Cyber Threats and Risks

About TripleP

- **TripleP Training and Consulting** is a consultancy company in the field of readiness for privacy regulations in Israel and around the world, as well as cyber training for companies in terms of professional training and employee awareness.

- **Mrs. Etti Berger, LLM.**, a professional Cyber and data privacy consultant. Hold a Master of law degree (LLM) and have recently begun working on my doctoral thesis on “privacy in the digital world”. Further, have over twenty years of practical technical technology experience in cyber security.

TABLE OF CONTENTS

TripleP
Practical Proactive Privacy

Indicators of a Cyberattack

- Unusual Outbound Network Traffic
- Anomalies In Privileged User Account Activity
- Geographical Irregularities
- Log-in Irregularities and Failures
- Swells In Database Read Volume
- HTML Response Sizes
- Large Numbers Of Requests For The Same File
- Mismatched Port-Application Traffic
- Suspicious Registry Or System File Changes
- DNS Request Anomalies

Anatomy of a Cyberattack

Research

- Before launching an attack, cybercriminals try to gather as much publicly available information about the target organization and its network as possible. This can include, network ranges, IP addresses, and domain/host names. Part of the reconnaissance may include looking for email addresses of key players in the organization (IT manager, CFO, etc.) that could be used in a phishing attack during the exploit phase

Anatomy of a Cyberattack

Penetrate

- Now the attacker is ready to engage with the intended target and subvert the perimeter defenses. This is often achieved through a phishing attack or another common attack vector. But hackers also have other tools that can be used to gain entry. These include port scanners, vulnerability exploitation tools, traffic monitoring tools, password crackers, and encryption tools.

Anatomy of a Cyberattack

Expand

- Once in, an attacker will employ a technique called pivoting, where they use a compromised device to access other devices that would not otherwise be accessible. This lateral movement optimizes transparency into available network assets in order to obtain high-value, sensitive information. Various techniques are deployed to escalate privileges and gain system administrator credentials.

Anatomy of a Cyberattack

Exploit

- Once an attacker finds what they are looking for, they take the final steps to achieve their goal. Successful outcomes include:
- Gaining administrative access
- Opening Command and Control communications
- Achieving persistence
- Denying access to systems
- Exfiltrating data
- Destroying data
- Covering their tracks

Common Attack Vectors

Phishing

- An email disguised as a legitimate message, enticing recipient to open an infected attachment or click a link that takes them to an infected website. Phishing accounts for 90 percent of all successful cyberattacks.

Drive-By-Downloads

- Malware inadvertently downloaded from a legitimate site that has been compromised without any action from the user. It typically takes advantage of vulnerabilities in the user's operating system or other program.

Malvertising

- These are online ads that are owned by cybercriminals. Malicious software is downloaded onto the user's systems when they click the ad, which can be on any site, including popular sites visited regularly.

TripleP
Practical Proactive Privacy

Common Attack Vectors

Domain Shadowing

- If a hacker can obtain domain registrar credentials, they can add host records to an organization's DNS records, then try to redirect visitors to these malicious, but trusted, IPs.

Malware

- Malicious code that disrupts computer operations, gathers sensitive information, or gains unauthorized access. There are various types of malware. They differ in infection and propagation characteristics .

Denial-of-Service

- An attempt to make a machine or network resource unavailable for its intended use. It often consumes more computer resources than a device can handle or disrupts by disabling communication services.

TripleP
Practical Proactive Privacy

Common Types of Malware

Ransomware

- Malicious file encryption that can prevent you from using your computer or mobile device, opening your files, or running certain applications.

Trojan

- Poses as a legitimate application. Typically connects to a Command and Control server, allowing the attacker to take control of the infected machine.

Worm

- A piece of malicious code that is designed to spread from one computer to another by exploiting known vulnerabilities. It replicates itself in order to spread to other computers.

Common Types of Malware

Virus

- Upon execution, a virus replicates itself by modifying other computer programs and inserting its own code. Viruses are designed to be destructive.

Bots

- Snippets of code designed to automate tasks and respond to instruction. An entire network of compromised devices is a botnet, which can be used to launch a distributed denial-of-service (DDoS) attack.

Rootkit

- A Rootkit is a collection of malicious software that allows access to unauthorized users. Once installed, it becomes possible to hide the intrusion, as well as to maintain privileged access.

Common Types of Malware

Spyware

- Spyware is designed to gather data from a computer or other device and forward it to a third-party without the consent or knowledge of the user.

Keylogger

- Keylogger is software that can record all information that is typed on a keyboard, giving attackers access to sensitive information like passwords or credit cards.

Incident Response

Incident Response - organized approach to addressing and managing the aftermath of a security breach or cyberattack.

The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

IR Process

TripleP
Practical Proactive Privacy

Preparation

- Incident response plan and methodologies
- Network diagrams
- Logs.. Logs.. Logs
- Artifacts
- Paper work
- Incident response team
- Tools
- Practice and training
- Contact list

Identification

There are 2 important things to detect:
Detection and verification of the incident
Understanding the size and affected systems

To do this as quickly as possible, the team must lean on the monitoring capabilities they have created through the deployment of security tools that provide visibility into the network’s main crossroads.

Identification Cont.

Gather all relevant data and evidence to support the case and reaffirm that the proper steps are being taken.

- Artifacts
- Logs
- Network traffic
- Human evidences
- Signature of the threat

TripleP
Practical Proactive Privacy

Containment

- Old school – Shutdown the computer

- Moving the threat to controlled area
- Opportunity to look at the attacker’s capabilities
- Avoiding leakage or spread of the threat

Eradication

- Attacker’s IP Block
- Removing threats or malwares files
- Disposal of computers
- Disabling or deleting suspicious users
- Patch
- Updating security systems

Recovery

- Formatting and cleaning computers
- Data recovery
- Normal security log level
- Decrease readiness of IR team and management

Closures

- Reports
- Management
- Technical
- Security systems – update rules, install agents, etc.
- Workers awareness – trainings
- Procedures – update the procedures

Threat Hunting is the PROCESS

“Cyber Threat Hunting is the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.”

TripleP
Practical Proactive Privacy

Background

Beyond all-too-common corporate attacks, 2019 saw accelerated threat activity across a diverse range of targets and victims.

A growing assortment of nation-states used cyber probes and attacks to access everything from corporate secrets to sensitive government and infrastructure systems.

So, what can we expect on the cyber security front in the coming future?

CaaS
CYBERCRIME as a SERVICE

- When cybercriminals wanted to launch cyberattacks, they once had to know how to code.

- No longer.
- Bad actors can now search among any number of underground online sites to buy or lease potent cyberweapons.

Targets

When people think of data breaches, they usually think of big corporate victims like Yahoo, Target and Home Depot. However, the reality is that cybercriminals are increasingly targeting small businesses over enterprises, because an small business can’t afford to spend what a large corporation does on cybersecurity.

Popular CaaS Attacks

CaaS offerings on the Dark Web that are most likely to impact small businesses:

Phishing kits
Professional “phishing kits” are now available online which are very good at helping criminals impersonate legitimate organizations like banks. These kits may come with pre-written form letters which imitate the language, format and logos of real organizations; fake web pages to solicit the victim’s information; “crimeware” that automates the theft of online credentials; spamming software and more.

Popular CaaS Attacks

Exploit kits

Professional hackers sell “exploit kits” online (such as RIG, Neutrino and Sundown/Nebula) that incorporate vulnerabilities into a ready-made hacking tool or set of tools that make it easier for a criminal to break into a company’s network and/or infect it with malware.

Popular CaaS Attacks

Malware

Worms, Trojans and viruses are the crown jewel of any attacker's toolkit. Today, anyone can go onto the Dark Web and buy malware and malware kits, which they can use as-is or customize for specific targets. These online offerings even come with antivirus evasion.

Ransomware is extremely popular together with banking Trojans, remote access Trojans (RATs), keyloggers and mobile malware.

Popular CaaS Attacks

Criminal phone banks
A service in which criminals have created their own call center operation that can be rented out to other criminals. These are usually operated over VoIP lines in order to conceal their true location and make it easier to spoof phone numbers and impersonate legitimate organizations.
A criminal might rent a call center to support a phishing email campaign (“Call this number for assistance with your IRS claim”), or to social engineer an office employee or impersonate a company official to fool a bank.

Popular CaaS Attacks

DDoS-for-hire

Distributed denial-of-service (DDoS) attacks can be crippling to any business, as they can knock out websites, customer portals, email service and network connectivity.

Criminals used to have to build up their own “botnet” containing thousands of infected computers in order to launch these attacks, but now all they have to do is **rent a botnet service online**.

Cybercrime provides infrastructure-as-a-service.

Risks

Crime-as-a-service will increase the risks of financial fraud, cyber extortion and data theft for all types of businesses, but smaller companies are at the greatest risk.
By planning ahead for a network breach, the company can minimize the damage.

DeepFake

Deepfake is a technique for human image synthesis based on artificial intelligence. It is used to combine and superimpose existing images and videos onto source images or videos using a machine learning technique known as generative adversarial network.

DeepFake

The ability to digitally insert actors into films has been available since the mid-1990s:

DeepFake

Deepfakes employ artificial intelligence and allow anyone with a decent computer to make their own realistic fake videos starring just about anyone in the world, working only from a set of images or videos of their target.

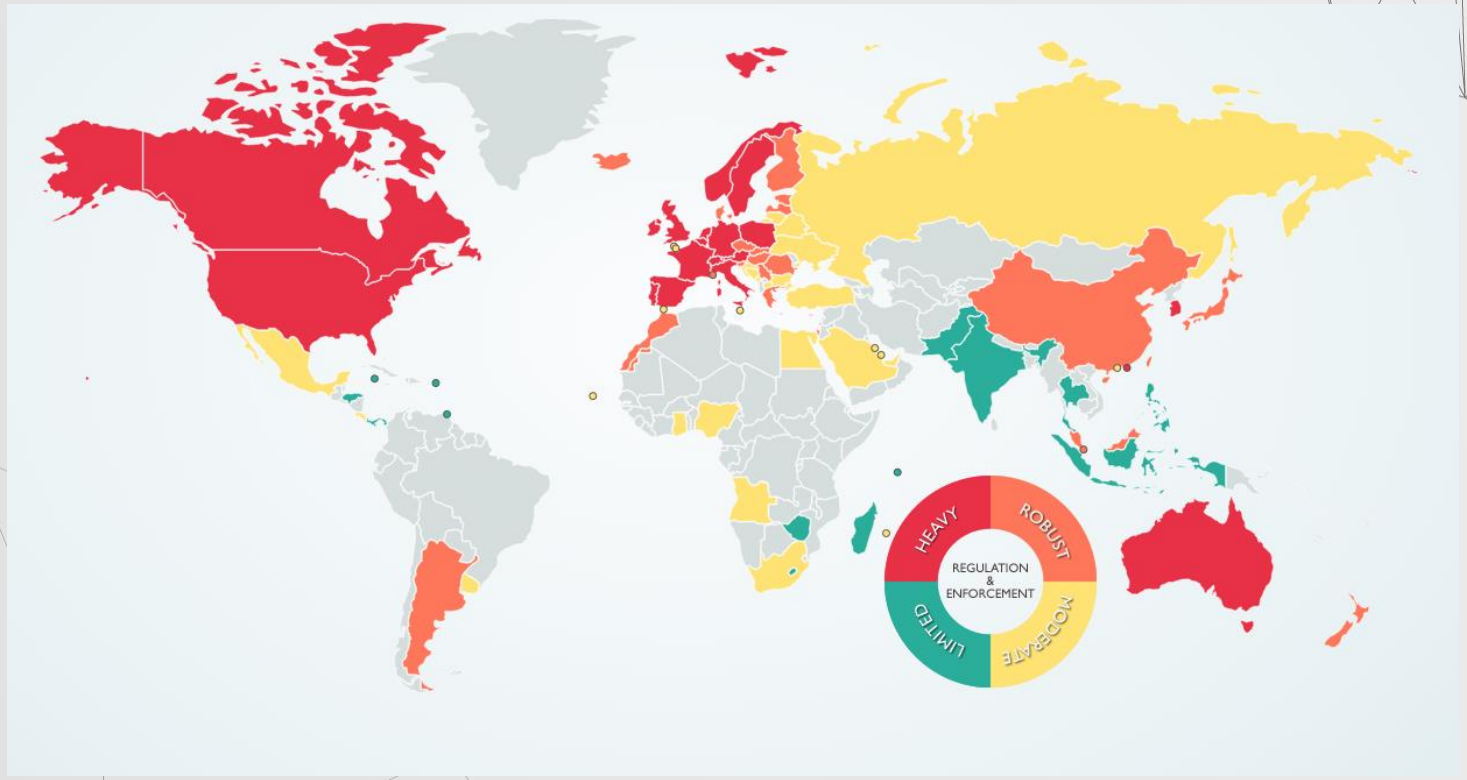
DeepFake

At the moment, the greatest worry is the use of it by state-sponsored actors that have the resources to create the most convincing possible videos. The real threat begins when anyone with a modern computer can create highly realistic manipulated videos at the push of a button.

DeepFake

Businesses must be vigilant and employ proper verification techniques – like multi-factor identification, facial recognition and comprehensive identity proofing – to thwart today’s AI threats,

Privacy



TripleP
Practical Proactive Privacy

Privacy

Privacy grow concern in:

- AI and Deepfake
- Social media
- Big Data
- Behavioral analysis
- Etc.

Privacy

As a result – Privacy regulations:

- IL Protection of privacy Law
- GDPR in EU
- CCPA in US
- LGPD in Brazil
- The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada
- Etc.

Privacy Regulations

The main subject:

- User’s rights
- Transparency
- Consent
- Data breach reports
- Sensitive personal information
- Organizations' risks

Privacy & Security

All this Means An Increased Need for Security
On top of improving transparency around the way we collect and use data, companies have to be prepared against data breaches to keep our customers' information secure.

Questions?

Privacy in Legal and Technical Aspects
Etti Berger, LLM. etti.berger@thetriplep.org
054-9222523

THANKS