Sun City Computer Club

Cyber Security SIG
June 6, 2024

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above
- Wake Words

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

New Leader???

- SIG Leader replacement
- Take over
  - Inclusion Zoom & Recording
  - Training, Counsel
  - Summers are Important
- Leader(s)???
- Contributors

- Chrome Version 125.0.6422.142 (Official Build) (64-bit)
- Edge Version 125.0.2535.85 (Official build) (64-bit)
- Firefox Version 126.0.1
- Safari version 17.5 (19618.2.12.11.6)
- Brave Version 1.66.118 Chromium: 125.0.6422.147
- Vivaldi Version 6.7.3329.39
- DuckDuckGo Version 0.8.3.1
- Arc Version 1.5.0

Browser Versions

- Blank html or htm attachments
- Scanned Remittance Advice

REALLY DON'T CLICK

Current Issues

- https://www.kxan.com/news/crime/georgetown-woman-defrauded-of-300k-man-federally-charged-facing-3-counts/
- NSA Advice Switch off phone 1/week
- Google Search

  AI Overviews, Simplified Answers, Multi-step reasoning
  Plan Ahead 3-day meal plan
  Video search "Why CD player rejects disks?"
  AI-organized search page
  Korean recipes not too spicy, less than hour to prepare
- Ashley Madison 2015 data breach 40 million
  Now 85 million
  $500,000 reward – unclaimed
- Google News outage May 31, 2024 8:00 ET -> 10:30 ET

US based Internet Routers destroyed

- A mid-west telecommunications company
- 600,000 +
- October 25-27
- Common methods
- Windstream?
- Malicious firmware update
- Deleted portions of operating code

Current Issues

- Fake download sites PuTTY WinSCP
  putty.org, wnscp.net

- BreachForums site seized again
  Un seized again
- SS7 protocol vulnerabilities
  FCC request public comment CISA member response
- Security updates:
  Microsoft, Apple, Adobe, Cisco, Google, VMware, …
- Free Credit Monitoring post breach
  You know that already Notification after the fact
  Way after the fact

Current Issues

- North Korea telework fraud
  US national with dozens of laptops in residence
- Slack messages used for AI training
  2023 terms of service
- Jamacia Bureau of Standards ransomware
  Jamacia state-owned oil refinery December
  Jamacia Financial Services Commission September
- US Intelligence warned of 2020 election deep fakes
  + 4 years of AI improvements visual & audio
- CSC ServiceWorks Internet connected laundry machines
- Android on-device eves dropper - scam avoidance
  "transfer the money" what could go wrong?
- Linux kernel infrastructure infected 2009
  Still

Current Issues

- Helsinki data breach
  education & training departments
  students & guardians
  city employees
  Patch to known vulnerabilities not in time
- Australian prescription company MediSecure
  Australian Medibank data breach 2022
- Dell data breach 50 million
  Notification to Ireland data protection authority
  EU residents GDPR 4% global annual revenue fine
- WebTA data breach 2,429,175
  Full name, DoB, SSN, insurance information
  April, 2023 Notification 2 yrs Identity theft monitoring

Current Issues

- Microsoft Copilot Plus PC
  Recall
  Local tool
  search and retrieve content you've interacted with
  Opt-in required NPU T0 TOPS
- AI has read everything, needs more data
  AI generated data to train AI?
- DocuSign credentials
- Foxit PDF Reader Malware delivery
- American Library Association Bill of Rights
  Parents view child's library access
  Audio Books with ads services
  Privacy restrictions or no
- Google Cloud "Unprecedented event"
  Customer account AND BACKUPS

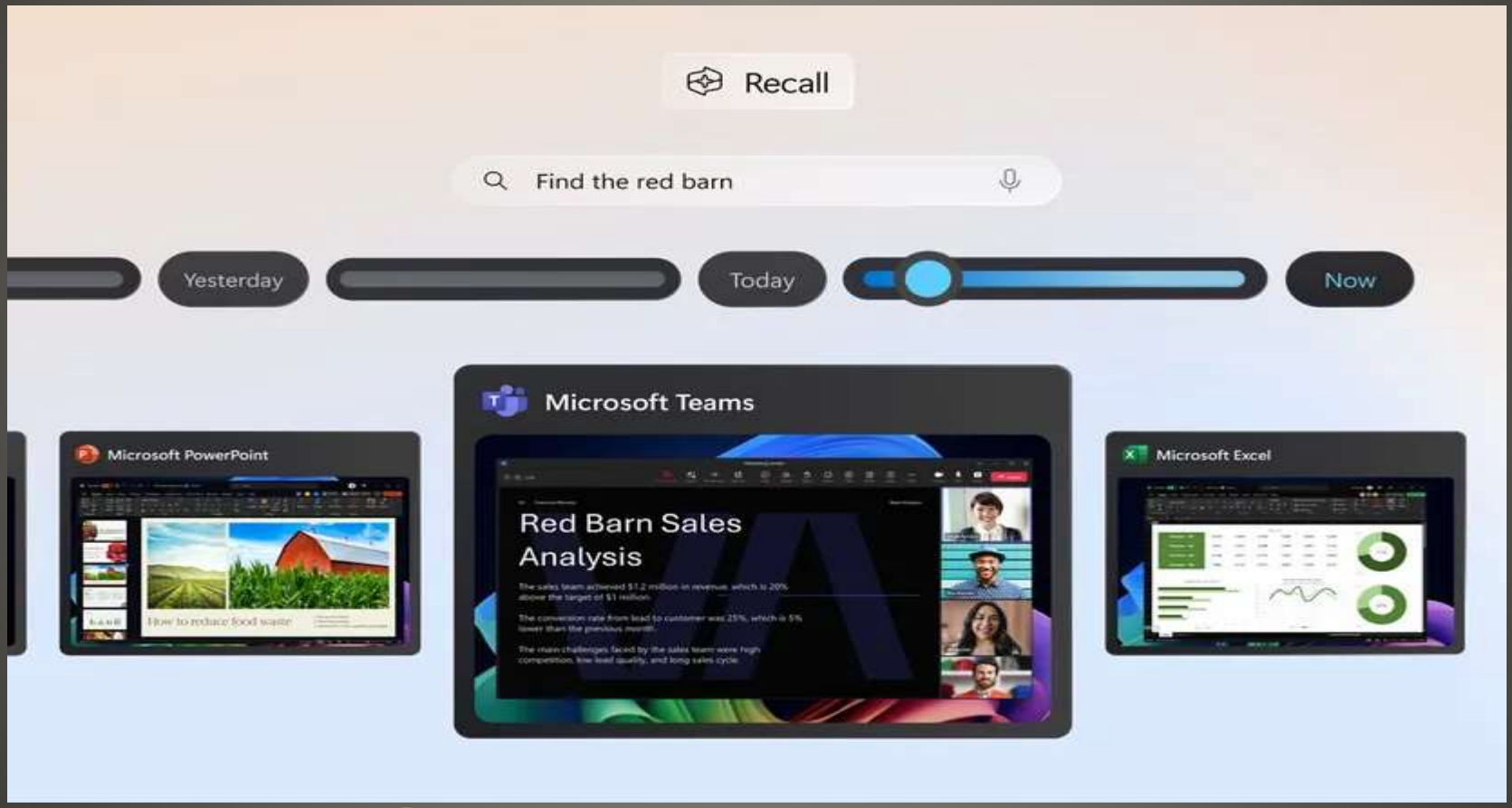
Microsoft Recall

- Microsoft Windows 11 Copilot+ laptop PCs
- Content you have viewed on your device
- Language aware searches 160 languages
- Text-to-Text
- Linux command history Windows 10 Timeline 2021
- AI + Machine Learning

==========

Copilot+ with advanced processing capabilities
Active images of screen every few seconds
Encrypted and saved to hard drive 50GB available
Scroll through snapshots -> Select -> Interact
Helpful <-> Harmful
Recall Settings Control
Edge InPrivate sessions DRM protections
BUT no content moderation “Show Password” Account Numbers

- Encrypted – Associated profile - local hard disk
- Videos -> transcribed & translated speech



Microsoft Recall

Microsoft Recall

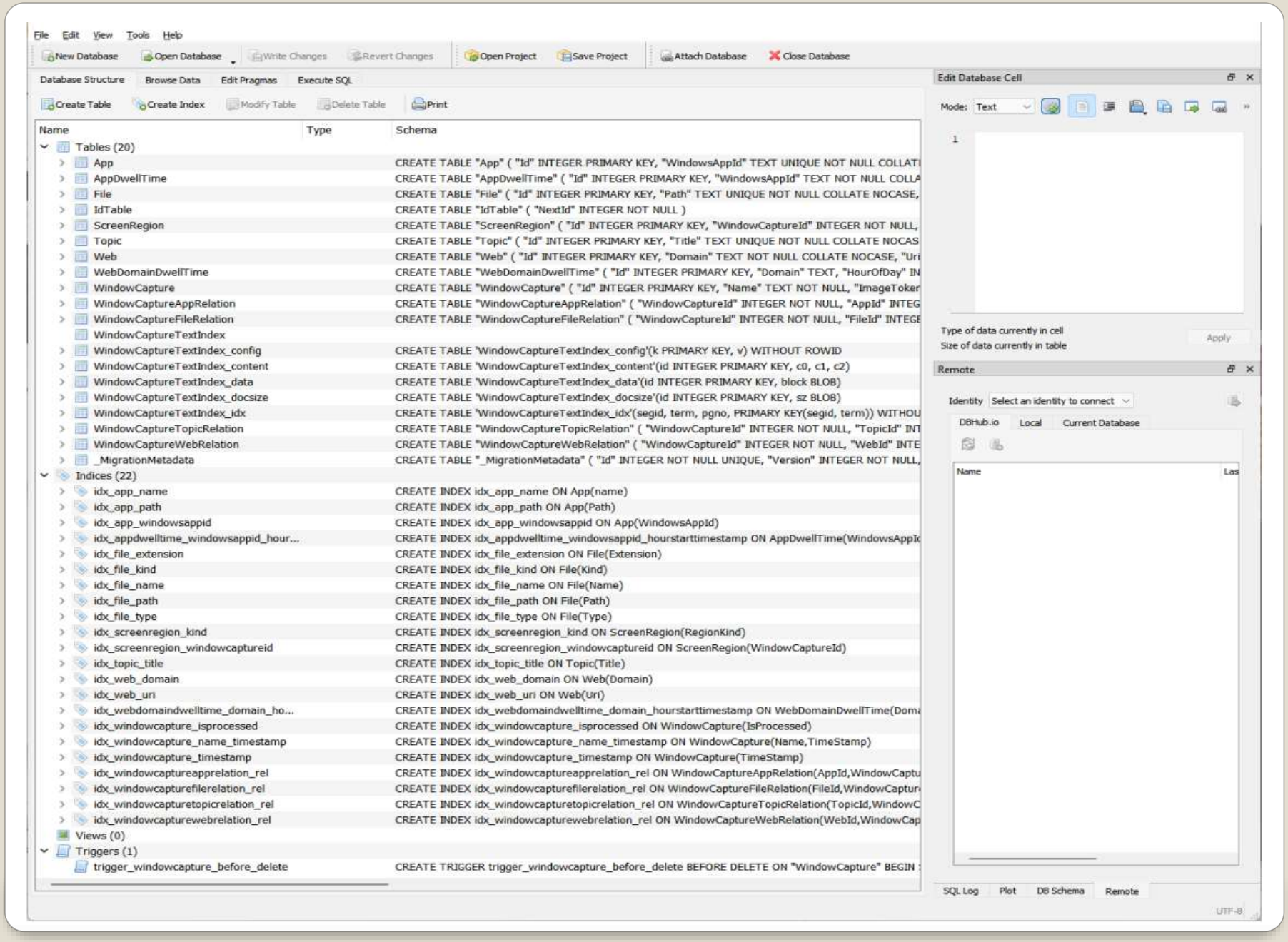
- End-to-End encrypted messages GOT IT
- Disappearing messages GOT It
- Grandma got run over by a reindeer GOT IT
- Help Center “Did you agree to this popup?”
  “No” Turn screen slowly toward client
- If Recall can search …..
- TotalRecall
- VMs
- Off by default?

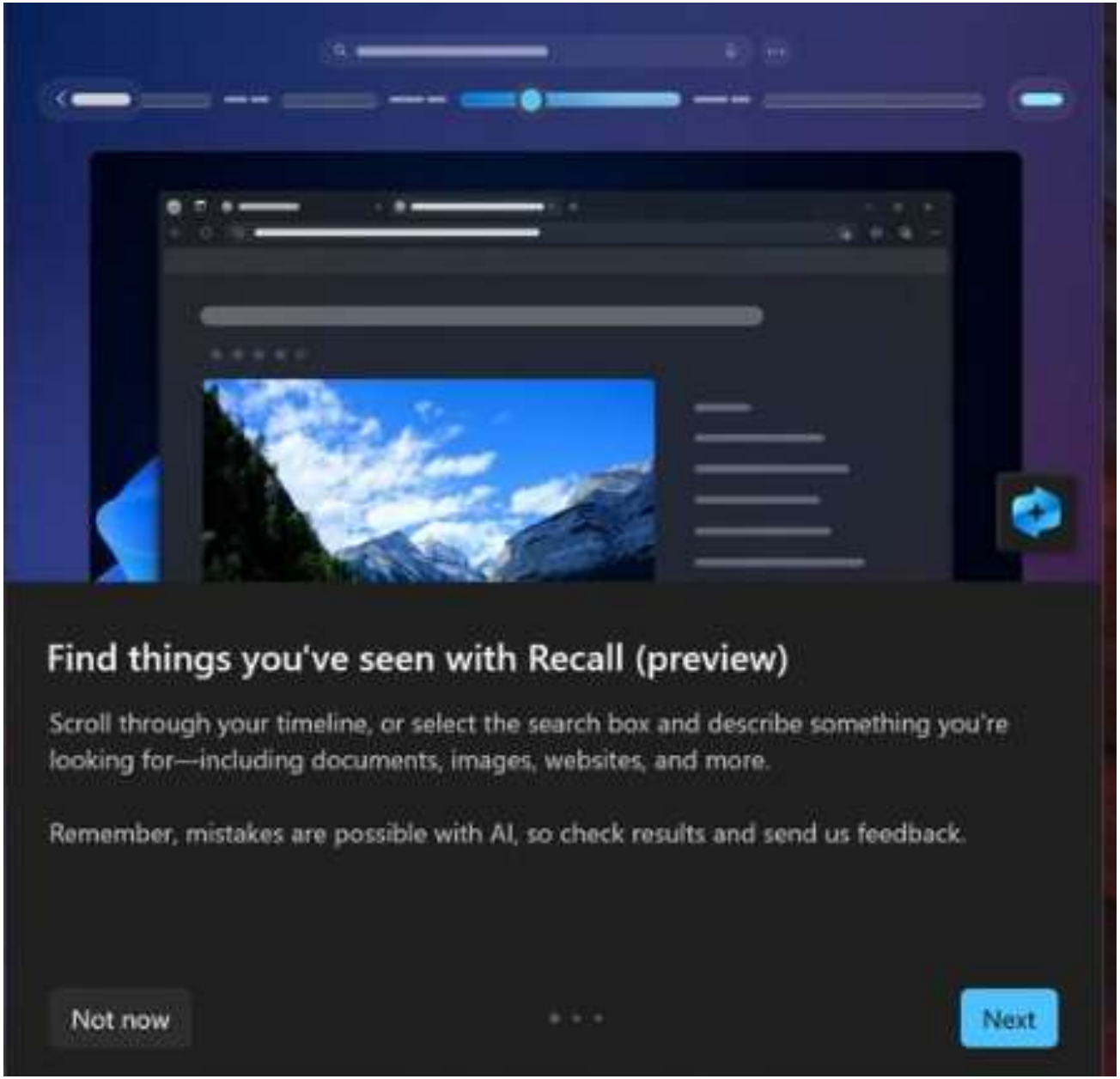
Recall

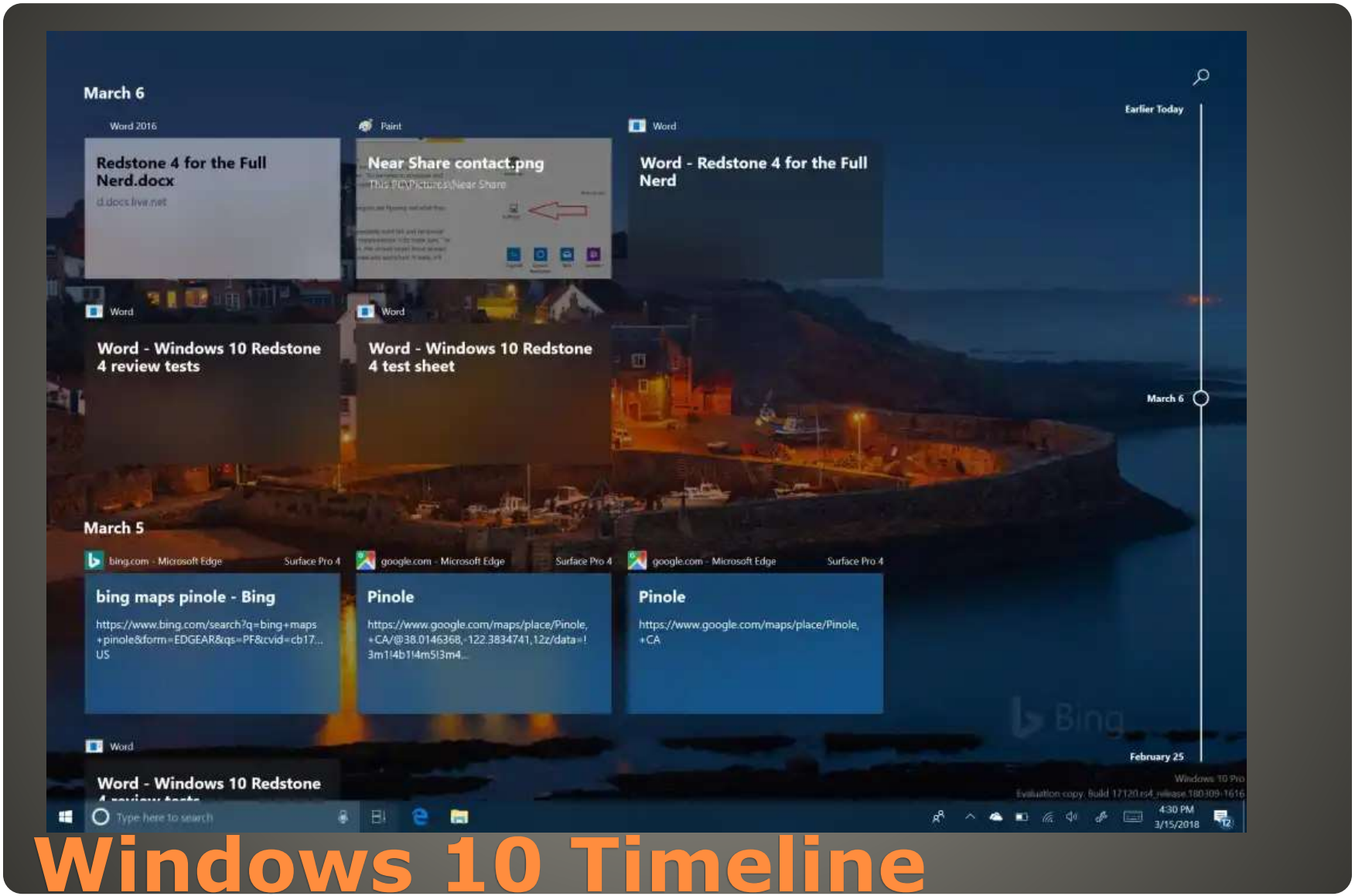
- Every few seconds screenshot
- Screenshot -> Azure AI OCR > SQLite
- SYSTEM rights NOT need
- Screenshots vs snapshots
- HIGH compression / large storage
- Any/everything you've seen/done on your PC available to AI

- Flawless Total Recall

- OpenRecall Open Source Windows, macOS, Linux,


File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Save Project
Attach Database
Close Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Create Table
Create Index
Modify Table
Delete Table
Print
Name
Type
Schema
Tables (20)
App
CREATE TABLE "App" ("Id" INTEGER PRIMARY KEY, "WindowsAppId" TEXT UNIQUE NOT NULL COLLATI
AppDwellTime
CREATE TABLE "AppDwellTime" ("Id" INTEGER PRIMARY KEY, "WindowsAppId" TEXT NOT NULL COLLA
File
CREATE TABLE "File" ("Id" INTEGER PRIMARY KEY, "Path" TEXT UNIQUE NOT NULL COLLATE NOCASE,
IdTable
CREATE TABLE "IdTable" ("NextId" INTEGER NOT NULL)
ScreenRegion
CREATE TABLE "ScreenRegion" ("Id" INTEGER PRIMARY KEY, "WindowCaptureId" INTEGER NOT NULL,
Topic
CREATE TABLE "Topic" ("Id" INTEGER PRIMARY KEY, "Title" TEXT UNIQUE NOT NULL COLLATE NOCAS
Web
CREATE TABLE "Web" ("Id" INTEGER PRIMARY KEY, "Domain" TEXT NOT NULL COLLATE NOCASE, "Uri
WebDomainDwellTime
CREATE TABLE "WebDomainDwellTime" ("Id" INTEGER PRIMARY KEY, "Domain" TEXT, "HourOfDay" IN
WindowCapture
CREATE TABLE "WindowCapture" ("Id" INTEGER PRIMARY KEY, "Name" TEXT NOT NULL, "ImageToker
WindowCaptureAppRelation
CREATE TABLE "WindowCaptureAppRelation" ("WindowCaptureId" INTEGER NOT NULL, "AppId" INTEG
WindowCaptureFileRelation
CREATE TABLE "WindowCaptureFileRelation" ("WindowCaptureId" INTEGER NOT NULL, "FileId" INTEGE
WindowCaptureTextIndex
WindowCaptureTextIndex_config
CREATE TABLE 'WindowCaptureTextIndex_config'(k PRIMARY KEY, v) WITHOUT ROWID
WindowCaptureTextIndex_content
CREATE TABLE 'WindowCaptureTextIndex_content'(id INTEGER PRIMARY KEY, c0, c1, c2)
WindowCaptureTextIndex_data
CREATE TABLE 'WindowCaptureTextIndex_data'(id INTEGER PRIMARY KEY, block BLOB)
WindowCaptureTextIndex_docsize
CREATE TABLE 'WindowCaptureTextIndex_docsize'(id INTEGER PRIMARY KEY, sz BLOB)
WindowCaptureTextIndex_idx
CREATE TABLE 'WindowCaptureTextIndex_idx'(segid, term, pgno, PRIMARY KEY(segid, term)) WITHOU
WindowCaptureTopicRelation
CREATE TABLE "WindowCaptureTopicRelation" ("WindowCaptureId" INTEGER NOT NULL, "TopicId" INT
WindowCaptureWebRelation
CREATE TABLE "WindowCaptureWebRelation" ("WindowCaptureId" INTEGER NOT NULL, "WebId" INTE
_MigrationMetadata
CREATE TABLE "_MigrationMetadata" ("Id" INTEGER NOT NULL UNIQUE, "Version" INTEGER NOT NULL,
Indices (22)
idx_app_name
CREATE INDEX idx_app_name ON App(name)
idx_app_path
CREATE INDEX idx_app_path ON App(Path)
idx_app_windowsappid
CREATE INDEX idx_app_windowsappid ON App(WindowsAppId)
idx_appdwelltime_windowsappid_hour...
CREATE INDEX idx_appdwelltime_windowsappid_hourstarttimestamp ON AppDwellTime(WindowsAppId
idx_file_extension
CREATE INDEX idx_file_extension ON File(Extension)
idx_file_kind
CREATE INDEX idx_file_kind ON File(Kind)
idx_file_name
CREATE INDEX idx_file_name ON File(Name)
idx_file_path
CREATE INDEX idx_file_path ON File(Path)
idx_file_type
CREATE INDEX idx_file_type ON File(Type)
idx_screenregion_kind
CREATE INDEX idx_screenregion_kind ON ScreenRegion(RegionKind)
idx_screenregion_windowcaptureid
CREATE INDEX idx_screenregion_windowcaptureid ON ScreenRegion(WindowCaptureId)
idx_topic_title
CREATE INDEX idx_topic_title ON Topic(Title)
idx_web_domain
CREATE INDEX idx_web_domain ON Web(Domain)
idx_web_uri
CREATE INDEX idx_web_uri ON Web(Uri)
idx_webdomaindwelltime_domain_ho...
CREATE INDEX idx_webdomaindwelltime_domain_hourstarttimestamp ON WebDomainDwellTime(Doma
idx_windowcapture_isprocessed
CREATE INDEX idx_windowcapture_isprocessed ON WindowCapture(IsProcessed)
idx_windowcapture_name_timestamp
CREATE INDEX idx_windowcapture_name_timestamp ON WindowCapture(Name,TimeStamp)
idx_windowcapture_timestamp
CREATE INDEX idx_windowcapture_timestamp ON WindowCapture(TimeStamp)
idx_windowcaptureapprelation_rel
CREATE INDEX idx_windowcaptureapprelation_rel ON WindowCaptureAppRelation(AppId,WindowCaptu
idx_windowcapturefilerelation_rel
CREATE INDEX idx_windowcapturefilerelation_rel ON WindowCaptureFileRelation(FileId,WindowCaptur
idx_windowcapturetopicrelation_rel
CREATE INDEX idx_windowcapturetopicrelation_rel ON WindowCaptureTopicRelation(TopicId,WindowC
idx_windowcapturewebrelation_rel
CREATE INDEX idx_windowcapturewebrelation_rel ON WindowCaptureWebRelation(WebId,WindowCap
Views (0)
Triggers (1)
trigger_windowcapture_before_delete
CREATE TRIGGER trigger_windowcapture_before_delete BEFORE DELETE ON "WindowCapture" BEGIN
Edit Database Cell
Mode: Text
1
Type of data currently in cell
Size of data currently in table
Apply
Remote
Identity
Select an identity to connect
DBHub.io
Local
Current Database
Name
Las
SQL Log
Plot
DB Schema
Remote
UTF-8


Find things you've seen with Recall (preview)
Scroll through your timeline, or select the search box and describe something you're looking for—including documents, images, websites, and more.
Remember, mistakes are possible with AI, so check results and send us feedback.
Not now
Next



Windows 10 Timeline

Current Issues

- AT&T AST SpaceMobile
- Russian hackers Lunar malware
  European government's diplomatic institutions
- EPA enforcement alert 20-May-2024
  70% failed compliance
  Default passwords
  SCADA technicians
  PLCs
- Fluent Bit vulnerability
  logging & metrics solution Very Popular
  Cloud, Kubernetes, AWS, Azure, CrowdStrike, Cisco, …
  Heap buffer overflow CVE-2024-4323
- Android alternatives: /e/OS, LineageOS, Micro G

ARPA-H UPGRADE

- US Advanced Research Projects Agency for Health
  ARPA-H
  $50m
  Technology to automate process securing hospital IT
  Universal PatchinG and Remediation for Autonomous Defense
  Create vulnerability mitigation software platform
  Develop twin of hospital environment/equipment
  Auto-detect flaws
  Auto develop custom defenses
  What Could Possible Go Wrong?
  Health and Human Services *voluntary* healthcare specific goals

WPS

- WPS Wi-Fi Positioning Systems
  Your mobile device
  Many MAC & BSSIDs & signal strength
  positioning without GPS more accurate
  Google 2 or more Apple up to 400 choose 8
  Google WPS shares with device
  Apple WPS on device with supplied data
  Starlink terminals with Wi-Fi access point
  Position of troops with Starlink terminals
  Starlink now randomizing BSSID
  Apple WPS Gaza war data power loss

- BSSID add _nomap to network name
- No Apple device yeahbut someone close by does
- Tracking research
- Travel routers

Crowd-sourced Wi-Fi and cellular Location Services

If Location Services is on, your device will periodically send the geo-tagged locations of nearby Wi-Fi hotspots and cell towers to Apple to augment Apple's crowd-sourced database of Wi-Fi hotspot and cell tower locations. While you're in transit (for example, driving or walking) and Location Services is on, a GPS-enabled iPhone or iPad will also periodically send GPS locations, travel speed and direction, and barometric pressure information to Apple to be used for building up Apple's crowd-sourced road traffic, roadway, pedestrian walkway, and atmospheric correction databases. The crowd-sourced location data gathered by Apple is stored with encryption and doesn't personally identify you.

The owner of a Wi-Fi access point can opt it out of Apple's Location Services — which prevents its location from being sent to Apple to include in Apple's crowd-sourced location database — by changing the access point's SSID (name) to end with "_nomap." For example, "Access_Point" would be changed to "Access_Point_nomap."

The Internet Service Provider or Wi-Fi access point manufacturer can provide more information about changing the name of an access point.

WPS

JAVS Viewer backdoor

- Application update unknown threat actor
- Part of JAVS Suite 8
- Live feed Audio & Video
- Signed BUT not by Justice AV Solutions
  Vanguard Tech Limited

- Supply chain attack example

Current Issues

- Gift card – the other threat
  Target card issuing organizations
- Apple iDevice photos reappear
  How so?
  PhotoLibraryServices
  PLMModelMigrationActionRegistration_17000
  reindex old files on local filesystems
  Thus, not restored from iCloud storage
  Advanced Data Protection more iCloud data – photos
  Encryption key on your devices
  CAUTION: less ability to recover
  CAUTION: Deleted files/folders not really deleted
- AI can't/won't say "I don't know" thus hallucinate
  Add glue to pizza so cheese won't slide off
- Bing outage => Copilot, ChatGPT, DuckDuckGo
  WAIT, DuckDuckGo?
- ChatGPT outage 2:30 ET - 7:30 ET June 4
- Linux kernel vulnerability added to CISA KEV
  Known Exploited Vulnerabilities CVE-2024-1086
  Use after free netfilter:nf_tables

- Smart Driver 2.0
  Hard cornering, forward collision alerts, lane departure warnings, seatbelt reminders
- Data about car – GM
- Data about driver – Personal data
- Multiple drivers?
- What are hard braking & rapid acceleration events?
- Speeding over 80 mph (Texas 85 mph)
- LexisNexis GM, Kia Subaru, Mitsubishi
- Verisk Ford, Honda, Hyundai and millions of vehicles

- Request your report(s)
- LexisNexis
  https://consumer.risk.lexisnexis.com/consumer
- Verisk
  https://fcra.verisk.com/#/

UPDATE: Verisk response Postal Mail

GM

Current Issues

- pcTattletale Hotel check-in systems
  Info not just to attackers, whole Internet

- https://www.foxnews.com/tech/reclaim-your-privacy-by-disabling-your-cellphone-carriers-data-tracking

Cellular Providers tracking

T-Mobile

- T-Mobile
- User behavior profiling: T-Mobile analyzes personal data to predict user behaviors and preferences, which can influence future services and marketing strategies.
- Research support: The carrier shares data to aid public and scientific research initiatives, ensuring that personal identifiers are removed.
- App usage analysis: Tracks the frequency and duration of app usage to gather insights into user preferences and habits.
- Advertising personalization: This process collects information on app usage and demographic details to tailor advertisements more closely to the user's interests.

Verizon

- Verizon
- Network usage insights: Verizon uses data like web browsing and app usage to offer additional services or upgrades.
- Aggregate consumer insights: Combines user data with external data to generate insights into consumer behaviors and trends.
- Customized user experience: Verizon analyzes the websites and apps users engage with to create a more personalized service experience.
- Marketing optimization: Uses detailed user data to refine and personalize marketing efforts and service offerings.

AT&T

- AT&T
- Browsing and location tracking: AT&T collects detailed records of users' web browsing and location to customize ads and offers.
- Automated decision-making: They employ algorithms to use collected data to make automated decisions that affect the ads and content presented to the user.
- Demographic and viewing data: Gathers demographic information alongside viewing habits to better understand and segment their user base.
- Identity verification services: AT&T shares certain data with third parties to facilitate identity verification and fraud prevention measures.

Hey cellular carrier

T-Mobile

- Log into your T-Mobile account.
- Navigate to My Account, then click on Profile.
- Scroll to the bottom and select Privacy and Notifications, then Privacy Dashboard.
- Here, you can toggle off various options:Share data for public and scientific research: Prevents the use of your data for external research projects.Analytics and reporting: Stops the aggregation of your usage data for business reports.Advertising options: Limits personalized ads based on your app usage and other collected data.Profiling and automated decisions: Opt out of data usage for profiling purposes.Do not sell or share my personal information: Ensure your data is not sold or shared externally.
- Share data for public and scientific research: Prevents the use of your data for external research projects.
- Analytics and reporting: Stops the aggregation of your usage data for business reports.
- Advertising options: Limits personalized ads based on your app usage and other collected data.
- Profiling and automated decisions: Opt out of data usage for profiling purposes.
- Do not sell or share my personal information: Ensure your data is not sold or shared externally.
- Additionally, T-Mobile offers a separate app to limit data shared with third-party advertisers through the Magenta Advertising Platform.

Verizon

- Verizon
- To manage privacy settings on a Verizon device:

- Log into your Verizon account.
- Go to Account, then Account Overview and select Edit Profile and Settings.
- Choose Manage Privacy Settings.
- You can adjust the following: Customer Proprietary Network Info: Opt out to stop Verizon from using your data to market additional services. Business and Marketing Insights: Disable this to prevent the use of your data for creating consumer insights. Custom Experience and Custom Experience Plus: Opt out to stop personalized marketing based on your web and app usage.
- Customer Proprietary Network Info: Opt out to stop Verizon from using your data to market additional services.
- Business and Marketing Insights: Disable this to prevent the use of your data for creating consumer insights.
- Custom Experience and Custom Experience Plus: Opt out to stop personalized marketing based on your web and app usage.
- Resetting the Custom Experience settings will also stop Verizon from using previously collected browsing and location data.

AT&T

- AT&T
- To disable data tracking on an AT&T device:

- Log into your AT&T account.
- Navigate to Profile, then Privacy Choices.
- AT&T offers four main toggles you can turn off:Personalized Plus: Stops the use of your location and browsing data for personalized ads. Personalized: Disables automated decision-making using your data. Share or sell my personal information: This prevents AT&T from sharing your data for advertising purposes.
- Personalized Plus: Stops the use of your location and browsing data for personalized ads.
- Personalized: Disables automated decision-making using your data.
- Share or sell my personal information: This prevents AT&T from sharing your data for advertising purposes.
- It's recommended that identity verification be kept active for security purposes.

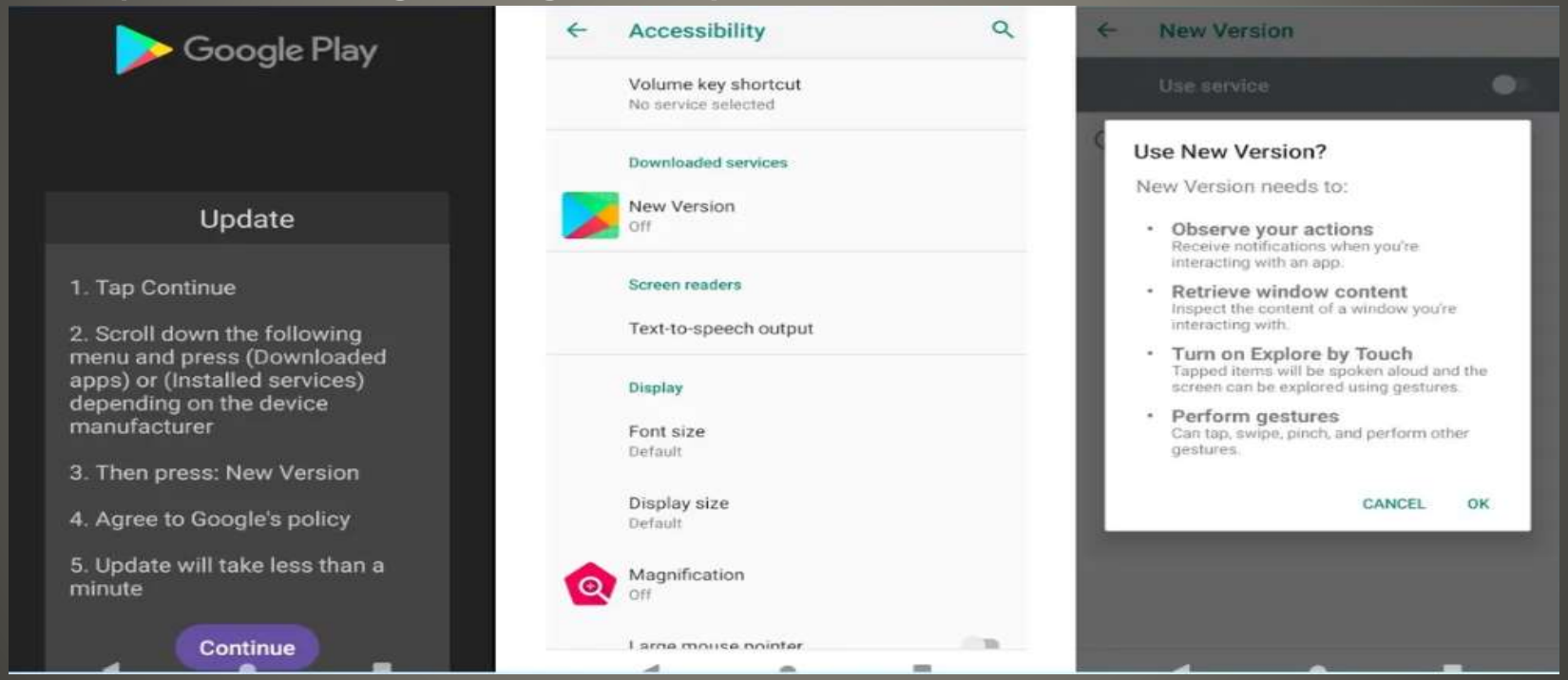
Current Issues

- Ultra Wide Band & Automotive key fobs
  Not Yet Improved
  Use PIN
  Tesla GPS – protection?
- Windows XP did not last long
  SQL Slammer and other scans still exists
  Korean elementary school
  How would ANY out-of-the-box fare?
- Bitlocker encrypts boot volume
  email address - no ransom notice
- BreachForums returns
- Corporate VPN attack – accounts with no MFA
- Internet Archive Wayback Machine under DDoS attack
- Ultrasonic fingerprint scanners to more devices
  Optical, Capacitive, Ultrasonic

Scam Alert

- "This is an urgent public service announcement."
- "You have won a free vacation!"
- "I need to verify your account details."
- "There's a problem with your payment."
- "Confirm your identity with your password."
- "This is your final warning."
- "You owe taxes and must pay immediately."
- "We've noticed suspicious activity on your account."
- "I'm calling from tech support."
- "Can you hear me?"
- Scams and Computer Safety SIG
- They contact you
- Problem or something of value
- Must act quickly
- Request personal information
- Money in advance, gift cards, P2P, wire transfer

- Fortinet SIEM vulnerability exploited
- Yet another NEW Android banking trojan
  Antidot
  Impersonating Google Play



Current Issues

Current Issues

- Sideloading on Android
  Google Play
  90 malicious apps on Google play
  Found and deleted
  5.5 million downloads
- Sav-Rx data breach
- YouTube ad blocker wars Mute Skip
  YouTube ToS, performance hiccup, Adblocker
- Law enforcement trolling hackers
  Reduce ability to scale
  LockBit
  Brand reputation & interpersonal relationships
  Leader not affected? Cooperating with law enforcement?
  Intelligence Advanced Research Projects Activity (Iarpa)

Current Issues

- Google 2500 leaked internal documents
  Yup, those are ours
  out-of-context, out-of-date, incomplete
  Search Engine Optimization
  Leaked on purpose?
  Regulatory requirements
- Mitre Corporation Rogue Virtual Machines
- Google “best fixed-term investment rates”

- Facewatch mistake

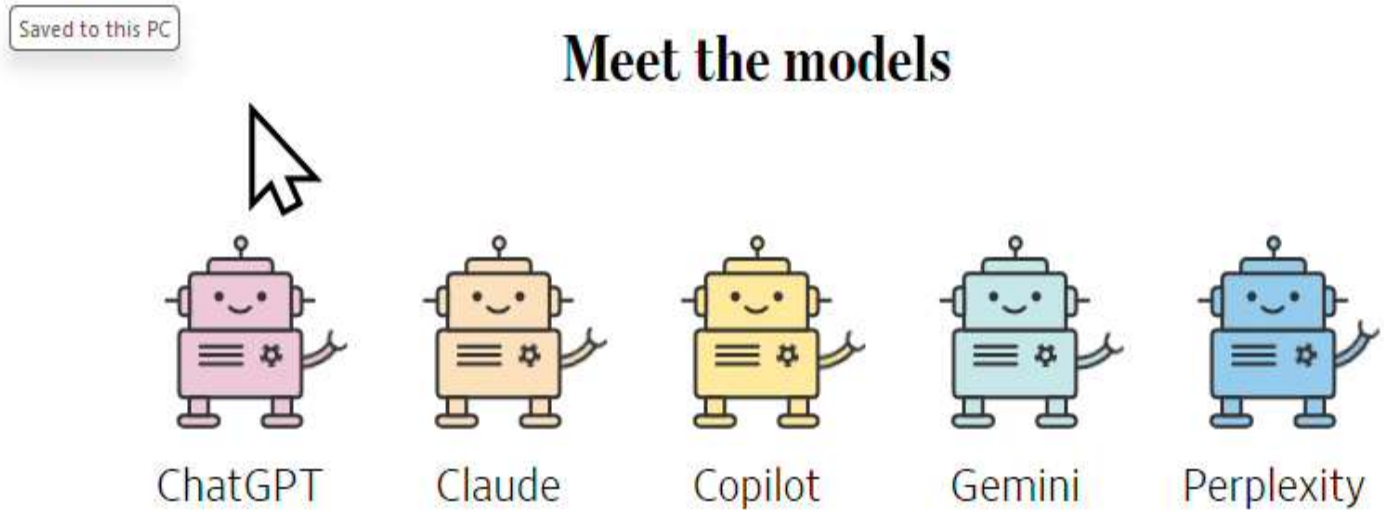
Bags searched, escorted from store, banned from all stores

Apology later

Facewatch


Live Facial
Recognition
In Operation
METROPOLITAN
POLICE

- Wall Street Journal Great AI Challenge



- Chat with Gemini (Chromebook Plus)
- Help Me Write (Chromebook Plus)
- Magic Editor for Photos
- AI backgrounds and wallpapers
- Game Dashboard
  keyboard input, record, capture, share
- Google Tasks in Quick Settings
- GIF recorder
- Google Chromebook Event

ChromeOS 125

- Nigerian prince
- Home title fraud
- Identity fraud
- Take control of Graceland mansion
- To sell A scam
- Ringleader

  Prey on dead, unsuspecting, elderly

"We figure out how to steal," the alleged thief said. "That's what we do."

Scams and Computer Safety SIG

Current Issues

- 11-year-old password for $3M crypto wallet
  Random number generator & parameters
  Great increase in value
  Frustrating if inability to access crypto wallet
- Christie's Auction House ransomware
  threats to release client details
  GDPR failure to disclose
- TP-Link C5400 gaming router RCE vulnerability
- 23-yearold - Incognito black market
  extorting that site's users
  legit cyber crime expert

"used his professional background and qualifications in the field"

- Hackers phish financial organizations
  Minesweeper clone
- Google to acquire HubSpot

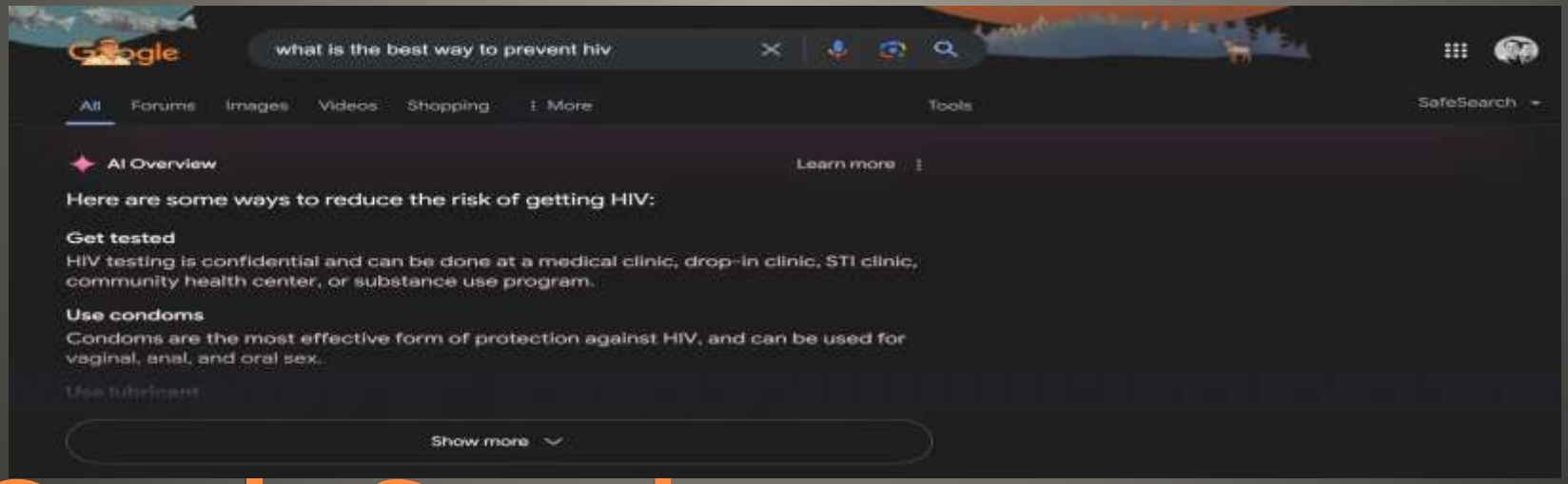
Current Issues

- 911 SS botnet taken down
- Ticketmaster data breach 560 million users
  Full name, home address, phone numbers, last 4 of credit and debit cards, card expiration dates, customer fraud data
  Just days after DoJ lawsuit monopolistic practices & behaviors
  Change Ticketmaster password ??
  Also, Santander Bank
  Claimed: Advance Auto Parts, Allstate, Anheuser-Busch, Mitsubishi, Neiman Marcus, Progressive, State Farm
- Google Wallet Advantages of each of your cards/methods
- WhatsApp warning
  Metadata who, when
  Complies with legal request for metadata
- WhatsApp account cloning
  Physical Access -> scan QR code
  Settings -> Linked Devices
- Google issues update Google TV and Android TV TV OS

Current Issues

- pcTattletale site defaced, archives leaked
  Wyndham hotels
  Site taken down
  Have I Been Pwned updated
- Telegram 361 million account credentials leaked
  Have I Been Pwned updated
- Cencora drug wholesaler data breach
  Full name, address, DoB, health diagnosis, prescriptions
- Microsoft Windows 11 24H2
  SMB file access
  SMB signing required Guest fallback disabled Windows Pro
  Guest No username/password
  Old NAS devices
- ChatGPT current Browse feature Ask current event question

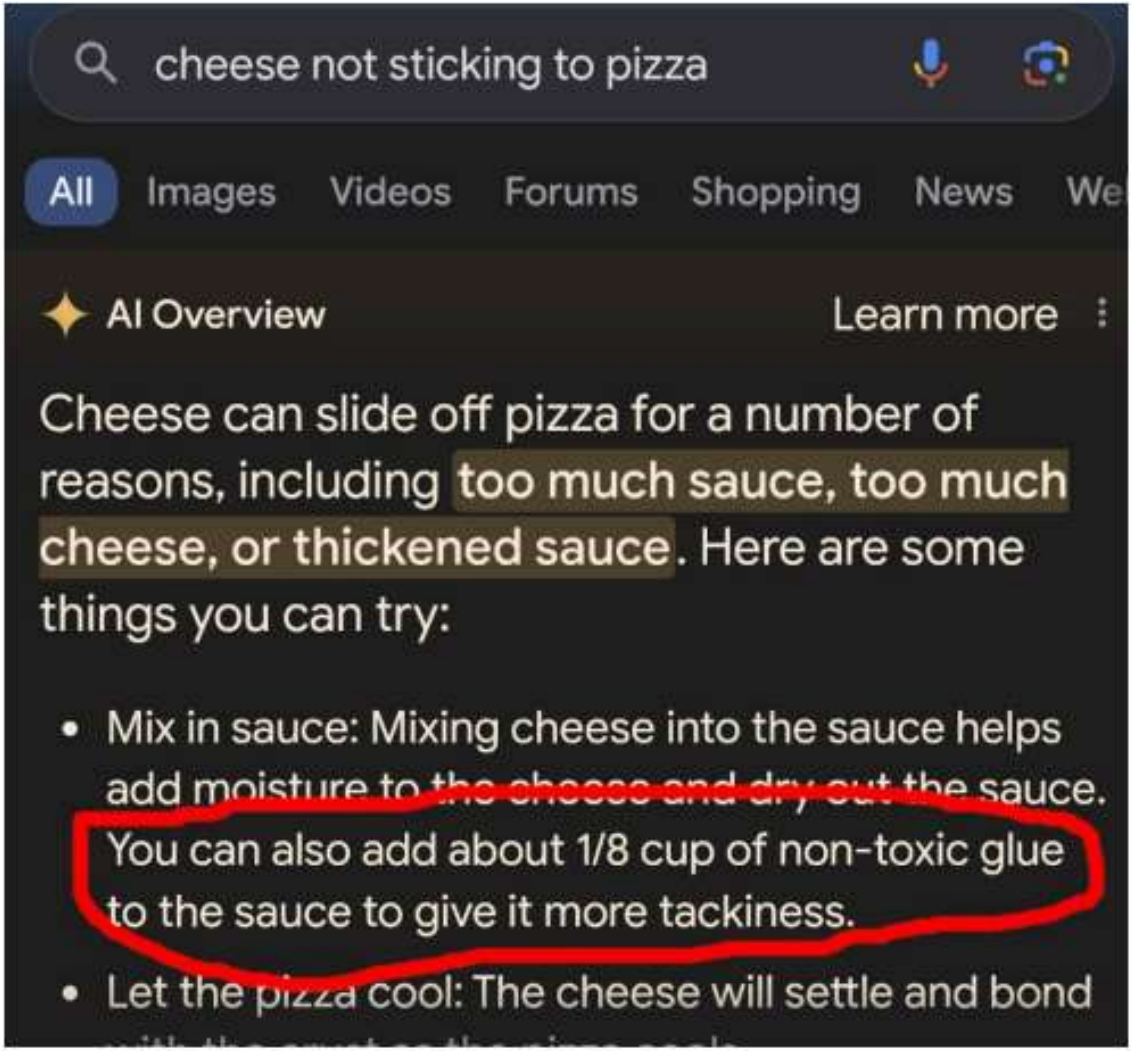
- HouseFresh
- Live by result, die by result
- Algorithm change
- AI
- Search -> Search and answer
- Search Engine Optimization
- Add reddit



Google Search

Current Issues

- Operation Endgame
  Law enforcement disrupts:
  IcedID, Smokeloader, Pikabot, Bumblebee
  SystemBC, Trickbot
- https://haveibeenpwned.com/
- LastPass to encrypt URLs stored in its vault
- Kaspersky free Linux standalone scanner
- Checkpoint VPN vulnerability
- CISA Apply all May Chrome updates or cease using Chrome
  4 zero-days and emergency updates in 10 days



Apparently, this latest AI "hallucination" is based upon an 11-year old Reddit posting which read *"To get the cheese to stick I recommend mixing about ⅛ cup of Elmer's glue in with the sauce. It'll give the source a little extra tackiness and your cheese sliding issue will go away. It'll also add a little unique flavor. I like Elmer's school glue, but any glue will work as long as it's non-toxic."*

Google AI Overview

- Add “udm=14”
- As with any answer
  Use your intelligence

https://udm14.com/

https://tenbluelinks.org/

Fit for Purpose

Google Chrome extension change

- Next week
- Manifest V2 -> Manifest V3
- Improve security, privacy, performance, trustworthiness
- Yeahbut V3 limits content filtering

  Fight Ads

  Proposed 2019

  uBlock Origin Lite V3

  uBlock Origin V2

- Many false Statements
- Shirt color change
- “The Kremlin has made spreading disinformation a core strategy for misleading people both inside Russia and beyond its borders,” he said. “It’s hard to think of a more convincing sign your decisions aren’t working out than having to resort to outright fakes to defend them to your own people, not to mention the rest of the world.”

US State Department Deep Fake

- Checkpoint appliance vulnerabilities
- Humane AI Pin owners “immediately stop using charging case:

Out of an abundance of caution, we are reaching out today to ask that you immediately stop using and charging your Charge Case Accessory due to an issue with certain battery cells for the Charge Case Accessory.

Upon receiving a single report of a charging issue while using a third-party USB-C cable and third-party power source, we identified a quality issue with the battery cell supplied by a third-party vendor used in your Charge Case Accessory.

Our investigation determined that the battery supplier was no longer meeting our quality standards and that there is a potential that certain battery cells supplied by this vendor may pose a fire safety risk. As a result, we immediately disqualified this battery vendor while we work to identify a new vendor to avoid such issues and maintain our high quality standards.

The issue identified is isolated only to certain battery cells used in the Charge Case Accessory and is not related to the Charge Case Accessory hardware design.

Importantly, Humane’s Ai Pin, its Battery Booster(s) and Charge Pad are not affected as the disqualified vendor does not supply batteries or any other components of those Humane products, and are safe for continued use.

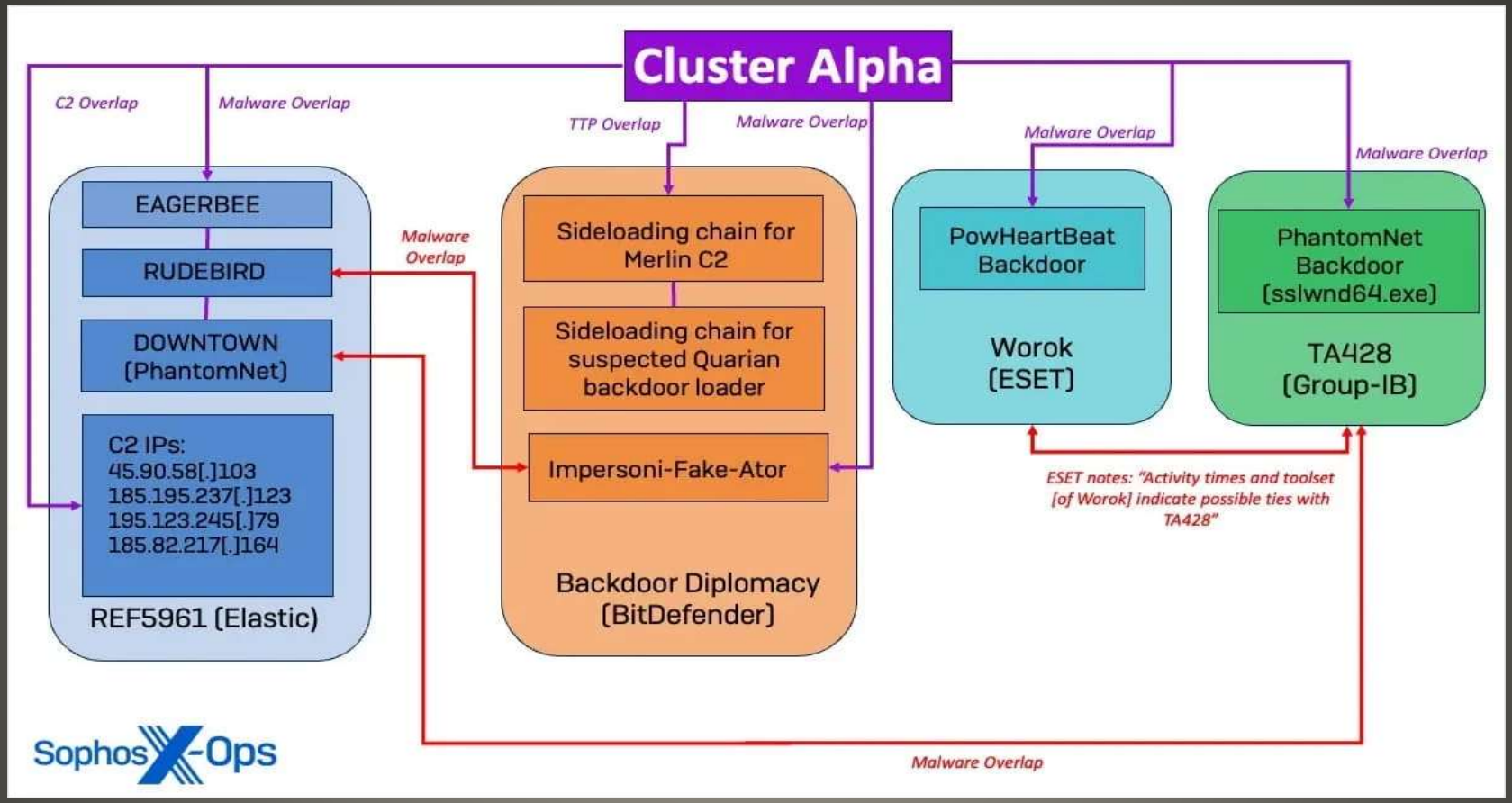
While we know this may cause an inconvenience to you, customer safety is our priority at Humane. We design Ai Pin and related accessories with safety top of mind, and rigorously test and certify them to applicable US and international safety standards.

We appreciate your understanding and will be providing you with two additional months free of the Humane subscription.

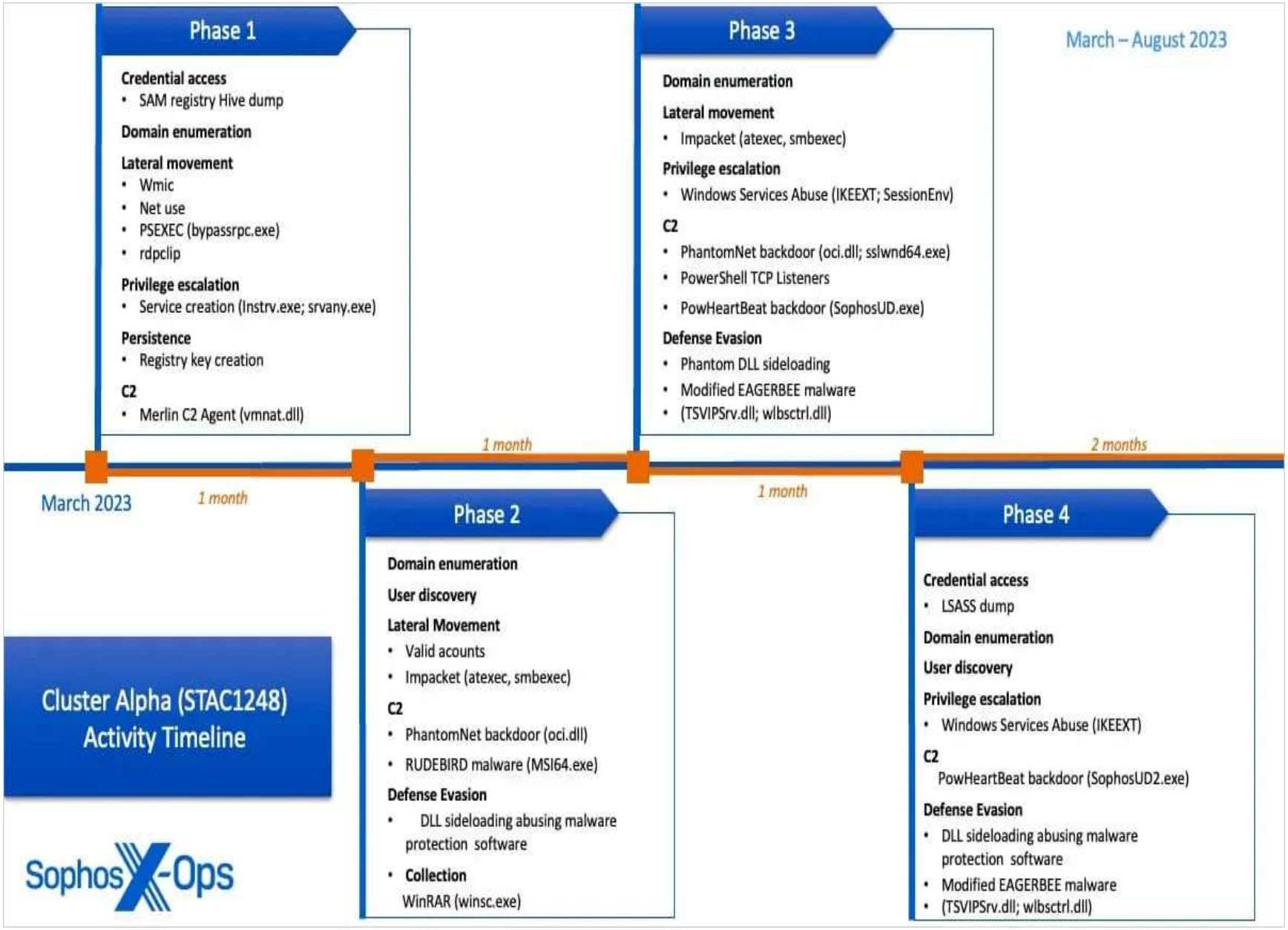
Rest assured we are committed to your safety and satisfaction and will share additional information when we have concluded our investigation.

The Humane Team

Current Issues



Chinese groups team up


Phase 1
Credential access
• SAM registry Hive dump
Domain enumeration
Lateral movement
• Wmic
• Net use
• PSEXEC (bypassrpc.exe)
• rdpclip
Privilege escalation
• Service creation (Instrv.exe; srvany.exe)
Persistence
• Registry key creation
C2
• Merlin C2 Agent (vmnat.dll)
Phase 3
Domain enumeration
Lateral movement
• Impacket (atexec, smbexec)
Privilege escalation
• Windows Services Abuse (IKEEXT; SessionEnv)
C2
• PhantomNet backdoor (oci.dll; sslwnd64.exe)
• PowerShell TCP Listeners
• PowHeartBeat backdoor (SophosUD.exe)
Defense Evasion
• Phantom DLL sideloading
• Modified EAGERBEE malware
• (TSVIPSrv.dll; wlbsctrl.dll)
March – August 2023
1 month
2 months
March 2023
1 month
1 month
Phase 2
Domain enumeration
User discovery
Lateral Movement
• Valid acounts
• Impacket (atexec, smbexec)
C2
• PhantomNet backdoor (oci.dll)
• RUDEBIRD malware (MSI64.exe)
Defense Evasion
• DLL sideloading abusing malware protection software
• Collection
WinRAR (winsc.exe)
Phase 4
Credential access
• LSASS dump
Domain enumeration
User discovery
Privilege escalation
• Windows Services Abuse (IKEEXT)
C2
PowHeartBeat backdoor (SophosUD2.exe)
Defense Evasion
• DLL sideloading abusing malware protection software
• Modified EAGERBEE malware
• (TSVIPSrv.dll; wlbsctrl.dll)
Cluster Alpha (STAC1248) Activity Timeline
SophosX-Ops


Heatmap of Threat Activity
Sophos X-Ops
Hour of the Day (UTC)
22:00
20:00
18:00
16:00
14:00
12:00
10:00
08:00
06:00
04:00
02:00
00:00
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Day of the Week
6 AM
4 AM
2 AM
12 AM
10 PM
8 PM
6 PM
4 PM
2 PM
12 PM
10 AM
8 AM
Time of Day (UTC+8)
80
60
40
20
0
Cluster Activity Gantt Chart by Day
Sophos X-Ops
Undetermined
Bravo
Alpha
Charlie
Mar 2023
Apr 2023
May 2023
Jun 2023
Jul 2023
Aug 2023
Sep 2023

Current Issues

- Tokyo dating app Tumbling birth rates
- Yet another Mac infostealer
- Russian criminals London hospitals
- Oral-B Alexa toothbrush -> AI toothbrush
- AT&T nationwide outage
- Enable Transparency Mode on AirPods
- New Apple devices with Thread radio capability

- Recovery Seminar
- https://vimeo.com/882272974?share=copy
- NOW, Your input, experiences, …

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com