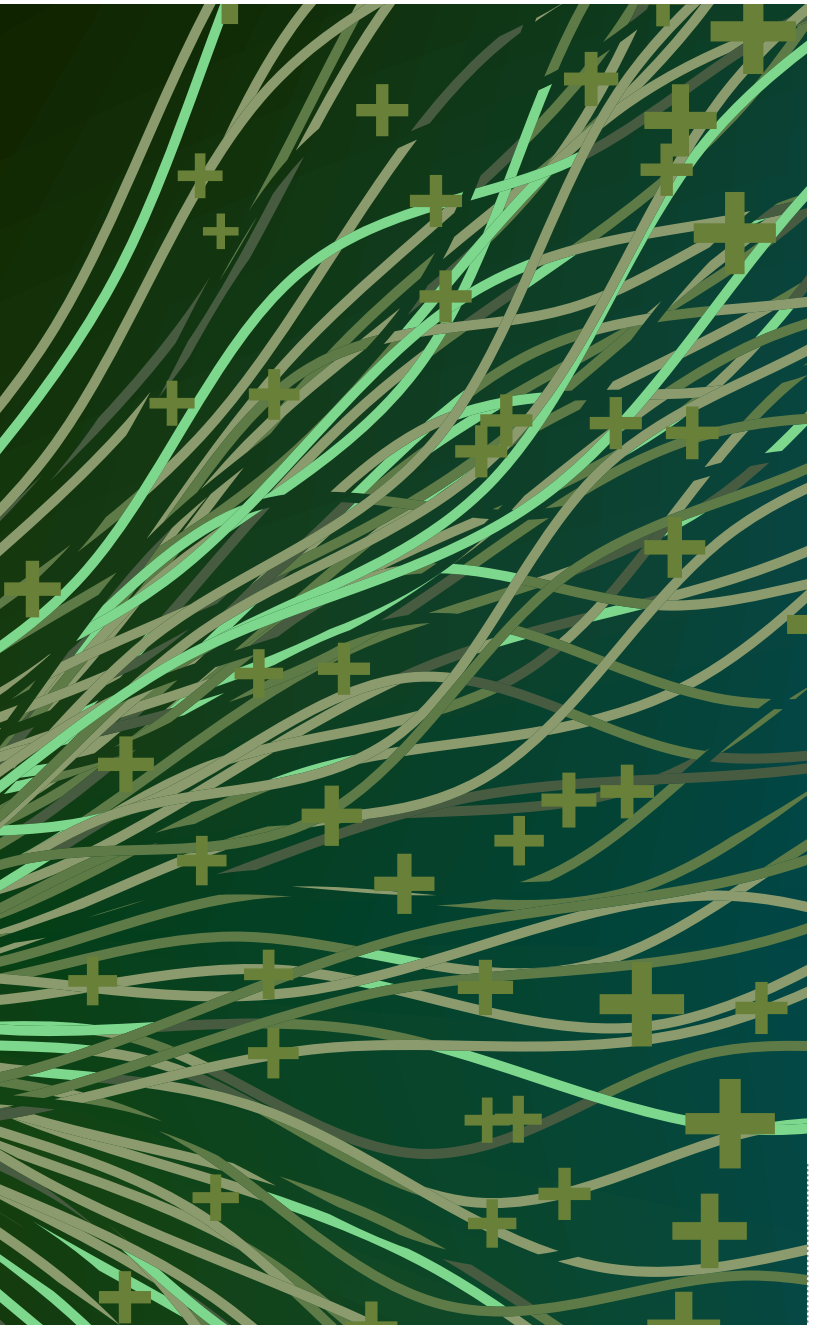

Handbook

BEKÄMPFUNG VON CRIMEWARE

TechTarget | SearchSecurity.de

BEKÄMPFUNG DES CYBERCRIME IM 21. JAHRHUNDERT

Brenda L. Horrigan, Ph.D

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Vergessen Sie den 45er Colt, mit dem Bonnie und Clyde unterwegs waren. Die Waffe der Räuber des 21. Jahrhunderts heißt Malware. Ob sie sich nun gegen Unternehmenssysteme oder Endbenutzer richtet, ihr Ziel ist immer das gleiche: sensible Finanzdaten, die den Zugriff auf Bankkonten und andere Finanzquellen ermöglichen.

In den letzten Monaten wurde die moderne Malware sogar noch ausgefeilter – daher erläutern unsere Experten in diesem dreiteiligen Leitfaden spezifische Bedrohungen und was IT-Sicherheitsabteilungen dagegen tun können. Wir starten mit dem von Rob Shapland verfassten Kapitel, das die neuesten Entwicklungen im Bereich Crimeware schildert und Tipps zur Untersuchung erfolgreicher Angriffe gibt. Formelle Untersuchungen von Sicherheitsverletzungen durch Malware sind keineswegs die Regel, so Shapland, obwohl sie dies sein sollten. Denn auch nach einem erfolgreichen Angriff bleiben Ihre Systeme aufgrund der Beschaffenheit heutiger Malware weiter infiziert. Daher müssen IT-Abteilungen zumindest verstehen, was eigentlich passiert ist, um zu entscheiden, welche Schulungen und

Anpassungen erforderlich sind, um die Chancen weiterer Angriffe zu verringern.

Im zweiten Kapitel erläutert Nick Lewis RAM-Scraping-Malware – die Waffe, die im letzten Jahr für den Angriff auf Target eingesetzt wurde. Das abschließende Kapitel stammt ebenfalls von Nick Lewis, der hier die neuesten Taktiken vorstellt, die Hacker anwenden, um nicht entdeckt zu werden, wie zum Beispiel Automation und Social Engineering, und wie man diese abwehren kann.

Die Hacker werden nicht aufgeben und Malware wird noch weiter verbreitet und hartnäckiger werden. Sie sollten daher im Hinblick auf neue Bedrohungen und modernste Abwehrmaßnahmen auf dem Laufenden bleiben. Denn die Frage lautet nicht, ob ein Angriff auf Ihre Finanzen stattfinden wird, sondern wann. Um es mit den Worten des berühmten Bankräubers Willie Sutton zu sagen: „That's where the money is."

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

CRIMEWARE: WORAUF SIE ABZIELT UND WIE MAN SICH VERTEIDIGEN KANN

Rob Shapland

Crimeware hat sich in den letzten Jahren stark weiterentwickelt. So beschreibt der Verizon Data Breach Investigations Report (DBIR) 2015 Crimeware, die für 25 % aller Vorfälle mit Malware eingesetzt wurde, als „in Unternehmen eingedrungene Infektionen mit Malware, die sich keinen spezifischeren Klassifizierungsmustern zuordnen lässt".

HER MIT DEM GELD

Sensible Finanzdaten sind ein primäres Ziel von Angreifern, weil sie den direkten Zugriff auf Bankkonten ermöglichen, um Gelder auf von den Angreifern kontrollierte Konten zu transferieren. Während die Angreifer zum einen erkannt haben, dass Attacken auf Verkaufsterminals sehr effektiv sind, bilden auch einzelne Endbenutzer ein sehr lukratives Ziel. Crimeware wird primär für Finanzziele eingesetzt und versucht mit einer Reihe von Methoden direkten Zugang zu Bankkonten zu erlangen oder Geld zu entwenden.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Dazu gehören Tracking-Anfragen an Banking-Websites und das heimliche Umleiten des Benutzers auf eine bösartige Website, um seine Zugangsdaten über Command-and-Control-Server zu erschleichen, das Installieren von Ransomware (wie TeslaCrypt), um Benutzer zu zwingen, für den Zugriff auf ihre Daten zu bezahlen, und das Stehlen von auf Computern gespeicherten Passwörtern, um damit auf Finanzsysteme zuzugreifen. Command-and-Control-Crimeware ist die gängigste Variante. Allerdings scheinen sich die Angreifer in diesem Jahr vermehrt auf Distributed Denial-of-Service (DDoS) als Angriffsmethode zu verlegen. So können sie das Opfer zur Zahlung eines Lösegelds zwingen, bevor sie den Betrieb wiederherstellen.

Ein aktuelles Beispiel für Crimeware ist die Dyre-Variante, die Umleitungsmethoden verwendet, um die Zugangsdaten zu Banking-Websites zu entwenden. Die Software wartet, bis der Benutzer auf eine Banking-Website zugreift, um dann seinen Browser auf einen Klon der Website umzuleiten, der auf einer von den Hackern kontrollierten Domäne gehostet wird. Wenn das Opfer seine Zugangsdaten auf der geklonten Website eingibt, werden diese zur Verarbeitung an Command-and-Control-Server geschickt. Die Crimeware wird gewöhnlich als Anhang in einer Phishing-E-Mail eingeschleust.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Dyre ist ein Beispiel für die immer ausgefeiltere Vorgehensweise von Crimeware, denn es werden zufällig generierte Adressen zur Kontaktierung des Servers genutzt, um so Erkennungsmethoden zu umgehen, die bestimmten URLs den Zugang verweigern.

UNBEDINGT ALLE FÄLLE UNTERSUCHEN

Der Verizon-Bericht zeigt, dass Crimeware-Vorfälle viel seltener formell untersucht werden, als andere Arten von Angriffen. Dabei sollten diese Vorfälle mit denselben formellen Analyseverfahren ausgewertet werden wie alle anderen Vorfälle. Auch wenn dies in manchen Fällen nicht machbar ist (beispielsweise bei zufälligen Angriffen auf private Benutzer), sollte bei jedem Eindringen von Crimeware in ein Unternehmen eine Untersuchung durchgeführt werden, da die Crimeware weiterhin genutzt werden kann, um sensible Unternehmensdaten auszulesen, selbst wenn die ursprüngliche Zielsetzung eine andere war.

Crimeware wird oft auch als Teil eines Exploit-Kits (wie Angler oder Nuclear) eingeschleust, weshalb die Entdeckung bestimmter Crimeware-Varianten ein Hinweis auf weitere Infektionen sein kann. Die Unternehmen müssen verstehen, wie diese Infektionen vorgehen, um so die Schwachstellen in ihren Abwehrsystemen zu identifizieren.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Der wahrscheinlichste Eintrittspunkt ist allerdings E-Mail-Phishing, was bedeutet, dass Mitarbeiterschulung und E-Mail-Filter verbessert werden müssen. Ohne eine Untersuchung der einzelnen Fälle bleibt Ihr System angreifbar.

Die meisten modernen Sicherheitsprogramme können das Eindringen von Crimeware erkennen, aber oft ist nicht genügend Personal vorhanden, um jeden Vorfall zu untersuchen, oder Unternehmen sind nicht zu entsprechenden Investitionen bereit. Der Großteil der Crimeware arbeitet nach wie vor mit Eindringmechanismen, die dann Command-and-Control-Server kontaktieren. Allerdings lässt sich in jüngster Zeit ein Trend zu mit Crimeware ausgeführten DDoS-artigen Angriffen erkennen, die man sogar als Crimeware-as-a-Service bezeichnen könnte, wobei spezifische Malware erstellt und eingeschleust werden kann. Um dieser Bedrohung entgegenzuwirken, ist eine umfassende Verteidigungsstrategie erforderlich. Starke technische Kontrollen in Verbindung mit laufenden Mitarbeiterschulungen können den meisten Infektionen vorbeugen. Investitionen in Überwachungssysteme und die Bereitschaft zur Untersuchung einzelner Vorfälle können Unternehmen dabei helfen, herauszufinden, wie eine Infektion entstanden ist, um sie beim nächsten Mal zu verhindern.

ROB SHAPLAND Senior Penetration Tester bei First Base Technologies, spezialisiert auf Web-Anwendungssicherheit. Er hat seine Fachkenntnisse bereits mehrfach eingesetzt, um die Websites verschiedenster Unternehmen zu testen, vom Großkonzern bis zur kleinen Firma, wobei eine breite Palette an Web-Technologien zum Einsatz kommt.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

WIE SICH UNTERNEHMEN VOR RAM-SCRAPERN SCHÜTZEN KÖNNEN

Nick Lewis

INHALT:

Malware für RAM-Scraping oder Memory-Scraping hat sich stark weiterentwickelt, seit sie erstmals durch den Verizon Data Breach Investigations Report 2010 allgemein bekannt wurde. Seit dem 2013 erfolgten Angriff auf Target, bei dem die Angreifer einen RAM-Scraper einsetzten, um Kreditkartendaten auszulesen, ist dieses Thema wieder in den Mittelpunkt des Interesses gerückt. Während sich die technischen Aspekte von mit RAM-Scraping agierender Malware seit 2010 nur wenig verändert haben, hat die allgemeine Komplexität der Angriffe doch enorm zugenommen.

DIE ZEITEN HABEN SICH GEÄNDERT

Zunächst einige Hintergrundinformationen zu RAM-Scraping-Malware: Während der Payment Card Industry Data Security Standard (PCI DSS) für Zahlungskarten eine durchgehende Verschlüsselung aller Zahlungsdaten vorschreibt, einschließlich

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Kreditkartennummern, Karteninhabernamen und Ablaufdaten, gibt es doch ein Zeitfenster während des Autorisierungsprozesses, in dem die Daten unverschlüsselt im RAM von Verkaufsterminals (POS) gespeichert sind. RAM-Scraping-Malware ist so konzipiert, dass sie in diese Terminals eindringt und deren RAM nach unverschlüsselten Daten durchsucht.

Wenn sie diese gefunden hat, liest die RAM-Scraping-Malware die Daten aus und übermittelt sie an die Angreifer.

Natürlich werden immer neue Malware-Angriffe und Variationen von Malware entwickelt, um die herkömmlichen Sicherheitsmaßnahmen von Unternehmen, wie Firewalls und Anti-Malware-Programme, zu überwinden – dies gilt heute noch genauso wie 2010. Und was RAM-Scraping-Malware anbelangt, ist nach wie vor der Zugang zum Verkaufsterminal und seinem Netzwerk erforderlich, weshalb diese Sicherheitsstandards bei einem Angriff auch weiterhin umgangen werden müssen.

Während also die Ausgangslage die Gleiche bleibt, fällt mir vor allem auf, wie ausgefeilt und automatisiert die Angriffe generell geworden sind. Die vermehrte Nutzung verschlüsselter Verbindungen hat die Angreifer gezwungen, sämtliche Punkte ins Visier zu nehmen, an denen Kreditkartennummern unverschlüsselt übermittelt werden.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Heutzutage ist dies häufig nur noch an Verkaufsterminals der Fall, an denen die Kartendaten erstmals eingelesen werden.

Beim jüngsten Datendiebstahl bei Target kam vermutlich auch Kartoxaa zum Einsatz, die neue Variante der BlackPOs-Malware. Diese Malware überwacht alle Einlesevorgänge von Kreditkarten und zeichnet diese in einer Datei auf. Soweit besteht kein Unterschied zu anderen Varianten von RAM-Scraping-Malware. Allerdings verwendete diese Angriffsart weiterentwickelte Schritte zum besseren Verbergen der Kommunikation sowie eine ausgefeiltere Malware, um die Entdeckung viel schwerer zu machen. Dem Sicherheitsjournalisten Brian Krebs zufolge haben die Angreifer das Konto eines Drittanbieters genutzt, um in das Target-Netzwerk zu gelangen und dann dort die Segmentierung auszunutzen, die Target verwendete, um das interne Netzwerk vom PCI-Netzwerk zu trennen. Mithilfe der BlackPOS-Malware konnten die Angreifer das Kopieren der erfassten Daten über einen Windows-File-Share auf einem gekaperten internen Target-Server automatisieren, um so die Daten zu extrahieren. Durch die Nutzung dieses Windows-File-Shares konnten die Angreifer ganz unauffällig vorgehen.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Der kompromittierte Server wurde mit einer unbekannten Malware infiziert und dann zur Speicherung der Daten verwendet, bis diese über FTP an Server außerhalb des Target-Netzwerks gesendet wurden, wie die Untersuchung von Dell SecureWorks ergab. Auch die Nutzung von FTP hat vermutlich dazu beigetragen, dass die Malware unentdeckt blieb.

SCHÜTZEN SIE SICH VOR RAM-SCRAPING

Viele der Strategien zum Schutz von Unternehmen vor RAM-Scraping-Malware sind heute noch die Gleichen wie 2010. Tools und Methoden wie Patching, Anti-Malware, Firewalls, die Einschränkung von Administratorzugriffen und Netzwerküberwachung sind weiterhin wirksam – und allesamt vom PCI DSS vorgeschrieben. Im Januar 2014 hat das U.S. Computer Emergency Readiness Team sogar den Technical Alert TA14-002A herausgegeben, was zum wiederholten Male unterstrich, wie entscheidend diese Sicherheitsmaßnahmen sind.

Weitere grundlegende Schritte – wie die Beschränkung der im Kassensystem auszuführenden Programme auf die POS-Software oder die Einschränkung des Zugangs zu dem für das POS-System verwendeten Konto – können die Sicherheit erheblich verbessern.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Ein hostbasiertes System zur Erkennung von Eindringversuchen (Host-based Intrusion-Detection-System, HIDS), das verdächtige Zugriffe auf RAM oder Systemgeräte überwacht, kann Alarme verschicken und so Administratoren veranlassen, bestimmte Systeme genauer zu untersuchen oder ggf. den Zugang ganz zu blockieren. Das HIDS oder eine integrierte Firewall können außerdem eine zusätzliche Sicherheitsstufe bilden, indem sie nur autorisierte Verbindungen zulassen.

Eine durchgehende Verschlüsselung vom mit dem POS verbundenen Gerät bis zum Zahlungsabwickler kann ebenfalls dazu beitragen, die Übertragung unverschlüsselter Kreditkartennummern zu begrenzen und die Kreditkartenverschlüsselung vor Malware auf dem POS-System zu schützen; ein Chip und eine PIN schränken die Möglichkeiten weiter ein.

Neben der Überwachung auf verdächtige Verbindungen ist auch das Überwachen von nicht SSL-verschlüsseltem Traffic entscheidend, um bösartige Kommunikation zu entdecken. POS-Malware wird oft per Fernzugriff installiert und häufig nutzen die Angreifer auch zum Exfiltrieren der Daten eine Remote-Verbindung, was ihre Entdeckung ermöglicht. Allerdings ist zu beachten, dass die Urheber von Malware zunehmend das standardmäßige HTTPS für ihre Kommunikation nutzen, um bei Analysen nicht aufzufallen.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Botnet-Kommunikation könnte jedoch anders aussehen als die normale browserbasierte HTTPS-Kommunikation und so einen Alarm seitens eines Systems zur Erkennung von Netzwerkanomalien auslösen, auf den eine Untersuchung folgt. Auch wenn in einem Netzwerk mit angemessener Firewall-Absicherung ein System erkannt wird, das mehrere ausgehende oder ins Internet gerichtete Kommunikationskanäle nutzt, könnte dies einen Alarm auslösen.

Aggressive Firewall-Konfigurationen im POS-System können zudem dafür sorgen, dass dieses nur mit den Kassensystemen und umgekehrt kommuniziert. Eine dedizierte Verbindung mit dem Zahlungsabwickler könnte ergänzend zu starken Firewall-Regeln eingesetzt werden.

Einige Unternehmen könnten nun anführen, dass sie auf das Erfassen von Kreditkartennummern angewiesen seien, um die Einkaufsgewohnheiten der Verbraucher zu verfolgen. Ihnen sei gesagt, dass dies trotzdem möglich ist, indem ein Token anstelle der Kreditkartennummer verwendet wird. Neben der Überwachung auf verdächtige Verbindungen ist es auch wichtig, nicht SSL-verschlüsselten Traffic zu überwachen. Dies könnte zwar für Unternehmen, die Kreditkartennummern zu Zwecken der Eindeutigkeit speichern, problematisch sein, aber alle anderen könnten vorhandene Kreditkartennummern mithilfe desselben Algorithmus oder

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Verarbeitungsvorgangs, wie ihn ihr Zahlungsabwickler verwendet, massenweise in neue Tokens umwandeln. Natürlich ist es sehr aufwändig, 40 Millionen Kreditkarten in Token zu konvertieren, aber dies würde immer noch weniger kosten, als ein Datendiebstahl mit Millionen von Kreditkartennummern.

AUS GELÖSTEN PROBLEMEN LERNEN

Die jüngsten Erkenntnisse in Hinblick auf Komplexität und Automation von RAM-Scraping-Malware zeigen, dass diese sich laufend weiterentwickelt. Es ist daher für Unternehmen unerlässlich, dass sie ihre Verteidigung ständig weiter verbessern, indem sie einige der hier genannten Best Practices umsetzen. So können sie nicht nur potenzielle Angriffe vereiteln, sondern zugleich auch sicherstellen, dass sensible Unternehmens- und Verbraucherdaten so wirksam wie möglich geschützt werden.

NICK LEWIS Information Security Officer an der Saint Louis University. Lewis hat 2005 einen Master of Science-Abschluss für Datenabsicherung von der Norwich University erworben sowie 2002 einen Master of Science-Abschluss für Telekommunikation von der Michigan State University. Vor seinem Eintritt in die Saint Louis University 2011 war Lewis an der University of Michigan und im Boston Children's Hospital tätig gewesen, der führenden Schulungsklinik für Pädiatrie der Harvard Medical School, ebenso wie bei Internet2 und an der Michigan State University.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

ABWEHR MODERNER BETRUGSMETHODEN

Nick Lewis

So lange es angreifbare Ziele gibt und leicht „verdientes“ Geld lockt, wird auch weiterhin Malware benutzt und optimiert werden.

Um weiter erfolgreich zu sein und bezahlt zu werden, wenden die Entwickler von Malware modernste Methoden zur Umgehung von Sicherheitsmaßnahmen an und integrieren immer neue Funktionen, um die Anforderungen ihrer Kunden zu erfüllen und die mit der Malware durchgeführten Angriffe effektiver und profitabler zu machen. Viele Malware-Varianten wurden in den vergangenen Monaten optimiert, darunter zum Beispiel Zeus mit dem Wechsel von 32-bit auf 64-bit und die erweiterten Funktionen der iBanking-Malware für den Einsatz auf Android-Geräten.

Neben neuen Funktionen bei Malware hat sich auch ein vergleichsweise neuer Ansatz durchgesetzt: „Living off the land“ – hierbei nutzen die Angreifer bereits integrierte oder ganz legitime Tools, um zu verhindern, dass ihre Angriffe von Anti-Malware-Software erkannt werden. Die Poweliks-Malware ist das jüngste Beispiel für diesen Trend.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

WEITERENTWICKLUNGEN VON MALWARE

Troj_Poweliks. A oder Poweliks ist eine dateilose Malware, die darauf ausgelegt ist, andere Malware herunterzuladen, die dann das kompromittierte System kontrolliert. Poweliks benötigt einen separaten anfänglichen Infektionsweg, um das lokale System zu kapern und die Malware zu installieren, wozu vermutlich eine bösartige Word-Datei dient. Nach der anfänglichen Infektion wird die Malware installiert und als codierte Dynamic Link Library (DLL) in der Registry gespeichert, die dann extrahiert und in auf einem System laufende legitime dllhost.exe-Prozesse integriert wird, die sie dann ausführen.

Da das Speichern einer DLL in der Registry keine gängige Methode zur Installation von Malware an einem Endpunkt darstellt, erschwert es die Erkennung der Malware erheblich, weil nicht alle Anti-Malware-Tools die Registry prüfen. Tools, welche die Registry überprüfen, würden dagegen angesichts eines Registry-Schlüssels mit einer erheblichen Datenmenge sicherlich einen Alarm ausgeben. Die Poweliks-Malware führt außerdem auch PowerShell-Befehle aus, um den Angriff zu vervollständigen. PowerShell-Befehle bilden eine gute Möglichkeit, um durch Nutzung vorhandener Prozesse einer Entdeckung zu entgehen, da PowerShell auf den meisten Systemen installiert ist und über die erweiterte Funktionalität

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

zur Interaktion mit dem Betriebssystem verfügt, die zur Ausführung des Angriffs erforderlich ist.

Andere Malware-Varianten haben ebenfalls Fortschritte gemacht, damit sie für ihre Urheber weiterhin profitabel sind. Die sehr ausgereifte Malware Zeus integriert immer neue Features. So wurde zuletzt offenbar eine verbesserte Funktion für Social-Engineering-Angriffe hinzugefügt, mit der die Malware einen Warnhinweis des Browsers imitierte, um die Benutzer zur Installation der Malware zu bewegen. Ähnlich hat auch iBanking.Android eine neue Funktion zu bieten, die mithilfe einer gefälschten Sicherheitssoftware den Benutzer zur Installation der Malware bewegt. Danach stiehlt diese zur Zwei-Faktor-Authentifizierung genutzte SMS-Nachrichten.

ERKENNEN VON MALWARE

Die Erkennung moderner Malware kann auf vielen verschiedenen Wegen erfolgen. Mehrstufige Malware wie Poweliks und mehrstufige Attacken können Unternehmen mehr Zeit für ihre Erkennung verschaffen, da jede einzelne Stufe eine gewisse Zeit benötigt. Allerdings muss nicht zwangsläufig jede Stufe erkennbar sein, da die einzelnen Schritte für sich genommen nicht unbedingt bösartig sind.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Im Falle von Poweliks kann der mehrstufige Aspekt schwer erkennbar sein, wenn man nur die einzelnen Stufen betrachtet, aber miteinander in Zusammenhang gebracht können die Stufen und Abläufe durchaus die Erkennung und Abwehr bösartiger Aktivitäten ermöglichen.

So sind beispielsweise PowerShell-Skripts für Systemadministratoren oder Power User hilfreich, doch nur wenige Endbenutzer entwickeln und verwenden sie. Das Erkennen bösartiger PowerShell-Befehle ist schwierig, da es in Unternehmen viele legitime Anwendungsbereiche für PowerShell-Funktionen gibt. Bevor aber ein Endbenutzer PowerShell-Skripts verwenden kann, könnten Systemadministratoren das Unterzeichnen des Skripts vor dessen Ausführung anfordern. Dies würde dazu beitragen, Malware an der Ausführung bösartiger Skripts zu hindern. Auch wenn dieses Vorgehen einen gezielt vorgehenden Angreifer nicht stoppen würde, so erschwert es doch die Angriffe, so dass vielleicht einige Hacker frustriert aufgeben.

Während die Erkennung des PowerShell-Aspekts der Poweliks-Malware schwierig sein kann, könnte das Erkennen ihrer Command-and-Control-Infrastruktur und Netzwerkverbindungen schon einfacher sein. Im TrendMicro-Blog wird eine spezifische IP genannt, die als Indikator für Eindringversuche dienen kann, sodass Unternehmen ihr Netzwerk auf Verbindungen an diese IP

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

überwachen und dann untersuchen können. Die Überwachung auf ungewöhnliche Netzwerkverbindungen kann ebenfalls dazu beitragen, kompromittierte Systeme zu identifizieren, die weitere Untersuchungen erfordern. Dabei könnten auch die NetFlow-Protokolle überprüft werden, um zu sehen, welche Systeme am meisten mit externen IPs kommunizieren oder auf welchen Systemen viele Fehler bei der Authentifizierung auftreten.

Die vor Kurzem überarbeitete Malware Zeus sowie die Malware iBanking. Android können mit ähnlichen Maßnahmen wie Poweliks identifiziert werden, da auch sie „unter dem Radar“ der Sicherheitsmaßnahmen agieren. So kann die Zeus-Variante durch Überwachung des Netzwerks auf Verbindungen zur Command-and-Control-IP entdeckt werden; iBanking.Android kann dagegen mithilfe eines Anti-Malware-Tools für Mobilgeräte erkannt werden, das nach bösartigen Dateien im System sucht.

Sie sollten aber immer bedenken, dass die Angriffserkennung nur eine Komponente einer effektiven Malware-Abwehr im Unternehmen bildet. Eine strikte Reaktion auf Vorfälle im Zusammenhang mit Malware ist ebenfalls entscheidend, um die Auswirkungen eines kompromittierten Systems auf ein Minimum zu beschränken.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

KEINE ÜBERRASCHUNGEN

Es dürfte keine Überraschung sein, dass Malware sich auch weiterhin fortentwickeln und dabei einige ihrer wirksamsten Angriffstechniken automatisieren wird. Während die in Unternehmen eingesetzten Maßnahmen zur Abwehr von Malware immer ausgefeilter werden, wird diese unweigerlich neue Wege finden, um diese zu umgehen. Daher werden Unternehmen stets wachsam bleiben müssen, um potenzielle Angriffe zu kontrollieren und abzumildern.

Die von Unternehmen zur Gewährleistung von Sicherheit eingesetzten Kontrollen und Technologien müssen dabei laufend überprüft werden, um zu gewährleisten, dass sie moderne Angriffsmethoden wirksam abwehren können. Um Angreifern immer einen Schritt voraus zu bleiben, müssen Sicherheitsprogramme und -kontrollen umgehend angepasst werden, wenn neue Angriffe oder Schwachstellen bekannt werden.

Ebenso ist es für die Unternehmen entscheidend, dass sie das Management ihrer Systeme auch dahingehend evaluieren, ob bestimmte Funktionalitäten – wie zum Beispiel PowerShell-Skripts – potenziell neue Risiken in ihre Umgebungen tragen könnten, und sie müssen zusätzliche Richtlinien festlegen, die das Ausnutzen von Schwachstellen verhindern.

NICK LEWIS Information Security Officer an der Saint Louis University. Lewis hat 2005 einen Master of Science-Abschluss für Datenabsicherung von der Norwich University erworben sowie 2002 einen Master of Science-Abschluss für Telekommunikation von der Michigan State University. Vor seinem Eintritt in die Saint Louis University 2011 war Lewis an der University of Michigan und im Boston Children's Hospital tätig gewesen, der führenden Schulungsklinik für Pädiatrie der Harvard Medical School, ebenso wie bei Internet2 und an der Michigan State University.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

KOSTENLOSE ONLINE-RESSOURCEN FÜR IT-EXPERTEN

TechTarget publiziert qualifizierte Medieninhalte für den IT-Bereich, die Ihren Informationsbedarf bei der Suche nach neuen IT-Produkten und Technologien abdeckt und Ihr Unternehmen somit gezielt bei der Strategieentwicklung unterstützt. Unser Ziel ist es, Ihre Entscheidung beim Kauf von IT-Produkten durch die Bereitstellung von informativen und aktuellen Online-Ressourcen zu erleichtern und kosteneffektiv zu gestalten. Unser Netzwerk an Technologie-Webseiten bietet Ihnen Zugriff auf eine der weltweit größten IT-Online-Bibliotheken, die es Ihnen ermöglicht, mithilfe von unabhängigen Expertenmeinungen und Analysen, sowie von zahlreichen White Papern, Webcasts, Podcasts, Videos, virtuellen Messen und Forschungsberichten zu einer ausgewogenen Kaufentscheidung gelangen. Unsere Inhalte berufen sich auf die umfangreichen Forschungs- und Entwicklungskompetenzen führender Technologieanbieter, und ermöglichen es Ihnen somit, Ihr Unternehmen für künftige Marktentwicklungen und Herausforderungen zu rüsten. Unsere Live-Informationsveranstaltungen und virtuellen Seminare bieten Ihnen die Möglichkeit, Ihre täglich anfallenden Herausforderungen im IT-Bereich mit den Experten der Branche zu diskutieren. Unser Social Network, „IT Knowledge Exchange“ ermöglicht Ihnen außerdem, in Echtzeit Erfahrungsberichte mit Fachkollegen und Experten austauschen.

Startseite

Bekämpfung des Cybercrime im 21. Jahrhundert

Crimeware: Worauf sie abzielt und wie man sich verteidigen kann

Wie sich Unternehmen vor RAM-Scrapern schützen können

Abwehr moderner Betrugsmethoden

WAS MACHT TECHTARGET SO EINZIGARTIG?

Bei TechTarget steht die Unternehmens-IT im Mittelpunkt. Unsere Autoren und das Redaktions-Team sowie auch unser großes Netzwerk an Industrieexperten bietet Ihnen Zugriff auf die neuesten Entwicklungen und relevantesten Themen der Branche. TechTarget liefert klare und überzeugende Inhalte und umsetzbare Informationen für die Profis und Entscheidungsträger der IT-Branche. Wir nutzen die Schnelligkeit und Unmittelbarkeit des Internets, um Ihnen in realen und virtuellen Kommunikationsräumen hervorragende Networking-Möglichkeiten mit Fachkollegen zu ermöglichen.