Anlage – 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