SOC ReLoad
#SOCReLoad21

TRACK 1 - LEADERS

The Threat Landscape, Paradigm Shifts & Their Impact

Max Heinemeyer
Director of Threat Hunting
DARKTRACE

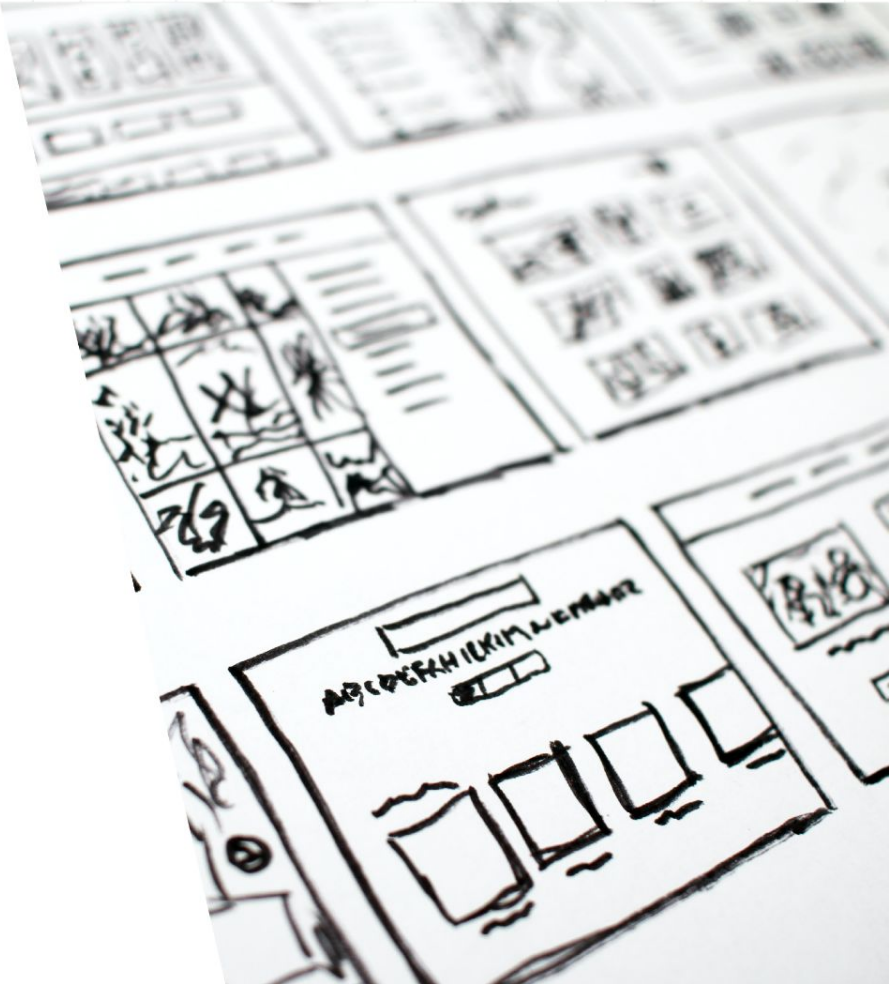
Süleyman Özarslan
VP of Picus Labs
PICUS

Agenda

1) Threat Landscape Overview

2) Real-Life Threat Stories

3) Key Takeaways



Threat Landscape Overview


DARKTRACE
LSE:DARK
30+
offices
1,500+
employees
#1 AI
First at-scale deployment of AI in cyber security
#1 PEER AWARD 2021
Darktrace
TIME
TIME 100 Most Influential Companies 2021
2021
GLOBEE AWARDS GOLD WINNER
CYBER SECURITY GLOBAL EXCELLENCE AWARDS
5,000+
customers
in 100+ countries
60+
patents
For AI and machine learning concepts
HQ: Cambridge, UK
Across every industry sector

Hafnium cyber-attack neutralized by AI in December 2020

SaaS security risks: Detecting a multi-account hijack with AI

APT35 ‘Charming Kitten' discovered in a pre-infected environment

How AI stopped a WastedLocker intrusion

Catching APT41 exploiting a zero-day vulnerability

How a SOC team neutralized the QakBot banking trojan

Threat Landscape Trends

Multi-Extortion Ransomware

Critical infrastructure targeted

Professionalization of cyber-crime

SaaS account takeovers

Decreased dwell time

Out-of-hours attacks

Red Report 2021
Top 10 ATT&CK Techniques

231.507
unique files were analyzed

204.954
files were categorized as malicious

89%
categorized as malicious

2.197.025
actions were extracted

11
actions per malware

1.871.682
ATT&CK techniques were determined in total

8
determined per malware

◆	#1 New	%26	T1059 Command and Scripting Interpreter — Execution
↑	#2 2020:4	%21	T1055 Process Injection — Defense Evasion, Privilege Escalation
◆	#3 New	%19	T1486 Data Encrypted for Impact — Impact
↓	#4 2020:3	%16	T1218 Signed Binary Proxy Execution — Defense Evasion
◆	#5 New	%14	T1003 OS Credential Dumping — Credential Access
◆	#6 New	%13	T1027 Obfuscated Files or Information — Defense Evasion
→	#7 2020:7	%11	T1053 Scheduled Task/Job — Execution, Persistence, Privilege Escalation
↓	#8 2020:4	%9	T1036 Masquerading — Defense Evasion
→	#9 2020:9	%8	T1082 System Information Discovery — Discovery
◆	#10 New	%6	T1497 Virtualization/Sandbox Evasion — Defense Evasion, Discovery

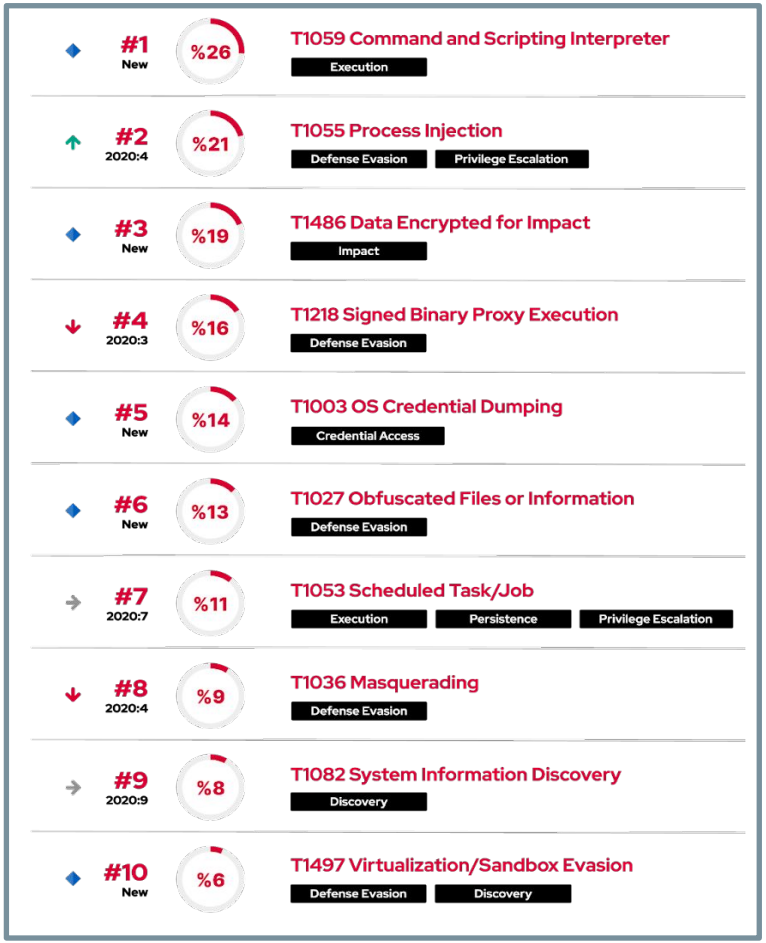
Trends in Adversary TTPs

Data encryption is more common.

Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



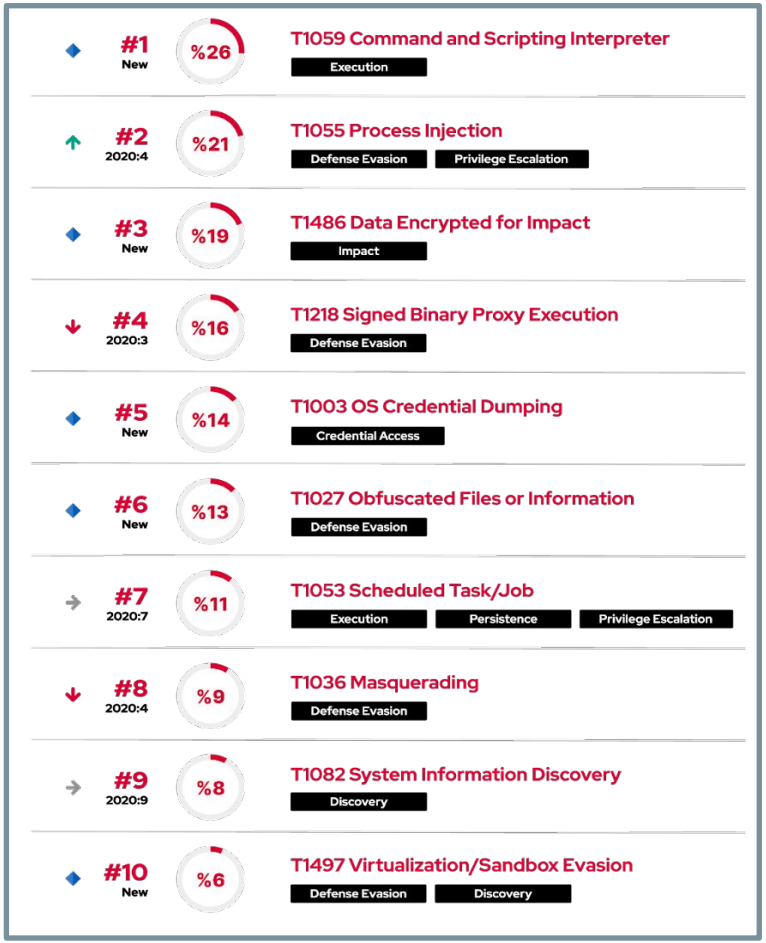
Trends in Adversary TTPs

Data encryption is more common.

Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



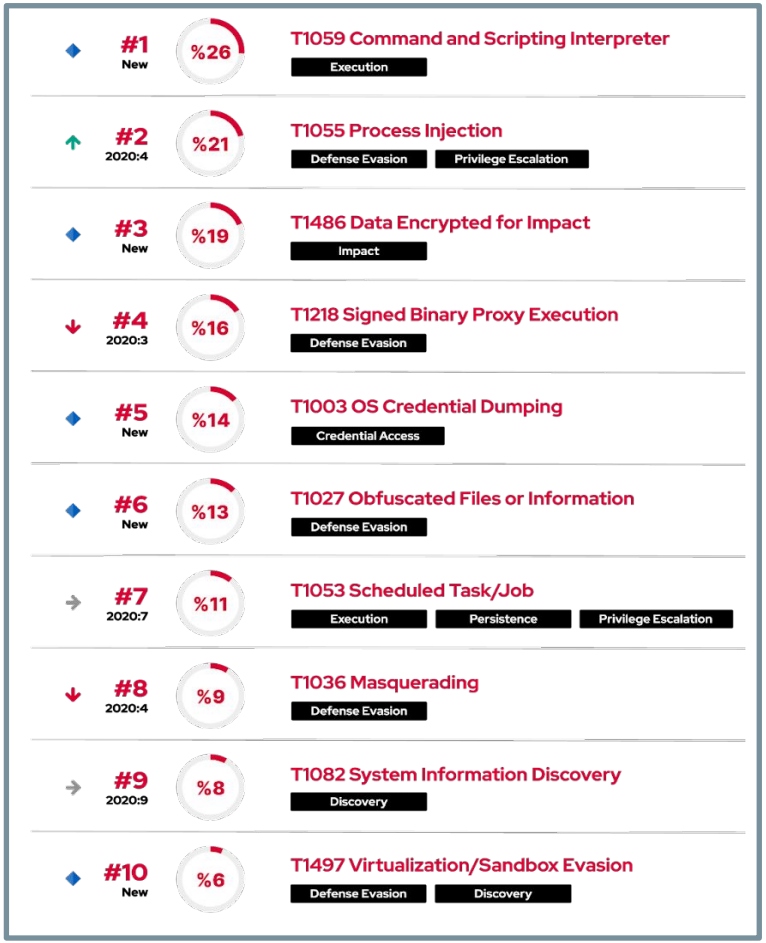
Trends in Adversary TTPs

Data encryption is more common.

Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



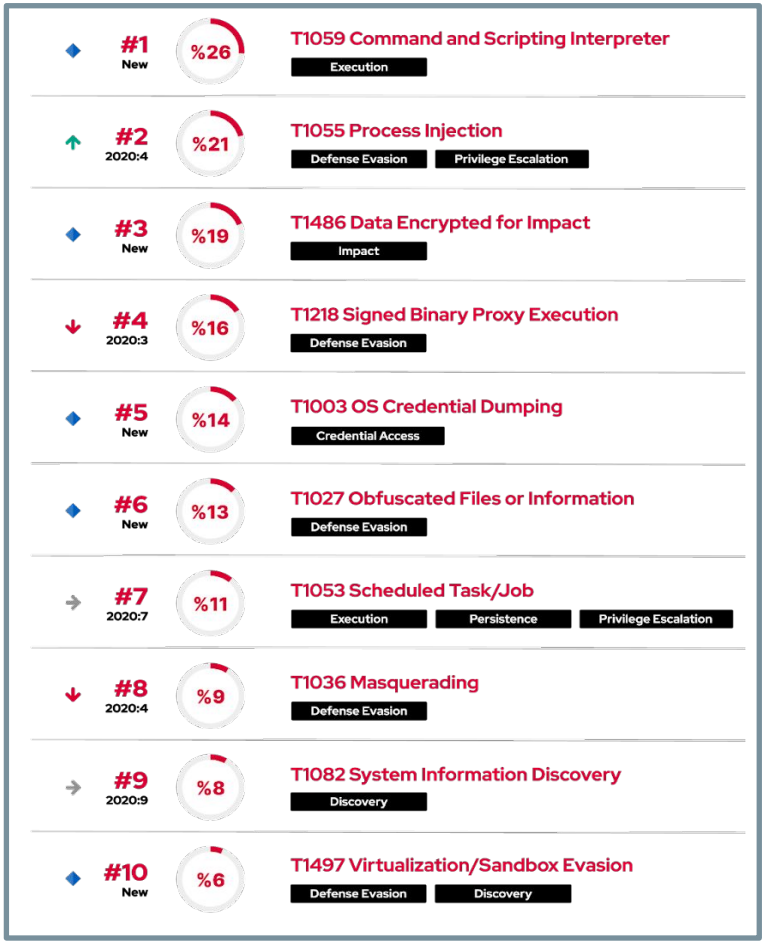
Trends in Adversary TTPs

Data encryption is more common.

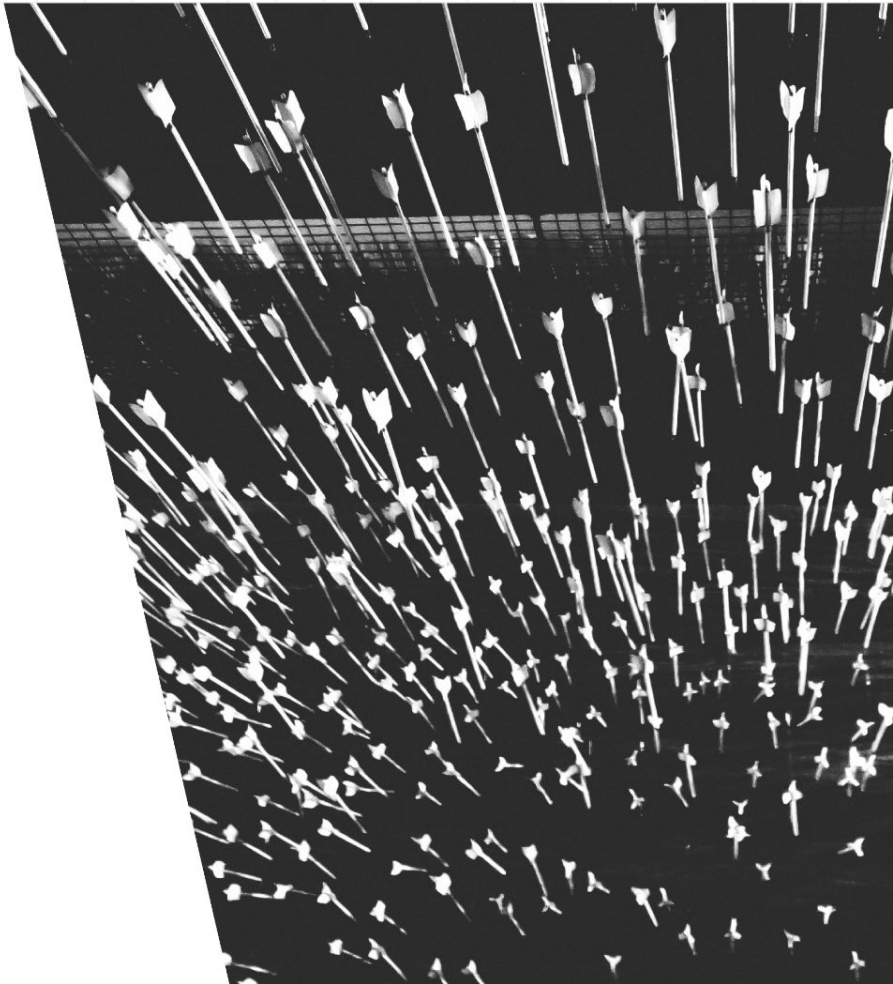
Malware is increasingly sophisticated.

Defense evasion is the most common tactic.

Adversaries prefer to abuse built-in tools.



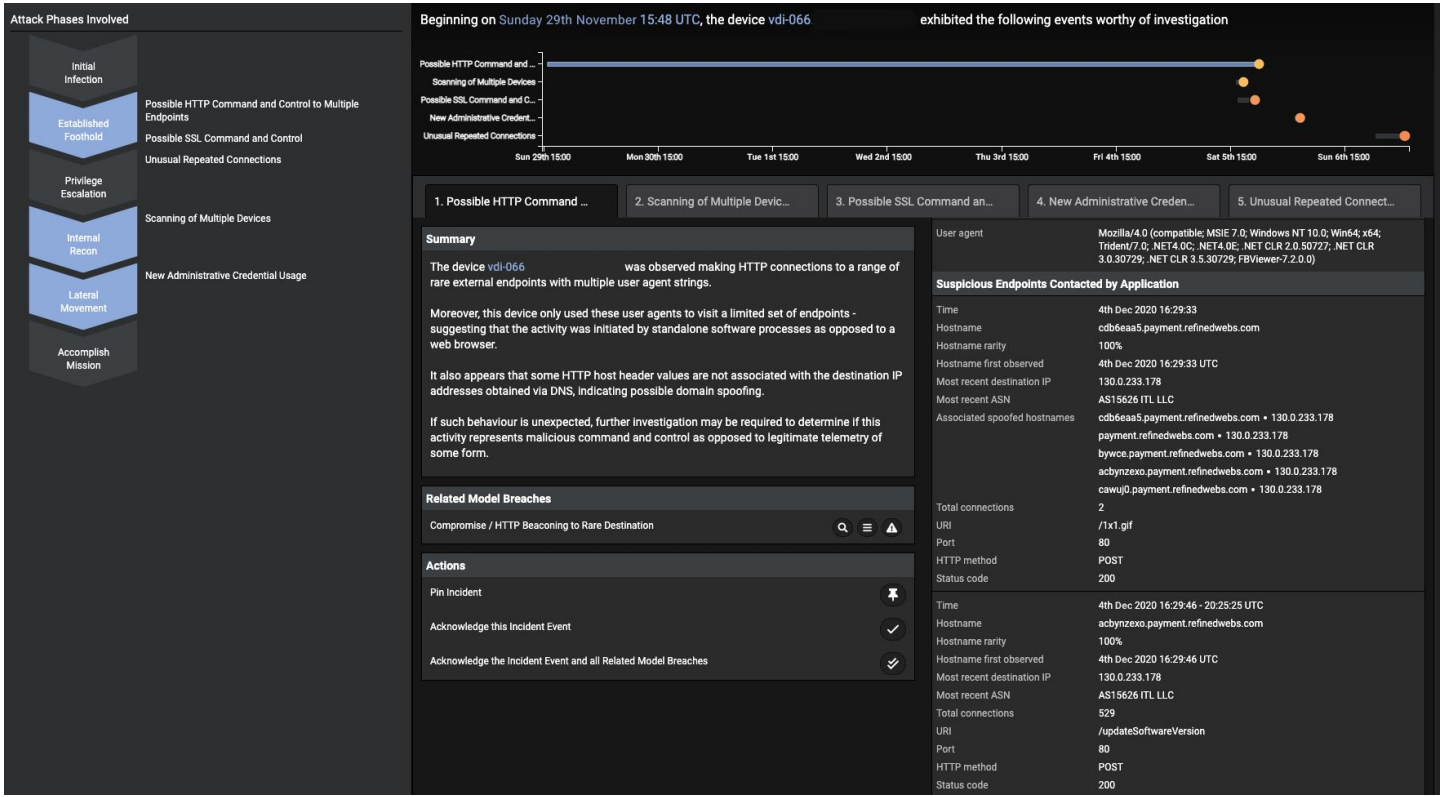
Real-Life Threat Stories



Targeted Ransomware

- ‘WastedLocker’ – Russian Nation-State Actor
- Detected during Proof of Value
- New Malware
- Living-Off-The-Land
- Double-Threat
- US Agricultural Organisation

Attack Overview



Exchange Zero-Days

- ‘Hafnium’ – Chinese State-Sponsored Attacker
- 4 Zero Days – ‘ProxyLogon’
- Protected Against 3 Months Before Public Attribution
- Likely Espionage Campaign
- Targeting Asian Key Infrastructure Organisation
- No Damage Done

Attack Overview

1. Initial Compromise
Possible Exchange vulnerabilities exploited; web shell deployed

3. Lateral Movement
Deploying further web shells on more mail servers via internal SMB

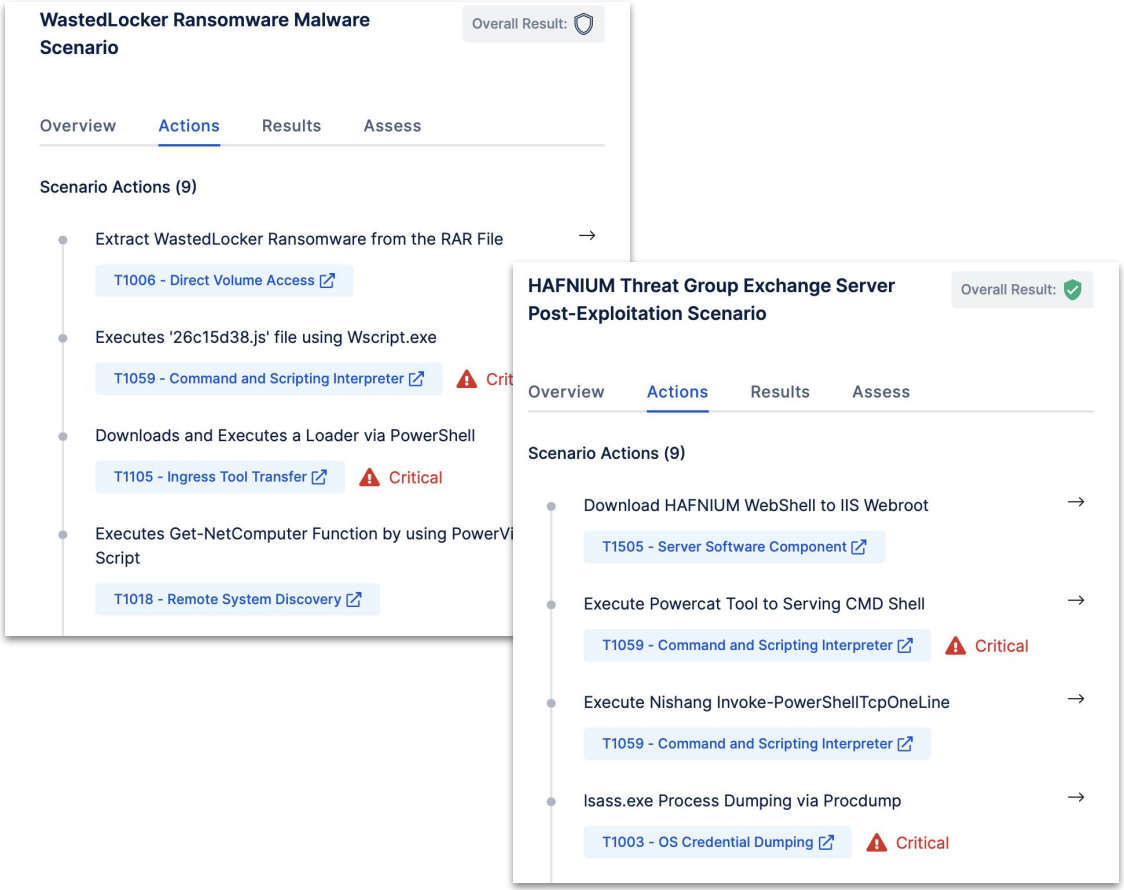
2. Internal Reconnaissance
Targeted network scan on four key ports

4. Further Lateral Movement
Deploying malicious .exe files to Domain Controller via SMB

Picus Threat Library

11000+ Threats

- Adversary Emulation Playbooks
- Atomic Attacks
- Malware Attacks
- Vulnerability Exploitation Attacks
- Web Application Attacks
- Email Attacks
- Data Exfiltration Attacks



Takeaways

Threats are Fast and Furious – Aggressive defensive automation required

- Automate big and small
- Leverage recent technology
- Use open source / crowdsourcing

Attacks Against Cloud - Familiarize your SOC with Cloud Security

- What does 'cloud' mean in security terms?
- Don't just prevent – detect and respond
- Upskill – what does a SaaS attack look like

Mid-game Hunting - Monitoring is not a nice to have, but a must today

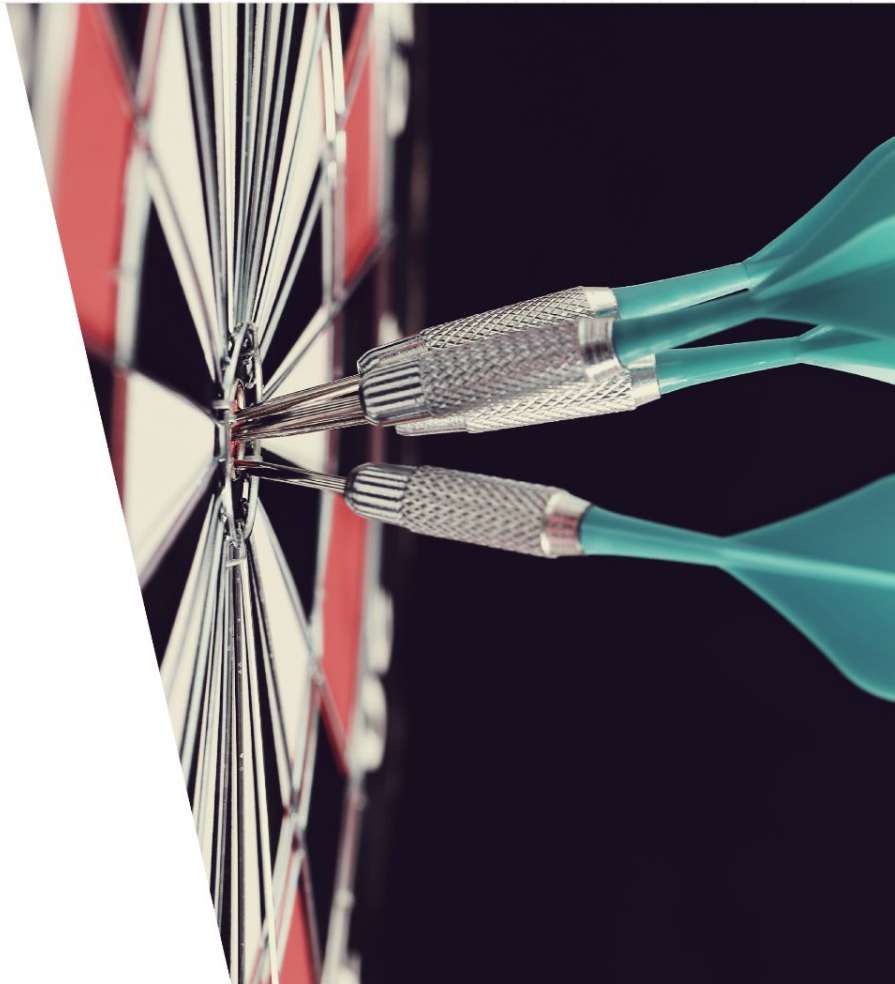
- Work in quick iterations, tangible successes (not the '24-month monolithic approach')
- Seek clever solutions – MSP, tech with heavy-automation, smart hiring

Breaches Happen – Prepare, drill, simulate

- Table-top / boardroom exercise / technology-driven / scenario-based / ...

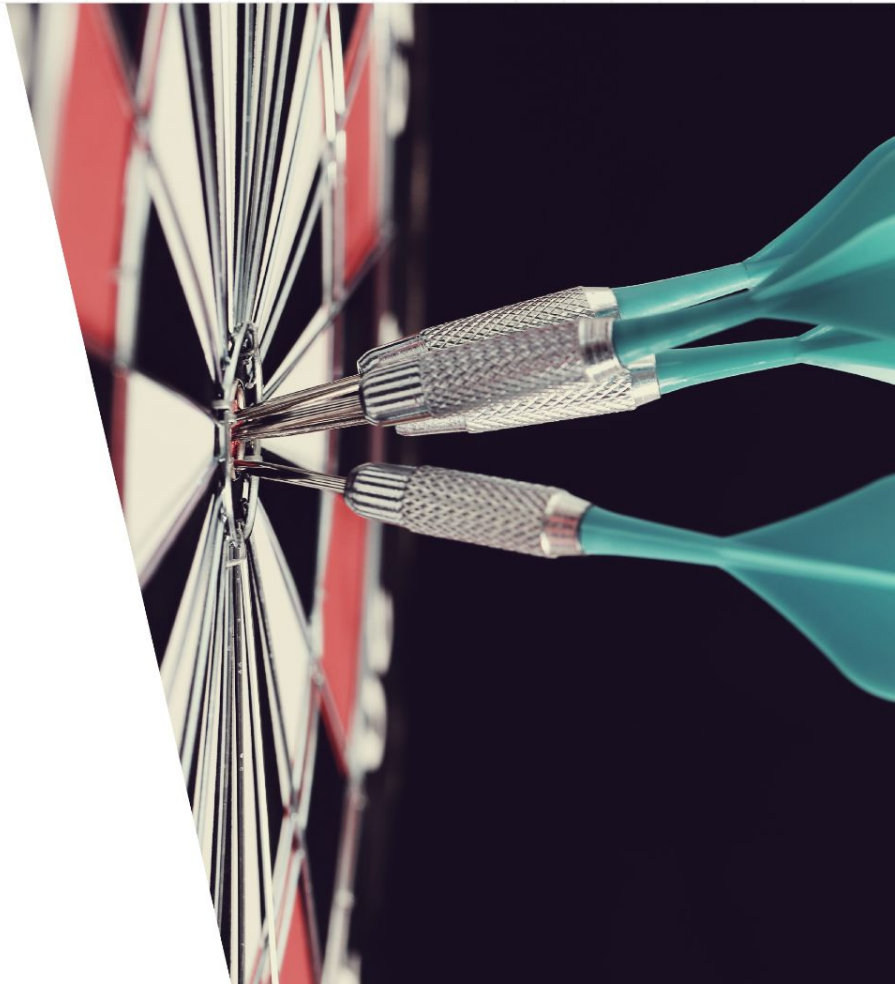
Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
  - **Focus on TTPs rather than IOCs.**
  - Leverage behaviour-based detection
  - Prioritise telemetry sources
  - Operationalize MITRE ATT&CK



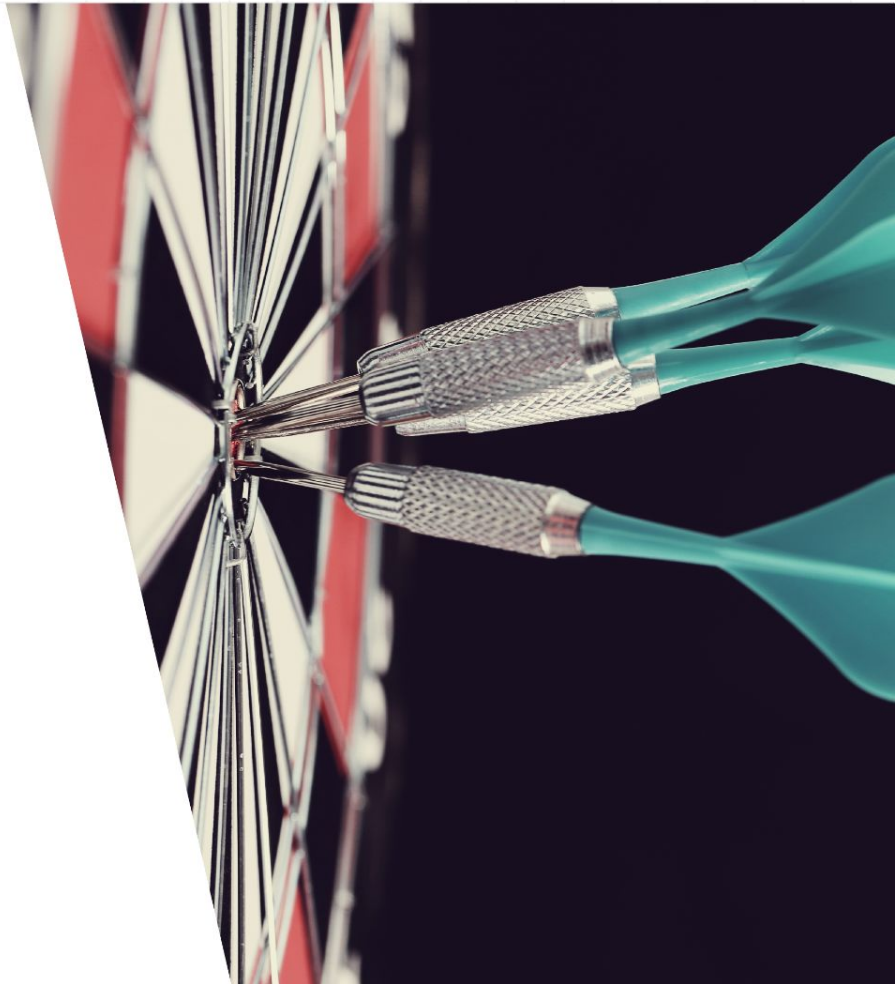
Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
  - Focus on TTPs rather than IOCs.
  - **Leverage behaviour-based detection**
  - Prioritise telemetry sources
  - Operationalize MITRE ATT&CK



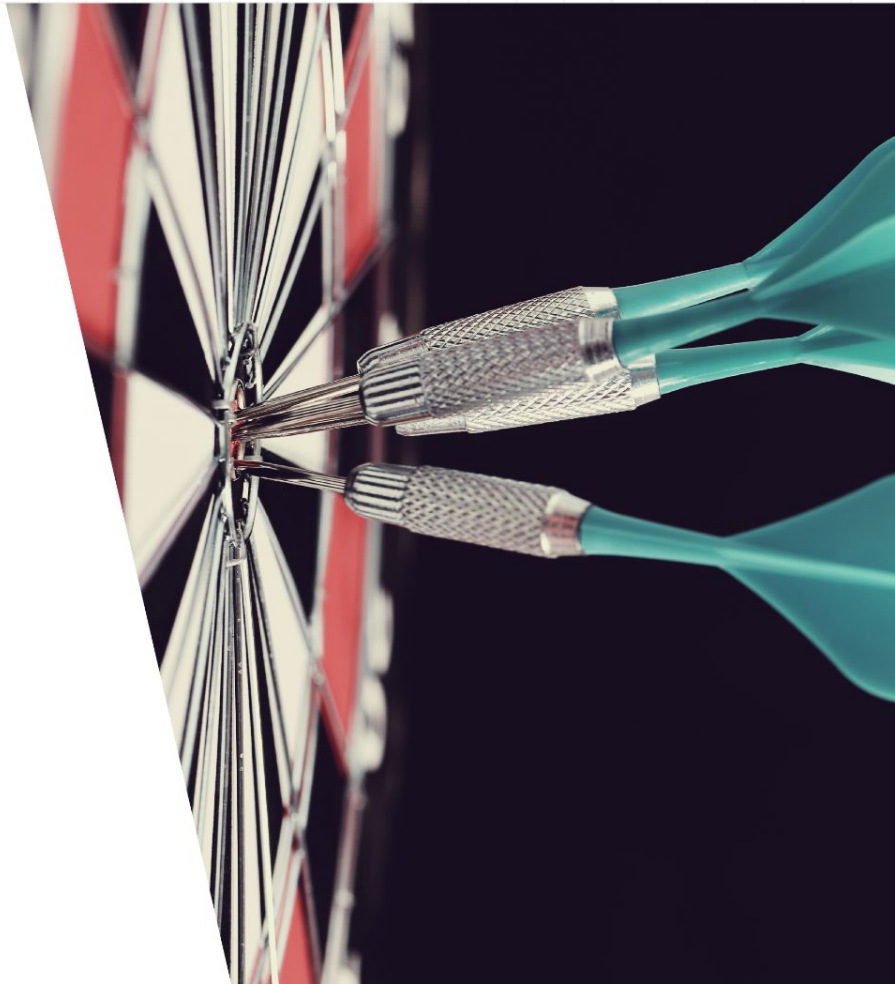
Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
  - Focus on TTPs rather than IOCs.
  - Leverage behaviour-based detection
  - **Prioritise telemetry sources**
  - Operationalize MITRE ATT&CK



Key Takeaways for SOCs from Red Report Research

- **Leverage the threat-centric approach**
  - Focus on TTPs rather than IOCs.
  - Leverage behaviour-based detection
  - Prioritise telemetry sources
  - **Operationalize MITRE ATT&CK**



THANK YOU!