ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat event	Threat source	Threat source characteristics **Capability**	Threat source characteristics **Intent**	Threat source characteristics **Targeting**	Relevance	Likelihood of attack initiation	Vulnerabilities and predisposing conditions	Severity and pervasiveness	Likelihood initiated attack succeeds	**Overall likelihood**	Level of impact	Risk
TE1	TS1	High	High	TS1	Possible	Moderate	IV1 and PD1	IV1	Moderate	Moderate	IM1	High
TE2	TS2	Moderate	High	TS2	Possible	High	IV2	IV2	Very high	Very high	IM2	Very high
TE3	TS3	High	High	TS3	Possible	High	IV3	IV3	Very high	Very high	IM3	Very high

THREAT EVENT

identifier	Threat event	Threat source	relevance
TE1	Exploited a web vulnerability on internal organizational information system (web server)	TS1	Possible
TE2	crafted phishing attack (Email)	TS2	Possible
TE3	delivered a targeted malware called ‘kaptoxa’ to control an internal systems(POS system) and exfiltration credit card data	TS3	Possible

THREAT SOURCES

identifier	Threat source	In scope	capability	intent	Targeting
TS1	Adversarial (an outside attacker)	Yes	High	High	Very high
TS2	Adversarial (an outside attacker)	Yes	Moderate	High	Very high
TS3	Adversarial (an outside attacker)	Yes	High	High	Very high

IDENTIFICATION OF VULNERABILITIES

identifier	Vulnerability source of information	Vulnerability severity
IV1	(**No public information**), hence a file stood out 'xmlrpc.php' since all files in the list were windows executable.	Moderate
IV2	The malware 'citadel 'was **publicly** known and was documented to have infected millions of computers in the past.	Very high
IV3	Malware was **publicly** known as 'kaptoxa'	High

IDENTIFICATION OF PREDISPOSING CONDITIONS

identifier	Predisposing conditions and source of information	Pervasiveness of condition

PD1	TECHNICAL(Architectural) Solutions for and/ approaches to user-based collaboration and information sharing (The Adversaries uploaded a php file leveraging the vulnerability, since it was likely the web application had a web upload functionality for legitimate documents (say, invoices)).	Moderate

IDENTIFICATION OF ADVERSE IMPACTS

identifier	Type of impact	Impact affected asset	Maximum impact
IM1	Harm to asset	(Information asset) the web server as exploited in order the adversary to execute code on the web application server	Very high
IM2	harm to individuals	Loss of personal identifiable information (stolen credentials of Target's HVAC vendor) (information asset)	Very high
IM3	harm to individuals and harm to asset	stolen customer credit card data (information asset) from the POS system (real asset)	Very high

NON-ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11
Threat event	Threat sources	Range of effects	relevance	Likelihood of event occurring	Vulnerabilities and predisposing conditions	Severity and pervasiveness	Likelihood event results in advice	Overall likelihood	Level of impact	risk
NTE1	NTS1	Very high	possible	Very high	NIV1 and NPD1	NPD1	Very high	Very high	Very high	Very high

THREAT EVENT

identifier	Threat event	Threat source	relevance
NTE1	Introduction of vulnerabilities into software products (where the php file ‘xmlrpc.php’ was uploaded to the web application)	NTS1	Possible

THREAT SOURCE

identifier	Threat source Source information	In scope	Range of Effects
NTS1	STRUCTURAL(software) –mission specific application (the web application)	yes	Very high

INDENTIFICATION OF VULNERABILITY

identifier	Vulnerability source of information	Vulnerability severity
NIV1	No security checks were performed in order to ensure executable files are not uploaded	Very high

INDENTIFICATION OF PREDISPOSING CONDITIONS

identifier	Predisposing conditions and source of information	Pervasiveness of condition
NPD1	TECHNICAL(Architectural) (uploads of legitimate files to the web application)	High

IDENTIFICATION OF ADVERSE IMPACTS

identifier	Type of impact	Impact affected asset	Maximum impact
NIM1	HARM TO ASSET	(Information asset) the web server as exploited in order the adversary to execute code on the web application server	Very high

Table of Controls

Identifier	Threat	Category	risk before control	risk after control	control
C1	TE1	Defend	High	Low	Continuous security monitoring
C2	TE2	Mitigate	Very high	Low	Education, Training and Awareness
C3	TE3	Mitigate	Very high	Low	Education, Training and Awareness Vulnerability analysis (from penetrations or scans)
C4	NTE1	Mitigate	Very high	Low	Training and continuous security monitoring

Risk Assessment Report

A risk assessment carried out on the 2nd December 2017 using the NIST standard. This is to evaluate and point out severities and priorities of risks to be able to draft their respective controls, regarding the Target attack incident which occurred on December 2013.Target is a discount retail shop in the United States.

From evaluation, the overall level of risk is very high. Two Treat event lead to the rise of risk, following an overall likelihood and a level of impact, both entities show a 'very high' chance of occurring when matched on the assessment scale of 'level of risk' on appendix I table I-2. The threat event is TE2 and TE3 with respect to the tables. Out of the Three (3) threats pointed out, one (TE1) had the least level of risk which pointed out to be 'high' with the sample methodology using the assessment scales of risk levels of overall likelihood and level of impact. Basically, the threat source for all three (3) threats were adversarial. The point of this evaluation is to scale overall likelihood and a level of impact in other to be able to prioritize risk, in such a way that would point out risk with higher priorities to the top. And to be able to draft controls in aim to defend, mitigate, transfer, accept or terminate risks.

A fitting control for TE2 (crafted phishing attack (Email), which points out to be 'very high', is education, the act of teaching and letting employees, contractors and anyone who holds confidential information, be aware of email phishing. Email phishing are scams carried out online by malicious persons with the use of fake websites or spam to look like real websites, email sand instant messages to trick one into divulging sensitive information like user credentials, credit card numbers or account passwords. The malware in use was the 'Citadel' which was publicly known to have infected millions of computers in the past. With proper education of letting employees know the ways and means of how this attack is carried out. Examples of awareness are:

- Providing personal or confidential information to any unsolicited website.
- Use websites with https
- Avoid opening strange messages from strange senders
- Amongst these the use of good antivirus antispyware software is also recommended

The second alarming risk is on the same level as the first, TE3 which was a malware was known as 'kaptoxa. The need of Training, Education, and awareness on malicious attacks like these, helps persons (employees be on the lookout). Penetration testing should also be a regular routine

The least on the late is the TE1 which point high and this was the Exploitation of the web application due to a vulnerability the attackers found. To top it all there was no public records regarding the vulnerability. There should be continuous security monitoring for security checks in order to ensure executable files are not uploaded future vulnerability exploitations there is the need to have formal procedures on application and operating system updates, since software are always updated to patch and fix loop holes in the source code. There is the need to update and apply available updates regularizes soon as possible.

For NTE1, The Adversaries uploaded a php file leveraging the vulnerability, since it was likely the web application had a web upload functionality for legitimate documents (say, invoices). Hence no security checks were performed in order to ensure executable files are not uploaded.

Awareness and training of employees is vital for an organization as said earlier. Continuous security monitoring of all devices, procedures, users and activities should be on track, logged and reported.