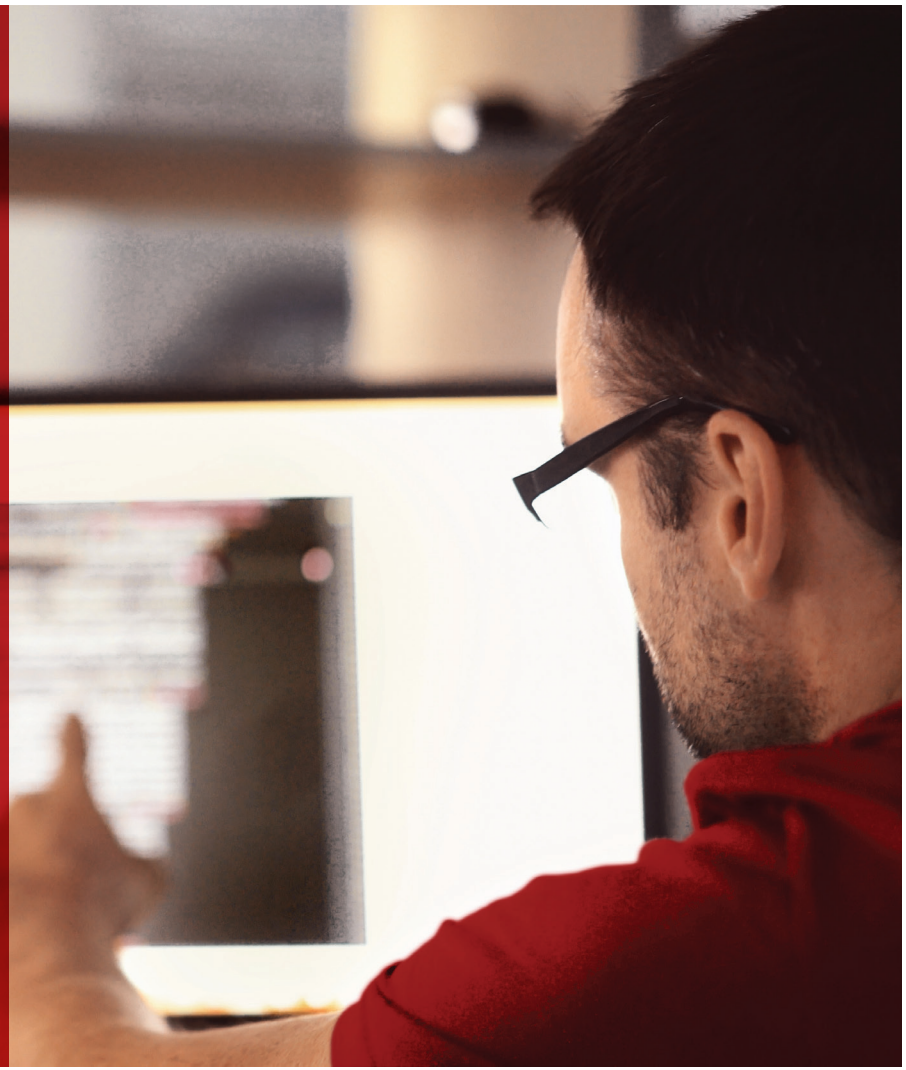
McAfee
Together is power.

Schutz vor Pinkslipbot

W32/Pinkslipbot ist eine sich selbst verbreitende Malware-Familie, deren Aufgabe der Diebstahl persönlicher und finanzieller Daten von seinen Opfern ist. Die Malware ermöglicht die vollständige Kontrolle infizierter Systeme durch eine kommandobasierte Backdoor, die vom Kontroll-Server betrieben wird, sowie durch eine VNC-basierte Backdoor (Virtual Network Computing). Pinkslipbot kann sich auch über Netzwerkfreigaben auf andere Systeme in der Umgebung verbreiten und mit dem Kontroll-Server kommunizieren, um eine aktuelle Version seiner selbst herunterzuladen.



Pinkslipbot wurde erstmals im Jahr 2007 entdeckt, doch die dahinter stehende Gruppe hat die Code-Basis gepflegt, indem sie inkrementelle Aktualisierungen hinzufügte sowie alle paar Monate eine neue Version veröffentlichte.

Mit den von Pinkslipbot gestohlenen Daten können Angreifer den Standort, die Organisation und den Inhaber des infizierten Systems ermitteln. Diese Informationen lassen sich an Dritte verkaufen (vor allem, wenn bekannte Organisationen oder Unternehmen infiziert wurden), und sobald die Zahlung eingegangen ist, laden die Angreifer in deren Auftrag gezielte Malware auf den kompromittierten Computer.

Einen detaillierten technischen Einblick in Pinkslipbot erhalten Sie im *McAfee Labs Threat-Report vom Juni 2016*. Im Bericht werden die Erstinfizierung, die Vorgehensweise für die Verbreitung, technische Details sowie allgemeine Schutzmöglichkeiten erläutert.

Richtlinien und Vorgehensweisen zum Schutz vor Pinkslipbot

Mit diesen allgemeinen Richtlinien und Vorgehensweisen können Sie sich vor Pinkslipbot schützen.

Zur Absicherung der Peripherie sollten Sie nicht genutzte Ports an allen Eintrittspunkten des Netzwerks blockieren, Verbindungsanfragen von und zu bekannt böswilligen IP-Adressen abweisen sowie Netzwerkfreigaben absichern, um die Bewegung von Pinkslipbot innerhalb des Netzwerks aufzuhalten. In den meisten Umgebungen sollten Sie auch die Autorun-Funktion von Microsoft Windows deaktivieren. Es ist absolut wichtig, das Windows-Betriebssystem sowie Anwendungen mit den neuesten Patches zu aktualisieren sowie die Malware-Schutz-Software auf dem neuesten Stand zu halten.

Nicht gepatchte Systeme enthalten Schwachstellen, die ausgenutzt werden können. In jeder Umgebung ist eine erfolgreiche Patch-Verwaltung notwendig. Wenn Patches vom Anbieter veröffentlicht werden, sollten sie unverzüglich getestet, überprüft und implementiert werden. In Fällen, bei denen das Patchen aufgrund von Abhängigkeiten mit einer älteren Version nicht möglich ist, sollte es einen weiteren Mechanismus geben, der die Ausnutzung bekannter Schwachstellen verhindert. Eine der effektivsten Methoden zur Abwehr von Pinkslipbot sowie weiterer Malware ist eine energische Patch-Verwaltung.

Obwohl Pinkslipbot in erster Linie per „Drive-by-Download" auf von Exploit-Kits kompromittierten Webseiten übertragen wird, gelangen die Opfer meist über Phishing-E-Mails dorthin. Wenn Sie E-Mails als „intern" oder „extern" kennzeichnen, können Ihre Benutzer Betrugs- oder Phishing-E-Mails leichter erkennen und klicken nicht so schnell auf unbekannte böswillige Links.

Pinkslipbot wird teilweise im Speicher ausgeführt, sodass es nicht genügt, einfach nur Systeme zu patchen, einen vollständigen Scan durchzuführen oder ein Malware-Säuberungs-Tool durchlaufen zu lassen. Infizierte Systeme erfordern einen Neustart, um die Malware aus dem Speicher zu entfernen, und sollten anschließend zur Sicherheit noch einmal überprüft werden. Wir raten auch zu starken Kennwörtern, um die Kompromittierung durch Wörterbuchangriffe zu vermeiden, sowie zum Deaktivieren des Autostarts und dem Gewähren minimaler Berechtigungen.

Pinkslipbot ist eine Weiterentwicklung des berüchtigten Trojaners Zeus. Ein schwaches Anmeldekennwort für ein Windows-System genügt, um eine Infektion durch Pinkslipbot zu ermöglichen – auch ohne Exploit-Kit und Benutzeraktivitäten. Sobald ein System infiziert ist, werden alle vom System durchgeführten Aktivitäten protokolliert und den Angreifern gesendet. Mit der Einführung der individuellen und sicheren Kommunikation mit den Kontroll-Servern wird die Entdeckung und Analyse von Pinkslipbot erheblich erschwert. Der bisherige Entwicklungsverlauf legt nahe, dass die Malware mit jeder neuen Version noch gefährlicher wird. Wenn Sie Ihre Umgebung kennen sowie unsere Empfehlungen zu Richtlinien und Vorgehensweisen umsetzen, können Sie den von Pinkslipbot verursachten Schaden minimieren.

So kann McAfee-Technologie vor Pinkslipbot schützen

McAfee VirusScan Enterprise (VSE) und McAfee Endpoint Security (ENS) 10

McAfee VirusScan Enterprise und McAfee Endpoint Security 10 bieten hochentwickelten Malware-Schutz für Endgeräte. McAfee VirusScan Enterprise wurde durch McAfee Endpoint Security 10 ersetzt, das mit einer optimierten Plattform schnellere Verarbeitung ermöglicht. Die McAfee-DAT-Dateien für McAfee VirusScan Enterprise und McAfee Endpoint Security 10 enthalten Erkennungs- und Bereinigungsfunktionen für Pinkslipbot-Komponenten. McAfee VirusScan Enterprise und McAfee Endpoint Security 10 bieten dank Speichererkennung, Rootkit-Schutz, Verhaltenserkennung und statischen Mechanismen mehrstufigen Schutz. Um zusätzliche Schutzmaßnahmen gegen neue Varianten hinzuzufügen, können Sie Zugriffsschutzregeln implementieren, die die Infektion mit Pinkslipbot verhindern.

- Erstellen und testen Sie eine Zugriffsschutzregel, mit der alle Prozesse am Ausführen sowie Erstellen neuer ausführbarer Dateien unter C:\Users*\AppData\Roaming\Microsoft**.exe gehindert werden.
- Erstellen und testen Sie eine Zugriffsschutzregel, mit der die Prozesse cscrpit.exe und wscript.exe am Lesen, Ausführen sowie Erstellen von WPL-Dateien im Ordner %LOCALAPPDATA%\Microsoft\ gehindert werden. Hierbei handelt es sich meist um JavaScript-Dateien. Durch das Blockieren dieser Dateien verhindern Sie, dass die Malware neue Versionen herunterladen kann.
- Erstellen und testen Sie eine Zugriffsschutzregel, mit der die Prozesse cscrpit.exe und wscript.exe am Lesen, Ausführen sowie Erstellen von Dateien im Ordner %UserProfile% gehindert (sofern möglich).
- Erstellen und testen Sie eine Zugriffsschutzregel, mit der verhindert wird, dass „updates_*new.cb“, „upd_* cb“ und „updates*_new.cb“ ausgeführt werden und neue Dateien erstellen können. Hierbei handelt sich meist um Pinkslipbot-Konfigurationsdateien. Durch das Blockieren dieser Dateien verhindern Sie, dass sich die Malware aktualisieren kann.
- Erstellen und testen Sie für die Ports 65200 bis 65400 eine Zugriffsschutzregel für die Prozesse iexplorer.exe und explorer.exe. Da sich Pinkslipbot in diese Prozesse injiziert, können Sie durch die Blockierung dieser Ports für diese Prozesse verhindern, dass Pinkslipbot mit seinem Kontroll-Server kommunizieren kann.

- Implementieren und testen Sie Zugriffsschutzregeln, mit denen die Remote-Ausführung von autorun.inf-Dateien verhindert wird.

McAfee Host Intrusion Prevention (HIPS)

McAfee Host Intrusion Prevention schützt Systeme vor Zero-Day-Bedrohungen, indem die Lösung ein signatur- und verhaltensbasiertes Eindringungsschutzsystem mit einer dynamischen, statusbasierten Firewall kombiniert. Geplante Inhaltsaktualisierungen schützen Systeme vor Anwendungs- und Betriebssystemschwachstellen, noch bevor Patches verfügbar sind. Stärken Sie die Sicherheit Ihrer Umgebung mit Signaturen, damit die Systeme vor den typischen Methoden geschützt sind, mit denen Malware häufig verwendete Software ausnutzt.

- Testen und aktivieren Sie in McAfee HIPS 6010 den integrierten Schutz vor generischen Anwendungs-Hooks.
- Testen und aktivieren Sie in McAfee HIPS 6011 den integrierten Schutz vor generischen Anwendungsaufrufen.
- Isolieren Sie mit Pinkslipbot infizierte Systeme, indem Sie ihnen eine Richtlinie zuweisen, bei der die Firewall-Regel alle Ports außer den Verwaltungsports blockiert.

McAfee Endpoint Security 10 und McAfee Host Intrusion Prevention sind in McAfee Complete Endpoint Protection enthalten.

McAfee Web Gateway (MWG)

Typische Methoden zur Verbreitung von Pinkslipbot sind Drive-by-Downloads und Links in E-Mails. McAfee Web Gateway bietet hochleistungsfähige Web-Sicherheit, mit der Systeme vor böswilligen Webseiten geschützt werden. Die Lösung kann als dedizierte Hardware-Appliance oder als VM-Abbild (virtuelle Maschine) bereitgestellt werden.

- Konfigurieren Sie McAfee Web Gateway für Spam-Filterung.
  - Spam-Filter bieten Schutz vor:
    - Böswilligen IP-Adressen
    - Böswilligen URLs
    - E-Mail-Spam
- Aktivieren Sie GAM-Untersuchungen.
- Aktivieren Sie McAfee GTI für URL- und Datei-Reputation.
- Integrieren Sie McAfee Advanced Threat Defense für Sandbox-Analysen und Zero-Day-Erkennung.

McAfee Active Response (MAR)

McAfee Active Response bietet kontinuierliche Erkennung von und Reaktion auf Systeme, die von hochentwickelten Bedrohungen wie Pinkslipbot angegriffen werden. Durch die automatische Ereignisüberwachung können Sie Kompromittierungsindikatoren finden, die auf eine Malware-Infektion hinweisen.

- Wenn sich folgende Domänen in einem DNS-Cache finden lassen, kann dies auf eine Pinkslipbot-Infektion hinweisen:
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org
  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org
  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- Führen Sie die folgenden DNS-Cache-Abfragen durch, um zu bestimmen, ob Systeme mit einer der oben genannten Pinkslipbot-Domänen kommuniziert haben.
  - DNSCache where DNSCache hostname equals "[Pinkslipbot-Domäne]"
- Diese Abfrage gibt eine Liste der von den Systemen in der Umgebung hergestellten Verbindungen mit Pinkslipbot-Domänen zurück. Sie können auf einfache Weise feststellen, welche Systeme mit diesen Domänen kommunizieren, indem Sie auf den Eintrag klicken und die entsprechenden Systeme anzeigen.
- Verwenden Sie eine lokale Firewall wie McAfee ENS 10 oder McAfee HIPS, um von Pinkslipbot betroffene Systeme zu isolieren. Weisen Sie diesen Systemen dazu in McAfee ePO eine Firewall-Sperrrichtlinie zu.
- Führen Sie auf dem System einen vollständigen On-Demand-Scan von McAfee ENS 10 oder McAfee VSE aus, indem Sie in McAfee ePO festlegen, dass der On-Demand-Task sofort ausgeführt werden soll. Reaktivieren Sie den Agenten, um den Scan zu starten.

Weitere Informationen

McAfee-Webinar-Reihe zu Malware: Pinkslipbot

Dieses Video bietet einen Überblick über Pinkslipbot, eine Übersicht der Regionen und Branchensektoren, Eigenschaften und Symptome sowie Empfehlungen zum Schutz vor dieser Bedrohung.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de