



**MEDIA + ENTERTAINMENT**  
**INFORMATION SHARING ANALYSIS CENTER**

---

# **ADVANCED PERSISTENT THREATS**

## **WHAT ARE THEY AND WHY SHOULD YOU CARE?**



**MEDIA + ENTERTAINMENT  
INFORMATION SHARING ANALYSIS CENTER**

**An ISAC is a member-driven non-profit organization that serves as the focal point for collection, analysis, and dissemination of risk and threat information among its members.**

# ME-ISAC SERVICES

Provides a means of communication and collaboration on risks, threats, and incident data



## Threat Intel Fusion Center

Analysts provide daily tactical info to inform security teams and tools in order to build a proactive defensive posture in members



## Research + Analysis

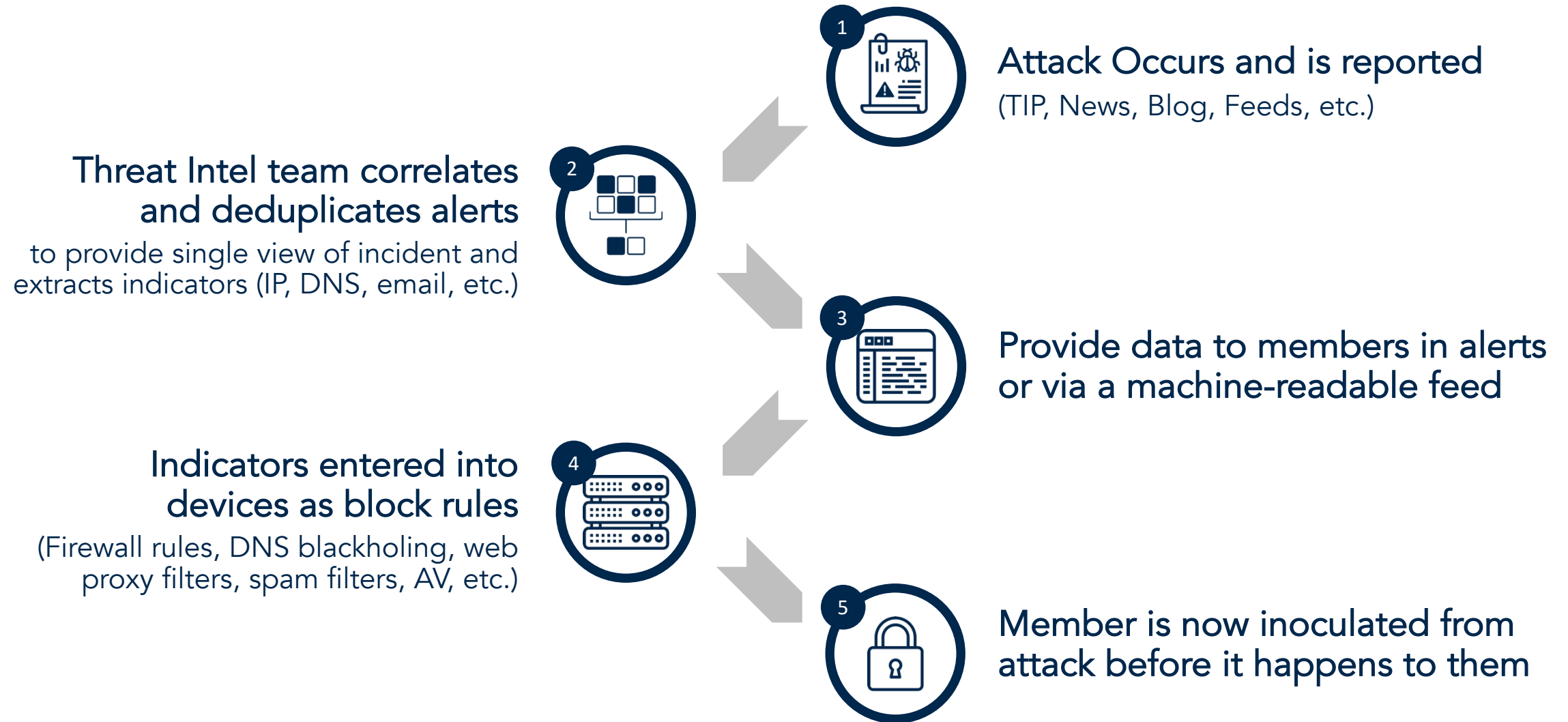
Analysts provide strategic trending, statistics, and summaries of industry-specific threat information



## Training + Outreach

Analysts provide industry-specific custom training, and cooperative purchasing of commercial training for members

# THREAT INTEL PROACTIVE DEFENSE





**MEDIA + ENTERTAINMENT**  
**INFORMATION SHARING ANALYSIS CENTER**

**APT GROUPS**

# APT

- Advanced – Skilled attackers. Methodology, not necessarily tools.
- Persistent – Determined, targeted, will return.
- Threat – Person (not a piece of malware).
- Refers to when the same attacker returns to multiple or same targets for specific purpose.
  - These are targeted attacks.
  - Tend to follow a specific MO.
  - Attacker has a specific purpose.
- Frequently uses simple tools and techniques,
  - until less simple tools are needed.

# APT ORIGINS


- Term coined by Air Force in 2006 as a way to talk at unclassified levels about specific classified threats
- Gained public use in 2008-2009
- Made headlines in 2010 when Google announced Operation Aurora, code name for a series of data breaches at Google, Adobe, and many others
- Even more headlines in 2013 when Mandiant released their APT-1 report attributing Aurora to China
- Definition grew from referring to a specific threat to meaning any of a growing list of similar threats
  - List of active APTs constantly growing, currently >430

# COMMON APT GROUPS

- What follows is NOT a complete list; just some that are notable
- Some groups are state sponsored
  - The actors are employed by military or intel agencies
  - Actions taken are generally espionage or warfare
- Some groups are organized crime
  - The actors may be from or affiliated with a particular country
  - Often the groups are multi-national
  - Actions taken are generally financially motivated
- Sometimes groups do both, e.g. North Korean military robs banks




# GRU UNIT 26165

- **AKA:** APT 28 (Mandiant), ATK 5 (Thales), Fancy Bear (CrowdStrike), Group 74 (Talos), Iron Twilight (SecureWorks), ITG05 (IBM), Pawn Storm (Trend Micro), Sednit (ESET), SIG40 (NSA), Snakemackerel (iDefense), Sofacy (Kaspersky), Strontium (Microsoft), Swallowtail (Symantec), T-APT-12 (Tencent), TAG-0700 (Recorded Future), TG-4127 (SecureWorks), Tsar Team (iSight), UAC-0028 (CERT-UA), and Grizzly Steppe (USG) when working together with APT 29 / Cozy Bear
- **Country:** Russia 
- **Attribution:** General Staff, Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS) military unit 26165
- **First Seen:** 2004
- **Description:** State-sponsored threat group associated with Russia's military intelligence responsible for espionage collection against hundreds of targets.

# GRU UNIT 26165

- Notable Incidents:
  - 2011 series of breaches using the sofacy and miniduke malware
  - 2015 Death threats against military wives
  - 2015 Breach of France's TV5Monde
  - 2015 Breaches of German and French parliaments, Bellingcat journalists, White House, NATO,...
  - 2016 Breach of DNC email server and released emails via Wikileaks
  - 2018 series of breaches to influence the Brexit vote
  - 2020 series of breaches to influence the US Presidential election
  - 2014-2022 series of breaches of various Ukrainian government sites
- Tools:
  - Cannon, certutil, Computrace, CORESHELL, DealersChoice, Dwndelph, Drovorub, Foozer, Graphite, HIDEDEV, JHUHUGIT, Koadic, Komplex, LoJax, Mimikatz, Nimcy, OLDBAIT, PocoDown, ProcDump, PythocyDbg, Responder, Sedkit, Sedreco, SkinnyBoy, USBStealer, VPNFilter, Winexe, WinIDS, X-Agent, X-Tunnel, Zebrocy, Living off the Land

# PLA UNIT 61398

- **AKA:** APT 1 (Mandiant), BrownFox (Symantec), Byzantine Candor (USG), Byzantine Hades (USG), Comment Crew (Symantec), Comment Panda (CrowdStrike), GIF89a (Kaspersky), Group 3 (Talos), Shanghai Group (SecureWorks), TG-8223 (SecureWorks)
- **Country:** China 
- **Attribution:** 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398
- **First Seen:** 2006
- **Description:** State-sponsored cyber espionage unit linked to Chinese military responsible for data breaches at hundreds of companies across almost every sector and in dozens of countries.

# PLA UNIT 61398


- Notable incidents:

- 2006 Operations ShadyRAT and Seasalt breached over 140 targets including defense contractors, businesses, the United Nations, and the Intl Olympic Committee
- 2009 Operation Aurora breaches of Google, Morgan Stanley, Adobe, Akamai, Juniper, Rackspace, Yahoo!, Symantec, and many more
- 2009 Operation GhostNet breach of embassies, foreign ministries, government offices of over 103 countries
- 2011 Breach of RSA, stole source code to MFA tokens
- 2014 Operation Siesta breaches of victims across a wide range of industries

- Tools:

- Auriga, bangat, BISCUIT, Bouncer, Cachedump, CALENDAR, Combos, CookieBag, Dairy, GDOCUPLOAD, GetMail, GLASSES, GLOOXMAIL, GOGGLES, GREENCAT, gsecdump, Hackfase, Helauto, Kurton, LIGHTBOLT, LIGHTDART, LONGRUN, Lslsass, ManItsMe, MAPiget, Mimikatz, MiniASP, NewsReels, Oceansalt, Pass-The-Hash Toolkit, Poison Ivy, ProcDump, pwddump, Seasalt, ShadyRAT, StarsyPound, Sword, TabMsgSQL, Tarsip, WARP, WebC2, Living off the Land

# BUREAU 121

- **AKA:** APT-C-26 (Qihoo 360), ATK 3 (Thales), CTG-6459 (SecureWorks), Group 77 (Talos), Hastati Group (SecureWorks), Hidden Cobra (Trend Micro), ITG03 (IBM), Labyrinth Chollima (CrowdStrike), Lazarus Group (Kaspersky), NewRomanic Cyber Army Team (McAfee), Nickel Gladstone (SecureWorks), Plutonium (Microsoft), SectorA01 (ThreatRecon), Stonefly (Symantec), T-APT-15 (Tencent), TA404 (Proofpoint), Whois Hacking Team (McAfee), Zinc (Microsoft), and closely associated with APT 37 (Mandiant), APT 38 (Mandiant), BeagleBoyz (USG), Bluenoroff (Kaspersky), Silent Chollima (CrowdStrike), Stardust Chollima (CrowdStrike)
- **Country:** North Korea 
- **Attribution:** Korean People's Army, General Staff Department, Reconnaissance General Bureau, Bureau 121
- **Active Since:** 2007
- **Description:** State-sponsored military intelligence unit that conducts espionage and attacks against both government and civilian targets. Notable for conducting financially-motivated criminal heists to steal money

# BUREAU 121


- Notable Incidents:

- 2007 Operation Flame targets South Korean government
- 2009 Operation Troy targets SK and US: White House, Blue House, Stock Exchange, banks, ...
- 2013 Operation DarkSeoul targets SK banks and at least three broadcasters
- 2014 Operation Blockbuster attack on Sony Picture
- 2016 theft of \$101 million from Bangladesh Bank via SWIFT
- 2017 release of WannaCry ransomware
- 2018 theft from several cryptocurrency exchanges
- 2022 theft of \$625 million in NFT from Axie Infinity video game

- Tools:

- AppleJeus, BanSwift, BTC Changer, Concealment Troy, Dacls RAT, DarkComet, Destover, DoublePulsar, Dtrack, DyePack, EternalBlue, Gh0st RAT, Hermes, HotelAlfa, HtDnDownloader, Http Dr0pper, HTTP Troy, KillDisk, Lazarus, MagicRAT, Mimikatz, Mydoom, OpBlockBuster, PowerShell RAT, PowerSpritz, Quickcafe, Romeo, SheepRAT, Tdrop, TFlower, ThreatNeedle, TigerRAT, Troy, WannaCry, WbBot, WolfRAT, Wormhole, Living off the Land, and a bunch more

# GRU UNIT 74455

- **AKA:** Sandworm Team (Trend Micro), Sandworm (ESET), Iron Viking (SecureWorks), CTG-7263 (SecureWorks), Voodoo Bear (CrowdStrike), Quedagh (F-Secure), TEMP.Noble (FireEye), ATK 14 (Thales), BE2 (Kaspersky), UAC-0082 (CERT-UA), UAC-0113 (CERT-UA), DCLeaks, Guccifer2.0
- **Country:** Russia 
- **Attribution:** General Staff, Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS) military unit 74455
- **First Seen:** 2009
- **Description:** State-sponsored threat group associated with Russia's military intelligence responsible for espionage and attacks on several high-profile victims.

# GRU UNIT 74455

- Notable Incidents:
  - 2009 attacks on Georgia preceding Russian invasion
  - 2014 attacks on Ukraine, NATO, and other western European gov orgs
  - 2015 widespread power outages in Ukraine
  - 2017 NotPetya attacks targets Ukraine, hits France, Germany, Italy, Poland, UK, US, Australia, ...
  - 2018 compromise of Winter Olympics and Paralympics
  - 2018 use of VPNFilter malware in widespread attack home routers and other network devices
- Retribution:
  - 2020 DOJ indicts six GRU officers responsible for above attacks
  - 2022 DOJ disrupts botnet controlled by this group
- Tools:
  - ArguePatch, AWFULSHRED, BlackEnergy, CaddyWiper, Colibri Loader, Cyclops Blink, DanaBot, DarkCrystal RAT, Gcat, Industroyer, Industroyer2, ORCSHRED, P.A.S., PassKillDisk, PsList, SOLOSHRED, VPNFilter, Warzone RAT, Living off the Land






# EVIL CORP


- AKA: Dridex, Indrik Spider (Crowd Strike), UNC2165 (Mandiant), Gold Drake (Secureworks)
- Country: Russia 🇷🇺
- Active Since: 2009
- Description:
  - Russian-based operator of Zeus, Bugat, and Dridex banking trojans and BitPaymer ransomware
  - Originated the Ransomware-as-a-Service model of recruiting affiliate attackers
- Retribution:
  - US DOJ offering \$5M for info leading to arrests (largest offer for cyber)
  - US DOJ has indicted Maksim Yakubets (pictured) and several others
- Tools:
  - BitPaymer, Bugat, Cobalt Strike, Covenant, Donut, DoppelPaymer, Dridex, Grief, Hades, Koadic, LockBit, Macaw Locker, Mimikatz, Payload.Bin, PhoenixLocker, PowerShell Empire, PowerSploit, SocGholish, WastedLocker, Zeus




# RYUK / CONTI

- AKA: Trickbot, Wizard Spider (CrowdStrike), Gold Blackburn (SecureWorks), Gold Ulrick (SecureWorks), ITG23 (IBM); Associated with TEMP.MixMaster (FireEye), Grim Spider (CrowdStrike), UNC1878 (Mandiant)
- Country: Russia , Ukraine , and Kurdistan 
- Active Since: 2014 inactive since 2021
- Description:
  - Russia-based operator of the TrickBot, used to deploy Ryuk and Conti ransomware
  - Trickbot is distributed by a variety of malware operated by other affiliated groups.
  - Software programmed to not install if IP is in Russia or if system is set to Russian language
- Tools:
  - AdFind, Anchor, BazarBackdoor, BloodHound, Cobalt Strike, Conti, Diavol, Dyre, Gophe, Invoke-SMBAutoBrute, LaZagne, LightBot, PowerSploit, PowerTrick, PsExec, Ryuk, SessionGopher, Sidoh, TrickBot, TrickMo, Upatre


# REvil

- AKA: Sodinokibi, Sodin, ATK168 (Thales), Pinchy Spider (CrowdStrike), Gold Southfield (Secureworks)
- Country: Russia 
- Active Since: 2018 Inactive since July 2021
- Description:
  - Operates REvil ransomware-as-a-service through affiliates
  - Took over GandCrab from Gold Garden
- Notable Incidents:
  - Breach of celebrity law firm; released data on Trump, Lady Gaga, others
  - JBS meat packing plant breach, resulted in food shortages
  - Kasaya VSA, supply chain breach that affected hundreds of victims
- Retribution: Under extreme pressure from US, EU, INTERPOL, Russia arrested five
- Tools: REvil, Privilege Escalation, PowerShell, Sodinokibi, MinerGate, XMRig, RIG Exploit Kit

# LOCKBIT

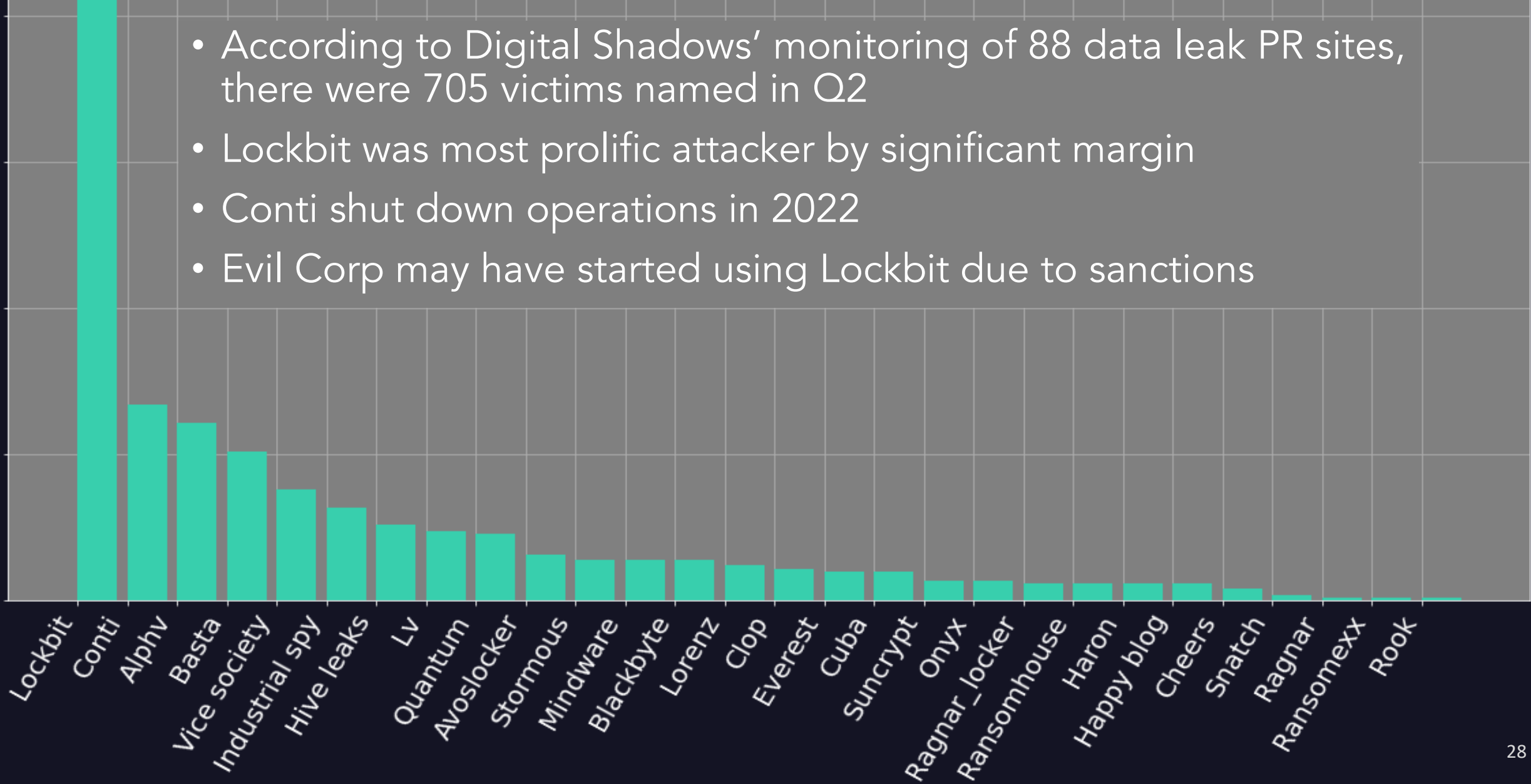
- AKA: ABCD, Bitwise Spider (CrowdStrike), Gold Mystic (Secureworks), Water Selkie (Trend Micro)
- Country: Russia 
- Active Since: 2019
- Description:
  - Operate Lockbit ransomware-as-a-service (RaaS) and Initial Access Broker (IAB) businesses
  - Uses automated processes for rapid spreading and antifoensics tactics to evade detection
  - Runs a bug bounty program where people get paid to improve their ransomware
- Tools:
  - Cobalt Strike, CrackMapExec, EmpireProject, Hackops Keylogger, LockBit, Mega, Metasploit, Mimikatz, PsExec, Powershell Empire, Process Hacker, StealBit, UACme

# ALPHV

- AKA: BlackCat, Noberus, Alpha Spider (CrowdStrike), Gold Blazer (Secureworks), White Dev 101 (PWC)
- Country: Russia 
- Active Since: 2021
- Description:
  - Operates the ALPHV ransomware and ransomware-as-a-service affiliate network
  - To maximize pain, can delete snapshots, stop processes, and stop virtual machines
  - Gains access via target's VPN when not stopped by MFA
  - Self propagates using psexec to speed up and automate spreading on target
- Tools:
  - BlackCat, GO Simple Tunnel, LaZagne, MEGAsync, Mimikatz, PsExec, WebBrowserPassView

# DATA LEAK SITE LISTINGS IN Q2 2022

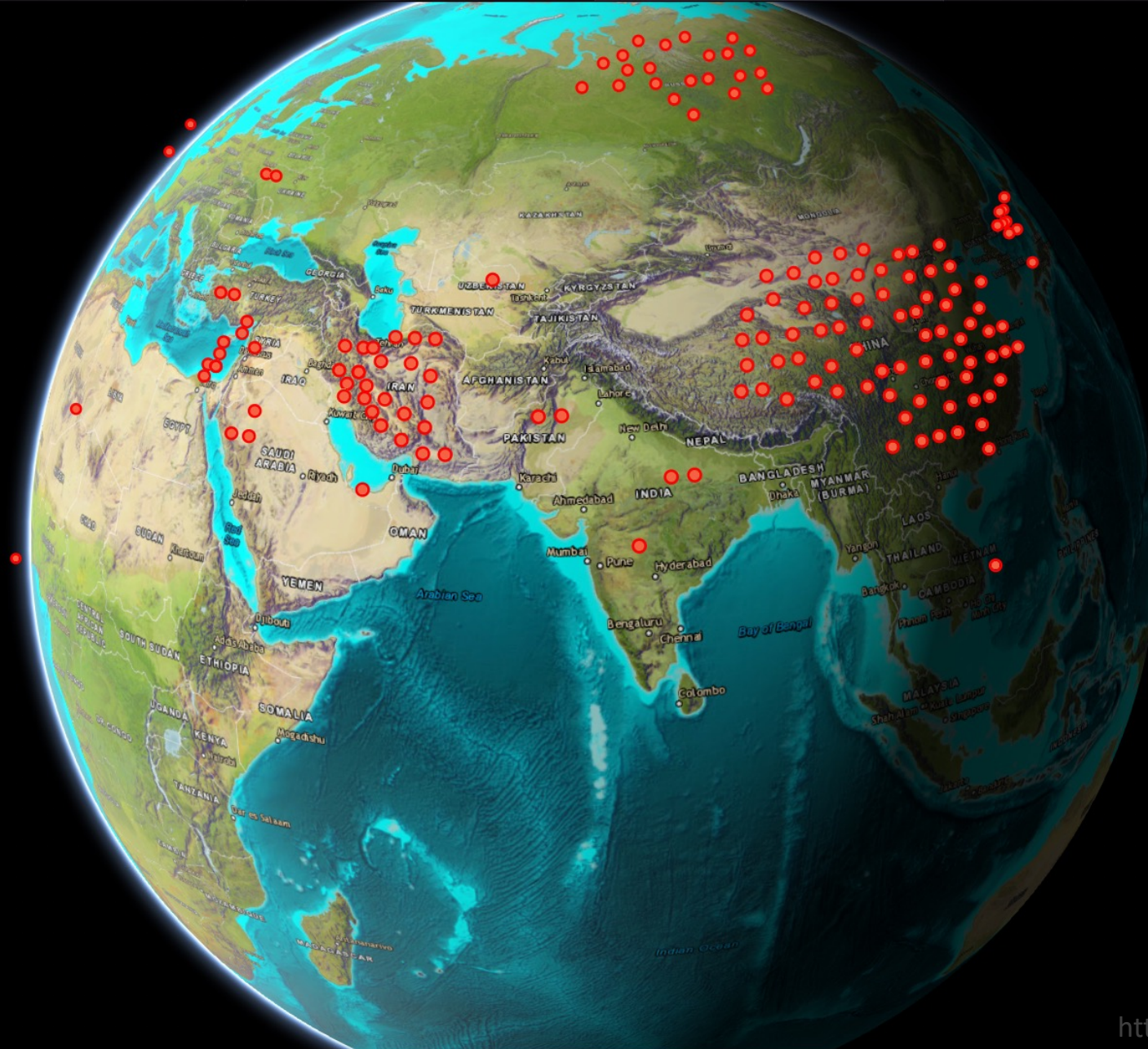
- According to Digital Shadows' monitoring of 88 data leak PR sites, there were 705 victims named in Q2
- Lockbit was most prolific attacker by significant margin
- Conti shut down operations in 2022
- Evil Corp may have started using Lockbit due to sanctions





Other APTs not in map

Search



About APTMAP

Esri, HERE, Garmin

<https://andreacristaldi.github.io/APTmap>

Powered by Esri



**MEDIA + ENTERTAINMENT**  
**INFORMATION SHARING ANALYSIS CENTER**

Chris Taylor

<https://meisac.org>

[info@meisac.org](mailto:info@meisac.org)