Security Onion Incident Response Report

Skills learned:

Virtualization Networking, Suricata, Zeek, Security Onion, Incident Response, Risk Mitigation, Network monitoring, Report writing, Project Planning

Lab Background:

For this project, I set up the *Security Onion* virtual machine to analyze pcap files using tools such as *Zeek* and *Suricata*. The pcap file that was being analyzed is from *malware-traffic-analysis[.]net*[1] and was so in a safe and enclosed environment. The company name that I will use for this project will be *Brick City Bits.* This lab was done for the learning purposes of network security.

Executive Summary:

While scanning the network I found multiple attempts to gain access to the company's webserver. The attack has been contained for the short term as well as long term. It was necessary to update the webserver's software since there have been multiple known vulnerabilities with past versions. Since there was an information leak, all users affected should change their passwords. Business operations have returned to normal.

What Happened and When?

Who is the response coordinator for this incident?	Francisco Di Giglio
What was the nature of the incident?	Threat actor sent malware into our network.
When did the incident occur?	The incident occurred on December 24, 2019.
Which specific IT resources were at risk?	The targeted resource was the web server of *Brick City Bits*.

[1] hxxps://www[.]malware-traffic-analysis[.]net/2019/12/25/index[.]html

What business processes were affected?	The webpage would be affected since the threat actor was able to gain access.
What is the severity or significance of the incident?	High severity.
Which third parties, such as vendors or customers (if any), were involved in or affected by the incident?	Any customers of *Brick City Bits* because it targeted their main form of business by targeting their webpage.
Did the incident result in the destruction or unauthorized disclosure or access of what might be considered personal data or personally identifiable information (PII)?	Yes. There was an information leak that the threat actor was able to access. This information can range from user accounts to employer information.
What might be the cybersecurity or privacy risks to the parties affected by the incident?	The risks from this attack could be data theft as well as increased chance of a follow-up attack specifically towards the users.
In which geographic regions was the affected data located?	Rochester, NY is where the web server is located, but the users affected are worldwide.
Who are the business owners and key stakeholders of the affected resources or data?	N/A

What Was the Root Cause?

What caused the incident?	The lack of updating key software, *ThinkPHP*, caused the issue.
How do we know?	Using Security Onion Web Interface and by using Suricata we have an alert of multiple exploits and two of them being

	ThinkPHP. To learn more about the alert we want to find the CVE related to it. To find the CVE I found an article talking about the ThinkPHP vulnerability and it had the CVE listed at the bottom. ***CVE-2018-20062***[2]
How confident are we in the assessment?	Confident only on specified network traffic since the data/information we have is limited.
What connections exist to past incidents, if any?	None

Details of Report:

Application Attacked	Source IP	Source Port	Destination IP	Destination Port	Attack Category
Joomla	139[.]199[.]184[.]166	52375	10[.]12[.]25[.]101	80	Web App Attack
ThinkPHP	139[.]199[.]184[.]166	61288	10[.]12[.]25[.]101	80	Admin Privileges
Web Server	10[.]12[.]25[.]101	80	139[.]199[.]184[.]166	58175	Information Leak

What Was and Remains to Be Done?

Identification: How was the problem detected?	Using the Security Onion VM, the packets that would come into the network were scanned using Suricata and Zeek. After the scan, the results of the scan were made available on the web interface of Security Onion. The results of the scans are

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20062

	known as alerts and these alerts showed us multiple attacks on the company's webserver.
Containment: How were we able to limit the incident's scope, including adverse effects on the affected data and systems?	In the short term, to limit the number of packets coming from the IP address of the threat actor, we will add their *temporary* IP address to the deny list for a short period of time (Approximately 24 hours).
Eradication: What steps were taken to eliminate adversarial presence from the affected environment, protect the affected data, or minimize the risks to the affected parties?	The first step would be to advise all users of such attacks so they can deal with their information leak as quickly as possible. The second step would be to update any software that the threat actor exploited. This will include ThinkPHP and Joomla. The third step would be to update passwords required to use Joomla.
Recovery: How and to what extent did we restore normal business operations or normal data processing activities?	After following the past steps of eradication there should be no reason not to restore normal business operations. Once the incident has been dealt with, it should be addressed publicly to let potential and current users know that it has been resolved.

What Lessons Can Be Learned?

How could the involvement of people help mitigate our future risks?	The involvement of people can help identify potential risks in a quicker manner.
How might we adjust processes to prevent the problem or allow us to respond better?	Increase the use of monitoring tools and keep updating software.
How might we use technology to enable us to improve?	Use technology to keep company up to date with recent vulnerabilities and if the company is using software that is vulnerable, proceed with the steps to secure said software.

What Are the Remaining Action Items?

Action	Responsible Party	Expected Start Date
N/A	N/A	N/A

Report Changelog

Date	Author	Change Description
10/24/2023	Francisco Di Giglio	Created Response Report

About this Document

This cybersecurity and privacy incident report is based on the template originally developed at Axonius Inc. by Lenny Zeltser and Elisabetta Tiani with input from Daniel Trauner. It's distributed according to the Creative Commons v4 "Attribution" License.