# Reading Response 3 - Verizon DBIR

## 1) Comment of some of the new terms picked up in the reading

**Incident:** A security occurrence that actually or potentially compromises the confidentiality, integrity, or availability of information management systems and results in violation of security policies, security procedures, or acceptable use policies.

**Breach:** An incident that results in unauthorized disclosure of personally identifiable information by an outsider or by an authorized user.

**Zero-trust model:** Zero Trust model is a set of security design principles, and management strategies based on creating a network infrastructure and policies that eliminates trust in any one element, node, or service implicitly and needs continuous real-time verification.

**VERIS Framework:** Vocabulary for Event Recording and Incident Sharing (VERIS) is an open framework providing a common repository describing security incidents in a consistent manner while considering four factors -- threat, asset, impact and control and four metrics -- incident description, demographics, discovery and mitigation and impact description that is useful to risk management.

**Pretexting:** Pretexting is a form of social engineering used by adversaries to manipulate victims into divulging sensitive information by creating a pretext.

**System Intrusion:** System Intrusion is verizon DBIR's one of the incident classification patterns that captures the complex human operated attacks that leverage malware infusion into systems to achieve their objectives including deploying ransomware.

## 2) Comment on some of the new attack vectors or profiles

**Magecart Attack:** Magecart attacks are classified as one of the system intrusion patterns that target and capture payment card data processed through web applications. Magecart attack is intended for stealing data using a malicious code inserted into code base that was accessed by exploiting inherent vulnerabilities.

**C2:** Command and Control Servers are referred to as C2 which are used by adversaries as entry paths for malwares, bots and communicate with the infected system through commands to download files, manipulate system data. HTTP/HTTPS, Internet Relay Chat (IRC) is considered few of the channels and protocols used by the malware for the C2 communication.

**RAM Scraper:** RAM scraping attack is one of the malware vectors that can extract consumer credit card information from retail PoS(Point of Sale) machines performed through intrusion into the random access memory(RAM).

**Credential Stuffing Attack:** Credential stuffing attack uses stolen usernames and passwords pairs that are obtained off of the dark web or data from a breach, add them to a botnet and automate a script to access user accounts, credentials of other multiple sites, organization at once.

**3) Comment on some of the know attack vectors or profiles**

**Social Engineering:** Social engineering is an attack vector that relies on manipulating or tricking people(users) to break normal security procedures and practices through exploiting human behavior and gaining unauthorized access to sensitive information, systems and networks. Few examples of social engineering are phishing and business email compromise (BEC).

**Password Dumper attacks:** Password dumper attacks extract password through credential hashes accessed by gaining fraudulent access to systems by cybercriminals to copy and steal saved passwords.

**Brute force attack:** A brute-force attack is a repeated process of submitting different credentials (usernames and passwords) to guess correctly and cracking credentials eventually. Brute force attack uses trial-and-error approach and can be executed using bots, automated tools, scripts.

**4) Picture that you've just been hired as a security consultant for an Enterprise with a burgeoning cyber security program. Given the current cyber threatscape and actors, what or 3-4 priorities would you put in place for your client (based on the DBIR)?**

As a security consultant for the enterprise with a burgeoning cyber security program, three main areas to focus with extreme scrutiny are program development, sensitive data controls, technical solutions and build action plans that cover all aspects of business's people, processes and technology. Finally, test and reassess the current plan, update the priorities constantly based on concurrent breaches.

As part of program development, developing an information security strategy should be of primary importance that concentrates how to protect the enterprise and its data. Information security strategy addresses aspects such as developing and implementing policies, procedures and configuration standards. It is also important to invest in operational expenses such as staffing, implementing a security awareness training program, training management and IT staff.

Sensitive data controls involve the process of developing a framework for sensitive data classification using sensitive data flow mappings in the enterprise and integrating that to the information security policies, training and control implementation. Proper documentation of all the systems that store, process, transmit sensitive data and remove unnecessary sensitive data storage repositories. Finally, proper controls should be implemented to reduce sensitive data storage using a data retention program strategy.

Technical Solutions include implementing solutions that have a balance of detection, prevention and response capabilities. Detection capability of the threat is implemented through monitoring systems for malicious activity to specifically detect malware using intrusion detection systems (IDS) put in place. Prevention capability focuses on removing vulnerabilities that could lead to a malware infection and secure the enterprise's network from unauthorized access using intrusion prevention systems(IPS). Response capability involves  developing an incident response plan and the security staff to respond to security incidents in real time. This can be done by investing in the purchasing tools and appropriate training or outsource.

First action plan to perform is to identify the human element that covers all the internal, external threat actors and recognize their methods and eventually mitigate vulnerabilities. Second, to perform inventory management of all the conduit devices present in the organization to know the environment and reduce the exposure of a cyber attack. Third, an important step is to oversee configuration exploitation that consists of knowing all the current information systems and their proper configuration to avoid a massive single point of failure. Finally, to identify all of the taxonomy related to threat actors tools, malicious softwares and assess all of their capabilities to install suitable controls to information systems architecture.