MITRE Engenuity ATT&CK Evaluations : Quick Guide

Wizard Spider & Sandworm Evaluation Results

Date: Evaluation results published March 31st, 2022

ABOUT MITRE ATT&CK

MITRE ATT&CK is a public knowledgebase of adversarial tactics and techniques, which can be used as a foundation for the development of specific cyber threat models and methodologies.

In short, it helps the industry define and standardize how to describe an attacker's approach. MITRE ATT&CK collects and categorizes common attack tactics, techniques, and procedures (TTPs), then organizes this information into a framework. This framework can be used to help explain how adversaries behave, what they are trying to do, and how they are trying to do it.

Having a common language and framework is important in the ability to communicate, understand, and respond to threats as efficiently and effectively as possible.

Executive Summary - Highlights of Trend Micro's results from the MITRE Engenuity ATT&CK Evaluation

This year's strong performance in MITRE Engenuity's ATT&CK Evaluation is the third in a row for Trend Micro

Trend Micro Vision One recorded the following impressive results:

- **100% detection of all 19 attack steps in the evaluation -** Highly enriched telemetry for better investigations.
- **Provided clear visibility of 105 out of 109 attack methods providing 96.33% coverage -** This broad visibility allows customers to have a clear picture of the attack and respond faster.
- **Ranked # 1 this year in the protection category –** Ensuring that attacks are prevented early in the attack lifecycle.
- **#1 performer in Linux, with 100% of attacks against the Linux host detected and prevented,** capturing attacker steps and preventing a simulated attack, which is especially important considering Linux is the most used OS in cloud-native applications.

Evaluation summary high level results for Trend Micro

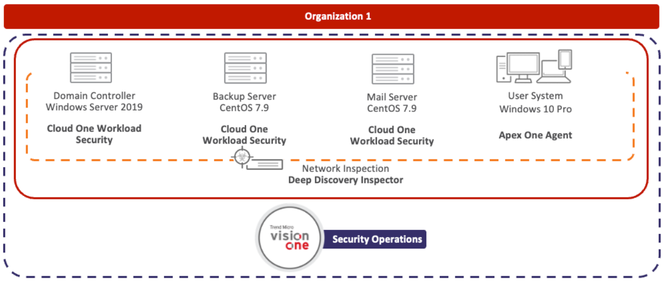
What are substeps? *These are the individual attacker tests carried out as part of the emulation – in total there were 109 across both simulations*

Analytic Coverage	Visibility	Protection
100 of 109 substeps	**105 of 109** substeps	**100%** Prevention
These are **enriched detections** that add context by adding ATT&CK technique mappings or alert descriptions.	Attacker visibility allows customers to **build a clear picture of the attack** and respond faster. This shows where analytic or telemetry information was available.	Deflecting risk early on frees up investigation resources, allowing teams to focus on the harder security problems to solve..
USEFUL DATA FOR **SOC Level 1 Analyst** - Triage	**USEFUL DATA FOR** **SOC Level 2 / 3 Analyst -** Hunters / Incident responder	**USEFUL FOR** **Defenders & Security Teams -** measuring defensive capabilities

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Trend Micro Solutions included in the evaluation

Attack Evaluation – Day 1 – Wizard Spider



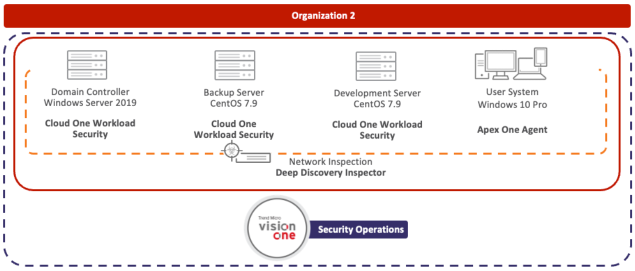
Day 1 Scenario

Emulated Group: Wizard Spider

Background: Russian-speaking cyber criminal gang associated with “big game hunting”

Scenario: Ransomware attack against a notional organization using malware (Emotet, TrickBot, Ryuk) associated with Wizard Spider campaigns

Attack Evaluation – Day 2 - Sandworm



Day 2 Scenario

Emulated Group: Sandworm Team (G0034)

Background: Destructive threat group attributed to Russian GRU

Scenario: Compromise of a notional organization with the goal of destroying data using malware (P.A.S. Webshell, Exaramel, NotPetya) associated with the Sandworm Team

Trend Micro Results

How the evaluation works:

The MITRE Engenuity ATT&CK Evaluation offers transparency to customers and real-world attack scenarios. This ensures that customers can actively evaluate security products to protect themselves from the latest advances from attackers based on their areas of greatest need.

The evaluation uses adversary emulation to ensure customers can address today’s threats. Using techniques, tools, methods and goals inspired by that of an attacker.

The simulations are executed in a controlled lab environment to ensure fair and accurate testing. Attacker techniques are then used in logical step-by-step in order to explore the breadth of ATT&CK coverage. Over the two scenarios 109 attacker steps were executed.

The evaluation this year emulated Wizard Spider and Sandworm tradecraft operational flows to simulate attacks similar to the behavior used in the wild by these groups.

After the simulation has been run, results are processed and publicly released, including the methodology.

How is the Evaluation scored?

MITRE ATT&CK does not score or rank the evaluation against other vendors. However the “Evaluation Summary” can be used to explore a variety of metrics on the underlying data from each participant.

This is something we have aligned to in this report and compared these to other vendors. The results are available directly from the website in full transparency for customers to also do self analysis in evaluating how to best protect themselves.

Additional Resources :

Trend Micro Public Results

Configuration Summary

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Trend Micro Results:

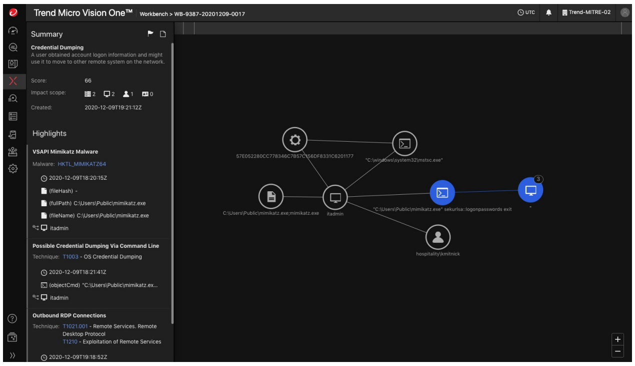
Vendor	Attack Steps	Analytic		Visibility		Visibility Rank	Protection Score
cybereason	109	108	99.08%	109	100%	1	100%
SentinelOne	109	108	99.08%	108	99.08%	2	100%
PaloAlto Networks	109	107	98.17%	107	98.17%	3	100%
Cynet	109	102	93.58%	107	98.17%	3	100%
McAfee	109	84	77.06%	107	98.17%	3	75%
Bitdefender	109	106	97.25%	106	97.25%	4	------------
Trend Micro	109	100	91.74%	**105**	**96.33%**	**5**	**100%**
CrowdStrike	109	94	86.24%	105	96.33%	5	100%
Check Point	109	103	94.50%	103	94.50%	6	77%
Microsoft	109	98	89.91%	98	89.91%	7	100%
elastic	109	71	65.14%	98	89.91%	7	------------
Fidelis	109	85	77.98%	94	86.24%	8	------------
Symantec	109	87	79.82%	92	84.40%	9	66%
Uptycs	109	81	74.31%	92	84.40%	9	11%
Cisco	109	74	67.89%	90	82.57%	10	77%
vmware	109	57	52.29%	90	82.57%	10	100%
fireeye	109	85	77.98%	89	81.65%	11	75%
Cylance	109	71	65.14%	89	81.65%	11	100%
Sophos	109	67	61.47%	88	80.73%	12	50%
FORTINET	90	85	94.44%	87	96.67%	13	100%
Malwarebytes	90	83	92.22%	83	92.22%	14	100%
AhnLab	90	59	65.56%	83	92.22%	14	62%
f-secure	109	66	60.55%	83	76.15%	15	------------
cycraft	109	64	58.72%	77	70.64%	16	44%
eset	90	69	76.67%	75	83.33%	17	37%
REAQTA	90	62	68.89%	71	78.89%	18	------------
somma	90	28	31.11%	68	75.56%	19	------------
Qualys	90	50	55.56%	66	73.33%	20	------------
Deepinstinct	90	59	65.56%	63	70.00%	21	100%
Rapid7	109	23	21.10%	62	56.88%	22	------------

Creating a story of an attack with Trend Micro Vision One

Trend Micro Vision One allows you to provide a complete story of the attack.

Automatically correlating threat data from different areas of the endpoint, server and network provides better alerts to security teams.

We don't just tell you these individual events have all occurred – we connect the dots for you, showing that they might be related and have similar indicators of compromise as a certain attack group or type.



Trend Micro Vision One™ Workbench > WB-9387-20201209-0017

Summary

Credential Dumping

A user obtained account logon information and might use it to move to other remote system on the network.

Score: 66

Impact scope: 2 2 1 0

Created: 2020-12-09T19:21:12Z

Highlights

VSAPI Mimikatz Malware

Malware: HKTL_MIMIKATZ64

2020-12-09T18:20:15Z

(fileHash) -

(fullPath) C:\Users\Public\mimikatz.exe

(fileName) C:\Users\Public\mimikatz.exe

itadmin

Possible Credential Dumping Via Command Line

Technique: T1003 - OS Credential Dumping

2020-12-09T18:21:41Z

(objectCmd) "C:\Users\Public\mimikatz.ex...

itadmin

Outbound RDP Connections

Technique: T1021.001 - Remote Services. Remote Desktop Protocol
T1210 - Exploitation of Remote Services

2020-12-09T19:18:52Z

UTC
Trend-MITRE-02
57E052280CC778346C7B57C156DF8331C6201177
"C:\windows\system32\mstsc.exe"
C:\Users\Public\mimikatz.exe;mimikatz.exe
itadmin
"C:\Users\Public\mimikatz.exe" sekurlsa::logonpasswords exit
3
hospitality\kmitnick

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Want to understand more about the ATT&CK Framework?

MITRE ATT&CK Framework

This type of framework is extremely useful to information security professionals helping to keep them updated on new attack techniques and to prevent attacks from happening in the first place.

Why are Organizations using ATT&CK Framework?

Organizations use ATT&CK to standardize community conversations, defense testing, and product/service evaluations.

MITRE ATT&CK Evaluation

The evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, they show how each vendor approaches threat detection in the context of the ATT&CK knowledge base.

Why are Organizations using ATT&CK Evaluations

ATT&CK Evaluations provide vendors with an assessment of their ability to defend against specific adversary tactics and techniques.

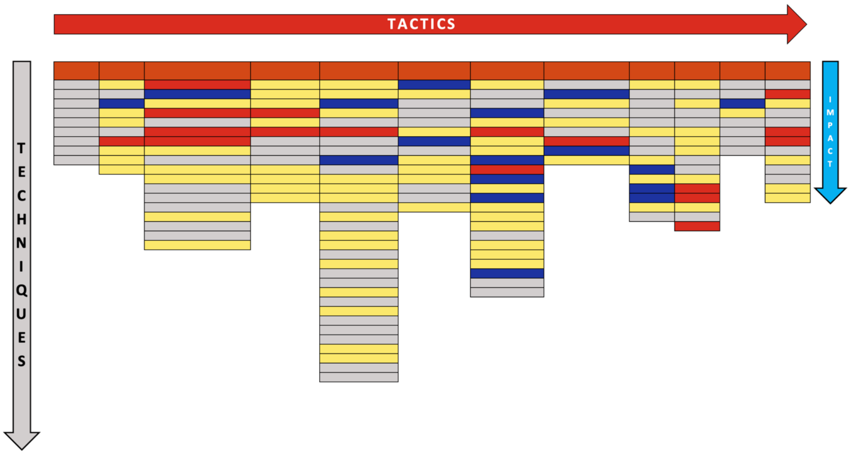
Anatomy of MITRE ATT&CK Framework

TACTICS are the description of what attackers are trying to achieve.

Tactics are similar to a chapter of a book. A CISO can outline a story they want to tell with the high level tactics used in an attack and then refer to the techniques to tell the story of how they accomplished the attack which provides extra detail.

TECHNIQUES

The are are how attackers accomplish those steps or goals.



IMPACT

Used by adversaries to follow through on their end goal or to provide cover.

Playbooks should be in place to defend against these.

Example Story : Building an attack story in a common language

The goal of the attacker was to gain initial access to the network. Using a drive-by compromise with a spear-phishing link and trusted relationship, the attacker gained initial access using this technique. ***Note : The framework lists all the known ways that an attacker can gain initial access.***

How does Trend Micro help?

Trend Micro maps our products to the ATT&CK Framework, showing tactics and technique on detections which demonstrates how we can can help you address the challenges of detecting and responding to threats.

What about prevention?

Preventative controls are an important part of a threat mitigations strategy which add resilience when under attack. Preventative controls were tested in the latest round with the ability to deflect risk early on allowing organizations to spend more time on harder security problems.

Learn More

https://resources.trendmicro.com/MITRE-Attack-Evaluations.html

MITRE ATT&CK vs Cyber Kill Chain

MITRE ATT&CK is designed to provide a deeper level of granularity in describing what can occur during an attack which is step forward from the Cyber Kill Chain.

MITRE ATT&CK	CYBER KILL CHAIN
Initial Access	Reconnaissance
Execution	Intrusion
Persistence	Exploitation
Privilege Escalation	Privilege Execution
Defense Evasion	Lateral Movement
Credential Access	Obfuscations / Anti Forensics
Discovery	Denial of Service
Lateral Movement	Exfiltration
Collection	
Command and Control	
Exfiltration	
Impact	