Latest trends in the Cyber security after the solar wind hacking attack

Author 1: Mr. Naveed Akhter
MS/MPHIL of Computer Science
Pakistan.
NFC Institute of Engineering and Technology Multan, Punjab, Pakistan
Head of IT / IT Systems Manager
Research and Solution Multan

Author 2: Dr. Omer Aziz
Ph.D. degree in computer science
University of Management and Technology,
Lecturer with
the Department of Computer Science,
NFC IET Multan
Omer.aziz@nfciet.edu.pk .

Author 3: Tariq Hussain
BS Computer Software Engineering
Foundation university Rawalpindi Campus
Trainer in Computer Course.
Multan
Tariqh1994@gmail.com

***Abstract*—** That dominance, in any case, has gotten to be a risk. On Sunday, Solar Winds alarmed thousands of its clients that an "outside country state" had found a back entryway into its most well-known item, an instrument called Orion that makes a difference organizations screen blackouts on their computer systems and servers. The company uncovered that programmers snuck a malevolent code that gave them inaccessible get to customers' systems into an upgrade of Orion. The hack started as early as Walk, Solar Winds conceded, giving the programmers bounty of time to get to the customers' inside workings. The breach was not found until the unmistakable cyber security company FireEye, which itself employments Solar Winds, decided it had experienced a breach through the program. FireEye has not freely faulted that breach on the Solar Winds hack, but it allegedly affirmed that was the case to the tech location Krebs On Security on Tuesday. FireEye depicted the malware's bewildering capabilities, from at first lying torpid up to two weeks, to stowed away. That was December 13, 2020. FireEye gauges programmers to begin with picked up get to in Walk 2020. For about eight months, malevolent on-screen characters carted absent untold sums of touchy information from contaminated organizations — and the total scope of the breach is still unfolding. Despite Microsoft seizing the code's command and control server (a common component in botnet assaults as well), a few security specialists think the assailants may still have get to the Solar Winds Orion program system. Others are conjecturing that these programmers cleared out behind extra, yet-to-be-seen malevolent code.

Keywords—USA,Solar winds Attack,FireEye,Cyber security

I. INTRODUCTION

The disclosure that first class cyber spies in past months conducted the biggest hack against US authorities in a long time has put the highlight on Solar Winds, the Texas-based company whose program was compromised whereas overhauling a few of the greatest offices and companies within the Joined Together States. Solar Winds gives computer organizing observing administrations to organizations and government organizations around the world, and has gotten to be a prevailing player since it was established in 1999. "They're not a family title the same way that Microsoft is. That's because their computer program sits within the back office," said Victimize Oliver, a investigate investigator at Baird who has taken after the company for a long time. "Workers may have gone through their entire career without hearing around Solar Winds. But I ensure your IT office will know almost it."The firm was established by two brothers in Tulsa, Oklahoma, ahead of the dreaded turn-of-the-millennium Y2K computer bug. On an October gaining call, the company's chief official Kevin Thompson touted how distant it had come since. There was not a database or an IT sending demonstrate out there to which the company did not give a few level of checking or administration, he told examiners. "We don't think anybody else within the showcase is truly indeed near in terms of the breadth of scope we have," he said. "We oversee everyone's organize gear. "

That dominance, in any case, has gotten to be a risk. On Sunday, Solar Winds alarmed thousands of its clients that an "outside country state" had found a back entryway into its most well-known item, an instrument called Orion that makes a difference organizations screen blackouts on their computer systems and servers. The company uncovered that programmers snuck a malevolent code that gave them inaccessible get to customers' systems into an upgrade of Orion. The hack started as early as Walk, Solar Winds conceded, giving the programmers bounty of time to get to the customers' inside workings. The breach was not found until the unmistakable cybersecurity company FireEye, which itself employments Solar Winds, decided it had experienced a breach through the program. FireEye has not freely faulted that breach on the Solar Winds hack, but it allegedly affirmed that was

the case to the tech location Krebs On Security on Tuesday.

FireEye depicted the malware's bewildering capabilities, from at first lying torpid up to two weeks, to stowed away.

On Dec 13, 2020, Solar winds, an IT company that makes program for organize administration, expressed they were examining an occurrence that shows up to be the item of a "highly-sophisticated, focused on and manual supply chain assault by a nation-state." Solar Winds said they are in contact with the FBI which a defenselessness which existed until the March-June 2020-time period was utilized to require advantage of their Orion program item. The assault could be a supply-chain based assault in which the enemy can use the software's overhaul instrument. The Solar winds assault has been connected to the Treasury Office and FireEye compromises at this time. Data is being discharged persistently by those exploring the occurrences over the thousands of organizations that utilize Solar Winds, counting governments, militaries, and commercial substances around the world.

The FireEye breach was nothing brief of venturesome; FireEye features a notoriety for being the primary company that corporate cyberattack casualties will call. But at that point the news broke that the U.S. Treasury, State, Commerce, the National Established of Wellbeing and Country Security — the office entrusted with ensuring the government from cyberattacks — had all been infiltrated. Each of the casualties has one thing in common: All are clients of U.S. computer program firm Solar Winds, whose organize administration devices are utilized over the U.S. government and Fortune 500 companies. FireEye's web journal clarifying the breach — which didn't say how it found its possess interruption — said the programmers had broken into Solar Winds' arrange and planted a backdoor in its Orion computer program, which makes a difference companies screen their systems and armadas of gadgets, and pushed it specifically to client systems with a polluted computer program update. Solar Winds said up to 18,000 clients had downloaded the compromised Orion program overhaul, giving it The Solar Winds security breach was gigantic. More than 18,000 companies and government organizations were contaminated with a Trojan horse that introduced a carefully marked backdoor into their network. While exploring their claim hack, cybersecurity company FireEye found a single line of code in a Solar Winds upgrade that was "trepan sing Solar Winds Orion commerce program updates". That was December 13, 2020. FireEye gauges programmers to begin with picked up get to in Walk 2020. For about eight months, malevolent on-screen characters carted absent untold sums of touchy information from contaminated organizations — and the total scope of the breach is still unfolding. Despite Microsoft seizing the code's command and control server (a common component in botnet assaults as well), a few security specialists think the assailants may still have get to the Solar Winds Orion program system. Others are conjecturing that these programmers cleared out behind extra, yet-to-be-seen malevolent code.

II . **LITERATURE REVIEW**

Latest Trends in cyber security 2020 1)Toll Group: Toll Gather tops the list for the year's most exceedingly bad cyber- attacks since it was hit by ransomware twice in three months. In any case, a representative for Toll Bunch told Look Security the two episodes were not associated and were "based on diverse shapes of ransomware." On Feb. 3 the Australia-based coordination's company reported on Twitter that it had endured a cyber-attack. "As a preparatory degree, Toll has made the choice to closed down a number of frameworks in reaction to a cyber- security occurrence. A few Toll customer-facing applications are affected as a result. Our quick need is to continue administrations to clients as before long as conceivable," Toll Bunch composed on Twitter. The foremost later assault happened in May and included a moderately unused ransomware variation: Nephilim.

2)Marriott international:

The prevalent inn chain currently suffered a breach of information in two long periods. Marriott released a joint on Walk 31 unlocking data from 5,2 million visitors using the two officials' log-in accreditations on a property possessed by a business According to the report, the penetrate affected a Marriott application used to give guest organizations. "We embrace this development, which started in mid-January 2020," the assertion said. "Upon revelation, we affirmed that the login accreditations had been undermined, promptly started an examination, performed improved perceptions, and facilitated resources for enlighten and help visitors." While the examination is progressing, Marriott expressed that it has no motivation to accept that the information contained Marriott Bonvoy account passwords or PINs, installment card information, worldwide id information, public IDs, or driver's permit numbers. Regardless, polluted information may have For any situation, traded off information may have included contact data and data about customer steadfastness accounts. assault. Risk on-screen characters had effectively exfiltrated logins, individual data and assess data. The scope of the assault included eight Magellan Wellbeing substances and around 365,000 patients may have been affected. "On April 11, 2020, Magellan found it was focused on by a ransomware assault. The unauthorized performing artist picked up get to to Magellan's frameworks after sending a phishing mail on April 6 that imitated a Magellan client," the letter said. The company, which has over 10,000 workers, said at the time of the letter they were not mindful of any extortion or abuse of any of

the individual data. Phishing, a common assault vector, heightens over the year as risk performing artists refined their pantomime abilities.

4).Twitter:

The pervasive online media organization was penetrated in July by three individuals in an embarrassing event that saw a couple of prominent Twitter accounts seized. Through a social structure attack, a while later insisted by Twitter to be telephone phishing, the aggressors took workers' accreditations and gotten get to the organization's internal organization systems; small bunches of prominent records tallying those of past President Barack Obama, Amazon CEO Jeff Bezos, and Tesla and SpaceX CEO Elon Musk, were hacked. The threat performing specialists by then used the records to tweet out bitcoin stunts that acquired them more than $100,000. Fourteen days after the break, the Office of Equity (DoJ) summoned the three suspects and charged 17-year-old Graham Ivan Clark as an adult for the attack he purportedly "arranged," consenting to trained professionals.**5). FireEye and solar Winds supply chain assault victims:**

December eighth, FireEye set off a chain of occasions when it found that supposed country state developers had disregarded the security shipper and gotten

Magellan HEALTH

FireEye's reddish gathering instruments. On December 13, the firm uncovered that the country state assault was the consequence of a monstrous inventory network assault on Solar Winds. The secondary passage crusade was named "UNC2452" by FireEye, and it permitted danger to enter the framework.

creen characters to access diverse government and business structures around the planet The assaults are progressing, as per a joint assertion gave on December 17 by the Government Bureau of Examination, the Cybersecurity and Foundation Security Office, and the Office of the Executive of National Insights. Besides, the clarification uncovered that the inventory network assault affected the Orion stage. As indicated by CISA, it has "demonstrated that the Orion store network bargain isn't the underlying defilement vector utilized by the Well-fit entertainer."

III. Working and Explanation

The scale of a sophisticated cyber assault on the U.S. government hat was uncovered as of late is much greater than to begin with expected. The Cybersecurity and Framework Security Agency said in a outline that the danger postures a grave chance to the federal government. It included that state, nearby, tribal, and regional governments as well as critical infrastructure substances and other private division organizations are too at chance. CISA believes the assault started at slightest as early as Walk. Since at that point, numerous government agencies have allegedly been focused on by the programmers, with affirmation from the Energy and Commerce offices so far. Microsoft has not affirmed what source code was gotten to by the hackers. However, the truth that the programmers got in so profound is very stressing, given source code is vital to how any piece of computer program works. As portion of its continuous examinations within the SolarWinds cyberattack, Microsoft has revealed that its inner source code was likely gotten .

Who is influenced by this?

1. The hack is said to have a worldwide impact. Typically, since the influenced program is in utilize in parts of a trade having the potential to annihilate organizations.
2. Solar Winds, of Austin, Texas, gives network-monitoring and other specialized administrations to hundreds of thousands of associations around the globe, tallying most Fortune 500 organizations and government associations in North America, Europe, Asia and the Center East.
3. Solar Winds is working with FireEye as well as the FBI, the insights community, and other law requirement agencies.
4. The Pentagon, Centers for infection control and prevention and state office, equity office at the side beat 10 telecom administrators of the US are said to be influenced.
5. It has been assessed that over 33000 companies are said to be utilizing Sun based Winds, hence beneath effect.

Who is behind the assault?

1. Solar Winds educated that it was an exterior nation-state that attempted to penetrate its frameworks with malware.
2. However, not one or the other the US government nor the influenced companies have educated the open approximately the nation-state they think is dependable for these assaults.

Cyber-defense may be a difficult thing to do. Be that as it may, countering against governments dependable for deplorable hacks happens. The Joined Together States can presently oust ambassadors and can force sanctions.

What has happened?

1. The assault has been named as a state-sponsored assault and is said to be carried out by a country with beat hostile capabilities. The aggressor needed to utilize the government client information as educated by Fire Eye.
2. The assault was named Campaign UNC2452.
3. The hack started in Walk when a pernicious code was slipped into upgrades for the program, Orion, made by the company Solar Winds. This company screens the equipment and program systems of businesses and governments for outages.
4. This gave a chance to all the programmers to get to an organizations arrange to take information.
5. The clear months-long timeline gave the programmers sufficient time to extricate data from numerous targets.

Solar Winds Was the Culminate Point of Passage

Reuters has broken numerous stories almost the Solar Winds hack and its aftermath, but this piece takes a step back to see at the company at the heart of it. The IT administration firm has hundreds of thousands of customers—including 18,000 who were defenseless to Russia's attack—who depend on it for organize observing and other administrations. Its security hones show up to have been missing on a number of fronts, counting the utilize of the secret word "solarwinds123" for its upgrade server. (That's not suspected of being tied to the current assault, but … still.).

Interior FireEye's Reaction to the Solar Winds Hack

The Divider Road Diary this week shared unused subtle elements almost what happened interior FireEye prior this month because it found and reacted to its claim compromise. The tip-off: An worker gotten an alarm that somebody had logged into the company's VPN utilizing their qualifications from a modern gadget. Over 100 FireEye representatives locked in within the reaction, which included combing through 50,000 lines of code to sass out any variations from the norm.

Who Precisely Got Hit?

It's a great address, and one that's reaching to take a long time to reply. Microsoft this week at slightest shared a few beginning discoveries: More than 40 of its clients were the casualties of progressed compromise by Russia. (Microsoft itself was too hacked as portion of the campaign.) Of those 40, about half were companies within the IT division, whereas another 18 percent were government targets. Eighty percent were based within the US. This isn't implied to be a comprehensive see at the casualties; there are likely bounty more than what Microsoft has found so distant. But it does provide at slightest a imply at geology and category, not one or the other of which is particularly comforting.

What do we know so distant?

Here is our understanding of the situation:

The FireEye, Solar Winds and government organization hacks show up to be connected.

According to The Washington Post, the assault started with the IT merchant Solar Winds. Solar Winds CEO Kevin Thompson said that Solar Winds had been compromised through computer program overhauls that it sent to clients of its Orion IT observing stage between Walk and June. (Solar Winds' government clients incorporate the Office of Equity; the Census Bureau; a few national research facilities; and state, nearby, and outside clients such as the European Parliament and Britain's National Wellbeing Service.)

Late Sunday evening, FireEye affirmed that the later cyber assaults all stemmed from the compromised Solar Winds Orion program update.

Nation-state programmers moreover broke into different government offices — counting the U.S. Divisions of Treasury and Commerce — in a campaign that shows up to be connected to the as of late unveiled hack of security firm FireEye. Programmers broke into the Nation.

SUNBURST TTPs

Whereas the danger on-screen character utilized a few modern procedures to stow away command and control activity, such as mirroring Solar winds Orion activity and leveraging cloud suppliers to disguise as trusted relocated situations, the DNS tunneling procedures utilized are able to be identified with behavioral analytics and arrange discovery and reaction technology. This aggressor connected progressed procedures regularly credited to nation-state danger on-screen characters:

The compromise of the Solar Winds Orion overhaul component that was utilized to put inserts enormously extended the attacker's target scene.

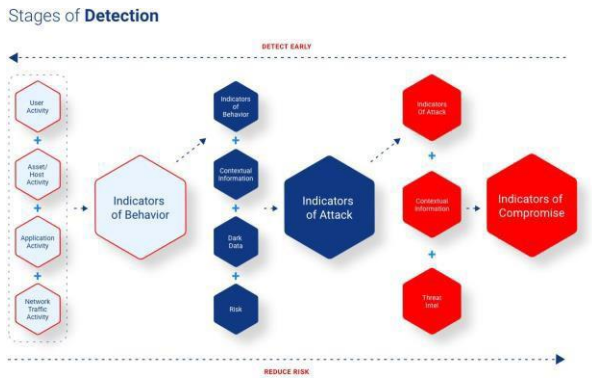
A apparently genuine program overhaul permitted them to use the supply chain to convey a backdoor computer program upgrade component called a energetic connect library.

Once interior, the risk on-screen character utilized different procedures to move along the side through computing systems undetected by utilizing modern avoidance capabilities, credential reuse, multi-factor confirmation bypass, and other progressed "living

Detect threats that have infiltrated your network

Organize Behavior and Reaction frameworks built on behavioral analytics can "see" these TTPs on the arrange. The NY Times reports that within the FireEye assault, for occasion, "the programmers went to uncommon lengths to maintain a strategic distance from being seen. They made a few thousand web convention addresses — numerous interior the Joined Together States — that had never some time recently been utilized in assaults.

By utilizing those addresses to arrange their assault, it permitted the programmers to way better conceal their whereabouts." This attack of unused space creation is something that behavioral analytics can identify amid this significant organize stay time. Stopping programmers in their tracks at the observation stage of interruption (or as "left of boom" as conceivable within the Miter ATT&CK System, for illustration) is basic. Once an foe moves along the interruption way, being able to outline recognized observables to threat techniques is additionally fundamental for way better deciding the leading and speediest course of remediation.



The part of behavioral analytics

There are methods for identifying nation-state movement prior utilizing behavioral analytics and a Master Framework, which can expect the activities of nation-state risk on-screen characters. Within the case of the Solar Winds assault, Iron Net examiners learned almost pointers that Iron Net analytics and its Master Framework are outlined to distinguish, counting:

Post compromise movement included sidelong development and information robbery. Our analytics and sensors are planned and situated to distinguish development inside the arrange, particularly when huge sums of information are exhilarated.

Solar Winds' Orion computer program system contains a backdoor that communicates by means of HTTP to third party servers. Iron Net's analytics particularly center on HTTP for space investigation, occasional and steady beaconing, and extraordinary rates.

Multiple trojanzied overhauls were carefully marked from Walk through May 2020 and posted to the Solar Winds overhauls site. Iron Net analytics look at certificates to distinguish abnormal activity.

Microsoft also affected

Microsoft on Thursday said it recognized a pernicious adaptation of the program from Solar Winds interior the company. Its examination so distant appeared no prove programmers had utilized Microsoft frameworks to assault clients, detailed news office Reuters. "Like other Solar Winds clients, we have been effectively searching for markers of this performing artist and can affirm that we recognized noxious Sun powered Winds doubles in our environment, which we confined and expelled," a Microsoft representative said, including that the company had found "no signs that our frameworks were utilized to assault others."

kmm/sms (Reuters, AP, AFP)

Investigation & Impact

The Inner group for Security and Investigate of the has found prove that the attackers gotten to a few inner source code within the company's frameworks. The Solorigate occurrence as Microsoft has named it within the composing, appeared there were attempted exercises past fair the nearness of malevolent Solar Winds code in our environment. They recognized unordinary action with a little number of inner accounts and upon review, they found one account had been utilized to see source code in a number of source code storehouses. Agreeing to the post, the account did not have required permissions to get to the code, to adjust it, nor was it authorized to get to the engineering systems. The company says so distant the examination affirmed no changes were made to this source code. These accounts were explored and remediated

Threat to Data

It is still not affirmed what source code was gotten to by the programmers. Be that as it may, the fact that the programmers got in so profound is very stressing, given source code is significant to how any piece of computer program works. Source code is the key to how a program item is built and in case compromised seem take off it open to unused, obscure dangers. Programmers could use this data to abuse any potential shortcoming within the programmed. Microsoft says this action has not put at chance the security of our administrations or any customer information, but includes they accept this assault was carried out by a very sophisticated nation-state performing artist. The company says that there's no prove that its systems were utilized to assault others.

Other Related Investigations

Based upon the advance examination, Microsoft assumed that aggressors might have knowledge of source code they depend on "open-source computer program advancement best practices" and "an open source-like culture" for advancement of program. Typically, source code is distinguishable by groups inside Microsoft, concurring to the web journal. Microsoft is downplaying the chance saying fair seeing the source code ought to not cause any new elevated risks. 3/6 Microsoft says it has bounty of defense assurances input to halt aggressors in case and when they do pick up get to. It says there's prove the exercises of the programmers were "thwarted" by the company's existing assurances.

Graveness

The issue with this cyberattacks is that it has been going on for so long that the full scale remains obscure. In truth, the assault may have begun prior than last spring as already accepted. It is expressed that at the minute the US government does not have difficult prove that classified government privileged insights were compromised by the hackers. The sheer scale of the assault too remains obscure, agreeing to most reports. Meanwhile, FireEye, which found the assault, has uncovered modern subtle elements around the Sunburst malware. The malware abused the Solar Winds Orion computer program, which is used by thousands of companies, counting a few US government organizations.

iv. Results & Conclusion

According to FireEye, Sunburst a noxious form of a carefully marked Solar Winds Orion plugin contains a backdoor that communicates by means of HTTP to third- party servers. It shows up that the plugin remains torpid period of up to two weeks, after which it begins executing commands and carrying out errands such as exchange of files, execute records, profile the framework, reboot the framework, and impair framework services. It moreover shows up that the malware "performs various checks to guarantee no analysis tools are present," agreeing to FireEye. This cautious approach is what made a difference the malware "evade discovery by anti-virus program and scientific agents for seven months after its presentation to the Solar Winds Orion supply chain," agreeing to the cyber- security firm.

v. References

1. Europol. Internet Organized Crime Threat Assessment, 2020. https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Sophos. The State of Ransomware 2020: Results of an independent survey across 26 countries, 2020. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020- wp.pdf

2. FBI. 2019 Internet Crime Report, 2020.https://pdf.ic3.gov/2019_ IC3Report.pdf [Accessed January 2020]

3. UK Government. Cyber Security Breaches Survey 2020, 2020. https:// www.gov.uk/government/publications/cyber-security- breaches-survey- 2020/cyber-security-breaches-survey-2020

4. Simoiu C, Gates C, Bonneau J, et al. "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In: Proceedings of USENIX Symposium on Usable Privacy and Security (SOUPS), Santa Clara, CA, 11–13 August 2019.

5. Connolly LY, Lang M, Guthega J, et al. Organizational culture, procedural countermeasures, and employee security behaviour: a qualitative study. Inf Comp Secur 2017;25:118–36.

6. Richardson R, North M. Ransomware: evolution, mitigation and prevention. Int Manage Rev 2017;13:10–21.

7. Connolly L, Wall SD. The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. Comput Secur 2019;87: 1–18.

8. Holt T, Bossler A. An assessment of the current state of cybercrime scholarship. Deviant Behav 2014;35:20–40.

9. Rege A. Incorporating the human element in anticipatory and dynamic cyber defense. In: Proceedings of the 2016 IEEE International Conference on Cybercrime and Computer Forensic, Vancouver, BC, 12–14 June 2016, 1–7.

10. Connolly L, Borrion H. Your money or your business: Decision-making processes in ransomware attacks. In: Proceedings of 2020 InternationalConference in Information Systems. Association for Information Systems, 14–16 December 2020.

11. Payne BK, Hawkins B, Xin C. Using labelling theory as a guide to examine the patterns, characteristics, and sanctions given to cybercrimes. Am J Crim Justice 2019;44:230–47.

12. Maimon D, Louderback E. Cyber-dependent crimes: an interdisciplina y review. Annu Rev Criminol 2019;2:191–216.

13. Atapour-Abarghouei A, Bonner S, McGough AS. Volenti non fit injuria: ransomware and its victims. In: 2019 IEEE International Conference on Big Data, IEEE, December 2019, 4701–7.

14. Choi KS, Scott TM, LeClair DP. Ransomware against police: diagnosis of risk factors via application of cyber-routing activities theory. Int J Forensic Sci Pathol 2016;4:253–8.

15. Zhao JY, Kessler EG, Yu J, et al. Impact of trauma hospital ransomware attack on surgical residency training. J Surg Res 2018;232:389–97.

16. Zhang-Kennedy L, Assal H, Rocheleau J, et al. The aftermath of a cryptoransomware attack at a large academic institution. In: Proceedings of the 27th USENIX Security Symposium. Baltimore, MD, 15–17 August 2018, 1061–78. ISBN 978-1-939133-04-5.

17. Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science 2019;8:2–22.

18. Shinde R, Van der Veeken P, Van Schooten S, et al. Ransomware: studyingtransfer and mitigation. In: Proceedings of the 2016 International Conference on Computing, Analytics and Security

Trends (CAST). Pune: IEEE, 19–21 December 2016, 90–.
19. Ioanid A, Scarlat C, Militaru G. The effect of cybercrime on Romanian SMEs in the context of wannacry ransomware attacks. In: Proceedings of the European Conference on Innovation and Entrepreneurship, Paris: Academic Conferences International Limited, 21–22 September 2017, 307–13.
20. Byrne D, Thorpe C. Jigsaw: an investigation and countermeasure for ransomware attacks. In: Proceedings of the European Conference on Cyber Warfare and Security. Dublin: Academic Conferences International Limited, 29–30 June 2017, 656–65.
21. Riglietti G. Cyber security talks: a content analysis of online discussions on ransomware. Cyber Secur 2017;1:156–64.
22. Agustina JR. Understanding cyber victimization: digital architectures and the disinhibition effect. Int J Cyber Criminol 2015;9:35–54.
23. Ngo FT, Paternoster R. Cybercrime victimization: an examination of Individual and situational level factors. Int J Cyber Criminol 2011;5: 773–93.
24. Furnell S, Emm D, Papadaki M. The challenge of measuring cyberdependent crimes. Comput Fraud Secur 2015;2015:5–12. Journal of Cybersecurity, 2020, Vol. 00, No. 0 13
25. Business Continuity Institute [BCI]. BCI Cyber Resilience Report.Business Continuity Institute, 2018.
26. Beazley. Breach Briefing, 2019. https://www.beazley.com/Documents/ 2019/beazley-breach- briefing-2019.pdf
27. Al-Rimy BAS, Maarof MA, Shaid SZM. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions. Comput Secur 2018;74:144–66.
28. Mansfield-Devine S. Securing small and medium-size businesses. Network Secur 2016;2016:14–20.
29. Renaud K. How smaller businesses struggle with security advice. Comput Fraud Secur 2016;2016:10–18.
30. Browne S, Lang M, Golden W. Linking threat avoidance and security adoption: a theoretical model for SMEs. BLED 2015 Proceedings, 2015, 35. http://aisel.aisnet.org/bled2015/35
32. Smith R. Ransomware is indiscriminate – secure your systems now, Petri, June 7, 2017. https://www.petri.com/ransomware-indiscriminate- securesystems-now
33. Kurpjuhn T. The SME security challenge. Comput Fraud Sec 2015;2015: 5–7.
34. Bergmann MC, Dreißigacker D, Skarczinski B, et al. Cyber- dependent crime victimization: the same risk for everyone? Cyberpsychol Behav Soc Network 2018;21:84–90.
35. Parkinson S. Are public sector organizations more at risk from cyberattacks on old computers?, The Conversation, 16 May 2017. https://the conversation.com/are-public-sector-organisations-more-at-risk- fromcyber-attacks-on-old-computers-77802
36. NIST. Guide for Conducting Risk Assessments, Information Security,NIST Special Publication 800-30. National Institute of Standards andTechnology, Gaithersburg, MD, 2012. https://nvlpubs.nist.gov/nistpubs/ Legacy/SP/nistspecialpublication800-30r1.pdf
37. Connolly L, Lang M, Wall DS. Information securitybehavior: a crosscultural comparison of employees in Ireland and United States. Inf SystManage 2019;36:306–22.
38. Connolly L, Lang M, Tygar JD. Employee security behaviour: the importance of education and policies in organisational settings. In: Paspallis N, Raspopulos M, Barry C, et al. (eds.), Advances in Information Systems Development Methods, Tools and Management. Lecture Notes in Information Systems and Organisation. Springer: New York, 2018: 79–96.
39. Brewer R. Ransomware attacks: detection, prevention and cure. Network Secur 2016;2016:5–9.
40. Connolly L, Wall SD. Hackers are making personalised ransomware to target the most profitable and vulnerable, The Conversation, 2019. https://theconversation.com/hackers-are-making-personalised- ransom ware-to-target-the-most-profitable-and-vulnerable-113583
41. Williams M. 10 disturbing facts about employees and cyber security, Pensar, 13 December 2018. https://www.pensar.co.uk/blog/i nfographic-10-disturbing-facts-about-employees-and-cyber-security
42. Browne S, Lang M, Golden W. The insider threat - understanding the aberrant thinking of the rogue 'Trusted Agent'. In: Proceedings of European Conference on Information Systems, Mu¨nster, Germany, 26–29 May 2015.
43. Creswell JW, Plano Clark VL. Designing and Conducting Mixed Methods Research, 2nd edn. Thousand Oaks, CA: Sage Publications, 2011.
44. Eisenhardt KM. Building theories from case study research. Acad Manage Rev 1989;14:532–50.
45. Zumbo BD, Gadermann AM, Zeisser C. Ordinal versions of coefficients alpha and theta for Likert rating scales. J Mod Appl Stat Meth 2007;6: 21–9.
46. Eurostat. Your key European statistics, Eurostat, 2020. https://ec.europa.

eu/eurostat/web/structural-business-statistics/structural-business- statis tics/sme
47. Porcedda MG, Wall DS. Cascade and chain effects in big data cybercrime: lessons from the TalkTalk hack. In: Proceedings of WACCO 2019: 1stWorkshop on Attackers and Cyber-Crime Operations, IEEE EuroS&P 2019, Stockholm, 20 June 2019.
48. UK Government. Procurement Policy Note 09/14: Cyber Essentials Scheme Certification, 2014. https://www.gov.uk/government/publicati ons/ procurement-policy-note-0914-cyber-essentials-scheme- certification
49. UK National Cyber Security Centre: Certificate Search. https://www.ncsc. gov.uk/cyberessentials/search
50. Eurostat, 2020b. https://ec.europa.eu/eurostat/tgm/table.do? tab ¼table& init ¼1&language ¼en&pcode ¼tin00170&plugin ¼1
51. Chapman J, Chinnaswamy A, Garcia-Perez A. The severity of cyber attacks on education and research institutions: a function of their security posture. In: Proceedings of ICCWS 2018 13th International Conference on Cyber Warfare and Security. Academic Conferences and Publishing Limited, 2018, 111–9.

About Authors:

Author2:

OMER AZIZ Received theM.S. degree in computer science from the National College of Business Administration and Economics, Lahore, Pakistan and the Ph.D. degree in computer science from the University of Management and Technology, Lahore He is currently working as a Lecturer with the Department of Computer Science, NFC Institute of Engineering and Technology, Multan. He has 14 years of professional experience in education and industry. He developed software applications, websites, and mobile application for different companies around the globe. He has strong analysis and software architecture design skills according to the emerging software market demand of data science, machine learning, cross platform, and artificial intelligence.

Author1:

NAVEED AKHTER Received MS degree in Computer Science from NFC IET Multan**.** Received the BS Degree in computer Software Engineering from Foundation University Rawalpindi. His research areas include big data, the Iot, and Software Design Architecture, Software Quality testing.

Author3:

Tariq Hussain Received the BS Degree in computer Software Engineering from Foundation University Rawalpindi. His research areas include big data, the Iot, and Software Design Architecture, Software Quality testing.

Latest trends in the Cybersecurity after the solar wind Hacking attack

Latest trends in the Cybersecurity after the solar wind Hacking attack

Latest Trends in the Cybersecurity after the solar wind Hacking attack on Public and Private Sector Companies in USA