CYBERSPRINT
BREAKTHROUGH SECURITY

EDITORIAL

AUTOMATED HACKING

A PROBLEM YOU NEED TO BE WORRYING ABOUT

BY **ROBERT KRENN**
RESEARCH DIRECTOR

BY ROBERT KRENN
RESEARCH DIRECTOR

AUTOMATED HACKING
A PROBLEM YOU NEED TO BE WORRYING ABOUT

Let me start by pointing out that automated hacking is not a new problem, it has been around for some time. However, with companies' attack surfaces becoming increasingly sprawling and complex, and with hacks getting more advanced, it is becoming a much more pressing problem for organisations.

WHAT EXACTLY IS AUTOMATED HACKING?

We're currently in the age of automation. Businesses of all sizes and sectors are turning to automation to improve performance and efficiency, as well as reduce costs. Unsurprisingly, with hackers increasingly running their operations like businesses, they have also learned the same processes, and are applying the concepts of automation to hacking.

In the past, launching a cyberattack was a manual process — one that required a physical level of expertise. You needed to do a lot of research, and develop your own tools and exploits. This meant that getting an exploit out into the wild could take days or weeks, even months for the really sophisticated ones. It gave

business a window of opportunity to react and prepare. Today, that window is closing rapidly. Using automation, hackers can target vulnerabilities within a matter of hours.

If we look at the cyber kill chain[1], attacks go through seven distinct phases: reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and actions on objectives. If a hacker is using a scattergun approach to their attacks and isn't targeting specific businesses, they can completely automate reconnaissance, weaponisation, delivery and exploitation parts of this process.

USING AUTOMATION, HACKERS CAN TARGET VULNERABILITIES WITHIN A MATTER OF HOURS.

HOW DO THEY DO THIS?

Let's start at the reconnaissance part. There are a lot of tools available that can be used to remove repetitive work. The two most powerful sources I'll focus on are Shodan and Censys — these are essentially search engines for connected devices. They scan the whole internet all the time and they collect information for every single IP address that's out there — over 4.2 billion.

This information is made readily available for anyone to search through, and effectively allows attackers to search for target servers or systems across the world. So, for example, if a new exploit is found in, let's say, Microsoft Exchange Server[2], they can just enter a query on Shodan to find all servers connected to the internet that are running that version of Exchange and get a list of IP addresses that they can then use to launch their attacks.

There are also integrated attack frameworks available nowadays, such as Autosploit, that will take this data from Shodan and Censys and allow an attacker to choose the type of exploit they want to run. So, at the proverbial press of a button they can run a search, launch an attack and receive a list of exploited servers.

With more and more of these types of tools becoming available, it's pointing to a potentially terrifying future for businesses.

IS PATCHING OUTDATED?

Once an exploit (or even a proof-of-concept exploit) is available, this kind of tooling means attacks can be launched around the world within hours of a vulnerability being announced. This makes the traditional first line of defence — patching — a challenge. Most organisations will install patches and updates on a weekly (or even monthly) basis. That's not enough anymore. While being up to date with your patches is more important than ever, it's almost impossible to patch quickly enough to defend against this speed of attack.

So, companies need to look at other measures to ensure they can protect their systems and give themselves time to run the necessary patches. With the Citrix attacks in December 2019, for example, we saw customers completely disable their working at home environments because of the vulnerability. It resulted in everyone having to travel to the office to work, leading to crowded office spaces and massive traffic jams. Although a severe measure, it gave them the window of opportunity they needed to install a work-around, work on a patch, and protect their environment.

DO YOUR CURRENT MEASURES OFFER ENOUGH PROTECTION?

You might think you've got a solid cybersecurity position, but the challenge is that automated hacking diminishes the effectiveness of many security measures your teams already have in place. For example, if you have a CSIRT (computer security incident response team) or CERT (Computer emergency response team), are you really able to detect and respond quickly enough, or is the attack already happening before you can even line up your response?

If you have an IDS (intrusion detection system) it's more than likely the damage is already done before you can respond. And, even with an IPS (intrusion prevention system) in place it is only effective if the systems being attacked are behind its scope — it won't cover your cloud service providers or that website hosted by a third party.

To protect your business today, you have to know about ALL the systems that belong to your organisation, especially the ones that are not within your core

> “TO PROTECT YOUR BUSINESS TODAY, YOU HAVE TO KNOW ABOUT ALL THE SYSTEMS THAT BELONG TO YOUR ORGANISATION, ESPECIALLY THE ONES THAT ARE NOT WITHIN YOUR CORE INFRASTRUCTURE BUT ARE STILL PROCESSING YOUR DATA.”

infrastructure but are still processing your data. You need to know where you're vulnerable and even where your vendors are vulnerable. Any entry point will do for an attacker, they don't care how they get in as long as they can. It's a cat and mouse game, so you have to think like your attackers and approach the problem in a similar way to them.

To stay ahead, you'd need the same types of tools. Preferably ones that are more powerful than the likes of Shodan and Censys. This allows you to run the same searches for the same vulnerabilities and find more of your organisation's vulnerable systems. However, instead of running exploits, it builds up a picture of your attack surface so you can protect systems and make yourself less of a target.

Being able to quickly know where you could be vulnerable or exposed means that whenever high severity vulnerabilities do get published you can open up that window of opportunity again and figure out a response plan.

At the end of the day prevention is relatively cheap compared to the cost of resolving an active incident. To me, this is definitely an area you should be investing in.

FURTHER READING

1. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
2. https://www.cybersprint.com/hubfs/Editorial%20-%20Exchange_v1.2.pdf

ABOUT THE AUTHOR

ROBERT KRENN is the research director at Cybersprint where he is involved in the development of Cybersprint's Attack Surface Management platform and advises clients on all kinds of IT-security challenges. Starting as a young ethical hacker, Robert now has over 22 years of experience in the IT and security industry as a broadly oriented technical specialist and solution- and security architect. Robert thoroughly enjoys the latest tech gadgets, difficult puzzles, reverse engineering, and travelling to remote locations.

ABOUT CYBERSPRINT

Cybersprint maps the attack surface of organisations and brands. We offer full visibility using continuous and automated digital asset discovery. Our zero-scope approach provides an outside-in perspective, eliminating blind spots.

Assets are individually scanned for a multitude of risk types. These insights empower cybersecurity professionals to prioritise the mitigation of vulnerabilities. Our integrated AI correlates dozens of data sources and uses a multitude of scanners, making risk relevant.

Cybersprint's SaaS platform allows organisations to manage and monitor risks with customisable filters and alerts, integrated into existing processes. Detect and prevent threats such as phishing, brand abuse, data theft and more.

Visit www.cybersprint.com