

ISSUE 005

UNREDACTEDMAGAZINE.COM

Q1 2023

UNREDACTED

THE MACOS VENTURA PRIVACY & SECURITY GUIDE

Refresh your macOS for optimal privacy and security



UNREDACTED
ISSUE 005

IN THIS ISSUE

- 5 From the Editor
- 6 The macOS Ventura Privacy & Security Guide
- 12 Wireless Security: Vehicle Remote Entry Attack and Defense
- 15 Malware or Mal-Awareness?
- 19 Social Links: Revolutionary AI-Driven OSINT solutions
- 20 An OSINT Practitioner's Perspective on Privacy, or, How I Learned to Stop Worrying and Embraced Obscurity
- 23 Hardening Measures for Multi-Factor Authentications
- 25 Google Analytics
- 28 The OSINT Corner
- 32 Pet Intelligence
- 34 10 Minutes of Google Dorking for COVID Documents
- 37 Supermarket Loyalty Card Privacy Strategy
- 38 Changing Your IMEI for Cellular Anonymity
- 40 Sign out of Apple
- 42 Reader Q&A
- 44 Updates
- 45 Letters
- 46 Verifiable Credentials: The Killer Feature of Decentralized Identity
- 49 Privacy-themed Puzzles
- 50 Final Thoughts
- 50 Affiliate links

UNREDACTED is published free of any charge to the reader, and this file may be publicly shared in its entirety. All issues are available for free download at [UNREDACTEDmagazine.com](https://unredactedmagazine.com). Contact details are also available at this site.

The contents of this publication are copyright © 2023 by [UNREDACTEDmagazine.com](https://unredactedmagazine.com), and are published via a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International license. You may share it for free as long as you keep the entire file intact. Commercial use is prohibited.

Cover Design by Anonymous Reader. Layout by [Astropost](#). Special thanks to everyone who helped make this happen. You know who you are.



FROM THE EDITOR

By Michael Bazzell

Happy new year everyone. We have been quite busy preparing for the publication of the 10th Edition of OSINT Techniques, which is now available. I want to take a moment to discuss the changes.

The previous (9th) edition of the book was originally written in late 2021. In late 2022, I was asked to update this book, as it is required reading for numerous college courses, university degrees, and government training academies. I never want stale or inaccurate information being presented within training programs, so I created this special revision. In many previous editions, I only published a new version once I had at least 30% new material and 30% updated content. The recycled material was kept to a maximum of 40%. With this edition (and the 9th), I have deviated away from that rule. I estimate that 20% of the content is brand new, 20% has been updated to reflect changes throughout 2022, and the remaining 60% is recycled from the from the previous edition.

Much of the ninth edition content was still applicable and only needed minor updates to reflect changes since 2021. If you have read the previous edition, you will find most of those overall strategies within this book. However, I have added many new OSINT methods which complement the original text in order to cater to those who always need accurate information. I also removed a lot of outdated content which was no longer applicable. I believe there is much new value within this updated text. The majority of the updates are available in chapters 2, 3, 4, 5, 6, 7, 8, 23, 28, 30, 31, 32, and 33, along with the digital files which accompany them. The other chapters all have minor updates.

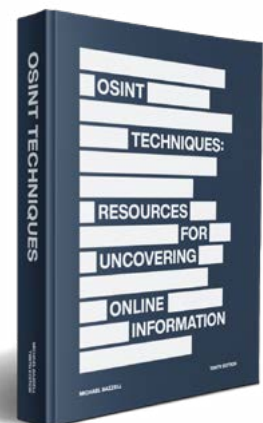
This edition also presents six new chapters unavailable within previous versions. These include Broadcast Streams (23), Application Programming Interfaces (28), and an entire new section containing four chapters about Data Leaks (30), Data Breaches (31), Stealer Logs (32), and Ransomware (33). I am very excited to release these new

chapters, as I believe they introduce the future of OSINT analysis.

Finally, I want to thank the OSINT community for the continued interest in my online investigation strategies. It has been over a decade since the first edition, and I would have never anticipated the popularity of OSINT when I published it. If you are interested in this new updated edition, please go to inteltechniques.com/book1.html.

Thanks,

MB





THE MACOS VENTURA PRIVACY & SECURITY GUIDE

By Michael Bazzell

The beginning of a new year is always a great time to revisit and refresh your digital security. For me, that means a deep cleaning of all devices. Often, I rebuild the operating systems on all of my hardware and optimally reconfigure my settings. This is quite easy for my daily Linux machine, especially with the various Linux Lifestyle articles from the past three issues. However, macOS is a different beast. The only macOS device I ever use is my OSINT machine which is a MacBook Pro M1. I choose this due to the virtualization options, and rarely touch the host. I explain more about that in the 10th edition OSINT book. Since I have several clients who rely on macOS products, I felt the need to create a macOS privacy & security protocol. The following assumes you are using the latest, fully-patched, Ventura operating system. I placed all commands provided here on my site at <https://unredactedmagazine.com/data/005.txt> for easy copy and paste.

Phase 1: Update to Ventura

From your Apple device, apply all updates and fully upgrade to Ventura. This can be done on a “dirty” machine. We just need the OS to fully install before we reset the device, which will erase all data.

Phase 2: Complete System Wipe

Next, we want to wipe out our entire system. This eliminates any junk leftover from unused apps and various cached files eating up valuable space. First, make a backup of any valuable data. Common locations include the Desktop, Downloads, and Documents folders within the home folder of the current user. I prefer to use SuperDuper (<https://www.shirt-pocket.com/SuperDuper>) for this, as the backup is a true clone and bootable. Once complete, conduct the following (based on M1). Warning: this will erase all data on your device!

- Open System Settings and type “reset” in the search box.

- Select “Transfer or Reset” and click “Erase All Content and Settings”.
- Enter your password, click continue, and confirm erase option.
- Allow device to reboot.
- Connect to Wi-Fi in the upper-right (Required for “Activation Lock”).
- Allow activation to complete (enter account password if required).
- Click “Restart” when activation completes then click “Get Started”.
- Select desired language and region.
- Click “Not Now” in the Accessibility screen.
- Click “Continue” without selecting a Wi-Fi network.
- Click “Continue” to confirm your choice.
- Click “Continue” on Data and Privacy screen.
- Click “Not Now” at the Migration Assistant.
- Click “Agree” to the Terms and Conditions and confirm “Agree”.
- Provide generic computer name and secure password.
- Click “Continue” then “Continue without enabling Location Services”.
- Click “Don’t Use” to confirm choice.
- Choose your desired time zone.
- Disable all analytics options and click “Continue”.
- Click “Set Up Later” for Screentime.
- Uncheck “Enable Ask Siri” and click “Continue”.
- Click “Set Up Touch ID Later” and click “Continue”.
- Choose your desired look and click “Continue”.

Phase 3: Basic Software Installation

Next, Install Rosetta (only for newer Apple hardware), Homebrew (package manager), Task Explorer (identify suspicious processes), and KnockKnock (identify persistent malicious files). I run Task Explorer and KnockKnock weekly.

```
softwareupdate --install-rosetta --agree-to-license
```

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

```
brew install --cask taskexplorer
```

```
brew install --cask knockknock
```

Phase 4: System Configuration

Next, I like to modify all stock macOS settings which provide additional layers of privacy and security. I conduct the following.

- Open “System Settings” and search “Update”.
- Click “Software Update” then “Automatic Updates”.
- Disable “Check for Updates” and click “Done”.
- Enter your password if prompted.
- Apply any pending updates and modify the following within “System Settings”.
- Bluetooth: Disable Bluetooth
- Network > Firewall: Enable Firewall
- Notifications > Show Previews: Never
- Notifications: Disable “Allow notifications when the screen is locked”
- Notifications > Each app: Disable
- General > Date & Time > Source: Change to “pool.ntp.org”
- General > Sharing: Disable All
- Siri and Spotlight: Disable “Ask Siri”
- Siri and Spotlight > Spotlight > Disable all
- Siri and Spotlight > Siri Suggestions > Disable all
- Privacy and Security > Analytics > Improvements: Disable all
- Privacy and Security > Apple Advertising > Disable personalized ads
- Lock Screen > Require password immediately
- Game Center: Disable all
- Wallet & ApplePay > Disable “Add Orders to Wallet”

Phase 5: Change DNS

I have explained NextDNS within previous issues, and that is what I use for DNS queries. Something simpler which can be applied until you create a NextDNS account is Cloudflare. Their server addresses are 1.1.1.1 and 1.0.0.1. Within System Settings, conduct the following.

- Select connection (Wi-Fi or Ethernet) and click "Details".
- Disable "Limit IP address tracking".
- Click "DNS".
- Enter desired servers.
- Open "Little Snitch Rules" from the menu bar.
- Click the "+" in the lower left and create profile titled "Apple Disabled".
- Click the "+" in the lower left and create profile titled "Apple Enabled".

Phase 6: Security Settings

Enable FileVault for full-disk encryption at the following location.

- System Settings > Privacy & Security > FileVault

Next, open Terminal and consider the following commands.

- Disable Spotlight completely: `sudo mdutil -a -i off`
- Delete Spotlight index from root: `sudo mdutil -X /`
- Confirm indexing disabled: `sudo mdutil -s /`
- Confirm FileVault status: `sudo fdesetup status`

I disable Spotlight because I do not need or want it. This prevents Apple from digesting all of your files, emails, images, etc.

Phase 7: Apply Firmware Password (Intel only)

This only applies to older Apple devices, as M1 and newer machines have something similar enabled by default.

- Boot computer into Recovery Mode with CMD-R.
- Choose active account and enter password.
- Click "Utilities" in the menu then "Startup Security".
- Click "Turn On Firmware Password".
- Provide desired secure password.
- Quit and restart.

Phase 8: Little Snitch

This is the big one. Little Snitch is a software firewall which prevents applications from sending out unnecessary data about our usage. This could be to block Apple from connecting to iCloud or to prevent Microsoft from sending analytics every time you open Word. For me, this is the most vital piece for a private macOS device. LuLu is a free alternative if you do not want to pay for Little Snitch, but I find the price to justify the advanced options.

- Execute `brew install --cask little-snitch` in Terminal.
- Choose "Silent" mode for now.
- Deselect macOS and iCloud options.

- Click the "+" in the lower left and create profile titled "Apple Update".
- While in the "Effective in all profiles" section, disable all options, except "Allow outgoing connections to local network".
- From Rule Groups, disable all options.
- In the menu bar, change Profile to "Apple Disabled".
- Change "Operation Mode" to "Alert Mode".
- When prompted by any Apple service, choose "Any connection", "Forever", and "Deny".

Your machine will start annoying you. You will soon see why we want this software. Your Apple device is constantly calling home to send details of your usage. With Little Snitch, we can block all of these intrusions. As I write this, macOS Ventura possesses 64 Apple applications which send telemetry about you to Apple's servers. We can set this "Apple Disabled" profile to block all of them. However, there are exceptions. The following will allow Apple to see your DNS servers (to connect to the internet) and keep your time synchronized.

- mDNSResponder: Allow to connect to chosen DNS servers
- mDNSResponder: Allow connections from local network
- timeD: Allow to connect to new time server

I also allow all Apple services which ask to "Allow incoming connections from local network". This will keep various internal devices synchronized and my macOS virtual machines happy within UTM. If I were on a public network, I would disable all of these. At my home, I have no objection.

Next, let's continue configuring our "Apple Disabled" profile.

- Open all apps once and reboot, confirming to "Deny" everything.
- Continue until Little Snitch alerts are finished.
- Copy all "Apple Disabled" rules into "Apple Enabled" and "Apple Updated".
- Change all "Apple Enabled" rules to "Allow".
- Change "AssetCacheLocatorService", "com.apple.MobileSoftwareUpdate", "CoreServiceUIAgent",

"mobileassetd", "nsurlsessiond", and "softwareupdated" in "Apple Updated" to "Allow".

These changes allow you to switch to other profiles when needed. When I want to check for updates and apply any pending upgrades, I select the "Apple Update" profile. It allows only the minimal services to send data. If I ever need to, I can allow all Apple services with the "Apple Enabled" option, but I would never do that. For daily use, I am always on "Apple Disabled".

Next, let's use Terminal to confirm a few things. These commands can be beneficial when you simply want to make sure your settings are as desired.

- Confirm Spotlight: `mdutil -s /`
- Confirm FileVault: `fdsetup status`
- Confirm SIP: `csrutil status`
- Confirm Assessments: `spctl --status`

I like to make sure that undesired programs are not set to launch in the background upon boot. The following commands open the two most common places these programs hide. Once open, you can delete them from Finder if desired.

```
open ~/Library/LaunchAgents/  
open /Library/LaunchAgents/
```

If I ever want to clear my Terminal history, I can conduct the following.

```
rm -f ~/.bash_history  
rm -f ~/.zsh_history
```

The following clears macOS logs and cache files.

```
sudo rm -rfv /Library/Logs/*  
  
rm -rfv ~/Library/Containers/com.apple.mail/  
Data/Library/Logs/Mail/*  
  
sudo rm -rfv /var/audit/*  
  
sudo rm -rfv /private/var/audit/*  
  
sudo rm -rfv ~/Library/Logs/*  
  
sudo rm -fv /System/Library/LaunchDaemons/com.  
apple.periodic-*.plist  
  
sudo rm -rfv /var/db/receipts/*  
  
sudo rm -vf /Library/Receipts/InstallHistory.  
plist  
  
sudo rm -rfv /private/var/db/diagnostics/*  
sudo rm -rfv /var/db/diagnostics/*
```

```
sudo rm -rfv /private/var/db/uuidtext/  
  
sudo rm -rfv /var/db/uuidtext/  
  
sudo rm -rfv /private/var/log/asl/*  
  
sudo rm -rfv /var/log/asl/*  
  
sudo rm -fv /var/log/asl.log # Legacy ASL  
(10.4)  
  
sudo rm -fv /var/log/asl.db  
  
sudo rm -fv /var/log/install.log  
  
sudo rm -rfv /var/log/*  
  
sudo rm -rfv /Library/Caches/* &>/dev/null  
  
sudo rm -rfv /System/Library/Caches/* &>/dev/  
null  
  
sudo rm -rfv ~/Library/Caches/* &>/dev/null  
  
sudo rm -rfv /var/spool/cups/c0*  
  
sudo rm -rfv /var/spool/cups/tmp/*  
  
sudo rm -rfv /var/spool/cups/cache/job.cache*  
  
sudo rm -rfv ~/.Trash/* &>/dev/null  
  
rm -rfv ~/Library/Developer/Xcode/DerivedData/*  
&>/dev/null  
  
rm -rfv ~/Library/Developer/Xcode/Archives/*  
&>/dev/null  
  
rm -rfv ~/Library/Developer/Xcode/iOS Device  
Logs/* &>/dev/null  
  
sudo dscacheutil -flushcache  
  
sudo killall -HUP mDNSResponder  
  
sudo purge
```

The following disables all leftover Siri services.

```
defaults write com.apple.assistant.support 'As-  
sistant Enabled' -bool false  
  
defaults write com.apple.assistant.backedup  
'Use device speaker for TTS' -int 3  
  
launchctl disable "user/$UID/com.apple.assis-  
tantd"  
  
launchctl disable "gui/$UID/com.apple.assis-  
tantd"  
  
sudo launchctl disable 'system/com.apple.assis-  
tantd'  
  
launchctl disable "user/$UID/com.apple.Siri.  
agent"
```

```

launchctl disable "gui/$UID/com.apple.Siri.
agent"

sudo launchctl disable 'system/com.apple.Siri.
agent'

defaults write com.apple.SetupAssistant 'Did-
SeeSiriSetup' -bool True

defaults write com.apple.systemuiserver 'NSSta-
tusItem Visible Siri' 0

defaults write com.apple.Siri 'StatusMenuVisi-
ble' -bool false

defaults write com.apple.Siri 'UserHasDeclined-
Enable' -bool true

defaults write com.apple.assistant.support
'Siri Data Sharing Opt-In Status' -int 2

```

Finally, the following disables various remote connections.

```

sudo systemsetup -setremotelogin off

sudo launchctl disable 'system/com.apple.tftpd'

sudo defaults write /Library/Preferences/com.
apple.mDNSResponder.plist NoMulticastAdvertise-
ments -bool true

sudo launchctl disable system/com.apple.telnetd

cupscctl --no-share-printers

cupscctl --no-remote-any

cupscctl --no-remote-admin

```

I know this seems like a lot of work. As a reminder, I placed all commands provided here on my site at <https://unredactedmagazine.com/data/005.txt> for easy copy and paste. Once finished, you will have the comfort of knowing you have stopped 99% of Apple's intrusions into your daily life. Or, this will convince you to move to Linux. Either way is a win.

The images below compare a partial section of the Apple Disabled, Apple Update, and Apple Enabled Little Snitch

rules. Images of the full configuration are available at <https://inteltechniques.com/ventura.html>.

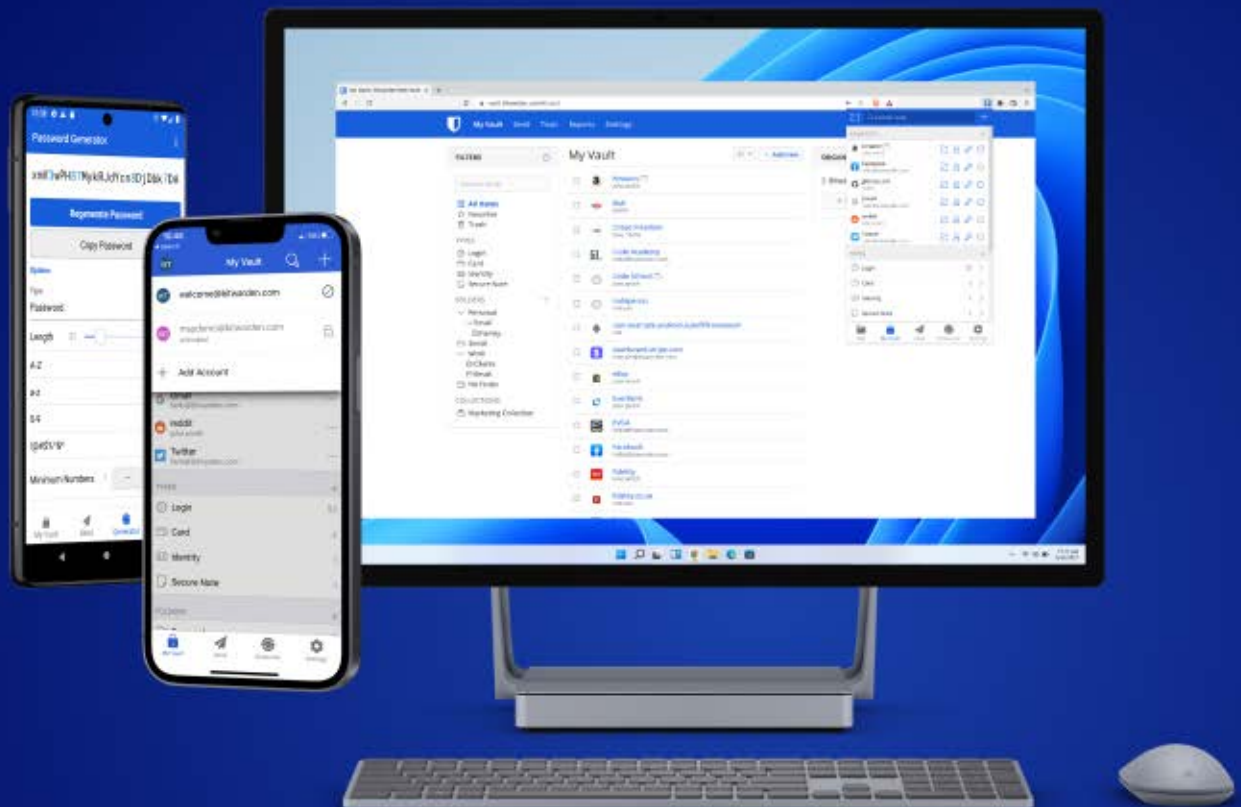
	remindd			Deny any outgoing connection	
	rtcreportindg				Deny any outgoing connection
	searchpartyuseragent			Deny any outgoing connection	
	softwareupdated				Deny any outgoing connection
	Spotlight			Deny any outgoing connection	
	Stocks			Deny any outgoing connection	
	StocksDetailIntents			Deny any outgoing connection	

	remindd			Deny any outgoing connection	
	rtcreportindg				Deny any outgoing connection
	searchpartyuseragent			Deny any outgoing connection	
	softwareupdated				Allow any outgoing connection
	softwareupdated				Allow any outgoing connection
	Spotlight			Deny any outgoing connection	
	Stocks			Deny any outgoing connection	
	StocksDetailIntents			Deny any outgoing connection	

	remindd			Allow any outgoing connection	
	rtcreportindg				Allow any outgoing connection
	searchpartyuseragent			Allow any outgoing connection	
	softwareupdated				Allow any outgoing connection
	Spotlight			Allow any outgoing connection	
	Stocks			Allow any outgoing connection	
	StocksDetailIntents			Allow any outgoing connection	

Hopefully, you see the value in blocking the constant telemetry being sent to Apple servers about the ways we use the machines which we purchased. Any updates to this guide will be posted at <https://inteltechniques.com/ventura.html>. ■

Secure all your passwords in one place



 **bitwarden**

Open source transparency.
Zero-knowledge encryption.



bitwarden.com/secure

Store, manage, and share your passwords across all your devices.

WIRELESS SECURITY: VEHICLE REMOTE ENTRY ATTACK AND DEFENSE

by Reginald

Wireless communications play a very large role in our daily lives. One of the more exposed items we use that rely on wireless signals is our car. Not since the early 2000s have we mainly relied on physically inserting a key into a lock to open the car door, and in the early 2010s we adopted wireless ignition in earnest. In the past 20 years, security holes in these technologies have come and gone, and some are still present. For instance, Honda key fobs are vulnerable to replay attacks with some simple know-how and cheap equipment. Focusing on key fob and remote entry vulnerabilities, we tested two vehicles as use-cases that anyone can reproduce, given access to these makes and models, the right tools, and the right permissions. Defensive strategies will be covered as well.

The Premise

Certain vehicles are susceptible to remote entry hacks given certain circumstances and criteria are met. Those are:

1. A vulnerable vehicle is available
2. The attacker has close access to the target vehicle's key fob
3. The attacker possesses the right equipment to exploit the key fob

The most common attack is a replay attack where the signal from the manufacturer's equipment is recorded and replayed, mimicking the original equipment and signal. Many modern vehicle remote entry systems implement different forms of security to disable these kinds of attacks, but not all are effective. The most common are rolling codes, where a unique signal accompanies each press of the key fob button supposedly denying reproduction unless certain criteria are met. One of those criteria is correct sequencing. For instance, if one were to capture and record a key fob unlock signal which was actively used to unlock the vehicle (a bystander witnessing an unlocking), and the vehicle responded to that signal, the sequence is then incremented in some fashion, meaning the captured signal will be ineffective if replayed in its original form.

If that same signal were captured and recorded, but the vehicle did not respond due to distance or RF-dampening media, a replay may still be successful, as that specific sequence of unlock codes remains valid. The vehicle is awaiting the rolling code increment that was just captured, since the vehicle did not "hear" the key fob. A subsequent signal from the key fob will still unlock the vehicle, as both the vehicle and the key fob are programmed to respond to the same rolling code sequencing,

matching a specific algorithm allowing for code increment prediction. By this, it means the car isn't just waiting for the next increment from the key fob; it will respond to any signal which matches the predicted code sequence. You can hit the button to unlock the vehicle any number of times without response, and still successfully gain entry when back in range. An attacker without that rolling code algorithm cannot; there is no way to predict the next code without it.

In the case of the captured signal but unsuccessful unlock, the attacker has just one shot and it must be used before the key fob is successfully used again.

The Legalities

Before you conduct any test, gain permission. Using equipment other than the manufacturer's specified items to gain remote entry into a vehicle without authorization is illegal, and could constitute breaking and entering, attempted larceny, or grand theft auto. These crimes are serious, and you must do your due diligence as the first step every time. If you choose to quibble on this matter, do it on your own time; the warning stands.

The Risks

Any test done with equipment other than the manufacturer's specified items

to gain remote entry into a vehicle carries a risk of system or equipment damage. While most wireless tests with a vehicle remote entry system will at worst deny you entry, some tests will trigger fail safes or uncover some other previously unknown result. We'll see this happen as a result of one of the upcoming tests. Be prepared to visit a mechanic if your tests result in some sort of system failure.

The Tools

We used a HackRF One with the Portapack configuration and a Flipper Zero. Both are software defined radios with very different capabilities, but appropriate for the task of capturing RF signals and replaying them. Researching the right signal to capture based on the target vehicle starts at the FCC but can expand out with simple search engine terms.

The Targets

We tested a 2012 Toyota Tacoma and 2016 Volkswagen Jetta. For safety reasons, the vehicle VINs and specific model details will be left out.

The Operation

Conducting the test required some homework. If the vehicle make, model, and year are known, the FCC ID of the key fobs can be researched to find the correct transmit frequency. The same is possible if in possession of the key fob itself. It is likely that information stored by the FCC for one vehicle of a certain model year is identical across all vehicles of that model year. When typing into our search engine "Toyota 2102 key fob frequency" we got the first hit as https://www.sigidwiki.com/wiki/Toyota_Car_Key. We learn it is either 315 MHz or 433 MHz. Adding "Tacoma" to the search got us to several sites which were selling replacement key fobs, and listing the FCC ID. The FCC will allow a search via the website listed in our tools, but must be split between Grantee Code and Product Code. For 2012 Tacoma key fobs, the fields will be GQ4 and the remaining characters, respectively. The process for the Volkswagen Jetta,

and any other vehicle key fob, will be similar. The results indicate 315 MHz for both upper and lower range for the key fob.

In our test, we had possession of the key fobs, but knowing which frequency to capture, we can perform the test without possession if an individual activates the key fob within capture range of our tools. For the HackRF One, we received a signal from the Toyota and Volkswagen key fobs as far away as 30 meters using a stock telescopic aerial antenna, but conditions will vary. The Flipper Zero captured the key fob signal for the Toyota as far as 6 meters, and 8 meters for the Volkswagen. Again, conditions will vary, and these results are based on our specific environment, which was outdoors with clear line of site. Having the fob only a few inches away from the capture tool is best. Yes, you're already scheming to never leave your keys lying around at the gym or a party anymore. Good on you.

Replaying the captured unlock signal is simple enough, but success depends on certain conditions being met. As mentioned, rolling codes inherent in modern key fob operations prohibit direct reuse of captured signals. This being the case, if the unlock signal is captured by both the vehicle and the capturing device, the vehicle will unlock, thus rendering that particular signal invalid for replay. A successful capture must be done out of receive range of the vehicle.

Achieving this, unlock was successful via replayed key fob unlock signals from both the HackRF One and the Flipper Zero for the 2012 Toyota Tacoma. The 2016 Volkswagen Jetta did not allow such shenanigans. Upon receipt of the replayed unlock signal from the first device, the HackRF One, the vehicle's remote entry system ceased normal operation and prohibited any subsequent remote entry via wireless signal, including from the original manufacturer key fob. While research is ongoing, it's assumed that this is a failsafe feature implemented after several replay attacks were successful against older Volkswagen models. Dealer repair costs to reset the remote

entry system can total between 200.00 and 300.00 USD. Of note, this model Jetta allows ignition via proximity detection of the key fob, thus keyless/push-button. This feature still functioned normally after failure of the remote entry replay attack.

Lessons Learned

The three biggest takeaways are:

1. The closer you are to the key fob for capture, the better the capture will be
2. Proper research is necessary to determine the correct target frequency
3. More recent vehicles can have replay attack countermeasures

Specifically for number three, we viewed this less as a failure to gain entry and more as a successful denial of service attack. Disabling remote entry is at best a nuisance and at worst a safety risk if quick entry is necessary. Keep this in mind if your remote entry fails--have a physical key at hand to manually unlock your door.

Defenses Against Replay Attacks

The most obvious deterrent is keeping your key fob in your possession at all times. If this isn't possible, avoid keeping valuables in the vehicle. Utilize a Faraday bag while storing your key fob inside your residence or workplace. These are the simplest and least costly solutions. Ask your dealer about remote entry system upgrades if that is a necessary step. For those of us who own vehicles lacking remote entry, your threats remain slim-jims and busted windows.

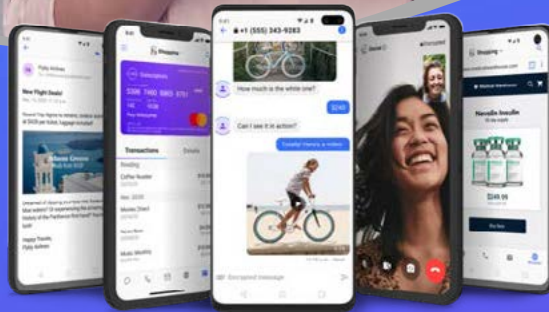
You may have noticed that wireless defense is squarely on the shoulders of the victim. Security in the RF domain is very weak and exploitation is difficult if not impossible to prevent. With some basic knowledge, though, you can gain the upper hand in preventing this simple attack. ■



The World's Only All-in-One Privacy App



Sudos act as digital firewalls to eliminate data trails.



Call, Text, Email, Browse, Shop and Pay
Privately and Securely



Create digital identities,
or **Sudos**, for different situations.



Research
Jackie Russell

jackierussell@sudomail.com



Travel
Jackie Russell

jackierussell02@sudomail.com



House Hunting
Jackie Russell

jackierussell03@sudomail.com

Sign up without an email, phone number or password | MySudo.com/bazzell



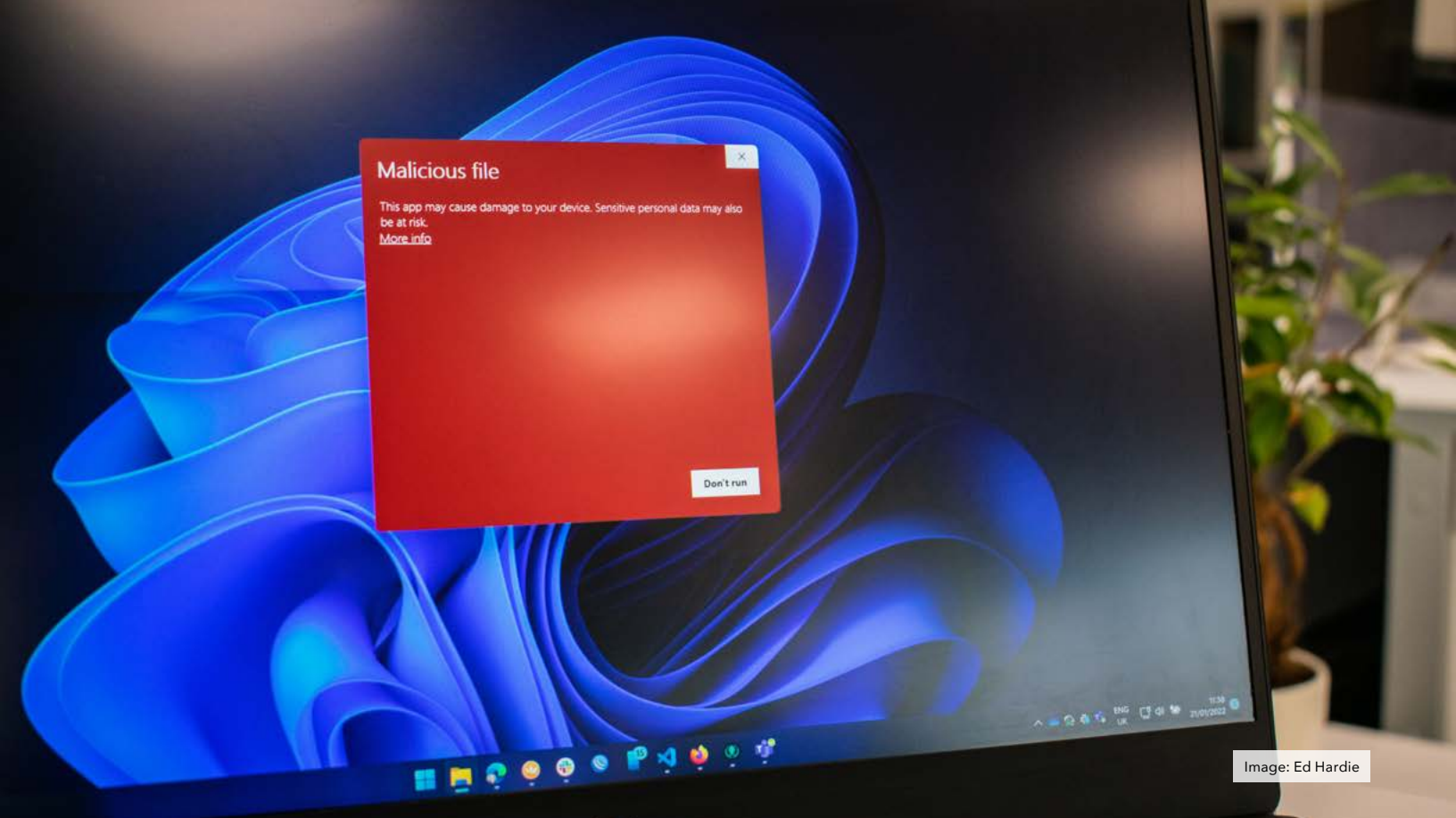


Image: Ed Hardie

MALWARE OR MAL-AWARENESS?

By KVKK

The Normalized Forms of Spyware and Ransomware that go Undetected by the Standard Cultural Antivirus

1. Whatever Happened to "Spyware"?

Do you remember in the late '90s and early '00s, the pioneering days of P2P file-sharing platforms like Napster and Kazaa, when the risk of downloading "spyware" was a common buzz? Sure, viruses and other malware were around then as now, but there was concern about "spyware" specifically. Within just a decade, we ceased to hear as much about "spyware" as such--for the basic reason that this malware had by then become synonymous with software: an

accepted part of virtually every "free" and soon-to-be "essential" service paid for in the currency of personal data. People know Facebook and Google are spying on them, but no one, not even privacy advocates, now articulate this fact as "Don't download/use Facebook or Gmail because it could contain spyware," let alone "It is spyware." Google Ngram shows the frequency of the word "spyware" skyrocketing between 2000-07, then halving from 2007-15 and continuing to drop off into the present.

More importantly than any technical reason for the word's decline is that it reflects the cultural normalization of digital spying: it would seem we no longer needed a term to specify what has become so obviously

abundant. Indeed, in the year 2000, which etymonline confirms is about the time that "spyware" first became widespread, the scale of digital surveillance that would soon emerge was far beyond this word's originally narrow scope. Yet, Wikipedia traces the word's first occurrence to "1995 in a Usenet post that poked fun at Microsoft's business model." How ironic and prescient, given that spyware now is part-and-parcel of virtually every big business model! The definition given by etymonline, "software used to obtain covert information about a computer's activities by transmitting data covertly from its hard drive to another computer," could now describe almost all software. By stark contrast, even though "spyware"

would be a much more descriptive term for some types of “cookies,” the latter cute moniker has survived and thrived, allowing webpages and apps that “courteously” ask to spy on us to depict this with JPEGs of chocolate-chip cookies, instead of what we might find in a culture where privacy is the default: the digital equivalent of a WHMIS biohazard symbol.

Clearly, there’s a point to be made here about how privacy is not just a technical battle, but a cultural one, in which public relations, branding, and terminology play an equally important part. Branding spyware as a “cookie,” one could say, is a successful virus, a linguistic virus, the sociocultural equivalent of malware, aliased as legit. Regardless of what software does at a technical, social, or organizational level, the ultimate measure of what is ugly gross “mal” versus cuddly chewy “soft”, is us. Hence begging the question: What forms of malware have we already unlearned to flag in our personal security policies, or never learned to flag? And what malwares of the present, like the “spywares” of the past, will become the software status quo of the future? Ransomware, I’ll suggest in section 2, could already be one.

So, while the infosec battleground is usually framed between “malicious” attackers and “legitimate” defenders, sometimes we all-too-easily forget that all of these battles themselves take place within larger cultural wars of what defines “legitimacy” in the first place, and who gets to decide that. The whole reason why “social engineering” is a thing at all (in the “malicious” sense) is because we’re already socially engineered. And the most successful social engineering therefore is what becomes so normalized as to become unconscious to us, so that we no longer even think of it as social engineering, or question its dominance. In the jargon of political philosophy, this utter domination (to the point of unconsciousness) is called hegemony.

The banalization of spyware, as marked by the term’s departure from the public discourse, is a prime

example of such hegemony, which is further illustrated by how even the most blatant and egregious forms of digital surveillance continue to go unmarked in the public media. Why, even in spite of the Cambridge Analytica scandal, does Facebook still even get labeled (i.e., socially engineered), in and by the media viruses, as a friendly-neighborhood “social media” platform instead of as a social surveillance, data-theft, and SaaS (spyware-as-a-service) platform? Ultimately, it’s because the culture has continued to accept its “un-malicious” PR marketing as such (much in the same way that FB has recently rebranded to Meta, to foment forgetfulness and obliviousness). The word “PR” itself is another example of good society-level social engineering: it’s still called “PR,” not “social engineering.” Software unmarked by the prefix “mal” may be no more than the maliciousness we’ve been conditioned to accept as “soft.” Controlling the definition of malware vs. “benevolent” “norm”-ware is itself part of the infosec battleground.

To illustrate the point, I’ll now tell a story of how software whose effect is indistinguishable from ransomware nevertheless passes unflagged by the cultural antivirus.

2. Forced 2FA as a Form of Ransomware: The Case of Google

My story builds on a previous Unredacted article: Michael Bazzell’s “When 2FA Harms More Than Helps” (Issue 2, Jun. 2022). Bazzell relates the story of a client who, after having her phone stolen, lost access to all her accounts because she was following some typical “good” security advice: she had a password manager and two-factor authentication. However, this meant that she no longer knew any of her passwords (because they were all stored on her phone) and could no longer access her 2FA tokenizer. Her security measures had a critical flaw, because they utterly depended on her having access to the physical device. A bureaucratic rigmarole with her cellular provider ultimately concluded in her getting a kiosk clerk to perform for her the equivalent of a SIM swap: thus, proving that “Any adversary could have

done the same thing in her name.” In short, in this situation, “soft” and “mal” traded places: her own good security policies backfired into her worst enemy, and her cell provider’s vulnerability to “malicious” SIM-swap attacks became her only friend. Bazzell’s key takeaway is, “Never use 2FA with your true cellular number.”

But what if she hadn’t been so “lucky”? What if the story had stopped there, at the kiosk clerk?

Let’s imagine, instead, that when she lost her phone, she hadn’t enabled 2FA on her accounts; but then, when she went to access, say, her Google account, it asked her for a secondary validation anyway--because Google, being the “good” security-conscious watchdog that it is, “protective” of its assets (including users!), unilaterally updated its user agreement and security policies to align with “good” infosec industry practices (which it also helped define!).

This is basically what happened to a friend of mine, albeit under slightly different circumstances. Back in 2011, she had had a YouTube account to host promotional videos for her small business. When she closed the business and cancelled its web domain hosting in 2013, she neglected to shut down the YouTube account as well, which was associated with an email account under the domain name of her former business website.

Unfortunately, it wasn’t until years later that she realized the YouTube account was still active. Fortunately, she still remembered her password. But when she went to log in, YouTube prompted her for a secondary validation code, from the now-defunct business email address. (Also, clearly, my friend was no longer signing in from the account’s last-known trusted device or IP.)

She personally had never activated 2FA on the Google account (it seems inappropriate to say “her” account at this point). But, because of changes in the infosec landscape (both at Google and in general) in the intervening years

(e.g., the legacy of the 2010 Operation Aurora hack), as well as Google's amalgamation of all its services like Gmail and YouTube under one general "Google" account circa 2015, Google by now had unilaterally imposed a stricter security policy onto all of its user accounts. In the intervening years, Google had probably at some point notified its users of updates to their user agreement, which surely would have informed her in the boilerplate legalese that by continuing to use Google's services she was agreeing to such-and-such terms. But as we all know, no user really "agrees" to such agreements; and in her case any such impersonal notification never would have reached her at the defunct email address anyway.

The hard lesson that my friend discovered is that Google provides no practical recourse to recover your account, in this situation or similar. The Google Help Centre provides a number of How-Tos ("Tips to complete account recovery steps", "account recovery," etc.), but these instructions address only a very limited number of situations, and the hyperlinks ultimately just send you into a loop, back to the sign-in page.

For example, when you click the "Try another way" option for the secondary validation, then unless you already configured your account with a cell number to receive a text, there is no other recourse except email. If you go to the "Can't sign in to your Google account" help page, select the issue "You're having trouble with 2-Step Verification," then select the "You can't sign in to your device or an application, like Outlook" option, it just leads you back to more instructions for how to set up 2FA. When you select "You're having a different issue," the button doesn't even work: it doesn't even provide you any information at all.

Remarkably, even when you go to the "Find out if your Google Account has been hacked" page, most instructions just assume you can still access your account! Under the "Suspicious account activity" subheading, there is a bullet for "If this setting was turned

on or off without your knowledge," but it provides hyperlinks only once again back to the basic "Two-step verification" info page.

Finally, of course, there isn't any readily available Google "customer service" to speak of. It's just an endless labyrinth of more DIY steps and community forums. In the latter, you'll find other users confirming your worst fears: you're screwed.

I'm not trying to suggest that Google's security policy is necessarily a bad practice. Nor am I suggesting my friend was without fault. Obviously, she made some key mistakes: when you open or close any account, you should also consider its interdependencies. And it would be a good idea to keep track of all digital assets you have in the first place, so you don't lose track of your digital footprint for years.

Nonetheless, the situation raises an important point: "good" security is not always your friend, especially if it's imposed on you from without; what's "good" may not be good for everyone. One person's fortress is another person's prison, because privacy and security are two sides of the same coin: a digital feudal lord grants security in exchange for other insecurities.

In my friend's case, the effect of Google's "protection" (corporate protectionism) was indistinguishable from a sort of ransomware: Google's umbrella/governance model of security had locked her out of her own data. (By contrast, in the original Proton Mail, the service at least made clear to you that if you forgot your password, there was no recovery option, due to their privacy policies.) And of course, she wasn't alone. When I Googled "Google is holding my data hostage" I found many worse stories of people losing all of their data to locked accounts, and having no legal recourse (not even the FBI). They, too, described this as a "hostage" situation, with one user even comparing Google to "living in China."

In the meantime, what happens to the data? It remains there, indefinitely. Google owns it, now, but the liability

is still assumed by the user. Because, just imagine, statistically, how many unrecovered accounts must exist, some subset of which have expired domains. And some subset of those accounts will have weak passwords, or will have usernames and passwords that match up to breached account datasets from some other service. Once a hacker has cracked the password, then they would simply need to either buy the domain name and set up the defunct email account anew, or otherwise exploit the Simple Mail Transfer Protocol to redirect the validation code... In this scenario, suddenly Google is a storehouse of defunct accounts ready to exploit. But of course, it already was this—it's just that the difference between "mal" and "norm" is a question of trust and perspective: whom you trust to protect your data, and which socially engineered version of the world you'll accept as "norm"-ware. Because the above vulnerability to users isn't the sort of thing you'd find on a bug bounty list; it's not a security "flaw," it's a security policy. And yet, as my friend's case shows, from another perspective there is indeed a gaping flaw here—in terms of security, privacy, and personal digital asset ownership.

My friend's last resort has been to file a DMCA Takedown notice with YouTube: claiming that her own account is violating her own copyrighted material. Ironically, in order to do so, you have to create a YouTube account, because you then have to fill a web-form whose selection options assume that you are complaining about another person on YouTube who copied your own YouTube videos. So you have to fudge one of the URL fields and then indicate in a free-text field that your "infringed" work isn't, in fact, online. So, the prospects already aren't good: this could be a prolonged and work-intensive task to prove that she is the rightful owner and, in the end, even if YouTube ends up taking down the account's video content, this still might not technically prove that she is the rightful owner of the account itself. ■

SL PROFESSIONAL



An all-in-one OSINT solution for conducting in-depth investigations across social media, blockchains, messengers, and the Dark Web

 SOCIAL LINKS

**FOCUS ON
DECISION MAKING,
NOT DATA GATHERING**

1000+
METHODS

500+
DATA
SOURCES

1.3
BILLION
IDENTITIES

DATA MODULES



SOCIAL MEDIA

Combine an expansive set of search methods for all major social networks and the basic configuration toolkit



MESSENGERS

Retrieve a range of data from WhatsApp, Telegram and other popular messengers



CORPORATE

Delve into corporate sources including OpenCorporates, CompaniesHouse, Offshores, and Google Companies



DARKNET

Gain full anonymous access to Dark Web marketplaces such as Dread, 8chan, Hydra, Raddle, and more



SL ISE

Search through an exclusive set of 2000 public data sources containing 1bln identity data sets



CRYPTO

View transactions, addresses, destinations, senders, and tokens from all main cryptocurrency blockchains

ABOUT SOCIAL LINKS

Learn more at sociallinks.io
Contact us at: sales@sociallinks.io

2015
FOUNDED

500+
CLIENTS

50+
COUNTRIES

HQ
USA, LATVIA, NETHERLANDS



BOOK A DEMO

SOCIAL LINKS: REVOLUTIONARY AI-DRIVEN OSINT SOLUTIONS

Sponsored Message

Since 2015, Social Links has operated at the forefront of the emergent open-source intelligence market. Their award-winning products have been the solutions of choice for law enforcement agencies around the globe, as well as many enterprise IT corporations from the S&P 500. As pioneers of OSINT technologies, the company continues to deliver advanced tools that empower organizations across a range of sectors to significantly streamline workflows and achieve key goals.

The developer's products offer various powerful features, which national law enforcement agencies frequently use to harness the potential of open data, drawing from social media among other sources. The **AI-driven facial recognition** tool included in the flagship solution SL Professional enables investigators to derive huge volumes of relevant data from a single photo or profile picture. Such technologies often provide crucial insights that lead to breakthroughs and the identification of criminal actors.

SL Professional has also proved to be an essential tool in cyber security. **Link analysis** and **digital footprinting** techniques enable security professionals to find subtle connections which would slip beneath the radar of conventional search methods. This facilitates a truly thorough detailing of cyber perimeters and greatly enhances threat intelligence processes such as penetration testing and incident response.

The sphere of corporate security likewise benefits tremendously from Social Links software. In particular, SL Professional has been a central tool for conducting high-quality due diligence and background checks. For instance, the bespoke search methods **hidden Facebook friend detection** and **image search by geolocation** have been used to great effect in establishing clandestine connections between organization employees and external contractors.

Furthermore, SL Professional can be essential for national security, allowing

analytical units to successfully monitor and detect organized groups that pose threats to attendees of public events. In such cases, features which have been instrumental are group identification and Telegram and Discord search functions.

SL Professional is a powerful all-in-one OSINT solution for conducting in-depth investigations across social media, blockchains, messengers, and the Dark Web. The solution provides sophisticated access to over 500 data sources, 1000+ built-in original search methods, plus AI/ML technologies, and has integrations supported by Maltego, i2, and Spiderfoot HX.

If you would like to learn more about how Social Links OSINT tools can help organizations streamline processes and accomplish core goals, follow the link below for a free product demonstration.

[BOOK A DEMO](#)

AN OSINT PRACTITIONER'S PERSPECTIVE ON PRIVACY, OR, HOW I LEARNED TO STOP WORRYING AND EMBRACED OBSCURITY

By Anonymous

For the past twenty years, I've been an "OSINT practitioner" and have used those capabilities to support operations to save lives and put bad guys in jail or in the dirt. I've used OSINT with a variety of organizations in a variety of settings and scenarios from intelligence-led academic research, situation awareness & understanding, strategic planning, cybersecurity operations, and investigations. Over the years, I've conducted OSINT activities against hostile nation-state actors, terrorists, interstate drug traffickers, hacktivists, estranged spouses, and ordinary criminals. I certainly acknowledge that others in the OSINT field are doing absolutely incredible work by using their knowledge sets and diverse data sources.

Open sources have evolved and changed over the years and the discipline requires an ability to adapt to those changes. For instance, social media sources such as Facebook and Twitter were excellent sources to obtain information on individuals and develop situation awareness. Over the years, those sources have been increasingly less available through user privacy settings and throttling by requiring payment to extend "reach". Likewise, what might have taken hours of querying in Lexis-Nexus would now take just seconds in a publicly available search engine.

Any OSINT analyst needs to be aware of how sources worked in the past, how they currently work, and how those sources may change in the future, and with that, how those analysts need to change their practices. "Change is the constant" applies to OSINT. An online tool may be free one day and become a limited or subscription-based the next. Many OSINT tools are provided free from others by their own largess. Those tools may not be updated or include bugs/errors.

As an analyst, my ability to get information on individuals and dig into their privacy is based on time available, search/analysis capability and efficiency, and data available. When I'm doing an investigation, it's usually time sensitive. I could spend numerous hours chasing dead ends and billing for those hours. That drives the cost up and makes for unhappy clients. In the same vein, I need to make sure I'm doing a complete investigation. Efficiency is key. Another part of this time factor is the workload: these investigations have deadlines. I may have multiple cases to work in a limited amount of time. I'm not a reddit investigator that has the ability to crowdsource the work.

Ethics, legal constraints, and privacy also play into the investigative process. I need to be 100% certain of derogatory material. If it's up for question, then it doesn't help to present a final conclusion on the case. Even though I'm digging into someone's privacy,

personally identifiable information (PII) protections come into play. On a state-by-state basis, the legal limitations on private investigations vary. Some states have some pretty strict requirements while others are loose. Another factor is ensuring that investigations are done in a forensically sound manner. The results need to be complete and repeatable as some intelligence or investigative material may wind up in court.

One of the most significant factors in OSINT analysis is the skillset of the analyst. What tools do they have available? How well experienced are they on the tools and do they use them on a routine basis? How well do they adapt to changing data sources—are they familiar with just Facebook or do they know TikTok as well? Can they think creatively in doing searches or collection? Can they stay focused on a case and avoid distractions during the full course of the investigation and stay in scope? To remain focused, I block parts of my brain with cyberpunk rave techno or melodic black metal, but everyone has their thing. How efficient are those analysts in time management and use of tools available?

A good example is building sock puppets. I have built several, but not kept them up. It's a lot of work to maintain them on multiple platforms and invent activity for them. Some of the fake person generators out there help in creating information to build out the background of these sock puppets,

but it's never an airtight process. I don't try and catfish with them because that's too much work and their legends aren't that well built out. Ultimately it becomes a time spent versus benefits gained matrix, and I haven't come up positive with the types of investigations I perform.

For those who are privacy-savvy, none of what I have below will come as a surprise. "Security through obscurity" works. As an investigator, I have Extreme Privacy and the Open Source Intelligence Techniques books and have read them. I know what a half-assed PMB looks like. I have a favorite set of tools and a second set in case I don't get the results I need. With all this being said, I offer the following set of tips and practices that diminish a sizable portion of your open source footprint. Keep in mind, other analysts and investigators out there are more skilled than me, have access to more tools, and have more time. Here are some privacy tips.

Avoid social media like the plague.

As hard as it might be, try to avoid being in photos from other family members. When I've run into dead ends on some investigations, I've "spiraled out" to look at family members or possibly known associates. I often start first with the target's mother and then work my way across the family tree. At this point in time, the cons greatly outweigh the pros when it comes to social media use. I have one social media account that I use for OSINT collection and that's it. I post nothing, just collect.

Counter facial recognition as much as possible. Most law enforcement agencies have the capability or access to the capability for it, but it requires significant detectable facial features for the analysis to be effective. Obscuring or disguising one's face remains an effective means of defense. Hats and sunglasses work, are cost effective, and don't raise unwarranted attention. Face coverings have become less ubiquitous in the past year as the pandemic winds down. In some places, those face

coverings may gain more attention depending on the environment. If you walk into a hospital, it's normal. If you walk into a bank, it will set the tellers on alert. You can fool facial recognition systems with bizarre haircuts and face paint—best applied if you're at some sort of comic convention at least. And, yes, I have used facial recognition in investigations. I found a subject on a swingers site and found that he was cheating or attempting to cheat on his wife.

Diversify usernames. One mistake that is frequently made is re-using the same username over and over again. I understand it's helpful for creating a sense of consistency among platforms. For instance, if you're running a small business, it makes sense to have the same handle across Google, Instagram, and Twitter (or Mastodon if you've been following the news). Each of those services is owned by a different provider and some crossover through shared authentication is possible. For privacy purposes, have a set of varying



INDUSTRY LEADING TECHNOLOGY AND A 24X7 SOC WORKING FOR YOU

Cyber threats are evolving rapidly. SMBs and Enterprise businesses are looking to their Managed Service Providers to provide them with cybersecurity solutions. Our managed SOC is highly-skilled in the constantly evolving threat landscape and will provide absolute security for you and your clients.



FORTIFY24X7.COM | (800) 989-2647 | INFO@FORTIFY24X7.COM

usernames and related accounts. If I can't directly connect a username to an individual, it's just a hunch and that's the end of it. Likewise, if it's a commonplace username, it makes attribution difficult as well.

Embrace "unintentional synthetic identities". While conducting an investigation on someone I already knew to a degree, I found that one personal information search tool compiled information together of him, a prior resident of an address, and someone with a similar name. That tool had created an "unintentional synthetic identity" for him. This was not the first time I'd seen such a phenomenon. From the privacy-focused camp, it helps to add a level of obscurity and requires an investigator chasing down what will likely be dead ends. This wastes time and introduces inefficiency into the whole process. A step further for those constructing their privacy defense-in-depth is intentionally seeding disinformation to amplify these synthetic identities.

Embracing cut outs. On a similar note, targeting for friend for demonstration purposes led to several people that

were certainly not him, but made for some good cut outs. I've known him for over twenty years and should easily find him with address and people searches. Instead, I found individuals with the same or similar name and age, good overlap with former states of residence, and even relatives with the same names. Had I been doing this as a "black box" investigation instead of a "white box" investigation where I knew what answers I should get; I may not have known the difference. Without a photograph, I'd be forced to head back to my original source information and re-evaluate. The rabbit hole and false positive potential is high.

Mundane SSIDs for Wi-Fi. Considered outside of the typical OSINT realm, but catching on. Any on-the-ground analyst or investigator looking at an electronic signature will have access to a decent Wi-Fi scanner tool and myriad repositories online. If down to close-access at or near a target's residence or place of work, wireless signatures can play a heavy role in confirming a host of other clues. You may discover a network broadcasting a target's name or something seen in previous hits like neighbors' names. Broadcasting a SSID

with an anonymous and bland identifier, like "2S19M2", helps blend in with all the other residential networks out there. Also, if you move, change it.

Be careful who you Venmo with. That information is available and it's very easy to follow who gives money to who and possibly for what. Again, using varying usernames helps in obfuscation. As always, cash and other more anonymous payment methods work better.

As OSINT evolves, so do the results in the final intelligence product. In turn, privacy measures must evolve too. It's a constant process. From the practitioner's side, the ability to successfully find useful information has clear limitations, mostly with the time and scope of the work, skills and mindset of the analyst, and information available. Let's not forget the money needed to access premium data or house the petabytes of free data. As a privacy-loving would-be target, the basics work. Stick to the foundations and take the time to get the low-hanging fruit picked, and something about a bear and being faster than someone else. ■



INVESTIGATORS TOOLBOX

An Exclusive Online Community
For Investigative Professionals

- *Interactive Member Forums
- *Educational Training & Webinars
- *Robust Curated OSINT Library
- * Exclusive Member Discounts



Try Our App

www.investigators-toolbox.com

Join Today As A Member
Use Code **UR23** To Save 20%

Invest in Your Business Invest in Yourself

Cynthia Hetherington- President, Hetherington Group & founder of OSMOSISCON
"The Investigator's Toolbox is an outstanding platform for PI's created by a PI with our profession in mind! This is one of those industry standards that will raise the bar for investigators who want to stay informed, communicate with others in the field and have access to tremendous vendors, education and business building tools."



HARDENING MEASURES FOR MULTI-FACTOR AUTHENTIFICATIONS

By André Monteiro

Authentication plays an important role in any system nowadays. It verifies whether someone is in fact who claims to be. Basic authentication comes in the form of a password but for some time now, Multi-Factor Authentication (MFA) has been seen as a standard and a “must have” since it provides extra protection. MFA can be implemented and used in many ways like physical tokens, biometrics, software apps, SMS and more.

Since not everyone is aware of tokens or biometrics as a means to perform MFA, app-based methods are being adopted as a safer way to authenticate users instead of SMS's or phone calls. A tendency that is growing according to Microsoft.

Basic MFA functioning relies on One-Time Passwords (OTP). Software apps like Authy or Microsoft Authenticator have implemented cryptographic

hashing functions such as Hash-based Message Authentication Code (HMAC) to generate OTPs, that usually are composed by a 6-digit number, computed with a timestamp and a secret key.

In order to use a Multi-Factor Authentication, **three factors** must be considered and **two of the three are required**.

Those factors are:

- Something you know.** This method is based on the usage of a password or passphrase, a PIN or the answers to secret questions (challenge-response). It involves verification of something provided by the user.
- Something you have.** This can be a token device, a smartcard, an e-mail, a cell phone number or a smartphone in combination with an OTP software app. It involves

verification of an item that the user has in their possession.

- Something you are.** Like fingerprint, facial or voice recognition, retina or iris scan. This method involves verification of characteristics inherent to the individual.

The subject of MFA has been suffering changes in order to become robust over the years. Malicious actors continue to discover new ways of compromising the authentication process as it has been seen most recently by groups like Lapsus\$ that take advantage of the state of the fatigue of the users.

Considering the basic functioning of the concept, the following are five hardening measures that enhance the use of corporate MFA. The measures are based on current best practices and recent forms of exploitation, employed by adversaries today.

1. Disable MFA Default Configuration for text messages

SMS as MFA tends to be widely used because it is easy to configure and only requires a phone number to receive the OTP. This out-of-band authentication is considered the weakest form of MFA and organizations like NIST and Microsoft consider it deprecated and have been increasingly advising to leave aside its usage.

This type of MFA is vulnerable to SIM Swapping, does not rely in encryption, can be intercepted using software-defined-radios, FEMTO cells or SS7 intercept services, is phishable and can be brute-forced. Changing the authentication process to physical tokens, biometrics or software based-app is highly recommended.

2. Disable Pop-Up Notifications to Avoid MFA Fatigue Attack (MFA Bypass)

Recently, threat actors, like the Lapsus\$ group, have begun looking for ways to compromise what should be a security enhancing practice like app-based authentication. After threat actors obtaining valid credentials, they have been successfully compromising accounts with spamming/bombing push notifications by exploiting "MFA Fatigue".

"MFA Fatigue" can be seen as a second factor authentication bypass and the modus operandi of the threat actors concerns the overload of notifications a user receives during a day to perform logins or approve different actions. With the overwhelming volume of notifications, fatigued users try to dispatch whatever pop-ups are upsetting them and start putting security best practices aside.

Since the Covid-19 era, the overwhelming mobile pop-ups and notifications have increased considering that different business models have turned to remote work and enabled Virtual Private Network (VPN) to access internal resources.

With all the considerations declared, the attack is not particularly effective

due the technology but the human state of constant attention in the context of the excessive number of notifications. Fatigued users tend to accept notifications when they want to make them disappear, and many MFA users are not familiar with this attack due its recent exploitation which ends in some cases in the approval of fraudulent notifications.

In sum, this type of MFA exploits the fatigue and human attention. It is advised to disable pop-up notifications.

3. Block User Account After Several MFA Denials

Nowadays, most compromised accounts come from gathering passwords from data breaches and performing password stuffing attacks. Considering people use software app-based or SMS for the MFA, threat actors may abuse the OTP authentication by brute-forcing it.

In this sense, it is not common to find security controls by default to restrict the abuse of OTP authentication. Whenever possible, every account should be configured to be blocked or to initiate a password recovering process after a certain number of MFA denials occur.

App-based MFA is vulnerable to brute-force, phishing and malware running in the victim's device. In this context, configuring a maximum number of MFA denials should be a necessary rule.

4. Block Access By Location

Foreigner origins not expected for daily labour should not be used for authentication. For example, in a scenario with no restrictions implemented, a threat actor after gathering a pair of credentials from a data breach and that bypasses the MFA using the MFA Fatigue attack, would not have his location as an obstacle, however distant might be, to successfully compromise the victim's account.

Blocking accesses by location consistently reduces the authentications

allowed which consequently reduces the attack surface. In summary, it is advised enabling authentication only for the countries known for daily work. Authentications from countries not recognized by the company as legitimate, should be blocked.

5. Configure Physical Token or Biometric Authentication

Physical tokens and biometric authentications use FIDO U2F protocol for authentication. The protocol is designed to act as a second factor to strengthen the username/password-based login flows. It uses public-key encryption, which means that for each service used, a new pair of keys is generated and an unlimited number of services can be supported, all while maintaining full separation between them to preserve privacy.

The U2F protocol can be used in 3 ways.

- a. **Passwordless** or **tokenless**: the user just needs to unlock the device using biometrics.
- b. **For mobile**: the user inserts the username and password and then touches the registered physical token. The communication between the token and the registered devices is made via NFC or bluetooth.
- c. **For USB**: the user types the username and password, inserts the physical token into the computer and touches the button.

The U2F protocol also guarantees that the user login is bound to the real site. In other words, the authentication will fail on a fake site even if the user is convinced it was real. In short, the origin binding mitigates most of the attack surface, including sophisticated phishing attacks.

For the token usage, this type of MFA is vulnerable to hardware theft. For this purpose, it is advised having a second physical token as backup stored in a safe location. ■

GOOGLE ANALYTICS

by **tlundgren**

In this article, I will explain what Google Analytics is and how it works, then I will tell you, and show you, how to see analytics in action on an Android device. Finally, I will briefly comment on why defensive measures are usually taken at the network level. The article will be simple, although you will need some technical knowledge if you want to replicate the hands on exercise.

Google Analytics is part of Firebase, a solution Google offers developers to integrate into their apps analytics, crash reporting, authentication and many other features that they would simply not be able to develop and operate on their own. It works on Android, iOS, the web, desktop apps and games, is moderately easy to use and for many use cases totally free.

Analytics, the main component handling telemetry, works by capturing "events". In the context of an app or a website, an event could be Bob adding a new item to his shopping list or Alice opening a help page. Events can be complemented with context. Following the previous examples, the name of the item Bob added to his list and whether Alice was a first time or regular visitor to the website.

Further, Analytics offers the possibility to attribute all generated data to a specific user id. How user ids are built and what they mean is a topic worthy

of its own article, but suffice it to say here that the id can identify the user of a specific app on a specific device, a user across different apps and different devices, etc. Analytics also logs some user attributes automatically when known, e.g. age, gender, interests, language, OS, device model (some restrictions apply in the case of iOS).

All this information is then sent regularly to a server, typically owned by Google, where it can later be analyzed. Google provides several tools and interfaces for completing that task.

Now let's see Analytics in action (note, however, that Google does not let us see information "captured" by them automatically, like gender, among other things because this data is not collected by the app, but rather is already known by Google). Connect your phone to your computer and make sure it is accessible from adb (see episode 246 "Android Sanitization" on IntelTechniques.com if you don't know what that means). Open a shell or command prompt window and set Analytics logging to verbose.

```
adb shell setprop log.tag.FA
VERBOSE
```

```
adb shell setprop log.tag.FA-
SVC VERBOSE
```

Display Analytics logs.

```
adb logcat -v time -s FA FA-
SVC
```

Open an app and interact with it. As you do so, some messages will start appearing on the screen (if none or just a few, it might be that the app does not use Google Analytics; try with another one). In my case, I opened an app similar to Ebay's and loaded My Favorites page. Among the events generated by the app were the transition to the Favorites page as well as the display of an ad. Details included the previous screen I was in, the ad provider and identifier, the type of connection I was using...

10-28 12:11:11.374 20106 21147 V
FA-SVC : Logging event:

```
origin=auto,name=screen_view(_
vs),params=Bundle[{ga_event_
origin(_o)=auto,
engagement_time_msec(_
et)=1992, ga_previous_class(_
pc)=BottomNavigationActivity,
ga_previous_id(_pi)=
3699676308727422989, ga_
screen_class(_sc)=
BottomNavigationActivity,
ga_screen_id(_
si)=3699787308727422994,
ga_screen(_sn)=View_Favorite_
Items}]
```

10-28 12:11:11.522 20106 21147 V
FA-SVC : Logging event:

```
origin=app,name=Impression_Ad_
Bid_Time,params=Bundle[{start_
time=137704413,
result=failure,
ga_event_origin(_o)=app, ga_
```

```
screen_class(_sc)=Bottom
NavigationActivity, ga_screen_
id(_si)=3699676308727422989,
request_id=/150868415/App_
Topbanner/Wall_Gad,
advertiser=Amazon, connection_
type=wifi, end_time=137704924,
AdUnit=5da46525-b241-4633-
94c9-10d78c22a86d}]
```

Later, I run a saved search and got more privacy relevant results. Notice how the event below includes the search keywords, my location (coordinates, street name and number, and distance to the vendor of the first item in the results page), whether the search returned any results, and what looks like the flavor of the algorithm used to determine the results that were displayed to me.

10-28 12:12:36.666 V/FA-SVC
(20106): Logging event:

```
origin=app,name=-
search,params=Bundle[{
latitude=51.50722, orderBy=
most_relevant,
hasResults=true, source=
```

```
stored_filters, screenId=111,
experiment=non_shippable_
boost_factor_variant_
baseline, ga_event_
origin(_o)=app, ga_screen_
class(_sc)=SearchWall
Activity, ga_screen_id(_si)=
-5842017622675563967,
longitude=-0.1275,
keywords=laptops,
newSearchLocation=221B Baker
Street,
London searchId=
a83ab289-17d4-4661-97dd-
07292ea40ca8, savedSearchId=
9f44a10d-8fff-4274-84af-27cfd-
b4adb3e,
firstItemDistance=390}]
```

If you run these tests it is very likely that you get a lot of messages on the screen. While there is a lot of clutter, it is also very likely that the app is recording most of your interactions with it.

You can restore Analytics logging to the default values (empty strings) by simply rebooting your phone. You can find your current values by running:

```
adb shell getprop log.tag.FA
adb shell getprop log.tag.
FA-SVC
```

Finally, since I referred to the Android sanitization episode of the IntelTechniques podcast, I will clarify that the commands provided by Mr. Bazzell then have no impact here since they target OS, not app, telemetry. Speaking of OS's, I don't know whether using GrapheneOS has any effect on Google Analytics: telemetry functionality is provided by libraries bundled with the apps we use, so GrapheneOS would have to override stock Android libraries that provide functionality to those other libraries without impacting acceptable use cases. That might be the case, but you should still bear in mind that not all telemetry solutions are provided by Google nor depend on Google code. At any rate, the simplest solution against telemetry is to prevent the data from leaving your phone or your network, a topic which has also been explored in the IntelTechniques podcast. ■



MDR | XDR | INCIDENT RESPONSE | PEN TESTING
VCISO | WEB3 & BLOCKCHAIN | MANAGED SIEM
HELPDESK | IDENTITY MANAGEMENT
DISINFO MANAGEMENT



**REAL-TIME THREAT
DETECTION**



**REAL-TIME THREAT
RESPONSE**



**PROTECT YOUR ENTIRE
NETWORK**



**PEN TESTING AND
VULNERABILITY SCANNING**



**REDUCE YOUR IT/SECURITY
WORKLOAD**



**AFFORDABLE
PRICING**

FORTIFY24X7.COM | (800) 989-2647 | INFO@FORTIFY24X7.COM

COOKIES BLOCKED. TO THE MOON.

Privacy-focused websites that sell.



Astropost

Astropost is the official design partner for this issue of UNREDACTED MAGAZINE. Need an ad designed for the magazine? We'll help you out!



Image: Dan Dimmock

THE OSINT CORNER

By Jason Edison

Jason instructs live and online open-source intelligence courses for IntelTechniques in addition to working as a cyber-crime detective for a large U.S. police department. Each issue will feature an OSINT tactic from the IntelTechniques online training.

In the investigative and analytical fields, we often discuss the importance of context as the keystone in transforming information into actionable intelligence. Our mission is almost always one where we want to work towards a small stack of neatly organized intelligence versus a large pile of information. The first section of our reports should represent the findings which respond directly to the questions posed by our clients so that they may quickly ingest the key takeaways without having to dig through the entire document. This, however, does not alleviate us of the responsibility to substantiate those findings. This is where proper sourcing becomes important as a means of supporting key findings while not overwhelming the reader with detail in the early stages of the report.

As someone who not only writes, but who also reviews intelligence reports regularly, I would like to share some general advice as well as some potential pitfalls in how we source our investigative findings. As always, these are just my opinions on the matter and keep in mind that your own mission and reporting parameters may vary.

I find it most useful to share recommendations and best practices in the context of a scenario. In this case let us look at sourcing in the context of a due diligence investigation. A due diligence report on an individual typically focuses on locating online sources which expose personal information which could damage that individual or associated entities, such as business interests, at some point in the future. Issues with sourcing may arise in the research

or documentation phases of the investigation.

During a due diligence investigation, we will be searching for accounts, identifiers, and references such as articles and other postings related to our target. These may be personal data exposures which pose an exploitation risk at the hands of cyber criminals, a reputational risk due to third-party postings, or even the target's own social media activity. We will typically list the most impactful findings at the beginning of the report, followed by a profile detailing exposed personal identifying information. In reviewing these types of reports there are two primary issues that I see arise on a regular basis:

1. **Proper Annotation** – Failure to properly source where the information was located

2. **Diversity of Sources** – Gathering information from a very narrow type or limited number of online sources (lack of comprehensive search)

The former issue is very straightforward: clients and other third parties must be able to verify the accuracy of any findings in our open-source intelligence reports by reviewing where we pulled the data from. The client should not have to trust our findings, but rather the documentation should provide an easy path for them to review or audit our investigation. Any data point referenced in the report should include an exact URL showing where it was located on the internet during our investigation. There are many methods for annotating reports to connect sources to stipulated findings, but some of the most common are:

Footnotes – This is one of the most common methods of including sources in documentation. It has the added benefits of looking professional and also being intuitive. URLs and references are listed at the bottom of the report pages which keep the narrative sections clean and easy to read.

Tables – Tables make for easy organization and association between specific identifiers (account, username, etc.) and the sites where they were located. This is the most common method of displaying data where we need to correlate identifiers with sources. If your report includes ratings, such as seriousness of data exposure, you may wish to color code cells and include a color key.

Embedded Links – Embedding the links in the listed identifier is an option but is often not ideal because it does not translate well to printing out hard copies of the report. There is also an increased risk that your client may click on and open links unintentionally, which could create an operational security issue or further exposure.

Combination – Footnotes can be included in tabled entries, or the links to the source may be listed in the table directly depending on formatting preferences. Including embedded links in your tables along with footnotes or full URLs is an option that some choose. It is wise ensure that any embedded links are not directing your client to questionable sites that could expose them to threats or an adversary.

Appendices – Your report appendix may include full captures, lists of sources, or both. Keep in mind that even if you include sources in your appendix, you may want to include them in the profiles portion of your report as well for convenience. If your client has to hunt through the appendix anytime they wish to see an exact source, they may find the report cumbersome and frustrating to navigate.

File Attachments/Supplemental Documentation – Larger captures of raw pages, images, or videos may be provided in a zip file or other archive. This should be in addition to proper sourcing in the report and not as a substitution for proper sourcing. Many clients will not be interested in digging through the raw data to find the source URLs, so we will increase the value of our report by properly annotating sources throughout the report.

The second issue with sourcing is less obvious: if you use only a small number of online sources during the research phase of the investigation, your findings have a much higher chance of being inaccurate and/or non-comprehensive. Let's say we did a good job listing the sources used to locate email addresses, phone numbers, and aliases for our target, in our due diligence report. Those sources may increase our "confidence" in the accuracy of our findings only if they come from a diverse set of sources. For example, if every listed source for the target's online accounts is Spokeo.com, that is problematic. People search engines

such as Spokeo do not vet their data, and they have a very high instance of false positives in how they associate people with accounts, locations, and other individuals. If someone hired you to do an OSINT investigation, and you provide them with what is essentially a regurgitated report from a single people search site, they are not getting a good return on their investment. Failure to search a broad selection of sources is usually indicative of lazy OSINT.

Fortunately, this problem is easy to recognize and remedy when reviewing your final report prior to submitting it to your client. Review all sources pertaining to specific findings and highlight any which are attributed to a single online source. Conduct additional research to hopefully locate additional, disparate sources for the same data. For example, if you list a residential address for your target, but you have only located it in a people search engine, such as Spokeo, the next step should be investigating that address for any public records which might corroborate the ties to your target. Maybe your target paid taxes on that property, which would likely be evident when looking at county records for that tax parcel, or maybe they used that address when filing for an LLC or other business license. We will not always find multiple sources for each key finding, but we should attempt to exhaust a diverse set of sources whenever possible.

In situations where we dig and dig but are unable to locate additional sources, we might consider including a list of sources that were checked to show that a comprehensive search was conducted, despite lack of substantiating results. For any results which we cannot further substantiate, we may want to add a note indicating a low level of confidence due to it being from a single source.

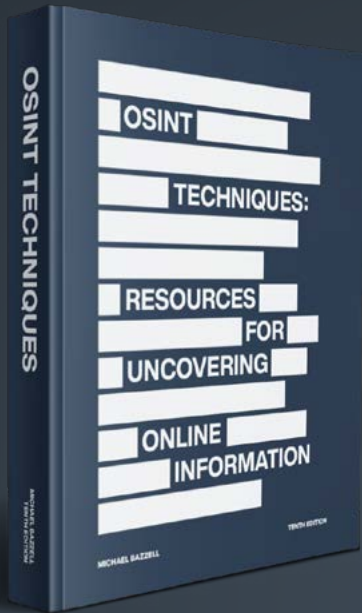
The following sample is provided as an example of very simple sourcing which meets the most basic requirements. There is room for improvement and

some polish, but we are providing the client with 1) a simple and intuitive table of identifiers 2) data points each associated with a footnote indicating the information source 3) a diverse set of sources used and 4) a note indicating where the client can review page captures of the sites listed without having to browse to the live pages. Analysis, such as level of risk, may or may not be included in your reports depending on the scope of the engagement. With this simple table as a foundation, we may then use any additional time to locate more data sources or make some aesthetic improvements prior to submitting our final work product. ■

Target: Jane Anne Doe

Phone: 555-555-1234	Fastpeoplesearch.com Targetsdomain.com LexisNexis	Risk: Moderate
Address: 55 Arcane Ln., Santa Fe, NM	Fastpeoplesearch.com Whitepages.com PertinentCountryrecords.gov	Risk: High
DOB: 10/12/2001	Fastpeoplesearch.com LexisNexis Judyrecords.com	Risk: High
Alias: Ms. Crabapple	Fastpeoplesearch.com Imgur.com	Risk: Low
Twitter: @randomperson66	Fastpeoplesearch.com Twitter.com Targetsdomain.com	Risk: Moderate
Email: someone@randomdomain.com	Spokeo.com Hunter.io LinkedIn.com	Risk: Moderate

New 2023 OSINT Book



- ✓ Hardcover & Paperback
- ✓ New & Updated Content
- ✓ 550 Pages @ 8.5 x 11
- ✓ Our Full OSINT Playbook
- ✓ Supports Our Free Podcast

Order at IntelTechniques.com

OSINT & Privacy Video Training

100+ Hours of Video Training | Optional OSIP Certification

Register at IntelTechniques.net





Image: Meritt Thomas

PET INTELLIGENCE

By Dennis Lawrence

Over half of American households own a pet. As a result, there is a significant likelihood that the subject of an investigation may have a dog or cat. This seemingly trivial issue can prove useful when attempting to locate an individual who may not want to be found or whose address is unclear in public records. In addition, pet ownership details can be misused by threat actors targeting a victim to help uncover their personal contact information for any number of reasons ranging from stalking to breaching an email account. Let's explore this topic from a few angles:

Social Media

People love posting content about their pets on social media, and some even create accounts for them on platforms like Instagram. This behavior can unintentionally lead to privacy exposures and a treasure trove of intelligence collection opportunities. Merely referencing a pet's name can

help threat actors create password cracking scripts to breach a victim's email account since pet names are commonly used to formulate passwords. In fact, a study released during May 2022's National Pet Month and World Password Day revealed that one third of US pet owners have used their pet's name as part of their password for an online account.

The simple act of posting a dog's photo on Facebook can also be exploited if the resolution of the image is high enough to where a user can read the writing on its tag. Not only can pet tags reveal previously unknown phone numbers and addresses belonging to an individual, but they can also include multiple phone numbers listed together that respectively belong to the owner and a previously unknown girlfriend or boyfriend who could be of value in an investigation. Another uncommon way to take advantage of this common oversight is to geolocate an individual's cell phone number seen on the pet tag using third party services that will ping the device.

In addition, background images in pet photos can provide insights into a person's location or pattern of life. Street signs, geographic landmarks, and property photos can be analyzed to help determine the possible location of a residence. Images taken inside a home can be compared with historical images of a possible residence identified on real estate websites. Reviewing the social media accounts of an individual's close associates may also prove beneficial as they may post content of the pet during visits or while dog-sitting due to its owner's trip to Mexico for the week.

Lastly, a review of an individual's "liked" pages on Facebook may reveal their pet's veterinarian and preferred kennel which probably have the individual's up-to-date contact information on file. These offer strong social engineering opportunities to threat actors who can elicit additional details about a victim via phone calls at a relatively low risk. In addition, phishing emails disguised as messages from an intended victim's preferred

animal hospital containing a malicious attachment labeled as an invoice are more likely to be opened.

Pet Owner Marketing Lists

Sooner or later, many pet parents end up on pet owner marketing lists. These lists are often divided by geographic location (i.e. state), and have been compiled using data sources as diverse as veterinary hospitals and online pet food websites. Why do they matter? They are filled with contact information such as names, email addresses, and physical addresses that can sometimes supplement content found in traditional data records aggregators. For example, an investigator may uncover a disposable email address used by an individual for his dog food subscription that was also used to create a social media account to harass a public figure which has direct relevance to their investigation.

Marketing companies like LISTGIANT and US Data Corporation have compiled pet owner lists for over 30

million Americans which represents about 10% of the US population. Even Experian has joined the pet marketing data business. Until April 2021, the credit bureau had a self-service option for purchasing pet enthusiast mailing lists which have since become restricted but may still be available to corporate clients.

Microchips and Pet Recovery Services

It is an increasingly common practice to implant microchips in pets, particularly in big cities, as a method of assigning them a unique identification number that is difficult to tamper with. Upon adoption, pet owners often make a nominal payment to one of a handful of pet recovery services in the United States that register both the pet's microchip number and owner's contact information in a database. This process helps animal shelters, rescue groups, and veterinarians identify the owner of a lost pet without a tag by scanning the animal's microchip using a radio frequency identification (RFID)

reader and calling a hotline to help reach its owner. However, pet recovery services can be socially engineered with nothing more than a pet's name, owner's name, and the owner's last known contact information under the auspices of the owner seeking to verify that their details are up to date. After all, pet owners are supposed to call these services every time they move or change phone numbers to make sure their information is current.

The human bond with pets can be very profound and impossible to break. In an increasingly digital world, these seemingly innocuous relationships can leave traces online that can be exploited by players on both sides of the law. Anyone with pets should understand how to manage the digital risks associated with having a furry friend. Conversely, investigators seeking to track down a suspect may benefit from following the digital paw prints. ■

Is privacy and security overwhelming? **We can help.**

Whether you are ready for a complete anonymous relocation with a full privacy reboot or simply need a one-hour call directly with Michael Bazzell, we can eliminate the frustrations encountered when trying to be invisible.

IntelTechniques.com





Image: Diana Polekhina

10 MINUTES OF GOOGLE DORKING FOR COVID DOCUMENTS

by Jon Gaines

Well now that we are all hopefully past the height of the pandemic. I thought I'd start to examine the technical debt left over from this. Now that isn't to say more won't be appearing online. That said, let's look at literally 10 minutes of some basic dorking and what we come up with!

First off, I found a lot of people posting their results to Scribd. I guess for easy access? Maybe they don't realize that this information is public? Here are some examples of French COVID tests and the results I found on Scribd. I must've found around 30 in a second. Note I blurred out a lot of the information even though technically it's public online.

These documents also linked to documents from other people via the recommended sidebar:



Fiche de résultat de test virologique de la Covid-19

Données démographiques et de contact du patient :

Nom de naissance: [redacted]
Prenoms: [redacted]
Date de naissance: 11/1 [redacted]
Adresse postale: 6 RU [redacted] PAMANDZI
Numéro de téléphone mobile: +26 [redacted]
Courriel: [redacted]

[illegible]

That said, I immediately noted the “2ddocNeg” within the Document titles. That led me to do some dorking for possible directories containing troves of these documents. Using a simple dork like: “2ddocneg” intitle:Index 0f came back with 0 results. Which was disappointing but also a good sign. That said, don’t let looks deceive you. I then used a different dork: “2ddocneg” inurl:uploads, which led to Google responding with two results, one link to Scribd and one to a UK site.

EC/REP	Activated Response time	EC/REP
1.8	1.8	1.8

As well as some classic French COVID tests like the ones shown above and then this:

CERTIFICATE OF SARS-CoV-2 PCR TEST RESULT

Patient:	ariast
Date of birth:	13
Social security number:	5B
Passport / ID number:	3
Address:	V 0 3

Result:	NEGATIVE
Time of test:	18.11.2021 17:24
Test:	ThermoFisher TaqPath™ COVID-19 CE-IVD RT-PCR
Sample:	Naso-pharyngeal swab
Method:	Polymerase chain reaction (PCR)
Laboratory:	SYT Kivi http

Patient Surn	
Patient Fore	
Date of Birth	
Address: 5B	n 167t United Kingdom
Passport Nu	
	HPA

CLINICAL PATHOLOGY : COVID-19 (SARS-CoV-2) RESULT

Test Type: RT-PCR Test
Test Sample Date: 29/05/2022
Test Sample Collection Time (24h): 16:00

RESULT: Negative / Non-Detected

ADMINISTERING HEALTHCARE FACILITY

Test Centre / I
Address: DAM
Member State
Certificate Issi
Contact Numi

1 London SW6 1NY
BR.COM

- Your coronavirus (COVID-19) test result is negative. It's likely you were not infectious when the test was done.
- If you develop symptoms of coronavirus, it is advised that you take a PCR test. If you have any of the main symptoms the public health advice is to avoid contact with other people where possible.
- For more information visit <https://www.gov.uk/coronavirus>
- If you do not live in England, please follow and adhere to your local government rules regarding travel abroad and returning home.

Which if you can't see, contains First + Last Name, DOB, Address, PASSPORT NUMBER, sometimes Social Security Number and more! Needless to say, I stopped there and have reached out to the organization in question to tell them about their data leak. Remember this was all found in under 10 minutes. As of the writing of this article, the leak has been sealed! The organization is no longer leaking this information. ■

Are Trusts and LLCs overwhelming? We can help.

We believe all large assets should be titled to a Trust or LLC for privacy protection. Doing this correctly requires a lot of experience. We make sure your homes, vehicles, and any other assets which require titling stay out of your name. Contact us to reserve a consultation.

IntelTechniques.com



SUPERMARKET LOYALTY CARD PRIVACY STRATEGY

By: the privacy pirate

A new supermarket opened near my home recently and was actively seeking new members for their rewards program. I normally don't sign up for marketing campaigns of any kind, however, when grocery stores offer cash savings for scanning a reward card, I'm willing to play the game. I'm just not interested in providing any of my personal information in the process.

The store was opening new accounts onsite by scanning customer driver's licenses into their database and issuing new cards ready for immediate use. I asked for a paper application and was instead asked for my driver's license and told "it only takes a minute". Since it was my privacy I was worried about and not my time, I declined. Instead, I printed a rewards card application from the store website when I returned home and completed it at my leisure. The form asked me to provide my date of birth, home address, phone number, driver's license number and state issued, number of people in my household and their names and email addresses; none of which I answered truthfully. The application also stated that a "driver's license verification is required to prevent program abuse."

I typically avoid any activity that requests identification to participate, but in the rare event that I do, I

minimize the potential risk as much as possible. In this scenario, since there was a good possibility that my ID would be requested, I entered an altered and misspelled version of my first and last name. I gave a date of birth that was close but not quite right, a physical address of a relative with the same last name in a faraway state, but the mailing address of my local post office box. I checked the box for "Seasonal Resident" and provided a new Sudo email address and a fictitious phone number. I left the number of people in the household blank, but added a completely different name for my "partner", as IDs are not checked for additional card holders.

When I returned to the store, I approached the customer service counter and told the clerk I was interested in getting a new rewards card. As she started to ask for my driver's license, I said "here is my completed application" and handed her the rather lengthy document that she would need to enter manually. I knew this would keep her occupied while I tackled the issue of showing my ID. While she was busy entering all of my incorrect information, I explained that I forgot my wallet in the car and would be right back. I walked outside and waited for a minute or two, then returned to the customer service desk where the clerk was finishing up. I displayed my passport book, NOT

my driver's license, but kept it at a distance and didn't hand it over. As the line behind me grew longer, the clerk had no interest in prolonging the transaction any longer than necessary, quickly glanced at the ID that was presented to her, and my new rewards card with fabricated information was issued and ready to use.

In this example, even though a driver's license scan was "required" for verification and faster processing of the discount card, doing so would have compromised my privacy. Completing the paper application allowed me to input lots of misinformation into their database, which all needed to be manually entered by the customer service clerk. The act of "forgetting" my wallet added another element of annoyance to the task and the extra data entry took the focus away from showing my driver's license. I took a calculated guess that the clerk would not bother to compare the true information on my passport, a credential likely not viewed very often in her position, with the altered name and date of birth on my application. If challenged for a driver's license, however, my response is always the same: "I travel frequently and choose to use my passport for identification. I can board a plane and enter any country in the world that credential." That statement usually gets the job done. ■

CHANGING YOUR IMEI FOR CELLULAR ANONYMITY

By SRLabs

Being anonymous in mobile networks is hard as mobile network operators can track users through multiple identifiers. Even users that often change their SIM cards can still be tracked through their device identifier, the International Mobile Equipment Identity (IMEI). Therefore, we suggest to change the IMEI each time the SIM card changes. We implement and verify our approach for a “portable 4G LTE privacy router” called Mudi.

We discovered that Mudi’s privacy promises can be undermined by tracking at Wi-Fi and cellular protocol levels. In addition, the device stores Media Access Control (MAC) addresses of connected devices, which may facilitate forensic analysis.

To address both, we randomize IMEI, Basic Service Set Identifier (BSSID),

and MAC addresses and wipe logs. We provide an OpenWRT package `*blue-merle*` that implements the proposed measures and publish source code and documentation (<https://github.com/srlabs/blue-merle>).

Privacy threat assessment

The Mudi router comes with a built-in Virtual Private Network (VPN) and onion routing (Tor) capabilities, promising anonymity online. However, the anonymity promises do not extend to the Wi-Fi and cellular protocol levels. In addition, the device stores MAC addresses of connected devices, which may facilitate forensic analysis. This permits two tracking scenarios:

1. Tracking of the user’s activity, the device’s location, and, in some cases, the identification of the purchaser is possible through the IMEI.

The simplest method of mobile-network tracking is based on the International Mobile Subscriber Identity (IMSI), which uniquely identifies a subscriber by their SIM card. This tracking threat can be mitigated by regularly changing SIM cards. However, each mobile device has a unique IMEI, which is persistent across SIM changes.

It is a common misconception that changing the SIM card – ideally to one that is not registered – results in a completely new mobile identity, dropping all traceability. In fact, a user changing SIM cards would only change their subscriber identity in the eyes of their mobile network. If the device remains the same, both identities can be linked through the IMEI. By changing the SIM, and therefore, the IMSI, a user can obtain a new subscriber identity. By changing the IMEI, a device can obtain a new identity.

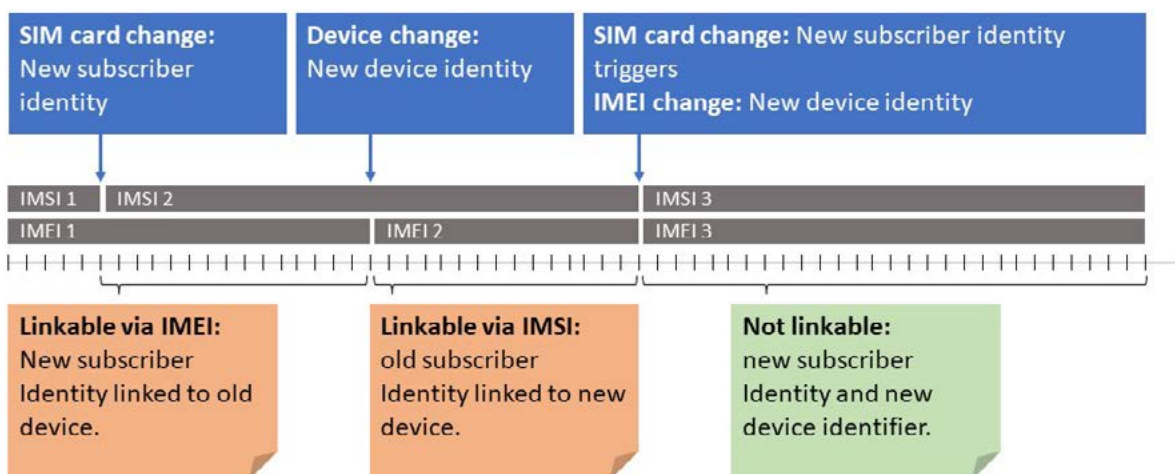


Figure 1: IMEI and IMSI change scenarios and linkability.

Figure 1 illustrates how IMSI and IMEI identifiers can be linked if not changed simultaneously. Only by changing IMEI and IMSI at the same time, the user can shake off the traces accumulated by the old subscriber- and device-based identities.

A device might even be traceable to a specific purchase, allowing identification of the purchaser.

2. MAC address and BSSID enable Wi-Fi-based location tracking.

The BSSID is an identifier associated with a specific WLAN access point, included in all wireless packets which correlates the access point to the associated clients. By convention, an access point's MAC address is used as the ID of a Basic Service Set (BSS).

BSSIDs are constantly transmitted by the Mudi router when it is offering a Wi-Fi network. By passively collecting BSSIDs, device identifiers can be mapped to locations. Mobile routers thereby also observe the MAC addresses of connected devices, each of which could be uniquely identifying a user. In case of loss, theft or confiscation, this data collection may prove detrimental to the users' privacy interests. Additionally, the MAC address can be collected by passive intercept. Therefore, the unique and static MAC address is in itself a risk for activity and location tracking.

Necessary features to mitigate these threats

To address the previous presented threats, one would need three additional features.

IMEI randomization

An IMEI change should be conducted upon every SIM card change to provide a new device identity. The Mudi router's IMEI can be changed by issuing Quectel LTE series-standard AT

commands. This command allows for two approaches to IMEI generation. The first method we implemented deterministically seeds the new IMEI with the SIM card's IMSI, while the second generates a random IMEI. To minimize the risk of an IMEI change, three things should be considered:

Multiple IMEI changes

Multiple IMEI changes increase the likelihood of alerting an ISP of suspicious behavior. Therefore, the IMEI should only be randomized when also the SIM card is changed.

IMEI randomization

Ideally the generation process would only allow for IMEI randomization when a SIM change takes place and would associate a single, randomly generated IMEI to that SIM card. However, this would require the new IMEI to be stored within the device. Therefore, the IMEI should be deleted from the router when the SIM card is removed.

Old IMEI leakage

To ensure that there is no leakage of the old IMEI after rebooting the device, the radio is switched off in advance. This disrupts the device's connection with the mobile network during the time the IMEI is changed, and the connection is only reestablished once the device is rebooted.

BSSID and MAC randomization

Since BSSIDs are another case of personally identifiable data, the protection of which can be eluded in certain legislative settings, randomizing it serves as a privacy measure.

To remove this uniquely identifying artifact, the BSSID should be randomized regularly. This also minimizes the risks of the BSSID being used to geolocate the user via open databases and the leakage of SSIDs and

BSSIDs of Wi-Fi clients such as mobile phones. This can be addressed by randomizing the MAC address on each boot. In this way, the device cannot be linked to past activities, whereabouts, and Wi-Fi connections.

MAC address log wiper

To prevent the risk that third parties with remote or physical access can enumerate the devices that have connected to the mobile router, all MAC addresses stored on the device should be wiped at each boot.

We have implemented an OpenWRT software package called **blue-merle** which takes all our considerations into account. A pre-built package, the source code and further documentation can be found at <https://github.com/srlabs/blue-merle>. We look forward to contributions from the community. We welcome pull requests to support other devices using the Quectel EP06-E/A baseband, or other basebands that allow changing the IMEI. We have not tested **blue-merle** on devices other than the Mudi mobile router. In principle, our approach can be adapted to other devices. Please keep in mind that the anonymity highly depends on the SIM card used which also depends on local laws and the possibility to obtain an anonymous SIM card. Furthermore, this is a research project without any warranty. ■

SIGN OUT OF APPLE

By NSDestr0yer

A big problem with many mobile apps is that they require you to log in via one of the abominable social media sites such as Facebook, Twitter or Snapchat. This is commonly referred to as Single Sign-On (SSO) where for your convenience, you don't need to remember additional passwords other than the one you use for a popular social media account. When you use SSO, those social media companies generate an access token that your app can use to verify you. That means the app has access to your token, and the company developing the app can often use that token for nefarious purposes.

An example is when Facebook SSO provides the token to a mobile app and on the back-end the app uses it to download all of your Facebook photos without your knowledge. While this has been changed so that the user has to consent to photo access, there's still other profile information and meta data that an app developer can harvest via your token. It's up to the developer of the app to respect your privacy and use the token responsibly. We know privacy is always top priority for the various executives and tycoons alike.

Apple attempted to fix the problem by introducing its own sign in mechanism that developers could use - Sign in with Apple. How it works is that you log in via your Apple account credentials and the app receives a similar token that it can validate on Apple's side with minimal information

about you. That way, you don't have to associate a social media account with the app or risk having it harvest a large amount of social media data about you.

Some parts of this alternative sound promising but there's a big caveat. You need iCloud to use this service. Apple states "To use Sign in with Apple, you need to use two-factor authentication and be signed in to iCloud with that Apple ID on your Apple device". I'm (fortunately) not an engineer at Apple but I know that tokens have been exchanged and validated in various forms for decades without requiring "the cloud".

Interestingly, Apple's developer guidelines state that if apps use SSO from a third party such as Facebook, they must also offer the Apple SSO. Apple assures us this is in no way about maintaining a monopoly position but is for your safety and security. You may also be surprised to learn that some developers have tried to fake the Apple button with their own sign-in methods. Apple's review process attempts to keep those developers at bay, making sure they use the real button.

Here's my problem with their implementation. As soon as you are forced to enable iCloud on your device, it immediately starts syncing your data to the cloud. You can turn that off, but can you turn it off so quickly that none of your data makes it to the cloud? For the data that does, is it already replicating across multiple redundancy servers? Does a delete truly destroy

the data? This seems like a strange trade-off. Instead of an app using your Facebook token to pull social media data about you, all of your device data is uploaded to the cloud.

One might think Apple's cloud may be more secure (ha), but we've seen many cases of iCloud breaches in the news, especially when the celebrities get breached. Apple had in fact planned end-to-end encryption for the cloud, but then backed off. Only some information is end-to-end encrypted such as health data, but the majority is not.

This auto-enabling and syncing of data is an inherently larger problem with Apple and it starts right from when you set up your phone or download your first app. Their prompts entice you to use their services, making the cancel or "no thanks" button very small, and it's often not clear what you are agreeing to.

For example, when you download an app from the app store, you are presented with a dialog to log in. Most people I've talked to think this is a prompt only to verify that one download. They do not understand that this has logged them in persistently and globally on their device up until they manually log out. Every action you do from that point onward is associated with that logged-in account. If you're feeling unconcerned by this, note the title to a previous podcast by Michael Bazzell - "The Creepy things Apple Knows About You".

So we're back to the same problem. Can I download an app and sign out right after, so quickly that no bits of personal data have a chance to escape my device? One solution is to use an anonymous iTunes account and not use any apps that mandate this type of sign-on. However, I feel that Apple's SSO checks both the "has potential" and "needs improvement" boxes.

For one, Apple's SSO offers the ability to mask your email. They have a private relay service that creates a unique and random address that forwards to your real email. That way, you can give the app a masked one. The app developer does get an option to know if the underlying email is verified – that is, whether Apple verified the email or not. But we don't know how they verify it and developers have to proactively implement this extra feature.

Another potential is that the service has some basic on-device machine learning capabilities to detect Apple spam accounts. This could be good for most of us when it comes to deterring

fraud. In a more detailed document, Apple states "Apple determines whether a user is a real person by combining on-device machine learning, account history, and hardware attestation using privacy-preserving mechanisms".

First off, what constitutes a real person? And does Apple have a list of them in their data center? In a perfect world, this hardware attestation would keep spammers out (preferably sending them to another planet). Again however, only if apps choose to can they use this feature to ensure the account is authentic.

In my experience, apps usually implement the bare minimum to get a feature working. When project managers are presented with rolling out an optional method, it almost always gets put in the "when we have more time" parking lot, which is in fact not a parking lot but a cemetery. And even if apps implement this feature, it's hardly reliable as there are all but three options returned from

Apple: "Likely Real", "Unknown" and "Unsupported". Would a spammer be unknown or unsupported? Or a "Likely Real" spammer? It beats me.

I thought I'd never say this but Google's account attestation is more seasoned. Android offers a full range of services, such as SafetyNet. But without getting into a comparison of each OS, I'll say there are some well-meant initiatives by both sides to provide the user with security and privacy. Now we just have to figure out a way to get the developers and companies to use them. Maybe we can do that if we push our privacy to the limits, only support companies that put privacy first, and Apple, if you're listening, make it so users don't have to sync their data just to use a more secure version of signing in. ■

A FACE WITH NO FACE.

Complete brand identities. For businesses that respect privacy.



Astropost



Image: Ludovic Migneault

READER Q&A

By Michael Bazzell

Q: If I share a Mac with one other user, so two user accounts, and I use Little Snitch to block Apple Telemetry, does that block it for both users or only for me and not the other user? Also, if I add a firmware password will that apply to the other user as well?

A: Little Snitch runs on the network level for all users. While you could eliminate the application from within a second profile, I assume your primary profile will still receive connection notifications if both are logged in. I would avoid this. I would set up Little Snitch identically on both user accounts with identical rules. Firmware passwords apply to the machine, and not specific users. You would only set that once.

Q: In the past, MB has mentioned using the Mint Mobile app to activate SIM cards. Would there be any advantages or disadvantages to activating Mint SIM cards using their website?

A: I have explained how one could use the customer service chat on their site, or call them via telephone, to activate a new account. All are acceptable.

Q: Mr. Bazzell, why do you install multiple versions of Firefox when Firefox can already run simultaneous profiles with the --no-remote option. Is there a benefit to using slightly different code? Or, perhaps you want to organically "spoof" the browser header?

A: I prefer multiple Firefox browsers for two reasons: isolation and simultaneous usage. When I have two isolated Firefox instances, I can make changes to the browser icon or appearance to immediately know which version I am in. I want them to appear visually different. Since I heavily modify my daily Firefox browser with various global settings, I want another copy of Firefox untouched. Sometimes I tweak things to the point of breaking. Having an untouched Firefox helps me always have a "clean" browser without restrictions. Often switching profiles is not enough for me.

Q: Are there any options to export Firefox settings including about:config to some file?

A: Yes. You can save the “prefs.js” file within your Firefox profile. It should contain all modifications, including settings and extensions. If you create a Firefox profile exactly as desired and export that file, you should be able to import the file into a new build to replicate the modifications.

Q: I’ve found that the worst data leak of our home address is voter registration data. While we are taking steps on our privacy journey, we have a way to go. We rent an apartment so it’s hard to conceal much of our info it seems, and the hardest yet is our address tied to our voter registration. Various people search sites have popped up that return addresses based on voter registration data. Not to mention, if you go to the Board of Elections page for our county, you can search by name and find anyone’s address (try searching Smith, for example, in Summit County, Ohio - <https://lookup.boe.ohio.gov/vtrapp/summit/vtrlookup.aspx>). Is there a way to be registered to vote without having your real home address divulged?

A: PMB nomads can register at their PMB address for national elections if desired. I would contact the appropriate office and tell them you are moving and currently using a local PO/PMB/CMRA address until you buy a new house.

Q: You mentioned that Stealer logs are becoming more prevalent. You also mention that you are gathering more Stealer logs to conduct your investigations. What operating systems do you believe is being adversely affected the most by stealer log malware? Is it primarily Windows systems that are being infected with this malicious malware or are you also seeing stealer logs from Linux systems as well?

A: In my experience, they are 100% targeting Windows systems.

Q: What happens when your YubiKey breaks? What do you do? Is it possible to get two identical YubiKeys for backup/redundancy?

A: I always have a backup YubiKey. When I attach my primary YubiKey to a service, I then add a second device and also connect my backup YubiKey for that service. They are not identical, but either can be used. They will each have a unique challenge and response.

Q: I am still not ready to be a GrapheneOS user and therefore trying to be as private as possible on my iPhone. I tried following the instructions on the latest edition of Extreme Privacy and installed ProtonVPN and setup NextDNS on my iPhone. However, for some reason, I cannot get them to work together. If ProtonVPN is connected, NextDNS is not being used. As soon as I disconnect ProtonVPN, NextDNS becomes active again. I tried looking for an option to use custom DNS, but iOS ProtonVPN app does not have that feature. Do you have a workaround for using ProtonVPN with NextDNS on an iPhone?

A: I have not used iOS in some time, but in the past, I changed the VPN protocol within Proton VPN in order to allow both to run. However, note that iOS now sends some Apple data outside of your VPN anyway.

Q: Any plans to introduce some type of notification system like emails for new podcasts/blogs/magazine uploads?

A: We have one. The feed at <https://inteltechniques.com/blog/feed/> will notify you of all new blog posts, podcast episodes, and magazine issues. Subscribe within your favorite RSS reader. I receive no information about you, I don’t have to worry about collecting email addresses, and you don’t have to worry about your information being abused/leaked/breached/etc.

Q: Can we get more guest episodes or client success/failure stories?

A: I would like to, but it is hard. My clients are mostly wanting to stay away from any attention. I never push any client to come on the show, but some have volunteered. I am open to more

of those shows if a client pursues the opportunity.

Q: What do you look for in a new car to minimize privacy invasiveness in terms of “features” to stay away from?

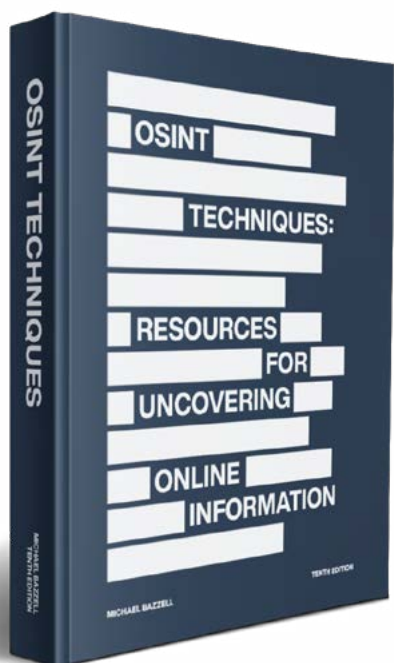
A: I like work trucks and base-model vehicles, but even those are not perfect. The big things I stay away from are embedded cellular connections and any type of assistant, such as On-Star. My newer vehicle has neither. Every year, this becomes more difficult. I used to avoid wireless tire sensors which each broadcast a unique ID, but those seem to be standard in most vehicles now. I predict there will be a huge market for vehicle privacy modifications soon. ■

UPDATES

By Michael Bazzell

Due to the release of the new OSINT book, I have applied several updates to the OSINT tools since the last edition. The current tools can always be accessed at <https://inteltechniques.com/tools/>. Below is a summary of a few of the changes.

- Search Engines Tool: Updated several Tor resources.
- Facebook Tool: Fixed issues with date queries.
- Instagram Tool: Added Toolzu.
- LinkedIn Tool: Added post timestamp decipher.
- Images Tool: Added FaceCheck reverse image search and replaced Google with Google Lens.
- Virtual Currencies Tool: Updated conversion utilities.
- Audio Streams Tool: Removed iframe due to insecure site access issues.
- API Tool: Added options for domain registration history. ■



This magazine serves as a compliment to the podcast, which can be found at IntelTechniques.com. Below are summaries of the episodes from last month.

279-Comms Ownership & Open Databases: I discuss true ownership of our communications including phone numbers, email addresses, domains, and monikers, and present two OSINT updates.

280-The Future Of Extreme Privacy: I offer a glimpse into the major projects we are working on for the next level of Extreme Privacy.

281-The Obsession Of Extreme Privacy: I revisit some impacts of extreme privacy and security on our mental health when we become obsessed with the little things, and offer ways I keep my own balance in check.

282-Major OSINT Updates: I offer numerous new OSINT strategies and their corresponding IntelTechniques tool usage, plus the latest news and updates.

283-Announcements, Updates, & News: I offer numerous announcements, updates, and news items related to privacy, security, & OSINT.

284-Back to Basics: Password Managers: I revisit the importance of password managers and offer new strategies for daily usage.

285-Travel Security Revisited: Jason joins me to revisit travel security protocols.

286-Closing Out 2022: I close out the year and announce the upcoming annual listener questions show.

287-Listener Questions: Our annual listener questions show.

LETTERS

By Michael Bazzell

Your Site Has Been Hacked by info@ji-gartenkonzepte.de

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS! We have hacked your website <https://unredactedmagazine.com> and extracted your databases. Our team has found a vulnerability within your site that we were able to exploit. After finding the vulnerability we were able to get your database credentials and extract your entire database and move the information to an offshore server. We will systematically go through a series of steps of totally damaging your reputation. First your database will be leaked or sold to the highest bidder which they will use with whatever their intentions are. Next if there are e-mails found they will be e-mailed that their information has been sold or leaked and your site <https://unredactedmagazine.com> was at fault thusly damaging your reputation and having angry customers/associates with whatever angry customers/associates do. We are willing to refrain from destroying your site's reputation for a small fee. The current fee is \$3000 in bitcoins (BTC). Please send the bitcoin to the following Bitcoin address (Make sure to copy and paste): 3KRAMntM9bwp96aTN4QbBZyc3LtPLQNYbS

Editor's note: *I wasn't aware we had any databases, please let us know where you post them!*

Response to 'WIFI Geolocation Concern' by nonattribution

When I finally read that article a month or so ago it helped explain a mystery that I have been trying to solve.

I subscribe to Cox Cable residential broadband and use a cox-provided cable modem/router/Wi-Fi AP. There is a "CoxWiFi" program where all cox modems can be used as Wi-Fi access points by all other Cox customers. But that option can be turned off in each user's Cox account. Also, there is the normal way to turn off the Wi-Fi networks on the cox-provided modem/router - in the modem web interface. However, even if both of these are turned off, the modem continues to broadcast a "hidden" Wi-Fi SSIDs on several channels and bands. That is - even if you turn off wireless networks on your cox modem it will still operate as a Wi-Fi node with a hidden SSID. The radios seem to be operating as WPA and WPA2 access points with WPS turned off. The only way that I can get the modem to not operate as a Wi-Fi radio is to unplug it. Many Cox modems have these hidden networks operating - and you can find them on Wifile or just by 'stumbling' around in a Cox coverage area. But I believe that Privacy Mike has provided the reason for their existence. They must be continually collecting information about other wireless networks within range. This could also explain why most ISP-provided Wi-Fi Access Point modems all seem to clump on the same channels even when auto-select channel is turned on. I will continue to do research on this, I just wanted to send a quick note as well as my kudos to everyone involved in creating the magazine.

Amateur Radio Privacy by Lucky225, WA6VPS

In the last issue someone asked for tips about privacy with the FCC

database. There's not much you can do if you ALREADY have a ham radio license as your name and address are already public in the database. That said, the FCC does allow common law names and PO BOX/CMRA mailing addresses as you pointed out in your response. There's also nothing illegal about having 2 separate Federal Registration Numbers (FRNs) which is how one typically identifies unique individuals on the FCC's ULS. So if you already have a ham radio license, the only way to make yourself private it is to voluntarily cancel your existing ham radio license, get a new FRN with a common law name in an alias and new mailing address, retake the ham radio test to get the license in the new name, you'll have to work with a VE team on a VEC that is friendly to common law names - there are some out there but I won't publish that here, the VE team will accept an affidavit in your real and common law name along with ID in your real name for the test. There is at least one individual I know of who goes by Log Killer (W2LOG) that only has that common law name and his PO BOX in the FCC database, there is no other link to their real name and/or home address. More info available here: <https://commonlaw.name/fcc.html>. ■

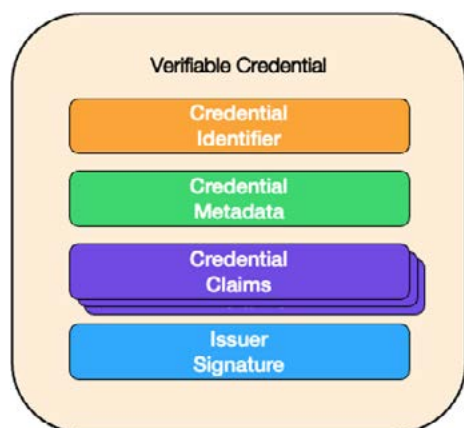
VERIFIABLE CREDENTIALS: THE KILLER FEATURE OF DECENTRALIZED IDENTITY

By Dr. Paul Ashley of Anonymome Labs

I've been exploring decentralized identity in Unredacted ([Issue 2](#) and [Issue 4](#)) so we can better understand this new technology that's giving users greater control over their personal data and identity. This issue, I go straight to decentralized identity's killer feature: verifiable credentials (VCs). What makes VCs the standout? Simple: VCs are what will make decentralized identity ubiquitous on the internet in the next decade.

What are VCs?

VCs are cryptographically protected and privacy-respecting digital documents that convey information about a user. [1] Trusted identity providers (called issuers) create these digital documents. Any physical card or document that a person can carry (e.g. in a wallet) could be replaced with a digital VC—think: digital driver license, digital passport, digital health card, digital travel visa, or even something as mundane as a digital gym membership card or a digital library card.



VC Structure

Every credential has an identifier and some metadata but, most importantly, it also has the claims or attributes the issuer is asserting about the holder (user). The issuer digitally signs the credential so verifiers receiving proofs based on the credential can confirm any credential information that is asserted plus the credential's authenticity.

Decentralized identity-based VCs are designed to be privacy preserving. The holder (user) maintains absolute control over which elements of their personal information (contained within the credential) they choose to provide. This is very different from physical credentials (e.g. a driver license), where the verifier can always see everything contained within the credential the user presents. Another key benefit of VCs is that the verifier can independently verify them without any communication with the credential's issuer, which ensures issuers cannot track when the holder uses their credentials.

How do VCs work?

You'll see here the parties involved in VCs, plus the data flow between those parties:



The VC process starts on the left with the issuer. An issuer is an entity (e.g. government or business) that wants to issue VCs. To do that, the issuer must first register some specification information on the blockchain (termed the verifiable data registry). Using the Hyperledger Indy network as an example, the issuer writes their decentralized identifier (DID), the credential schema [2] (which defines the elements of the VC), and the credential definition (linking the issuer DID and credential schema) to the blockchain.

Once the issuer has registered information on the blockchain, they can create and issue VCs. It begins with the holder (a user) and issuer forming a DIDComm connection (e.g. [Aries RFC 0160: Connection Protocol](#)). Over that connection

the issuer sends the VC (e.g. [Aries RFC 0036: Issue Credential Protocol 1.0](#)), which will be stored in the holder's wallet (e.g. [Aries RFC 0050: Wallets](#)).

At this point, the holder can present their information from the VC to service providers who require it. To do this, the holder establishes a DIDComm connection to the verifier and transfers the VC proof presentation (e.g. [Aries RFC 0037: Present Proof Protocol 1.0](#)). The verifier must connect to the blockchain to read the issuer DID (which includes their public key), credential definition, and credential schema, so they can verify the presentation proof.

The key privacy-preserving capabilities of this process include:

- The verifier can determine that the credential has not been altered and is authentic.
- Verification happens without the verifier communicating with the issuer.
- The holder (user) can select which

information from a credential they present to the verifier.

What are AnonCreds?

The [AnonCreds](#) or anonymous credentials specification is based on the open source verifiable credential implementation stemming from the [Hyperledger Indy](#) project. Extensive use of AnonCreds worldwide has made it a de facto standard for VCs.

Some important concepts around AnonCreds make it a very attractive solution for VCs, such as:

- Anonymity—Using unrevealed identifiers for holder-to-VC binding prevents correlation based on those identifiers. [3] This prevents colluding organizations from correlating user-specific identity information.
- Revocation—AnonCreds provides a revocation scheme that proves a presentation is based on credentials that the issuer has not revoked.

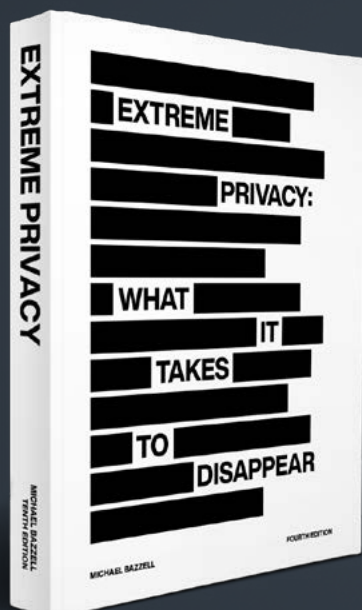
- Reduced PII exposure—An implementation of zero knowledge proofs (predicate proofs) helps eliminate the need to share specific PII (e.g. holders can prove they are over age 21 without disclosing their specific birth date).

The current AnonCreds specification matches the existing [Hyperledger Indy SDK \("libindy"\)](#) and [Indy Credential Exchange \("credx"\)](#) implementations, [4] but recently there was a proposal to make AnonCreds a standalone Hyperledger project, which will help it to grow with future enhanced capabilities.

One key factor to note is the use of the term proof presentation. This term describes the holder presenting one of three items to the verifier:

1. all of the data in the credential
2. part of the data in the credential (a partial disclosure)
3. a zero knowledge proof for some data in their credential.

Extreme Privacy Book



- ✓ Hardcover & Paperback
- ✓ New & Updated Content
- ✓ 500 Pages @ 8.5 x 11
- ✓ Our Full Playbook
- ✓ Supports Our Free Podcast

Order at IntelTechniques.com

Using ZKPs is a critical aspect of AnonCreds—that is, it is not the actual VC that is presented to the verifier, but rather a cryptographically derived proof that allows the data in the credential to be presented securely. As such, the user can keep more of their PII private while still answering questions such as, “Are you over 21?”, “Do you live in this country?”, or “Do you have a college degree?”

What are W3C VCs?

In addition to AnonCreds, the World Wide Web Consortium (W3C) has created the Verifiable Credentials Data Model v1.1. [5] This W3C recommendation is published and being used in government and commercial applications.

W3C VCs are also open source and provide the same basic functionality as AnonCreds—that is, this standard provides holder, issuer, subject, verifier, and verifiable data registry roles and supporting functionality. Some of the main target use cases [6] are:

- education—transcripts, test taking, transferring schools, online classes
- retail—address verification, adult beverages, fraud detection
- finance—Know Your Customer, money transfer, closing an account, trying a new service, create a bank account from home
- healthcare—prescriptions, pharmacy, insurance, traveling

illnesses, proving legal disability status

- professional credentials—find a doctor, quality training, job applications
- legal identity—driver license, immigration, air travel, refugee status
- intelligent devices—manufacturing, delivery, autonomous.

The W3C VCs standard also supports ZKPs, [7] but not all W3C VCs support being asserted as ZKP responses. The choice of whether to enable this capability is left up to the credential issuer. In order for a holder to assert a ZKP response, they must use a credential that has been created to allow for this purpose. Using W3C VCs for ZKPs requires the issuer to do two things:

1. Add a proof property to the VC.
2. Where they use a credential definition, also define it in the credential schema property.

So long as those two requirements are met, W3C VCs can be asserted in a zero knowledge fashion, as we covered.

AnonCreds and W3C VCs have a lot of similarities and some key distinctions, but that’s a topic for another issue. The main point is that both standards describe great implementations of VCs and mainstream platforms will be using both for the foreseeable future. ■

[1] This is the most common case. It is also possible for other scenarios such as the user issuing a credential related to an organization.

[2] In the future it may be uncommon for issuers to write their own schemas. Instead a standards body could write the schemas and issuers would only write credential definitions.

[3] [This paper by Kaliya Young](#) challenges the notion of “link secrets” as a viable alternative to including the credential subject information. This opinion is in turn refuted by [this paper by Daniel Hardman](#).

[4] [It is also argued in the paper by Kaliya Young](#) that not having a mature specification is a weakness not allowing sufficient analysis by the industry and it also lacks a standard for interoperability testing.

[5] Verifiable Credentials Data Model v1.1, World Wide Web Consortium, 3 March 2022, <https://www.w3.org/TR/vc-data-model/>

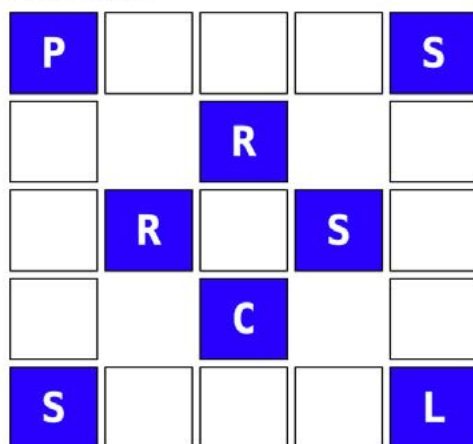
[6] Verifiable Credentials Use Cases, World Wide Web Consortium, 24 September 2019, <https://www.w3.org/TR/vc-use-cases/>

[7] Verifiable Credentials Data Model v1.1, World Wide Web Consortium, 3 March 2022, <https://www.w3.org/TR/vc-data-model/#zero-knowledge-proofs>

PRIVACY-THEMED PUZZLES

Security Word Puzzle #3

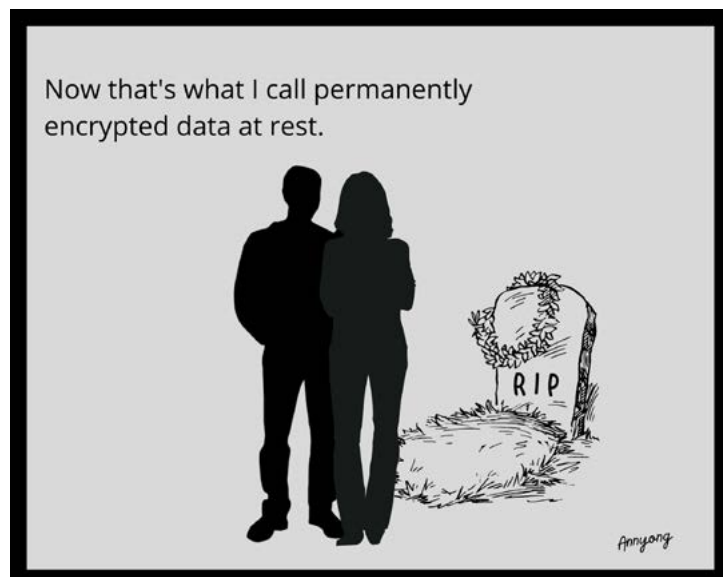
Michael J. Ross



The objective of this puzzle is to discover the six five-letter words — all related to computer and network security — that fit in the above puzzle. Three of the words are horizontal and the other three are vertical, with overlap of some shared letters. Several letters have already been added to the puzzle to help you start. Here are the remaining letters needed to complete the puzzle:



The solution to the previous security word puzzle consists of the following six words (three horizontal and three vertical): ASSET, TEAMS, RISKS, ACTOR, SCAMS, TESTS.



FINAL THOUGHTS

By Michael Bazzell

I again thank everyone involved in getting this issue published. I also announce yet another release schedule. This issue felt somewhat rushed, which I blame on the holiday season. I have decided that all future issues of UNREDACTED will be released based on content, and not a scheduled date. Once we have enough quality content to satisfy an entire issue, we will release it. Hopefully, that keeps us within the quarterly release schedule (or sooner). However, I am willing to take more time and publish whenever the issue feels “done”. The pressure is now on you. What will you submit? Will we have a new issue ready to go by April? I look forward to what you create.

MB ■

AFFILIATE LINKS

If you would like to support this free publication, please consider using the following affiliate links. If you plan to purchase any of the items below, or other items from the vendor (such as Amazon), the following links provide a small financial contribution to us without costing you anything extra. We see nothing about you or your order.

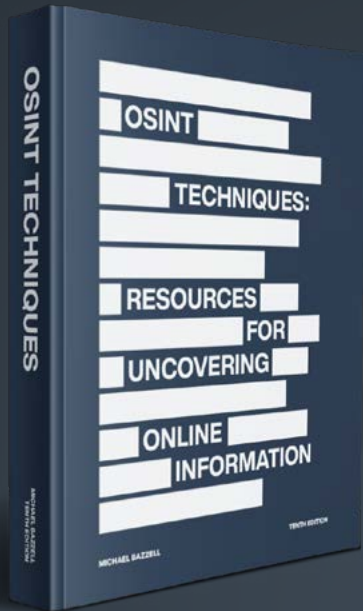
Extreme Privacy Book (Amazon): <https://amzn.to/3D6aiXp>

OSINT Book (Amazon): <https://amzn.to/3zoMZpZ>

ProtonVPN VPN Service: https://go.getproton.me/aff_c?offer_id=26&aff_id=1519

ProtonMail Encrypted Email: https://go.getproton.me/aff_c?offer_id=7&aff_id=1519

New 2023 OSINT Book



- ✓ Hardcover & Paperback
- ✓ New & Updated Content
- ✓ 550 Pages @ 8.5 x 11
- ✓ Our Full OSINT Playbook
- ✓ Supports Our Free Podcast

Order at IntelTechniques.com

OSINT & Privacy Video Training

100+ Hours of Video Training | Optional OSIP Certification

Register at IntelTechniques.net

