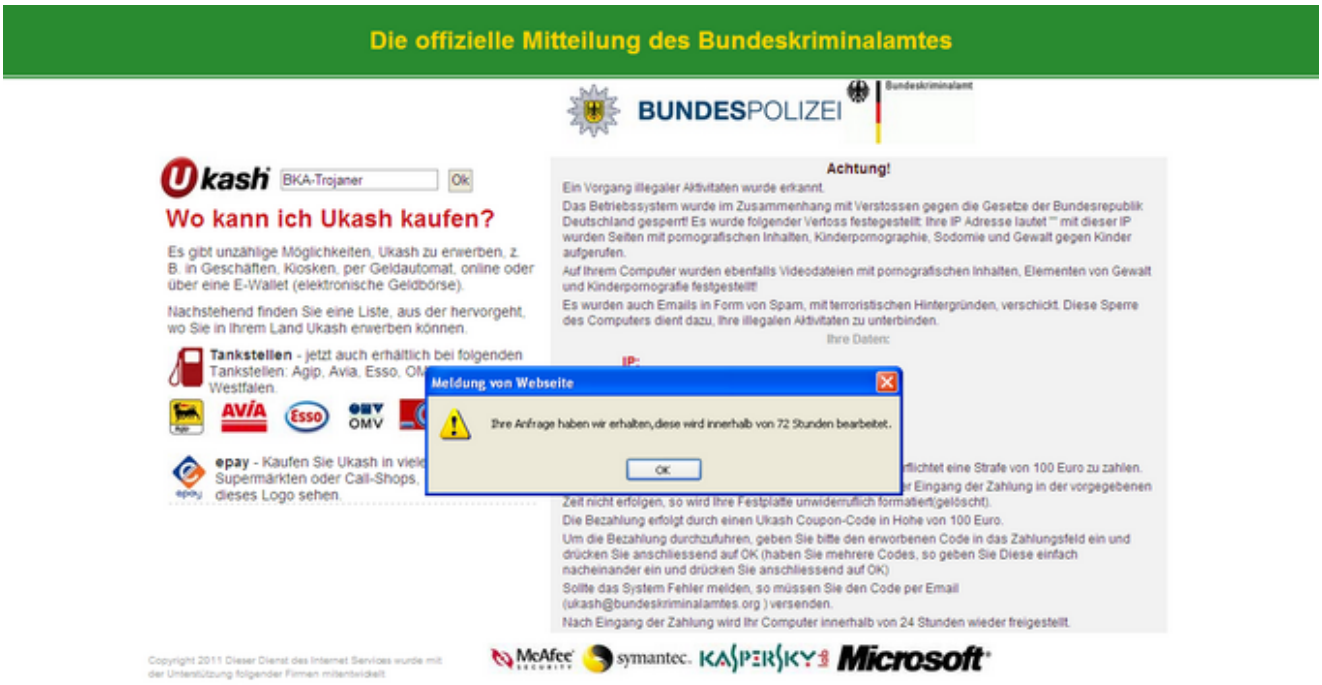
BKA-Trojaner (Ransomware)

evild3ad.com/405/bka-trojaner-ransomware/

evild3ad

Seit dem 24.03.2011 wird im Internet vor einer neuen Betrugs- bzw. Erpressungsvariante von Cyberkriminellen mittels Schadsoftware gewarnt (Ransomware). Die Schadsoftware soll auf den infizierten PC‘s sämtliche Zugriffe auf das System blockieren und eine angeblich offizielle Mitteilung der Polizei einblenden, in der der Nutzer zur Zahlung einer vermeintlichen Strafe via Ukash in Höhe von 100 Euro aufgefordert wird. Andernfalls werde seine Festplatte gelöscht.

Nach der Eingabe des Ukash Voucher Codes bzw. nach der Eingabe eines Phantasiewertes erscheint folgendes Fenster…eine “Freischaltung” erfolgt jedoch nicht!



Dateisystem:
Im Rahmen einer Infektion werden unter C:\Dokumente und Einstellungen\"Benutzerkonto"\Lokale Einstellungen\Temporary Internet Files\Content.IE5\ mehrere Unterverzeichnisse mit zufälligen Namen (8 Zeichen) angelegt (z.B. "SRKBUTOP", "S6JZACFV", "DNYHQU88").

C:\Dokumente und Einstellungen\"Benutzerkonto"\Lokale Einstellungen\Temporary Internet Files\Content.IE5\SRKBUTOP\QQkFBwQEBwECAQMGEkcJBQcEBgUDDQ0HAw==[1].htm
C:\Dokumente und Einstellungen\"Benutzerkonto"\Lokale Einstellungen\Temporary Internet Files\Content.IE5\SRKBUTOP\setup[1].exe (MD5: ba9a4732e63ed72d1c77d4a2828f777e)

Registry:
Damit der BKA-Trojaner bei jedem Neustart eines infizierten PC's automatisch wieder aufgerufen wird, legt er eine Kopie der EXE und folgenden Registry-Key an:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon –>C:\Programme\T-Online\T-Online_Software_6\Browser\test.exe (MD5: ba9a4732e63ed72d1c77d4a2828f777e)

Connections:
IP: 70.86.96.219:80
Host: http://tools.ip2location.com
IP: 78.26.187.235:80 (Ukraine)

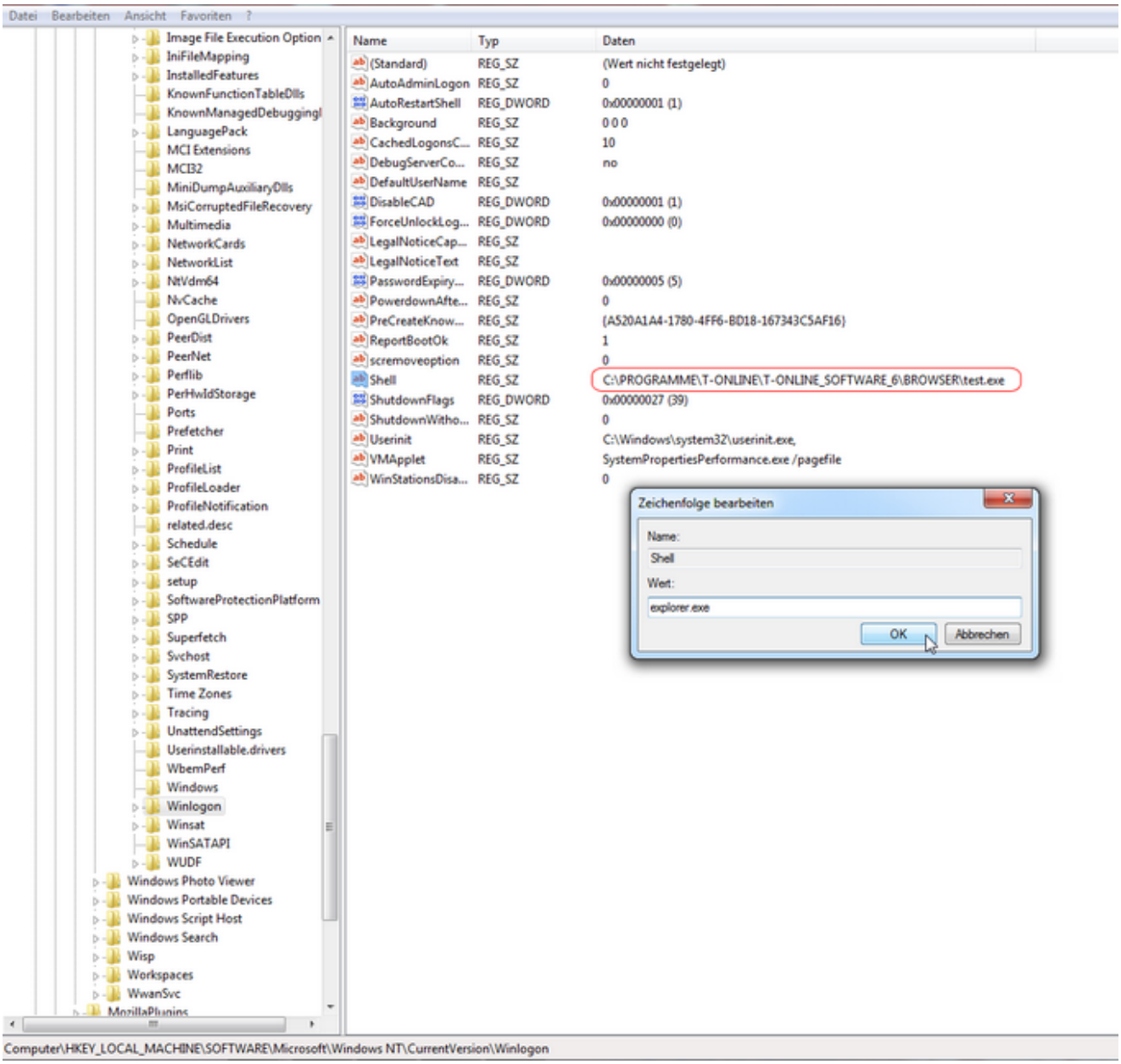
Infektionsweg:
Der BKA-Trojaner wird primär über Webseiten mit pornografischem Inhalt verbreitet. Die Infektion erfolgt dabei, ohne Interaktion des Nutzers, über eine ungepatchte Betriebssystem-, Browser- oder Anwendungsschwachstelle beim Zugriff auf den präparierten bzw. manipulierten Web-Server (Drive-By-Infektion).

z.B. Exploit.Java.CVE-2010-0840.b

Bereinigung des infizierten Systems:
1. Neustart des Rechners
2. Drückt F8 (ggf. F5) vor Erscheinen des Windows-Start-Bildschirmes, um in das erweiterte Optionsmenü von Windows zu gelangen. Wählt hier den “Abgesicherten Modus mit Eingabeaufforderung“ aus.
3. Wählt anschließend das Benutzerkonto “Administrator” und gebt dann in der Konsole “regedit” ein, um den Reg-Editor von Windows zu starten.
4. Navigiert dann zu dem Registry-Schlüssel “Shell” unter folgendem Pfad:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

5. Doppelklickt auf den Registry-Schlüssel “Shell”. Entfernt hier den Dateipfad zu der EXE des BKA-Trojaners (Kopie) und gebt “explorer.exe” ein. Die bösartigen Dateien solltet ihr dann nach einem Neustart des Rechners mit einem Virenscanner entfernen (Tipp: Kaspersky Rescue Disk 10).



Video:

Download Sample
PW: infected