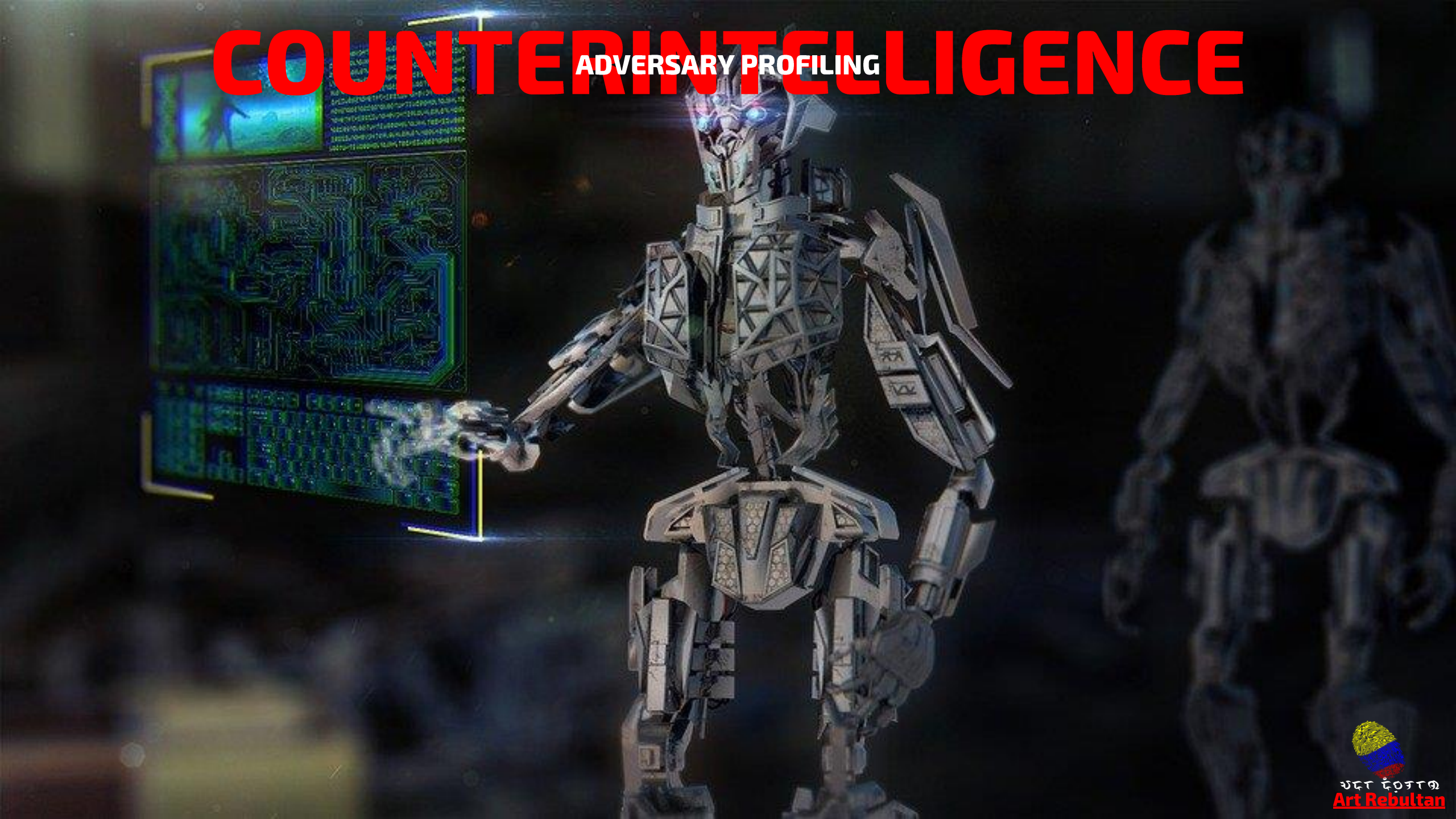
COUNTERINTELLIGENCE

ADVERSARY PROFILING



Art Rebultan

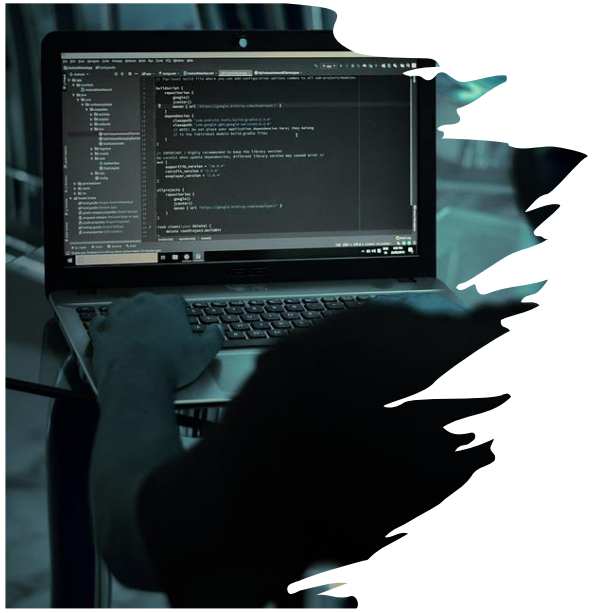
APT29 aka COZYBEAR

PROFILE
APT29 is a cyber espionage actor with a Russia nexus. Historically, targets have included Western governments, foreign affairs and policymaking bodies, government contractors, universities, and possibly international news outlets. Based on available data, we assess that APT29 is a nation-state-sponsored group located in Russia. The group appears to have formidable capabilities, to include a range of custom developed tools, extensive command and control (C2) infrastructure that includes compromised and satellite infrastructure (via apparent service providers), and significant operational security. In investigations we worked where APT29 was present, they demonstrated a high regard for operational security but were also fairly aggressive in their continued operations and efforts to evade investigators and remediation attempts.

- Aliases/Associations
  - Dukes, Group 100, Cozy Duke, CozyDuke, EuroAPT, CozyBear, CozyCar, Cozer, Office Monkeys, OfficeMonkeys, APT29, Cozy Bear, The Dukes, Minidionis, SeaDuke, Hammer Toss, YTTRIUM, Iron Hemlock, Grizzly Steppe

SUMMARY
This campaign shares all the signs of Nobelium's approach to compromising a significant list of targets by breaching their service provider. Just as in previous attacks, the Russian state hackers used a diverse and ever-changing toolkit, including a long list of tools and tactics ranging from malware, password sprays, and token theft to API abuse and spear phishing. The main targets of these new attacks are resellers and technology service providers that deploy and manage cloud services and similar tech for their customers. Microsoft notified impacted targets of the attacks after spotting them and also added detections to their threat protection products enabling those targeted in the future to spot intrusion attempts. ~ As Burt added, in all, more than 600 Microsoft customers were attacked thousands of times, although with a very low rate of success between July and October. ~ "Between July 1 and October 19 this year, we informed 609 customers that they had been attacked 22,868 times by Nobelium, with a success rate in the low single digits". ~ A command-and-control backdoor dubbed 'GoldMax,' an HTTP tracer tool tracked as 'GoldFinder,' a persistence tool and malware dropper named 'Sibot.' ~ A malware downloader known as 'BoomBox,' a shellcode downloader and launcher known as 'VaporRage,' a malicious HTML attachment dubbed 'EnvyScout,' and a loader named 'NativeZone'.

Credit: [Microsoft: Russian SVR hacked at least 14 IT supply chain firms since May (bleepingcomputer.com)]



VICTIMOLOGY
- Country
  - Australia, Austria, Canada, Denmark, France, Germany, Hong Kong, Israel, Italy, Jordan, Liechtenstein, Netherlands, New Zealand, Philippines, Qatar, Singapore, South Africa, Sweden, Switzerland, United Arab Emirates, United Kingdom, United States of America

- Industry
  - Aerospace & Defense, Automotive, Chemicals & Materials, Civil Society & Non-Profits, Construction & Engineering, Education, Energy & Utilities, Financial Services, Governments, Healthcare, Hospitality, Insurance, Legal & Professional Services, Manufacturing, Media & Entertainment, Oil & Gas, Pharmaceuticals, Retail, Technology, Telecommunications, Transportation

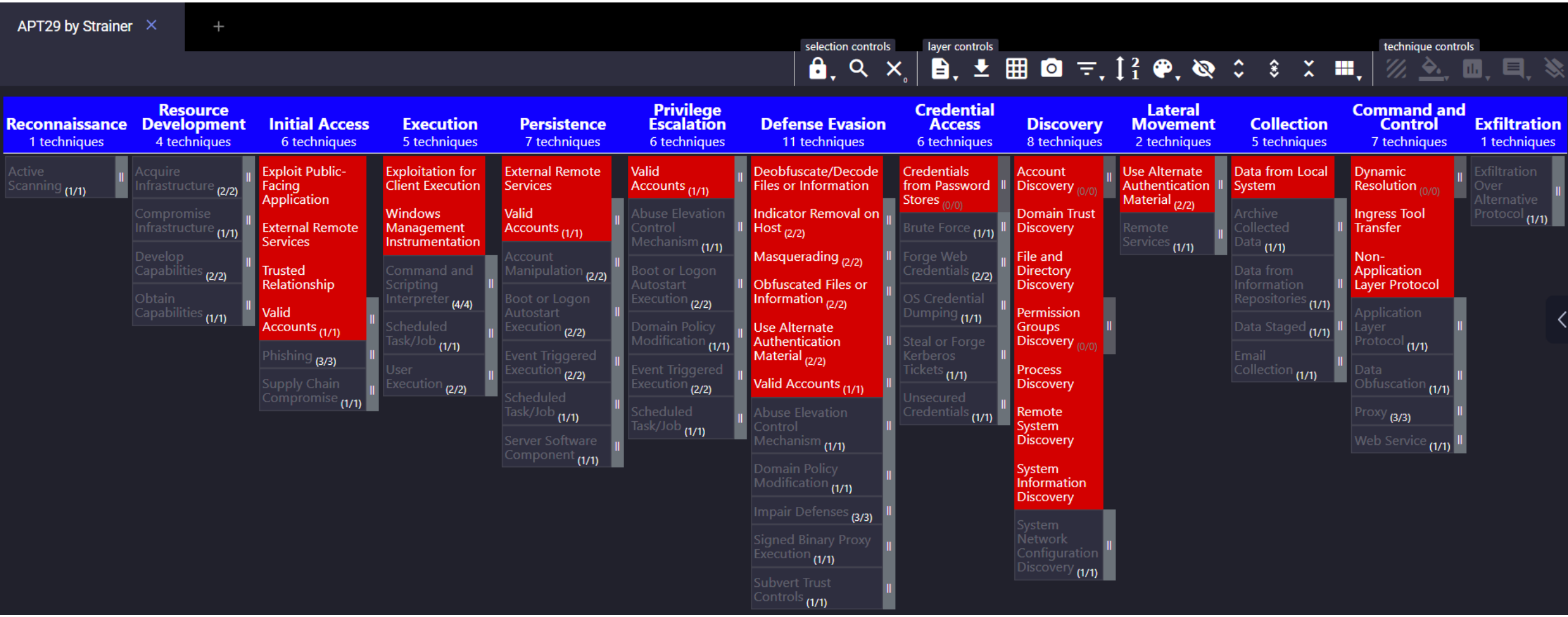
APT29 aka COZYBEAR

OPERATIONS

- Associated Malware
  - ELF.WELLMAIL
  - ELF.WELLMESS
  - PS1.POSHSPY
  - WIN.ATI_AGENT
  - WIN.CLOUD_DUKE
  - WIN.FATDUKE
  - WIN.LITEDUKE
  - WIN.MINIDUKE
  - WIN.ONIONDUKE
  - WIN.POLYGLOTDUKE
  - WIN.POWERDUKE
  - WIN.SEADADDY
  - WIN.SOREFANG
  - WIN.TDISCOVERER
  - WIN.COBALT_STRIKE
- Exploited Vulnerabilities
  - CVE-2020-0688
  - CVE-2020-1472
  - CVE-2021-1879
  - CVE-2021-21166
  - CVE-2021-30551
  - CVE-2021-34527
  - CVE-2018-13379
  - CVE-2019-0708
  - CVE-2019-11510
  - CVE-2020-1350
  - CVE-2020-14882
  - CVE-2020-5902
  - CVE-2021-26855
  - CVE-2021-33742
  - CVE-2019-19781
  - CVE-2019-2725
  - CVE-2019-7609
  - CVE-2019-9670
  - CVE-2020-4006
  - CVE-2021-21972
  - CVE-2019-13379
  - CVE-2020-13169
  - CVE-2019-1653

APT29 aka COZYBEAR

TACTICS, TECHNIQUES, & PROCEDURES (High-Level)



Detailed MITRE ATT&CK Mapping

- GitHub
  - Json File and MS-Excel File

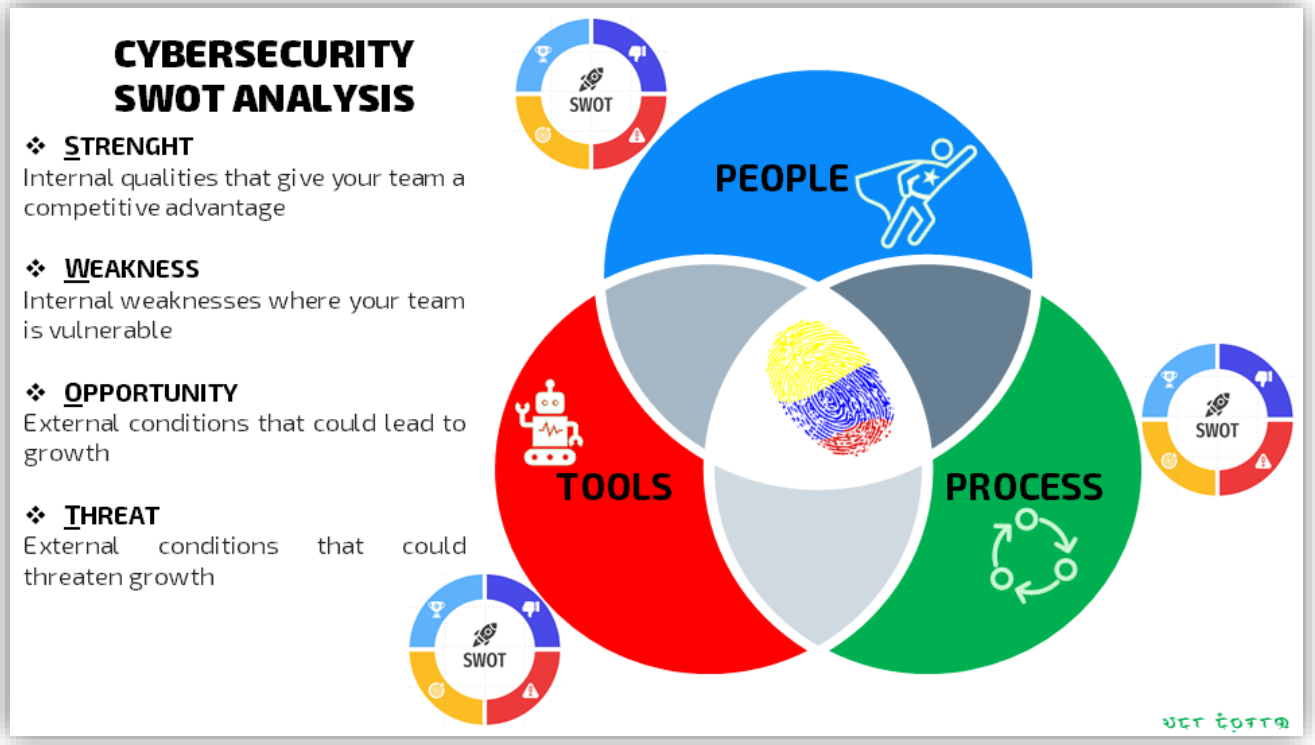
APT29 aka COZYBEAR

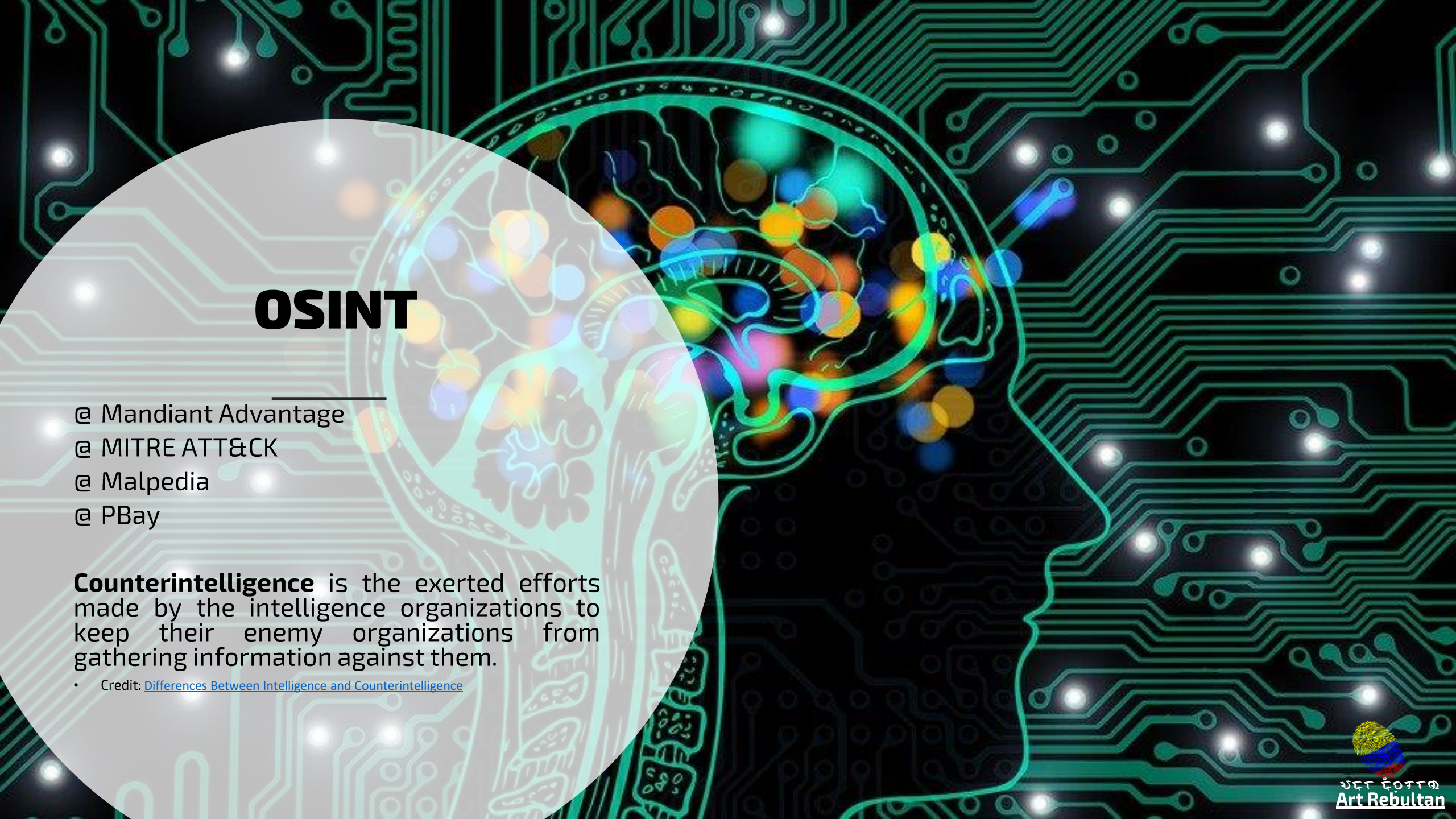
MITIGATION
- Patch Exploited CVEs
- Exploit Protection
- IEC62443 Standard for Network Segmentation
- Leverage Threat Intelligence Provider
- Vulnerability Scanning
- CIS Benchmark for OS and Application Hardening
- Application Code Scanning and Signing
- Application Whitelisting
- Data Back-Up (3-2-1-1 Rule)

GOVERNANCE, RISK, & COMPLIANCE
- Ensure 3rd Party Policy In Place
  - Security Assessment Questionaire
- Privileged Account Management

DETECTION & THREAT HUNTING
- Leaving of the Land Binaries and Scripts (LoLBAS)
- Anomalous Network Activities and Exfiltrations
- Assume Breach Threat Hunting

PEOPLE
- Continuous Training and User Awareness
- Proactive Mindsets for SOC and DFIR





OSINT

@ Mandiant Advantage
@ MITRE ATT&CK
@ Malpedia
@ 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