Kurzvorstellung

Schutz vor Kennwortdieben

Wir werden immer abhängiger von elektronischen Geräten. Firmen verlegen immer mehr wichtige Daten in die Cloud. Und für den Zugriff auf solche Daten sind Anmeldeinformationen erforderlich – die damit immer wertvoller werden. Heutzutage setzen Angreifer bei praktisch allen verbreiteten hochentwickelten hartnäckigen Bedrohungen bereits in der Anfangsphase gestohlene Kennwörter ein.

Kennwortdiebe sind darauf gerichtet, die Sicherheitsvorkehrungen von Netzwerken und Systemen zu überwinden, um sich wichtige Anmeldeinformationen zu verschaffen. Aufgrund seiner besonderen Fähigkeiten ist Fareit daher seit mehr als fünf Jahren die beliebteste Kennwortdiebstahl-Malware. Seit seiner Entdeckung im Jahr 2012 wurde Fareit ständig weiterentwickelt, um auch den neuesten Verteidigungsstrategien entgehen zu können.

Anfangs begnügte sich Fareit noch damit, Anmeldedaten aus Web-Browsern zu entwenden, um Zugriff auf Anwendungen (z. B. Online-Banking), E-Mail-Konten und Identitäten (für Identitätsdiebstahl) zu erhalten. Seitdem hat sich Fareit jedoch zu einem weitaus aggressiveren Informationsdieb weiterentwickelt, der sich mithilfe mimetischer Taktiken versteckt (z. B. durch Änderung seines Datei-Hash-Werts bei jeder Infektion). Im Jahr 2016 tauchte eine neue Generation der Fareit-Malware für den Diebstahl von Kennwörtern auf, die eine Reihe infizierter Netzwerkressourcen einsetzt, um DDoS-Angriffe (Distributed Denial of Service) durchzuführen. Außerdem wird Fareit inzwischen als eine Art Service angeboten, d. h. Cyber-Kriminelle verdienen ihr Geld nun mit der Verbreitung von Malware, und da die Bezahlung pro Infektion erfolgt, bedeuten mehr Infektionen auch mehr Geld.

Phishing-Angriffe, über die Kennwortdiebe wie Fareit zugestellt werden, zählten in den letzten zehn Jahren zu den wichtigsten Angriffsvektoren.

Richtlinien und Vorgehensweisen zum Schutz vor Kennwortdieben

McAfee empfiehlt die folgenden Maßnahmen zum Schutz vor Kennwortdieben:

- Da Kennwortdiebe häufig über Malware verbreitet werden, gilt auch hier die Standardempfehlung: Halten Sie Ihre Malware-Schutzprodukte immer auf dem neusten Stand.
- Malware kann unbemerkt heruntergeladen werden, während die Benutzer im Internet surfen. Halten Sie Web-Browser und Add-Ons immer auf dem neuesten Stand. Das gewährleistet einen zusätzlichen Schutz vor Angriffen.
- Lassen Sie Anwendungen nicht mit Administratorberechtigungen, sondern unter einem Benutzer mit eingeschränkten Berechtigungen ausführen.

McAfee
Together is power.

- Sichern Sie die Netzwerkperipherie ab. Firewalls können verhindern, dass sich Angreifer Zugriff auf interne Anwendungen verschaffen, die zuvor durch erfolgreiche Angriffe mit Kennwortdieben kompromittiert wurden.
- Setzen Sie Anmeldeinformationen, die zur Authentifizierung im Unternehmen verwendet werden (z. B. für Web-Proxys, Datenbankanwendungen, freigegebene Ordner usw.) auch wirklich nur für die Verwendung geschäftlicher Ressourcen ein. Im vertrauenswürdigen Unternehmensnetzwerk dürfen ausschließlich Systeme zugelassen werden, die von der firmeneigenen IT-Sicherheitsgruppe verteilt oder zertifiziert wurden.
- Malware, die Kennwortdiebe enthalten kann, wird gern auch in seriöser Software eingebettet, die mit einem Trojaner versehen wurde. Um erfolgreiche Angriffe dieser Art zu verhindern, empfehlen wir dringend, strenge Mechanismen für die Übertragung und Verteilung von Software zu implementieren. Es ist äußerst sinnvoll, für in Unternehmen eingesetzte Software ein zentrales Repository zu betreiben, aus dem die Benutzer dann genehmigte Software herunterladen können.
- Falls Benutzer auch Anwendungen installieren dürfen, die nicht zuvor von der IT-Sicherheitsgruppe überprüft wurden, sollten sie zumindest dahingehend geschult werden, dass sie nur Anwendungen mit vertrauenswürdigen Signaturen von bekannten Anbietern installieren. Es ist ein gängiger Trick, „harmlose“ Anwendungen online anzubieten, in denen dann ein Kennwortdieb oder andere Malware eingebettet ist.
- Downloads aus anderen Quellen als dem Web sollten überhaupt vermieden werden. So ist bei Downloads aus Usenet-Gruppen, IRC-Kanälen, Instant-Messaging-Clients oder P2P-Netzwerken die Wahrscheinlichkeit sehr hoch, sich mit einer Malware zu infizieren. Links zu Webseiten in IRC oder Sofortnachrichten führen ebenfalls häufig zu infizierten Downloads.
- Stellen Sie ein Schulungsprogramm auf, um Phishing-Angriffen vorzubeugen. Kennwortdiebstahl-Malware wird gern über Phishing-Praktiken übertragen.

Wenn Sie glauben, dass Systeme von einem Kennwortdieb kompromittiert wurden, helfen Ihnen die folgenden empfohlenen Vorgehensweisen, eine weitere Verbreitung der Infektion einzudämmen:

- Verringern Sie die Angriffsfläche, indem Sie in Anwendungen, die dies unterstützen, zweistufige Authentifizierung aktivieren. Der Angreifer mag dann zwar über das gestohlene Kennwort verfügen, wird aber an der zweiten Stufe scheitern.
- Durch Einsatz einer Endgeräte-Firewall lassen sich Einbrüche mit gestohlenen Kennwörtern eindämmen, wenn der bei dem infizierten Computer ein- und ausgehende Datenverkehr durch Firewall-Regeln begrenzt wird.

So schützen McAfee-Produkte vor Kennwortdieben

McAfee VirusScan® Enterprise 8.8 oder McAfee Endpoint Security 10

- Halten Sie Malware-Schutz-Software auf Endgeräten immer auf dem neuesten Stand (inklusive Patches, DAT-Version und Scan-Modul). Stellen Sie sicher, dass McAfee Global Threat Intelligence (McAfee GTI) im Einsatz ist.
- Erstellen Sie Zugriffsschutzregeln, um die Installation und Inhalte von Malware zu stoppen:
  - Informationen dazu finden Sie in den Wissensdatenbank-Artikeln KB81095 und KB54812.
  - Lesen Sie die empfohlenen Vorgehensweisen zur Konfiguration von McAfee VirusScan Enterprise 8.8: PD22940.
  - Lesen Sie die empfohlenen Vorgehensweisen zur Konfiguration von McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

Eindringungsschutz-Tools sind nicht geeignet, einen erfolgreichen Angriff mit einem Kennwortdieb aufzudecken. McAfee Host Intrusion Prevention kann jedoch helfen, eine weitere Ausbreitung der Malware-Schaddaten zu verhindern, die möglicherweise einen Kennwortdieb enthalten.

- Dank benutzerdefinierter IPS-Signaturen können Sie Regeln erstellen, mit denen von der Malware generierte Dateiaktionen (z. B. Erstellen, Schreiben, Ausführen, Lesen) blockiert werden.
- Aktivieren Sie die Signatur 3894 von McAfee Host Intrusion Prevention, „Access Protection—Prevent svchost.exe executing non-Windows executables“ (Zugriffsschutz, um zu verhindern, dass „svchost.exe“ ausführbare Dateien ausführt, die nicht von Windows stammen).
- Aktivieren Sie die Signaturen 6010 und 6011 von McAfee Host Intrusion Prevention, um die Injektion sofort zu blockieren.
- Dies erreichen Sie mit zwei Unterregeltypen:
  1. Erstellen Sie im Files-Modul eine benutzerdefinierte IPS-Signatur sowie eine Unterregel mit den folgenden Kriterien:
     - Name: <Namen einfügen>
     - Rule type: Files
     - Operations: Create, Execute, Read, Write
     - Parameters: Include - Files - <Pfad/Dateiname der Malware>
       - Der Dateiname muss einen Pfad enthalten. Wenn Sie im Pfad Platzhalter verwenden möchten, beginnen Sie den Dateinamen mit „**\“ bzw. „?:\“, wenn sich der Platzhalter auf den Laufwerkbuchstaben beziehen soll (z. B. „**\Dateiname.exe“ oder „?:\Dateiname.exe“).
       - Sie können für den Parameter „Files“ keine MD5-Hash-Werte, sondern nur Pfad/Dateiname verwenden.
       - Sie können den Laufwerktyp angeben, um den Pfad auf ein bestimmtes Laufwerk zu beschränken (z. B. Festplatte, CD-ROM, USB, Netzwerk, Diskette).
     - Executables: Kann leer bleiben, sofern Sie nicht die Signatur auf bestimmte Prozesse beschränken möchten, die die Dateiaktion ausführen (z. B. explorer.exe oder cmd.exe).
  2. Erstellen Sie im Program-Modul eine benutzerdefinierte IPS-Signatur sowie eine Unterregel mit den folgenden Kriterien:
     - Name: <Namen einfügen>
     - Rule type: Program
     - Operations: Run target executable
     - Parameters: <leer lassen>
     - Executables: Kann leer bleiben, sofern Sie nicht die Signatur auf einen bestimmten Prozess als ausführbare Quelle beschränken möchten (z. B. wenn Sie verhindern möchten, dass „explorer.exe“ ein Target Executable (z. B. notepad.exe) ausführen kann).
     - Target Executables: Definieren Sie die ausführbaren Eigenschaften, für die Sie die Ausführung verhindern möchten (z. B. wenn Sie die Ausführung von „notepad.exe“ blockieren möchten, geben Sie Pfad/Dateiname der ausführbaren Datei an). Die ausführbare Datei kann mit mehreren Kriterien definiert werden (Dateibeschreibung, Dateiname, Fingerabdruck, Signaturgeber).

McAfee SiteAdvisor® Enterprise oder McAfee Web Protection

- Nutzen Sie die Reputation von Webseiten, um Benutzer vor Webseiten zu schützen oder zu warnen, über die Kennwortdiebe verbreitet werden.

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense

- Richtlinienkonfiguration bei McAfee Threat Intelligence Exchange:
  - Starten Sie im Beobachtungsmodus: Wenn Endgeräte mit verdächtigen Prozessen erkannt werden, nutzen Sie System-Tags, um die Durchsetzungsrichtlinien von McAfee Threat Intelligence Exchange anzuwenden.
  - Säubern bei Reputation „Known malicious“ (Bekannt böswillig).

  - Blockieren bei Reputation „Most-likely malicious“ (Höchstwahrscheinlich böswillig). (Die Blockierung bei Status „Unknown“ (Unbekannt) würde besseren Schutz bieten, aber möglicherweise auch den Anfangsaufwand für Administratoren erhöhen.)
  - Legen Sie für die Option „Submit files to McAfee Advanced Threat Defense“ (Dateien an McAfee Advanced Threat Defense senden) die Statuswerte „Unknown“ (Unbekannt) und darunter fest.
  - McAfee Threat Intelligence Exchange Server-Richtlinie: Akzeptieren Sie die von McAfee Advanced Threat Defense festgelegten Reputationen für Dateien, die von McAfee Threat Intelligence Exchange noch nicht erkannt wurden.
- Manueller Eingriff bei McAfee Threat Intelligence Exchange:
  - Erzwingung der Datei-Reputation (bei Betriebsmodus): Bereinigen/Löschen bei Reputation „Most likely malicious“ (Höchstwahrscheinlich böswillig).
  - „Might be malicious“ (Möglicherweise böswillig): Blockieren.
- Die Reputation innerhalb des Unternehmens kann McAfee GTI außer Kraft setzen.
  - Sie können optional festlegen, dass unerwünschte Prozesse blockiert werden (z. B. nicht unterstützte oder anfällige Anwendungen).
  - Kennzeichnen Sie die entsprechende Datei als „Might be malicious“ (Möglicherweise böswillig).
- Oder Sie erlauben einen unerwünschten Prozess zu Testzwecken:
  - Kennzeichnen Sie die entsprechende Datei als „Might be trusted“ (Möglicherweise vertrauenswürdig).

McAfee Advanced Threat Defense

- Integrierte Erkennungsfunktionen:
  - Erkennung auf Signaturbasis: Die McAfee Labs-Malware-Datenbank enthält über 600 Millionen Varianten.
  - Erkennung auf Reputationsbasis: McAfee GTI.
  - Statische Analyse und Emulation in Echtzeit: Werden zur signaturlosen Erkennung verwendet.
  - Benutzerdefinierte YARA-Regeln.
  - Vollständige statische Code-Analyse: Führt ein Reverse Engineering des Datei-Codes durch, um Attribute sowie Befehle zu untersuchen und den Code vollständig zu analysieren, ohne ihn dabei auszuführen.
  - Dynamische Sandbox-Analyse.
- Erstellen Sie Analyseprofile für die Bereiche, unter denen Kennwortdieb-Malware vermutlich ausgeführt wird:
  - Gängige Betriebssysteme, wie Windows 7, 8, 10.
  - Installieren Sie Windows-Anwendungen (Word, Excel), und aktivieren Sie Makros.
- Internetzugriff für das Analyseprogramm-Profil:
  - Viele Malware-Varianten führen ein Skript aus einem Microsoft-Dokument aus, das eine ausgehende Verbindung herstellt und den Schadcode aktiviert. Dem Analyseprogramm-Profil wird eine Internetverbindung bereitgestellt, was die Erkennungsraten weiter erhöht.

McAfee Network Security Platform

- McAfee Network Security Platform verfügt in den Standardrichtlinien über Signaturen zur Erkennung des Netzwerks Tor, das zur Übertragung von Dateien genutzt werden kann, die in Verbindung mit Kennwortdieben stehen.
- Integrieren Sie McAfee Advanced Threat Defense zur Abwehr neuer Angriffsvarianten:
  - Konfigurieren Sie die Integration von McAfee Advanced Threat Defense in der erweiterten Malware-Richtlinie.

  - Konfigurieren Sie McAfee Network Security Platform so, dass EXE-Dateien, Microsoft Office-Dateien, Java-Archivdateien und PDF-Dateien zur Überprüfung an McAfee Advanced Threat Protection gesendet werden.
  - Überprüfen Sie, ob die Konfiguration von McAfee Advanced Threat Defense auf Sensorebene angewendet wird.
- Aktualisieren Sie die Callback-Erkennungsregeln (zum Schutz vor Botnets).

McAfee Web Gateway

- Aktivieren Sie die Malware-Analyse durch McAfee Gateway.
- Aktivieren Sie McAfee GTI für URL- und Datei-Reputation.
- Integrieren Sie McAfee Advanced Threat Defense für Sandbox-Analysen und Zero-Day-Erkennung.

VirusTotal Convicter: Automatischer Eingriff

- Convicter ist ein Python-Skript, das vom automatischen Reaktionssystem von McAfee ePolicy Orchestrator® (McAfee ePO) ausgelöst wird, um eine Datei, die ein McAfee Threat Intelligence Exchange-Bedrohungsereignis erzeugt, mit VirusTotal abzugleichen.
- Sie können das Skript so ändern, dass Daten mit anderen McAfee Threat Intelligence Exchange-Modulen, z. B. GetSusp, ausgetauscht werden.
- Wenn der Schwellenwert zum Vertrauen der Community erreicht wird, setzt das Skript automatisch die Unternehmensreputation fest. Vorgeschlagener Schwellenwert: 30 % der Anbieter und zwei wichtige Anbieter müssen zustimmen.
- Filter: Target File Name Does Not Contain (Name der Zieldatei enthält nicht): McAfeeTestSample.exe.
- Dies ist ein kostenloses, von der Community unterstütztes Tool (wird von McAfee nicht unterstützt).

McAfee Active Response

- McAfee Active Response findet hochentwickelte Bedrohungen und reagiert darauf. Wenn die Anwendung zusammen mit Bedrohungsdaten-Feeds von McAfee Labs, Dell SecureWorks oder ThreatConnect eingesetzt wird, können Sie nach neuen Bedrohungen suchen und diese entfernen, bevor sie die Gelegenheit haben, sich auszubreiten.
- Benutzerdefinierte Kollektoren ermöglichen die Entwicklung spezieller Tools, um mit Kennwortdieben in Verbindung stehende Kompromittierungsindikatoren zu finden und zu identifizieren.
- Auslöser und Reaktionen werden vom Benutzer zusammengestellt, um Aktionen festzulegen, die beim Eintreten bestimmter Bedingungen durchgeführt werden sollen (z. B. wenn bestimmte Hash-Werte oder Dateinamen gefunden werden, soll automatisch ein Löschvorgang erfolgen).

Weitere Informationen

Phishing Attacks Employ Old but Effective Password Stealer (Phishing-Angriffe nutzen alte, aber bewährte Kennwortdiebe)

Fareit Virus Profile (Profil des Fareit-Virus)

Fareit Virus Profile (Profil des Fareit-Virus)

McAfee
Together is power.

3185_0617_brf-protecting-against-password-stealers
Juni 2017

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/de