DS-7349 – Data and Network Security

Case Study - 1

**Apurv Mittal**

**In Collaboration with: Ravi Sivaraman**

Table of Contents

[Question 1: 2](#_Toc84090303)

[Main Differences between the reports: 2](#_Toc84090304)

[Main Similarities between the reports: 7](#_Toc84090305)

[Question 2: 8](#_Toc84090306)

[Question 3: 10](#_Toc84090307)

[Question 4: 14](#_Toc84090308)

[Next steps and trends for 2021 from Radware report: 14](#_Toc84090309)

[Next steps and trends for 2021 from Verizon report: 15](#_Toc84090310)

[Reference: 19](#_Toc84090311)

# Question 1:

Two Reports under consideration for this question:

1. DRIB – 2021 Data Breach Investigations Report by Verizon
2. Radware Research: The state of web application and API protection

## Main Differences between the reports:

1. Trends over the years

**Verizon**

Verizon report discusses the pattern over the years. It gives a comparative analysis of a certain trend shaping up over the years. For example: we can clearly see that the Ransomware attacks see a huge growth this year compared to previous years. It has really shot up after 2018.

Chart, line chart

Description automatically generated

Picture Reference: DRIB – 2021 Data Breach Investigations Report by Verizon

Radware

Radware report on the other hand is about the specific year 2020. It doesn’t give insights into how things are changing over the years and if there is a clear pattern.

1. Threat actors

Verizon

Verizon report does discuss about the threat actors for each attack types. It gives us details about who are the attackers to initiate such events. This will help organizations to be aware and may take necessary steps to protect themselves against such perpetrators.

For example: Social Engineering attacks are 100% of times from external to the organization. However, Privilege misuse is 99% of times internal users.

Radware

Radware report doesn’t give us insights into the actual attackers and their profiles. It does talk about the actual risk and attacks but seldom about whom organizations are protecting against.

1. Report Structure.

Verizon

Verizon report is more about the actual events. It’s based on hard evidence and real incidences. It goes into details of each kind of attacks, who were behind it, what were their intentions were, what was the loss for the organizations, what assets were compromised.

Radware

Radware is a survey of opinions of experts in the industry. It’s not based on the hard evidence or actual events. Its rather about what survey respondents thing is bigger issue and its impact.

1. Coverage

Verizon

Verizon report covers the attacks on the organizations over the past few years. It also includes the details about the industries, the impact of attacks on certain domain/industry higher over others, involved parties, impacted systems etc.

Radware

Radware is more about Infrastructure security. For example, the risk of attacks on API infrastructure, Mobile App security, SQL injection etc. Its focus is not on the industry or assets though it briefly talks about it.

1. Impact

Verizon

Verizon report effectively covers the impact of the different attacks like what assets are impacted, the frequency of such attacks, which industries are impacted, the dollar losses from the attacks etc.

Radware

Due to the nature of the report, it doesn’t cover the actual impact of the incidences or attacks on the organization. It does cover the kinds of attacks possible and where the organization should protect their assets but doesn’t really talk in length about the impact of each attack on the organizations.

1. Gini Coefficient

Verizon

Verizon report is very thoughtfully done. It talks about the Gini coefficient to give us a picture about how the incidents are spread across the organizations. It tells a clear tale that not all organizations are impacted equally or targeted equally by the attackers. For example, in below Gini plot, we can see the attack is not equally distributed over the days. Some days are worse than the others.

Chart, histogram

Description automatically generated

Source: Verizon 2021 Data Breach Investigations Report

Radware

We get no such in-depth details in Radware report.

1. Data Analysis

Verizon

Verizon report shares the details about how the data was collected and what data analysis was done on the captured data. It talks about the statistical models they tried however unsuccessful in providing the information and were discarded and replaced with more relevant models.

Radware

Radware report doesn’t share such details about the data analytics on the captured data.

1. Purpose

Verizon

The purpose of Verizon report appears to be more altruistic. Its more for the education of their readers. It does show the expertise of Verizon on this topic and confidence on the company grows at least about their expertise in this field.

Radware

Radware is not written for any altruistic reasons. Its main purpose is to market themselves and their services.

## Main Similarities between the reports:

1. Automation

Both reports are encouraging and recommending the automation over manual effort. It is consensus between two reports is that automation will help identify the vulnerabilities and prevent future attacks.

1. Ransomware

Both reports talk at length about the increased incidences of Ransomware attacks. It’s been reported that Ransomware attacks are becoming common and growing much faster than other attack types.

1. Education

Both reports succeed in educating their readers of the current trends in the cyber security. How organizations are getting attacked and what should be the focus of the organizations to protect their assets.

# Question 2:

Reports under consideration for this question:

*Radware Research: The state of web application and API protection*

|  |  |  |
| --- | --- | --- |
| **#** | **Emerging Trend** | **Business Impact** |
| 1 | Emerging Architecture – Containerization | Containerization approach is being preferred to isolate an application or business function from rest of the organization. This way even if a container gets breached the impact is localized to that application only and doesn’t impact rest of the systems/infrastructure easily. |
| 2 | Migration to Public Cloud | Organizations are migrating their applications to the public cloud. It helps with availability of computing resources, easy scalability etc. This way organizations pay for what they need and can easily upgrade both infrastructures to meet the demand as well as growing security needs.  Easy access to the best in-class security features though it still needs to be implemented and not available right out of the box. |
| 3 | Use of WAF (Web Access Firewall) | WAF (Web Access Firewall) is becoming popular due to its availability to thwart Denial of Service attacks.  There are many ways WAF protects against DDoS attacks, it has ability to monitor the API traffic, it can check for request patterns and can block certain requests, has ability to monitor the geo location and IP addresses of the requests etc.  DDoS is among the topmost attacks on the organizations. Majority of big corporates have seen multiple attacks on their infrastructure through brute force attack.  If successful DDoS attacks can bring down the servers and lead to major reputational and revenue loss for the organizations. |

|  |  |  |
| --- | --- | --- |
| **#** | **Emerging Trend** | **Business Impact** |
| 4 | Use of APIs | APIs are becoming popular, and most organizations depends upon APIs for their data needs and transfer of information. APIs are being used for large volumes of sensitive and  confidential information, which creates huge security risk of an attack on APIs.  APIs are a must have for the organizations these days to be able to operate efficiently. However, having a secured API layer is equally important to prevent breaches. |
| 5 | Increased use of Mobile Apps | With the advent of smartphones and their growing popularity all big and small companies are releasing their mobile apps.  As per the Radware report, mobile apps are not nearly as secure as web apps or pages. It’s reported that only 36% of mobile apps have fully integrated security and a large  proportion have no security at all.  This puts the organizations at huge risk of data breach via mobile apps. |

# Question 3:

Report under consideration for this question:

*DRIB – 2021 Data Breach Investigations Report by Verizon*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Major Incidences** | **What Happened?** | **How it Happened?** | **How was it fixed?** | **Impact** |
| 1 | ‘Sodinokibi’ Ransomware attack on Travelex | Foreign exchange company Travelex was hacked and lost access to its files and resources. All the important files were encrypted as part of the Ransomware attack.  Attackers wanted to be paid to allow Travelex to decrypt the files. | Its reported that the attackers could have got access to Travelex system by exploiting a vulnerability in their VPN servers which were not patched for 8 months.  Travelex uses Pulse Secure virtual private network (VPN) servers to provide employees with remote internet access to its central computers.  In addition, Travelex had allowed Microsoft's RDP to be accessible from the internet, without using network-level authentication, which means that it would be possible for hackers to access the login screens of computers on Travelex’s network and to use “brute force” software to guess passwords. | It’s been reported that Travelex has to pay ransom in the form of 285 bitcoins amounting to $2.3 million.  The attackers had instructed Travelex staff to use the secure Tor browser to visit a website which had a long pass key that unlocked instructions on how to pay a ransom to release decryption tools. | The attack resulted in at least 20 Travelex websites in different countries becoming inaccessible and left its outlets in airports and other retail sites without access to the internet or email or Travelex’s IT systems  The attack has also disrupted banks, including Sainsbury’s Bank, Barclays, HSBC, Virgin Money, First Direct and Asda Money, along with others that rely on Travelex to provide their foreign exchange services. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Major Incidences** | **What Happened?** | **How it Happened?** | **How was it fixed?** | **Impact** |
| 2 | Logistics Firm Toll Group Second Ransomware attack | The Toll Group got second Ransomware attack in 3 months. | MailTo, also known as Netwalker, attacked the company in early 2020. Then again in May of 2020 it got attacked by Nefilim ransomware that is likely distributed through exposed Remote Desktop Protocol (RDP) setups.   The malware used AES-128 encryption to lock files and asked for payments to share the keys. | Surprisingly, all the transactions were made through emails rather than the Tor network. However, the second time around The Toll group decided not to pay the ransom and decided to rebuild the core systems, scrubbed infected servers clean, and the used backups to restore files. | The Toll had to go back the manual process as more than 1000 servers were brought down. Since the firm got attacked the second time in 3 months, it took a big hit in terms of reputation in addition to the operational losses. |
| 3 | SolarWinds Supply Chain Attack | A highly sophisticated identity-based supply chain attack into a SolarWinds update server.  Hackers compromised the software updates posted on the SolarWinds website.  The backdoor in the update can execute commands to transfer and execute files, profile the system, reboot the machine and disable system services. | It’s suspected that - Hackers successfully accessed a software build server using the password “solarwind123.”  The hackers were able to bypass multi-factor authentication by using Admin rights. They forged SAML tokens to bypass multi-factor authentication. Since the SAML tokens are signed with their own trusted certificate, they can be used to log in to any on-premises resource or cloud environment, regardless of vendor. | A security firm FireEye discovered the attack and released a toolkit and instructions for user to check if they are compromised and take corrective action to plug the backdoor in the software updated downloaded. | -Treasury department - Pentagon - Commerce department - Other 6 govt. agencies - Oil and Gas Companies across the globe - SolarWinds has communicated that the number of customers that have this update is about 18,000.   Due to this large-scale attack, the impact has been huge. Large amount of sensitive information could have been exposed since major government agencies systems were compromised. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Major Incidences** | **What Happened?** | **How it Happened?** | **How was it fixed?** | **Impact** |
| 4 | Zero-day vulnerabilities in Adobe Type Manager Library | Microsoft reported that there is a vulnerability with how its OS handles Adobe Type 1 PostScript fonts. An attacker can craft a Type 1 PostScript font in such a way, that they gain the ability to execute arbitrary code on a Windows machine.  Id a user opens or previews the malicious document through the “Preview Pane” in outlook there is a high risk that an attacker may be able to take control of the machine.  Attackers can also exploit an extension to the HTTP called Web Distributed Authoring and Versioning (WebDAV), which allows users to collaborate on a document. | Earlier there were few proprietary fonts by Adobe which could be viewed in Windows machine only if user install a software called Adobe Type Manager. To improve user experience and improve their ability to have support for these fonts inbuilt into windows, Microsoft built the font support into its operating systems. Now, Windows Adobe Type Manager Library is used to support these fonts. | Microsoft suggested to its customers to disable the Web Client service, which allows users to use this feature and released a patch to fix this vulnerability in April of 2020. | This vulnerability was present in 40 different versions of the operating systems Windows 10, Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2012, Windows Server 2016, and Windows Server 2019. Though it was mostly impacting Windows 7 customers. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Major Incidences** | **What Happened?** | **How it Happened?** | **How was it fixed?** | **Impact** |
| 5 | Scripting Engine Memory Corruption Vulnerability | Microsoft reported that a vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. | Attackers exploiting this vulnerability may perform attacks by convincing a user to access to malicious websites or open maliciously crafted Microsoft Office documents. | Microsoft released a security update to address the vulnerability by modifying how the scripting engine handles objects in memory. | Impacted IE version were IE 9, IE 10, and IE 11  An attacker could gain access to the users’ machine with same user rights as the exploited user. which means if the user with admin rights logged in and the vulnerability is exploited then the attacker can assume the identity of admin user and take control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. |

# Question 4:

Two Reports under consideration for this question:

1. DRIB – 2021 Data Breach Investigations Report by Verizon
2. Radware Research: The state of web application and API protection

## Next steps and trends for 2021 from Radware report:

1. API Security

Applications are increasingly relying on APIs to speed up their development. APIs provide great flexibility and ability to efficiently exchange data among systems. With the increase in demand and usage of API based development, the security of information is also of grave concerns.

As reported in Radware report, majority of respondents believe that API security is one of the top priorities and they will be investing heavily in the API security.

1. Migration to Public Cloud

There is a growing trend of organizations moving to public cloud. As reported in the Radware report even though about 71% of the application development happens on-premises or private cloud the applications are increasingly hosted on the public cloud once they are in production.

Due to various benefits of public cloud like ease of scaling, latest security features, economies of scale, low maintenance, cost effectiveness, on-demand availability of resources etc. are the leading reasons organizations moving to public cloud.

1. Automation and Orchestration tools

Automation is the well accepted strategy used by organizations and expected to increase in 2021 and beyond. Automation not only reduces the manual tasks and makes it more efficient for the organizations, it helps with better security, reduces the errors and leads to identification of vulnerabilities earlier.

## Next steps and trends for 2021 from Verizon report:

Verizon report mentions that they are not in the business of predicting. So, there are no clear trends mentioned for future. However, we can infer the trends based on the trendline and details mentioned in the report. Following are the expected trends from the Verizon report:

1. External Actors involved in majority of attacks

The involvement of internal users (employees) is reducing over the years and most of the incidents are not instigated by the external actors. Which means the organizations have to continually invest in protecting their properties from the external attack even though the treat from internal employees still exists.

Social engineering incidences are still on the rise and among the major factors in the breaches.

Graphical user interface, chart, line chart

Description automatically generated

Source: Verizon 2021 Data Breach Investigations Report

1. Financial vs Espionage

Another important trend to notice in the Verizon report is the motive behind the attacks. Espionage as a motive is on the decline over the years while the financial motive appears to the be the biggest motive behind the cyber-attacks and rapidly increasing.

Chart, line chart

Description automatically generated

Source: Verizon 2021 Data Breach Investigations Report

1. Ransomware attacks on the rise

The ransomware attacks are on the rise and as mentioned in the previous trend, finance is among the biggest motives behind the attacks. It’s expected that Ransomware which is done with the motive to embezzle money is also on the rise.

Chart, line chart

Description automatically generated

Source: Verizon 2021 Data Breach Investigations Report

1. Denial of Service

Denial of service – DDoS attacks on the rise. In fact, majority of attacks in previous years are DDoS attacks. Organizations are continually getting attacked. WAF and other tools are being deployed by the organizations to protect themselves against such attacks. Nevertheless, it’s one of the biggest threat companies are facing and most have experienced that in past few years.

Chart, line chart

Description automatically generated

Source: Verizon 2021 Data Breach Investigations Report

# Reference:

1. DRIB – 2021 Data Breach Investigations Report by Verizon
2. Radware Research: The state of web application and API protection
3. <https://www.computerweekly.com/news/252476283/Cyber-gangsters-demand-payment-from-Travelex-after-Sodinokibi-attack>
4. <https://securityaffairs.co/wordpress/102012/apt/winnti-hit-south-korean-gaming-firm.html>
5. <https://blog.talosintelligence.com/2020/12/solarwinds-supplychain-coverage.html>
6. <https://securityboulevard.com/2020/12/the-solarwinds-supply-chain-hack-what-you-need-to-know/>
7. <https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language>
8. <https://spycloud.com/solarwinds-attack-breakdown/>
9. <https://www.bleepingcomputer.com/news/security/new-ransomware-strain-halts-toll-group-deliveries/>
10. <https://www.zdnet.com/article/transport-logistics-firm-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/>
11. <https://usa.kaspersky.com/blog/windows-adobe-type-manager-vulnerability/21223/>
12. <https://www.itpro.com/security/vulnerability/360887/microsoft-patch-tuesday-internet-explorer-zero-day>
13. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0674>
14. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601E-2020-0601>