ATTACK VECTOR CATEGORIES AND SUBCATEGORIES

Introduction

The CyCognito platform gives you an advantage over attackers by using their tools, tactics and procedures to map your attack surface. Using that approach, the platform discovers your Internet-facing assets and detects the security issues that will allow attackers to follow a path of least resistance through your digital footprint to your applications and data. The CyCognito platform prioritizes and presents these attack vectors so that they can be remediated or mitigated before attackers use them.

Information Presentation

The CyCognito platform's continuous monitoring enumerates outstanding issues along with an indication of whether they are new, unchanged, or improved to demonstrate progress towards a more secure environment. Each attack vector is clearly presented with details about:

1. Organization at Risk (including subsidiaries and acquisitions)
2. Attack Vector Categories and Subcategories
3. Discoverability of the Issue
4. Potential Impacts
5. Affected Assets
6. Description
7. Remediation Steps
8. References
9. Appendices (as available) - for screenshots and supplemental evidence

See the following pages for attack vector categories, subcategories and examples.

Category		Description	Examples
NETWORK SECURITY HYGIENE		This category includes attack vectors where the network topology itself provides an easy avenue of attack. This includes unknown and unmanaged assets, remotely accessible servers with misconfigured and insecure authentication mechanisms or services such as unsecured databases, Remote Desktop Protocol (RDP) and Secure Shell (SSH).	Any unmanaged asset that is exposed for extended periods of time without any facility to detect an attack is an attractive target. A server that permits remote administration is attractive as a beachhead for attacks on more sensitive assets with more valuable data.
SUBCATEGORY	Exposed Internal Asset	Most issues in this subcategory involve assets which should be protected by at least a firewall or DMZ because they are internet-facing, yet were discovered with seemingly no mitigating security controls in place.	An example here would be a printer exposed to the Internet that does not require any authentication and can be accessed by any remote user. The printer may expose internal information (e.g. versions, network settings, geolocation, data in memory, etc.) that attackers can leverage. The printer may also enable configuration changes without requiring any authentication.
	Exposed Remote Access Service	Issues in this subcategory cover systems that offer remote access services. These are attractive to attackers for obvious reasons: gaining access allows full system administration privileges and a convenient platform for further attacks into the network.	Remote Desktop Protocol (RDP) and Secure Shell (SSH) are the most commonly used remote access protocols and are notoriously popular targets especially when unconfigured or misconfigured. In addition to being directly targeted by attackers, attack vectors such as these have been weaponized via worms such as Morto which propagated in the wild. The BlueKeep vulnerability raised the specter of another widespread and wormable attack.
	Exposed Sensitive Ports	Issues is this subcategory address services running on internet-facing hosts with non-standard ports which might indicate an already compromised host or one that could be easily compromised.	An example is an SMTP server using a non-standard port (i.e., something other than 25, 587, 465). This might indicate a backdoor was set up by an attacker in order to send spam or even control the host machine. Because the open port is nonstandard, security tools might not identify this server as a potential attack vector.
	Abandoned Asset	These are assets that appear old and abandoned because they haven't been updated in a long time, are running end-of-life/out-of-date services, or are part of extinct domains. Our experience shows that such assets tend to be vulnerable and targeted by attackers, while at the same time failing to provide any value to the organization.	Examples include (1) abandoned assets exposed for extended periods of time without any mechanism to detect attacks in place and (2) abandoned assets running end-of-life or out-of-date software with multiple easily exploitable vulnerabilities and public POC tools that can exploit these paths of least resistance.

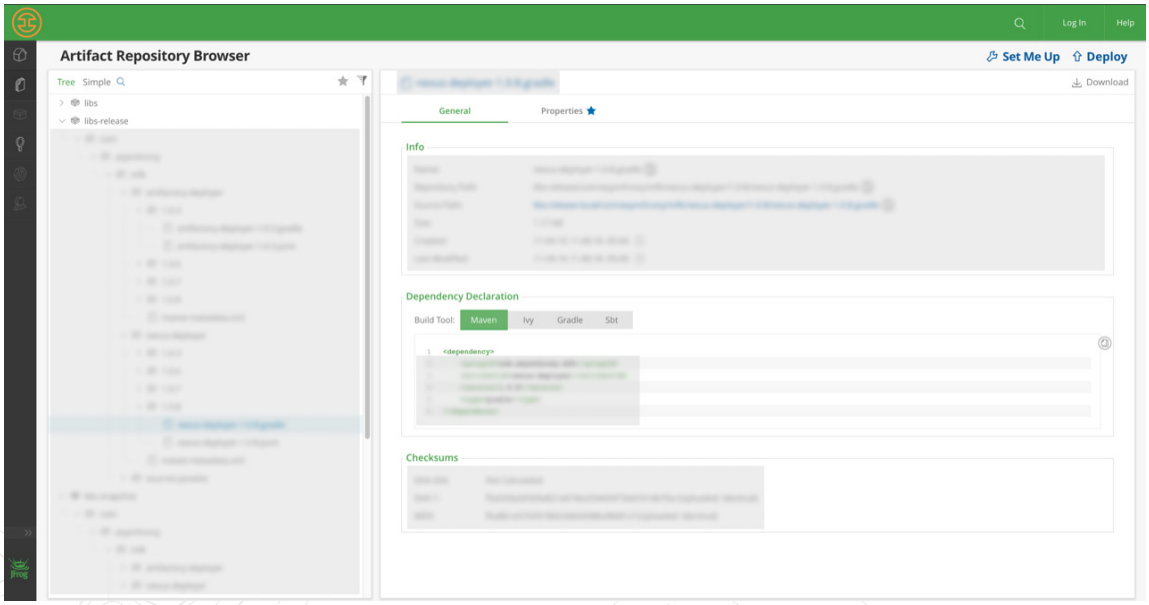

Figure 1: A JFrog artifactory that was exposed and required no authentication, placing highly sensitive intellectual property at risk.

Category		Description	Examples
CONFIDENTIALITY RISKS		These attack vectors allow man-in-the-middle attacks and expose data about a system, or on a system, to attackers.	An example would be weak and misconfigured encryption protocols and ciphers.
SUBCATEGORY	Weak Authentication	Issues in this subcategory exist when there is an unsafe login mechanism.	Examples here would be a login mechanism that does not mitigate brute force attacks because there is no limit on password attempts, or because challenge-response authentication is not enabled.
	Unencrypted Communications	These issues exist because the login mechanism or communication channel is either unauthenticated or unencrypted.	An example is when the Telnet protocol is in use or when a web page uses unsecured HTTP authentication.
	Cryptographic Weakness	These are issues due to the fact that the cryptography used to secure communications is exploitable.	Examples include the use of MD5 for storing passwords, weak proprietary cyphers, or cyphers designated to comply with US export controls.
	Exposed System Data	Issues in this subcategory are typically associated with file-include and directory traversal vulnerabilities, they may also involve non-web servers like databases that permit metadata to be extracted from the system without authorization.	An example would be if a vulnerability existed in PostgreSQL database that exposed internal information attackers could leverage for further attacks.
	Exposed Data (Not System)	These issues address exposed sensitive files or personnel data, that typically occur due to misconfiguration or default configurations. Exposed data may be intellectual property, user or password lists, logs or history, code, and other sensitive information.	An example is exposed video conference recordings that enable attackers to gather information about the company and its managerial decisions without requiring any authentication. Other examples include DevOps components, file sharing servers, server directories, and knowledge management systems that expose sensitive information.

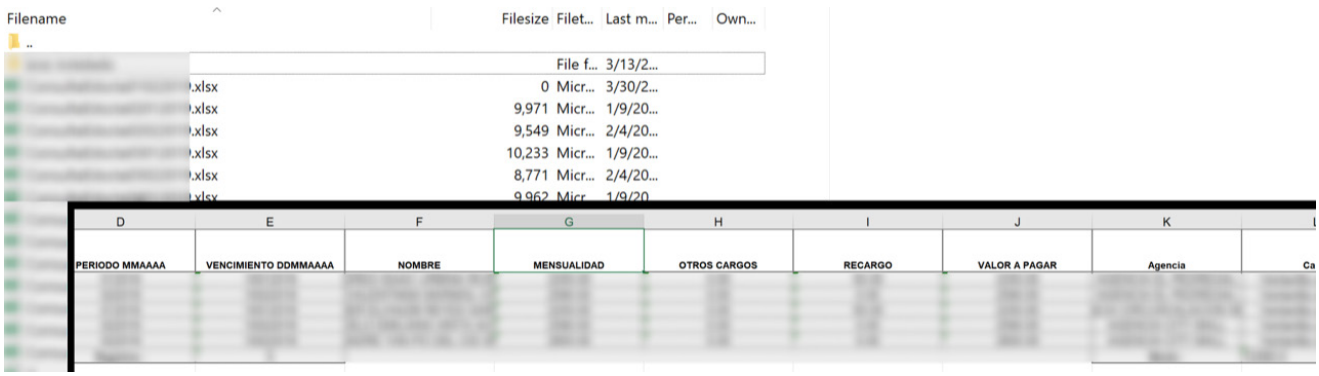

Figure 2: An exposed FTP server with anonymous authentication provided access to Excel files with information about payments to sales representatives.

Category		Description	Examples
REPUTATION RISKS		These are attack vectors that could result in damage to an organization's reputation, resulting in a loss of money and market share -- and the subsequent loss of employees and customers.	Examples include email attacks, phishing waterhole operations, domain takeovers, DNS hijacking, third-party hosting risks, acquired businesses, and subsidiary risks.
SUBCATEGORY	Email Spoofing	Issues in this subcategory are for email servers that may be taken over resulting in email impersonations. This vector is the most popular mechanism for phishing an organization's shareholders, executives and other employees, partners, subsidiaries and customers.	Attackers could spoof your organization's email addresses and send phishing emails that appear to originate from your organization. DNS issues such as missing SPF are common here.
	Domain Hijacking	Issues in this subcategory could allow attackers to hijack domains or subdomains and redirect domain traffic.	Subdomain takeover enables attackers to take control of a subdomain, such as the "sales" subdomain in the example: sales.yourco.com. Legitimate users accessing the sales subdomain will be directed to applications, web content, etc. under attacker control.
	Trust Chains	These are issues that involve certificate trust chains.	In the digital world, certificates are a way to identify assets and to secure communications. Being able to misuse an organization's certificates creates a trust issue, as does being able to intercept encrypted communications via man-in-the-middle attacks.

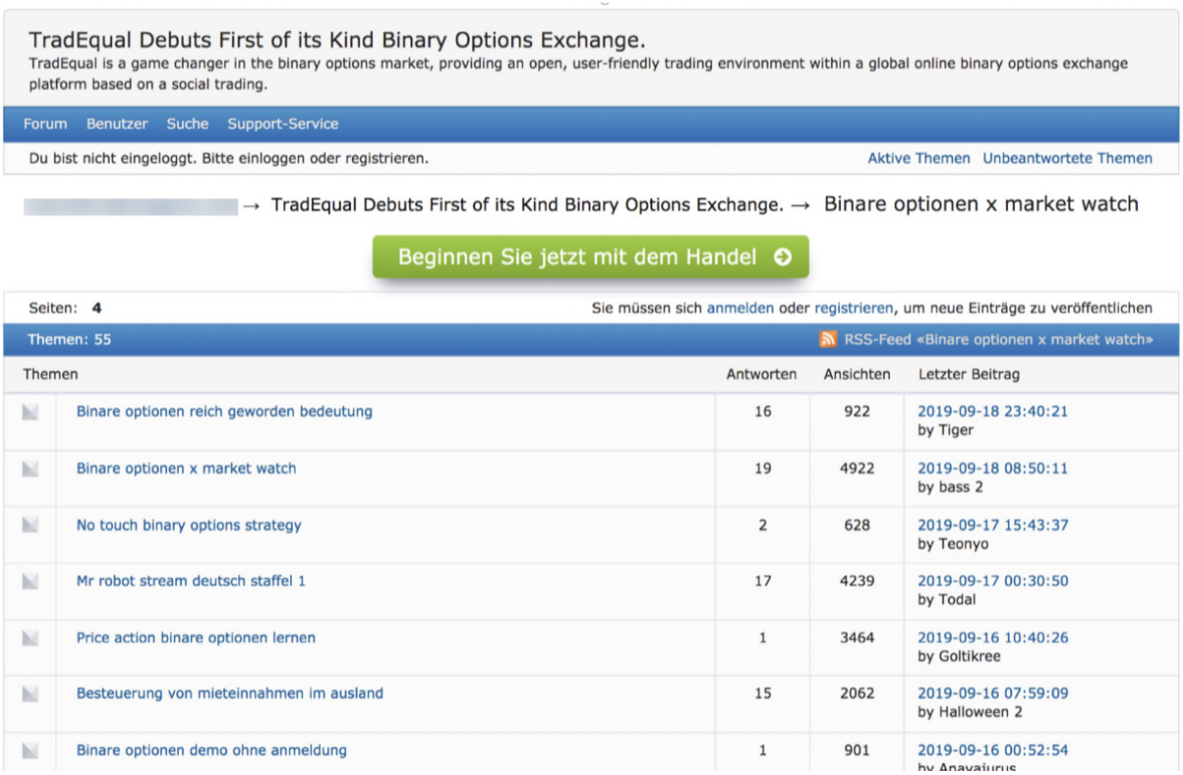

Figure 3: An abandoned domain pointed to an IP address that was taken by a binary options company (binary options are widely used in fraud).

Category		Description	Examples
APPLICATION SECURITY HYGIENE		Attack vectors in this category are for insecure code issues and vulnerable third-party software components that enable attackers to take control of assets.	Examples include software with a known Common Vulnerability and Exposure (CVE), typically identified by vulnerability scanners. Other examples in this category are use of default credentials and unconfigured or misconfigured components that are insecure and easily exploitable.
SUBCATEGORY	Unpatched / Vulnerable Software	Issues in this subcategory are like those typically identified by vulnerability scanners where a flaw exists in commercial software that potentially can be exploited with attack tools. For the most part, these will be high severity vulnerabilities that are well known and easily exploited.	An example issue here is CVE-2020-3421, Cisco Small Business RV042 and RV042G Routers Cross-Site Scripting Vulnerability - A vulnerability in the web-based management interface of Cisco Small Business RV042 Dual WAN VPN Routers and Cisco Small Business RV042G Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device.
	Default Credentials	Issues in this subcategory involve credentials that have shipped with the device and remain unchanged. Any attacker with access to the user manuals would have access to the device.	Examples include a router where the default username and password are in use because they were never changed, or where remote attackers can access some of the device's files and folders, gather internal information such as credentials, and take over the device. Default credentials almost always represent a path of least resistance, especially when they are internet-facing and connect to devices within your organization.
	Misconfigured Software	These issues address configurations that allow attackers easy access to information or systems. Vulnerability assessment products rarely enumerate these as they are not a typical code flaw. Misconfigurations represent a large chunk of the likely paths an attack will follow because almost all software needs to be configured manually.	An example would be a misconfigured ElasticSearch node or cluster where external users could enumerate its list of indices and possibly gain sensitive information.

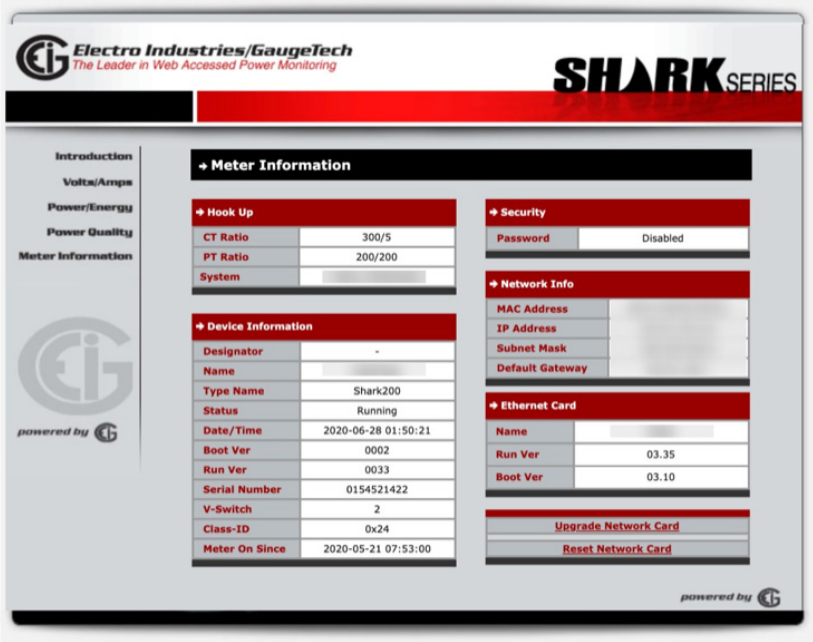

Figure 4: An exposed electrical power management system with no authentication (password requirement was disabled).

CYCOGNITO
420 Florence Street
Palo Alto, CA 94301
cycognito.com

CyCognito is solving one of the most fundamental business problems in cybersecurity: the need to understand how attackers view your organization, where they are most likely to break in, and how you can eliminate that risk.