arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

3 Schritte zum Schutz vor Wiper-Malware

Von Florian Malecki, Executive Vice President Marketing, Arcserve

Wiper-Malware stellt eine alarmierende Bedrohung für Unternehmensdaten dar. Im Gegensatz zu Ransomware, die Dateien verschlüsseln und deaktivieren kann, bis Unternehmen ein Lösegeld zahlen, verfolgen Cyber-Kriminelle mit Wiper-Malware andere Ziele: Daten dauerhaft zu löschen und so viel Zerstörung wie möglich zu verursachen. Sobald eine Wiper-Malware das System infiziert hat, zerstört sie Daten völlig unwiederbringlich. Diese Art von Malware ist für die Opfer besonders gefährlich, weil sie keine Möglichkeit der Wiederherstellung durch Zahlung eines Lösegelds bietet.

Wiper-Malware ist in den letzten Jahren immer häufiger aufgetreten und gleich mehrere prominente Angriffe sorgten für Schlagzeilen. Sicherheitsexperten vermuten, dass der zerstörerische WannaCry-Angriff im Jahr 2017, der weltweit Hunderttausende von Computern betraf, ein Wiper-Angriff war. Weitere Wiper-Angriffe der letzten Zeit waren Olympic Destroyer im Jahr 2018, das auf die Olympischen Winterspiele in Südkorea abzielte, und ZeroCleare im Jahr 2020, das den Energie- und Industriesektor im Nahen Osten zum Ziel hatte. Zudem war der berüchtigte Sony Pictures-Hack ein Wiper-Angriff.

Auch im Zuge des anhaltenden Konflikts zwischen Russland und der Ukraine wurde die Ukraine von Wiper-Angriffen heimgesucht. Kürzlich berichteten Forscher von Fortinet, dass Kriminelle Wiper-Malware auch gegen andere Länder eingesetzt haben. In der ersten Hälfte des Jahres 2022 kamen in Kampagnen gegen private, staatliche und militärische Organisationen sieben neue Wiper-Varianten zum Einsatz. Tatsächlich gab es über die Ukraine hinaus Wiper-Malware-Angriffe in 24 Ländern. Einige dieser Angriffe zielten auf kritische Infrastrukturen ab, wobei Malware zum Löschen von Festplatten eingesetzt wurde.

Eine der grundlegenden Herausforderungen im Umgang mit Wiper-Bedrohungen besteht darin, dass sie sehr oft schwer zu erkennen und zu verhindern sind. Im Gegensatz zu

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

anderen Formen von Malware, deren Vorhandensein in der Regel Spuren hinterlässt, löscht Wiper alle Spuren selbst, sobald die Malware ihr zerstörerisches Werk vollendet hat. Das macht es für IT-Sicherheitsexperten schwierig, auf diese Angriffe zu reagieren und deren Ausbreitung zu verhindern.

Unternehmen müssen deshalb robuste, mehrschichtige Sicherheitsmaßnahmen einführen, um sich gegen Wiper-Bedrohungen zu schützen – einschließlich regelmäßiger Backups wichtiger Daten. Außerdem ist für Unternehmen die Aufrechterhaltung eines starken Sicherheitssystems wichtig und auf Anzeichen eines potenziellen Wiper-Angriffs zu achten. Folgende drei Schritte helfen Unternehmen, das Risiko zu minimieren, Opfer eines zerstörerischen Wiper-Angriffs zu werden.

1. Daten sichern

Die Bedeutung von Datensicherungen für die Abwehr von Wiper-Malware kann gar nicht hoch genug eingeschätzt werden. Backups können einen Angriff zwar nicht verhindern, aber sie sind ein Rettungsanker für die Wiederherstellung von Daten, wenn diese durch Wiper-Malware – oder eine andere Art von Angriff – beschädigt wurden.

Durch die ordnungsgemäße Verwaltung der Backups können Unternehmen sicherstellen, dass sie über Kopien ihrer Daten verfügen, die von Produktionssystemen getrennt sind. Sollte die aktive IT-Umgebung von Wiper-Malware, Ransomware oder anderer Malware befallen werden, können Unternehmen Backups, die auf einer unveränderlichen Speicherlösung gespeichert sind, wiederherstellen. Die Wiederherstellung von Backups ist nicht nur kostengünstiger und schneller als die Zahlung eines Lösegelds zur Wiederherstellung von Daten. Bei einem Wiper-Angriff ist sie wahrscheinlich auch die einzige Option, da die Zahlung eines Lösegelds in der Regel nicht in Frage kommt.

2. Die 3-2-1-1-Regel befolgen

Die 3-2-1-1-Datenschutzstrategie ist ein bewährtes Verfahren zur Abwehr von Malware, einschließlich Wiper-Angriffen. Bei dieser Strategie werden 3 Kopien der Daten auf 2 verschiedenen Datenträgern aufbewahrt, wobei 1 Kopie außerhalb des Unternehmens

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

gespeichert wird. Die letzte 1 in der Aufstellung steht für die unveränderliche Objektspeicherung. Wenn Unternehmen mehrere Kopien ihrer Daten aufbewahren, können sie sicherstellen, dass eine Sicherheitskopie zur Verfügung steht, falls eine Kopie verloren geht oder doch beschädigt wird.

Dies ist für den Fall eines Wiper-Angriffs, bei dem Daten zerstört oder gelöscht werden, unerlässlich. Unternehmen können beispielsweise eine Kopie ihrer Daten auf einer Festplatte, eine weitere Kopie bei einem Cloud-basierten Speicherdienst und die dritte auf einem Wechsellaufwerk oder Band aufbewahren. Auf diese Weise haben sie im Falle eines Angriffs auf einen Medientyp über die anderen Kopien immer noch Zugriff auf ihre Daten. Die Aufbewahrung von mindestens einer Kopie der Daten sollte außerhalb des Unternehmens, entweder an einem physischen Standort oder in der Cloud, erfolgen. Dieser Ansatz bildet eine zusätzliche Sicherheitsebene. Wenn ein Wiper-Angriff die Kopien der Daten vor Ort zerstört, haben Unternehmen immer noch Zugriff auf ihre Offsite-Sicherung.

Ein weiterer Vorteil dieser Schutzstrategie ist die unveränderliche Objektspeicherung. Bei der unveränderlichen Objektspeicherung werden alle 90 Sekunden Snapshots der Daten erstellt, so dass Unternehmen diese selbst bei einem Wiper-Angriff schnell wiederherstellen können. Dieses Datensicherheits-Tool der nächsten Generation hilft Unternehmen, ihre Informationen zu sichern und vor Verlust oder Beschädigung zu schützen.

2. Air-Gapping-Methoden verwenden

Air Gapping ist eine effiziente und effektive Methode zum Schutz von Sicherungsdaten vor Wiper-Angriffen. Es gibt zwei Arten von Air Gapping: traditionelles physisches und logisches Air Gapping. Beim physischen Air Gapping wird ein digitales Element von allen anderen Geräten und Netzwerken getrennt, so dass eine physische Distanz zwischen einem sicheren Netzwerk und jedem anderen Computer oder Netzwerk entsteht. Unternehmen können Sicherungsdaten auf Bändern oder Festplatten speichern und diese Medien dann vollständig von ihrer IT-Produktionsumgebung trennen.

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Logisches Air Gapping hingegen stützt sich auf Netzwerk- und Benutzerzugriffskontrollen, um Sicherungsdaten von der IT-Produktionsumgebung zu isolieren. Die Daten werden über eine „Einbahnstraße" an das vorgesehene Ziel, z. B. einen unveränderlichen Speicher oder eine benutzerdefinierte Appliance, übertragen und können nur über separate Authentifizierungskanäle verwaltet oder geändert werden. Air Gapping macht Daten für Wiper-Malware-Angriffe nahezu unsichtbar, so dass es für Cyberkriminelle fast unmöglich ist, Backups zu kompromittieren.

Ein Sicherungs- und Wiederherstellungsplan ist unverzichtbar

Die zunehmende Verbreitung von Wiper-Malware ist eine deutliche Mahnung, dass sich Unternehmen beim Schutz ihrer Daten in einer gefährlichen Situation befinden. Ein solider, gut verwalteter Plan zur Datensicherung und -wiederherstellung ist der Schlüssel zur Gewährleistung der Datensicherheit angesichts der wachsenden Zahl von Bedrohungen. Ganz gleich, welche Taktiken Cyberkriminelle anwenden, um den Zugriff auf Daten zu stören, ein solider Sicherungs- und Wiederherstellungsplan sorgt für eine zuverlässige Sicherheit von Unternehmensdaten.

Folgen Sie Arcserve auf LinkedIn oder Twitter und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de