网络空间安全攻防趋势分享：
高级持续威胁（APT）与大语言模型（GPT）

彭峙酿

2023年9月27日

自我介绍

彭峙酿

首席安全研究员/首席架构师 @Sangfor

密码学博士

隐私计算、软件安全、威胁猎捕、AI

进攻性安全研究 & 防守性安全研究

PrintNightmare、Zerologon、ExplodingCan、EOS百亿美金漏洞

https://sites.google.com/site/zhiniangpeng

Some of My Bugs

CNVD-2012-13926,CVE-2017-7269,CVE-2018-20694,CVE-2018-20746,CVE-2018-20693,CVE-2018-20692,CVE-2018-20696,CVE-2018-20689,CVE-2018-20690,CVE-2018-10812,
CVE-2019-6184,CVE-2019-6186,CVE-2019-6487,CVE-2019-1253,CVE-2019-1292,CVE-2019-1317,CVE-2019-1340,CVE-2019-1342,CVE-2019-1374,CVE-2019-8162,CVE-2019-1474,
CVE-2019-18371,CVE-2019-18370,CVE-2020-0616,CVE-2020-0635,CVE-2020-0636,CVE-2020-0638,CVE-2020-0641,CVE-2020-0648,CVE-2020-0697,CVE-2020-0730,CVE-2020-3808,
CVE-2020-0747,CVE-2020-0753,CVE-2020-0754,CVE-2020-0777,CVE-2020-0780,CVE-2020-0785,CVE-2020-0786,CVE-2020-0789,CVE-2020-0794,CVE-2020-0797,CVE-2020-0800,
CVE-2020-0805,CVE-2020-0808,CVE-2020-0819,CVE-2020-0822,CVE-2020-0835,CVE-2020-0841,CVE-2020-0844,CVE-2020-0849,CVE-2020-0854,CVE-2020-0858,CVE-2020-0863,
CVE-2020-0864,CVE-2020-0865,CVE-2020-0868,CVE-2020-0871,CVE-2020-0896,CVE-2020-0897,CVE-2020-0899,CVE-2020-0900,CVE-2020-0934,CVE-2020-0935,CVE-2020-0936,
CVE-2020-0942,CVE-2020-0944,CVE-2020-0983,CVE-2020-0985,CVE-2020-0989,CVE-2020-1000,CVE-2020-1002,CVE-2020-1010,CVE-2020-1011,CVE-2020-1029,CVE-2020-1068,
CVE-2020-1077,CVE-2020-1084,CVE-2020-1086,CVE-2020-1090,CVE-2020-1094,CVE-2020-1109,CVE-2020-1120,CVE-2020-1121,CVE-2020-1123,CVE-2020-1124,CVE-2020-1125,
CVE-2020-1131,CVE-2020-1134,CVE-2020-1137,CVE-2020-1139,CVE-2020-1144,CVE-2020-1146,CVE-2020-1151,CVE-2020-1155,CVE-2020-1156,CVE-2020-1157,CVE-2020-1158,
CVE-2020-1163,CVE-2020-1164,CVE-2020-1165,CVE-2020-1166,CVE-2020-1184,CVE-2020-1185,CVE-2020-1186,CVE-2020-1187,CVE-2020-1188,CVE-2020-1189,CVE-2020-1190,
CVE-2020-1191,CVE-2020-1196,CVE-2020-1199,CVE-2020-1201,CVE-2020-1204,CVE-2020-1209,CVE-2020-1211,CVE-2020-1217,CVE-2020-1222,CVE-2020-1231,CVE-2020-1233,
CVE-2020-1235,CVE-2020-1244,CVE-2020-1257,CVE-2020-1264,CVE-2020-1269,CVE-2020-1270,CVE-2020-1273,CVE-2020-1274,CVE-2020-1276,CVE-2020-1277,CVE-2020-1278,
CVE-2020-1282,CVE-2020-1283,CVE-2020-1304,CVE-2020-1305,CVE-2020-1306,CVE-2020-1307,CVE-2020-1309,CVE-2020-1312,CVE-2020-1317,CVE-2020-1337,CVE-2020-1344,
CVE-2020-1346,CVE-2020-1347,CVE-2020-1352,CVE-2020-1356,CVE-2020-1357,CVE-2020-1360,CVE-2020-1361,CVE-2020-1362,CVE-2020-1364,CVE-2020-1366,CVE-2020-1372,
CVE-2020-1373,CVE-2020-1375,CVE-2020-1385,CVE-2020-1392,CVE-2020-1393,CVE-2020-1394,CVE-2020-1399,CVE-2020-1404,CVE-2020-1405,CVE-2020-1424,CVE-2020-1427,
CVE-2020-1441,CVE-2020-0518,CVE-2020-1461,CVE-2020-1465,CVE-2020-1472,CVE-2020-1474,CVE-2020-1475,CVE-2020-1484,CVE-2020-1485,CVE-2020-1511,CVE-2020-1512,
CVE-2020-0516,CVE-2020-1516,CVE-2020-1517,CVE-2020-1518,CVE-2020-1519,CVE-2020-1521,CVE-2020-1522,CVE-2020-1524,CVE-2020-1528,CVE-2020-1538,CVE-2020-8741,
CVE-2020-1548,CVE-2020-1549,CVE-2020-1550,CVE-2020-1552,CVE-2020-1590,CVE-2020-1130,CVE-2020-16851,CVE-2020-16852,CVE-2020-1122,CVE-2020-1038 ,
CVE-2020-17089,CVE-2020-16853,CVE-2020-16879,CVE-2020-16900,CVE-2020-16980,CVE-2020-17014,CVE-2020-17070,CVE-2020-17073,CVE-2020-17074,CVE-2020-17075,
CVE-2020-17076,CVE-2020-17077,CVE-2020-17092,CVE-2020-17097,CVE-2020-17120,CVE-2021-1649,CVE-2021-1650,CVE-2021-1651,CVE-2021-1659,CVE-2021-1680,
CVE-2021-1681,CVE-2021-1686,CVE-2021-1687,CVE-2021-1688,CVE-2021-1689,CVE-2021-1690,CVE-2021-1718,CVE-2021-1722,CVE-2021-24072,CVE-2021-24077,
CVE-2021-3750,CVE-2021-24088,CVE-2021-26869,CVE-2021-26870,CVE-2021-26871,CVE-2021-26885,CVE-2021-28347,CVE-2021-28351,CVE-2021-28436,CVE-2021-28450,
CVE-2021-31966,CVE-2021-34527,CVE-2021-42321,CVE-2021-36970,CVE-2021-38657,CVE-2021-40485,CVE-2021-41366,CVE-2021-42294,CVE-2021-42297,CVE-2021-43216,
CVE-2021-43223,CVE-2021-43248,CVE-2022-21835,CVE-2022-21837,CVE-2022-21878,CVE-2022-21881,CVE-2022-21888,CVE-2022-21971,CVE-2022-21974,CVE-2022-21992,
CVE-2022-23285,CVE-2022-23290,CVE-2022-24454,CVE-2022-29108,CVE-2022-24547,CVE-2022-23270,CVE-2022-26930,CVE-2022-29103,CVE-2022-29113,CVE-2022-38036,
CVE-2022-35793,CVE-2022-35755,CVE-2022-35749,CVE-2022-35746,CVE-2022-34690,CVE-2022-21980,CVE-2022-22050,CVE-2022-22024,CVE-2022-22022,CVE-2022-30226,
CVE-2022-30157,CVE-2022-29108,CVE-2022-21999,CVE-2023-21683,CVE-2023-21684,CVE-2023-21693,CVE-2023-21801,CVE-2023-23403,CVE-2023-23406,CVE-2023-23413,
CVE-2023-24856,CVE-2023-24857,CVE-2023-24858,CVE-2023-24863,CVE-2023-24865,CVE-2023-24866,CVE-2023-24867,CVE-2023-24907,CVE-2023-24868,CVE-2023-24909,
CVE-2023-24870,CVE-2023-24872,CVE-2023-24913,CVE-2023-24876,CVE-2023-24924,CVE-2023-24883,CVE-2023-24925,CVE-2023-24884,CVE-2023-24926,CVE-2023-24885,
CVE-2023-24927,CVE-2023-24886,CVE-2023-24928,CVE-2023-24887,CVE-2023-24929,CVE-2023-28243,CVE-2023-28296,CVE-2023-29366,CVE-2023-29367,CVE-2023-32017,
CVE-2023-32039,CVE-2023-32040,CVE-2023-32041,CVE-2023-32042,CVE-2023-32085,CVE-2023-35296,CVE-2023-35302,CVE-2023-35306,CVE-2023-35313,CVE-2023-35323,
CVE-2023-35324,CVE-2023-36898,……

大纲

网络攻击简介

攻防对抗：ATT&CK

猫鼠游戏：从杀软到GPT

不对称战争：谁会胜利?

总结

网络攻击简介

网络攻击

通过未经授权访问计算机系统

来窃取、泄露、更改、禁用或破坏信息的不受欢迎的尝试。

网络攻击的动机

主要分为三大类：

犯罪、政治和个人。

犯罪：盗窃金钱、数据盗窃或业务中断来谋取经济利益

个人：如心怀不满的前任员工，破坏公司的系统

政治：间谍活动、国家对抗等

幕后黑手

外来威胁：

有组织的犯罪分子或犯罪集团

专业黑客，例如国家资助的行动者

业余黑客，比如黑客主义者

内部威胁：

员工对于安全政策和程序粗心大意

心怀不满的现任或前任雇员

具有系统访问权限的业务合作伙伴、客户、承包商或供应商

攻击者的目标

组织、国家行为者或私人想要达成一个或多个目的，例如：

企业财务数据

客户数据库，包括个人身份信息 (PII)

电子邮件地址和登录凭据

知识产权，如商业秘密或产品设计

军事秘密、武器

IT基础设施访问

IT 服务，接受财务付款

敏感的个人数据

政府部门和政府机构

攻防对抗：ATT&CK

攻击者手法(企业版ATT&CK)

企业版ATT&CK


Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (2)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (6)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Valid Accounts (4)
Execution
10 techniques
Command and Scripting Interpreter (8)
Exploitation for Client Execution
Inter-Process Communication (2)
Native API
Scheduled Task/Job (5)
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation
Persistence
19 techniques
Account Manipulation (4)
BITS Jobs
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (11)
Implant Container Image
Office Application Startup (6)
Pre-OS Boot (3)
Scheduled Task/Job (5)
Server Software Component (3)
Traffic Signaling (1)
Valid Accounts (4)
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
Boot or Logon Autostart Execution (12)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Event Triggered Execution (15)
Exploitation for Privilege Escalation
Hijack Execution Flow (11)
Process Injection (11)
Scheduled Task/Job (5)
Valid Accounts (4)
Defense Evasion
37 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (7)
Hijack Execution Flow (11)
Impair Defenses (7)
Indicator Removal on Host (6)
Indirect Command Execution
Masquerading (6)
Modify Authentication Process (4)
Modify Cloud Compute Infrastructure (4)
Modify Registry
Modify System Image (2)
Network Boundary Bridging (1)
Obfuscated Files or Information (5)
Pre-OS Boot (3)
Process Injection (11)
Rogue Domain Controller
Rootkit
Signed Binary Proxy Execution (11)
Signed Script Proxy Execution (1)
Subvert Trust Controls (4)
Template Injection
Traffic Signaling (1)
Trusted Developer Utilities Proxy Execution (1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (4)
Valid Accounts (4)
Credential Access
15 techniques
Brute Force (4)
Credentials from Password Stores (3)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Man-in-the-Middle (2)
Modify Authentication Process (4)
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (6)
Discovery
25 techniques
Account Discovery (4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Collection
17 techniques
Archive Collected Data (3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
Data from Information Repositories (2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Email Collection (3)
Input Capture (4)
Man in the Browser
Man-in-the-Middle (2)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (4)
Communication Through Removable Media
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Encrypted Channel (2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (4)
Remote Access Software
Traffic Signaling (1)
Web Service (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Exfiltration Over Physical Medium (1)
Exfiltration Over Web Service (3)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
12 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Endpoint Denial of Service (4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

ATT&CK 评估

巫师蜘蛛+沙虫

企业评估2022

结果

呼吁参与 ✓ — 评估 ✓ — 准备中 ✓ — 发表 ✓

ATT&CK 说明

Wizard Spider是一个出于经济动机的犯罪集团，至少自 2018 年 8 月以来一直在针对从大公司到医院的各种组织开展勒索软件活动。 [1] [2]

Sandworm Team是一个具有破坏性的俄罗斯威胁组织，已被美国司法部和英国国家网络安全中心归咎于俄罗斯 GRU 74455 部队。Sandworm Team 最引人注目的攻击包括 2015 年和 2016 年针对乌克兰电力公司的攻击以及 2017 年的 NotPetya 攻击。沙虫团队至少从 2009 年开始就一直活跃。 [1] [2] [3] [4]

仿真笔记

本轮将重点关注多个团体如何滥用 数据加密影响 (T1486)。在 Wizard Spider 的案例中，他们利用了勒索软件的数据加密，包括广为人知的 Ryuk 恶意软件 (S0446)。另一方面，Sandworm 利用加密来破坏数据，最引人注目的可能是 伪装成勒索软件的NotPetya 恶意软件 (S0368)。虽然今年评估的共同点是为影响而加密的数据，但两个小组都对广泛的利用后贸易技术进行了大量报告。

结果

AhnLab · Bitdefender · BlackBerry CYLANCE · Symantec A Division of Broadcom · CHECK POINT · CISCO · CROWDSTRIKE · CYCRAFT · Cynet · deep instinct · elastic · eset Digital Security Progress. Protected. · Fidelis Cybersecurity · FIREEYE · FORTINET · Malwarebytes · McAfee · Microsoft · paloalto NETWORKS · Qualys · RAPID7 · REAQTA · SentinelOne

ATT&CK 评估

微软概述

参与者配置： APT3、 APT29、 Carbanak+FIN7、 巫师蜘蛛+沙虫

选择对手

下载 JSON

对手回合下载

MITRE Engenuity 不分配分数、排名或评级。评估结果对公众开放，因此其他组织可能会提供自己的分析和解释——这些结果未经 MITRE Engenuity 认可或验证。

概述 | APT3 (2018) | APT29 (2020) | 卡巴纳克+FIN7 (2021) | 巫师蜘蛛 + 沙虫 (2022)

评估总结

以下是微软参与的评估：

评价	分析覆盖率	遥测覆盖	能见度	检测计数
APT3 (2018)	136 中的 41 子步骤	136 中的 103 子步骤	136 中的 108 子步骤	149 跨 136 子步骤
APT29 (2020) 包括 MSSP	134 中的 79 子步骤	134 中的 108 子步骤	120 的 134 子步骤	199 跨 134 子步骤
卡巴纳克+FIN7 (2021)	174 中的 134 子步骤	148 的 174 子步骤	174 中的 151 子步骤	356 跨 174 子步骤
巫师蜘蛛 + 沙虫 (2022)	109 中的 98 子步骤	5 的 109 子步骤	109 中的 98 子步骤	

猫鼠游戏：从杀软到GPT

攻防对抗就是在卷

图片来源： SentinelOne产品介绍PPT

攻防的趋势

攻防的对抗在加强（企业安全方面）

攻击者的难度和门槛在提高

攻击手法、技术多样化

IT基础设施变化：移动互联网、云

安全产品发展趋势

产品多元化： WAF EDR XDR SIEM SOC SIP SOAR 等

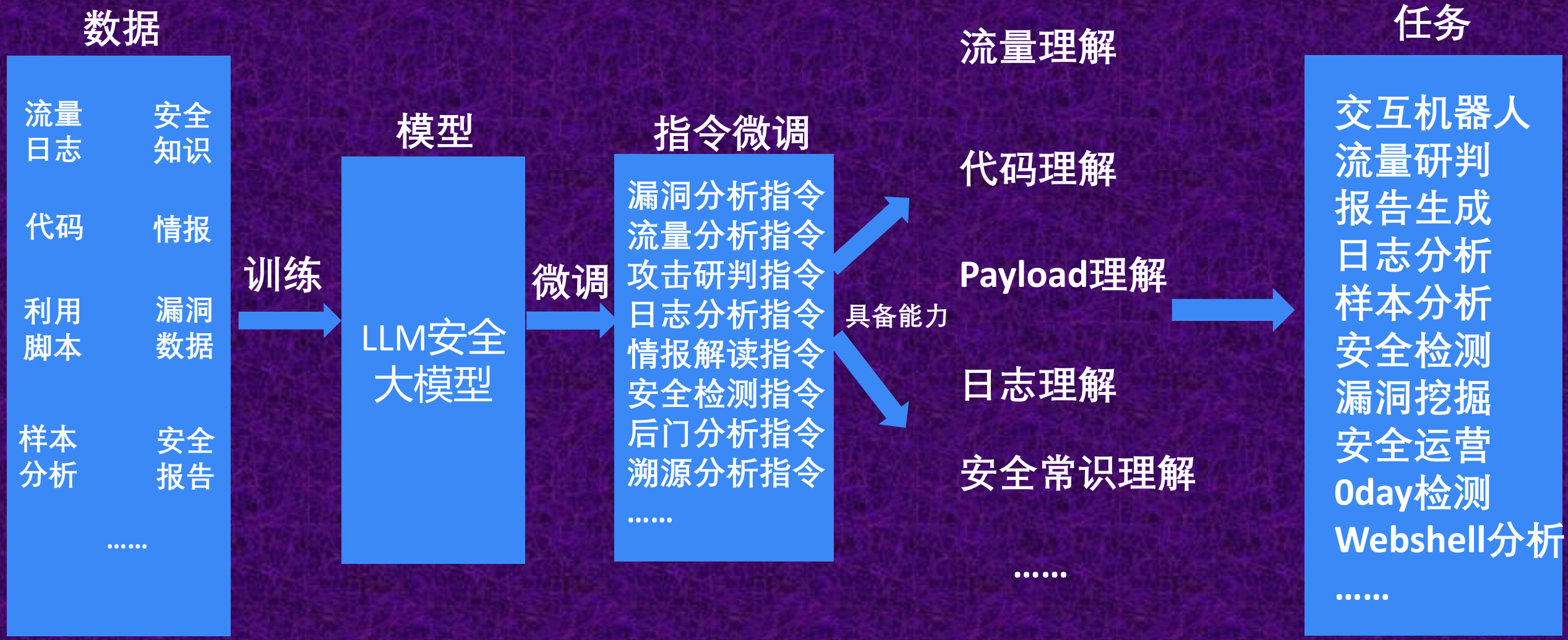
人工智能驱动: 聚合、自动化、秒级响应

Security Copilot:

AI speed and scale Defense

AI 助手

大模型安全能力构想


数据
流量日志
安全知识
代码
情报
利用脚本
漏洞数据
样本分析
安全报告
……
训练
模型
LLM安全大模型
微调
指令微调
漏洞分析指令
流量分析指令
攻击研判指令
日志分析指令
情报解读指令
安全检测指令
后门分析指令
溯源分析指令
……
具备能力
流量理解
代码理解
Payload理解
日志理解
安全常识理解
……
任务
交互机器人
流量研判
报告生成
日志分析
样本分析
安全检测
漏洞挖掘
安全运营
0day检测
Webshell分析
……

AI will Speed and Scale Defense

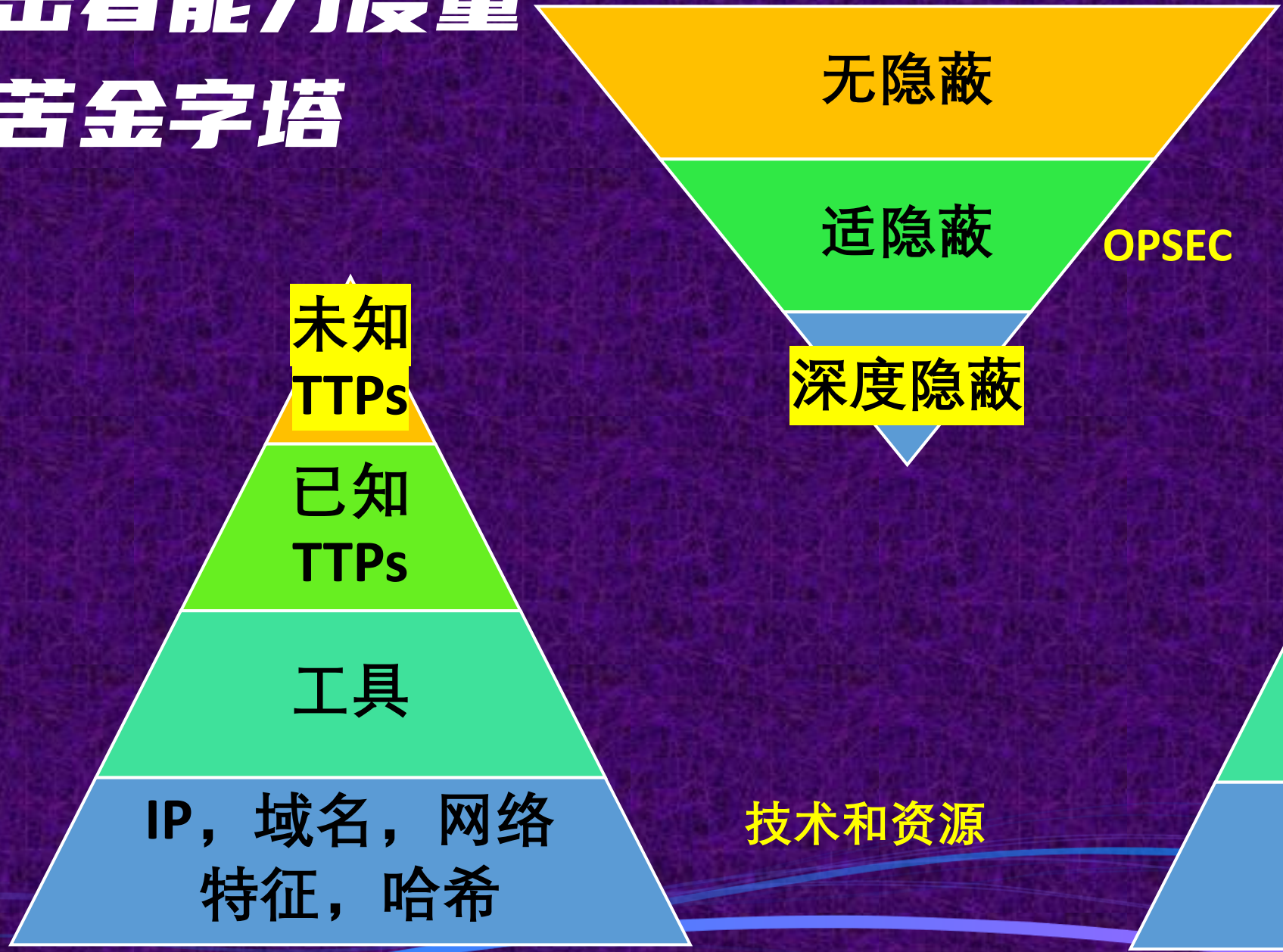
攻击者没得玩了吗?

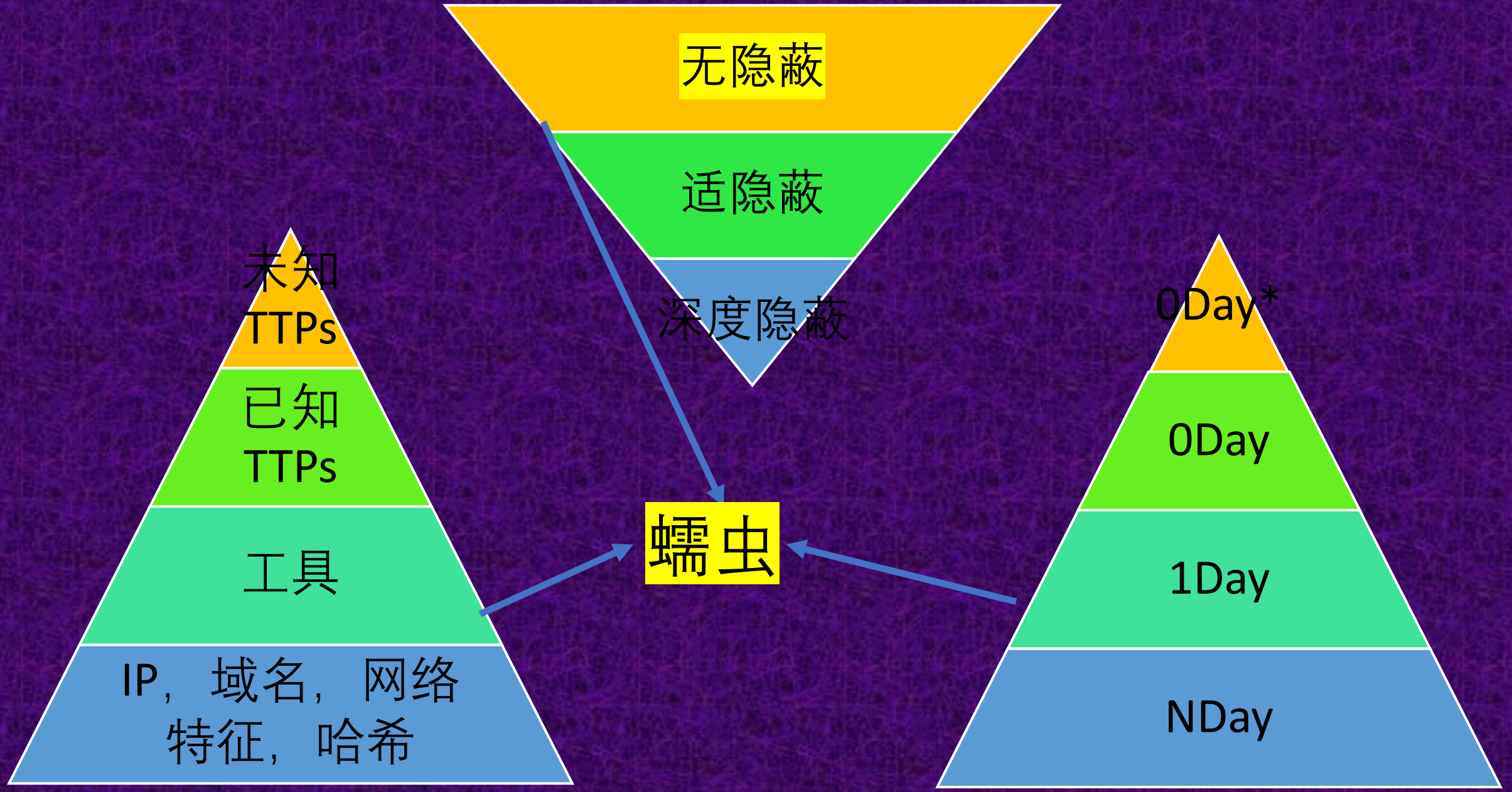
不对称战争：谁会胜利?

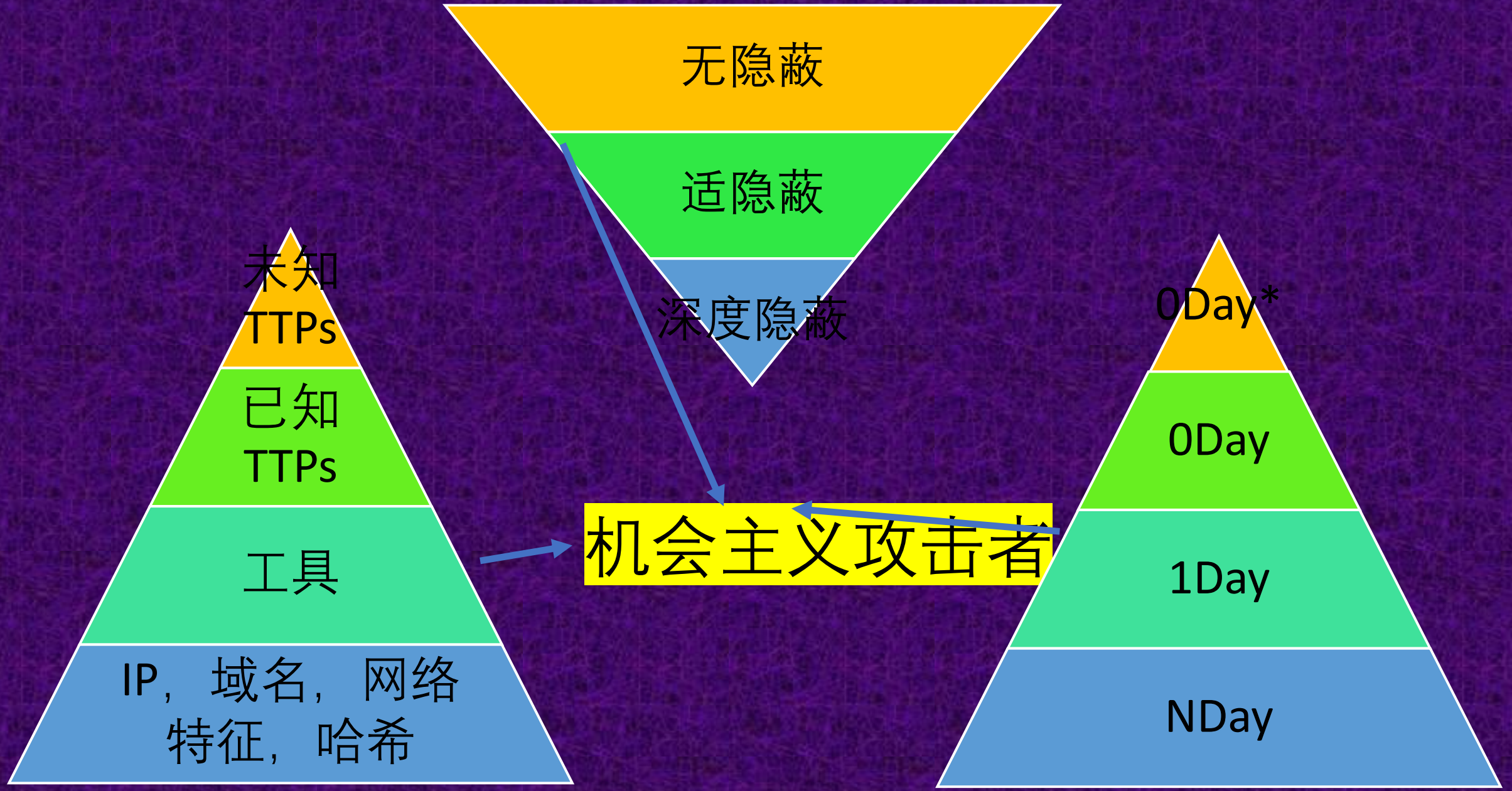
防守方在变强

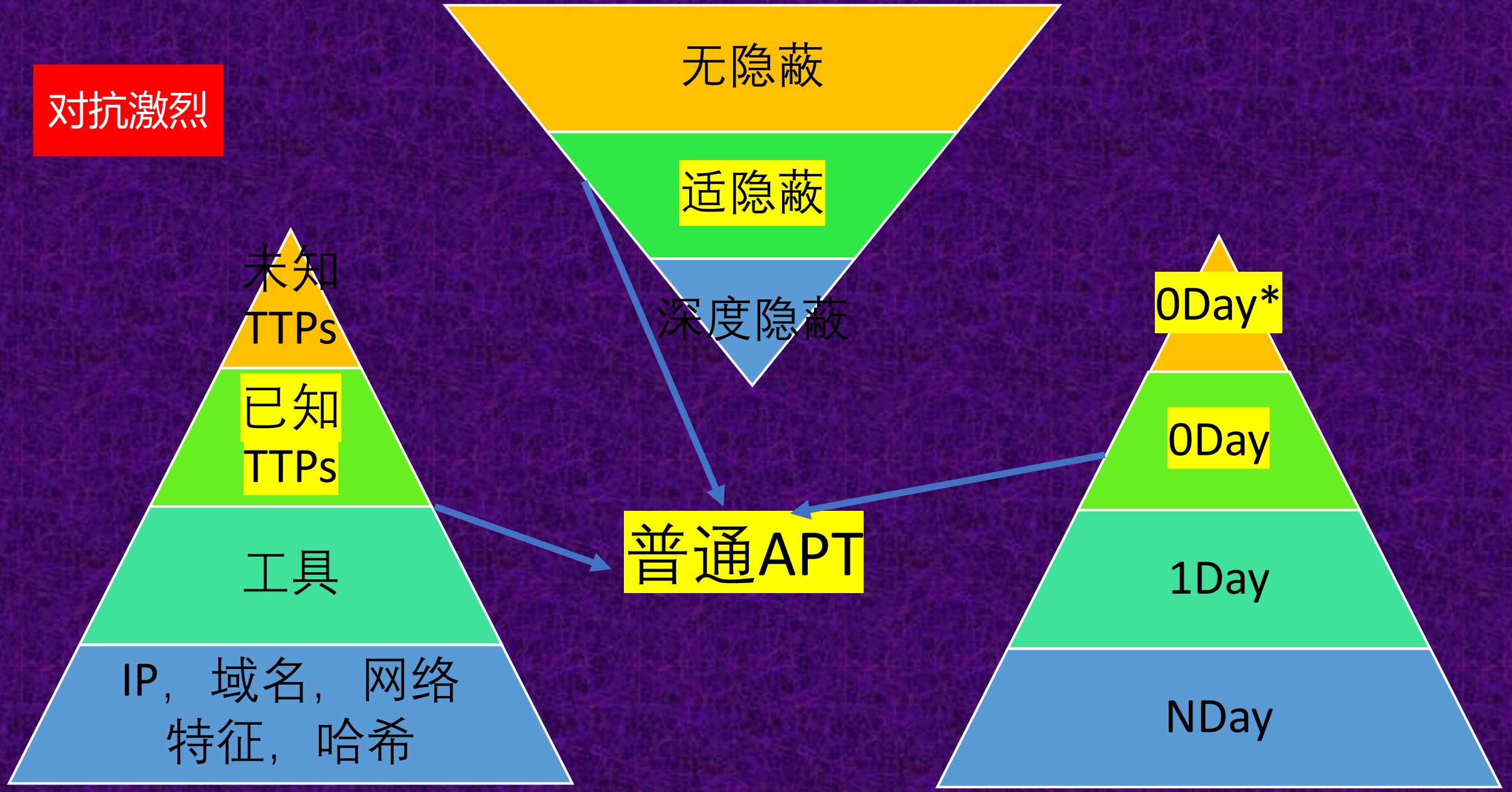
hackers

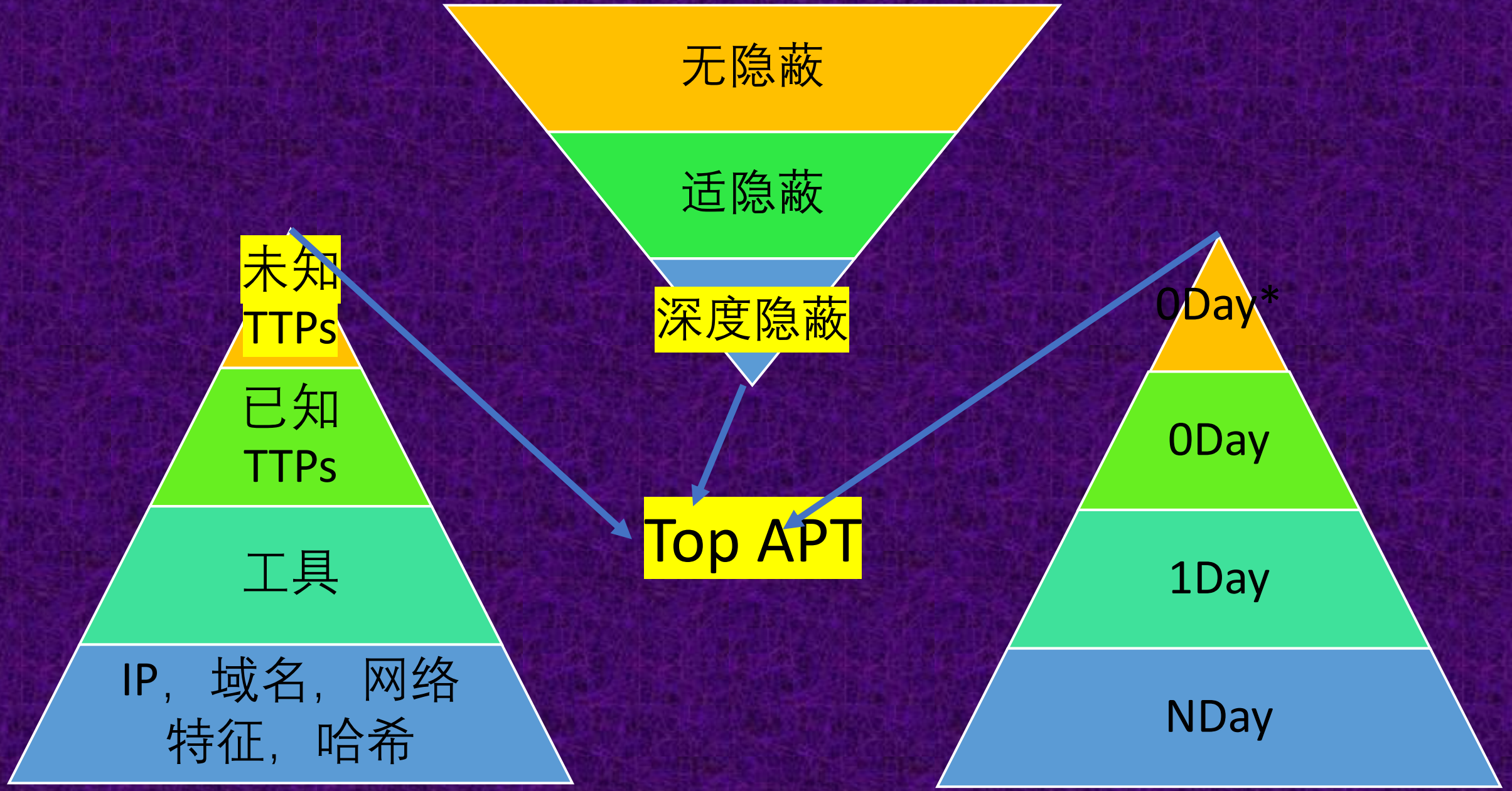
攻击者能力度量
痛苦金字塔




无隐蔽
适隐蔽
深度隐蔽
未知
TTPs
已知
TTPs
工具
IP，域名，网络
特征，哈希
蠕虫
0Day*
0Day
1Day
NDay


无隐蔽
适隐蔽
深度隐蔽
未知
TTPs
已知
TTPs
工具
IP，域名，网络
特征，哈希
机会主义攻击者
0Day*
0Day
1Day
NDay


对抗激烈
无隐蔽
适隐蔽
深度隐蔽
未知
TTPs
已知
TTPs
工具
IP，域名，网络
特征，哈希
普通APT
0Day*
0Day
1Day
NDay


无隐蔽
适隐蔽
深度隐蔽
未知
TTPs
已知
TTPs
工具
IP，域名，网络
特征，哈希
Top APT
0Day*
0Day
1Day
NDay

三角测量行动：

利用iPhone零点击漏洞进行监控的APT攻击；2023年6月被卡巴斯基公开

二

消息不会显示给用户，漏洞在没有任何感知的情况下执行

四

恶意软件在内核漏洞后以 root 权限执行

一

受害者通过iMessage收到一条信息

三

附件中嵌入了多个攻击阶段等等

所有消息都将从设备中删除
全部流量加密

三角测量行动:

恶意软件功能：

- 地理定位（位置、速度、方向）
- 对所有文件和数据库的完全访问权限
- 从iOS钥匙串中提取密钥
- 操作正在运行的进程（如第三方消息应用程序）
- 访问摄像头和麦克风
- 访问地址簿
- 收集附近其他苹果设备的信息

防守者还有很长路要走

未知的攻击手法

深度隐蔽的操作策略

不为人知的攻击面

安全产品的视野盲区

正常业务流量中的攻击

不可思议的0day漏洞

.....

Top APT Groups

总结

未知攻，嫣知防

攻防对抗，猫鼠游戏

攻击者门槛逐渐提高

防守者还有很长的路要走

THANKS!