THREAT INTELLIGENCE

WHAT IS A THREAT?

Cybersecurity threats are **acts** performed by **individuals** with **harmful intent**, whose goal is to **steal data**, **cause damage** to or **disrupt** computing systems.

Common categories of cyber threats include **malware**, **social engineering**, man in the middle (**MitM**) attacks, denial of service (**DoS**), and injection attacks

APT – ADVANCE PERSISTENT THREAT

An advanced persistent threat (APT) is an attack or state-sponsored group that occurs when an unauthorized user utilizes advanced and sophisticated techniques to gain access to a system or network. Phishing, ransomware, malware, and data breaches are common techniques used by APTs to attack their targets.

TOP APT TEAMS

Lazarus Group

- AKA: APT38, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team, Hidden Cobra
- Targets: Bitcoin exchanges, Cryptocurrency, and Sony Corp; South Korea, United States, Australia, Germany, Guatemala, Hong Kong, India, Israel, Japan Russia, Mexico
- Techniques/Tools: Bankshot, DDoS, EternalBlue, Mimikatz, Bankshot, Http Troy, PowerShell RAT
- Significant Attack: 2014 Sony Pictures Hack, Operation Troy, WannaCry Software, Covid-19 Spear Phishing, New Mac variant of Lazarus Dacis RAT distributed
- Location: North Korea

UNC2452

- AKA: Dark Halo, Nobelium, SilverFish, StellarParticle
- Targets: SolarWinds, Pentagon, United Kingdom Government, European Parliament
- Techniques/Tools: Supply chain attack
- Significant Attack: SolarWinds Orion software attack
- Location: Unknown

Equation Group

- AKA: Tilded Team
- Targets: Afghanistan, Iran, India, Mali, Pakistan, Syria
- Techniques/Tools: DoublePulsar, EQUATIONDRUG, FANNY, Lambert, Regin, GRAYFISH, Duqu, Flame
- Significant Attack: iOS exploit 2020
- Location: United States

Wizard Spider

- AKA: Grim Spider, Gold Blackburn
- Targets: Defense, financial, government, and telecommunications sectors; worldwide
- Techniques/Tools: AdFind, Anchor, BazarBackdoor, BloodHound, Cobalt Strike, Dyre, Gophe, Invoke SMBAutoBrute, LaZagne, PowerSploit, PowerTrick, Ryuk, SessionGopher, TrickBot, TrickMo, Upatre
- Significant Attack: Trickbot campaigns in Italy targeting COVID-19
- Location: Russia

Carbanak

- AKA: Anunak, Carbon Spider
- Targets: Australia, Austria, Brazil, Bulgaria, Canada, China, Czech, France, Germany, Hong Kong, Iceland, India, Luxembourg, Morocco, Nepal, Norway, Pakistan, Poland, Russia, Spain, Sweden, Switzerland, Taiwan, UK, Ukraine, USA, Uzbekistan
- Techniques/Tools: Antak, Ave Maria, BABYMETAL, Backdoor Batel, Bateleur, BELLHOP, Boostwrite, Cain & Abel, Carbanak, Cobalt Strike, DNSMessenger, DNSRat, DRIFTPIN, FlawedAmmyy, Griffon, HALFBAKED, Harpy, JS Flash, KLRD, Mimikatz, MBR Eraser, Odinaff, POWERPIPE, POWERSOURCE, PsExec, SocksBot, SoftPerfect Network Scanner, SQLRAT, TeamViewer, TinyMet
- Significant Attack: Bank and financial institutions were targeted with one victim losing $7.3 million and another losing $10 million
- Location: Ukraine

Sandworm Team

- AKA: Telebots, Electrum, Voodoo Bear, Iron Viking
- Targets: Industrial control systems and SCADA; Georgia, Iran, Israel, Russia, Ukraine, Kazakhstan
- Techniques/Tools: BlackEnergy, Gcat, PassKillDisk, PsList
- Significant Attack: Widespread power outage in Ukraine, Russian military hack, cyber espionage attacks against NATO
- Location: Russia

Evil Corp

- AKA: Indirk Spider
- Targets: Financial, government, and healthcare sectors
- Techniques/Tools: BitPaymer, Cobalt Strike, Cridex, Dridex, EmpireProject, FriedEx, Mimikatz, PowerSploit, PsExec, WastedLocker
- Significant Attack: BitPaymer ransomware paralyzed the IT systems of an Alaskan town, Arizona Beverages knocked offline by ransomware attack, Apple Zero-Day exploited in new BitPaymer campaign, Treasury sanctions Evil Corp, the Russia-based cybercriminal group behind Dridex malware
- Location: Russia

Fancy Bear

- AKA: APT28, Sofacy, Sednit
- Targets: Democratic National Committee and Democratic National Convention; Germany, United States, Ukraine
- Techniques/Tools: Cannon, Coreshell, Responder, MimiKatz, spear-phishing
- Significant Attack: U.S. Department of Justice indictment
- Location: Russia

LuckyMouse

- AKA: Emissary Panda, Iron Tiger, APT27
- Targets: Aerospace, education, and government sectors; Australia, Canada, China, Hong Kong, India, Iran, Israel, Japan, Middle East, Philippines, Russia, Spain, South Korea, Taiwan, Thailand, Tibet, Turkey, UK, and USA
- Techniques/Tools: Antak, ASPXSpy, China Chopper, Gh0st RAT, gsecdump, HTTPBrowser, Htran, Hunter, HyperBro, Mimikatz, Nishang, OwaAuth, PlugX, ProcDump, PsExec, TwoFace, SysUpdate, Windows Credentials Editor, ZXShell, Living off the Land
- Significant Attack: Operation Iron Tiger
- Location: China

Sodinokibi

- AKA: REvil, Sodin Targets: GandCrab, Oracle, Golden Gardens
- Techniques/Tools: REvil ransomware, privilege escalation, PowerShell, Sodinokibi ransomware
- Significant Attack: Breached managed service providers, impacting hundreds of dental offices
- Location: Unknown

Mirage

- Targets: European Union, India, United Kingdom
- Techniques/Tools: Cobalt Strike, Mimikatz, MS Exchange Tool, phishing, Royal DNS
- Significant Attack: Attack on a company that provides a range of services to UK government
- Location: China

Magecart

- Targets: British Airways, eCommerce, Magento, Newegg, Ticketmaster Entertainment
- Techniques/Tools: Web-skimmers, skimmer scripts
- Significant Attack: Ticketmaster breach

OilRig

- AKA: APT 34, Crambus, Helix Kitten, Twisted Kitten, Chrysene
- Targets: Aviation, chemical, education, and energy sectors; Iran, Israel, Middle Eastern government; Saudi Arabia, United States
- Techniques/Tools: GoogleDrive RAT, HyperShell, ISMDoor, Mimikatz, PoisonFrog, SpyNote, Tasklist, Webmask
- Significant Attack: Shamoon v3 attack against targets in Middle East Asia, Karkoff
- Location: Iran

Comment Crew

- AKA: APT 1, Byzantine Hades, Comment Panda, Shanghai Group
- Targets: Aerospace, chemical, construction, education, energy, engineering, entertainment, financial, and IT sectors; Belgium, Canada, France, India, Insrael, Japan, Luxembourg, Norway, Singapore, South Africa, Switzerland, Tawan, United Kingdom, United States
- Techniques/Tools: GetMail, Mimikatz, Pass-The Hash toolkit, Poison Ivy, WebC2 significant attack: Operation "Oceansalt"
- Location: China

Temper Panda

- AKA: Admn@338, Magnesium, Team338
- Targets: Financial, government, media sectors; Hong Kong, United States
- Techniques/Tools: Bozok, LOWBALL, Poison Ivy, Systeminfo, Poison Ivy, Living off the Land
- Location: China

Syrian Electronic Army

- AKA: Deadeye Jackal, SEA, Syria Malware Team
- Targets: Facebook, Forbes, Microsoft, Skype; Canada, France, United States, United Kingdom
- Techniques/Tools: DDoS, malware, phishing, spamming, website defacement
- Significant Attack: Defacement attacks against news websites such as BBC News, Associated Press, National Public Radio, CBC News, The Daily Telegraph, The Washington Post
- Location: Syria

PLATINUM

- AKA: TwoForOne
- Targets: Malaysia, Indonesia, Vietnam
- Techniques/Tools: AMTsol, Dipsind, hot-patching vulnerabilities, spear-phishing, Titanium, zero-day exploits
- Significant Attack: Southeast Asia attack
- Location: China

Calypso

- Targets: Brazil, Kazakhstan, Russia, Thailand, Turkey
- Techniques/Tools: EternalBlue, EternalRomance, Mimikatz, PlugX, SysInternals
- Significant Attack: Attacked governments in India, Brazil, Kazakhstan, Brazil, Russia, Thailand, Turkey
- Location: China

Numbered Panda

- AKA: APT 12, Calc Team, Crimson Iron
- Targets: Organizations in East Asia, media outlets, high-tech companies and governments, New York Times
- Techniques/Tools: DynCalc, DNSCalc, HIGHTIDE, RapidStealer, spear-phishing
- Significant Attack: New York Times breach, Taiwanese government
- Location: China

Cozy Bear

- AKA: APT 29, CloudLook, Grizzly Steppe, Minidionis, Yttrium
- Targets: Norwegian Government, United States
- Techniques/Tools: Cobalt Strike, CozyDuke, Mimikatz, spear-phishing
- Significant Attacks: Attack on the Pentagon, phishing campaign in the USA
- Location: Russia

Elfin

- AKA: APT 33, Magnallium
- Targets: Aerospace and energy sectors; Saudi Arabia, South Korea, United States
- Techniques/Tools: Mimikatz, NETWIRE RC, PowerSploit, Shamoon
- Significant Attacks: Organizations in Saudi Arabia and US
- Location: Supported by government of Iran

Charming Kitten

- AKA: Group 83, NewsBeef, Newscaster, APT 35
- Targets: Saudi Arabia, Israel, Iraq, United Kingdom, U.S. government/defense sector websites
- Techniques/Tools: DownPaper, FireMalv, MacDownloader
- Significant Attack: HBO cyberattack
- Location: Iran

Team TNT

- Targets: Amazon, Kubernetes, Windows, Alpine, Docker
- Techniques/Tools: Cryptojacking. Botnets, Cryptominers, TNTbotinger
- Significant Attack: AWS Worm attack, Chimaera campaign
- Location: Unknown

Mythic Leopard

- AKA: APT 36, ProjectM, TEMP. Lapis, Transparent Tribe
- Targets: India, Indian Army
- Techniques/Tools: Andromeda, beendoor, Bozok, Breachrat, spear-phishing
- Significant Attack: Spreading fake coronavirus health advisory
- Location: Pakistan

Muddy Water

- AKA: Static Kitten, Seedworm, TEMP .Zagros
- Targets: Georgia, Iraq, Israel, India, Pakistan, Saudi Arabia, Turkey, United Arab Emirates, United States
- Techniques/Tools: ChromeCookiesView, chrome-passwords, CrackMapExec, Mimikatz, PowerSploit, POWERSTATS, spear-phishing
- Location: Iran

WHAT IS A VULNERABILITY

A vulnerability is a **weakness**, it is a flaw in software or hardware or process that can be exploited by an attacker.

WHAT IS A RISK?

A risk is the likelihood of a weakness(vulnerability)

to be exploited.

WHAT IS A CVE?

Common Vulnerabilities and Exposures (CVE) is a list of publicly disclosed information security vulnerabilities and exposures.

- It is a vulnerability ID

SAMPLE CVE'S

CVE-2021-1675

CVE-2022-30190

CVE-2021-44228

CVE-2022-22965

CVE-2022-1388

CVE-2017-0144

CVE-2022-0609

CVE-2017-11882

CVE-2022-41082

CVE-2022-27925

CVE-2022-26134

CVE-2022-30525

QUESTION??????

Does every vulnerability have a CVE number?

ZERO DAY VULNERABILITY/ATTACK

A **zero day** is a security flaw(vulnerability) for which the vendor of the flawed system has yet to make a patch(fix) available to affected users.

CVE CALCULATOR

https://chandanbn.github.io/cvss/

VULNERABILITY RATING

CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

→→ https://nvd.nist.gov/vuln/detail/CVE-2021-1675

VULNERABILITY MANAGEMENT TOOLS

✅1. Vulnerability Scanning Tools

https://lnkd.in/gbKnkgdt

✅ 2. Greenbone OpenVAS

Download Link: https://www.openvas.org/

✅ 3. Tenable Nessus Essentials

Download Link: https://lnkd.in/gzNsE_kW

Nessus Training: https://lnkd.in/gQEUxFeu

✅ 4. Qualys

Link: https://www.qualys.com/

Training: https://lnkd.in/gvNKJnni

✅ 5. Rapid7 InsightVM

Nexpose Link: https://lnkd.in/gdARCttE

InsightVM Link: https://lnkd.in/gCtiQgyA

Training: https://lnkd.in/g3Q5i6fT

✅ 6. Agentless Vulnerability Scanner for Linux/FreeBSD: https://vuls.io/

✅ 7. Vulnerability Database / Datasource
NVD Full Listing: https://lnkd.in/gSNNgY9W
Link: https://nvd.nist.gov/
CVE Details: https://lnkd.in/gXm_2Z5h
CVE Report: https://cve.report/
Mitre CVE: https://cve.mitre.org/
Mitre CWE: https://cwe.mitre.org/
Vulnerability search: https://vulners.com/
Vulnerability database: https://vuldb.com/
Known Exploited Vulnerabilities: https://lnkd.in/gHAFJEtS
Cyberscan : https://lnkd.in/eRS6W_w3

✅ 8. CVSS Calculator
Link: https://lnkd.in/gNqYyqKx

✅ 9. Bug Bounty Programs: find vulnerability and get paid - https://www.hackerone.com/
Mozilla Observatory: https://lnkd.in/e7AbJDEh

VULNERABILITY MANAGEMENT STAGES

1. Discover
2. Assess
3. Remediate
4. Verify
5. Report

DISCOVER

- Make sure you detect all vulnerabilities in all web applications before a hacker finds them
- Create an accurate inventory for websites
- Check all your Web Applications regularly

ASSESS

- Which vulnerability is more important for us? Which one to fix first?
- Severity of the vulnerability (CVSS score, CVSS vector string),
- Asset criticality
- Risk and impact

REMEDIATE

- Effectively communicate the risk to the organization, provide practical recommendations, and empower defenders so validate fixes are properly implemented.

- Remediation options-solutions

- Compensating controls-if there is no patch, upgrade or configuration settings; enhanced monitoring, WAF

- Accepting a risk

- Check if it is a False positive

VERIFY

- Track and verify that the vulnerability has been remediated
- Run a Remediation Scan
- Assign a confidence value, reduce false positives or negatives
- Understand the source of vulnerabilities to enable upcoming remediation

REPORT

- share scan report with web app owner
- Document vulnerability findings
- Scan remediation process should be documented

VULNERABILITY ANALYST DAY-TO-DAY

- Check scans results
- Communicate all vulnerability findings to the web application owner
- Validate remediation-rerun the scan
- Attend meetings with InfoSec and web owners/developers
- Research on latest vulnerabilities

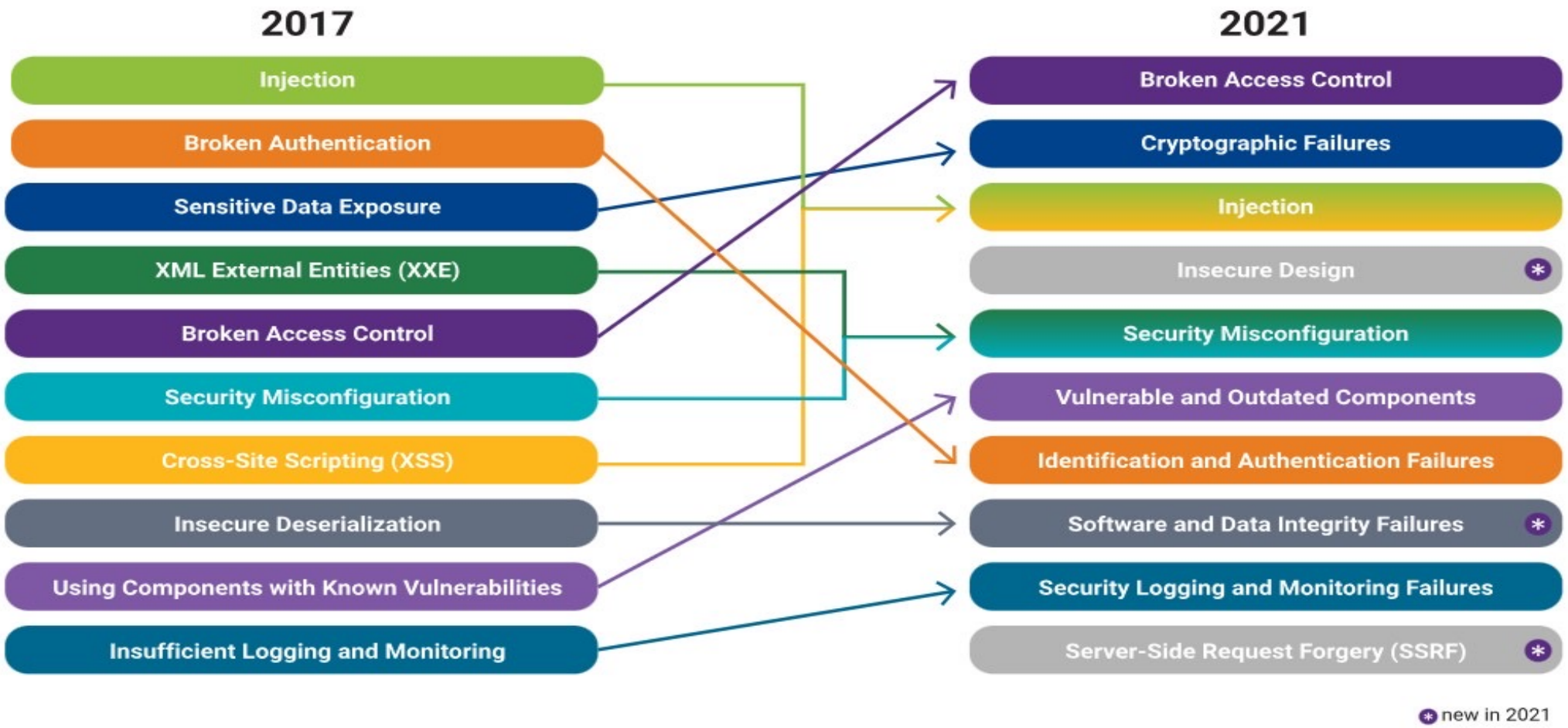
OWASP TOP-10

The Open Web Application Security Project (OWASP) is a nonprofit foundation dedicated to improving software security(web apps).

- The OWASP Top 10 provides rankings of the top 10 most critical web application vulnerabilities.

- It provides remediation guidance for those vulnerabilities.

OWASP IS UPDATED EVERY 4 YEARS



WHAT IS AN EXPLOIT?

An exploit is a piece of **software**, data or sequence of commands that takes **advantage** of a **vulnerability** to cause unintended behavior or to gain **unauthorized access** to sensitive data.

EXPLOIT DATABASE

ExploitDB is an archive of exploits for the purpose of public security, and it explains what can be found on the database.

https://www.exploit-db.com/

IOC - INDICATORS OF COMPROMISE

* IOCs serve as forensic evidence of potential intrusions on a host system or network.

* These artifacts enable information security (InfoSec) professionals and system administrators to detect intrusion attempts or other malicious activities.

* Security researchers use IOCs to better analyze a particular malware's techniques and behaviors.

QUESTION???

What is the difference between vulnerability assessment and penetration testing?

ioSENTRIX

Vulnerability Assessment

This assessment looks for known vulnerabilities and classifies them based on their magnitudes and impact.

Automated Test

Includes false positive

Uncover possible vulnerabilities

Frequently Done

VS

Penetration Testing

In the pen-test, known vulnerabilities are exploited or often chained up to gain access or perform malicious activities to determine the security posture.

Includes Automated and Manual Tests

Only successful exploits

Done On Demand

Show exploitable vulnerabilities

Global Ransomware Damage Costs*

- **2015: $325 Million**
- **2017: $5 Billion**
- **2021: $20 Billion**
- **2024: $42 Billion**
- **2026: $71.5 Billion**
- **2028: $157 Billion**
- **2031: $265 Billion**

Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.

CYBERSECURITY VENTURES

* SOURCE: CYBERSECURITY VENTURES