Cybersecurity threats and mitigation practices

Cyberattacks remain an increasing threat across all critical infrastructure sectors in Kazakhstan. Threat to the various industries has increased dramatically along with the sophistication of cyberattacks.

We have witnessed in recent times massive attacks on IT infrastructure of Kazakhstani state bodies, financial and educational institutions, which led, among other things, to disabling emails and online-banking transactions which means that we are under constant cyberattack in the said sectors, and no organization can escape that reality.

Given the increasingly sophisticated and widespread nature of cyberattacks industries and government should fully recognize the dawning of this new era of cybercrime and make cybersecurity a highest priority.

Today one must take every step possible to protect information systems by implementing of vetted cybersecurity practices and organizations should be moved towards consistency in mitigating the current most pertinent cybersecurity threats to the sectors mentioned. For each gain delivered by automation and data analytics, the vulnerability to malicious cyberattacks increases as well. To thwart these cyberattacks before they occur, it is crucial for local organizations to establish, implement, and maintain current and effective cybersecurity practices.

The goal of this publication is to raise awareness, provide practices and move towards consistency in mitigating the current most impactful cybersecurity threats.

The three threats explored in this publication are as follows:

- Phishing Attack
- Ransomware Attack
- Tech Support Fraud

Phishing Attack

Email phishing is an attempt to trick you, a colleague, or someone else in the work place into giving out information using email. The email often appears to come from a legitimate source such as a friend, coworker, manager, company or even the user's own email address. An inbound phishing email includes an active link or file, often a picture or graphic. Clicking to open the link or file takes the user to a website that may solicit sensitive information or proactively infect the computer. Accessing the link or file may result in malicious software being downloaded or access being provided to information stored on your computer or other computers within your network. Cybercriminals behind phishing attacks are called phishers.

The information that phishers attempt to steal can be user names and passwords, credit card details, bank account information, or other credentials. Attackers can then use stolen information for malicious purposes, such as hacking, identity theft, or stealing money directly from bank accounts and credit cards. Phishers can also sell the information in cybercriminal underground marketplaces.

Phishing emails can be very effective, and so attackers can using them to distribute ransomware through links or attachments in emails. When run, the ransomware encrypts files and displays a ransom note, which asks you to pay a sum of money to access to your files.

Practices to consider

Be suspicious of emails from unknown senders, emails that request sensitive information. Don't open attachments or click links in unsolicited emails, even if the emails came from a recognized source. If the email is unexpected, be wary about opening the attachment and verify the URL.

Organizations should educate and train their employees to be wary of any communication that requests personal or financial information and instruct them to report the threat to the

company's security operations team immediately. To lower cybersecurity risks one needs to reduce the use of unlicensed software and keep software up-to-date. Doing so requires implementing effective software management policies and procedures and investing resources in increasing awareness of the potential dangers associated with using unlicensed software.

Ransomware Attack

Ransomware is a type of malware, malicious software, distinct from other malware. Its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. Afar the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker usually in a cryptocurrency to receive a decryption key.

However, hackers may deploy ransomware that destroys or exfiltrates data, or ransomware in conjunction with other malware that does so. Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data. Ransomware threats may incorporate tactics or techniques that are the same as or identical to other threats. For example, successful phishing attacks may lead to the installation of ransomware.

Most ransomware infections start with:

- Email messages with attachments that try to install ransomware.
- Websites hosting exploit kits that attempt to use vulnerabilities in web browsers and other software to install ransomware.

Once ransomware infects a device, it starts encrypting files, folders, entire hard drive partitions using encryption algorithms like RSA or RC4.

Ransomware is one of the most lucrative revenue channels for cybercriminals, so malware authors continually improve their malware code to better target enterprise environments. Ransomware-as-a-service is a cybercriminal business model in which malware creators sell their ransomware and other services to cybercriminals, who then operate the ransomware attacks. The business model also defines profit sharing between the malware creators, ransomware operators, and other parties that may be involved. For cybercriminals, ransomware is a big business, at the expense of individuals and businesses.

Practices to consider

Organizations can be targeted specifically by attackers, or they can be caught in the wide net cast by cybercriminal operations. Large organizations are high value targets and attackers can demand bigger ransoms.

We recommend:

- Back up important files regularly. Use the 3-2-1 rule. Keep three backups of your data, on two different storage types, and at least one backup offsite.
- Apply the latest updates to your operating systems and apps.
- Educate your employees so they can identify social engineering and spear-phishing attacks.
- Controlled folder access. It can stop ransomware from encrypting files and holding the files for ransom.

Tech Support Fraud

Tech Support Fraud is an industry-wide issue where scammers use scare tactics to trick users into paying for unnecessary technical support services that supposedly fix contrived device, platform, or software problems.

Scammers attempt to convince victims to provide remote access to their devices by impersonating a wide range of reputable technology companies. Victims spend hundreds of dollars on these phony tech support services.

Scammers may call you directly on your phone and pretend to be representatives of a software company. They might even spoof the caller ID so that it displays a legitimate support phone number from a trusted company. They can then ask you to install applications that give them remote access to your device. Using remote access, these experienced scammers can misrepresent normal system output as signs of problems.

Scammers might also initiate contact by displaying fake error messages on websites you visit, displaying support numbers and enticing you to call. They can also put your browser on full screen and display pop-up messages that won't go away, essentially locking your browser. These fake error messages aim to trick you into calling an indicated technical support hotline. When you engage with the scammers, they can offer fake solutions for your “problems” and ask for payment in the form of a one-time fee or subscription to a purported support service.

It is worth mentioning that malware authors are always looking for new ways to infect computers. Follow the simple tips mentioned above to stay protected and minimize threats to your data and accounts.

Practices to consider

- Do not reply to unsolicited email messages or unsolicited phone calls to request personal or financial information, or to fix your computer.
- Download software only from official vendor websites. Be wary of downloading software from third-party sites, as some of them might have been modified without the author’s knowledge to bundle support scam malware and other threats.
- Enable antivirus programs to use them when browsing the internet. They can help blocking known support scam sites as well as detecting and removing known support scam malware.

What to do if information has been given to a tech support person

- Uninstall applications that scammers asked to install. If access has been granted, consider resetting the device.
- Monitor anomalous logon activity.
- Run a full scan with antivirus programs to remove any malware. Apply all security updates as soon as they are available.
- Change passwords.
- Call your credit card provider to reverse the charges, if you have already paid.

Author:

Bolat Assylkhanov

Senior Lawyer, Industry & Trade department

Almaty, Kazakhstan

M +7 701 762 5165

bassylkhanov@gratanet.com