COMMON TYPES OF VULNERABILITIES

CONCEAL

The National Institute of Standards and Technology (NIST) released a graph showing 18,378 vulnerabilities reported in 2021. [1]

MISCONFIGURATIONS

Endpoint misconfiguration accounts for 27% of entry points exploited by attackers today. [2]

UNPATCHED SOFTWARE

60% of data breaches stem from unpatched software. [3]

CREDENTIALS

61% of all breaches involve credentials, whether they be stolen via social engineering or hacked. [4]

VULNERABILITY TYPES

A KEY PATH TO YOUR CROWN JEWELS

In the past year, vulnerability exploitation, as the entry point of threat actors, has doubled. To find these vulnerabilities, threat actors are leveraging a wide variety of techniques including scanning IPs and open ports, crawling for specific services, testing specific CVEs from the catalog discussed above, and running remote code execution.

MALICIOUS INSIDER

Insiders are responsible for approximately **22%** of security incidents. [5]

SUPPLY CHAIN VULNERABILITIES

Software supply chain attacks hit three out of five companies in 2021. [6]

ZERO-DAYS

A total of 83 zero-days were recorded in 2021 - up **55%** from 2020, which recorded 36 zero-days. [7]

TECHNOLOGY CHALLENGES

MISCONFIGURATIONS

Challenge: System, software and hardware misconfigurations are becoming extremely common as digitalization continues to be part of the security team's transformation strategy. Security teams are overwhelmed with the changes happening around them and oftentimes put configuration validation on the back burner. Misconfigurations give adversaries specific targets to probe, looking at common software and hardwares for common configuration errors.

UNPATCHED SOFTWARE

Challenge: Unpatched and out of date software opens an organization's network up to a variety of vulnerabilities. Threat actors are able to target softwares with known patches to test an organization's patch management strategy. With unpatch software, threat actors can exploit vulnerabilities that the patches are looking to remediate.

MALICIOUS INSIDER

Challenge: When legitimate credentials of employees, contractors, business associates or others are maliciously or intentionally abused, extreme harm can be caused to the target organization. Detection and response capabilities are less likely to pick up on the malicious activity of a legitimate user in the moment. This reality makes the exfiltration of confidential data such as personal identifiable information of employees or customers or financial information related to the organization extremely hard to catch in the act.

CREDENTIALS

Challenge: With weak and non-existent authorization for employee credentials, adversaries can brute force their way into a user account. Without complex authorization requirements, cyber criminals are able to gain an employee's credentials through trial and error, giving them the keys to the kingdom once they are inside.

SUPPLY CHAIN VULNERABILITIES

Challenge: Vulnerabilities in an organization's supply chain affect the service of the organization to the end user. This disturbance commonly stems from a vulnerability in the application code of the supplier as a result of poor code practices. Threat actors can target vulnerabilities in the supply chain to cause havoc to organization's that have the supplier installed in their network.

ZERO-DAYS

Challenge: Unknown vulnerabilities discovered by adversaries are extremely harmful to organizations that have invested in the software with the zero day. When exploited, these vulnerabilities can cripple the victim organization until they are able to identify the vulnerability themself. Since zero-days are not defendable until after the attack has happened, threat actors that discover a zero day are able to cause extreme havoc in the industry.

To learn how Conceal helps address all of these challenges and more, check out our use case repository here.

Sources:
1 - https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time 2 - https://hbr.org/sponsored/2021/07/tech-misconfigurations-vs-vulnerabilities-how-different-are-they 3 - https://www.darkreading.com/vulnerabilities-threats/missing-patches-misconfiguration-top-technical-breach-causes 4- https://www.verizon.com/business/en-gb/resources/reports/dbir/ 5 - https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf 6 - https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=e88f53a7864a 7 - https://purplesec.us/resources/cyber-security-statistics/