Running head: Journal Specs for courses with Dr. Chris Veltsos

Journal Specs

Tram Nguyen

TABLE OF CONTENTS

[Entry 1 4](#_T-Mobile_data_breach)

**T-Mobile data breach exposed the personal info of more than 47 million people**

[Entry 2 4](#_Ransomware_Unplugged:_What)

**Ransomware Unplugged: What does the most recent cyber plague mean?**

[ENtry 3 5](#_How_to_Quantify)

**How to Quantify the Actual Cost of a Data Breach for Your Own Organization**

[ENtry 4 6](Our_IT_teams#_)

**“Our IT teams have an Incident Response Plan. We’re prepared for a cyberattack.” Maybe not.**

[ENtry 5 6](#_Hackers_Leak_VPN)

**Hackers Leak VPN Account Passwords From 87,000 Fortinet FortiGate Devices**

[ENtry 6 7](#_Stolen_Credentials_Led)

**Stolen Credentials Led to Data Theft at United Nations**

[ENtry 7 7](#_Pegasus_spyware:_All)

**Pegasus spyware: All you need to know**

[ENtry 8 8](#_How_APTs_become)

**How APTs become long-term lurkers: Tools and techniques of a targeted attack**

[ENtry 9 8](#_A_new_APT)

**A new APT is targeting hotels across the world**

[ENtry 10 9](#_China_declares_all)

**China declares all crypto-currency transactions illegal**

Tram Nguyen

CIS 450

Journal Specs – First Round

# **T-Mobile data breach exposed the personal info of more than 47 million people**

8/30/2021, T-Mobile data breach exposed the personal info of more than 47 million people |[link](https://www.theverge.com/2021/8/18/22630446/t-mobile-47-million-data-breach-ssn-pin-pii) |August 18,2021 | Richard Lawler

**Quick summary:** The article talks about the breach of T-Mobile in exposing the personal information of the customer and how T-Mobile investigates and troubleshooting.

**Reflection:**I was surprised to learn that T-Mobile had suffered a data breach that affected 100 million users and exposed the IMEI / IMSI data of 36 million of them. After reading this article, I can understand the importance of cyber security. I will appreciate taking this course to learn new technical skills and knowledge about cyber security. So, I think it is time to consider what I should do when I am affected by the data breach. I will change my password and PIN at least once a month and set up two-factor authentication for my all-online accounts right now.

“It’s offering two years of free identity protection services from McAfee, recommends postpaid customers change their PIN.” However, I wonder two years of free identity protection service is enough because most of the information is still relevant two years later such as SSN.

# **Ransomware Unplugged: What does the most recent cyber plague mean?**

**9/2/2021, Ransomware Unplugged: What does the most recent cyber plague mean? |** [link](https://vimeo.com/showcase/7413472/video/596172425) **| August 31 2021 | Sam Curry & Sean Costigan**

**Quick Summary: This is a live webinar between Sam Curry and Sean Costigan to answer some tough questions around ransomware such as should a company ever pay the ransom? Or what is the potential impact of an assault on revenue, brand, morale, and insurance premiums? And what can a company do to recover from such an assault or prevent it from happening in the first place?**

**Reflection:**

* **What are you hearing that's new/different? I heard that the bad guy uses social media to show donations, however, the truth is that they were stealing 2 million but donating 20 thousand, and the organizations who have allegedly donated to could not accept it. Another thing they develop is the ability to go back, and they try to maintain it and try to keep a footprint an interesting case. In the past, you could call up and they would walk you through getting your data back. Those are not the services they provide to companies and government organizations. Even though you have paid already, you are not likely to get your data back.**
* **How advanced is the ransomware industry? The attackers keep looking for more victims and more able to pay, so many of the cybercriminals operate from places where American law does not apply. The Justice Department has charged hackers in Iran, North Korea, and Russia, but none appear to risk extradition because those governments turn the blind eyes. If you are a ransomware producer and you do not target Russian companies and Russian citizens, you will be fine.**
* **Are things getting better (from the defense perspective, from law enforcement)? In the United States, which is a high-risk jurisdiction, OFAC laws impose sanctions on US persons (including corporations) doing company with or providing or getting benefits to or from governments, commercial entities, or persons located in, or foreign citizens of, Cuba, Iran, North Korea, North Sudan, Syria, and the Crimea region of Ukraine. Sanctions are also placed on persons on different US lists, particularly those designated international terrorists, regardless of country.**
* **What are the basics to defend from & mitigate ransomware impacts? The organization should back up data on a regular basis and ensure its safety. If the system has been infected, the organization should notify law police. They should give investigators vital information that will allow them to hunt down ransomware offenders, make them responsible under US law, and avoid future attacks.**

# **How to Quantify the Actual Cost of a Data Breach for Your Own Organization**

9/4/2021, How to Quantify the Actual Cost of a Data Breach for Your Own Organization | [link](https://securityintelligence.com/posts/how-to-quantify-cost-of-data-breach/) | August 25, 2021 | Julian Meyrick | (Barcomb, 2021) (Lakshmanan, 2021) (Montalbano, 2021)Security Intelligence

**Quick Summary:** The article talks about why organizations need risk quantification and provide the model or the services that help them quantify and address security risks. Key quotes:

* “Making up 14 percent of breaches in the survey, the average cost to companies of vulnerabilities in third-party software was USD 4.33 million. These cyberattacks include on the supply chain and the Internet of Things (IoT).”
* Using FAIR model and threat intelligence, “security experts in threat intelligence can assess the capability of the threat actors and their probability to attack your organization”
* “An assessment of your potentially disruptive business risks and quantifying in financial terms the potential business impact of the security risk scenarios that you face.”

**Reflection:**The report in this article makes me surprise. The cost of a data breach can be higher than 4 million and “the vulnerabilities in third-party software ranked among the top four most frequent initial attack factors listed.”. And I realize that risk quantification is a key strategy for a business’s risk management to adapt to the ever-changing threat landscape. As well, analyzing the probability and frequency of threat allows the organization to discover vulnerabilities in present controls or procedures that could put the company in danger of a bigger financial loss. That helps for my future career in understanding how business executives, and IT security officials address data breach disruptions to their organizations. After reading this article, I would like to learn more about the difference between risk quantification and the incident response plan. I am planning to write a reflection about that in my next journal.

# **“Our IT teams have an Incident Response Plan. We’re prepared for a cyberattack.” Maybe not.**

9/8/2021, “Our IT teams have an Incident Response Plan. We’re prepared for a cyberattack.” Maybe not | [link](https://securityintelligence.com/posts/incident-response-vs-cyber-crisis-management-plan/) | June 23, 2021 | Michael Barcomb | Security Intelligence

**Quick Summary:**The article consists of the difference between an incident response plan and a cyber crisis management plan, elements of a cyber crisis plan, and IBM Security X-Force. Key quotes:

* “IBM Security X-Force has experts who’ve worked with organizations to develop both incident response plans as well as business-wide cyber crisis management plans.”
* “It’s critical for a business to have a well-defined plan of action in place to respond as efficiently and quickly as possible to a cyber crisis.”

**Reflection:**There are a lot of new things I can learn from this article such as Cybersecurity incidents are handled efficiently by IT, but cybersecurity crises can have profound aftershocks that require a company's CEO to explain the incident to the board and its shareholders. So, it explains why the previous article says the business executives and IT security officials need to work together to address data breaches and the organization should respond in unison. Moreover, it provides detailed steps to prepare a cybersecurity crisis plan as defining the crisis and the path toward resolution.

This article reinforces that the risk quantification or cybersecurity crisis plan is essential for organizations. Last but not least, IBM Security X-Force, which is a threat intelligence and incident response system that helps guard against cybercrime. So, I realize the knowledge of cyber security is broad and interesting. I wish I can have a chance to do the team in preparing for a cyberattack.

# **Hackers Leak VPN Account Passwords From 87,000 Fortinet FortiGate Devices**

9/12/2021, Hackers Leak VPN Account Passwords From 87,000 Fortinet FortiGate Devices |link | September 9, 2021| Ravie Lakshmanan |The Hacker News

**Quick Summary:** By scanning unpatched computers, a criminal actor got the login names and passwords for 87,000 FortiGate SSL-VPN devices. Key quotes:

"These credentials were obtained from systems that remained unpatched against CVE-2018-13379 at the time of the actor's scan. While they may have since been patched, if the passwords were not reset, they remain vulnerable,"

**Reflection:**The new thing from the article is CVE-2018-13379. CVE-2018-13378 is a critical path security flaw in the FortiOS SSL VPN web interface. It allows the attacker to read the system file which includes password and username. I’m surprised that the threat actor leaked credentials for 74 countries, including the U.S, and CVE-2018-13379 was also one of the most often exploited issues in 2020.

I think the companies should install or upgrade the new critical Fortinet security version immediately to avoid falling victim to ransomware and other attacks that exploit vulnerability CVE-2018-13379. I wonder if Fortinet has any other solutions to prevent the attack such as multi-factor authentication instead of patching VPN serves when a vulnerability occurs.

# **Stolen Credentials Led to Data Theft at United Nations**

9/15/2021, Stolen Credentials Led to Data Theft at United Nations | [link](https://threatpost.com/data-theft-united-nations/169357/) | September 10, 2021| Elizabeth Montalbano | Threat Post

**Quick Summary:** The article talks about that how a threat actor used stolen credentials from a UN employee to access critical data in April, and the way UN response to that attack. Key quotes:

* “The attack ultimately was found to be the result of a Microsoft SharePoint flaw, allowing attackers to steal 400 GB of sensitive data.”
* “The attack highlights why simply using a username/password combination to secure entry into a system”

**Reflection:** I won’t surprise that the attacker can access deeper into the network because the user has not enabled 2FT to secure. That once again confirms the importance of 2-layer security. Upon discovery of the breach, Resecurity told the UN of the attack, and the UN did not believe the security firm's allegations until it provided proof of the breach's scope. After then, the UN stops responding with Resecurity. I think UN should work together with a security firm to address the problem

One story about my friend related to password security. She used only one password for all websites like Facebook, Inst, or Gmail. One day, one website with bad security she used was hacked that also meant the hacker already had both her username and password. It had put other accounts using the same password at r00isk. However, luckily, after she realized her account was hacked, she immediately enabled the 2-layer security for all access.

After practicing lab 3 and lab 4 in class, I know that once the attackers can hack into your security system, many tools support them to crack your password easily, and they can get your private information such as your bank account. That's why the second confirmation steps are becoming more and more important, and more and more companies are using 2-layer security, especially for remote employees, via cloud systems.

# **Pegasus spyware: All you need to know**

9/17/2021, Pegasus spyware: All you need to know |[link](https://www.deccanherald.com/specials/pegasus-spyware-all-you-need-to-know-772667.html) |November 1,2019 |David Binod Shrestha | DH Web Desk

**Quick Summary:**Pegasus has two vectors – zero-click and one-click to install and attack the target devices.

“The one-click vector is what was used in Mansoor's case, and involves a well-known technique called phishing”

“The zero-click vector is far more insidious as it does not require the target user to click or open a link.”

**Reflection:**Users receive the text message that contains a malicious link that does not make me surprise because I know that issues since many years ago. However, attacks can access to user’s device even they do not click or open the link. That makes me feel shocked. The spyware code via an internet connection installs itself into devices when the phone rings even though users ignore it. Moreover, the newest version of Pegasus can break two-factor authentication to access the data from cloud-based accounts.

Thanks to this article, I can know how the zero-click is dangerous and how to prevent the consequences of a virus or spyware infestation such as avoiding clicking on links or downloading files from unknown sources, disabling SMS push messages, disabling Wi-Fi, Bluetooth, and location services, and backing up the phone.

I wonder if the government consider buying the Pegasus spyware and use it to fight terrorism and organized crime. Another, whether Apple, Google, or other smartphone models will develop their security or any application to prevent hackers and notify users about their phones are infected while Pegasus becomes more powerful.

# **How APTs become long-term lurkers: Tools and techniques of a targeted attack**

9/18/2021, How APTs become long-term lurkers: Tools and techniques of a targeted attack |[link](https://www.csoonline.com/article/3633632/how-apts-become-long-term-lurkers-tools-and-techniques-of-a-targeted-attack.html)| September 16, 2016|Lucian Constantin |

**Quick summary**: McAfee’s report highlights how to detect highly skilled attackers despite having a simple malware infection investigation.

**Reflection:**After reading that article, I realize there are too many tools, backdoor programs, or techniques McAfee finds the APT attackers use such as PSexec, ProcDump, Mimikatz, PlugX…. However, to prevent the APT attack is a big program because it requires multi-layered approaches and investments that are too small to compare the number of victims who are attacked by APT.

I believe that the major reason why existing security has failed to reduce the danger of APT targeted assaults for so long is that the organization has placed too much emphasis on preventative security systems. Organizations' security architectures are frequently so focused on "Prevention" that they overlook other critical security components such as "Detection" and "Response." "Detection" is a security technique that aids in recognizing an attack as soon as it occurs and "Reacting" in the quickest time possible to obtain the best effect while minimizing needless losses. In fact, "Detect" and "React" security mechanisms are the most important security approaches for identifying and reducing threats from targeted assaults or sophisticated attacks if done correctly.

# **A new APT is targeting hotels across the world**

9/23/2021, A new APT is targeting hotels across the world|[link](https://therecord.media/a-new-apt-is-targeting-hotels-across-the-world/) | September 23, 2021| Catalin Climpanu | The Record

**Quick Summary:** For the past several months, the sophisticated persistent threat known as FamousSparrow has been hitting hotels all over the world, as well as governments, international organizations, engineering businesses, and legal firms.

**Reflection:**The new thing in this article is FamousSparrow uses vulnerabilities in the web application to gain access to their victim’s networks in Microsoft Exchange, Oracle Opera (application for hotel management), Microsoft SharePoint. After FamousSparrow gained access to a target network, ESET researchers discovered that the attackers installed a proprietary backdoor called SparrowDoor, which they utilized as a pivot point to organize ways to move laterally inside a compromised company using public tools like Mimikatz and Metasploit.

As I write for the article above, the organizations’ security architectures need to focus on “Response” and “React” systems also. And another, any attacker's objective is to obtain access to the Data layer. The Data Layer usually contains sensitive information that must be protected. Unfortunately, despite its importance, the Data layer receives minimal attention and few security measures when compared to the Network and Operating System. As a result, security measures for "Prevention," "Detection," and "Response" must be included in all four layers of an information system (Network, Operation System, Application, Data)

# **China declares all crypto-currency transactions illegal**

9/24/2021, China declares all crypto-currency transactions illegal |[link](https://www.bbc.com/news/technology-58678907) | BBC News

**Quick Summary:** All cryptocurrency-related operations are prohibited, according to the People's Bank of China, warning that this "seriously endangers the safety of people's assets."

**Reflection:**I've never been interested in Bitcoin, and I don't know much about it, so I was startled to learn that many crypto currencies, including Bitcoin, rely on a network of scattered computers to verify and authenticate transactions on a huge, shared ledger known as the blockchain. Individuals that participate in this work, known as crypto "mining," are given new "coins" at random.

However, I am aware that not only China has announced a crackdown on Bitcoin mining and trade, but also Korea, Thailand, and even my nation, Vietnam, have consistently said that Bitcoin and other similar virtual currencies are not legal currencies or payment methods. Bitcoin appears to be a component of efforts in these nations to address financial risks such as money laundering, illicit fundraising, multi-level investment fraud, and other unlawful and criminal activities.

As well, many risks happen on Bitcoin transactions related to cybersecurity. For example, users must pay the attacker to access a device and their accounts – ransomware. Cybercriminals benefit from the value victims have on their locked data and their readiness to pay a price to recover access to it in this sort of assault, rather than from the resale of stolen information on underground markets.

# **REFERENCE**

Barcomb, M. (2021, June 23). *“Our IT teams have an Incident Response plan. We’re prepared for a cyberattack.” Maybe not.* Retrieved from Security Intelligence: https://securityintelligence.com/posts/incident-response-vs-cyber-crisis-management-plan/

*China declares all crypto-currency transactions illegal*. (2021). Retrieved from BBC News: https://www.bbc.com/news/technology-58678907

Climpanu, C. (2021, September 23). *A new APT is targeting hotels across the world*. Retrieved from The Record: https://therecord.media/a-new-apt-is-targeting-hotels-across-the-world/

Cnstantin, L. (2016, September 16). *How APTs become long-term lurkers: Tools and techniques of a targeted attack*. Retrieved from https://www.csoonline.com/article/3633632/how-apts-become-long-term-lurkers-tools-and-techniques-of-a-targeted-attack.html

Lakshmanan, R. (2021, September 9). *Hackers Leak VPN Account Passwords From 87,000 Fortinet FortiGate Devices*. Retrieved from The Hacker News: https://thehackernews.com/2021/09/hackers-leak-vpn-account-passwords-from.html?utm\_source=feedburner&utm\_medium=feed&utm\_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29

Lawler, R. (2021, August 18). *T-Mobile data breach exposed the personal info of more than 47 million people*. Retrieved from Theverge: https://www.theverge.com/2021/8/18/22630446/t-mobile-47-million-data-breach-ssn-pin-pii

Meyrick, J. (2021, August 25). *How to Quantify the Actual Cost of a Data Breach for Your Own Organization*. Retrieved from Security Intelligence: https://securityintelligence.com/posts/how-to-quantify-cost-of-data-breach/

Montalbano, E. (2021, September 10). *Stolen Credentials Led to Data Theft at United Nations*. Retrieved from Threat Post: https://threatpost.com/data-theft-united-nations/169357/

Sam Curry & Seen Costigan. (2021, September 2). *Ransomware Unplugged: What does the most recent cyber plague mean?* Retrieved from vimeo: T-Mobile data breach exposed the personal info of more than 47 million people

Shrestha, D. B. (2019, November 1). *Pegasus spyware: All you need to know*. Retrieved from DH Web Desk: https://www.deccanherald.com/specials/pegasus-spyware-all-you-need-to-know-772667.html