isep Instituto Superior de Engenharia do Porto

Let's rob a bank
DACYS TP5

Nuno Peralta

Nsp@isep.ipp.pt

Threats

- Cyber Terrorists
- Government-Sponsored/State-Sponsored Actors
- Organized Crime/Cybercriminals
- Hacktivists
- Insiders
- Script Kiddies
- Internal User Errors

Cyber Terrorists

Cyber Terrorists are a modern mutation of a widespread global problem that has plagued most countries for decades. These threat actors are usually focused on disrupting critical services and causing harm.

Chief Goal: Cause harm and destruction to further their cause.

Typical Targets: Cyber terrorists can target businesses, state machinery, and critical services that would cause the most harm, disruption, and destruction.

State Sponsored

These threat actors are funded, directed, or sponsored by nations. They've been known to steal and exfiltrate intellectual property, sensitive information, and even funds to further their nation's espionage causes.

Chief Goal: Espionage, theft, or any other activity that furthers the interests of a particular nation/group of nations.

Typical Targets: Businesses and Government-run Organizations.

Organized Crime/Cybercriminals

Crime is everywhere, and the internet is no different. Criminals who want to steal sensitive data, money, and personal information are out there. However, since they're after financial gain, the data they take does tend to show up on the black market or is sold to the highest bidder. These threat actors are also known to use ransomware to extort business owners directly.

Chief Goal: Financial Gain.

Typical Targets: Cash and/or Data-Rich Organizations and Businesses.

Hacktivists

Hacktivists focus on bringing awareness. For example, almost all the information leaked by WikiLeaks was a result of hacktivists who wanted to expose the truth. They're usually motivated by ideological activism.

Chief Goal: Exposing secrets and disrupting services/organizations that are perceived as evil.

Typical Targets: Not limited to any specific type of organization or business.

Insiders

Sometimes, you don't need to look far to find infiltrators. Some threat actors can go as far as infiltrating your workforce themselves or turning an insider towards their cause/goal. Insiders are a particularly nasty threat to any organization's cybersecurity because of the amount of access they'd have when working from within.

Chief Goal: Work from within an organization to get around its cybersecurity framework.

Typical Targets: Not limited to any specific type of organization.

Script Kiddies

Some attackers aren't skilled/advanced enough to design penetration tools on their own. Script Kiddies use tools developed by other attackers to penetrate a network or system.

Chief Goal: Attack computer systems and networks, vandalize, and inflict as much damage as possible.

Typical Targets: Easy-to-penetrate systems, which are vulnerable to widely-known threats.

Internal User Errors

Not all threat actors are malicious. But the damage they do cause can be quite extensive. Even simple user errors can end in catastrophe because of their elevated permissions within an organization's systems and networks.

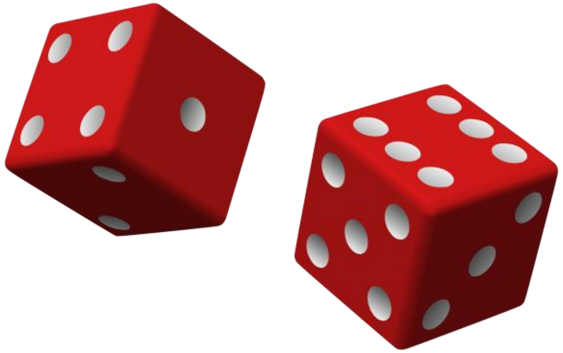
Chief Goal: Not malicious, often inadvertent.

Typical Targets: Can affect any organization, however secure.

https://www.redlegg.com/blog/cyber-threat-actor-types

Bonus

Tenta adivinhar o próximo...



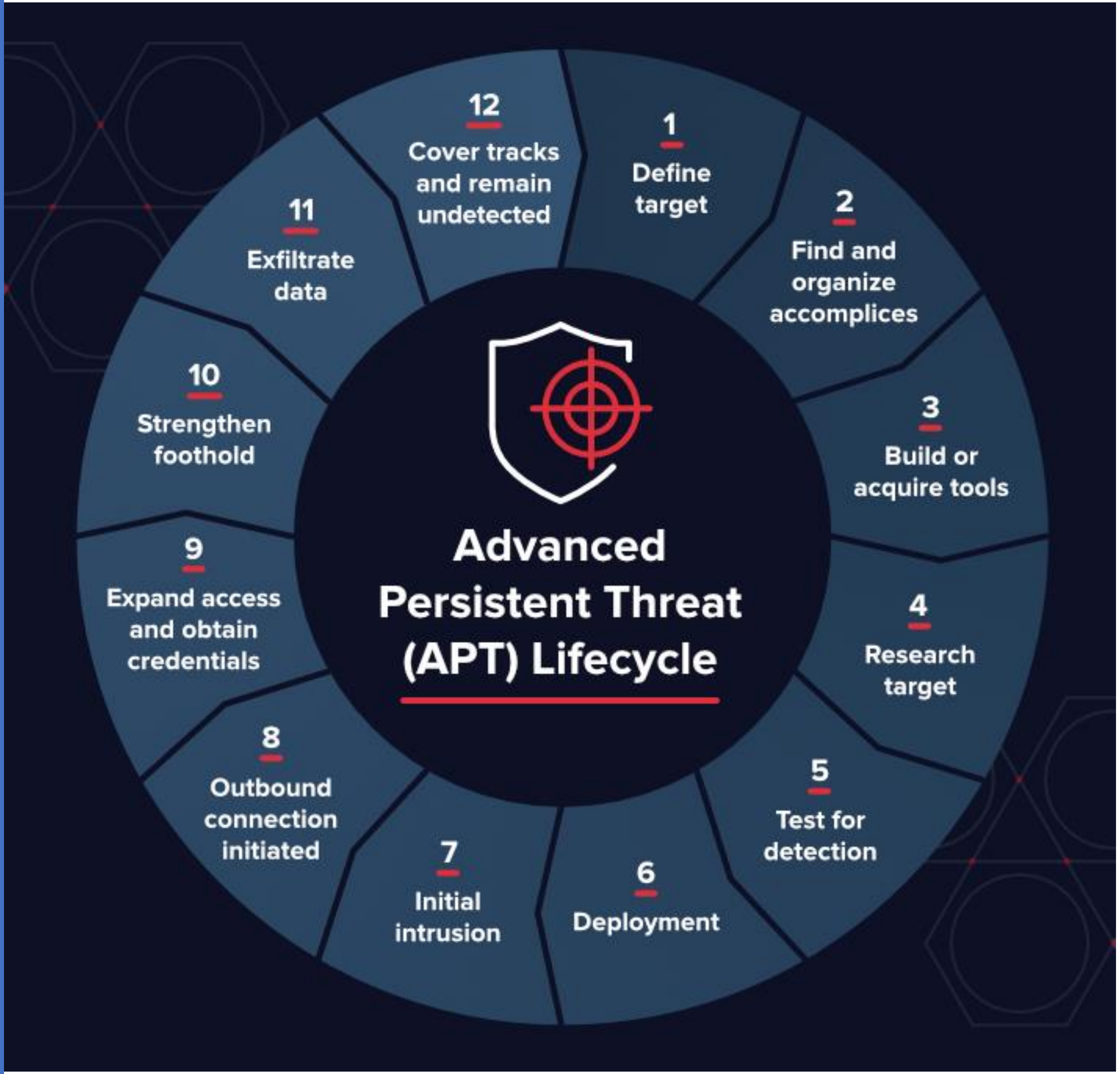
is **a free-software user interface that works with core libraries to handle the installation and removal of software on Debian, and Debian-based Linux distributions**.

APT (Advanced Persistent Threats)

An Advanced Persistent Threat (APT) is a malicious actor who possesses extraordinary skill and resources—enabling them to infiltrate and exfiltrate an organizations’ network. APTs use a variety of techniques, tactics, and tools—such as highly-targeted social engineering attacks, ransomware, vulnerability exploits, and zero-days to accomplish their illicit objectives.

While some threat actors work alone, multiple government authorities such as the Cybersecurity and Infrastructure Security Agency (CISA) have linked attacks to APT groups—with some having ties to specific nation-states who use them to further their country’s interests.

Resumo

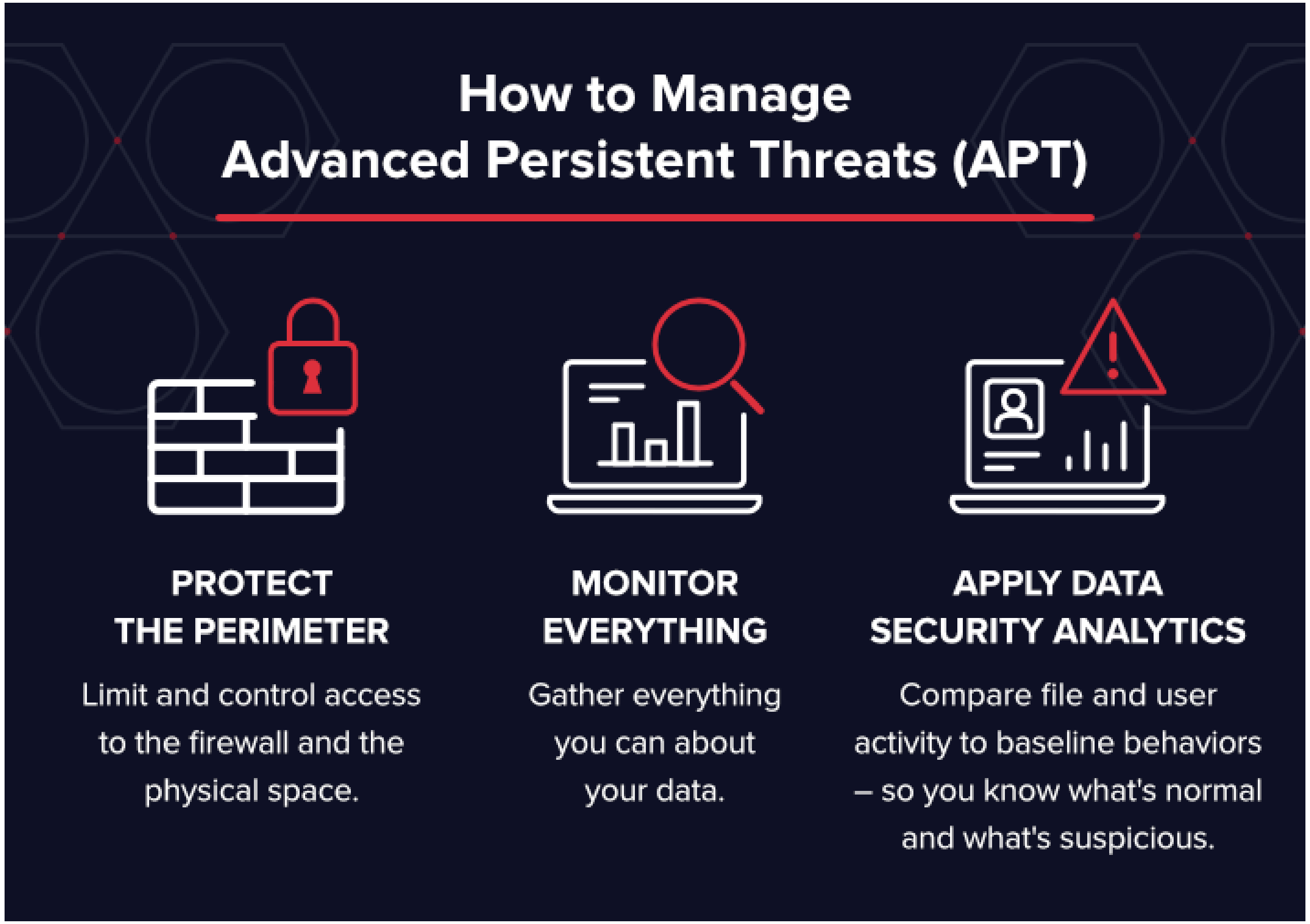

Advanced Persistent Threat (APT) Lifecycle
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
12 Cover tracks and remain undetected

Então... mas prometeram-me que haveriam bancos e assaltos

Demonstração

https://www.youtube.com/watch?v=mCX-Px7H4h4

Mitigação?



How to Manage Advanced Persistent Threats (APT)

PROTECT THE PERIMETER

Limit and control access to the firewall and the physical space.

MONITOR EVERYTHING

Gather everything you can about your data.

APPLY DATA SECURITY ANALYTICS

Compare file and user activity to baseline behaviors – so you know what's normal and what's suspicious.

Dúvidas?