stolen my phone number : 00201016029799 from vodafone attacker to hacking my facebook,google,github,gitlab,etc
stolen my phone number : 00201147766447 from etisalte attacker to hacking my facebook,google,github,gitlab,etc
https://github.com/gellanyhassan1/maadi_attacks
https://www.interpol.int/en/Contacts/Report-a-suspected-fraud-and-abuse-of-INTERPOL-s-name
I Pet Goat 2 Operation = Operation Olympic Games [victim : Elgilany Hassan Sayed , Ariel Koren , Hasan Fakhrizadeh]

Am So Sorry to Say the FBI.gov , HHS.gov , intezer.com , checkpoint.com dirty works about APT41_202308161700 INJ3CTOR3_Operation
https://cn.linkedin.com/in/fu-qiang-299a6343?trk=people-guest_people_search-card
https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-275a
https://www.huntandhackett.com/threats/countries/israel

Operation Olympic Games Started under the administration of George W. Bush in 2006, Olympic Games was accelerated under President Obama, who heeded Bush's advice to continue cyber attacks on the Iranian nuclear facility at Natanz. Bush believed that the strategy was the only way to prevent an Israeli conventional strike on Iranian nuclear facilities.
This attack was triggered by President Obama’s acceleration of “Code Olympic Games,” initially developed under the Bush Administration
https://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=1023&context=inthebalance
Andrew "Weev" Auernheimer, a hacker sentenced to three and a half years in prison for obtaining the personal data of more than 100,000 iPad owners from AT&T’s unsecured website is about to go free, after a ruling today that prosecutors were wrong to charge him in a state where none of his alleged crimes occurred.
Andrew "Weev" Auernheimer was in Arkansas during the time of the hack, his alleged co-conspirator was in California, and the servers that they accessed were physically located in Dallas, Texas and Atlanta, Georgia. Prosecutors therefore had no justification for bringing the case against Auernheimer in New Jersey.
https://www.wired.com/2014/04/att-hacker-conviction-vacated/

#Linkedind_Hack_2012
“LinkedIn Security professionals suspected that the business-focused social network LinkedIn suffered a major breach of its password database. Recently, a file containing 6.5 million unique hashed passwords appeared in an online forum based in Russia. More than 200,000 of these passwords have reportedly been cracked so far.”
The consensual aggregation of personal and employment information online has greatly simplified the task of finding targets for intelligence gathering. The technology that makes finding a project manager with an MBA and five years of experience fast and convenient also makes it easy to track down missile and radar engineers on LinkedIn. The publicly available information on LinkedIn is a trove of intelligence in itself regarding military, government, and contract employees that work in defense related industries. Having the private email addresses and passwords of LinkedIn members has staggering spearfishing implications ala STUXNET.

Andrew Auernheimer, a controversial computer hacker who looked through the files, used Twitter to publicly identify Adult FriendFinder customers, including a Washington police academy commander, an FAA employee, a California state tax worker and a naval intelligence officer who supposedly tried to cheat on his wife.
https://money.cnn.com/2015/05/22/technology/adult-friendfinder-hacked/
https://cimsec.org/for-a-good-time-hack-opm/

Washington CNN — Morocco has become the fourth country in the Middle East and North African region to agree to establish full diplomatic relations with Israel, an 11th-hour foreign policy achievement for the lame duck Trump administration as it seeks to shore up regional support for Israel as a countermeasure to Iranian aggression.

#macron_gate_2017
It was no secret that Macron's opponent, Marine Le Pen, was the Kremlin's favoured candidate. In 2014, her party, the Front National, received a loan of €9.4 million from the First Czech-Russian Bank in Moscow. One month before the election, Le Pen travelled to Moscow to meet with Putin; she claimed that it was their first meeting, but in reality it was their third. This suggests that the Kremlin made a major 'investment' in the Front National.
for 'Macron Gate' two days before the leak, may in fact be an American neo-Nazi hacker, Andrew Auernheimer.24 Given the well-known alliance that exists between the Kremlin and American far-right movements.
as per Correction of cyberscoop.com: A review by cybersecurity firm Area 1 Security of a previous version of this story revealed a technical error that had led to inaccurate analysis by Flashpoint. Flashpoint acknowledged and apologized for the mistake but stands by its overall assessment of "moderate confidence that the group is likely linked to Russia's Main Intelligence Directorate (GRU)" and, furthermore, with APT28.
https://cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/
https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017
Duqu + Dutch Spy + Stuxnet + Sysjoker = Operation Olympic Games
https://malpedia.caad.fkie.fraunhofer.de/actor/unit_8200
https://malpedia.caad.fkie.fraunhofer.de/details/win.duqu
https://malpedia.caad.fkie.fraunhofer.de/backend/download_yara/3e967b3c-4d1f-4271-97e1-82cee9e1f14b
https://malpedia.caad.fkie.fraunhofer.de/backend/download_yara/69e8e53d-1141-4bb2-9599-56ba5b9c4f61
https://malpedia.caad.fkie.fraunhofer.de/backend/download_yara/55e34469-553e-474a-bcca-6b74e69837c4
https://malpedia.caad.fkie.fraunhofer.de/backend/download_yara/13f69f49-29e4-480c-9a61-75aa3e9baf60

"Today we live in a world in which it is difficult to hide secrets, in which data companies such as Google already have more knowledge and insight about the population than Stalin ever did

about his population. This reality represents a challenge for our freedom and human rights, and opens the question about the relationship between liberty and security. Finally, it is not a fantasy to think about “Digital Countries” as a new concept of world organization .This ability to use big data is a result of the development of the capability to save and to tag data, and then manipulate it through high-performance computing , The key to addressing this risk is to create novel ways to collaborate between cyber capabilities and AI capabilities , Their decisions include using AI to improve the ability to build cyber-attack tools; to improve defense capabilities to find new viruses; and to enable attackers to find relevant files in their rivals’ and enemies’ networks. For example, China is developing a department of AI tools for cyber-defense and cyberattack. They believe that cyber is a strong domain in China and that AI is a relevant innovation that can empower their cyber capabilities. As a result, China decided to establish a new unit that will focus on cyber and AI to enable the acceleration of this specific new ability. In cyberspace, there are myriad viruses and cyber-attack tools that can act against your network. There is no option to “clean” your network of
viruses. Viruses mutate all of the time, and viruses create new viruses. In addition, there are people and computers that want to attack your network for different reasons. One of the challenges is that even when a cyberattack tool is caught, it is still possible for the cyber-attacker to alter this tool a bit and to use the new version of the virus to attack again. For that reason, we don’t have any choice in cyberspace. We are required to deal with viruses and cyber-attack tools. The mission is not to clean the
network, but rather to build our network with the ability to “live” with some viruses and to choose which of them we need to totally destroy." as per YOSSI SARIEL Commander, Israeli Military Surveillance Agency Unit 8200.
https://leorugens.wordpress.com/wp-content/uploads/2024/09/yossi-sariel-the-human-machine-team-how-to-create-synergy-between-human-artificial-intelligence-that-will-revolutionize-our-world-ebookpro-publishing-2021.pdf
https://medium.com/nfactor-technologies/part-1-navigating-the-threat-of-evasion-attacks-in-ai-4d7ea9831143

The Google engineer who was suspended by the company after claiming the firm’s AI system, LaMDA, seemed sentient has said a question he posed to the software about Israel, and a joke it gave in response, helped him reach that conclusion.

Ariel Koren, director of educational product marketing, said she resigned from Google because of harassment of employees when discussing the company's values and the policy of revenge against those who defend Palestinians.
https://www.notechforapartheid.com/
https://www.facebook.com/ariel.koren.77
https://medium.com/@arielkoren/googles-complicity-in-israeli-apartheid-how-google-weaponizes-diversity-to-silence-palestinians-cb41b24ac423

Evasion attacks pose significant challenges to cybersecurity efforts: Bypassing malware detection: Attackers can modify malware signatures to evade detection by AI-powered antivirus systems.

Compromising intrusion detection systems: Network intrusion detection systems relying on AI can be fooled by carefully crafted network traffic patterns.
Undermining facial recognition: Security systems using facial recognition can be bypassed using adversarial patches or manipulated images.
Manipulating autonomous systems: Self-driving cars and other autonomous systems can be tricked into making dangerous decisions through environmental perturbations.
https://www.kfsensor.net/kfsensor/free-trial/

Hijacking and man in the middle attacks of the Telecommuncations communications Central of Maadi and Tur Sinai , cutting off communications, transferring, passing, spying, eavesdropping, and controlling unreliable Internet services and Creating diseases for humans through loopholes and spreading them to the rest of the Telecommuncations mobile companies.
{ radio/telecommunication bandmode/channel : ULE/PBX/CAT/DECT+Ultrasonic }
full range of frequencies 0 hertz to 3000000000 hertz
ELF frequency : 1800 to 1500 HERTZ
VHF frequency: 136.00000 to 174.00000 MHz == Self Spy earpieces
UHF frequency: 400.00000 to 470.00000 MHz
UFH frequency : 1880 MHZ to 1900 MHZ == DECT Telephone.
https://www.dect.org/dect-technology
https://isbgpsafeyet.com/
maadi ISP (Telecom Egypt, AS8452) implements BGP
https://bgp.tools/as/8452#connectivity
https://bgp.he.net/AS8452#_traceroute
ISP (Telecom Egypt, AS8452) does not implement BGP safely
https://doi.org/10.1016/j.diin.2018.04.007
https://opencellid.org/#zoom=18&lat=32.085299&lon=34.781806
https://www.youtube.com/watch?v=3HlBB5JzI0Y

Such as the leaking of General Petroleum Corporation companies documents with more than 130,000 documents, geophysical , petrophysical and Well test records reports for areas of exploration, espionage, bank theft, and some military and security information as first political , Industrial and Cyber adversary competitions between Sahara oil field services company #SAPESCO , #BP_Egypt , TV/Automative//Military Manfuraction information's Companies , Official Students Exams Hacking Among us, people and police investigator officers in Egypt, and organ and drug dealers involved in expelling people from their homes and having sexual relations outside of marriage to control people, leak documents, spy on oil and gas companies, fraud, and create illusionary operations.
https://www.6wresearch.com/industry-report/egypt-signals-intelligence-sigint-market-outlook
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017

Stealing intellectually protected programs and electronic accounts and The Gaza Strip tunnels were penetrated by the resistance factions .

“Anonymous,” the well-known international “hacktivist” group, has also joined the virtual war between pro-revolution and counterrevolutionary forces. The group quickly declared its support of the Egyptian revolution after 25 January, launching “Operation Egyptian” in which it targeted Egyptian government websites.
On 11 November, several Brotherhood websites received thousands of hits per second from Germany, France, Slovakia and San Francisco, temporarily downing four of the Islamist group’s better known online forums, including its flagship “Ikhwan Online” website.
The official Facebook page of the ultraconservative Salafist Nour Party in Egypt’s Fayoum governorate, meanwhile, was also hacked in November by an unknown group that posted images of scantily dressed women on the site.
https://english.ahram.org.eg/NewsContent/1/64/31488/Egypt/Politics-/Revolutionary-activists-take-fight-into-cyberspace.aspx

Phonito Nano headsets and nano radio invisible-in-the canal (IIC) are compatible with a wide range of professional radios (including the latest TETRA models from Motorola, Sepura and Hytera).
PTT over IP is a service providing group communication like Two-Way Radio communication systems (TETRA, DMR and the classic analogue PMR). Existing systems can be easily substituted, including DECT systems! Medium for that communication standard is an internet connection .
https://www.nidcd.nih.gov/health/hearing-aids
https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/hearing-aids
https://www.phonak-communications.com/en/product/phonito-nano/
https://www.sciencedirect.com/science/article/abs/pii/S000578947580075X
https://www.cia.gov/readingroom/docs/CIA-RDP80-00809A000600330387-6.pdf

#Maadi_SpyCameras_RTSP_Exposed_security_significant_risks
I am [Elgilany Hassan Sayed Mohamed] involuntarily connected to control projects such as the Nimbus project, artificial intelligence, Cyberwarfare and the learning of quantum machines in Tel Aviv, and international technology companies linked to corruption operations of local and international intelligence because of the policies of Israel and countries against the freedom and rights of Palestine , the Palestinians and participation owner rights of my cybersecurity research projects .
Unfortunately, I Am [Elgilany Hassan Sayed Mohamed] (Ransomware Readiness Auditing Expert Reviewer) will move in an international direction for human rights after encountering affliction and torment and being exposed to a major fraud operation by those manipulating human freedoms in beloved Egypt by expelling them from my residence illegally. They steal citizens’ property and expel them from... My house (36 Hamed Nafea St., off Ahmed Zaki St. - Al-Basateen).
Am victim of the extraction of stem cells from my body and the conduct of practical and cyber research from high-risk groups in the encounter with torture on individuals who have unique mental abilities for foreign and terrorist interests.
The family of Ashraf Helmy Mohamed Faraj and Omar Abdel Shakur Ahmed Mohamed witnessed me leaving the house and stealing my property and belongings from the house and

apartment, then liquidating and killing me after I left the house and the house, me and my children, to erase all evidence of the implantation of spy devices.
And spying on me and on others with thermal cavitation devices, cameras with different sensitivities and technologies, eavesdropping devices, and exposing my private parts to the public with permits from investigation officers without prosecutor's permission or prosecutor's orders.
The puzzling question: Why should I and my children be liquidated, and why should the My The unfaithful wife.
Many poorly configured security cameras are being hacked by hackers in Egypt and Palestine, putting the owners who use them and the people around them at great risk.
https://book.hacktricks.xyz/network-services-pentesting/554-8554-pentesting-rtsp
https://nmap.org/nsedoc/scripts/rtsp-url-brute.html
https://gitlab.com/woolf/RTSPbrute
https://securityaffairs.com/152265/hacking/security-cameras-israel-and-palestine.html?fbclid=IwY2xjawFC2W9leHRuA2FlbQIxMAABHYxa7x90oMkddZ7vEkpiN-TzqmyMkVQym8Pe2FaQusbZpUca0KMGOYEm-A_aem_gHnkwPy4GLhDxEAmOim_kg
https://cybernews.com/security/exposed-security-cameras-pose-risk-in-israel-palestine/
https://leorugens.wordpress.com/wp-content/uploads/2024/09/yossi-sariel-the-human-machine-team-how-to-create-synergy-between-human-artificial-intelligence-that-will-revolutionize-our-world-ebookpro-publishing-2021.pdf
https://mx.linkedin.com/in/arielkoren?trk=people-guest_people_search-card
---
https://isbgpsafeyet.com/
https://github.com/RBReif/bgp-hijack-detection
https://github.com/papastam/HY436
https://github.com/FORTH-ICS-INSPIRE/artemis
https://github.com/PopLabSec/BGP-Security

https://www.researchgate.net/figure/Sequence-of-BGP-takeover-method-not-applying-a-virtualization-technology_fig11_314225077
https://loicmiller.com/uploads/master-thesis.pdf
https://abhandshake.com/community/pbx-hacking/
https://devopedia.org/pbx-hacking

#Maadi_Direct_Volume_Access
Adversaries may directly access a volume to bypass file access controls and file system monitoring. Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique may bypass Windows file access controls as well as file system monitoring tools. [1]
Utilities, such as NinjaCopy, exist to perform these actions in PowerShell.[2] Adversaries may also use built-in or third-party utilities (such as vssadmin, wbadmin, and esentutl) to create shadow copies or backups of data from system volumes.[3]
https://attack.mitre.org/techniques/T1006/

#Understanding_the_PBX_VOIP_and_SIP_Protocols_Trunking_and_Attacks_Pentesting_VoIP
Hackers attack your private branch exchange (PBX) to overload your systems and place costly international calls. This private network also allows them access to gather confidential information.
The Session Initiation Protocol (SIP) allows us to establish, end or change voice or video calls. The voice or video traffic is transmitted via the Real Time Protocol (RTP) protocol.
Session Initiation Protocol is defined as a protocol that enables call handling sessions, specifically two-party audio conferences.
SIP is an application layer protocol that uses UDP or TCP for traffic. By default SIP uses port 5060 UDP/TCP for unencrypted traffic or port 5061 for TLS encrypted traffic
Call tampering is an attack which involves tampering a phone call in progress. For example, the attacker can simply spoil the quality of the call by injecting noise packets in the communication stream. He can also withhold the delivery of packets so that the communication becomes spotty and the participants encounter long periods of silence during the call.
https://www.nextiva.com/blog/what-is-sip-trunking.html

#Network_Boundary_Bridging
Devices such as routers and firewalls can be used to create boundaries between trusted and untrusted networks. They achieve this by restricting traffic types to enforce organizational policy in an attempt to reduce the risk inherent in such connections. Restriction of traffic can be achieved by prohibiting IP addresses, layer 4 protocol ports, or through deep packet inspection to identify applications. To participate with the rest of the network, these devices can be directly addressable or transparent, but their mode of operation has no bearing on how the adversary can bypass them when compromised.
https://attack.mitre.org/techniques/T1599/
#CAPEC_584_BGP_Route_Disabling
An adversary suppresses the Border Gateway Protocol (BGP) advertisement for a route so as to render the underlying network inaccessible. The BGP protocol helps traffic move throughout the Internet by selecting the most efficient route between Autonomous Systems (AS), or routing domains. BGP is the basis for interdomain routing infrastructure, providing connections between these ASs. By suppressing the intended AS routing advertisements and/or forcing less effective routes for traffic to ASs, the adversary can deny availability for the target network.
https://capec.mitre.org/data/definitions/584.html
#maadi_voip_man_in_the_middle_attacks
VoIP is particularly vulnerable to man-in-the-middle attacks, in which the attacker intercepts call-signaling SIP message traffic and masquerades as the calling party to the called party, or vice versa
https://attack.mitre.org/techniques/T1557/
#Sip_guid_enumeration
https://tomtalks.blog/microsoft-teams-direct-routing-sip-tester-powershell-script/
https://nmap.org/nsedoc/scripts/sip-enum-users.html
https://svn.nmap.org/nmap/scripts/sip-enum-users.nse

https://book.hacktricks.xyz/network-services-pentesting/pentesting-voip/basic-voip-protocols/sip-session-initiation-protocol
https://book.hacktricks.xyz/network-services-pentesting/pentesting-voip
https://www.splunk.com/en_us/blog/security/take-a-sip-a-refreshing-look-at-subject-interface-packages.html
https://github.com/g0ldbug/bgp-hijacking/tree/master/countermeasure
https://medium.com/tenable-techblog/grandstream-pbx-hacking-29f61c0d9179
Looking for a free security toolset to test your SIP infrastructure?
How to install: sudo apt install sipvicious
https://www.kali.org/tools/sipvicious/
https://www.enablesecurity.com/sipvicious/
https://github.com/EnableSecurity/sipvicious/tree/master
#maadi_subvert_trust_controls_sip_and_trust_provider_hijacking
Adversaries may tamper with SIP and trust provider components to mislead the operating system and application control tools when conducting signature validation checks. In user mode, Windows Authenticode [1] digital signatures are used to verify a file's origin and integrity, variables that may be used to establish trust in signed code (ex: a driver with a valid Microsoft signature may be handled as safe). The signature validation process is handled via the WinVerifyTrust application programming interface (API) function, [2]
https://attack.mitre.org/techniques/T1553/003/
https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Endler.pdf
https://book.hacktricks.xyz/network-services-pentesting/pentesting-voip
https://www.slideshare.net/slideshow/the-art-of-voip-hacking-defcon-23-workshop/51569342
http://startrinity.com/VoIP/VoipTroubleshootingBook/VoipTroubleshootingBook.aspx
https://specterops.io/wp-content/uploads/sites/3/2022/06/SpecterOps_Subverting_Trust_in_Windows.pdf
https://github.com/mattifestation/PoCSubjectInterfacePackage
https://startrinity.com/VoIP/SipTester/SipTester.aspx
https://medium.com/vartai-security/practical-voip-penetration-testing-a1791602e1b4
https://www.hackingarticles.in/penetration-testing-on-voip-asterisk-server/
https://medium.com/vartai-security/practical-voip-penetration-testing-a1791602e1b4

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry/registry_set/registry_set_sip_persistence.yml
https://github.com/cs4404-mission2/writeup

#Cisco_Unified_Communications_Manager_Denial_of_Service_Vulnerability
A vulnerability in the SIP call processing function of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.
This vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a crafted SIP message to an affected Cisco Unified CM or Cisco Unified CM SME device. A successful exploit could allow the attacker to cause the device to reload,

resulting in a DoS condition that interrupts the communications of reliant voice and video devices.
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-dos-kkHq43We?fbclid=IwY2xjawFo7wFleHRuA2FlbQIxMAABHTI7gtZxnvmK0WXdT9A4TuTiHUz-KXOFPSqhPeCdZTuiJw-0l1sCcIuTuQ_aem_rfOmlC-BLRI4n967SrBtdw
https://www.infopulse.com/blog/sip-hacking-protecting-voip-services
https://www.youtube.com/watch?v=pGH-gd4T6dc

#CVE_2019_19006_critical_vulnerability_in_Sangoma_PBX
45.143.220.0 (45.143.220.0/23)
ASN: AS 216014 (BestDC Limited)
While investigating the exploitations, researchers identified several online profiles associated with private Facebook groups that deal with VoIP, and more specifically, SIP server exploitation. After close examination of the admins, active users and carriers seen in the Facebook groups, we found that most of them were located in Gaza, the West Bank and Egypt.
https://otx.alienvault.com/indicator/ip/45.143.220.116
https://research.checkpoint.com/2020/inj3ctor3-operation-leveraging-asterisk-servers-for-monetization/

RoIP Wireshark POC
(filter or regex in Wireshark search : noise)
https://book.hacktricks.xyz/todo/hardware-hacking/radio
https://www.youtube.com/watch?v=VfPHU3301hw
https://www.youtube.com/watch?v=crrLeUu4ez8
https://www.youtube.com/watch?v=PV5fML0spHc
https://www.youtube.com/watch?v=sHAoz1OUHsw
https://www.youtube.com/watch?v=krJJKjYdwgc
https://www.youtube.com/watch?v=rOtnq7H2-5o
https://www.youtube.com/watch?app=desktop&v=tRPJJUK0TT4
https://www.youtube.com/watch?v=3HlBB5JzI0Y

Malware Family : Mirai - BumbleBee_Round Two
Exploited CVEs: 2002-0013
Antivirus Ms Defender: Backdoor:Linux/Mirai.YA!MTB
Antivirus Ms Defender: DDoS:Linux/Gafgyt.YA!MTB
Malware: flbpfuh.exe
151.101.0.0/16 ASN: AS54113 (fastly) [USA]
119.23.0.0/16 ASN: AS37963 (Hangzhou Alibaba Advertising Co.,Ltd.) [China]
47.254.0.0/16 ASN: AS45102 (Alibaba US Technology Co., Ltd.)[USA]
mazen158.biz 41.32.0.0/16 ASN:AS8452 (TE Data)[Egypt]
47.254.37.11 (47.254.0.0/16) AS 45102 (Alibaba US Technology Co., Ltd.)
51.75.78.103 (51.75.0.0/16) AS 16276 (OVH SAS)
JA3 Digests: a0e9f5d64349fb13191bc781f81f42e1
JA3 Digests: bd0bf25947d4a37404f0424edf4db9ad

https://www.virustotal.com/gui/ip-address/151.101.0.0/relations
https://www.virustotal.com/gui/ip-address/119.23.0.0/relations
https://www.virustotal.com/gui/ip-address/47.254.37.11/relations
https://www.virustotal.com/gui/file/2f9eede4555bbcc943340dec4269a339fe0888253f8702855c58152ba950abdb/behavior
https://www.virustotal.com/gui/file/1d241ad990b650d9ead70ba399dfaf4a1aa0880c2d830a2a4db0c79c780e09e3/behavior
https://www.virustotal.com/gui/file/04b67519d40f9e55b2577af784c9f19a677071b3595ba859ca81721b66040d94/behavior
https://www.virustotal.com/gui/file/05e538a578569dcefe530ce7693f6a891c53f16ad235bf66f8986dc1829a7490/behavior
https://otx.alienvault.com/indicator/file/a0e9f5d64349fb13191bc781f81f42e1
https://www.shodan.io/host/41.32.140.15
https://www.virustotal.com/gui/domain/mazen158.biz/relations
https://otx.alienvault.com/indicator/domain/mazen158.biz

https://otx.alienvault.com/malware/Backdoor:Linux%2FMirai/fileSamples
https://otx.alienvault.com/pulse/66fada7a38eb139826f9eb7e/

Antivirus Detections : Unix.Trojan.Mirai-7669677-0
43.132.64.0/22 ASN: AS139341 ace [United Kingdom of Great Britain and Northern Ireland]
180.76.64.0/18 ASN: AS 38365AS38365 beijing baidu netcom science and technology co. ltd. [China]
JA3 Digests: ce5f3254611a8c095a3d821d44539877
https://www.virustotal.com/gui/ip-address/43.132.64.0/relations
https://www.virustotal.com/gui/file/61988d6d281197aed2605574577c91fcaaf3ea59bacb528660bee59b56276443/behavior
https://otx.alienvault.com/indicator/file/ce5f3254611a8c095a3d821d44539877
https://otx.alienvault.com/pulse/63319f8437950bd1f1207747

https://www.virustotal.com/gui/domain/f3322.net/relations
https://www.virustotal.com/gui/domain/zhudaji.f3322.net/relations
https://www.virustotal.com/gui/domain/mdoj7i.top/relations
https://www.virustotal.com/gui/domain/willta.com/relations

#resteex_mirai_egypt_2022_lvl0
https://otx.alienvault.com/pulse/6264d60c994aac998ce85e32
https://otx.alienvault.com/pulse/6263396a7faae35e8fdba502
https://otx.alienvault.com/pulse/6263286eada505ae5743dcb4
https://otx.alienvault.com/pulse/627136c8b95024f5508312fb
https://otx.alienvault.com/pulse/626204dff57a48d08dfdb69a

https://intezer.com/blog/malware-analysis/evasion-techniques-dissected-mirai-case-study/

Compromise Accounts: Social Media Accounts
Adversaries can use a compromised social media profile to create new, or hijack existing, connections to targets of interest. These connections may be direct or may include trying to connect through others.[2][3] Compromised profiles may be leveraged during other phases of the adversary lifecycle, such as during Initial Access (ex: Spearphishing via Service).
https://attack.mitre.org/techniques/T1586/001/
https://attack.mitre.org/groups/G0065/
https://www.cisa.gov/sites/default/files/publications/CSA_TTPs-of-Indicted-APT40-Actors-Associated-with-China-MSS-Hainan-State-Security-Department.pdf
https://blog.talosintelligence.com/china-chopper-still-active-9-years-later/

Server Software Component: IIS Components
Adversaries may install malicious components that run on Internet Information Services (IIS) web servers to establish persistence. IIS provides several mechanisms to extend the functionality of the web servers.
https://attack.mitre.org/techniques/T1505/004/

#Application_Layer_Protocol_Web_Protocols
Protocols such as HTTP/S[1] and WebSocket[2] that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.
https://attack.mitre.org/techniques/T1071/001/
https://intezer.com/blog/research/wildcard-evolution-of-sysjoker-cyber-threat/
https://www.attackiq.com/2022/08/02/malware-emulation-attack-graph-for-sysjokers-linux-variant/
https://securityaffairs.com/154748/malware/hamas-linked-apt-sysjoker-backdoor.html
google search = "/api/attach" country:Israel
https://book.hacktricks.xyz/generic-methodologies-and-resources/external-recon-methodology/github-leaked-secrets
https://www.boxpiper.com/posts/google-dork-list

Application Layer Protocol: DNS
Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.[1][2]
https://attack.mitre.org/techniques/T1071/004/

https://jpassing.com/2021/01/05/hijacking-other-users-tcp-tunnels/

#intrusion_detection_system_tools
https://hexed.it/
https://www.kfsensor.net/kfsensor/download/WinPcap_4_1_3.exe
https://www.kfsensor.net/kfsensor/download/kfsens40.ms
https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170#latest-microsoft-visual-c-redistributable-version
https://www.kfsensor.net/kfsensor/download/WinPcap_4_1_3.exe
https://www.kfsensor.net/kfsensor/download/kfsens40.msi
https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview
https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer
https://aka.ms/vs/17/release/vc_redist.x86.exe
https://aka.ms/vs/17/release/vc_redist.x64.exe
https://npcap.com/dist/npcap-1.80.exe
The VoIP PBX Honeypot Advance Persistent Threat Analysis
https://www.scitepress.org/PublishedPapers/2021/104435/104435.pdf
https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1&limit=10&q=resteex0&indicatorsSearch=resteex0,resteeex0
Honeypots for Windows
https://link.springer.com/content/pdf/10.1007/978-1-4302-0007-9.pdf
ransomware + showmang server static ip + hexadecimal editor

The final solution to the entire case (solution system)
1- The names mentioned in the Cairo Etiquette and Anti-Spoofing Investigations must be visited with the candidates. The counterfeit cards, until the links are closed, are linked inversely with variables linked to mobile and fixed phone numbers and national ID numbers in separate categories for each variety, until the lines are blocked because there are no new cards for each series.
يجب مراجعه الاسماء الوارد ذكرها في مباحث اداب ومكافحه المخدرات القاهره مع مراجعه البطاقات المزيفه حتي قفل السلاسل مربوطه عكسيه بمتغيرات مربوطه بارقام الهواتف المحموله والثابته واراقم الهويات القوميه في سلاسل منفصله لكل متغير حتي يتم قفل السلاسل بعدم وجود اي بطاقات جديده في كل سلسله
A- complete series of counterfeit cards linked to mobile phone numbers, starting with the first suspicious card and linking it with the suspect's name on the card to the mobile phone numbers in all mobile phone companies, then linking each mobile phone number by searching for the cards linked to it in the Ministry of Interior's system, and so on and so on..... ..until there is no other new card.
سلسله كامله من البطاقات المزوره بربطها بارقام الهواتف المحموله ببدء بالبطاقه المشبوها الاولي وربطها باسم المشبوه في البطاقه بالارقام الهواتف المحموله في جميع شركات المحمول ثم ربط كل رقم هاتف محمول بالبحث عن البطاقات المربوطه بها في نظام وزاره الداخليه وهكذا وهكذا الخ ..... حتي يتم ان لا يوجد اي بطاقه جديده اخري
B - A complete series of counterfeit cards linked to fixed phone numbers, starting with the first suspicious card and linking it to the suspect's name on the card to the fixed phone numbers, then linking each fixed phone number to a search for the cards linked to it in the Ministry of Interior's system, and so on, and so on, etc..... until There is no other new card

سلسله كامله من البطاقات المزوره بربطها بارقام الهواتف الثابته ببدء بالبطاقه المشبوها الاولي وربطها باسم المشبوه في البطاقه بالارقام الهواتف الثابته ثم ربط كل رقم هاتف ثابت بالبحث عن البطاقات المربوطه بها في نظام وزاره الداخليه وهكذا وهكذا الخ ..... حتي يتم ان لا يوجد اي بطاقه جديده اخري

C - A complete series of counterfeit cards by linking them to the national number, starting with the first suspicious card and linking it to the suspect's name on the card with the national number, then linking each to the national number by searching for the cards linked to it in the Ministry of Interior system, and so on, and so on, etc..... until it is not There is no other new card

ج - سلسله كامله من البطاقات المزوره بربطها بالرقم القومي ببدء بالبطاقه المشبوها الاولي وربطها باسم المشبوه في البطاقه بالرقم القومي ثم ربط كل بالرقم القومي بالبحث عن البطاقات المربوطه بها في نظام وزاره الداخليه وهكذا وهكذا الخ ..... حتي يتم ان لا يوجد اي بطاقه جديده اخري

D - Collecting the full names and mobile phone numbers after the three strings, linking the national identity cards and the three variables.

د - تجميع الاسماء كامله وارقام الهواتف المحموله بعد الثلاث سلاسل الربط بين البطاقات الهويات القوميه والمتغيرات الثلاثه

2- Phone log data in mobile companies must be analyzed in call forward settings, similar to the numbers of employees in embassies, consulates, etc.

يجب تحليل بيانات سجل الهواتف في شركات المحمول في اعدادات تحويل الاتصالات (call forward setting) متشابه مع ارقام الموظفين في السفارات والقنصليات والخ

3- Repeat the previous steps together with the numbers of the suspected cars, starting from the first owner to the last owner, with their agencies.

اعاده الخطوات السابقه معا ارقام السيارات المشتبه فيهم ابتداءا من المالك الاول حتي المالك الاخير بتوكيلاتهم

4- Review and accurately review banking units and accounts, internal and external transfers, and encrypted Transfer printing for more than one million Egyptian pounds in an average month or year Income abroad.

- Take out the bank and internal accounts of the living cost and Fees

مراجعة ومراجعة الوحدات والحسابات المصرفية بدقة والتحويلات الداخلية والخارجية وطباعة التحويلات المشفرة لأكثر من مليون جنيه مصري في متوسط الدخل الشهري أو السنوي بالخارج.

- إخراج الحسابات البنكية والداخلية لتكاليف المعيشة والرسوم

#maadi_sip_trunking_man_in_the_middle_attacks
#maadi_sip_guid_enumeration_attacks
#maadi_call_tampering_attacks
#maadi_isp_bgp_ssh_pbx_hijacking
#maadi_cyber_automotive_attacks
#maadi_acoustic_cybercrime_attacks
#acoustic_digital_forensics_ultrasonic_firewall

شاهد اثبات لحظه مكالمه بين شخص يدعو اسامه مع حلمي اشرف حلمي محمد فرج وعند الانتهاء من المكالمه وانا في الطابق الاسفل من حلمي اشرف حلمي محمد فرج بعدها بدقائق اعاده المكالمه بجوده عاليه جدا ولكن بطرف صوتي وحيد (حلمي اشرف حلمي محمد فرج) بتسمع المكالمه من اجهزه موبيل ساميه حلمي محمد فرج وسمير في الشقه المقابله بدون التنصت عليهم ,

شاهد الاثبات : لحظه تواجدي يوم 23/3/2024 امام بعض كاميرات مراقبه داخليه لمسجد حسن صدقي - المعادي

حق يقين : "لا كلام مع الجن والانسان هذه لسان و هذه لسان"

الاثبات : لايمكن التكلم مع الحيوانات او التخاطب معها في العالم الملموس الحقيقي من حولنا مهما بلغت التقنيات ولذلك لايمكن التحدث مع الجن في العالم الغير ملموس مع الانسان - انتهي الاثبات

شهود

انس جابر عبد الحميد

مجلس اداره في مكتب المحماه / Links & Gains

اسماء المتورطين والمشتبه فيهم للدرجه الاولي

Andrew Auernheimer [weev] “Anonymous_NeoNazi_Stuxnet”
ricky camilleri “Anonymous_NeoNazi_Stuxnet”
Erik Jacob van Sabben “Anonymous_NeoNazi_Stuxnet"
Yossi Sariel “Anonymous_Stuxnet”
Yossi cohen “Anonymous_Stuxnet”
Avigayil Mechtinger “Stuxnet_Sysjoker”
Nicole Fishbein “Stuxnet_Sysjoker”
Ido Solomon "inje3t0r3"
Ori Hamama "inje3t0r3"
Omer Ventura "inje3t0r3"
Ahmed El-Sayid El-Mandouh, popularly known as Ahmed “Spider.”
“Anonymous_SpyCamera_Pegasus”
Monalisa Octocat “metasploit_modules_developer/contributing_Rail_on_Ruby"
Nona Said "Facebook_Employee/Anonymous"
ehab shakery armani
Helmy Ashref Helmy Mohamed Farag “Anonymous_Showmang_SpyCamera_Pegasus”
Ahmed Ashref Helmy Mohamed Farag “Anonymous_Showmang_SpyCamera_Pegasus”
Mohamoud Samir “Anonymous_Showmang_SpyCamera_Pegasus”
Amr Abdel Shakour Ahmed Mohamed "Data_exfiltration/Data_ID Spoofer"
Faten Abdel Shakour Ahmed Mohamed "unfaithful wife""Data_exfiltration/Data_ID Spoofer"
hidden Sexual Relationship with Ahmed Hamey "English Teacher"
Alaa Mohamed Ahmed Mohamed "Data_exfiltration/Data_ID Spoofer"
Aieman Mohamed ElSayed
Omnia Ragab "Data_exfiltration/Data_ID Spoofer"
Ahmed Ragab "Data_exfiltration/Data_ID Spoofer"
https://www.youtube.com/watch?v=37oBowW7vyQ
https://english.ahram.org.eg/NewsContent/1/64/31488/Egypt/Politics-/Revolutionary-activists-take-fight-into-cyberspace.aspx
https://malpedia.caad.fkie.fraunhofer.de/actor/unit_8200

علي عبد الونيس

توفيق عكاشه

اليوتيوبر / احمد مندو الشهير باحمد سبيدر

اليوتيوبر / احمد حسن وزوجنه زينب

نرمين عادل

مهندس بترول : ايمن محسن

مهندس بترول : محمود سيد
موظف في شركه بترول : احمد رجب
اللواء سامح نبيل مدير إدارة المعلومات بقطاع الأمن
العقيد أحمد عبد العزيز، رئيسًا لمباحث التلفزيون
مدير مباحث العاصمه السابق اللواء / عمرو إبراهيم
لواء مهندس /أحمد عدلى أحمد محمد – مساعد وزير الدلخليه لقطاع نظم الإتصالات وتكنولوجيا المعلومات
مدير مباحث البساتين السابق / أحمد طارق العسكري
مدير مباحث دار السلام السابق / وسام عطية
مدير مباحث المعادي / اسلام بكر
نائب مامور قسم البساتين / محمد مصطفي
ضابط مباحث قسم شرطة البساتين / كمال محمد كمال سليم
معاون مباحث قسم البساتين / وليد محمود محمد سليم
امنيه رجب صديقه فاتن عبد الشكور احمد محمد واخوها احمد رجب
عبد الشكور احمد محمد
ساميه حلمي محمد فرج
محمود سمير حسنيين واحمد سمير حسنيين ابناء ساميه حلمي محمد فرج
حلمي اشرف حلمي محمد فرج
احمد اشرف حلمي محمد فرج
محامي / علاء محمد احمد محمد
زوجه واقارب محامي / علاء محمد احمد محمد
دكتور / محمد السعد الرفاعي
العامليين والمالكين بمستشفي /مستشفى بنها للصحة النفسية وعلاج الإدمان
العامليين والمالكين بمستشفي / مصحة النيل للصحة النفسية
العامليين والمدعيين في مكتب المحماه / علاء محمد احمد محمد
احمد حسن سيد محمد
ساره حسن سيد محمد
مصطفي سعيد
اسامه عمر
هند الباز
ايمان محمود
ريم سعيد العسال
رامي سعيد العسال
احمد حمدي (مدرس لغه انجليزي)
ايمان محمد السيد
(بعض العاملين بمطاعم ماكدنولذ وبيتزا هت (شارع 9 المعادي
---
https://attack.mitre.org/tactics/enterprise/

VEILEDSIGNAL malware - UNC4736
remote code execution vulnerability in Chrome, CVE-2022-0609
Cascading software supply chain compromises
https://www.3cx.com/blog/news/mandiant-security-update2/
https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise/
89.45.67.160

172.93.201.88
185.38.151.11
VEILEDSIGNAL is a backdoor written in C that is able to execute shellcode and terminate itself. Additionally, VEILEDSIGNAL relies on additional modules that connect via Windows named pipes to interact with the C2 infrastructure.

Initial Access
T1190 Exploit Public-Facing Application
T1195 Supply Chain Compromise
T1195.002 Compromise Software Supply Chain

Mandiant Security Validation
Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID
A106-319
Command and Control - UNC4736, DNS Query, Variant #1
A106-321
Command and Control - UNC4736, DNS Query, Variant #2
A106-323
Command and Control - UNC4736, DNS Query, Variant #3
A106-324
Host CLI - UNC4736, 3CX Run Key, Registry Modification
A106-322
Malicious File Transfer - UNC4736, SUDDENICON, Download,
S100-272
Evaluation: UNC4736 Conducting Supply Chain Attack Targeting 3CX Phone Management System
https://github.com/cs4404-mission2/writeup
---
https://drive.google.com/file/d/1Uw7DVz4Qv9MjpJEef8bIkUEFq7zWU0NQ/view?usp=sharing
https://drive.google.com/file/d/1qF4z4Ahh8Nm1buXOUEhQdZ5UFtH8nyKW/view?usp=sharing
https://www.udacity.com/certificate/AS9T2XYD
https://www.youtube.com/watch?v=alrFbY5vxt4
---
https://drive.google.com/file/d/1Uw7DVz4Qv9MjpJEef8bIkUEFq7zWU0NQ/view?usp=sharing
https://drive.google.com/file/d/1qF4z4Ahh8Nm1buXOUEhQdZ5UFtH8nyKW/view?usp=sharing
https://www.udacity.com/certificate/AS9T2XYD
---
https://www.tcibr.com/tci-delivers-soldier-portable-sigint-systems-to-u-s-government-customer/
https://www.tcibr.com/wp-content/uploads/2023/06/TCI-612_625-datasheet.pdf
https://www.cia.gov/readingroom/docs/CIA-RDP88-01315R000400410023-1.pdf
---

This ultrasound-firewall may protect your digital devices
https://research.fhstp.ac.at/en/projects/sonicontrol-2.0-the-first-ultrasonic-firewall
acoustic_cookies_attacks
https://www.welivesecurity.com/2023/06/07/hear-no-evil-ultrasound-attacks-voice-assistants/

(الحل النهائي للقضيه كاملا (نظام الحل

4- (اختراق الحواسيب والهواتف والحياه الرقمية وارسال تقارير التجسس الي عناصر استخارتيه متخفيه تحت الأجهزة الأمنية المصرية المختلفة بعد عمل أوامر تتبع للضحايا و سرقه ملفات من المواطنين والمؤساسات والتجسس علي الكاميرات وحواسيب الاشخاص والعمل عن طريق RDP) تم سرقه ملفات من محل سكني و سرقه جميع محتوياتها بطردي من سكني لسرقه ملفات مهمه (منها) تقرير عن الامن السيبراني لجامعه سيناء لهجمات سيبرانيه)

ا- فحص بروتوكول سطح المكتب البعيد RDP ونجاح الاتصال Windows RDP Event Logs ID في اتصالات مشبوها وغير قانونيه وغير مصرح بها
ب- network logs sniffing
ت- dns routing
ث- man in middle
ج- OTP one time password
ح- modified Pegasus
خ - dslam setting radio two way protocols example Push to Talk PTT
د- يتم استهداف المواطنين و جمع معلومات عن اسم رباعي فقط ويتم عمل بطاقات قوميه باسم خامس مضاف الي الاسم الرباعي - باختراق حياتهم واجهزتهم الإلكترونية والتجسس علي جميع الحسابات اذا بقطع الاتصالات والتجسس علي مكالمات المواطنين
ذ- اختراق شبكات المحمول واستغلال ثغره wifi data وتنزيل مكالمات المواطنين من wifi data unencrypted المنقولة بين أبراج الاتصالات وتصنيف البيانات علي اسم المواطن والمكالمة المسجلة
ه- عدم تمكن مباحث الانترنت والمصنفات بالسيطره علي برامج الشات الراديويه المحمله ومثبته الاصل علي الهواتف المحموله ومستخدمه الشبكه المصريه للاتصالات والانترنت
https://www.youtube.com/watch?v=myzG11BP3Sk
https://systemweakness.com/windows-rdp-event-logs-identification-tracking-and-investigation-part-1-d1f23e26cc05
5- مراجعه وتدقيق الحسابات البنكيه والتحويلات الداخليه والخارجيه والعملات المشفره لاكثر من مليون جنيه في الشهر او متوسط السنه - تحرك حسابات البنوك الخارجية والداخلية تحرك شاذه في الداخل والخارج لأرقام غير عاديه في السحب والايداع لأشخاص نافذين في الدولة وربط حسابات خارجيه لنقل أموال كويسترن يونيون فالخارج بالداخل علي السبيل المثال وليس الحصر وشهادات ادخار للعائلة والابناء بأرقم مبالغ فيها حتي يتم التخفي و يتم سحب الأموال من البنوك وتحويلها الي الخارج في مده زمنيه معينه وبمقدار معين للأموال المرسلة حسب قانيين البنك المركزي
يتبقى قاده القوات المسلحة اعلي الهرم بعمليات خاصه للتخلص منهم و هناك حسابات بنكيه وماليه لأشخاص متوفيين ومفقودين في جميع بنوك المصرية تقدر ب 7 تريليون دولار تقريبا و تم جميع البيانات من اشخاص ضمن للمجموعه

6 -
التلاعبات بمنظومه الراديو لوزاره الداحليه والدفاع بثغره عميقه مؤثره سهله بنسخ الترددات والقنوات من اجهزه الالسلكي الردايويه AIR Copy/Clone - وعدم التزام الامنيين بتطبيق معاير نشره وزاره الداخليه والدفاع بظبط واعدادات الترددت المحدده في النشرات وتحديثها طبقا للتعليمات و قله الاهتمام بعدادادت اجهزه الراديو في نسخ الترددات عبر الاجهزه

https://www.youtube.com/results?search_query=aircopy+
https://github.com/PFGimenez/radio-ids

https://github.com/open-sdr/openwifi
https://github.com/xmikos/qspectrumanalyzer
8- اتصالات الراديو و radio trunking scanner والاتصالات المخفيه برتوكولات PTT push to talk في وزراه الاتصالات والداخليه والسنترالات المصريه في اخفاء الاتصالات المشبوه بين افراد الخليه وتلويث الاثيري والرديو الاصلي ب تغير الاصوات والاسماء ب voice changer والعملاء ويمكن قلب analog radio signal الي رقمي ثم Regex filter لاثبات حثق اليقين في في بيانات وموجات في السنترالات للمشتركيين في خدمات وزاره الاتصالات وتكنولوجيا المعلومات PTT تواجد الاتصالات

https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1&limit=10&q=Israeli&indicatorsSearch=Israeli

http://www.insecam.org/en/bycountry/IL/
http://82.102.164.18/cgi-bin/guestimage.html
http://82.102.164.18/cgi-bin/guestimage.html
http://82.102.164.18/cgi-bin/faststream.jpg?stream=half&fps=15&rand=COUNTER
http://82.102.164.17/cgi-bin/faststream.jpg?stream=half&fps=15&rand=COUNTER
Reverse DNS 82-102-164-18.orange.net.il
Rishon LeZiyyon,
https://otx.alienvault.com/indicator/ip/82.102.164.18
https://www.virustotal.com/gui/ip-address/82.102.164.18/details/
12 -
#VoIP_Google_Hacking_Database_Israel
https://nmap.org/dist/nmap-7.95-setup.exe
https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Endler.pdf
IP-cams-dork-list
List of dorks to find unsecured ip cams
IP to ASN json list
https://github.com/rootac355/IP-cams-dork-list/blob/master/google%20dorks%20for%20ip%20cams.txt
https://github.com/ProtDos/IP-Address-List/blob/main/Israel/ips.txt#L3
https://github.com/cbuijs/ipasn/blob/master/country-asia-israel.list
https://github.com/cbuijs/ipasn/blob/master/country-asia-israel4.list
https://github.com/cbuijs/ipasn/blob/master/country-asia-israel6.list
https://github.com/hightemp/col_ip_ranges_by_countries/blob/main/data/israel-ip-address-ranges.json
---
indicator of compromise IOCs
ASN
AS13335 CLOUDFLARENET, US
https://urlscan.io/domain/ntunhs.net
https://urlscan.io/domain/tracker.derekr.com
Mitre Attack : T1505 - Severity High - Server Software Component: IIS Components
Virustotal Security vendors' analysis: Phishing - Malicious - Suspicious - Identified malicious by Google Safe Browsing
https://otx.alienvault.com/indicator/hostname/en.ntunhs.net

https://otx.alienvault.com/indicator/hostname/kr.ntunhs.net
https://www.virustotal.com/gui/domain/en.ntunhs.net/details
https://www.virustotal.com/gui/domain/kr.ntunhs.net/detection
https://otx.alienvault.com/indicator/url/http:%2F%2Fnetworksolutions.com
https://otx.alienvault.com/indicator/domain/ntunhs.net
https://www.virustotal.com/gui/domain/ntunhs.net/relations

Last HTTPS Certificate - JARM fingerprint
27d3ed3ed0003ed1dc42d43d00041d6183ff1bfae51ebd88d70384363d525c

Communicating Files: trojan.mint/zard
https://www.virustotal.com/gui/file/751d03476f91b324fe70a33c76debd1d5e267cf69d4a54650ed7ee74b997d1ae/detection

ASN
AS 396982
(GOOGLE-CLOUD-PLATFORM)
https://otx.alienvault.com/indicator/ip/35.201.97.160
https://urlscan.io/result/83b7391a-8371-4cbd-82e8-e687c57baf4d/
https://urlscan.io/result/d53c0686-cbb6-48c3-916b-4798daad8629/
https://urlscan.io/result/556e090c-e7b0-4db0-9e96-792f3e356b48/
https://urlscan.io/result/4a5b5613-0778-4082-9efb-14dc2d7eb5a7/
https://urlscan.io/result/95c065a7-897f-4b83-b6fa-770007731cfc/

ASN
AS15169 google llc
https://otx.alienvault.com/indicator/ip/142.251.37.206
https://www.virustotal.com/gui/ip-address/142.251.37.206/relations

ASN
AS15169 google llc
https://otx.alienvault.com/indicator/ip/74.125.206.188
https://www.virustotal.com/gui/ip-address/74.125.206.188/relations
https://otx.alienvault.com/indicator/cve/CVE-2011-0404
Win.Packer.pkr_ce1a-9980177-0

CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Description
Stack-based buffer overflow in NetSupport Manager Agent for Linux 11.00, for Solaris 9.50, and for Mac OS X 11.00 allows remote attackers to execute arbitrary code via a long control hostname to TCP port 5405, probably a different vulnerability than CVE-2007-5252.

Metrics

CVSS 2.0 Severity and Vector Strings:
Score: 7.5 HIGHVector: (AV:N/AC:L/Au:N/C:P/I:P/A:P)
https://nvd.nist.gov/vuln/detail/CVE-2011-0404
https://www.exploit-db.com/exploits/15937
https://www.exploit-db.com/exploits/16838

17-

cd C:\Snort\bin
snort -?
snort -V
snort -W
snort -i 4 -A console

#socat_windows
netstat -atyno
socat TCP-LISTEN:3702 TCP:google.com:80
https://sourceforge.net/projects/unix-utils/files/socat/1.7.3.2/socat-1.7.3.2-1-x86_64.zip/download

#Slow_scan_television
https://en.wikipedia.org/wiki/Slow-scan_television
https://github.com/colaclanth/sstv
---
20 - WildCard: The APT Behind SysJoker Targets Critical Sectors in Israel
Cyber Toufan operations - Operation Electric Powder - Gaza Cybergang (aka Molerats) - SysJoker and DazzleSpy
https://research.checkpoint.com/2023/israel-hamas-war-spotlight-shaking-the-rust-off-sysjoker/
https://intezer.com/blog/research/new-backdoor-sysjoker/
https://intezer.com/blog/research/wildcard-evolution-of-sysjoker-cyber-threat/
https://intezer.com/blog/threat-hunting/detection-rules-sysjoker-osquery/
https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html
https://www.sentinelone.com/blog/sneaky-spies-and-backdoor-rats-sysjoker-and-dazzlespy-malware-target-macos/
https://op-c.net/blog/sysjoker-malware-depth-look-newest-backdoor-malware/

23- CWE-287: Improper Authentication

PMKID and 802.1x authentication vulnerability
MAC Authentication Bypass (MAB) Authentication

MAC authentication bypass is easy to manipulate and lacks granular control making it further vulnerable. Granular control adds a layer of security that if some hacker manages to access the network, he might not reach the sensitive information.
https://www.portnox.com/cybersecurity-101/mac-authentication-bypass/
رجاء تنفيذ عكسي لما ورد في المرجع
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-usr-mac-auth-bypass.pdf

CWE-1220: Insufficient Granularity of Access Control
The product implements access controls via a policy or other feature with the intention to disable or restrict accesses (reads and/or writes) to assets in a system from untrusted agents. However, implemented access controls lack required granularity, which renders the control policy too broad because it allows accesses from unauthorized agents to the security-sensitive assets.

https://me.kaspersky.com/blog/wi-fi-pmkid-attack/11521/
https://osqa-ask.wireshark.org/questions/49385/bss-transition-supported-relationship-to-80211r-support/
https://www.fortiguard.com/psirt/FG-IR-18-199
https://mrncciew.com/2014/08/21/cwsp-rsn-information-elements/
https://networklessons.com/cisco/ccnp-encor-350-401/wpa-and-wpa2-4-way-handshake

اكتشاف الثغره : Wireshark filter :
IEEE 802.11 wireless lan management frame > TAGGED parameters > TAG RSN information > PMKID list > PMKID empty
802.1x authentication > WPA Key Nonce empty
WPA Key Data > PMKID empty
حل الثغره : firewall reject and black listed : (PMKID list and WPA Key Data) > PMKID empty
---
اغلبيه ثغرات الامن السيبراني الحرجه في جمهوريه في مصريه تتلخص في هذه المرجع-22
https://www.ge.com/digital/sites/default/files/download_assets/Top-10-Cyber-Vulnerabilities-for-control-systems.pdf
https://www.mdpi.com/2076-3417/14/1/204
https://socradar.io/major-cyber-attacks-targeting-the-automotive-industry/
https://www.huawei.com/en/psirt/security-advisories/2024/huawei-sa-chvishhr-d50dedde-en
---
https://accounts.google.com/signin/recovery/lookup
https://www.openappsec.io/post/top-10-free-wafs-web-application-firewalls-for-2024

#sensitive_information_discloure_israel

inurl /admin/index.php username=admin&password=password israel
inurl /inurl /admin/index.php israel
inurl /view/viewer_index.shtml israel

inurl /sym404/root israel
inurl /admin/index.php israel
inurl /proc/self/cwd israel
inurl /.well-known/security.txt israel
inurl /pcap.dll israel
inurl /wp-includes/uploads israel
inurl /upload button.html israel
inurl /upload/shell.php israel
inurl /uploads/ktp israel
inurl /admin/upload.php israel
inurl /upload image israel
inurl /wp-content/uploads israel
inurl /wp-includes/uploads israel
inurl /assets upload ktp israel
inurl /assets/kcfinder/upload israel
inurl /assets upload ktp israel
inurl /assets/kcfinder israel
inurl /assets/filemanager/ israel
inurl /userpwd.txt israel
inurl /users / username / downloads israel

israel camera

3 inurl:ViewerFrame?Mode=Motion
4 inurl:MultiCameraFrame?Mode=Motion
5 intitle:liveapplet
6 intitle:"live webcam"
7 intitle:"Network Camera NetworkCamera"
8 intitle:"Live View / – AXIS"
9 inurl:/view.shtml
10 inurl:/view/index.shtml
11 inurl:view/view.shtml beach
12 inurl:view/view.shtml street
13 inurl:appletvid.html
14 inurl:CgiStart?page=Single
15 intitle:EvoCam inurl:webcam.html
16 inurl:indexFrame.shtml "Axis Video Server"

https://www.csoonline.com/article/2139598/sleuthcon-cybercrime-emerges-in-morocco-and-law-enforcement-gets-creative.html

---

https://myaccount.google.com/u/1/signinoptions/rescuephone?