COUNTERINTELLIGENCE

ADVERSARY PROFILING

Art Rebultan

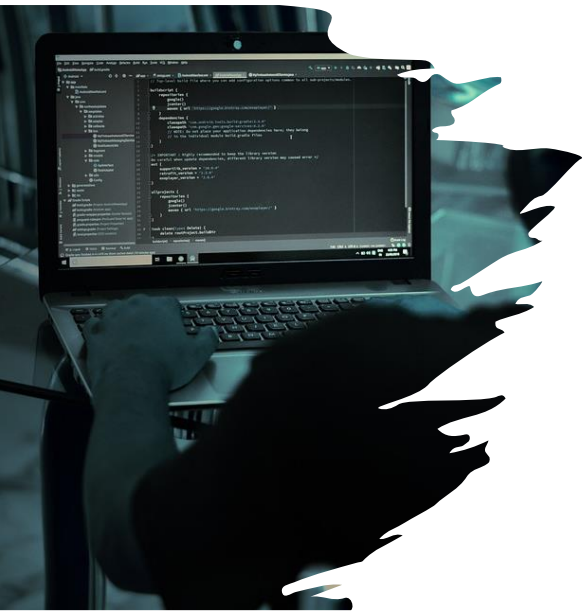
LightBasin aka UNC1945

PROFILE
UNC1945 is a group that has been observed targeting several organizations in the telecommunications, financial, and business services industries since at least early 2018. The assessed goal of UNC1945 is currently unknown as Mandiant has not been able to observe the objectives that followed UNC1945 compromises. Based on available information Mandiant has not been able to assess a general location that the group operates from.

- Aliases/Associations
  - TH-239 (Yoroi Security)

SUMMARY
A group of hackers that security researchers call LightBasin has been compromising mobile telecommunication systems across the world for the past five years. Since 2019, the group hacked into more than a dozen telecommunication companies and maintained persistence through custom malware, to steal data that would serve intelligence organizations. LightBasin is active since at least 2016 and targets Linux and Solaris servers in particular, although it did interact with Windows systems where needed, in their mission to steal subscriber information and call metadata. In a report today, CrowdStrike cybersecurity company says that the threat actor is a sophisticated group with strong operational security strategy. ~ During their investigation, CrowdStrike found that the threat actor first accessed an eDNS server through an SSH connection from the network of another compromised company. The researchers found evidence of LightBasin brute-forcing their way on the system by trying the default credentials for the targeted system. Following a successful compromise, the threat actor installed and executed custom malware that is currently tracked as SLAPSTICK - a backdoor for the Solaris Pluggable Authentication Module that gives access to the system based on a hardcoded password. ~ PingPong would receive commands through an ICMP request to set a TCP reverse shell to an IP address and port specified in the packet.

" If connectivity to the IP address fails, the script executes the SGSN emulator in a loop, attempting to connect to a set of nine pairs of International Mobile Subscriber Identity and Mobile Subscriber Integrated Services Digital Network numbers that are used as arguments to the SGSN emulator; These numbers identify specific mobile devices, or mobile stations, for the SGSN emulator to create tunnels to. This process generates Packet Data Protocol context requests for mobile stations with the IMSI/MSISDN number pairs until a connection is established. ~ SIGTRANslator - an ELF binary that can send and receive data via telecommunication-specific protocols ~ While there is no attribution from neither Mandiant nor CrowdStrike, the latter found a clue suggesting that the developer of SIGTRANslator has some knowledge of the Chinese language. Credit: LightBasin hacking group breaches 13 global telecoms in two years (bleepingcomputer.com)



VICTIMOLOGY
- Country
  - Iraq, Italy, New Zealand, Philippines, South Africa, United Kingdom of Great Britain and Northern Ireland, United States of America
- Industry
  - Financial Services, Legal & Professional Services, Manufacturing, Retail, Telecommunications

LightBasin aka UNC1945

OPERATIONS

- Aside from using legit CIDR and IPV4, malware and CVEs are also being exploited by the threat actor.

  - STEELCORGI is a packer for Linux ELF programs that uses key material from the executing environment to decrypt the payload.

  - SLAPSTICK is a Linux Pluggable Authentication Module (PAM) with a backdoor that grants a user with a secret, hardcoded password access to the system.

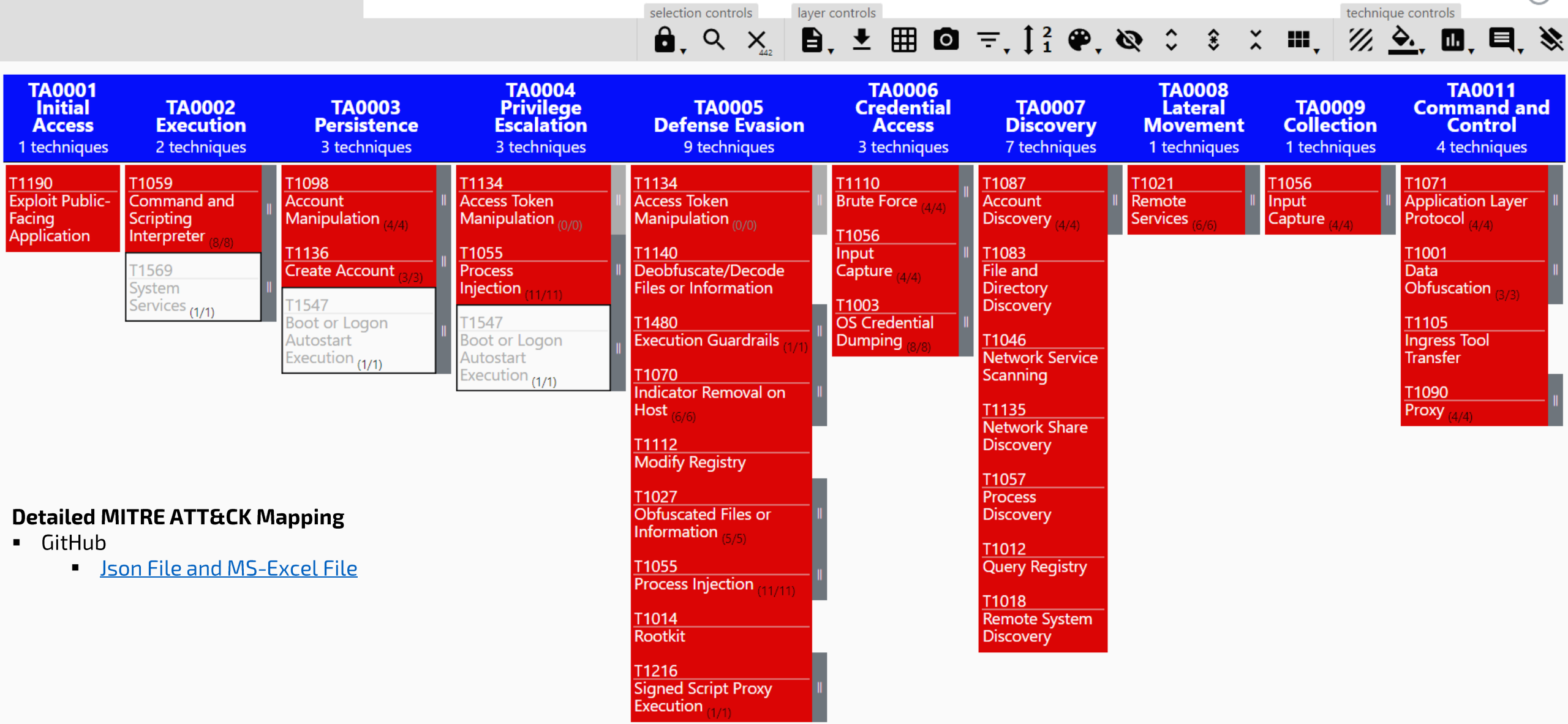
  - EVILSUN is a remote exploitation tool that gains access to Solaris 10 and 11 systems of sparc or i386 architecture using a vulnerability exposed by SSH keyboard-interactive authentication. The remote exploitation tool makes SSH connections to hosts passed to it on the command line. The default port is the normal ssh port (22) but this may be overridden. EVILSUN passes the banner string SSH-2.0-Sun_SSH_1.1.3 over the connection in clear text as part of handshaking.

  - BINBASH
  - CAKETAP
  - EVILSUN
  - LEMONSTICK
  - LOGBLEACH
  - OPENSHACKLE
  - SLAPSTICK
  - STEELCORGI
  - STEELHOUND
  - SUN4ME
  - TINYSHELL
  - WIPERIGHT

  - CVE-2020-14871 – Vulnerability in the Oracle Solaris product of Oracle Systems (component: Pluggable authentication module).
  - CVE-2020-14781 – Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI).

LightBasin aka UNC1945

TACTICS, TECHNIQUES, & PROCEDURES (High-Level)



Detailed MITRE ATT&CK Mapping

- GitHub
  - Json File and MS-Excel File

LightBasin aka UNC1945

INDICATORS OF COMPROMISE

INDICATOR TYPE	INDICATOR
CIDR	139.162.156.0/24
CIDR	167.179.91.0/24
CIDR	172.104.129.0/24
CIDR	172.104.236.0/24
CIDR	172.104.79.0/24
CIDR	207.148.24.0/24
CIDR	45.32.116.0/24
CIDR	45.33.77.0/24
CIDR	45.76.215.0/24
FileHash-MD5	3a5a7ced739923f929234beefcef82b5
FileHash-SHA1	9728cd06b3e5729aff1a146075d524c34c5d51df
FileHash-SHA256	05537c1c4e29db76a24320fb7cb80b189860389cdb16a9dbeb0c8d30d9b37006
FileHash-SHA256	16294086be1cc853f75e864a405f31e2da621cb9d6a59f2a71a2fca4e268b6c2
FileHash-SHA256	3a259ad7e5c19a782f7736b5ac50aac4ba4d03b921ffc6a3ff6a48d720f02012
FileHash-SHA256	4480b58979cc913c27673b2f681335deb1627e9ba95073a941f4cd6d6bcd6181
FileHash-SHA256	4668561d60daeb7a4a50a9c3e210a4343f92cadbf2d52caab5684440da6bf562
FileHash-SHA256	65143ccb5a955a22d6004033d073ecb49eba9227237a46929495246e36eff8e1
FileHash-SHA256	6d3759b3621f3e4791ebcd28e6ea60ce7e64468df24cf6fddf8efb544ab5aec0
FileHash-SHA256	78c579319734a81c0e6d08f1b9ac59366229f1256a0b0d5661763f6931c3b63c
FileHash-SHA256	917495c2fd919d4d4baa2f8a3791bcfd58d605ee457a81feb52bc65eb706fd62
FileHash-SHA256	97d4c9b5750d614face73d11ba8532e53594332af53f4c07c1543195225b76eb
FileHash-SHA256	9973edfef797db84cd17300b53a7a35d1207d166af9752b3f35c72b4df9a98bc
FileHash-SHA256	a388e2ac588be6ab73d7e7bbb61d83a5e3a1f80bf6a326f42b6b5095a2f35df3
FileHash-SHA256	ad9fef1b86b57a504cfa1cfbda2e2ac509750035bff54e1ca06f7ff311d94689
FileHash-SHA256	b06f52e2179ec9334f8a3fe915d263180e538f7a2a5cb6ad8d60f045789123b6
FileHash-SHA256	bf5806cebc5d1a042f87abadf686fb623613ed33591df1a944b5e7879fb189c8
FileHash-SHA256	c5ddd616e127df91418aeaa595ac7cd266ffc99b2683332e0f112043796ede1d
FileHash-SHA256	cdf230a7e05c725a98ce95ad8f3e2155082d5a6b1e839c2b2653c3754f06c2e7
FileHash-SHA256	e9c0f00c34dcd28fc3cc53c9496bff863b81b06723145e106ab7016c66581f72

Full List Here

- GitHub
  - Indicators of Compromise (IOCs)

LightBasin aka UNC1945

MITIGATION

- XDR Solution for anomalous Network, Endpoint, and User Behaviour
- IEC62443 for Network Segmentation
- CIS Benchmark for OS and Application Hardening
- Basic Hygiene for Asset Visibility and Patch Management
- Vulnerability Scanning
- Application Code Scanning and Signing
- Application Whitelisting
- Data Back-Up (3-2-1-1 Rule)

GOVERNANCE, RISK, & COMPLIANCE

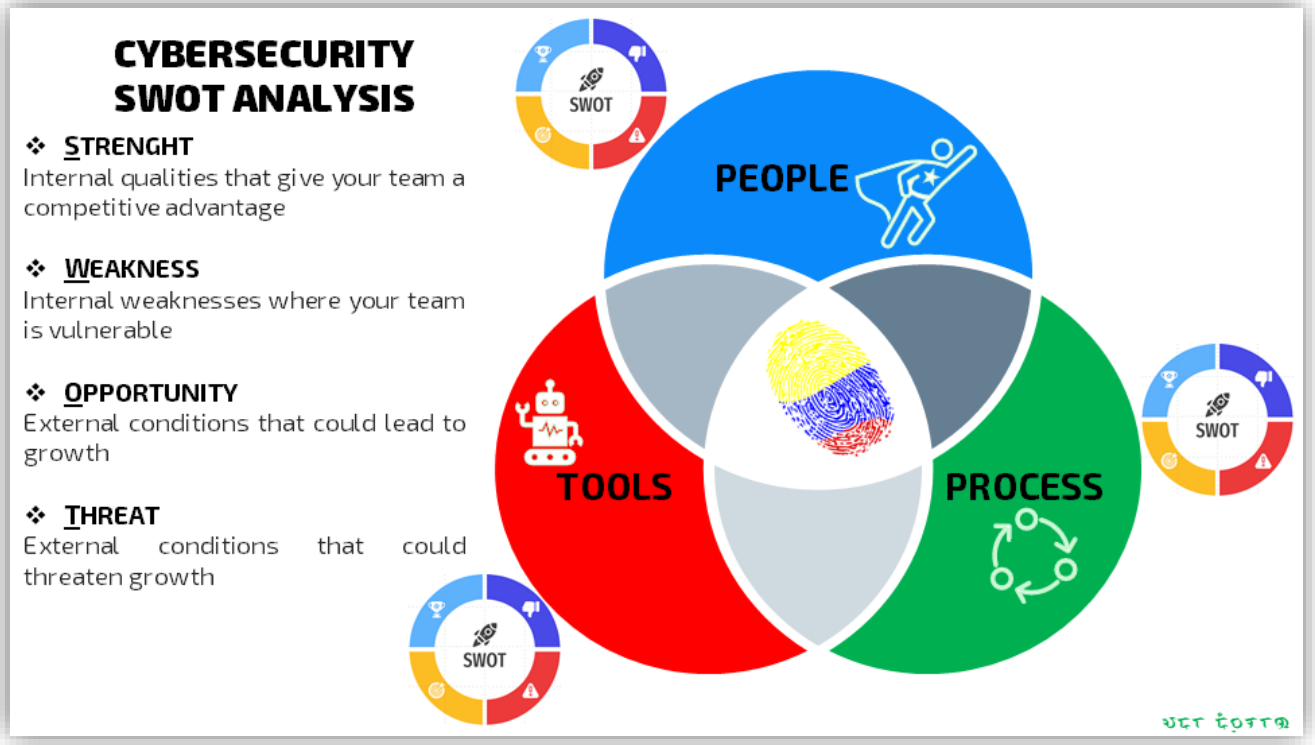
- Basic Policies
  - Physical Access Policy
  - BYOD Policy
  - Acceptable Usage Policy
  - Password Policy
  - Device Control Policy

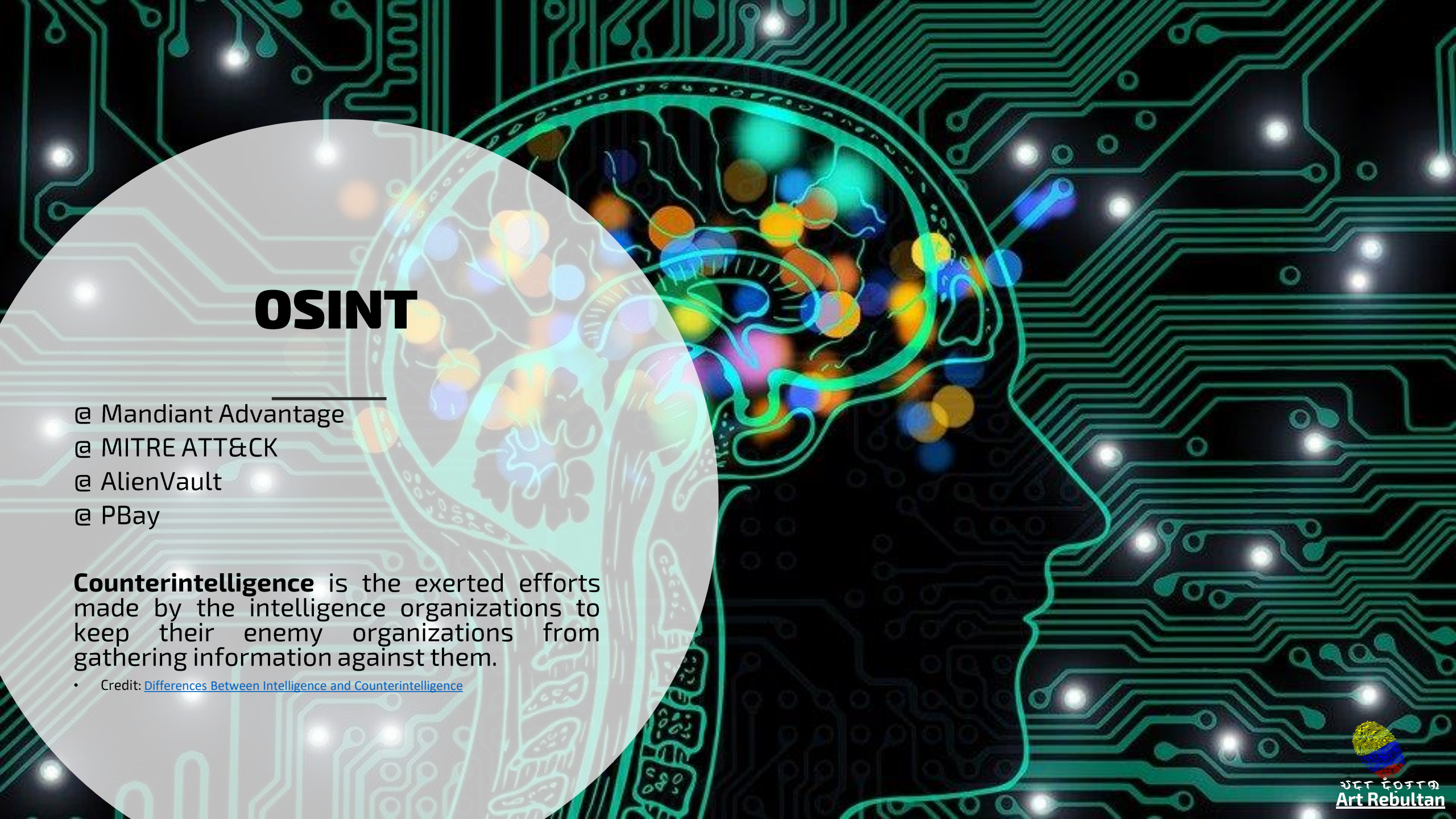
DETECTION & THREAT HUNTING

- Leaving of the Land Binaries and Scripts (LoLBAS)
- Anomalous Network Activities and Exfiltrations
- Assume Breach Threat Hunting for Internal and External

PEOPLE

- Continuous Training and User Awareness
- Hacker's Mindsets for SOC and DFIR





OSINT

@ Mandiant Advantage
@ MITRE ATT&CK
@ AlienVault
@ PBay

Counterintelligence is the exerted efforts made by the intelligence organizations to keep their enemy organizations from gathering information against them.

- Credit: Differences Between Intelligence and Counterintelligence