Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 29-33 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

MODERN THREATS OF CORPORATE NETWORKS

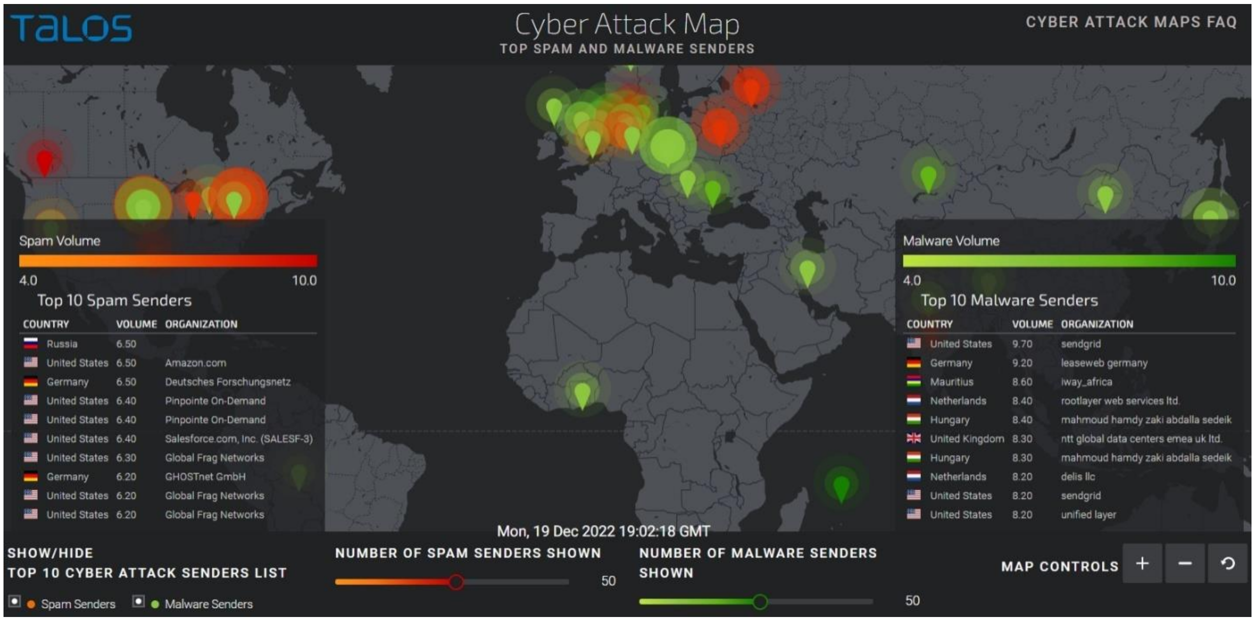
Giorgi Totladze, School Student
Nikoloz Erkomaishvili, School Student, N55 Public School
Nugzar Tomashvili, N166 Pubic Shool
Vano Mamporia, student, BTU
David Nioradze, N97 public school student

ABSTRACT:In our article, we reviewed modern threats in corporate computer networks and systems, will which cybercriminals have caused billions of dollars in damage to hundreds of medium-sized organizations and Giant Companies.we have discussed in detail the technologies through which various types of cyber-attacks were carried out around the world

KEYWORDS:*Dos Attack, Trojan, Malwares, Modern threats, Network security.*

Dos Attack

Denial of Service (DOS) attack is a type of attack that involves shutting down or delay a device or network. In other words, only one computer is used during attack and flooding servers with TCP and UDP packets. The goal of this attack is to overwhelm the target with traffic and making it inaccessible to users. The victims of this attack are such large companies as Google and GitHub on June 1, 2022, at 9:45 a.m., Google servers from 132 countries were receiving 10,000 requests per second. In exactly eight minutes, this rate increased tenfold, and this time 100,000 requests were made per second. Google's network security team immediately used the rule recommended by Cloud Armor and started blocking the traffic. In the two minutes the attack began to ramp up, growing from 100,000 Rps to a peak of 46 million Rps (request per second). Since Cloud Armor was already blocking the attack traffic, the attack continued as usual. Also, Google's work process was functioning normally. Over the next few minutes, the requests decreased significantly and finally at 10:54 am, the attacker probably determined that they did not manage to have the desired effect and slow down Google's work process, which would cause them the greatest financial loss. Also, an attack of such a scale needs huge financial support. There is a version that the attack stopped after 69 minutes because they did not get what they wantedand they could no longer see the point of continuing such an attack which requires gathering many DDOS bots and using them properly, as well as funding it all and organizing the biggest attack ever seen in the world in other words, the attackers saw that they could not achieve the result they wanted and stopped the attack and avoided spending more money. In addition to the fact that they wanted to cause financial damage by slowing down their service, they also researched how strong Google's servers are and how well they can withstand, an attack of like this and block traffic from different addresses and countries


TALOS
Cyber Attack Map
TOP SPAM AND MALWARE SENDERS
CYBER ATTACK MAPS FAQ
Spam Volume
4.0
10.0
Malware Volume
4.0
10.0
Mon, 19 Dec 2022 19:02:18 GMT
SHOW/HIDE
TOP 10 CYBER ATTACK SENDERS LIST
● Spam Senders
● Malware Senders
NUMBER OF SPAM SENDERS SHOWN
50
NUMBER OF MALWARE SENDERS SHOWN
50
MAP CONTROLS
+
−

Top 10 Spam Senders

COUNTRY	VOLUME	ORGANIZATION
Russia	6.50	
United States	6.50	Amazon.com
Germany	6.50	Deutsches Forschungsnetz
United States	6.40	Pinpointe On-Demand
United States	6.40	Pinpointe On-Demand
United States	6.40	Salesforce.com, Inc. (SALESF-3)
United States	6.30	Global Frag Networks
Germany	6.20	GHOSTnet GmbH
United States	6.20	Global Frag Networks
United States	6.20	Global Frag Networks

Top 10 Malware Senders

COUNTRY	VOLUME	ORGANIZATION
United States	9.70	sendgrid
Germany	9.20	leaseweb germany
Mauritius	8.60	iway_africa
Netherlands	8.40	rootlayer web services ltd.
Hungary	8.40	mahmoud hamdy zaki abdalla sedeik
United Kingdom	8.30	ntt global data centers emea uk ltd.
Hungary	8.30	mahmoud hamdy zaki abdalla sedeik
Netherlands	8.20	delis llc
United States	8.20	sendgrid
United States	8.20	unified layer

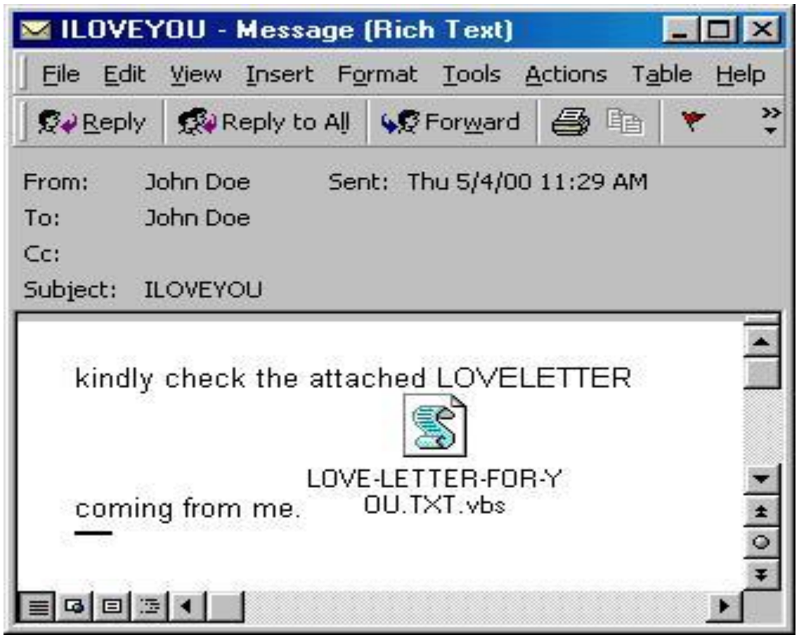
Trojan Horseand Malwares

Trojan horse is a type of malware that can pretend to be a legitimate program whilst it attempts to cause damage. There are myriad types of trojan horses which daily infiltrate our personal computers, and corporate networks and employees might be endangered by them Rootkit Trojan: firstly aids other malicious programs by concealing their activity so they can deal Maximum harm to the victim Backdoor Trojan: can create backdoors at the corporate networks which in advance will give remote access to the hacker, having access to the network hacker can get any kind of private information it can phone numbers of employees information of debit and credit cards by knowing this information hacker can still money from employs.

Remote access tool(RAT) [1,2] : Remote access tool gives the user ability to interact with the victim's personal computer, laptop, mobile phone, or server. By giving access to a user to join the private network so the user and victim will be on the same network, viruses created with the Remote access tool can be evasive. Furthermore, the virus can cover itself instantly when it gets on the victim's gadget. If victim download or open this type of virus hackers can access their desktops, files, emails, social media accounts, and webcams too. Programs such as NJ rat, Orcus, and quasar. Belong to the family of Remote access tools (RAT)[1,2] Worm is a type of virus that can replicate itself and spread in the network If the worm bypasses security then without alarming the owner of the personal computer, network, server, etc. will install malevolent programs on the victim's workstation. This malevolent program could be any type of virus pretending a legitimate program. I love you worm I love you is a type of worm it was created in 2000 4. I love you is also known as the “love letter virus” and the “love bug worm”. It was spreading so quickly that many companies (Microsoft, Ford Motor company, as well as government organizations like the pentagon) had to completely shut down their services as they tried to mitigate virus damage. It is written in Guinness records as the most destructive virus. It was replicating himself and scanning for multi-media files and was replacing the theme His clones would lead to files being destroyed and more worms being produced. I love you worm reached 45 million users in just 10 days and eventually, it resulted in more than 15 billion worth of harm.

A Backdoor Trojan attack on a corporate network may galvanize employees to be intimidated and taken advantage of Using social engineering because this type of malware only can get into the network by downloading and opening it. gives remote access to the hacker, which in advance helps a hacker to get the credentials of the victim and can gain access to the corporate network by using the victim's (employee) computer and get private information about a company. Remote access tool(RAT) can be used like a back door trojan but it gives hackers more accurate information cause he or they can see the victim's desktop and get information about every little thing happening on the victim's (employee) computer and use this information to exploit company and hacker can camouflage themselves as a victim's persona towards others by having information about a victim.

Defense against trojans and worms



From: John Doe Sent: Thu 5/4/00 11:29 AM
To: John Doe
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

Trojan defense program technologically takes on the classic defense [3-5]. Trojans trick users by letting in their personal computer most infections, this can be avoided by remaining cautious and using good security programs. Trojans look just like a game that has been downloaded for long time or an email that was sent from unknown source or from suspicious websites offering free content, it is better to download free programs from creator's site rather than unauthorized servers. Protection against common cyber threats and cybersecurity should on front line of defending yourself. A security solution must run fast, scan and alert you if Trojan virus is detected. There are many different types of Trojans, and each can do many different things. Once Trojan is inside, it can lay low and start collecting information. As well as start making back doors without getting detected, or it could just take over your computer. There are many ways to protect yourself:

- Having a fully patched computer behind a firewall
- Run diagnostic scans
- Automatically updating your operating system, ensuring the latest security updates
- Avoiding suspicious websites
- Being skeptical of unverified attachments and links in unfamiliar emails staying behind firewall
- Using strong password

The 21st century is the time that most people call the era of technology and the era of opportunity. Imagine in the 1950s if you told your friend who is in France, you would see him and talk to him from America. Your friends would laugh at you and consider you crazy, but today modern means of communication allow us to reduce the distance to a minimum and through virtual reality work together on different projects even from different continents of the earth. Cyberwar is one of the mandatory things when there is any conflict between countries [6]. By means of cyber war and the secret information obtained, the country can use all this to its advantage. Securing your company's digital data is incredibly important if you want to protect the sensitive data that might be contained on your network and computers, whether it be employee data, customer data, or company secrets. But no system is safe. A simple example of this is the well-known story of how a Russian hacker hacked the FBI with just one computer and symbolically left 1 dollar in all FBI bank accounts. Here I will also say thatthe program can help a person but not change the brain. Most people will understand what I want to say with all this later. Evgeniy Bogachev is a Russian hacker who has been indicted by the United States Department of Justice for his alleged role in several high-profile cyberattacks. He is believed to be the mastermind behind the Gameover Zeus botnet, which was used to steal sensitive information from computers around the world. In 2015, the U.S. government offered a $3 million reward for information leading to his arrest and prosecution. According to the public opinion Bogachev showed everyone that we can achieve a lot without support of servers and huge hardware. The main thing here is our brain and how we use it. The program can help a person but not change the brain. Perhaps you will have a question: How was the attack organized? While Bogachev knowingly acted in a role as an administrator, others involved in the scheme conspired to distribute spam and phishing emails, which contained links to compromised websites [7]. Victims who visited these websites were infected with the malware whichBogachev and others utilized to steal money from victim’s bank accounts.

Conclusions:

As we can see from our research, we investigated various well-known methods of compromising modern computer networks, as well as methods and technologies for protecting against such threats. The main thing is that we have received special skills to analyze different degrees of threats in modern computer networks and have learned the process of implementing these technologies in real everyday network service.

Acknowledgement: This work was supported by Shota Rustaveli National Science Foundation of Georgia [SPG-22-218]

BIBLIOGRAPHY

1. Johnson, N.T.; Waddell, P.G.; Clegg, W.; Probert, M.R. Remote Access Revolution: Chemical Crystallographers Enter a New Era at Diamond Light Source Beamline I19. *Crystals* 2017, *7*, 360. https://doi.org/10.3390/cryst7120360
2. D. Hou, Z. Miao, H. Xing and H. Wu, "V-RSIR: An Open Access Web-Based Image Annotation Tool for Remote Sensing Image Retrieval," in *IEEE Access*, vol. 7, pp. 83852-83862, 2019, doi: 10.1109/ACCESS.2019.2924933.
3. Z. Huang, Q. Wang, Y. Chen and X. Jiang, "A Survey on Machine Learning Against Hardware Trojan Attacks: Recent Advances and Challenges," in *IEEE Access*, vol. 8, pp. 10796-10826, 2020, doi: 10.1109/ACCESS.2020.2965016.
4. D. Yang, C. Gao and J. Huang, "Dynamic Game for Strategy Selection in Hardware Trojan Attack and Defense," in IEEE Access, vol. 8, pp. 213094-213103, 2020, doi: 10.1109/ACCESS.2020.3040395.

5. K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia and Y. Makris, "Amplitude-Modulating Analog/RF Hardware Trojans in Wireless Networks: Risks and Remedies," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3497-3510, 2020, doi: 10.1109/TIFS.2020.2990792.
6. Maksim Iavich, SergiyGnatyuk, Giorgi Iashvili, AndriyFesenko, ENSURING EUROPEAN CIVIL AVIATION CYBERSECURITY, Scientific and practical cyber security journal, 2019.
7. Maksim Iavich, SergiyGnatyuk, Giorgi Iashvili, AndriyFesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019.