Softwaretipps

Dies ist ein Artikel den ich gerne in Wiki Systemen ablege, der aber eher 08/15 Natur ist, weil er wirklich nur dafür da ist um Software zu empfehlen:

Websachen

- Listen to Wikipedia: macht zu jeder Änderung bei irgendwelchen Artikeln bei Wikipedia einen Ton. Kommt was sehr meditatives bei raus. (github-source)
- Blip.net, Sharedrop.io (Badware Risk) oder localsend.org: OpenSource Kopien von Googles Quick Share oder Apples AirDrop
- draw.io: sonst müsstet ihr euch sicher vorab mindestens eine halbe Stunde lang um Visio-Lizenzen kümmern, habt ihr kein Bock drauf, oder?
- Archive.today, archive.ph... Mit Extension für Firefox: Haste irgendwo ne Paywall klickst auf die Extension und dann kannste den Artikel lesen.

Obfuscation

- AdNauseam: uBlock Origin mit Aufsatz um alles was geblockt wird unsichtbar anzuklicken, was Interessensbasierte Werbung komplett unmöglich macht
- TrackMeNot: Führt im Hintergrund verschiedene Websuchen durch um die Interessensprofilbildung von Suchmaschinen zu stören.

  Diese Erweiterungen sind relativ schnell aus dem Google Chrome Webstore rausgeflogen, weil sie erste wirkliche Gegenmaßnahmen gegen Googles Kerngeschäft waren. Daher werden sie nicht mehr ohne weiteres in Chrome-basierten Browsern funktionieren (also auch MS Edge und Opera)...

Windows

- Everything: Indexiert sich NTFS Filesysteme und UNC Pfade und kann diese ähnlich MAC OS X Spotlight in Sekundenbruchteilen durchsuchen, weil die Datenbank effizienter als beim Windows-Suchindex gewählt ist und vollständig lokal läuft.

- ShareX: Eher Endanwenderunfreundliches, dafür funktionsüberladenes Screenshotting-Tool. (Eckpunkte: Komplette Workflow-Automation, Anbindung eigener APIs als Bildsharing etc. Extrembeispiel: Screenshot -> Auf Share speichern -> auf Facebook hochladen -> auf Google hochladen -> auf FTP hochladen -> FTP Link nehmen -> QR Code von FTP-Link generieren -> Bild des QRs auf SMB-Share speichern -> den Pfad des Bilds auf dem SMB-Share in die Zwischenablage kopieren...)
- Maltego: Das Go-To für OSINT mit Fokus auf Netzwerke, oft als Hackingtool von AV-Software erkannt, weil es auch als solches eingesetzt wird. Dennoch ist Social Engineering nur Psychomanipulation und kein richtiger "Virus", weshalb es etwas irrsinnig ist, das AV schon bei OSINT-Tools anschlägt.
- nmap: Schneller Überblick über ein Netzwerk. Netzwerk- & Portscanner mit erweiterten Funktionen, z.B. Erraten eines Rate Limitings eines IDS-Systems und adaptive Anpassung an dieses inkl. spezifische Randomisierung der Portscans.
- Zenmap: stark eingeschränkte GUI für Nmap
- Chocolatey: ein Paketmanager für Windows. Mit den "choco upgrade all at" Paketen automatisierte Softwareupdates.
- EasyBCD: Bootsektor aus laufendem Windows bearbeiten. (VORSICHT: Einige Probleme mit Bitlocker und aktuellen vermurksten UEFI-Systemen)
- DISM: Systemtool in jedem Windows. Es lohnt sich, sich dazu mal einzulesen, weil es beinahe sämtliche Downloads von irgendwelchen Images und Neuinstallationen verhindern kann. z.B. Editionswechsel von dem nur für Endanwender gedachten Windows 11 Pro hin zum Windows 11 Enterprise, welches die einzige Variante ist, für die Firmenkunden Support erhalten. Ebenfalls die Vorstufe für PXE-Boot zur Imageerstellung.
- AnyBurn: ImgBurn ohne AdWare-Ausrutscher

Workarounds

- uupdump: baut sich eine tagesaktuelle Windows ISO von den Windows Update Servern zusammen. Geht dafür dann alle Einzelschritte die man sonst händisch tut (RemoveApps Scripts, DISM, Updateintegrationen, WIM-ESD converts etc) halbwegs automatisch durch.
- Windows Update Assistent: Vollständig an GPO und SCCM (oder halt dem alten WSUS) vorbei ein Windows auf aktuellen Patchstand bringen, ohne Vertrauensverlust zur Domäne.
- WSUS Offline Update: Umgeht genauso die GPO, sofern der Download der Windows Update Kataloge außerhalb des durch die GPO beschränkten Netzwerks passiert ist.
- MouseJiggler: Hebelt den Bildschirmtimeout durch automatisierte Cursorbewegung aus. Praktisch für Citrix- oder RDP-Umgebungen ohne Administrationsrechte. Bei "Zen Jiggle" vorsichtig sein, manche Systeme brauchen einen tatsächlich bewegten Mauszeiger (Zen Jiggle funktioniert aber mit vielen Citrix Umgebungen)

    - in Kombination mit: Don't sleep setzt man einen Wake Lock der nur über erzwungenes Herunterfahren von Windows (Sprich: Auch Citrix Workern) beendet werden kann.
- Bugmenot.com - eine Sammlung geteilter Logindaten für Websites wie VMware die ihre Downloads nur nach Anmeldung anbieten
- Die user.js von Firefox ermöglicht es about:config Werte zu setzen, auch dann noch, wenn about:config über Gruppenrichtlinien gesperrt wurde.

Android

- Terminal Emulator: Irgendwann benötigt man ein Terminal auf einem Android Telefon, versprochen.
- Toast Source: Die Quelle von Toast-Benachrichtigungen herausfinden
- Sesame Shortcuts: Bohrt die Suche des Nova Launchers etwas auf, so dass z.B. auch Kontakte aus dem Adressbuch und anderes in der direkten Nova-Launcher Suche auftauchen.
- Corona Contact Tracing Germany: Ein Fork der offiziellen deutschen CoronaWarnApp, der - zusammen mit der Warn-App-Companion -genaueres Tracking durch Datenbankexport ermöglicht. Dinge wie exakte GPS-Pinpoints sind so dank Google Maps Standorthistorie möglich. Das ermöglicht einen weitaus genaueren Einblick, wo und wann eine Infektion passiert ist. Auf gerooteten Geräten kann der Zwischenschritt über die CCTG App übersprungen werden, weil beim root die Datengrenze zwischen den Apps aufgehoben ist.

Klassiker

- GIT: Muss man GIT erklären?

Version #16
Erstellt: 2023-08-15 09:30:39 UTC von Konstantin
Zuletzt aktualisiert: 2026-04-07 08:28:08 UTC von Konstantin