precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 19 March 2023

Dr. Ronald Walcott
Managing Director

Today we will look at How to identify hacking attempts and techniques (illegitimate websites, phone calls, social engineering, email phishing, etc.) and mitigate them.

Most computer vulnerabilities can be exploited in an array of different ways. Hackers have developed varying exploit techniques and may either use one or multiple, different techniques at the same time. It is also very common for weaknesses or vulnerabilities to be exploited because of human error such as misconfigurations or even a backdoor left open from a previous attack that was never rectified. Knowing all these possibilities exist, detecting hacker attacks is still not an easy task, especially for someone who is inexperienced and doesn't know exactly what trends, patterns or inconsistencies to look for.

These are a few things you can look out for that would most likely help you to identify a threat:

- **Suspiciously high levels of outgoing network traffic -** if you notice the rate of traffic on your network between IP addresses have been irregular, then it is likely an indication of a compromise. Your device may be the target of a hacker who is sending copies of information or just using computer resources.
- **Increased activity or suspicious looking files** - If a hacker manages to hack into a system, they usually run a scan to locate important files, such as logins, passwords, etc. If you notice major disk activity or memory usage even when the system is idle, then this could be an indication of compromise (system hack or malware infection).
- **Escalated program privileges -** if applications are using excess resources or have privileges to do certain processes that it shouldn't, then it is likely that there is a compromise on the system.
- **Attacks using credentials -** Some hackers may gain access to user accounts and may be able to log on and use the user privileges as a means of monitoring, stealing or compromising information.

Once you know how to identify threats and indications of compromise, then you can take the next step and take action to help mitigate the risk of these compromises and threats happening.

In this Issue:

COMMON TECHNIQUES CYBER CRIMINALS USE TO STEAL INFORMATION.

Hackers use a variety of different techniques that are still being proven effective up to this day. These techniques help hackers unknowingly or disguisedly steal sensitive information from people who may not be able to identify these tactics or may not be alert at all times:

- **Social Engineering:** This refers to a manipulation technique that hackers/cyber criminals use to exploit human error to gain access to private information, secured access or credentials and valuables (money, privileges, etc.). Cyber criminals may pretend to be someone they are not, and extract information from individuals who may not know any better.
- **Phishing:** This a type of online scam where cyber criminals impersonate legitimate organizations via email, text, websites, etc. in order to steal sensitive information. People may receive links in their emails or via text messages that would direct them to a replica website that looks legitimate, that would capture any information being entered on the site.

HERE ARE A FEW WAYS TO HELP MITIGATE THE RISKS OF COMPROMISES:

- **Find all possible internal breaches -** Information security officers could use application whitelisting, as a means to ensure security resilience.
- **Security and Audit logs**
- **Use protective software -** Some software, like Azure Advanced Threat Protection for example, will create profiles about users to know what is classified as normal behaviour through logs and network activity. This means that Azure is able to notice any irregular behaviour and alerts and prevents hacking attempts and breaches before it gets any further.
- Backup data and information - Having backups of information in multiple locations such as on a backup hard disk, tape or even in the cloud could ensure that the business is able to function and recover even after an attack or data has been compromised.
- **Proper training -** Employees must know the practices and procedures when dealing with company related data. Human error accounts for 88% of breaches today. Having the knowledge and correct training could help reduce the risk of vulnerabilities being exploited by hackers.
- **Having and enforcing good policy -** Policies help guide a business' operations. If a business has good policies in place, they can use the best practices to help ensure or reduce the likelihood of a breach or attack occurring. Just like any rules or laws, policies must also be enforced by the company

Frequently Asked Questions:

WHAT ARE SOME OF THE MOST COMMON VULNERABILITIES THAT HACKERS EXPLOIT?

Hackers exploit any vulnerabilities they encounter. Some of these are human errors, faulty configurations, software flaws, opened ports, broken authentication, cross-site scripting, SQL Injection, weak passwords and security.

IS THERE ANY WAY TO COMPLETELY REMOVE THE RISK OF BEING HACKED?

The short answer is no. Hackers are always devising new ways and techniques to exploit people. Just as new technology and defensive techniques and strategies develop, hackers are always evolving and coming up with new ways to find holes and cracks in our defences. It is our responsibility to reduce the chances of them being successful.

WHAT IS THE WORST THAT CAN HAPPEN IF A BREACH IS SUCCESSFUL? CAN INFORMATION AND RESOURCES NOT BE EASILY RETRIEVED?

In most instances, hackers monitor systems and networks before taking any noticeable action. They usually make minor changes to remain unnoticed until their plan to reveal themselves and their intention is ready. By this time, device may have been locked, backups deleted, configurations tampered with etc. This makes it even more difficult to find out what exactly they were after, it makes recovery even more expensive and could also mean a business having to close down operations.

Headline News

Ransomware operators retooling their approach to make their attacks more effective

Stung by the FBI's infiltration and takedown of the Hive ransomware group, other ransomware operators have been retooling their approaches to make their attacks more effective and operations tougher to disrupt, says Yelisey Bohuslavskiy, chief research officer at threat intelligence firm Red Sense.

Credit needs to go to defenders both public and private, he says, for having upped their game. In response, ransomware operations have been forced to find replacements for tools and strategies they previously relied on, including botnets, Cobalt Strike beacons and dedicated blogs for naming victims and dumping stolen data.

"Groups that are operating now, they're going away from this blog-centric infrastructure," Bohuslavskiy says. "Some of them, like Karakurt for instance, or Silent Ransom Group, they're not even using blogs for extortion. They communicate with their victims via ProtonMail, exactly in order to avoid a situation in which you have all your negotiations being taken over by the government."

In this video with Information Security Media Group, Bohuslavskiy also discusses:

- Major "damage amplification" innovations across what he characterizes as the three modern ransomware eras - from WannaCry to REvil to the post-Conti landscape.
- How "hacking is weaponized creativity" for cyber criminals.
- Why ransomware groups are ready to embrace social engineering and business email compromise attacks.

Bohuslavskiy is chief research officer and a partner at Red Sense. He previously served as co-founder and head of research and development at threat intelligence firm Advanced Intelligence. He has also worked in other roles including cyberthreat intelligence analyst at Flashpoint and due diligence researcher at Kroll.

Upcoming Events

ISMG ENGAGE
April 19th, 2023
Washington, DC

ISMG ENGAGE
May 11, 2023
London

CYBERSECURITY SUMMIT
May 23, 2023
North America West