most common failure in corporate environments

joas antonio dos santos


```
[~]$  whami
      Red team leader and instructor at hackersec
      Contributor and researcher at miter att&ck
      owasp project leader
      author and speaker
      +90 international certifications
      Numerous CVs reported
[~]$
```

global

botnet	31%
infostealer	21%
cryptominers	19%
banking	19%
mobile	14%
ransomware	8%

americas

botnet	25%
infostealer	18%
cryptominers	15%
banking	15%
mobile	14%
ransomware	6%

emea

botnet	30%
infostealer	23%
cryptominers	19%
banking	19%
mobile	14%
ransomware	8%

apac

botnet	43%
infostealer	30%
cryptominers	25%
banking	25%
mobile	13%
ransomware	10%

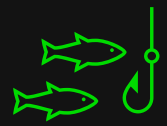
source:checkpoint

top 10 top cybersecurity threats

vulnerabilities:
newly discovered critical vulnerabilities in microsoft exchange and advances in phishing create new areas for msps to monitor.

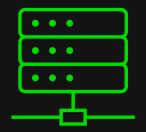
Commitment corporate email:
when a cybercriminal gains access to a corporate email, they can use it to send phishing, steal confidential information or use the account to launch attacks.

crime-as-a-service:
this describes the provision of cybercriminal tools, services and expertise through an underground, illicit market.



supply chain attacks:
Hackers infiltrate supply chain technology to access source code, builds, and other infrastructure components of benign software applications.

cloud-based attacks:
With so many companies using the cloud and cloud networks becoming more complex, your infrastructure has become an easy target for digital threat actors.



data center attacks:
these malicious activities are aimed at compromising the security of data centers, facilities that house computer systems, and other critical infrastructure.

ransomware:
this form of cyber attack has been around for decades, and hackers continue to develop and evolve their methods.

iot device hacking:
with many employees accessing sensitive company platforms and data from multiple dispersed endpoints, hackers have more opportunities for infiltration.

internal threats:
once internal system users are compromised, they can become an even greater threat to the system than external attackers.

State-sponsored cyber warfare:
cyberattacks by one nation-state against another for strategic or military purposes, often carried out by well-funded companies and highly skilled teams of hackers or cyber soldiers.

source:connectwise

apt115 ac3r0l4

ac3r0l4timeline

06/2015

emerged in 2015 in Brazil

01/2018

Presence on popular surface hacking forums such as raidforums, breached, cracked, and xss.

03/2020

ransomwareknown as t1r4d3nt3s

10/2022

task force created by fireeye + mandiant + trendmicro resulted in apt115

02/2016

dominant player in selling ransomware and 0days

04/2019

detection of your operations in 15+ countries with multiple ransomware operators

09/2021

variants sold on genesis marketing

modus operandi

- social engineering kit
- vulnerability exploit kit (0days), e.g. 0daytoday
- buying company access to forums
- Private virtual private servers from countries like (Iran, Venezuela, Panama and Switzerland)
- vpn (airvpn, alerdium and mullvad) and tor (whonix or tails)
- shared command and control server (cobalt strike)
- polymorphic ransomware + sophisticated ttps
- bitcoin, monero and ethereum wallets
- invasions + theft and kidnapping of data in fortune 1000 companies

tactics, techniques and procedures (ttps)

mitre att&ck and ttps

“att&ck mitre is a framework that maps cyber adversary tactics and techniques to help defend and understand cybersecurity threats.”

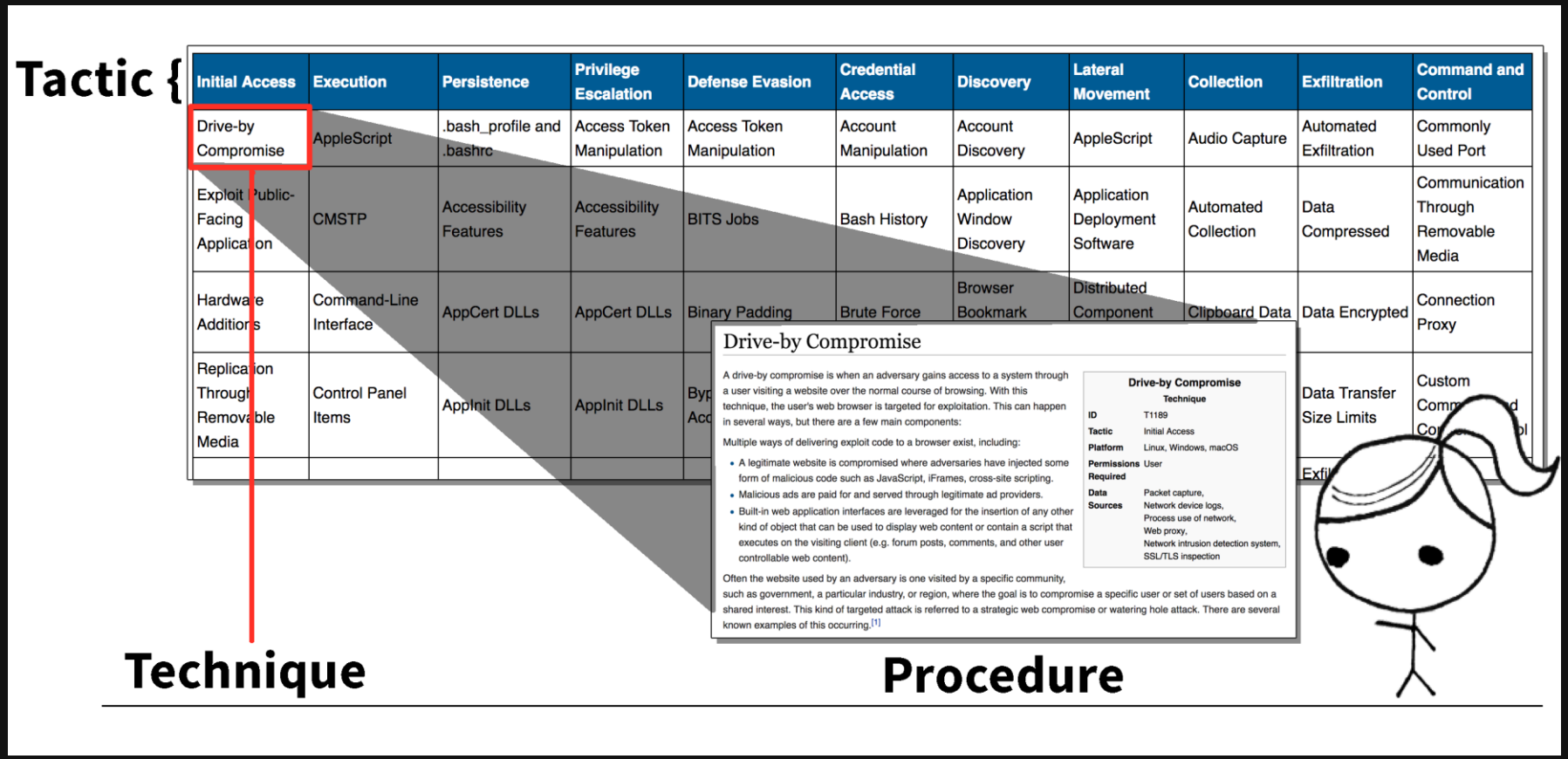
ttps (tactics, techniques and procedures) are a set of specific strategies and actions used by adversary actors to carry out cyber attacks, being important for understanding and defending against these threats.

mitre att&ck and ttps

to the **tactics** are the tactical objectives that a threat can use during an operation.

to the **techniques** describe the actions that threats take to achieve their goals.

You **procedures** are the technical steps required to perform the action.



source:redteam.guide

apt115 ac3r0l4 simulation

[~]$ initialaccess.ps1 --help

initial access
refers to the point at which the opposing team gains initial unauthorized access to a target system or network

social engineering (spear-phishing + malicious pdf)

0day exploit: cve-2022-22965 (rce spring framework), cve-2021-44228 (log4j) and cve-2022-30190 (follina)

credential dump (i have been pwned + dump leak)

creation of payloads to manage compromised targets through a c2

initialaccess

metasploit framework (msfvenom)

vulnerability exploitation and shellcode generation

exploit pack

development of exploits and 0days

macro pack

generate malicious documents with vba macro

bad pdf generator

generate malicious pdf: https://github.com/cybersecurityup/badpdf-generator

gophishing + evilginx

carry out phishing campaigns

cobalt strike

manage compromised machines on a command and control server, using beacons and payloads

[~]$ evasion.cpp --help

evasion
    refers to when the opposing team uses techniques to evade detection of a protection mechanism and persist in a compromised environment.

configure a vpn to cloak network traffic

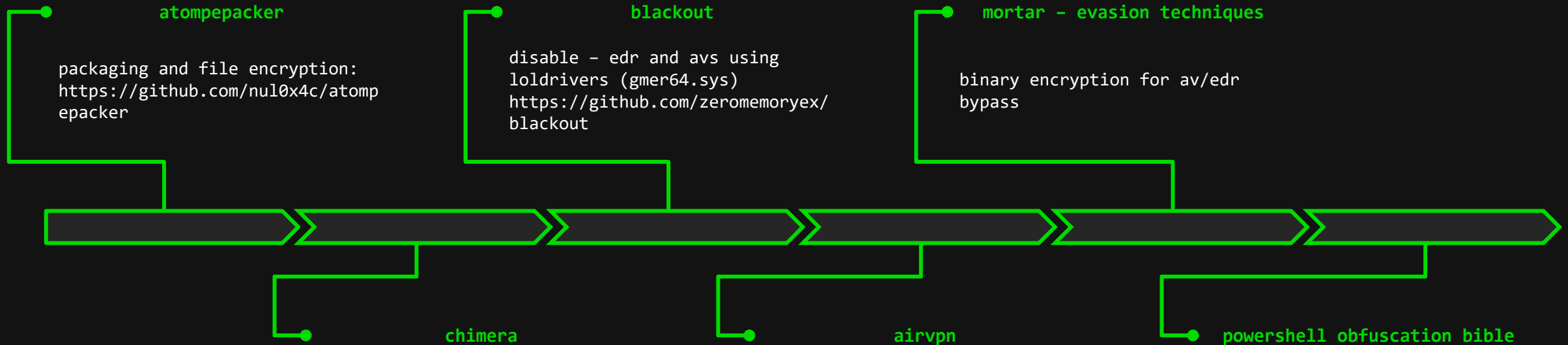
process injection techniques

exploration of defense mechanisms

obfuscation and payload encryption

use of valid accounts

evasion



atompepacker

packaging and file encryption:
https://github.com/nul0x4c/atompepacker

blackout

disable – edr and avs using loldrivers (gmer64.sys)
https://github.com/zeromemoryex/blackout

mortar – evasion techniques

binary encryption for av/edr bypass

chimera

automation of automatic third-party dll execution attacks (dll sideloading):
https://github.com/georgesotiriadis/chimera

airvpn

vpn service based on openvpn and wireguard for hacktivism:
https://airvpn.org/

powershell obfuscation bible

collection of evasion techniques in powershell:
https://github.com/t3l3machus/powershell-obfuscation-bible

[~]$ privesc.py --help

privilege escalation
    refers to the point at which the adversary seeks to gain higher privileges on a compromised system.

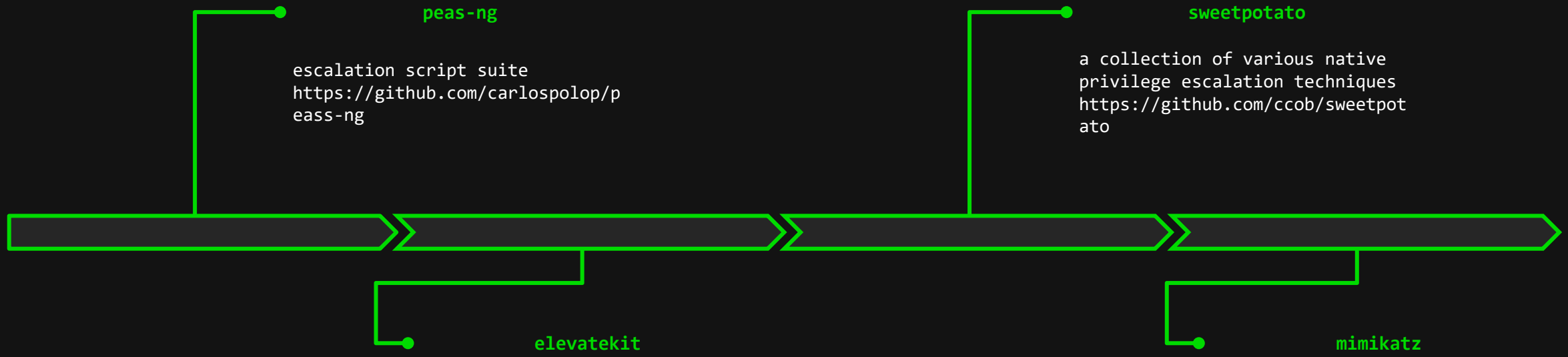
exploiting local vulnerabilities in cve

using lolbas to exploit incorrect permissions of an application

hash dump and domain controller attacks

valid accounts collected

privesc


peas-ng
escalation script suite
https://github.com/carlospolop/peass-ng
sweetpotato
a collection of various native privilege escalation techniques
https://github.com/ccob/sweetpotato
elevatekit
privilege escalation kit for cobalt strike
mimikatz
extract sensitive information such as clear text passwords and password hashes

[~]$ persistence.bat --help

persistence
    refers to the point at which the opposing team gains continued access to a compromised system

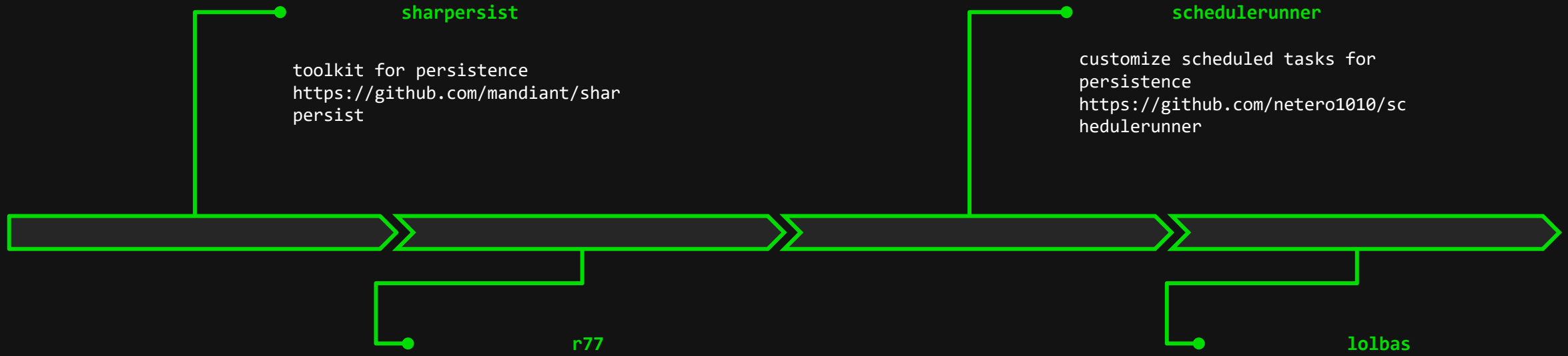
creation and modification of processes

create accounts on the machine

create scheduled tasks

rootkits (ring 3)

persistence



[~]$ exfiltration.c --help

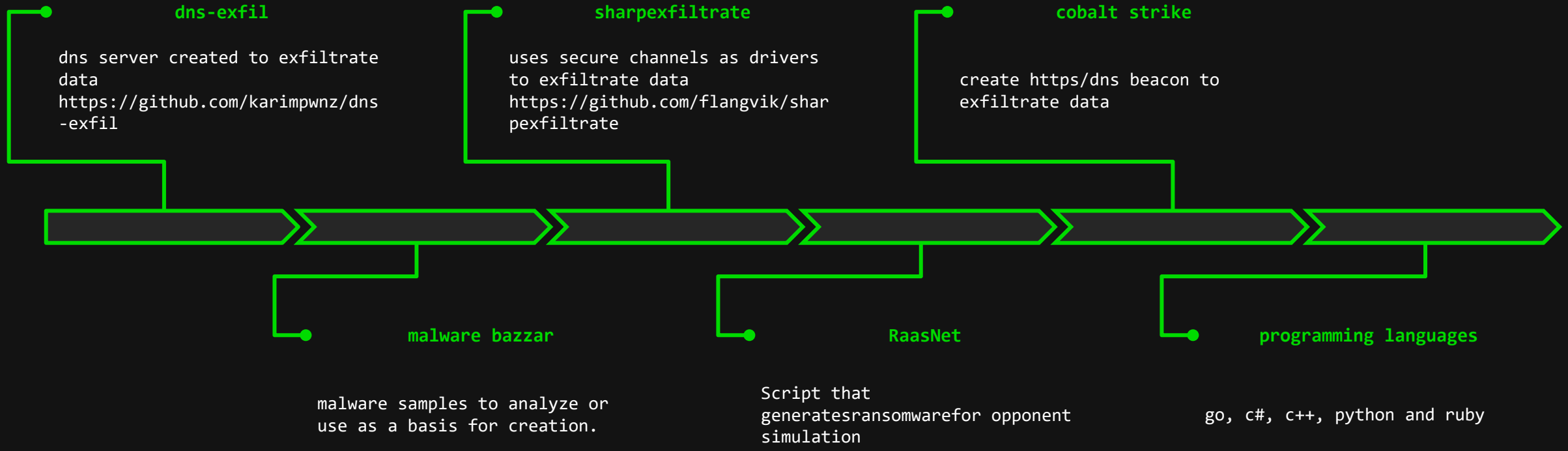
exfiltration and impact
    refers to the point at which the opposing team steals information from the network and compromises the availability of the environment.

data exfiltration via alternative protocols

data exfiltration through c2

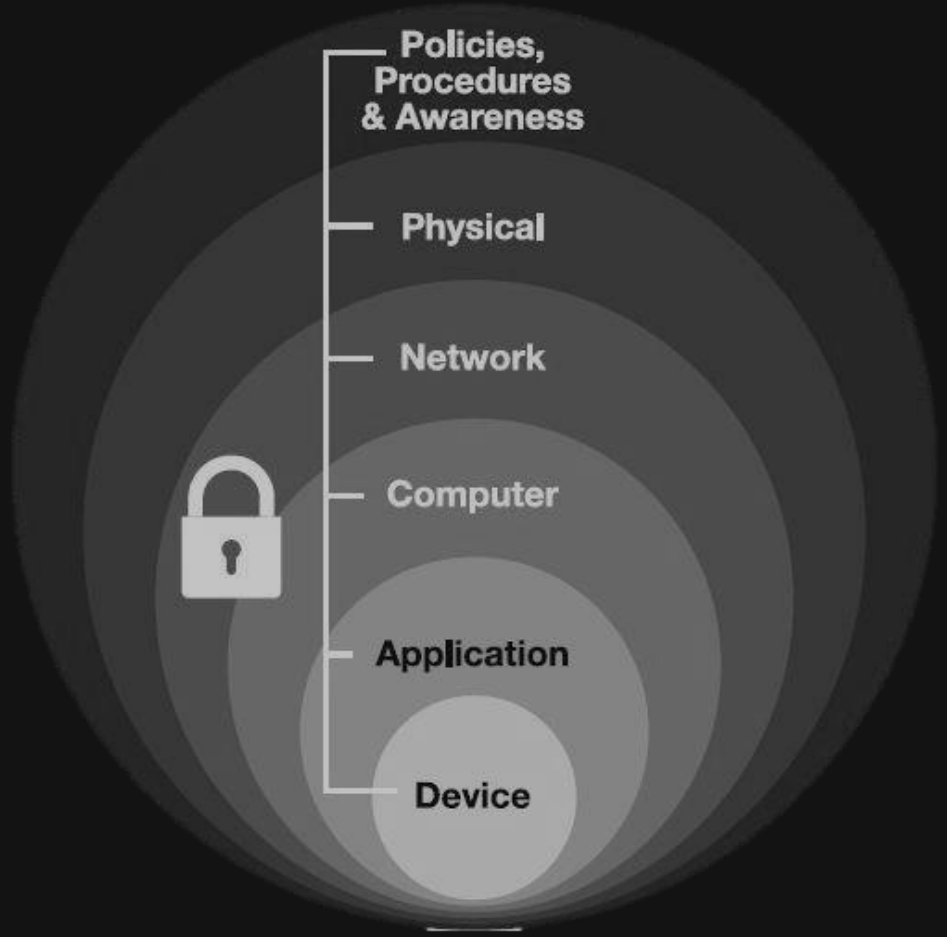
ransomware development

exfiltration



prevention methods

security in depth



source:network access

Risk management

risk management is the process of identifying, assessing and mitigating risks that may affect an organization, project, process or activity.

The primary objective of risk management is to take proactive measures to reduce the likelihood of adverse events occurring and to minimize their impact if they do occur.

maturity	in	until	recommendation
insufficient	0.00	3.00	deal with
regular	3.01	5.00	to develop
good	5.01	7.50	to improve
very good	7.51	9.00	improve
great	9.01	10.00	to maintain

nist-based maturity process

the nist cybersecurity framework (csf) is a set of guidelines and best practices developed by the us national institute of standards and technology (nist) to help organizations manage and improve their cybersecurity posture.

csf offers a flexible, risk-based model that allows organizations to tailor their cybersecurity strategies to their specific needs.

identify	protect	to detect	to respond	to recover
asset Management	access control	anomalies and events	response	recovery
business environment	awareness and training	continuous security monitoring	planning	planning
governance	data security	detection processes	communications	improvements
risk assessment	information protection processes and procedures		analyzes	communications
risk assessment strategy	maintenance		mitigations	
supply chain risk management	protection technology		improvements	

cybersecurity solutions

“Facilitate cybersecurity operations and ensure effective controls across your environment.”

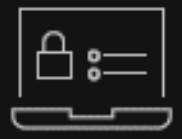
this summarizes cybersecurity solutions and their importance, and cis categorizes at least 18 essential solutions for your security maturity

and thesansmaps the top 20 security controls through existing solutions on the market.

source:cis

Future of the cybersecurity market

Future outlook of cybersecurity market



$101.5

billion in projected spending on service providers[1] by 2025

15%

annual increase of costs related to cybercrime; will reach **$10.5 trillion** a year in 2025

85%

of small and midsize enterprises intend to increase IT security spending until 2023

3.5

million cybersecurity positions now open worldwide

+21%

forecast of compound annual growth for direct cyber insurance premiums until 2025

[1]Service providers include consultants, hardware support, implementation, and outsourcing.
Source: Center for Strategic & International Studies; IBM; Identity Theft Resource Center; Kaspersky Lab; National Cyber Security Centre; press; PurpleSec data survey; Statista; McKinsey Cyber Market Map

source:burrelles

The hackersec as a business strategy

HACKER SEC

[~]$ cat thanks.txt

linkedin – joas antonio dos santos