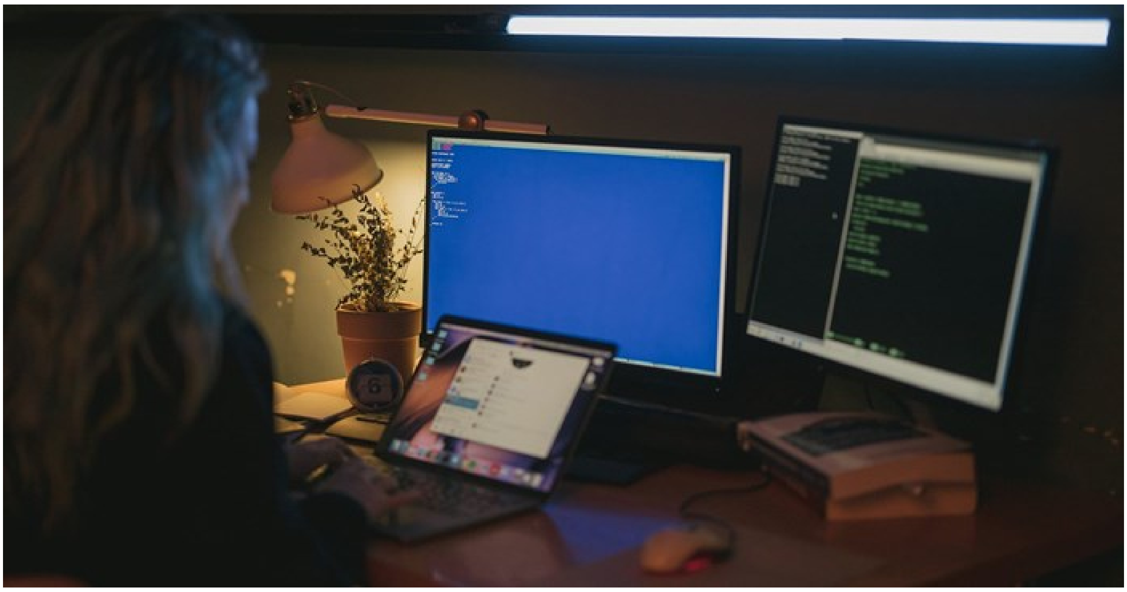
Want to stay ahead of cybercrime? Think like a hacker

By Dale de Kok

28 Jul 2023

If your idea of a hacker is still informed by that one Hugh Jackman movie or *Mr. Robot* then you need to evolve your thinking. Hackers are not solely technical experts who spend their days seeking vulnerabilities and developing malware. The landscape has evolved, and the term "hacker" now encompasses a broader range of malicious actors.



Hackers are not lone technical experts anymore. Source: Cottonbro Studios/Pexels

Today, attackers can easily access hacker forums, crime-as-a-service (CaaS) platforms, and ransomware-as-a-service (RaaS) offerings, allowing almost anyone to purchase the necessary tools, services, and attack methodologies.

According to research by FortiGuard Labs, hackers are using a combination of social engineering, hacking, and malware distribution to carry out increasingly destructive attacks. In a typical ransomware attack, hackers introduce malware into a victim's computer system through phishing or other methods.

In these attacks, they steal data and threaten to release it on the dark web, causing their victims to suffer financial losses and/or reputational damage. We are also seeing an increase in business email compromise attacks.

Standard Bank to acquire remainder of Liberty Two Degrees

Tannur Anders 28 Jul 2023

Hackers usually prefer to carry out multiple attacks to increase their chances of success and to avoid making things difficult for themselves. They often try to blend into the environment by using legitimate business software and applications to achieve their objectives.

Why create custom malware when you can opt for off-the-shelf remote access tools that can bypass the victim's anti-virus software? Using legitimate tools allows them to move laterally within the system and steal data, such as installing a normal backup application and backing up the stolen data to the cloud.

Monitoring hackers on the dark web and deep web

The dark web and deep web can serve as valuable sources of information about hacker operations. However, for most organisations, monitoring these hidden networks poses significant challenges.

Gaining access to these forums requires invitations and establishing trust, which can take some time. It also takes experience to determine the credibility of individuals within these forums. As they span across international boundaries, you need security experts proficient in different languages.

Recent trends have also shown a migration of dark web activity to popular social media platforms such as Telegram and access-controlled groups on Facebook. These platforms offer anonymity and easy accessibility for attackers. Monitoring these forums allows security experts to gain insights into ongoing discussions, and identify advertisements for stolen data, hacking tools, or proof-of-concept exploits for unpatched vulnerabilities.

Working together to get the inside track

Dale de Kok, system engineer, Fortinet

Collaborative efforts and information sharing among stakeholders play a vital role in proactively preparing for potential cyber threats.

Initiatives like the World Economic Forum’s Centre for Cybersecurity and its Partnership Against Cybercrime (PAC) facilitate the exchange of intelligence on cybercrime, bringing together the digital expertise and data of the private sector with the public sector’s threat intelligence to inform the development of improved security tools and defense tactics.

One of its notable projects, the Cybercrime ATLAS, aims to map cybercriminal ecosystems and gain a better understanding of their structures.

Cyber hygiene and the art of deception

Cyber deception can also serve as a powerful tool in an organisation’s security arsenal, allowing them to turn the tables on attackers to some extent.

Similar to honeypots, cyber deception involves deploying decoys, lures, and a fake network resource with realistic-looking files and workflows, all hidden from legitimate users. Security teams can divert hackers away from actual systems and into a pseudo network designed to detect malicious activity immediately. This not only triggers detection but also exposes the attacker’s tactics, tools, and procedures (TTPs), enabling vulnerabilities to be addressed and closed.

One challenge with generic honeypots is getting the hacker to interact with them, as they could be just one Windows server among thousands.

However, with more advanced cyber deception technology, organisations can strategically “advertise” the fake services by leaving “breadcrumbs,” such as lured credentials, which lead attackers into the decoy environment. Cyber deception technology can monitor and record these interactions, helping organisations understand the motives and objectives of attackers.

For effective implementation, deception technology should be fully integrated with next-generation firewalls, network access control, security information and event management (SIEM) systems, sandboxes, security orchestration automation and response (SOAR) platforms, and endpoint detection and response (EDR) solutions.

Getting ahead and staying ahead

Thinking like a hacker is just one aspect of a layered approach to defense. Organisations also need to implement traditional network security measures, including endpoint monitoring, network segmentation, intrusion prevention with SSL decryption turned on and centralised logging.

Also, organisations need help in managing alert fatigue that arises when every anomaly is noted. To effectively manage alerts, the deployment of AI and machine learning products can provide additional context and prioritise alerts accordingly.

Besides these measures, organisations need to attend to basic hygiene practices such as regular patching and training. Equally crucial is having a well-defined incident response plan in place.

Many organisations are ill-prepared to handle a compromise and must be able to scope the attack, mitigate its impact, ensure evidence is not tampered with and respond without alerting the attacker to their actions.

ABOUT THE AUTHOR

Dale is a systems engineer at Fortinet