(en) zugegriffen werden. Da lediglich die VM gemounted wird, sollte der Endpoint-Schutz keine bösartigen Dateien erkennen oder entfernen, um weitere forensische Erkenntnisse daraus zu gewinnen.

Methode 2: RecuperaBit
RecuperaBit ist ein automatisiertes Tool, das alle NTFS-Partitionen wiederherstellen kann, die in der verschlüsselten VM gefunden werden. Wenn es eine NTFS-Partition findet, erstellt es die Ordnerstruktur dieser Partition neu. Bei einem Erfolg können die Expert:innen dann auf die Datei(en) zugreifen und sie wie gewünscht aus der neu erstellten Verzeichnis-/ Ordnerstruktur kopieren und einfügen. RecuperaBit wird wahrscheinlich den Endpunktschutz nicht auslösen, sofern ransom.exe oder andere bösartige Dateien vorhanden sind. Daher sollte RecuperaBit beispielsweise in einer Sandbox ausgeführt werden.

Methode 3: bulk_extractor
Der automatisierte bulk_extractor ist ein Tool für Windows- oder Linux-Umgebungen. Es kann sowohl Systemdateien wie Windows-Ereignisprotokolle (.EVTX) als auch Mediendateien wiederherstellen. Wie bei RecuperaBit wird bulk_extractor wahrscheinlich Erkennungen des Endpunktschutzes deaktivieren, wenn ransom.exe oder andere bösartige Dateien vorhanden sind. Daher sollte der Extraktions-Versuch mit bulk_extractor ebenfalls in einer Sandbox durchgeführt werden.

Methode 4: EVTXtract
Dieses automatisierte Linux-Tool durchsucht einen Datenblock beziehungsweise eine verschlüsselte VM nach vollständigen oder teilweisen .evtx-Protokolldateien. Wenn es solche findet, werden diese in ihre ursprüngliche Struktur, das heißt XML, zurückverwandelt. XML-Dateien sind bekanntermaßen schwierig zu bearbeiten. In diesem Fall besteht die Datei aus fehlerhaft eingebetteten EVTX-Fragmenten, so dass die Ausgabe etwas unhandlich sein kann.

Methode 5: Scalpel, Foremost und weitere Tools zur Dateiwiederherstellung
Zu den Tools, die für die Wiederherstellung anderer Dateitypen entwickelt wurden, gehören Scalpel und Foremost. Obwohl es sich bei beiden um ältere Technologien handelt, hat das Sophos IR-Team bei seinen Untersuchungen gute Ergebnisse mit diesen beiden Tools erzielt. Beide stellen hauptsächlich Medien- und Dokumentdateien wieder her und bei beiden kann die Konfiguration geändert werden, um sich auf bestimmte Dateitypen zu konzentrieren.

Methode 6: Manuelles Zerlegen der NTFS-Partition
Im Gegensatz zu den beschriebenen Tools und Techniken erfordert das manuelle Carving eine gründliche Vorbereitung und ein genaueres Verständnis der verfügbaren Optionen. Für das korrekte manuelle Carving müssen die Ermittler:innen drei Switches auf dd setzen – bs (Bytes pro Sektor), skip (der Offset-Wert des NTFS-Sektors, den Sie neu erstellen wollen) und count – bevor das Dienstprogramm ausgeführt wird. Schlussendlich wird die neue, ge-carvte Datei gemounted, um das wiederherzustellen, was benötigt wird.

Schlussfolgerung
Verschlüsselte Daten oder VMs sind eine große Bedrohung für Unternehmen und deren Business. Daher ist es wichtig, die Handlungsfähigkeit des Unternehmens so schnell und umfassend wie möglich wiederherzustellen, wobei die vorgestellten Techniken helfen können. Der beste Weg zur Wiederherstellung von verschlüsselten Daten besteht allerdings darin, eine Kopie von einem sauberen, nicht betroffenen Backup zur Verfügung zu haben. Und noch wichtiger ist es, durch Prävention mit wirkungsvoller Security einen solchen Fall möglichst zu verhindern.

Den detaillierten Artikel von den Sophos-Expert:innen Lee Kirkpatrick, Paul Jacobs, Sai Lakshmi Ghanasyam, Antoni Fertner, Andy French über die sechs Methoden mit weiteren technischen Informationen finden Sie unter: https://news.sophos.com/en-us/2024/05/13/extract-data-from-encrypted-vms/

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de