



Type Search Term ...



FOOTPRINTING A TARGET WITH DATASPLOIT

Share this...



DATASPLOIT:- Datasploit is a tool used in footprinting a target or defending target. It allows you to collect relevant information about the domain, email, phone number, person, etc, as per ethical hacking courses. It collects the information about a target which can expand your attack, defense. This tool is used in kali linux penetration testing. As per past researches done by [ethical hacking](#) researcher of International Institute of Cyber Security this tool quite come handy which gathering the information of the target.

For installing Datasploit:

- Type `git clone https://github.com/datasploit/datasploit`
- Then type `cd /root/Downloads/Datasploit`.
- Then type `pip install -r requirements.txt`
- Type `mv datasploit_config.py config.py`
- In the config.py you have to enter API key/secrets for different components in datasploit.

- For generating the API keys go to <https://datasploit.readthedocs.io/en/latest/apiGeneration/>

Shodan_api

- [Register](#) an account in shodan.
- Visit your registered email id and activate the account.
- [Login](#) to your account and you will find the API keys.

Copy the API key and this is the value for `shodan_api`

Censysio ID and Secret

- [Register](#) an account in censysio.
- Visit your registered email id and activate the account.
- [Login](#) to your account.
- Visit [Account](#) tab to get API ID and Secret.
- Your API key is the value for `censysio_id` field and API secret for `censysio_secret` field in `config.py` file.

Clearbit API

- [Register](#) an account in clearbit.
- It will auto redirect to the account.
- Visit [API keys](#) tab to get API key.
- Copy the API key and this is the value for `clearbit_api`

Emailhunter API

- [Register](#) an account in emailhunter.
- Click on activation link send to your registered email address.

- For generating the API key you have to create account in each of the website like – shodan API, censysio API etc and follow the instruction as needed.

NOTE; the more you get API's, more information can be enumerated.

- After generating API go to config.py and save generated API in config.py
- cd /root/Downloads/Datasploit
- vim config.py
- Save API in config.py as shown below:

```
shodan_api= EroHxdDHnnPanFbt[REDACTED]FaFHahxoLSXXzk  
sys_id= ead7e[REDACTED]6-3533-4711-a85c-1833998[REDACTED]7d9  
sys_secret= j...bfvEcDBjeX0DDWbv[REDACTED]b0ugEu1czQM
```

```
root@kali:~/Downloads/datasploit# cat config.py
shodan_api= 1HxdDHnnPanFbttKFaFHahxoLSX
censys_id= eu4ue386-3532-17ff-a856-13339917d9
censys_secret= j0SbfvEc[eX0DDWbv]pOugEu4OzQM
```

- The above API keys will be used while executing the queries.

```
= pe ./datasploit.py
```

```
root@kali:~/DataSploit# ./datasploit.py
```



```
Open Source Assistant for #OSINT
website: www.datasploit.info
```

```
Traceback (most recent call last):
  File "./datasploit.py", line 54, in <module>
    main()
  File "./datasploit.py", line 28, in main
    print "User Input: "+ sys.argv[1]
IndexError: list index out of range
```

- Type python domainOsist.py arinagrande.com as shown below:

```
root@kali:~/DataSploit# ./datasploit.py arinagrande.com
```

```
=====OUTPUT SNIP=====
```

```
--> Finding Whois Information.  
{  
    "updated_date": [  
        "2017-05-11 00:00:00",  
        "2017-05-11 07:56:15"  
    ],  
    "status": "clientTransferProhibited https://icann.org/epp#clientTransferProhibited",  
    "name": "Hose-McCann Telephone Company Inc",  
    "dnssec": "Unsigned",  
    "city": "DEERFIELD BEACH",  
    "expiration_date": [  
        "2020-07-10 00:00:00",  
        "2020-07-10 04:00:00"  
    ],  
    "zipcode": "33442-7738",  
    "domain_name": "ARIANAGRANDE.COM",  
    "country": "US",  
    "whois_server": "whois.networksolutions.com",  
    "state": "FL",  
    "registrar": "NETWORK SOLUTIONS, LLC.",  
    "referral_url": "http://networksolutions.com".  
}
```

```
"org": "Hose-McCann Telephone Company Inc",  
"creation_date": [  
    "2008-07-10 00:00:00",  
    "2008-07-10 04:00:00"  
],  
"emails": [  
    "abuse@web.com",  
    "asmith@hosemccann.com"  
]
```

=====OUTPUT SNIP=====

```
---> Searching Domain history in Netcraft
185.11.125.127: Incapsula Inc.
192.230.66.127: Incapsula Inc 3400 Bridge Parkway, Suite 200 Redwood Shores CA US 94065
206.188.193.10: Network Solutions, LLC 12808 Gran Bay Parkway West Jacksonville FL US 32258
```

=====OUTPUT SNIP=====

```
---> Finding hosts from ZoomEye
2
IP: [u'45.64.64.184']
Site: www.arianagrande.com
Title: www.arianagrande.com
X-CDN: Incapsula415-22634416 SNNN RT(1498509204002 716) q(0 0 0 -1) r(2 2) US
Location: {u'city': {u'geoname_id': 5391959, u'names': {u'zh-CN': u'\u65e7\u91\x5c71', u'en': u'San Francisco'}}, u'country': {u'geoname_id': 6252001, u'code': u'US', u'names': {u'zh-CN': u'\u7f8e\u56fd', u'en': u'United States'}}, u'is': u'Incapsula', u'asn': 19551, u'subdivisions': {u'geoname_id': 5332921, u'code': u'CA', u'names': {u'zh-CN': u'\u52a0\u5229\u798f\u5c3c\u4e9a\u5dde', u'en': u'California'}}, u'location': {u'lat': 37.7749, u'lon': -122.4194}, u'organization': u'Incapsula', u'aso': u'Incapsula Inc', u'continent': {u'geoname_id': 62551, u'code': u'NA', u'names': {u'zh-CN': u'\u5317\u7f8e\u6d32', u'en': u'North America'}}}

IP: [u'185.11.125.127', u'192.230.66.127']
Site: arianagrande.com
```

- After executing the above query information like- domain history, whois information fetched from the target which can be used in further hacking activities.
- The target contain information like domain history, whois information, finding hosts. All these information can be used in information gathering.

(Visited 447 times, 1 visits today)

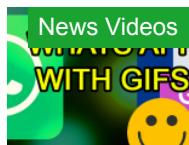
Share this...



BY: JIM GILL / ON: NOVEMBER 19, 2018 / IN: NETWORK TOOLS, TUTORIALS / TAGGED: DATASPLOIT, FOOTPRINTING



LATEST VIDEOS



WHATSAPP HACKED USING JUST A GIF. UPDATE YOUR APP AS SOON AS POSSIBLE



VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

[VIEW ALL](#)

POPULAR POSTS:



How to exploit new Facebook feature to access...



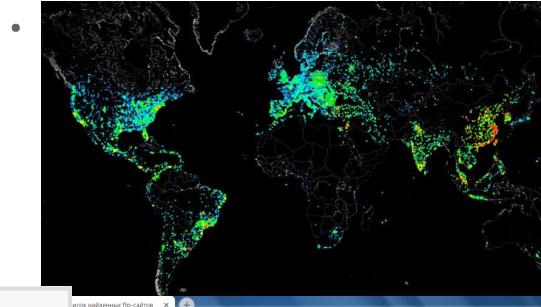
How to Hack Wi-Fi: Cracking WPA2-PSK Passwords Using...



How to fake your phone number: Make it look like...



How to intercept mobile communications (calls and...



How to scan whole Internet 3.7 billion IP addresses...

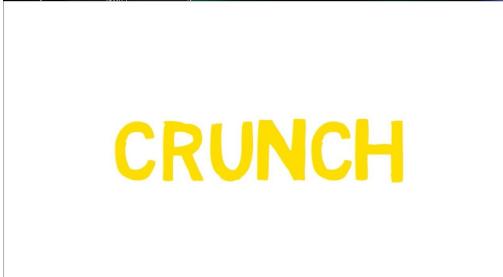
Список найденных ftp-сайтов

IP Address	Port	Server Name
212.85.101.181	212.85.105.135	ftp.uni-klu.ac.at
83.239.50.182	62.117.111.152	f4d-gridz.de
212.85.101.183	202.117.111.220	77.220.85.118
1-video.utv.ru	00911_ftp.beckhoff.com	ftp.pasarts.co.uk
212.85.107.44	00914_ftp.ast.cam.ac.uk	192.168.1.19
212.85.107.49	00915_ftp.astro.cz	ftp.coplri.ru
212.85.104.99	00920_ftp.uni-heidelberg.de	ftp.campbellsoft.com
ftp.cbrf.nosa.gov	00925_ftp.ipn.org	00926_ftp.cs.rut.ac.uk
212.85.104.145	00927_ftp.ipn.org	00928_ftp.zanex.pl
ftp.homenet.org	00929_ftp.cs.rut.ac.uk	00929_ftp.knackered.org
ftp.webspy.com	00930_81.216.17.31	00931_ftp.maliciousdomain.com
212.85.101.120	00932_00932171219	00932_ftp.dns.ens.fr
212.85.101.123	00933_00933171219	00934_ftp.ncbi.nlm.nih.gov
ftp.kmmt.ru	00941_ftp.megahosts.com	00935_ftp.ncbi.nlm.nih.gov
212.85.101.173	00942_ftp.kmmt.ru	00936_ftp.gutenberg.org
212.85.101.177	00943_ftp.kmmt.ru	00937_ftp.gutenberg.org
212.85.107.71	00944_ftp.eartbyte.org	00938_ftp.melbydeelen.co...
212.85.107.76	00945_ftp.jku.at	00939_194.114.132.17
212.85.99.194	00946_ftp.karlsruhe.cz	00940_ftp.effector.com
168.144.177.116	00947_193.15.253.65	00941_ftp.effector.com
212.85.101.20	00948_212.85.101.20	00942_ftp.netwarsolutions...
212.85.101.20	00949_ftp.fluiddreams.de	00943_ftp.machines.com
95.87.126.1	00950_95.87.126.1	

List of all Open FTP Servers in the World



Hack Whatsapp account of your friend



CREATE YOUR OWN WORDLIST WITH CRUNCH

- **PASSWORD CRACKING** Crack Windows password with john the ripper



```
r@debian:~$ sudo -l
    ching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
(root) NOPASSWD: /bin/echo
(root) NOPASSWD: /usr/bin/find
(root) NOPASSWD: /usr/bin/nano
(root) NOPASSWD: /usr/bin/vim
(root) NOPASSWD: /usr/bin/man
(root) NOPASSWD: /usr/bin/awk
(root) NOPASSWD: /usr/bin/less
(root) NOPASSWD: /usr/bin/ftp
(root) NOPASSWD: /usr/bin/nmap
(root) NOPASSWD: /usr/sbin/apache2
(root) NOPASSWD: /bin/more
(root) NOPASSWD: /usr/bin/wget
user@debian:~$
```

How to exploit SUDO via Linux Privilege Escalation

- How to Connect Android to PC/Mac Without WiFi



Do Hacking with Simple Python Script



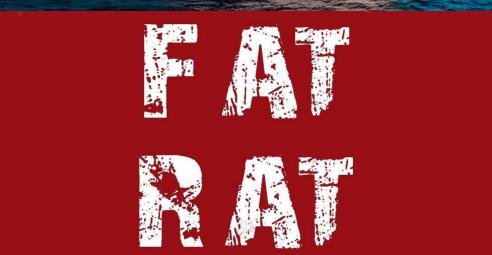
- Fake any website in seconds Facebook, Snapchat, Instagram :-



- Find Webcams, Databases, Boats in the sea using Shodan

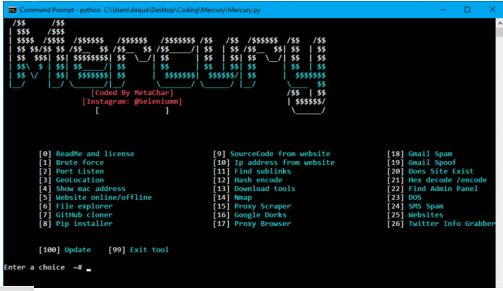


- Hack Windows, Android, Mac using TheFatRat (Step by...



- HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB





Hack any website with All in One Tool

Create your own BotNet (Step By Step tutorial)



Mascerano Bachir - Dev-labs

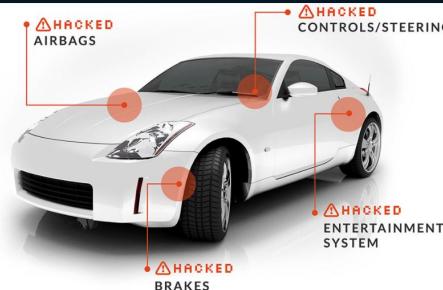
Evil-Droid Framework v0.3
Hack & Remote android platform

- [1] APK MSF
- [2] BACKDOOR APK ORIGINAL (OLD)
- [3] BACKDOOR APK ORIGINAL (NEW)
- [4] BYPASS AV APK (ICON CHANGE)
- [5] START LISTENER
- [c] CLEAN
- [q] QUIT
- [?] Select>: █

Bypass antivirus detection With Phantom Payloads



How to hack any car with this tool

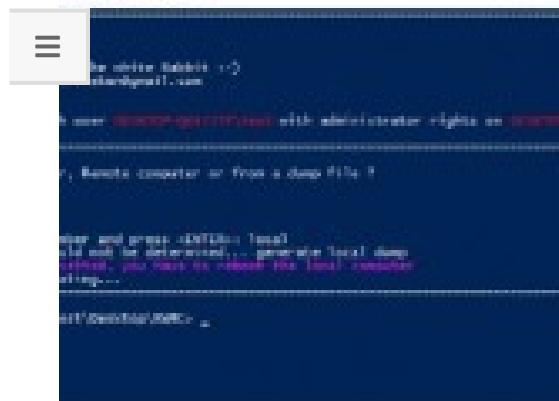


- 1



List of credit cards, proxies on Deep Web

- [View Details](#)



Extracting Hashes & Plaintext Passwords from Windows 10

- 1

RECON-NG



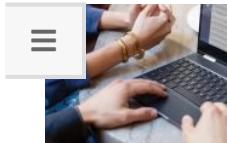
recon-**ng** – Good tool for Information Gathering

- 1

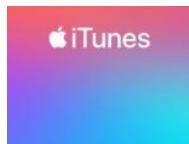
Best Hacking Tools Of 2017 For Windows, Linux, And OS X



CRITICAL VULNERABILITY IN CYBEROAM FIREWALL, BY SOPHOS: PATCH NOW AVAILABLE



MILLIONS OF HP LAPTOPS AND DESKTOPS ARE EASY TARGETS FOR HACKERS: NEW VULNERABILITIES ARE REPORTED



CRITICAL ITUNES VULNERABILITY EXPLOITED BY RANSOMWARE. UPDATE NOW



CRITICAL VULNERABILITY FOUND IN JOOMLA! UPDATE AS SOON AS POSSIBLE



PALO ALTO, FORTINET AND PULSE SECURE VPNS ARE VULNERABLE TO ATTACKS: NSA



CRITICAL FOXIT PDF READER VULNERABILITIES: UPDATE AS SOON AS POSSIBLE



PIXEL, HUAWEI, XIAOMI, OPPO, MOTOROLA AND SAMSUNG SMARTPHONES ARE EASILY HACKABLE; UPDATE ASAP. FULL LIST HERE



EXPERTS FOUND CRITICAL VULNERABILITY IN AIRCRAFT OPERATING SYSTEMS



VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



CRITICAL VULNERABILITY AFFECTING CLOUD SERVERS: THOUSANDS OF SERVERS INFECTED



CRITICAL ROOT ACCESS VULNERABILITY ON CISCO DEVICES ALERT! PATCH IMMEDIATELY



ZERO-DAY VULNERABILITY IN VBULLETIN EXPLOITED BY HACKERS; THOUSANDS OF WEBSITES AFFECTED



XSRF VULNERABILITY IN PHPMYADMIN; THERE IS NO PATCH TO FIX THIS FLAW SO FAR



ALMOST EVERY CISCO DEVICE IS VULNERABLE TO DOS ATTACKS; FIX NOW USING THIS PATCH



SECURE YOUR D-LINK & COMBA ROUTERS' PASSWORDS; CRITICAL VULNERABILITY FOUND



EXPERTS FOUND NEW CRITICAL VULNERABILITIES AFFECTING INTEL CPUS



VIEW ALL

TUTORIALS



MR. ROBOT 1 – CAPTURE THE FLAG CHALLENGE, WALK THROUGH



CYBERCRIMES SEXTORTION & REVENGEPORN, WHAT TO DO IF IT HAPPENS TO YOU?



HACK WIFI WITHOUT ROOTING ANDROID DEVICES



20 WAYS OF DOING SOCIAL PROTEST WITHOUT EXPOSING YOUR IDENTITY, JUST LIKE IN CHINA



FAKE TEXT MESSAGE ATTACK. HOW PRANK OR HACK YOUR FRIENDS WITH FAKE SMS BOMBER



SPOOFING CALLS, MAKE IT LOOK LIKE SOMEONE ELSE IS CALLING



Google Hacking

HACK WEBSITE USING GOOGLE HACKING OR GOOGLE DORKING – PART I



CRACK ANY WIFI PASSWORD WITH WIFIBOOT



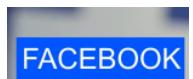
4 BROWSERS FOR SAFE ANONYMOUS SURFING



HOW TO CHECK IF SOMEONE IS SPYING ON YOUR MOBILE



BEST ANDROID APPS TO HACK WIFI NETWORKS



HACK YOUR FRIENDS FACEBOOK ACCOUNT USING HIDDEN EYE

HACKING



ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART II



ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART I



ALL-NEW WINDOWS EXPLOIT SUGGESTER IS HERE, WES-NG



ALL-NEW APP STORE FOR HACKERS, KALI NETHUNTER



TURN ANY ANDROID DEVICE INTO AN PENETESTING DEVICE



8 METHODS FOR BYPASSING SURVEILLANCE CAMERAS AND FACIAL RECOGNITION SOFTWARE

[VIEW ALL](#)



PAYING THE RANSOM OF A CYBERATTACK IS NOW LEGAL: FBI



ONTARIO GOVERNMENT HAD TO PAY HACKERS A \$75K USD RANSOM



DOWNLOAD THE FREE DECRYPTOR FOR YATRON, FORTUNECRYPT AND WANNACRYFAKE RANSOMWARE VARIANTS



MICROSOFT BANNED CCLEANER



A CALIFORNIA CITY SHUTS DOWN ALL OPERATIONS DUE TO VIRUS ATTACKS ON ITS GOVERNMENT SYSTEMS



CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !



FACEBOOK SUSPENDED THOUSAND OF APPS



UNINSTALL THESE ANDROID BEAUTY APPS RIGHT NOW !



MASSACHUSETTS TO PAY \$400K USD TO HACKERS DUE TO RANSOMWARE ATTACK



HOW CAPTCHA IS BEING USED TO BYPASS ANTI MALWARE SECURITY SCANS AND FIREWALLS



JOKER: THE MALWARE THAT HACKS SMS MESSAGES INFECTS 500K USERS OF THESE 24 ANDROID APPS



VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP



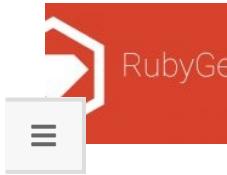
LILU, THE RECENTLY DISCOVERED AND DANGEROUS RANSOMWARE VARIANT



THE SCHOOL KID WHO HACKED OVER A MILLION IOT DEVICES



IDaho schools under ransomware attack. Will ransomware make America great again?



Stop programming in Ruby, applications using Ruby libraries have a backdoor



You want to make millions in Fortnite? This videogame hacking tool is a ransomware

[View All](#)

CYBER SECURITY CHANNEL



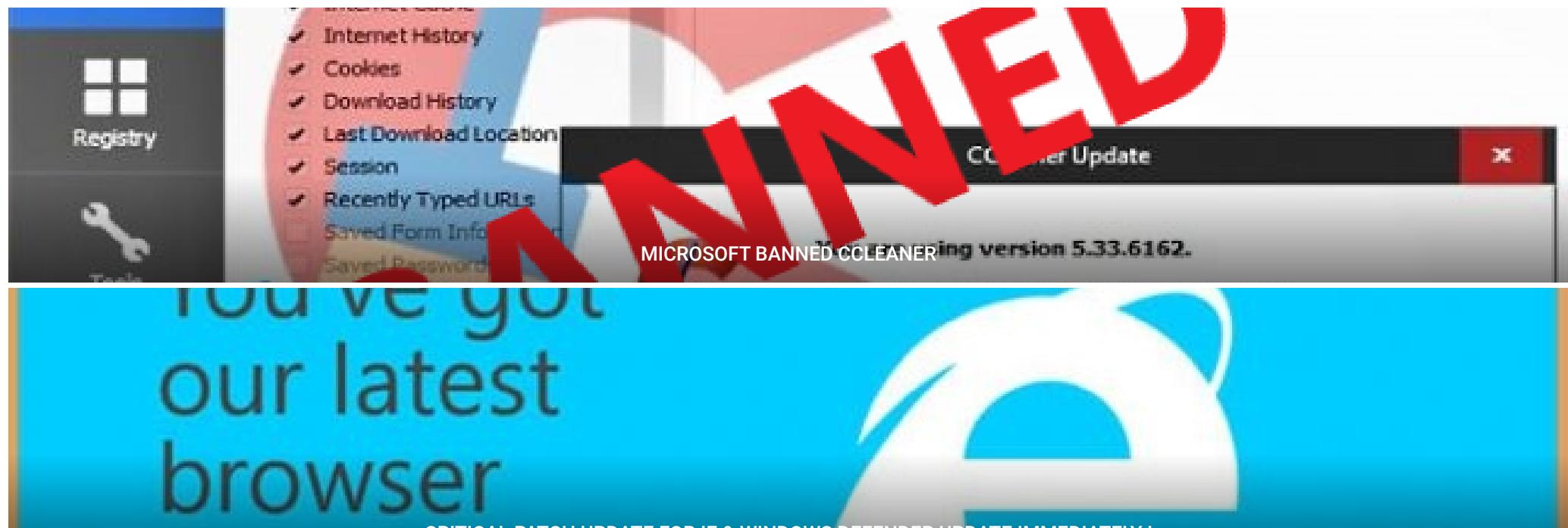
VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS



GAMING COMPANY ZYNGA INC. BECOMES A VICTIM OF HACKERS; 218 MILLION PLAYERS AFFECTED



CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !



FACEBOOK SUSPENDED THOUSAND OF APPS



SMS CRITICAL VULNERABILITY TO HACK ANY MOBILE



VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP