WELCOME

to the year A.G. **8**

[after chatGPT / A.D. 2018]


01

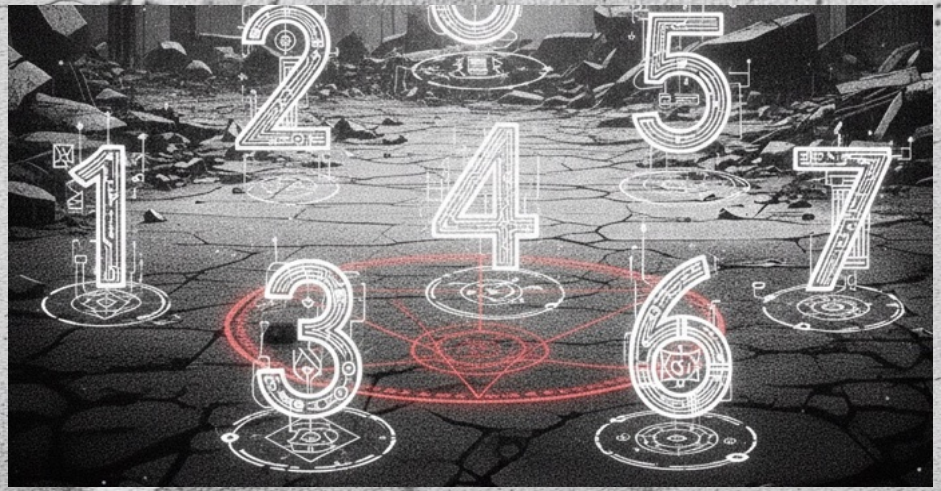

10


AskTheAnalyst
Training
IR-Services
CTI
Takedown-Service
Takedown-Service
Iot
Barrichas
CyberCrime
APTS
Samael
Target
System
Botnet
Botnet
AI

- Identifies which tasks adversaries must complete in order to achieve their objectives
- Enhances visibility into attacks and each individual step
- **Enables defense options at each stage**

Developed by Lockheed Martin as part of “Intelligence Driven Defense”

SEVEN STAGES OF ATTACK



1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

Stage 1: Reconnaissance

Attackers research and identify targets

Attack Methods:

- Email harvesting
- Vulnerability scanning

Defense:

- Limit public information
- Monitor for scanning activity

Target Breach 2013

- Attackers identified Target's third–party HVAC vendor “Fazio Mechanical”
- Discovered vulnerabilities in vendor's network security
- Harvested employee email addresses from public sources
- Mapped vendor's connection to Target's network infrastructure

Stage 2: Weaponization

Creating the attack payload

Attack Methods:

- Exploit development
- Malware customization

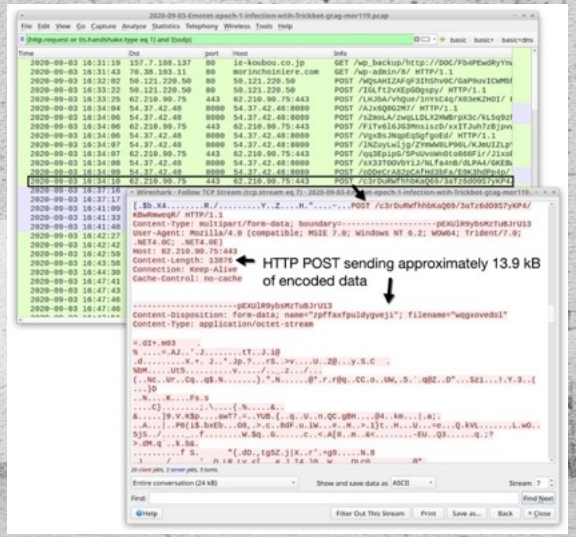
Defense:

- Threat intelligence sharing
- Monitor malware indicators

Emotet 2020

Weaponization Phase

- Malicious Word document containing VBScript macros
- Obfuscated PowerShell downloader script
- Remote Access Trojan (RAT) payload



Stage 3: Delivery

Transmitting the payload to the target

Attack Methods:

- Phishing emails
- Malicious websites

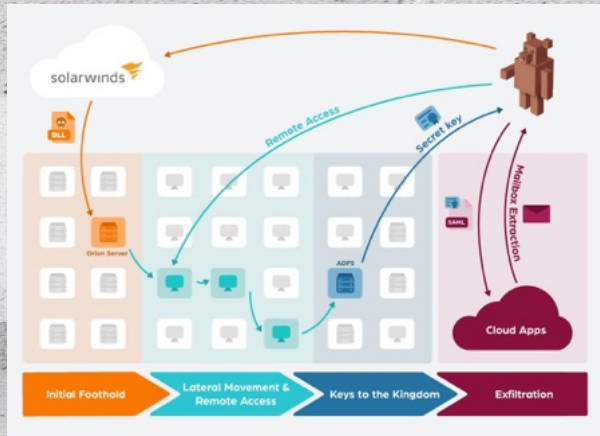
Defense:

- Email filtering and scanning
- Web content filtering

SolarWinds 2020

Delivery Phase

- SUNBURST backdoor in Orion update
- 18,000+ customers compromised
- Included valid digital signature



Stage 4: Exploitation

Triggering the vulnerability

Attack Methods:

- Code execution
- Vulnerability exploitation

Defense:

- Patch management
- Endpoint protection (EDR)

NotPetya 2017

Exploitation Phase

- EternalBlue SMBv1 exploit
- Mimikatz credential harvesting
- No user interaction required

Stage 5: Installation

Establishing persistence on the system

Attack Methods:

- Backdoor installation
- Persistence mechanisms

Defense:

- System integrity monitoring
- Application whitelisting

Target Breach 2013

Installation Phase

- Installed memory–scraping malware on POS systems
- Deployed KAPTOXA/POSWDS RAM scraper malware
- Created persistent backdoor for ongoing access
- Malware survived system reboots via registry modifications

Stage 6: Command & Control

Establishing external communication channel

Attack Methods:

- C2 channel establishment
- Remotely controlled activation

Defense:

- Network traffic analysis
- Block C2 domains/IPs

SolarWinds 2020

Command & Control Phase

- SUNBURST backdoor contacted C2 located at “avsvmcloud[.]com”
- Usage of HTTPS for encrypted C2 communications
- Deployment of TEARDROP dropper delivering Cobalt Strike Beacon
- Domain Generation Algorithms (DGA) for C2 resilience

Stage 7: Actions on Objectives

Executing the attack's primary goal

Attack Methods:

- Data exfiltration
- Ransomware deployment

Defense:

- Data loss prevention (DLP)
- Backup and recovery plans

NotPetya 2017

Actions on Objectives Phase

- Master Boot Record (MBR) overwritten with custom bootloader
- Encrypted Master File Table (MFT) using Salsa20 cipher
- Encrypted files across network – accumulated $10B+ in global damage
- Destroyed encryption keys – data recovery impossible

Stage 1–7: A Real World Example From 2025

Anthropic AI Attack (Nov 2025)

1. **Reconnaissance**
   - Conducted by Claude autonomously
2. **Weaponization**
   - Claude generated exploits + attacks
3. **Delivery**
   - Claude automatically delivered
4. **Exploitation**
   - Claude autonomously performed
5. **Installation**
   - Claude established persistence
6. **Command and Control (C2)**
   - Claude independently managed compromised systems
7. **Actions on Objectives**
   - Claude executed the final objectives

Kill Chain Prevention Strategies

Awareness & Prevention

- Monitor external attack surface
- Minimize exposed services
- CTI/Threat Intelligence
- Trainings

Execution / Detection & Prevention

- Patch Management
- Data Feeds
- EDR/MDR/xDR
- YARA rules for Detection

Incident Response / Recovery

- IR and Forensic Services
- Expert Support Services
- Backup (tested!)
- Guidelines/Playbooks


AI-Driven Cyber Threats
Compute Power as Cryptocurrency
Nation-State Cyber Warfare
AI System Vulnerabilities

AI–Driven Cyber Threats

- Adversaries fully embrace AI as the norm
- Dark AI enables autonomous attacks at scale
- AI enhances speed, scope, and effectiveness
- Minimal human oversight required for attacks

Nation–State Cyber Warfare

- Escalating attacks on critical infrastructure
- Targets communication networks
- Supply chain infiltration is increasing
- Geopolitical tensions elevate cyber operations

AI System Vulnerabilities

- Prompt injection attacks target enterprise AI
- Manipulate AI to bypass security protocols
- Semi–autonomous, AI–assisted malware
- Environment–aware obfuscation techniques

Compute Power as Cryptocurrency

- LLMjacking: hijack infrastructure for AI
- Steal compute capability to train LLMs
- Run autonomous AI agents on stolen resources
- Monitor GPU utilization like network traffic

Defense Strategy

- Deploy automated detection and response
- Strengthen identity and access management
- Implement Zero Trust architecture
- Regular security awareness training

The cybersecurity landscape in 2026 is evolving rapidly

- AI transforms both attack and defense capabilities
- Understanding attack frameworks enables prevention
- Proactive defense is more essential than ever

So, is there any good news in cybersecurity?

2025: The Year Law Enforcement Struck Back

- Over 1,000 arrests globally
- More than €75 million in cryptocurrency and assets seized
- Hundreds of servers and thousands of domains taken down in LEA operations
- Multiple major ransomware operations disrupted
- Billions of stolen credentials recovered from infostealer operations

https://breached.company/global-cybercrime-crackdown-2025-a-mid-year-assessment-of-major-arrests-and-takedowns/

2025: The Year Law Enforcement Struck Back

European Union Operations

Operation Synergia (Phase 2):

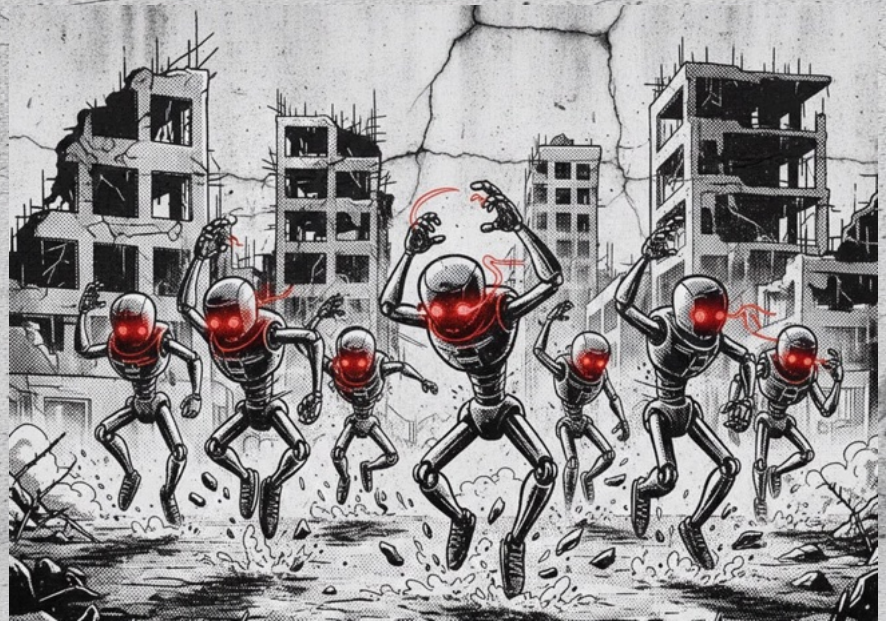
- Timeline: April 1 – August 31, 2025
- Results: 41 arrests, 43 devices seized, 65 individuals under investigation
- Infrastructure: 22,000+ malicious IP addresses taken down (75% of identified targets)
- Participation: 95 Interpol member countries

https://breached.company/global-cybercrime-crackdown-2025-a-mid-year-assessment-of-major-arrests-and-takedowns/

Not the end just yet …

“Blinde tanzen auch durch Trümmer, sie sehen die Zerstörung nicht.”

Oswald Henke, 1993



marco preuß // marco@wintercode.eu