Baden-Württemberg
LANDESKRIMINALAMT

Warnmeldung für Unternehmen und Behörden

PRESSESTELLE LKA BW
TELEFON 0711 5401-2012 ODER -3012 FAX 0711 5401-1012
PRESSESTELLE-LKA@POLIZEI.BWL.DE WWW.LKA-BW.DE

Stuttgart, 18. April 2019

Hintertür (sog. Backdoor) in mehreren Unternehmen festgestellt

Das Landeskriminalamt Baden-Württemberg, Inspektion 510 Cybercrime, führt aktuell Ermittlungen zu mehreren Fällen der gewerbs- und bandenmäßigen Erpressung mittels einer Ransomware zum Nachteil von Wirtschaftsunternehmen. Die bisherigen Angriffe auf betroffene Firmen führten zur Verschlüsselung sämtlicher Daten. Für eine mögliche Entschlüsselung der Daten wird eine Lösegeldzahlung gefordert.
Eine Analyse der bislang betroffenen IT-Systeme zeigt einen gemeinsamen Angriffsvektor, dessen Merkmale der Anlage "Indikatoren" entnommen werden können. Diese Indikatoren können von IT-Verantwortlichen genutzt werden, um eine mögliche Betroffenheit durch eine sog. Backdoor zu überprüfen und entsprechende Maßnahmen einzuleiten.
Sollten Sie bei Ihrer IT-Infrastruktur feststellen, dass die genannten Indikatoren zutreffen, ist nach derzeitigem Stand davon auszugehen, dass Angreifer unberechtigt Zugang zu Ihren IT-Systemen haben.

In diesem Fall empfehlen wir eine vollständige Überprüfung aller IT-Systeme. Bitte berücksichtigen Sie dabei auch, dass aktuell genutzte Passwörter eventuell ausgespäht wurden. Wir empfehlen darüber hinaus, zu überprüfen, ob unberechtigt Benutzerkonten bzw. Passwörter verändert oder hinzugefügt wurden.
Bei der Bereinigung Ihrer IT-Systeme kann es mitunter sinnvoll sein, entsprechende IT-Sicherheitsdienstleister hinzuzuziehen.
Sollten Sie eine Kompromittierung Ihrer IT-Systeme feststellen, empfehlen wir Ihnen Strafanzeige bei der für Sie zuständigen Zentralen Ansprechstelle Cybercrime (ZAC) zu erstatten.

Zentrale Ansprechstelle Cybercrime
beim Landeskriminalamt Baden-Württemberg

Erreichbarkeit der ZAC:
Telefon: +49 (0)711 5401 2444
E-Mail: cybercrime@polizei.bwl.de

Anlage 1 – Indikatoren

Bisherige Analysen einzelner kompromittierter Windows-Systeme zeigten folgende voneinander unabhängige Merkmale:

Möglicherweise (zyklisch) auftretende Netzwerkkommunikation

Im Nachfolgenden sind verdächtige Domains sowie die jeweils zugeordneten IP-Adressen (Stand: 17.04.2019) aufgelistet. Die IP-Adressen können variieren und sollten deshalb tagesaktuell verifiziert werden. Eine abweichende IP-Adressauflösung der www-Subdomain ist ggf. zu berücksichtigen.

Verdächtige Domains	Zugewiesene IP-Adressen
rasggagadfa.pw	185.163.45.181
hitterda.icu	185.163.45.181
suppl.icu	185.163.45.181
gidjshrvz.xyz	185.225.17.150
winserver.icu	185.225.17.150
vinomag.pw	185.225.17.150
ref345.icu	185.225.17.150
esupdate.icu	195.123.246.17

Verdächtige Dateien
Fundort: \Windows\Temp

termsvc.dll

- Hierzu wurde der Registry-Eintrag von der regulären 'termsrv.dll' auf die verdächtige Datei im Pfad \Windows\Temp\ geändert:
  HKLM:\SYSTEM\CurrentControlSet\Services\TermService\Parameters\ ServiceDll
- Ein Löschen der Datei ist aufgrund der Einbindung in den Remotedesktop-Dienst im laufenden Zustand ggf. nicht möglich.

bekannte Größen	123.904 oder 57.856 Bytes
bekannte MD5-Hashes	930496D2D14BEA80F3310660FCEA48A3 **oder** 8AB1F8E274316BE89BB63E987D32CA88

64.dll

- Die Datei ist bereits auch in anderen Namensvarianten (z.B. 64.Vvdll) aufgetreten.

bekannte Größen	990.720 oder 1.020.416 Bytes
bekannte MD5-Hashes	91B1D09F8303D0A090F0C88CE9D36C7C **oder** AE75B3D779594CCE5A4B761031FCD6CA

netconwiz.ini

- Enthält Konfigurationsparameter in Textform

bekannte Größen	136.444 Bytes
bekannter MD5-Hash	3375A5E55FA0228689C8946D7FF5016B

Verdächtige Skripte (Power-Shell oder VBS)
Fundort: \Users*<Name-Administrator-Account>*\AppData\Local\Temp*<1-2-stellige-Zahl>*

installer.ps1

bekannte Größen	35.444 Bytes
bekannter MD5-Hash	F168CB2CB3B712A61A2E6DDC51C87DDD
Bemerkung	Enthält evtl. auskommentierte URL z.B. 'ref345.icu'.

installer.vbs

bekannte Größen	95 Bytes
bekannter MD5-Hash	AAAE6AD0B5D724B64D8A8C03DC8D2654