SOPHOS

Evaluation Brief

2024 MITRE ATT&CK® Evaluations: Enterprise

Sophos excels in the 2024 MITRE ATT&CK® Evaluations: Enterprise

MITRE ATT&CK® Evaluations help organizations better understand how effectively EDR and XDR solutions can protect against sophisticated, multi-stage attacks.

In the latest evaluation, Sophos XDR achieved:

- The highest possible ('Technique') ratings for **100%** of adversary activities (sub-steps) in the Windows and Linux ransomware scenarios
- The highest possible ('Technique') ratings for **78 out of 80** total sub-steps across three comprehensive attack scenarios
- 'Analytic coverage' ratings for **79 out of 80** total sub-steps **(99%)**

MITRE ATT&CK® Evaluations: Enterprise (Round 6)

MITRE ATT&CK® Evaluations are among the world's most respected independent security tests. They emulate the tactics, techniques, and procedures (TTPs) leveraged by real-world adversarial groups and evaluate each participating vendor's ability to detect, analyze, and describe threats, with output aligned to the language and structure of the MITRE ATT&CK® Framework.

Round 6 focused on behaviors inspired by three known threat groups:

- **Democratic People's Republic of Korea (DPRK)**
  The evaluation emulated DPRK's adversary behaviors targeting macOS via multi-stage operations, including elevating privileges and credential theft.
- **Ransomware (CL0P and LockBit)**
  The evaluation emulated behaviors prevalent across campaigns using CL0P and LockBit ransomware, including abusing legitimate tools and disabling critical services.

Evaluation results

Sophos achieved full 'technique' level coverage — the highest possible rating — for 78 out of 80 adversary activities (sub-steps) across three comprehensive attack scenarios.

Attack scenario:
CLOP Ransomware

100%

Full 'technique' level coverage for 19 out of 19 sub-steps

Attack scenario:
LockBit Ransomware

100%

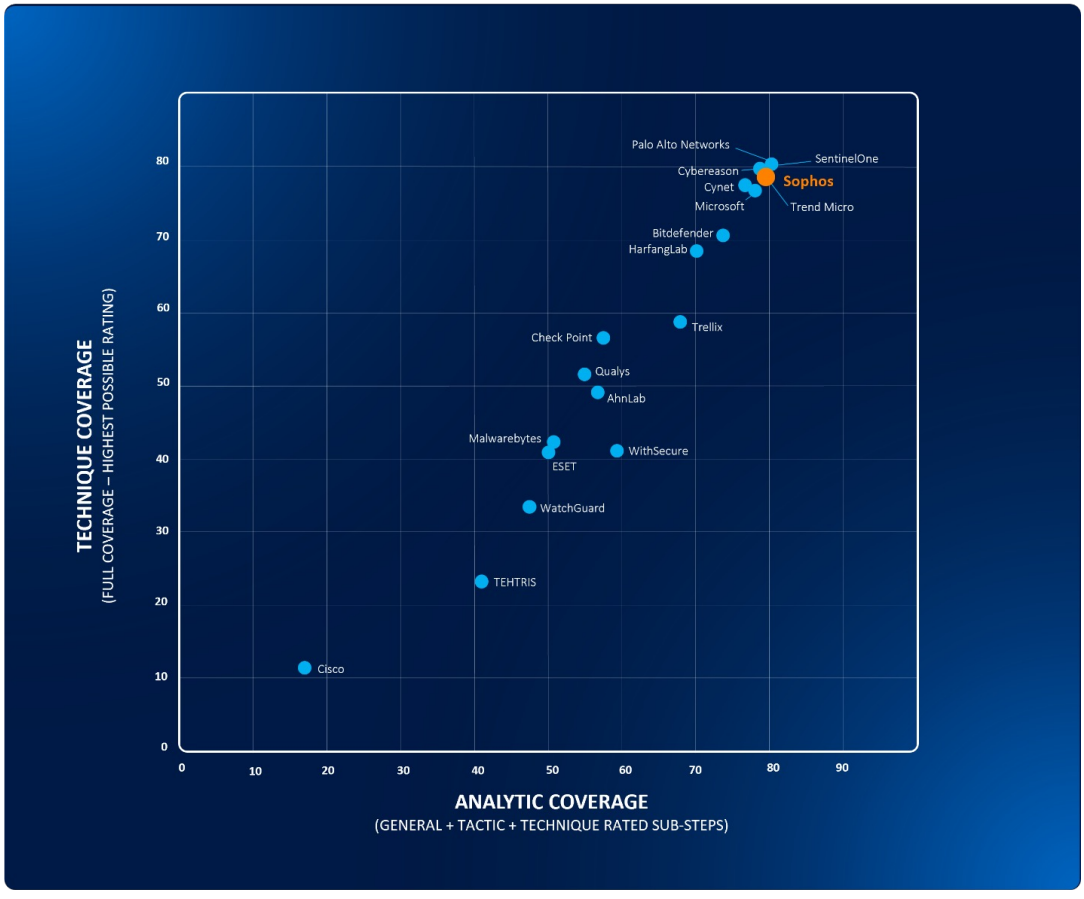
Full 'technique' level coverage for 40 out of 40 sub-steps

Attack scenario:
DPRK (macOS)

95%

Rich 'analytic' coverage for 20 out of 21 sub-steps

Detection quality is critical for providing security analysts with the information to investigate and respond quickly and efficiently. The chart below compares the number of sub-steps that generated a detection providing rich detail on the adversarial behaviors (analytic coverage) and the number of sub-steps that achieved full 'technique' level coverage, for each participating vendor.

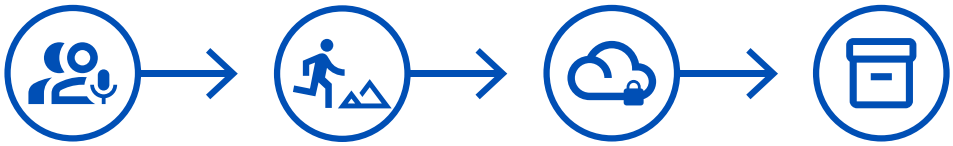


MITRE does not rank or rate participants of ATT&CK Evaluations.

Evaluation attack scenarios

The evaluation comprised 80 adversary events (sub-steps) across three attack scenarios.

Attack scenario 1: DPRK (macOS)



Step 1: **Command and Control**

Step 2: **Persistence**

Step 3: **Defence Evasion**

Step 4: **Collection**

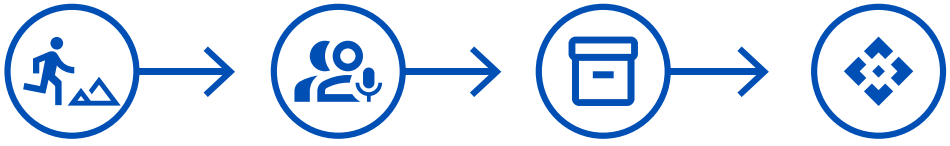
North Korea has emerged as a formidable cyber threat, and by expanding its focus to macOS, they have gained the ability to target and infiltrate additional high-value systems. In this attack scenario, the MITRE team used a backdoor from a supply chain attack, followed by persistence, discovery, and credential access, resulting in the collection and exfiltration of system information and macOS keychain files.

4 steps | 21 sub-steps | macOS only

Sophos XDR detected and provided rich 'analytic' coverage for 20 out of 21 (95%[1]) sub-steps in this scenario

19 sub-steps were assigned 'technique' level categorization — the highest possible rating

Attack scenario 2: CL0P Ransomware (Windows)



Step 5: **Establish Persistence**

Step 6: **Command and Control**

Step 7: **Discovery and Exfiltration**

Step 8: **Defence Evasion and Impact**

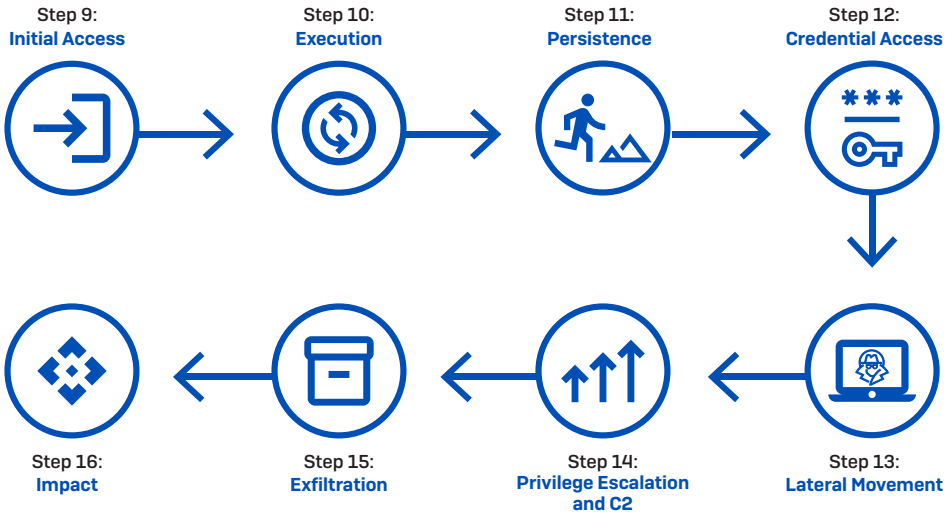
Active since at least 2019, CL0P is a ransomware family affiliated with the TA505 cyber-criminal threat actor (also known as Snakefly) and is widely believed to be operated by Russian-speaking groups. In this attack scenario, the MITRE team used evasion techniques, persistence, and an in-memory payload to perform discovery and exfiltration before executing ransomware.

4 steps | 19 sub-steps | Windows only

Sophos XDR detected and provided full 'technique' level coverage of 100% of sub-steps

[1]*Sophos XDR generated alerts for all 80 adversary activities (sub-steps) in the evaluation and achieved an 'analytic coverage' rating for 79 out of 80 sub-steps. The alert generated for one sub-step in the DPRK (macOS) attack scenario did not rise to an 'analytic coverage' detection level based MITRE's detection category definitions.*

Attack scenario 3: LockBit Ransomware (Windows and Linux)



Operating on a Ransomware-as-a-Service (RaaS) basis, LockBit is a notorious ransomware variant that has gained infamy for its sophisticated tools, extortion methods, and high-severity attacks. In this attack scenario, the MITRE team gained access using compromised credentials, ultimately deploying an exfiltration tool and ransomware to stop virtual machines and exfiltrate and encrypt files.

8 steps | 40 sub-steps | Windows and Linux

Sophos XDR detected and provided full 'technique' level coverage of 100% of sub-steps

Why we participate in MITRE ATT&CK® Evaluations

MITRE ATT&CK® Evaluations are among the world's most respected independent security tests. Sophos is committed to participating in these evaluations alongside some of the best security vendors in the industry. As a community, we are united against a common enemy. These evaluations help make us better, individually and collectively, for the benefit of the organizations we defend.

19 EDR/XDR security vendors participated in this evaluation:

To explore the full results for this evaluation, visit the MITRE website:
https://attackevals.mitre-engenuity.org/results/enterprise/

A market leader in detection and response solutions

Sophos is an established leader in extended detection and response (XDR), with industry recognition to back it up.

Sophos is a 2024 Gartner® Peer Insights™ Customers' Choice for Endpoint Protection and Managed Detection and Response

Gartner

Sophos is a Leader in the 2024 Gartner Magic Quadrant for Endpoint Protection Platforms for the 15th consecutive time

Leader

Sophos is the only vendor named a Leader for Endpoint, Firewall, MDR, XDR and EDR in the Fall 2024 Grid Reports from G2

SE Labs

Sophos consistently achieves industry leading protection results in independent tests

MITRE ENGENUITY | ATT&CK® Evaluations

Sophos is a strong performer in MITRE ATT&CK Evaluations

Try Sophos XDR for free

Register for a free 30-day trial
at sophos.com/xdr

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2024-12-10 EN (PS)

SOPHOS