Cyber Threat Intelligence Glossary, Acronyms & Metodologias

0-day Vulnerability
A zero-day vulnerability in a disclosed, but not yet fixed system or device is a vulnerability. A zero-day exploit is considered an exploit that exploits a zeros-day vulnerability.

A

Advanced Persistent Threat (APT)
An attacker with advanced know-how and considerable resources, which enables him to create opportunities for his purposes by using multiple attack vectors, which are usually to establish and extend the foundation of an IT infrastructure of organisations, in order to continually exfiltrate information or to damage it or prevent it.

Attack Surface
ASM is the process of discovering, listing, classifying, analyzing, prioritizing, and monitoring all information that can be collected on the internet and informing your organization about sensitive data by searching external digital assets.

B

Backdoor
Remote access through a compromised system.

Business Email Compromise (BEC)
BEC is a sort of fraud targeting firms with wires transferring and providing international suppliers. Executives' email or high-level workers' accounts connected to finance or wire transfer payments, whether openly or publicly visible, are either faked or compromised by keylogging or fraudulent transfers by phishing assaults which result in losses of hundreds of thousands of dollars.

Black Market
Illegal trafficking or trading in items publicly regulated or scarce.

Botnet
Network of infected devices.

C

Carding Fraud
Using stolen credit cards.

Clearweb
Websites with no entrance barrier.

Continuous Security Monitoring (CSM)
The Continuous Security Monitoring (CSM) methodology automates the monitoring of security records, vulnerabilities, and other cyber risks, with the objective of supporting corporate decisions on risk management.

Credential Stuffing

Credential Stuffing is a technique that involves an automatic injection attack to access online services with stolen credentials. In an attack on the login data, fraudsters use it to access consumer accounts to make fraudulent purchases, carry out phishing attacks, and steal information and money.

D

Dark Net

Dark net is an Internet overlay network that may only be accessed with particular software, settings, or authorization and frequently employs a unique customized communication protocol.

Dark Web

The dark web is a part of the internet that isn't indexed by search engines.

Data Breach

Data breach is an occurrence involving the stealing or removal of information from the system without the knowledge or permission of the system owner.

Databroker

A threat actor who sells dataset and/or information.

Distributed Denial of Service (DDoS) Attack

A technique of denial of service used to conduct the attack on several hosts.

Digital Asset

Any asset which is purely digital or which represents a physical asset on a digital basis.

Digital Fingerprint

A hash that identifies data in a unique way. The modification of a single bit in the data stream for the digest message produces a different digest of the message.

Digital Footprint

Information on a certain individual who exists through their online activities on the Internet.

Denial of Service (DoS)

To deny authorized access to resources or to postpone crucial time activities.

Doxxed

When an individual's private information gets made public.

Drive-by Compromise

Malicious code was unintentionally downloaded.

E

Enumeration
The process of listing all of a system's characteristics.

Exploit Kit
A toolkit that exploits various vulnerabilities in order to distribute malware.

Exploit Leveraging
Use of a flaw to gain an advantage.

I
Initial Access Broker
A threat actor who sells their initial network foothold.

Indicators of Attack (IoA)
An IOA provides a unique construction into a dynamic, situational representation which directs the reaction of unknown attributes, IOCs and contextual information (including organizational intelligence and risk).

Indicator of Compromise (IoC)
IoCs are the evidence that prove a cyber-attack has taken place.

L
Loader
Malware distribution system.

M
Magecart
Threat actors who target Magento based online shopping cart systems.

Malware Information Sharing Platform (MISP)
A threat intelligence platform for collecting, distributing, storing, and correlating Indicators of Compromise from targeted assaults, threat intelligence, financial fraud information, vulnerability information, and even counter-terrorism information.

P
Patch Gap
Time elapsed between the publication of a software patch and its application by suppliers.

Phishing
A method used to try to collect sensitive information, such as a bank account, using a fake email request or a website in which the criminal disguises himself as a respectable company or a trustworthy individual.

Personally Identifiable Information (PII)
Any information representation that allows the identification of the individual to whom the information relates to be properly inferred through direct or indirect means.

R

Ransomware

Ransomware is a malicious software that uses encryption to ransom victims. Critical information of a person or organization is encrypted so that files, databases or apps are not accessible.

Remote Code Execution (RCE)

Describes a form of attack that an attacker can use on a target system to execute arbitrary instructions or code. It allows attackers to run malicious programs to control the increased privileges of vulnerable devices.

S

Shadow IT

Shadow IT, by definition, includes software, applications, and services used by different departments without the company's IT department's knowledge and control. Today, many staff can use different software and tools, thinking that they can carry out their work faster and easier without notifying the IT department.

Shell

Command and script interpreter deployed on a compromised system.

Security Information and Event Management (SIEM)

SIEM combines security information management with security event management in software products and services. They analyze security alarms issued by apps and network devices in real time.

Skimmer Malicious

A script that collects form data from a website.

SMiShing

Phishing via SMS.

Security Orchestration, Automation, and Response (SOAR)

Threat and vulnerability management, security incident response, and security operations automation are the three software capabilities described by the term.

Security Operation Center (SOC)

SOC is the centralized role of a person, process and technology organization to continually monitor and enhance the security position of a business while avoiding, detecting, analyzing and responding to cyber security incidents.

Spear Phishing

A colloquial concept used to characterize any phishing attempt that is extremely focused.

State-Sponsored

Financially supported or authorized by a sovereign state.

Strategic Threat Intelligence
Data that assists you safeguard your organization from cyber threats are strategic threat intelligence. Data is collected, processed and analyzed to offer you actionable intelligence to improve your security.

Supply Chain Attacks
Attacks which let the attacker use implants or other vulnerabilities implanted before the installation to infill or modify the hardware, software, operating systems, peripherals or services of information technology at any time during the lifetime cycle.

Supply Chain Risk
The risk of sabotage, malicious introduction of undesirable functions, or other subvertments of the design, integrity, manufacturing, manufacturing, distributing, installing, operating or maintaining a supply item or systems in order to control, deny or disrupt the function, use or operations of a system or otherwise degrade it.

T
Tactical Threat Intelligence
Tactical threat intelligence provides information about the tactics, techniques, and procedures (TTPs) used by threat actors to achieve their goals.

Take-Down Service
A take-down service, also known as a notice and take down request, is a method of requesting that an Internet Service Provider (ISP) or search engine delete or block access to unlawful, irrelevant, or obsolete content.

Threat Actor
A participant (individual or group) in an activity or process defined by malice or harm using computers, devices, systems or networks.

Threat Intelligence Report
A prose document describing TTPs, actors, systems and information types being targeted and associated threats.

Threat Information (TI)
TI is information on present or upcoming risks that might jeopardize an organization's security.

Traffic Light Protocol (TLP)
TLP is a collection of designations for the sharing of sensitive information with the relevant public.

Tactics, Techniques, and Procedures (TTP)
It explains the analysis methodology of the functioning of an APT or can be used to profile a specific actor of threat.

Typosquatting
It is a social engineering technique of a hacker who sells their initial network foothold. that targets online users who mistakenly enter a URL in their browser rather than search engines.

V

Vishing

Voice-based phishing.

Y

YARA Rules

YARA rules are used to categorize and identify samples of malware using textual or binary patterns to provide descriptions of malware families.

Acronym Description

APT: Advanced Persistent Threats
BEC: Business Email Compromise
BGH: Big Game Hunting
CNOs: Computer Network Operators
CTI: Cyber Threat Intelligence
CVE: Common Vulnerabilities and Exposures
CWE: Common Weaknesses Enumeration
FUD: Fear, Uncertainty, Doubt
HOK: Hands-On-Keyboard
HOR: Human-Operated Ransomware
HUMINT: Human Intelligence
IoA: Indicators of Attack
IoC: Indicator of Compromise
IOs: Influence Operations
I2P: The Invisible Internet Project
MISP: Malware Information Sharing Platform
MSM: Main-Stream Media
OPSEC: Operational Security
OSINT: Open-Source Intelligence
PII: Personally Identifiable Information
PIR: Priority Intelligence Requirements
RFI: Request for Information
SIGINT: Signal Intelligence
SOCMINT: Social Media Intelligence
SOP: Standard Operating Procedure
SOAR: Security Orchestration, Automation, and Response
TA: Threat Actor
TIP: Threat Intelligence Portal
TLP: Traffic Light Protocol
TOR: The Onion Router
TTP: Tactics, Techniques, and Procedures

Metodologia

Cyber Kill Chain

It is a model for identification and prevention of cyber intrusions activity.

Diamond Model of Intrusion Analysis

It is an approach to conducting intelligence on network intrusion events.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

The framework reflects the many phases of an adversary's attack life cycle and platforms known to be targeted. Curated information base and model for cyber adversaries conduct.

Paris Model of Threat Hunting

It is a model that expresses what good threat hunting is all about.