PRÄVENTION & RECOVERY BEI RANSOMWARE

Werden Sie nicht zum nächsten Opfer

Die SamSam (aka Samas oder Samsa) Ransomware ist eine neue Generation von Ransomware, die nicht branchenspezifisch ist.

Diese Bedrohung:

- Beruht nicht typischerweise auf traditionellem Spear-Phishing oder Watering-Hole Vektorangriff
- Nutzt verwundbare externe Services, so dass Täter gut getarnt manuell horizontal angreifen und ihre Präsenz ausweiten können
- Kann über Skripte und automatisierte Verfahren ganze Netzwerke verschlüsseln statt nur einer Handvoll von einzelnen Hosts
- Zielt auf Backup-Systeme innerhalb des Netzwerks ab und löscht Archive, statt sie nur zu verschlüsseln, wodurch die Opfer keine Optionen zur Wiederherstellung haben[1]

1 FBI-FLASH MC-000070-MW: Am 25. März 2016 durch das FBI an bestimmte Instanzen (TLP:GREEN) verteilt..

Aktuelle Ransomware-Bedrohungslage

Die heutigen Ransomware-Kampagnen unterscheiden sich von dem, was wir in der Vergangenheit gesehen haben. Auf der einen Seite ist Ransomware leicht von Kriminellen, die wenig bis keine Hacking-Fähigkeiten haben, zu erhalten und erfolgreich zu verwenden; so gibt es heute Dienste, die als „Ransomware as a Service (RAAS)“ bezeichnet werden. Auf der anderen Seite sehen wir, wie Ransomware für mehr als nur Lösegeld verwendet wird. In einigen Fällen haben wir gesehen, wie sie als Ablenkung verwendet worden ist. So gibt es z.B. Ransomeware, die zunächst die Anmeldeinformationen für die spätere Verwendung erbeutet und dann das Laufwerk verschlüsselt hat, um die IT-Mitarbeiter zu abzulenken, während die Angreifer ihre Spuren verdeckt haben und sich nun in dem Unternehmen bewegen konnten, um Ihre eigentliche Informationsbeschaffung zu betreiben. Und in jüngster Zeit sehen wir sehr opportunistische Kampagnen, die ganze Netzwerke in einer Organisation verschlüsseln und vor der Verschlüsselung auch Host-Backups löschen, wodurch die gesamte Organisation erpresst wird und nicht mehr in der Lage ist zu arbeiten.

Cylance® bietet zwei sich ergänzende Serviceangebote, die Organisationen helfen, diesen neuen Bedrohungen zu begegnen.

Proaktive Prävention und optimaler Einsatz der Lösung

Cylance bietet bewährte Verfahren zur Malware Prävention, Netzwerk-Architektur, interne Incident Response-Workflows, Schwachstellen- und Patch-Management und die Sicherheitsbewertung der internen Hosts und externen Services.

Wenn es um Ransomware geht, sind Prävention und Vorbereitung die beste Methode. Sobald Ransomware zur Ausführung kommt, steigen die Unternehmenskosten und Geschäftsrisiken exponentiell. Ebenso können Organisationen, die gut auf Ransomware vorbereitet sind, die Geschäftsauswirkungen von einem IT-Vorfall allgemein minimieren.

Die proaktive Prävention und die Bereitstellungsdienstleistungen von Cylance schützen vor einer Ransomware-Epidemie durch:

- Nutzung der Leistungsfähigkeit von maschinellem Lernen und künstlicher Intelligenz, um eine prädiktive, autonome Verhinderung der Ausführung von Ransomware umzusetzen
- Bereitstellung von sachkundigen Beratern, die über das notwendige Know-How verfügen, um die Wiederherstellung nach einem Angriff von Ransomware zu ermöglichen
- Die Anwendung von Know-How VOR dem Eintritt eines Angriffs ist die beste Vorbereitung und gewährleistet, dass präventive Technologien und Prozesse eingerichtet sind

Zugehörige Dienstleistungen und Produkte

INDUSTRIELLE STEUERUNGSSYSTEME

- Bewertung der ICS-Infrakstruktur
- ICS-Bedrohungseinschätzung
- Automatisierungssysteme aufbauen und Sicherheit implementieren
- Incident-Response-Services für Steuerungssysteme

Internet der Dinge/Embedded

- Incident Response für das Internet der Dinge und eingebettete Systeme
- Penetrationstests für eingebettete Systeme

ThreatZERO™

- ThreatZERO + Bedrohungseinschätzung
- ThreatZERO Resident Expert

Gesundheitswesen

- Entwicklung eines Sicherheitsprogramms für klinische Informationssysteme
- Bewertung der Sicherheit von klinischen Anwendungen
- Risikobewertung von medizinischen Geräten
- HIPAA Compliance

Schulung

- Custom Incident Response und Forensik-Training
- ICS Security Essentials, Incident Response und Bedrohungseinschätzung
- Malware und Incident Response Retainer-Service
- Incident-Readiness Bewertung
- Emergency Incident Response

Leistungen für Unternehmenssicherheit

- Intern/externe Penetrationstests
- Social Engineering
- Bewertung von Webanwendungen

Incident Response, schnelle Eindämmung und Risikominderung

Nicht jede Ransomware ist gleich. Sobald eine Variante freigesetzt wird, ergibt sich eine Vielzahl von „Copy-Cat“ Varianten und einige von ihnen nutzen völlig verschiedene Verschlüsselungsalgorithmen und einen unterschiedlichen Austausch von Schlüsseln, während andere auch noch neue Kommando-und Kontrollinfrastrukturen oder andere Angriffsvektoren nutzen. Für den Fall, dass eine Organisation Incident Response-Dienste in Anspruch nehmen muss, ist es wichtig, auf erfahrene Responder mit einem strukturierten Prozess und maßgeschneiderten Tools zurückgreifen zu können, so dass die Analyse schnell erledigt werden kann, um eine rasche Eindämmung vorzunehmen.

Das IR-(Incident Response) Team von Cylance hat allein im vergangenen Jahr Hunderte von IR-Einsätzen durchgeführt. Sie sind Experten bei der Jagd nach Schlüsselindikatoren von Bedrohungen aktuell aktiver Kampagnen. Dazu nutzen sie die künstliche Intelligenz der Cyclance-Engine im IR-Prozess für die sofortige Eindämmung, und zwar ohne Agenten zu installieren und ohne von den Angreifern hinter der Kampagne aufgedeckt zu werden.

Das Ziel bei allen Ransomware-Vorfällen ist das gleiche: Verringerung von Risiko und Kosten und eine Wiederherstellung des normalen Betriebs durch einen leisen, schnellen und gezielten Einsatz.

Cylance Consulting ist auf die sofortige Eindämmung fokussiert. Wir beseitigen die Schwachstellen und verhindern eine weitere permanente Exposition. Wir sind davon überzeugt, dass Sie keinen Dienstleister finden, der Vorfälle und deren erneutes Auftreten schneller verhindern kann.

Cylance Incident Response, schnelle Eindämmung und Risikoreduktion bei Ransomware-Vorfällen:

- Vor-Ort-Experten, die Hunterte von IRs pro Jahr abgeschlossen haben
- Individuell entwickelte Tools, um die fortgeschrittene Ransomware von heute zu behandeln
- Strukturierte und proprietäre Response Workflows, um die Kampagne schnell zu identifizieren und einzudämmen
- Ransomware-Analyse, um festzustellen, ob es Möglichkeiten gibt, eine Lösegeldzahlung zu vermeiden
- Unterstützung bei der Verhandlung mit kriminellen Akteuren, die hinter Angriffsampagnen stecken, sollte es sich um einen Vorfall im fortgeschrittenen Stadium handeln
- Nutzung der Vorteile der künstlichen Intelligenz, ohne die Notwendigkeit, einen hostbasierte Agenten zu installieren, der die Verbrecher hinter der Kampagne warnen könnte

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman Ave., Suite 700, Irvine, CA 92612, EUA

CYLANCE™