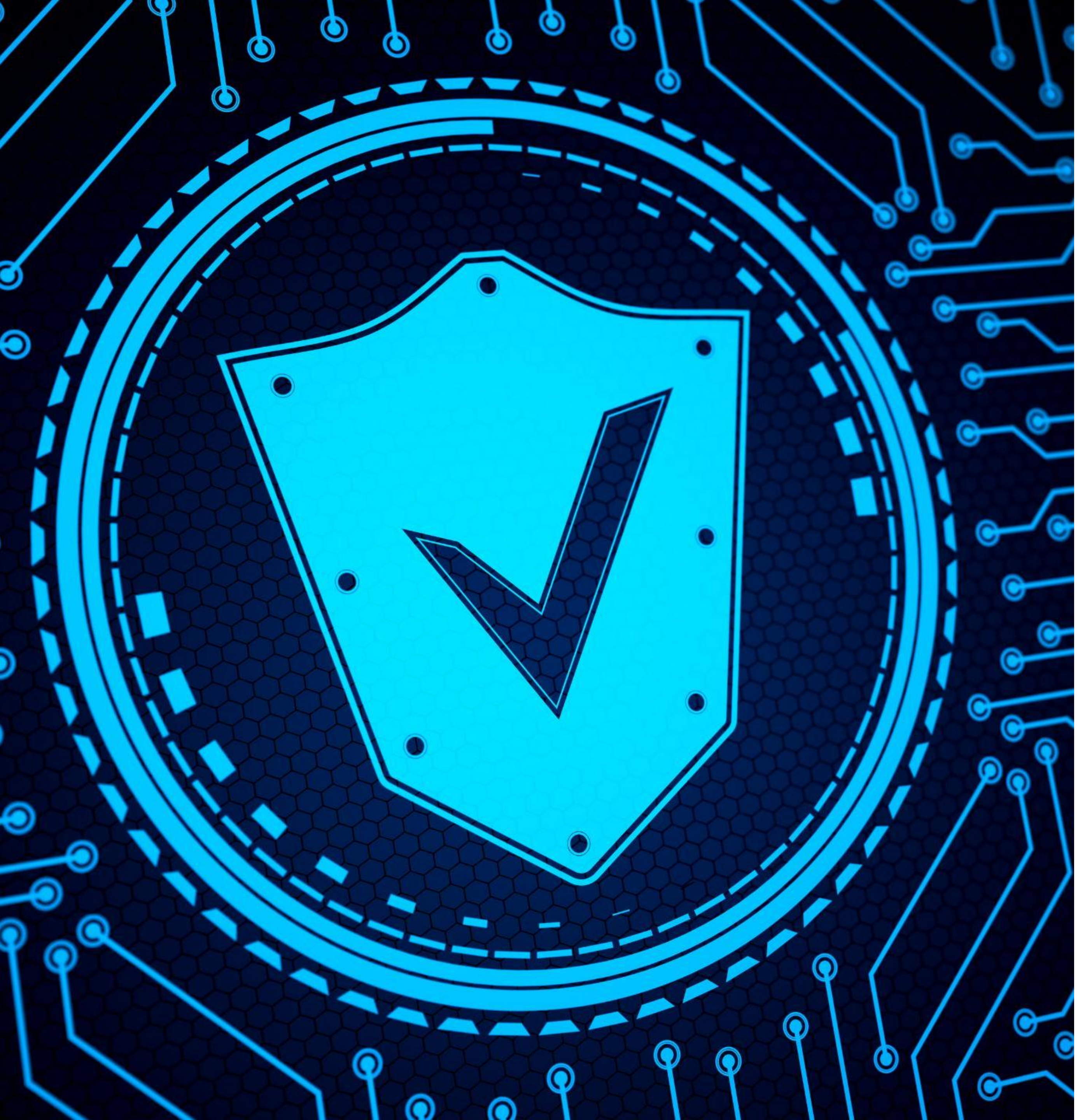


Beyond the Checkbox: Implementing a Zero Trust Endpoint Security Framework with Microsoft Services

Comprehensive strategies for modern cybersecurity challenges

Agenda Overview

- Theoretical Overview of Zero Trust in Modern Cybersecurity
- Red Teaming: Understanding and Countering Modern Attack Kill Chains
- Implementing Zero Trust Endpoint Security with Microsoft Services
- Strategic Alignment and Economic Value of Zero Trust with Microsoft

Theoretical Overview of Zero Trust in Modern Cybersecurity

The Current Cybersecurity Landscape in Eastern Europe: Attack Statistics and Trends

Dynamic Threat Landscape

64% of European businesses expect to suffer a cybersecurity incident in the next 12 months.

Only **29%** report being **highly prepared** for it...

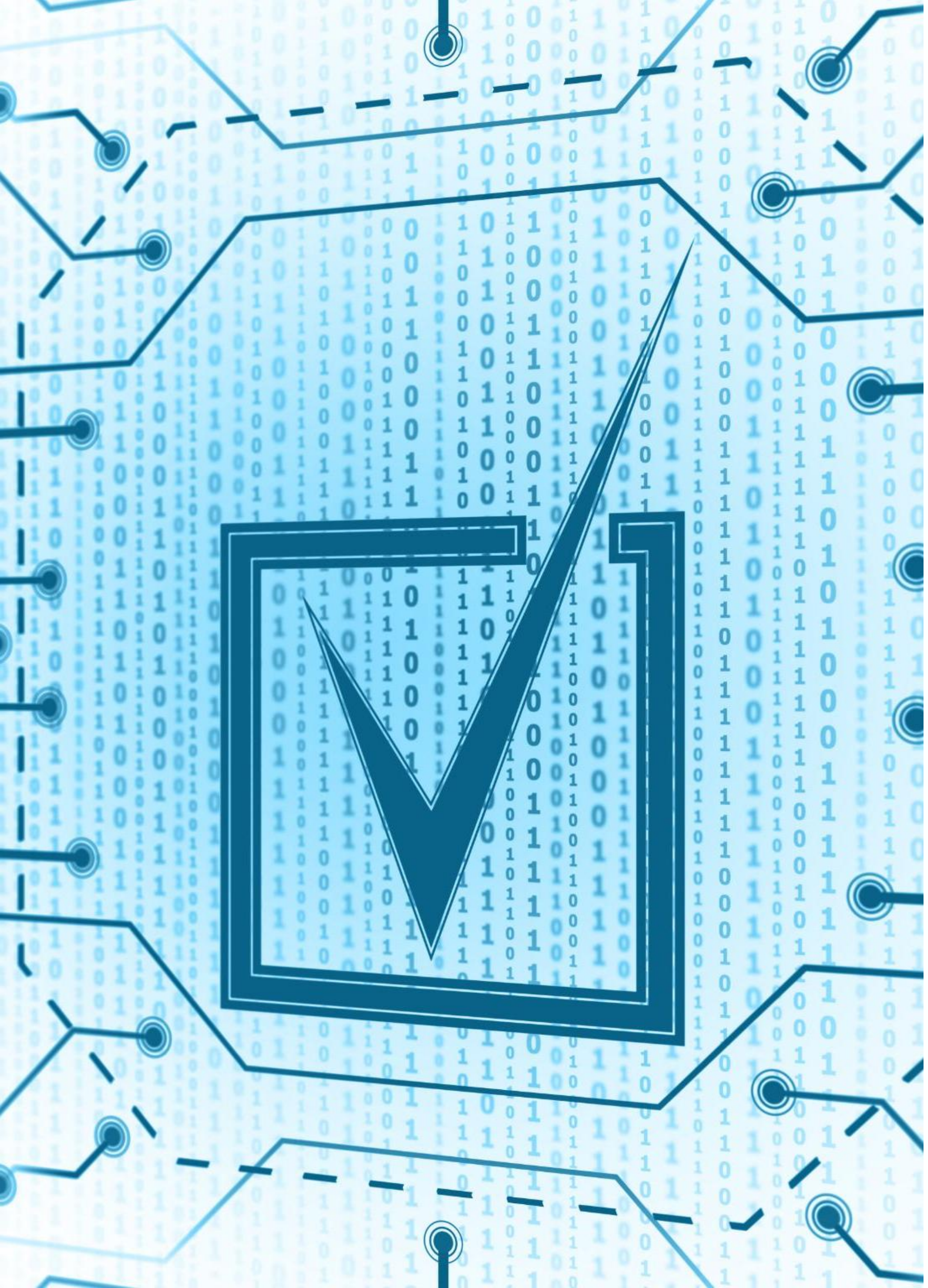
Attack Statistics Overview

40% of organizations experienced a cybersecurity incident in the last 12 months, with **64%** expecting to suffer one in the next year

Supply Chain Attacks Are Near-Universal for Major Firms

98% of Europe's top 100 companies had a breach in their **third-party ecosystem** in the last year

1)IBM Cost of a Data Breach Report 2024
2)Cloudflare Inc. 2024
3) SecurityScorecard Report on Europe's Top 100 Companies (2024)



Defining Zero Trust: always verify, never asume trust

Zero Trust Philosophy

Zero Trust is based on the principle of never trusting and always verifying every access attempt.

Identity Verification

Strict identity verification is essential to ensure only authorized users access sensitive resources.

Continuous Validation

Devices and users undergo continuous validation before and during access to maintain security integrity.

Quantifiable Value: Measuring ROI and Risk Reduction with Unified Zero Trust Approaches

Reduced Breach Impact

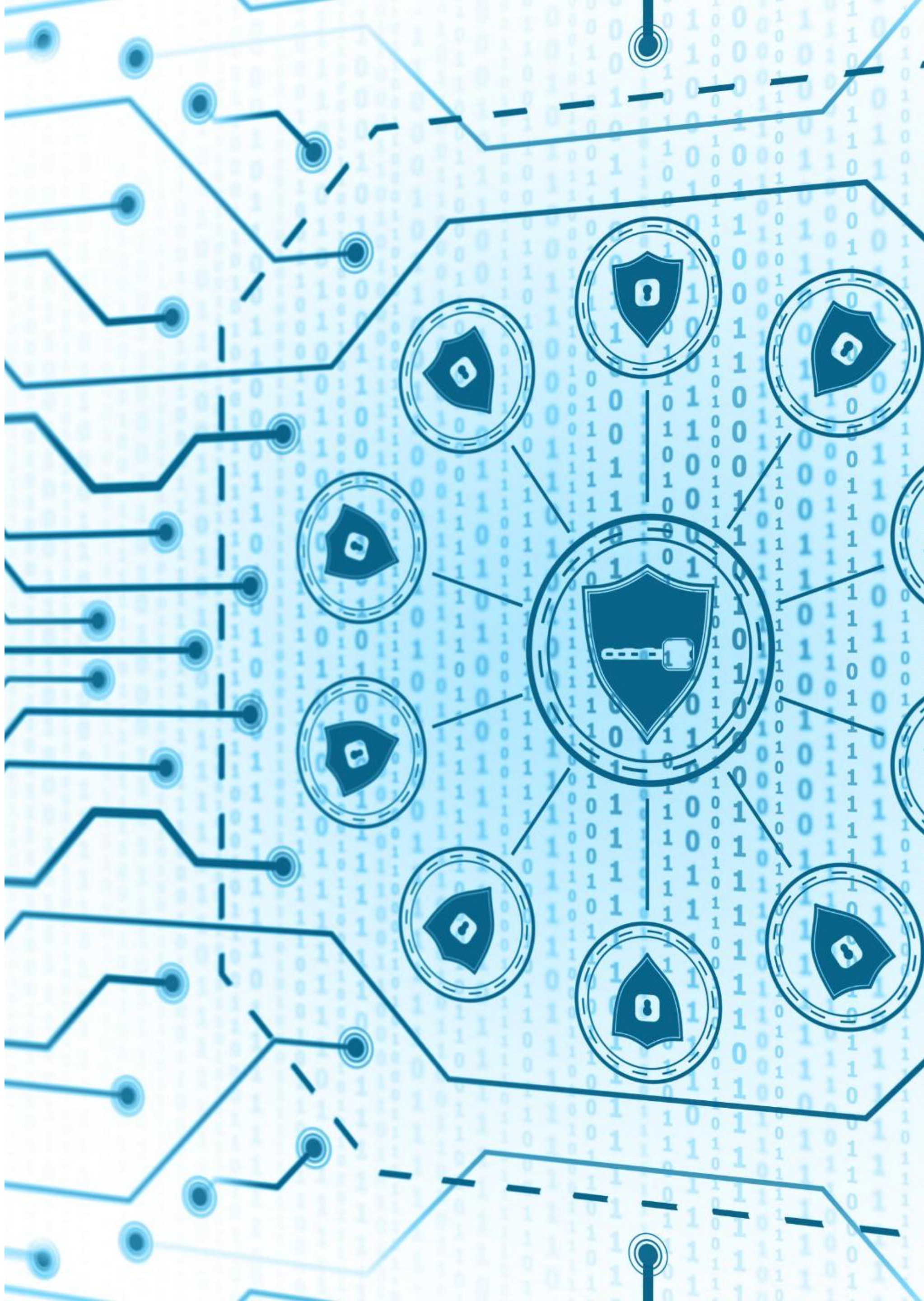
Zero Trust implementation significantly lowers the severity and cost of security breaches in organizations.

Operational Cost Savings

Unified Zero Trust approaches optimize security operations, leading to measurable reductions in operational expenses.

Measuring Financial ROI

Key financial metrics help quantify the return on investment from Zero Trust security adoption.



Red Team: Understanding and Countering Modern Attack Kill Chains

The Attacker's Kill Chain: From Reconnaissance to Post-Breach Rootkits and Associated Tools

Reconnaissance and Weaponization

Attackers gather information about the target and prepare specialized malware to exploit discovered vulnerabilities.

Delivery and Exploitation

Malware is delivered, often through email or USB, and activates by exploiting system weaknesses.

Installation and Command & Control

A backdoor is installed, granting attackers ongoing access and control over the compromised system.

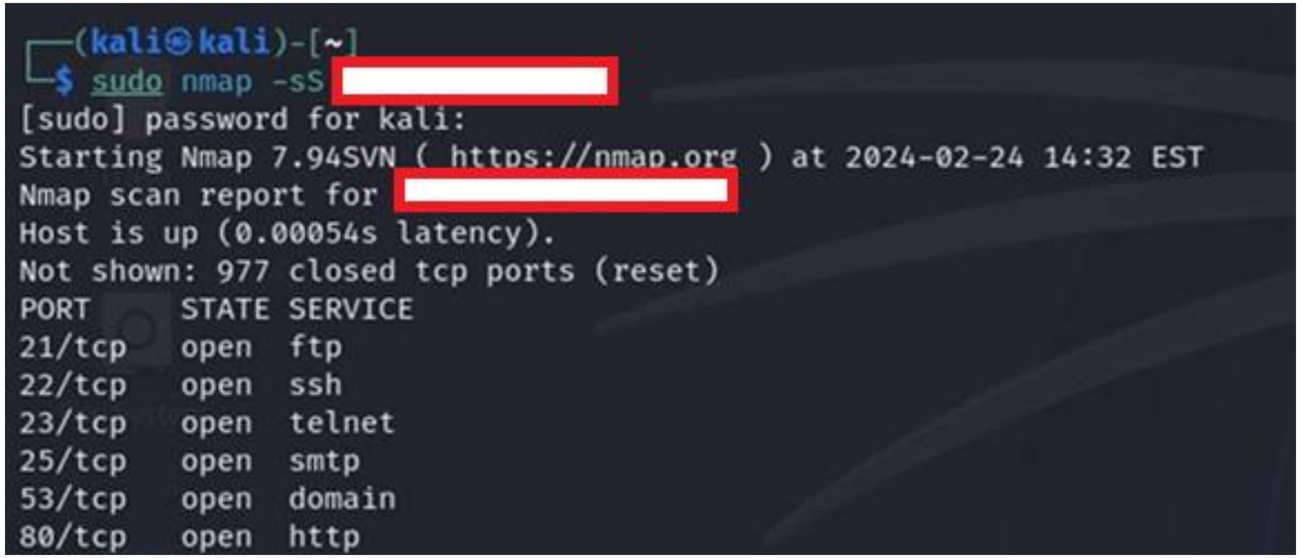
Actions on Objectives

Attackers achieve their goals, such as stealing data, causing damage, or demanding ransom.

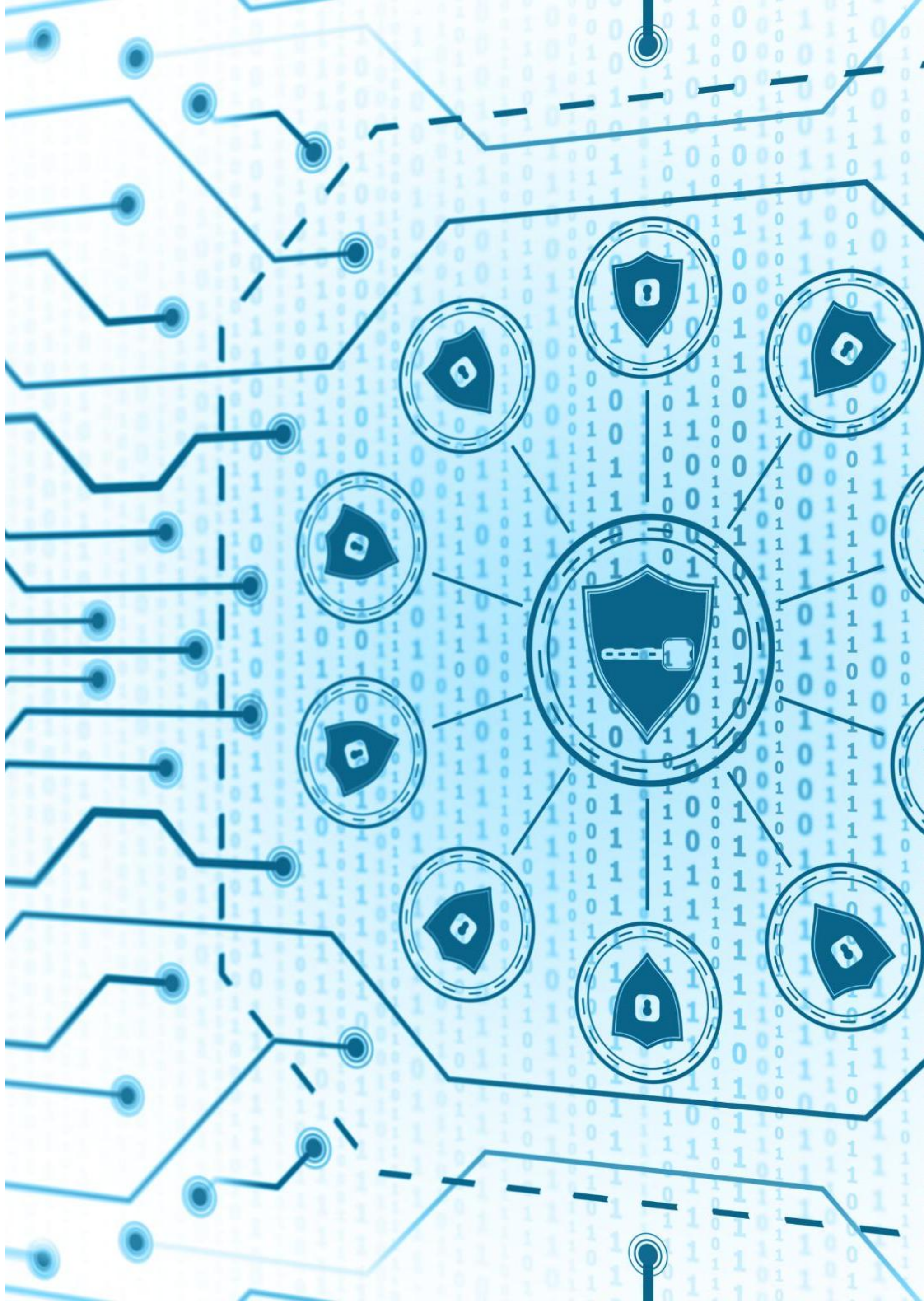
Intrusion Kill Chain Phases

Reconnaissance Phase

In this initial phase, attackers gather information about their target to plan their approach and identify vulnerabilities.



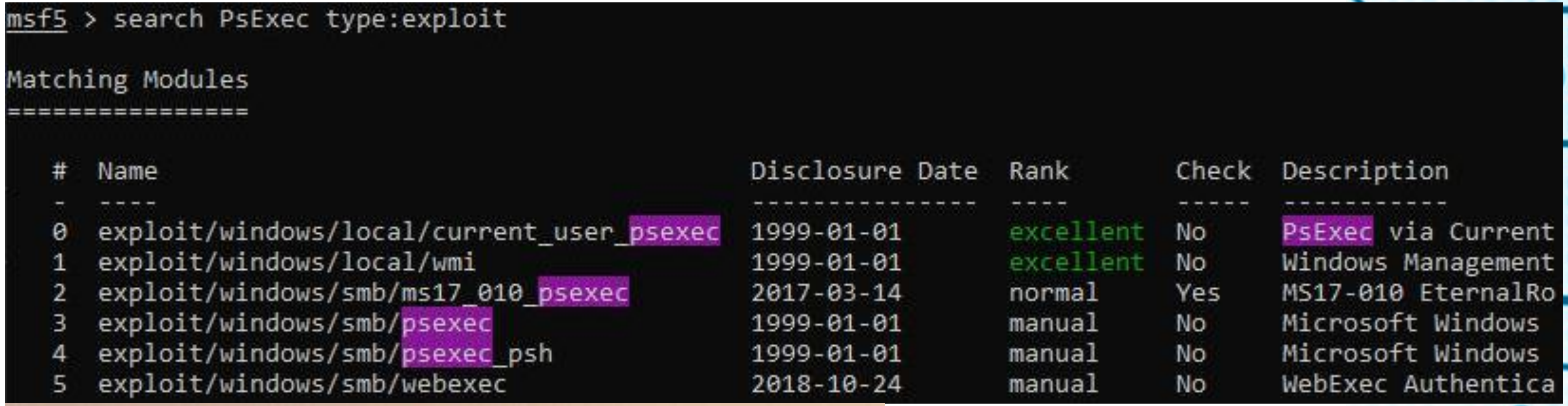
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS [redacted]
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 14:32 EST
Nmap scan report for [redacted]
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```



Intrusion Kill Chain Phases

Weaponization Phase

Intruder creates malware weapon tailored to one or more vulnerabilities.

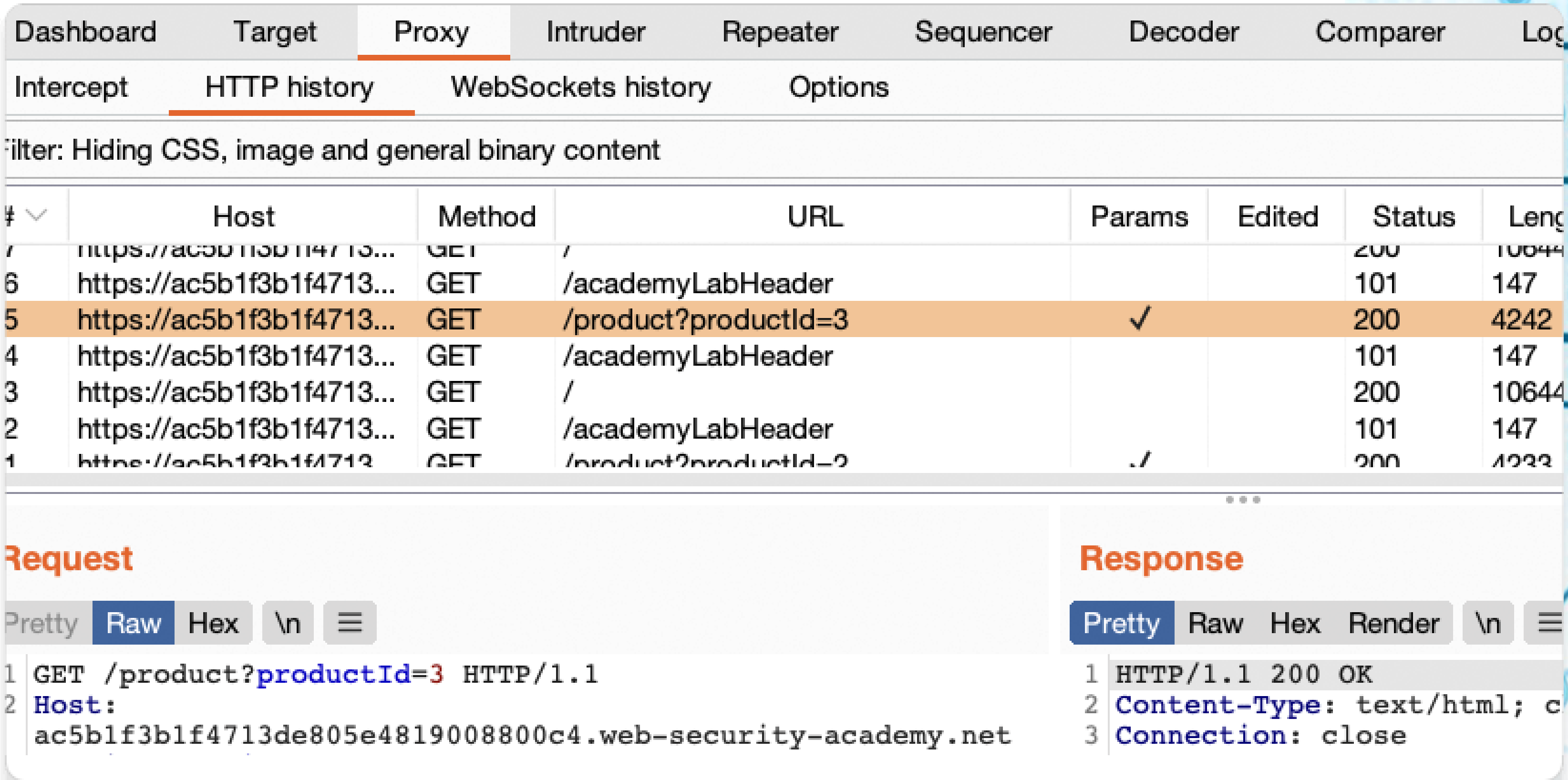


```
msf5 > search PsExec type:exploit

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/windows/local/current_user_psexec  1999-01-01       excellent  No     PsExec via Current
   1  exploit/windows/local/wmi                  1999-01-01       excellent  No     Windows Management
   2  exploit/windows/smb/ms17_010_psexec        2017-03-14       normal     Yes    MS17-010 EternalRo
   3  exploit/windows/smb/psexec                 1999-01-01       manual     No     Microsoft Windows
   4  exploit/windows/smb/psexec_psh             1999-01-01       manual     No     Microsoft Windows
   5  exploit/windows/smb/webexec                2018-10-24       manual     No     WebExec Authentica
```

Intrusion Kill Chain Phases

Delivery Phase

Intruder transmits weapon to target



ilter: Hiding CSS, image and general binary content

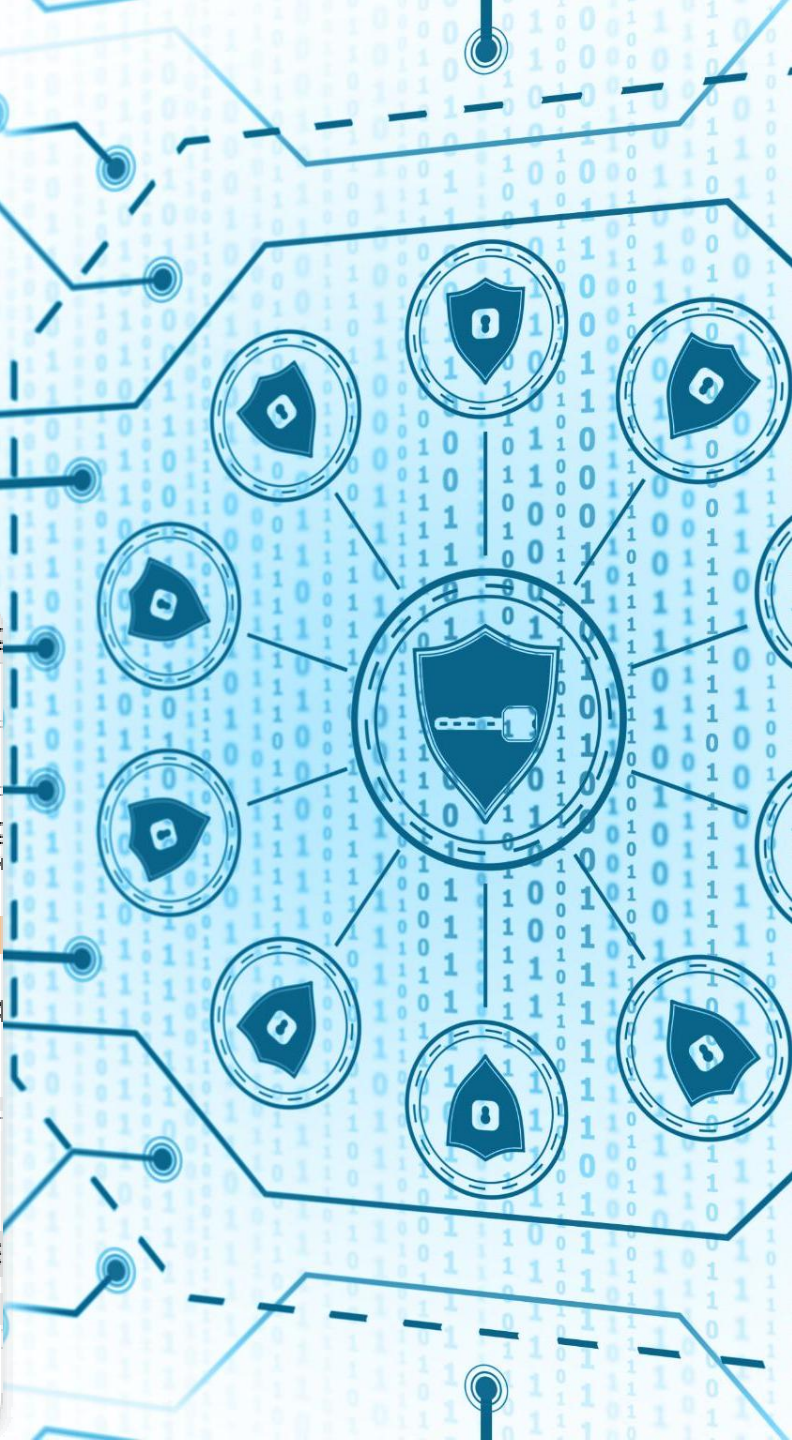
#	Host	Method	URL	Params	Edited	Status	Leng
7	https://ac5b1f3b1f4713...	GET	/			200	10644
6	https://ac5b1f3b1f4713...	GET	/academyLabHeader			101	147
5	https://ac5b1f3b1f4713...	GET	/product?productId=3	✓		200	4242
4	https://ac5b1f3b1f4713...	GET	/academyLabHeader			101	147
3	https://ac5b1f3b1f4713...	GET	/			200	10644
2	https://ac5b1f3b1f4713...	GET	/academyLabHeader			101	147
1	https://ac5b1f3b1f4713...	GET	/product?productId=2	✓		200	4233

Request

```
GET /product?productId=3 HTTP/1.1
Host:
ac5b1f3b1f4713de805e4819008800c4.web-security-academy.net
```

Response

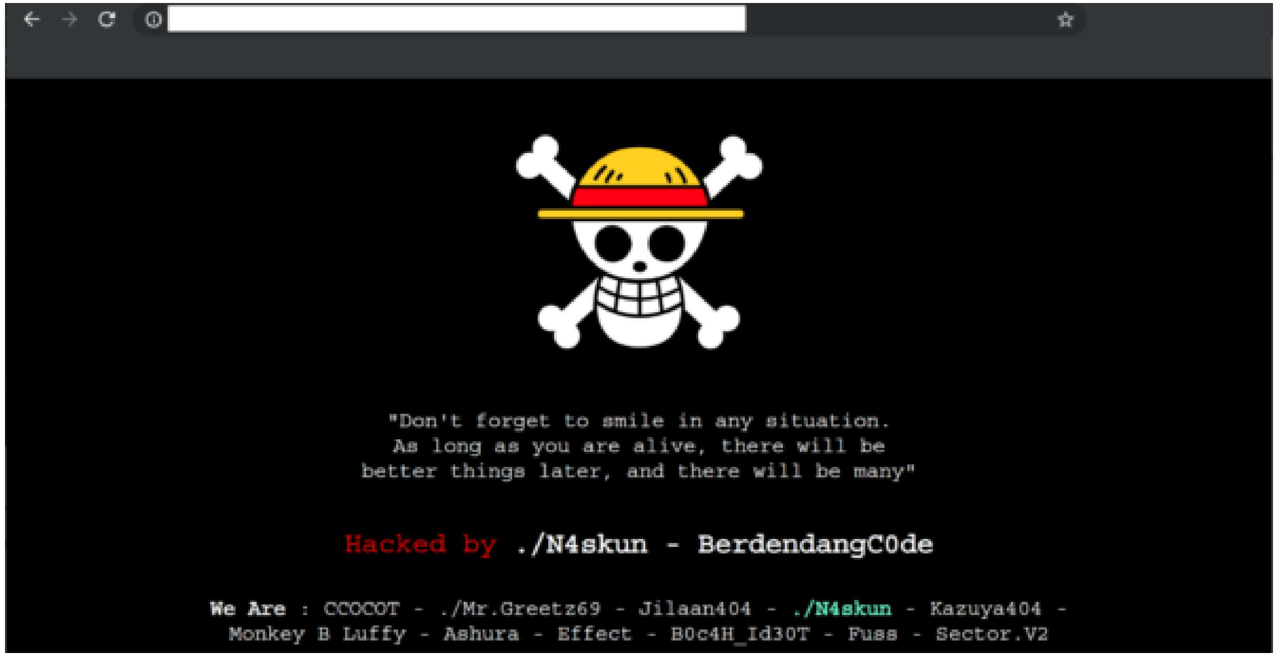
```
HTTP/1.1 200 OK
Content-Type: text/html; c
Connection: close
```



Intrusion Kill Chain Phases

Exploitation phase

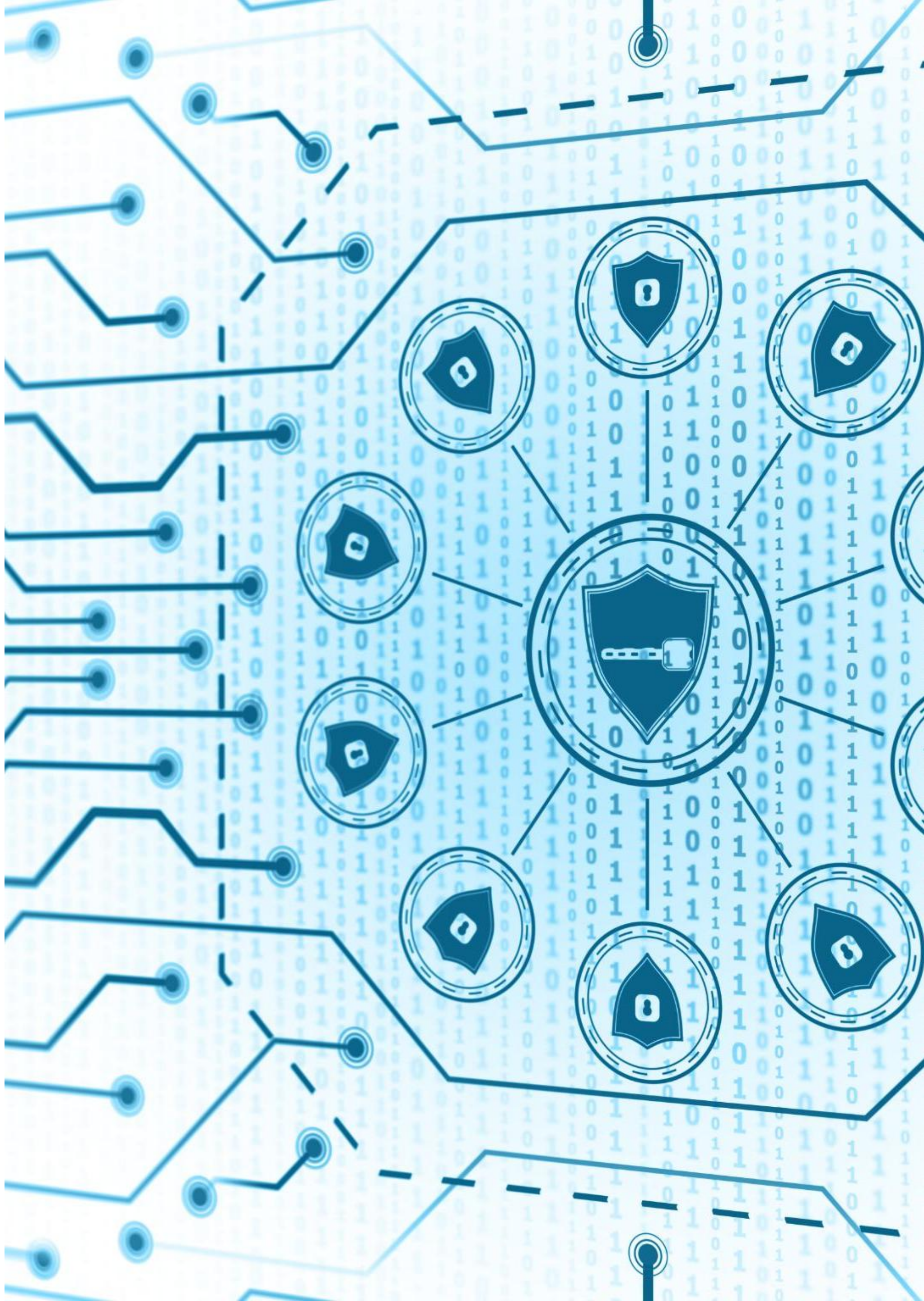
Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.



"Don't forget to smile in any situation.
As long as you are alive, there will be
better things later, and there will be many"

Hacked by ./N4skun - BerdendangC0de

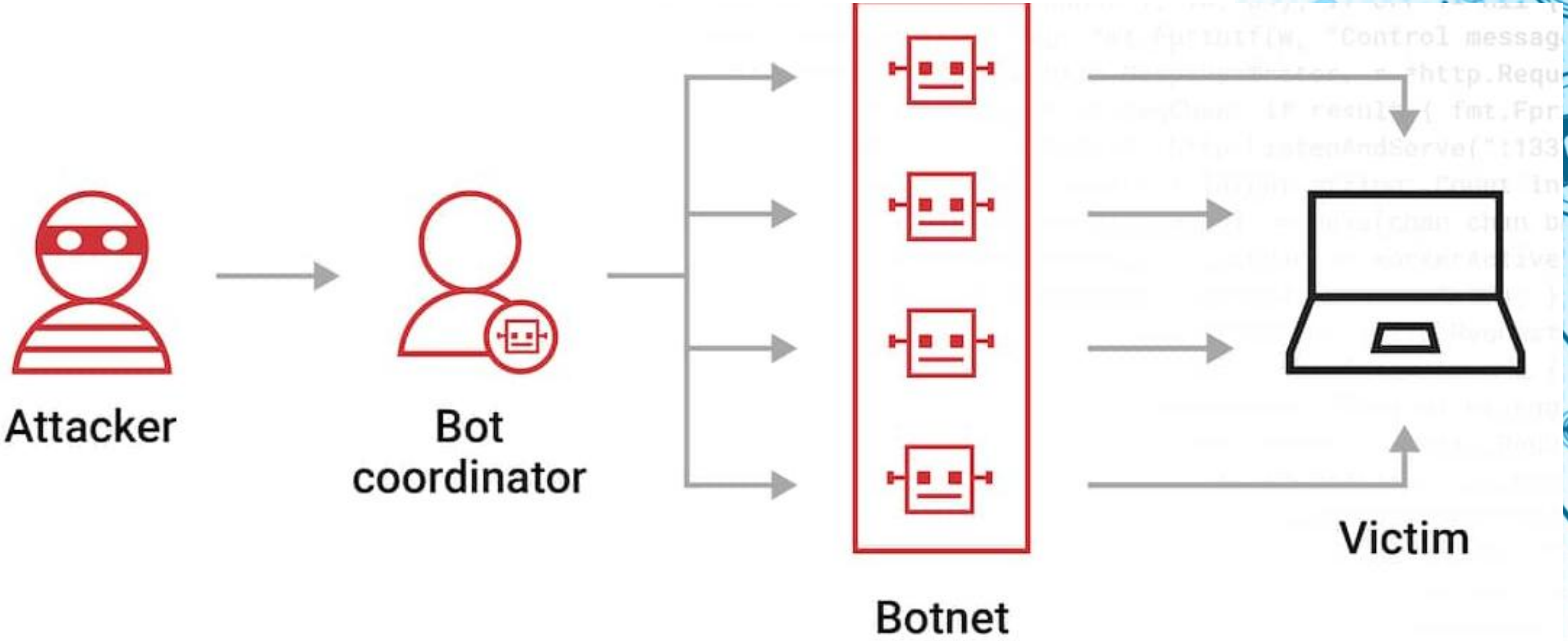
We Are : CCOCOT - ./Mr.Greetz69 - Jilaan404 - ./N4skun - Kazuya404 -
Monkey B Luffy - Ashura - Effect - B0c4H_Id30T - Fuss - Sector.V2

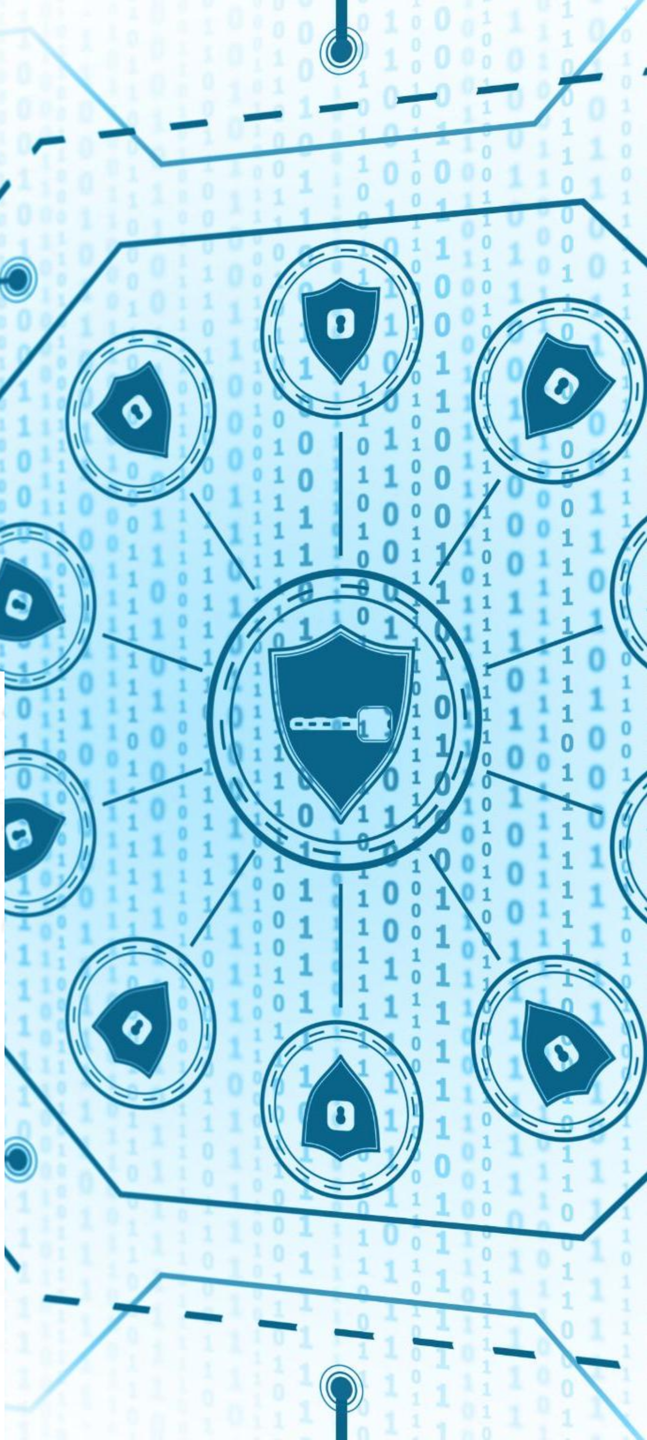


Intrusion Kill Chain Phases

Installation, Command and Control

Malware weapon installs an access point usable by the intruder thorugh which „hands on action” is delivered by attacker





Actions on Objectives

Financial gain

primary driver for most cybercriminals, representing 55% of all threat actors in 2024

Espionage

key motivator in geopolitically targeted attacks, accounting for 72% of incidents in the aerospace and defense sector in 2024

Revenge and disruption caused by insider threats

responsible for 20% of cybersecurity breaches in 2023

Mandiant M-Trends 2025 Report
PwC Cyber Threats 2024: A Year in Retrospect
Cybersecurity Insiders 2023: Insider Threat Report

Implementing Zero Trust Security with Microsoft Services

Operationalizing Zero Trust: Microsoft Ecosystem Approach and Strategies

Integrated Identity Security Services

Microsoft provides integrated Entra Suite that unifies identity protection across various IT environments.

Defend against threats with XDR

Microsofr XDR collects and correlates data across multiple security layers to provide unified threat detection and response.

Zero Trust Framework for devices

The Zero Trust framework assumes no implicit trust and verifies each access request thoroughly.

Measured protection on every level with Secure Score

Environment is comprehensively checked to in order to achieve golden standard of security.

Zero Trust in Entra ID

Continuous User Verification

User identities are verified continuously with multi-factor authentication and conditional access, preventing unauthorized access at every step.

Least-Privilege Enforcement

Access is limited to only necessary resources, minimizing risks by not granting excess permissions to users.

Real-Time Threat Monitoring

User activity is monitored in real time to quickly detect and respond to potential security threats across environments.

Intune and Zero Trust

Comprehensive Endpoint Security

Intune manages and secures devices and apps, safeguarding endpoints across various platforms with cloud-based controls.

Zero Trust Principles Enforcement

Intune enforces strong access controls and verifies device compliance before granting access, supporting Zero Trust architecture.

Continuous Protection and Monitoring

With ongoing monitoring, policy management, and threat detection, Intune helps organizations protect resources and identities.

Use Least Privilege Access: Addressing Endpoint Privilege Challenges with Intune EPM and JIT/JEA

Principle of Least Privilege

Grant users only the permissions they need to minimize security risks and reduce attack surfaces.

Endpoint Privilege Management

Use Endpoint Privilege Management to enforce least privilege policies on devices centrally and effectively.

Just-In-Time and Just-Enough Administration

Implement JIT/JEA to grant temporary, limited access only when needed to enhance security.

Microsoft XDR Security Solution

Real-Time Threat Detection

Microsoft XDR identifies security threats as they occur, enabling organizations to respond quickly and reduce potential damage.

Automated Incident Response

XDR automates many responses to security incidents, improving efficiency and minimizing the risk of human error.

Centralized Security and AI Integration

By unifying security data and integrating AI, XDR enhances threat analysis and strengthens overall cybersecurity posture.

Microsoft Secure Score

Security Posture Evaluation

Secure Score measures an organization’s current security posture within Microsoft 365, highlighting strengths and vulnerabilities.

Actionable Security Recommendations

It offers specific recommendations to enhance security and allows organizations to track their progress over time.

Compliance Framework Integration

Secure Score aligns with recognized standards like ISO, NIST, and GDPR, helping organizations meet compliance requirements.

Strategic Alignment and Economic Value of Zero Trust with Microsoft

Strategic Alignment: Leveraging Zero Trust as a Business Accelerator

Enhanced Security

Zero Trust strengthens security by verifying every access request continuously.

Business Agility

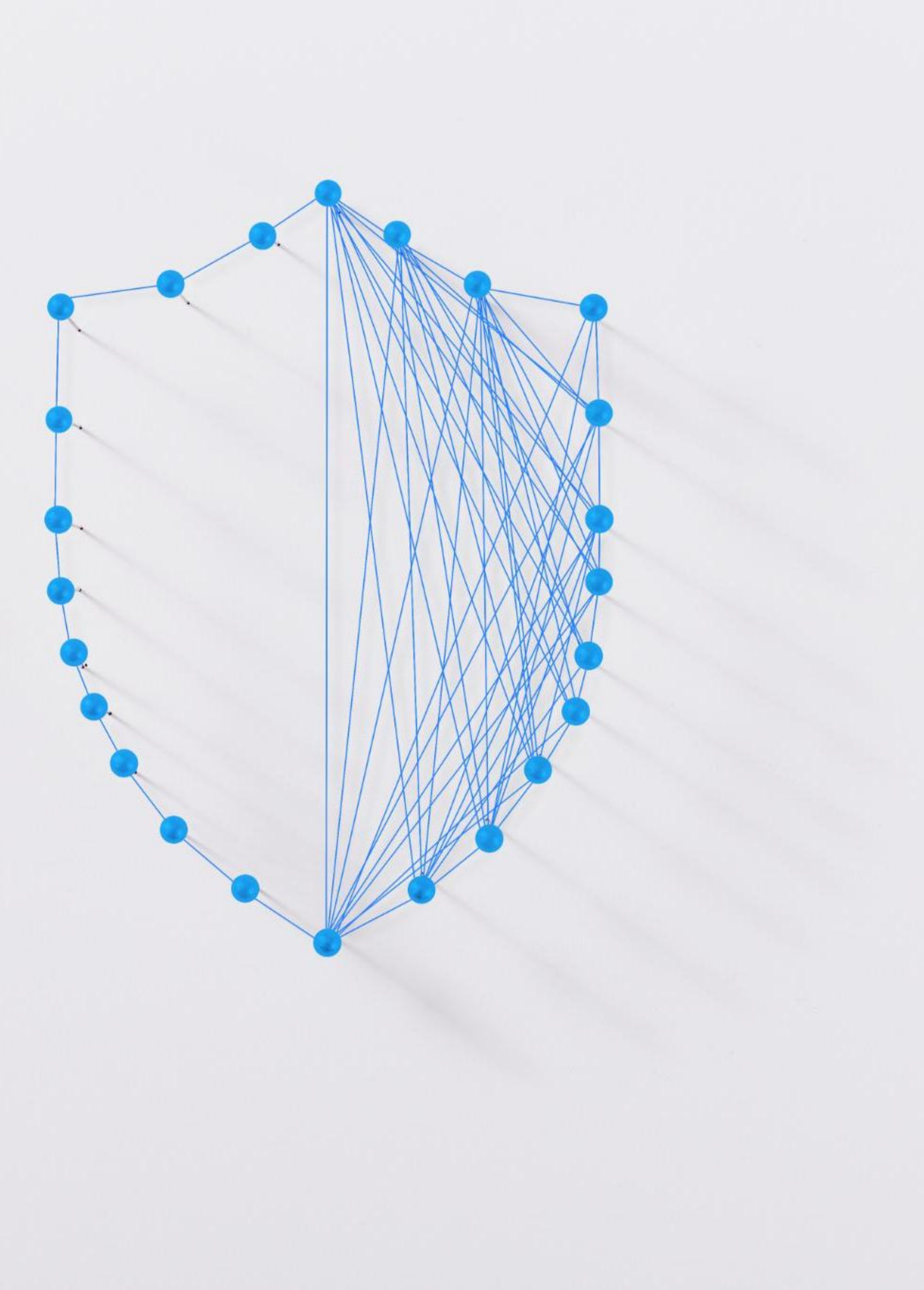
Zero Trust enables flexible and secure access, accelerating business agility and innovation.

Support for Digital Transformation

Zero Trust supports digital transformation by safeguarding critical resources and data.

Fostering Customer Trust

Implementing Zero Trust builds greater customer confidence through robust security measures.



Competitive Leadership: Microsoft’s Position in Zero Trust Platform Innovation

Zero Trust Security Leadership

Microsoft leads innovation in Zero Trust security with cutting-edge, integrated platform solutions.

Simplified Implementation

The platform simplifies Zero Trust implementation for organizations of varying sizes and complexities.

Robust and Scalable Solutions

Microsoft’s security platform delivers scalable, robust solutions adaptable to evolving organizational needs.

Quantifying ROI: Key Financial Metrics, Consolidation, and Cost Avoidance

Lowered Incident Response Costs

Zero Trust solutions reduce expenses related to managing and mitigating security incidents effectively.

Infrastructure Consolidation

Combining IT systems under Zero Trust reduces complexity and operational costs across the infrastructure.

Cost Avoidance from Breaches

Implementing Zero Trust helps prevent costly breaches, avoiding financial losses and reputational damage.

Strong Return on Investment

The combined financial benefits of Zero Trust lead to a significant and measurable ROI for organizations.

Conclusion

Strategic Security Approach

Zero Trust framework is essential for protecting modern digital environments against evolving threats.

Combining Principles and Innovation

Integrates proven security principles with advanced Microsoft technologies for enhanced protection.

Business Value and Risk Reduction

Implementing this framework reduces risks and delivers measurable value to organizations.