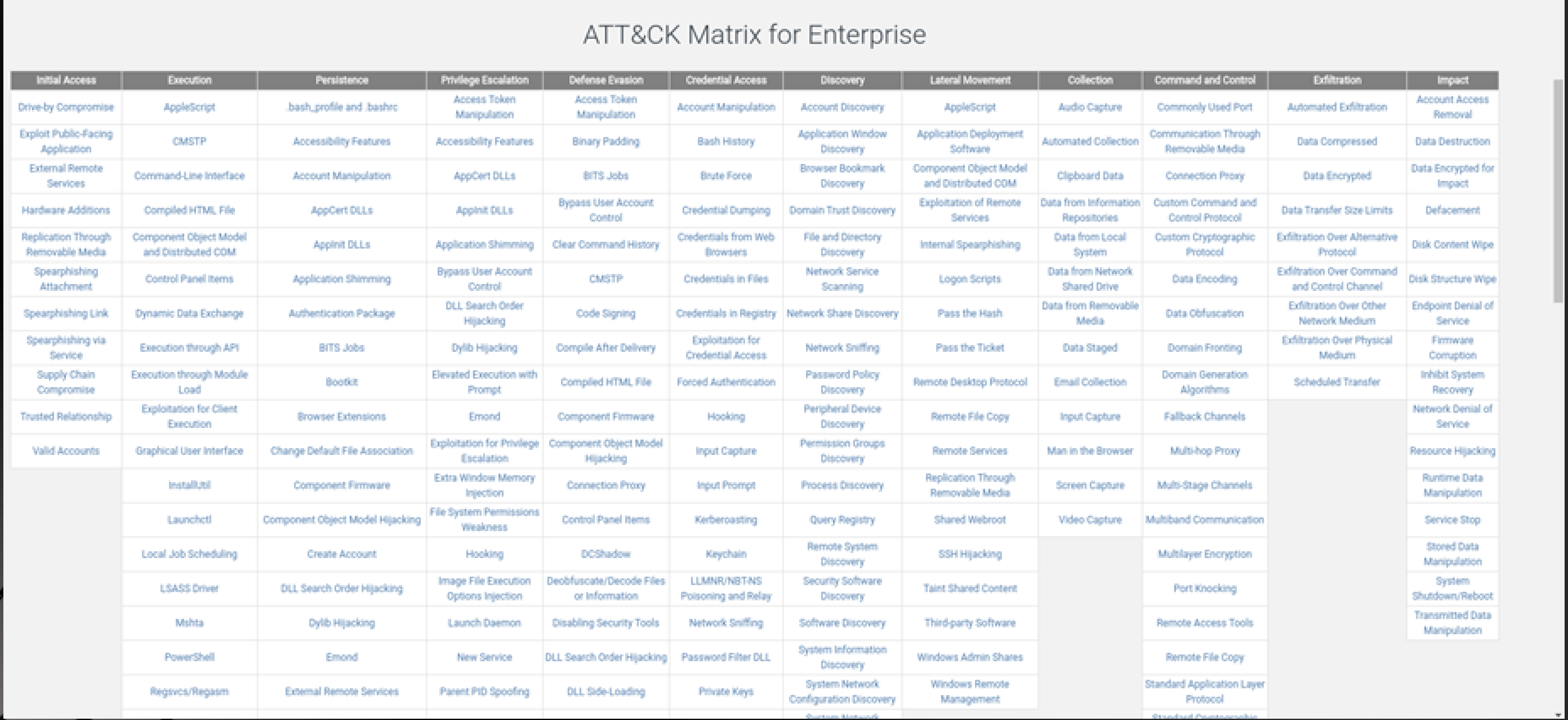
Internet Allow Listing

MITRE



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
						System Network			Standard Cryptographic		

Why Denylists Fail

Map of the Internet, The Opte Project, www.opte.org

The Internet is big…
… really big

You just won't believe how vastly hugely mindboggingly big it is…

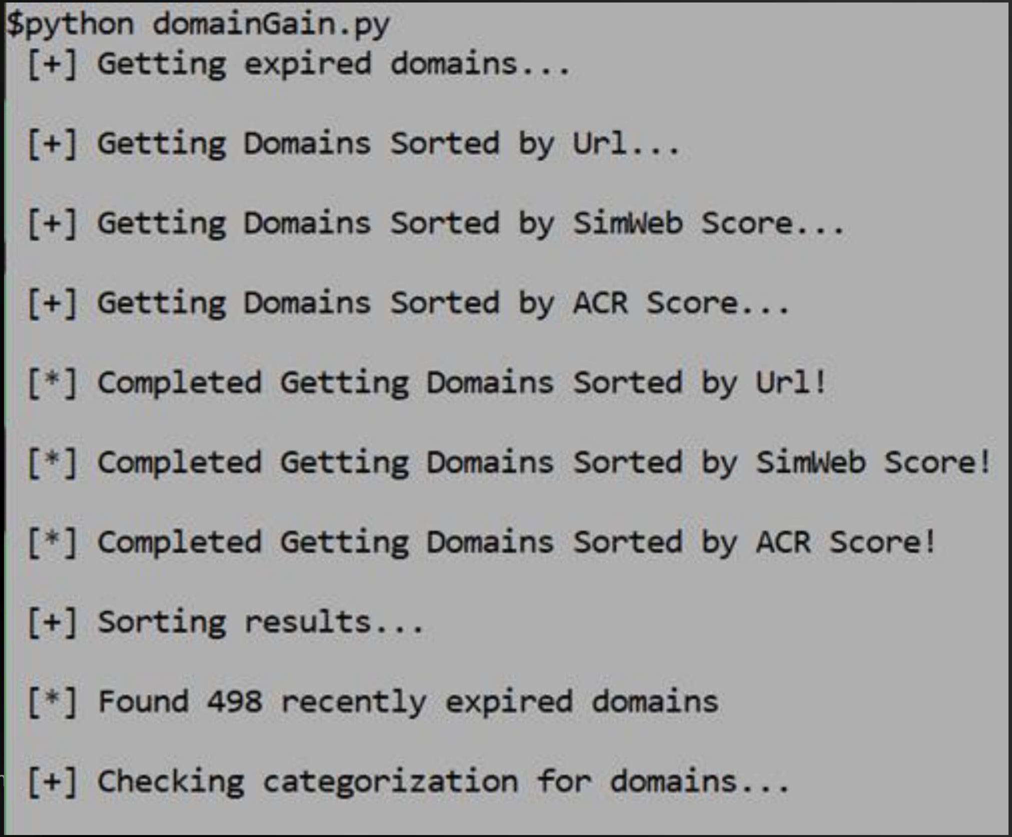
Most of it is worthless.. and Evil!

Many of your users will not stop clicking until they visit every site

Getting Domains

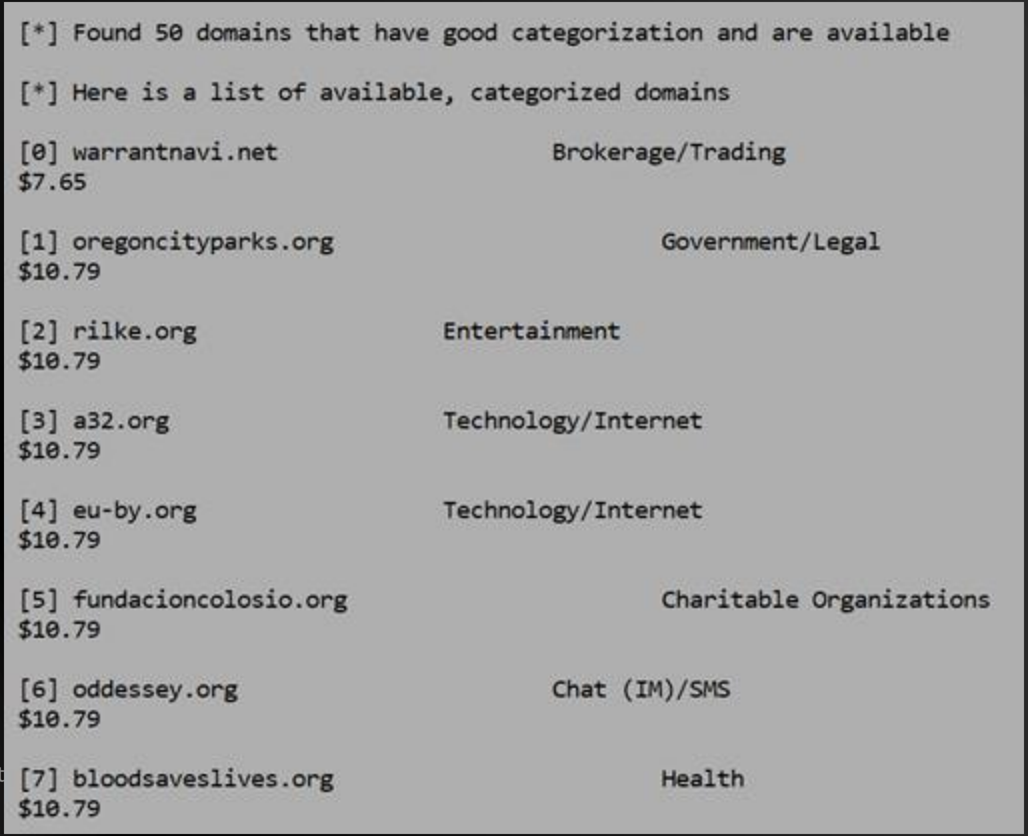
- Buying an existing and expired domain is so much easier than trying to get a new domain to be trusted
- So, go find those for your C2/phishing sites
  - https://github.com/threatexpress/domainhunter
  - https://github.com/fullmetalcache/domainGain/tree/master/src
- Fantastic post on the topic:
  - https://posts.specterops.io/being-a-good-domain-shepherd-57754edd955f

domainGain.py



```
$python domainGain.py
 [+] Getting expired domains...

 [+] Getting Domains Sorted by Url...

 [+] Getting Domains Sorted by SimWeb Score...

 [+] Getting Domains Sorted by ACR Score...

 [*] Completed Getting Domains Sorted by Url!

 [*] Completed Getting Domains Sorted by SimWeb Score!

 [*] Completed Getting Domains Sorted by ACR Score!

 [+] Sorting results...

 [*] Found 498 recently expired domains

 [+] Checking categorization for domains...
```

domainGain.py

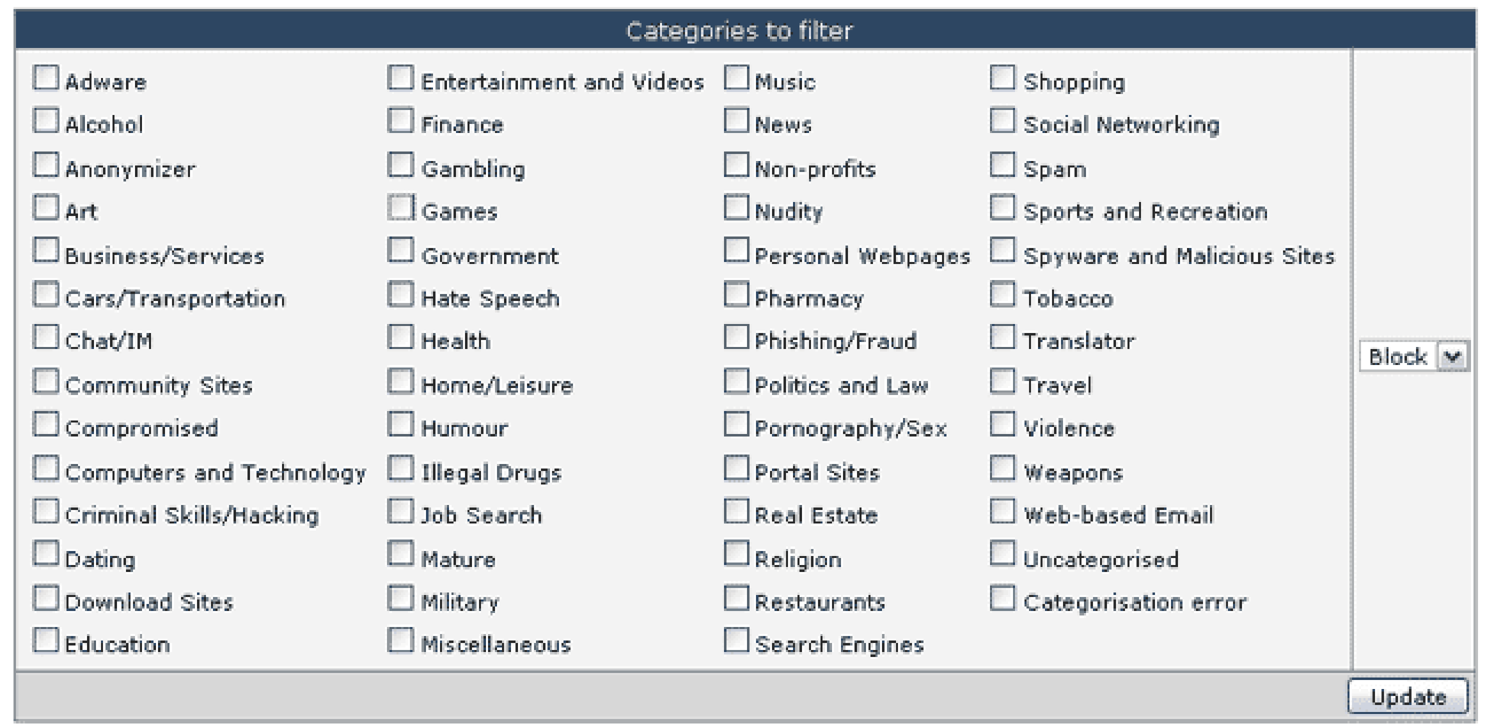


```
[*] Found 50 domains that have good categorization and are available

[*] Here is a list of available, categorized domains

[0] warrantnavi.net                    Brokerage/Trading
$7.65

[1] oregoncityparks.org                        Government/Legal
$10.79

[2] rilke.org                  Entertainment
$10.79

[3] a32.org                    Technology/Internet
$10.79

[4] eu-by.org                  Technology/Internet
$10.79

[5] fundacioncolosio.org                       Charitable Organizations
$10.79

[6] oddessey.org                       Chat (IM)/SMS
$10.79

[7] bloodsaveslives.org                        Health
$10.79
```

Let’s Play a Game

- How many “legitimate” sites do your users go to?
  - 200? 500? 1000? 2000?
  - Really, let's find this out.
- Let's say we allow all of them (within reason)
- But! We remove ads… Please… Let them die.
- What would your exposure be?

Filtering



Categories to filter

□ Adware
□ Alcohol
□ Anonymizer
□ Art
□ Business/Services
□ Cars/Transportation
□ Chat/IM
□ Community Sites
□ Compromised
□ Computers and Technology
□ Criminal Skills/Hacking
□ Dating
□ Download Sites
□ Education

□ Entertainment and Videos
□ Finance
□ Gambling
□ Games
□ Government
□ Hate Speech
□ Health
□ Home/Leisure
□ Humour
□ Illegal Drugs
□ Job Search
□ Mature
□ Military
□ Miscellaneous

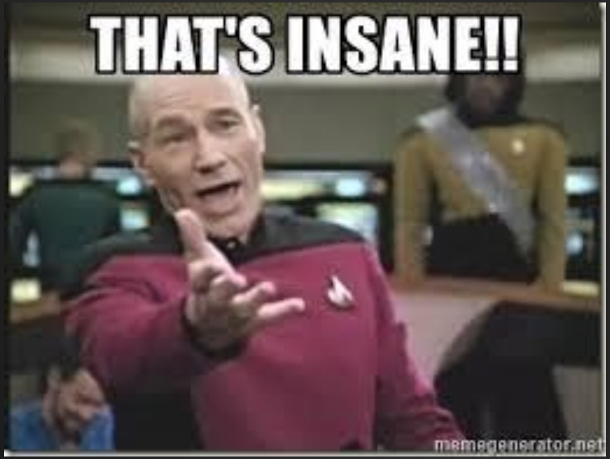
□ Music
□ News
□ Non-profits
□ Nudity
□ Personal Webpages
□ Pharmacy
□ Phishing/Fraud
□ Politics and Law
□ Pornography/Sex
□ Portal Sites
□ Real Estate
□ Religion
□ Restaurants
□ Search Engines

□ Shopping
□ Social Networking
□ Spam
□ Sports and Recreation
□ Spyware and Malicious Sites
□ Tobacco
□ Translator
□ Travel
□ Violence
□ Weapons
□ Web-based Email
□ Uncategorised
□ Categorisation error

Block

Allow Listing Approaches

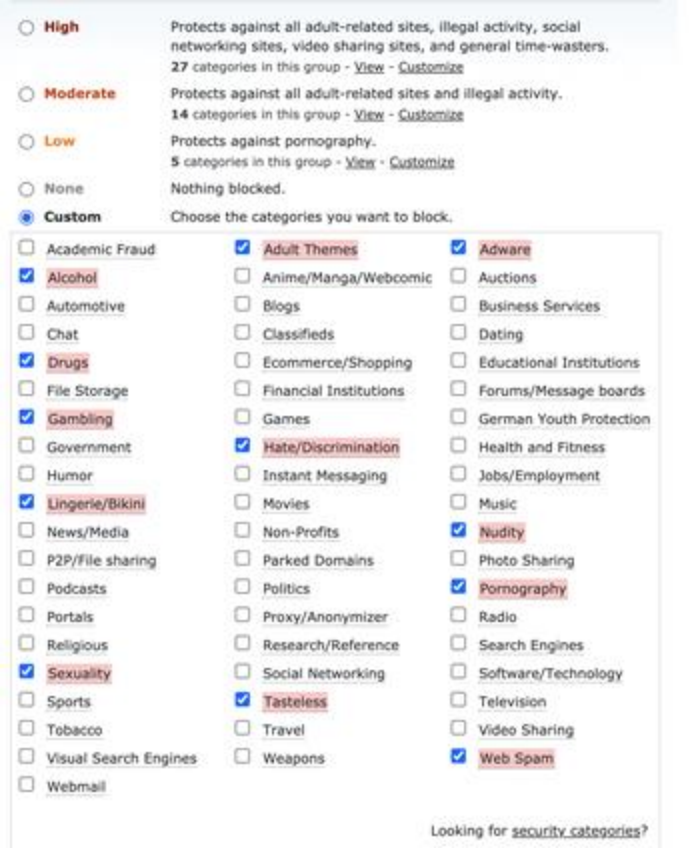
- Allow List every site (dumb… Most of the time)
- Allow List categories
- Let the users choose to go to sites
  - Seems insane..
  - Kind of is
  - Let's talk about it



Malware and Allow Listing

- You can get compromised via a “legit” site
    - Drudge
    - Facebook
    - Movie sites
    - Porn
- But! Many times the C2 site will not be the same as the site that infected your system
- This gives us an opportunity to detect and react

OpenDNS



○ **High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.
27 categories in this group - View - Customize

○ **Moderate** Protects against all adult-related sites and illegal activity.
14 categories in this group - View - Customize

○ **Low** Protects against pornography.
5 categories in this group - View - Customize

○ None Nothing blocked.

● **Custom** Choose the categories you want to block.

□ Academic Fraud	☑ Adult Themes	☑ Adware
☑ Alcohol	□ Anime/Manga/Webcomic	□ Auctions
□ Automotive	□ Blogs	□ Business Services
□ Chat	□ Classifieds	□ Dating
☑ Drugs	□ Ecommerce/Shopping	□ Educational Institutions
□ File Storage	□ Financial Institutions	□ Forums/Message boards
☑ Gambling	□ Games	□ German Youth Protection
□ Government	☑ Hate/Discrimination	□ Health and Fitness
□ Humor	□ Instant Messaging	□ Jobs/Employment
☑ Lingerie/Bikini	□ Movies	□ Music
□ News/Media	□ Non-Profits	☑ Nudity
□ P2P/File sharing	□ Parked Domains	□ Photo Sharing
□ Podcasts	□ Politics	☑ Pornography
□ Portals	□ Proxy/Anonymizer	□ Radio
□ Religious	□ Research/Reference	□ Search Engines
☑ Sexuality	□ Social Networking	□ Software/Technology
□ Sports	☑ Tasteless	□ Television
□ Tobacco	□ Travel	□ Video Sharing
□ Visual Search Engines	□ Weapons	☑ Web Spam
□ Webmail		

Looking for security categories?

DNS Over HTTPS

- Many browsers are starting to support DNS over HTTPS
- Seems more secure
- Encryption.. Yeah.. Encryption is important
- But!
- Control DNS and you control the world
- Gives tremendous power to the DoHTTPS vendors
- Enterprises lose a lot of visibility
- So, kind of good and bad