A Trend Micro Report | **January 2022**

Trend Micro Service One: Targeted Attack Detection

Proactive detection and response

YOU CAN HAVE IT ALL

The threat landscape is constantly evolving. Now, threat actors can infiltrate their target with a variety of approaches using advanced techniques and legitimate tools. They are no longer limited to traditional phishing, compromising a remote desktop protocol (RDP) account, exposing a vulnerability on a server, etc. The rise of new techniques and tactics mean that customers need enhanced security monitoring so they can detect a possible attack before it causes business disruptions.

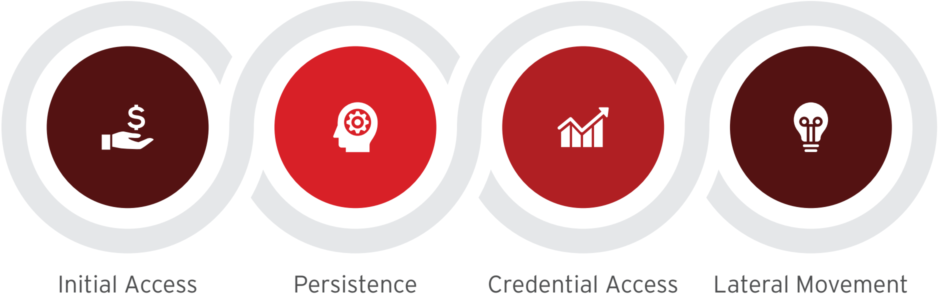
- Out of 3,239 eligible TAD customers, only 237 have received high/medium alerts.
- On average, there are 2.7 at-risk endpoints per high/medium alert.

TARGETED ATTACK DETECTION

By leveraging our industry-leading threat research and the Trend Micro™ Smart Protection Network™, Targeted Attack Detection (TAD) uses a comprehensive, holistic, and machine-learning augmented approach to identify notable attacks, providing qualified, high-risk alerts and remediation guidance. This 24/7/365 service will specify if any indicators of attack (IoA) were found, and which customer assets were affected. In addition, you'll receive recommended actions based on the threat actor's predicted next moves.

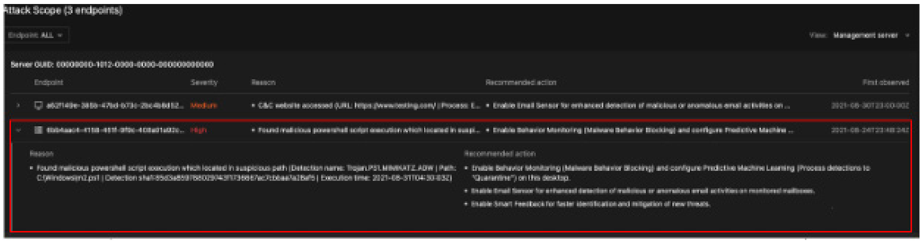
LESS, BUT MORE HIGH-QUALITY ALERTS

Security teams that are bombarded by a large amount of frequent alerts can cause a delay in response time or for an attack to be missed altogether. TAD helps you avoid alert fatigue by only sending alerts for verified threats. This is achieved by analyzing the detection and query logs communicated by Trend Micro™ Smart Feedback to the Smart Protection Network. Through constant analysis, TAD can identify notable indicators of compromise (IoC) and categorize an indicator into attack phases, generating a timeline of events for an incident and identifying any affected assets like endpoints, servers, network devices, and more. It also determines the risk and progress level of an attack, saving teams precious time and enabling a targeted response.



The four attack phases covered by TAD

This use case will demonstrate how TAD and Smart Protection Network work in tandem to detect attacks. Figure 1 is a detection log of a malicious PowerShell script on a Microsoft Windows server. The log also provides a record of the time it occurs, filename and file full path of the malware file, detection name, affected client ID, file SHA1 hash, and a host of other useful data.



Attack Scope (3 endpoints)

Endpoint: ALL ▾ View: Management server ▾

Server GUID: 00000000-1012-0000-0000-000000000000

	Endpoint	Severity	Reason	Recommended action	First observed
›	a62f149e-385b-479d-b73c-2bc4b8d52...	Medium	• C&C website accessed (URL: https://www.testing.com/ | Process: E...	• Enable Email Sensor for enhanced detection of malicious or anomalous email activities on ...	2021-08-30T23:00:00Z
⌄	6bb4aac4-4158-481f-8f0c-408a01a02c...	High	• Found malicious powershell script execution which located in suspi...	• Enable Behavior Monitoring (Malware Behavior Blocking) and configure Predictive Machine ...	2021-08-24T23:48:24Z

Reason

- Found malicious powershell script execution which located in suspicious path [Detection name: Trojan.PS1.MIMIKATZ.ADW | Path: C:\Windows\m2.ps1 | Detection sha1:85d3a8597b8029743f1736667ac7cbbaa1a2baf5 | Execution time: 2021-08-31T04:30:03Z]

Recommended action

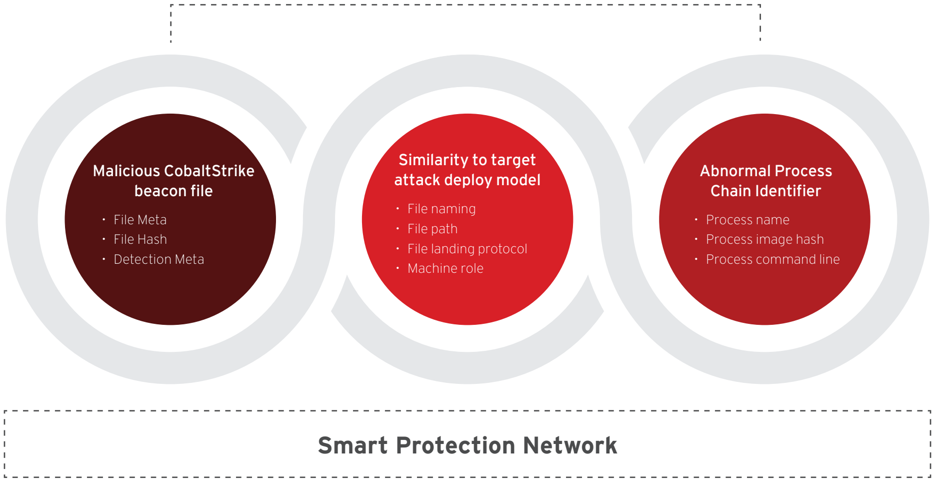
- Enable Behavior Monitoring (Malware Behavior Blocking) and configure Predictive Machine Learning (Process detections to "Quarantine") on this desktop.
- Enable Email Sensor for enhanced detection of malicious or anomalous email activities on monitored mailboxes.
- Enable Smart Feedback for faster identification and mitigation of new threats.

TAD analysis a malicious Powershell script file landing.

After automatically analyzing the detection log, TAD will determine it is a noteworthy IoC, but there is not enough evidence to indicate it is an active attack that customer needs to be aware of and therefore, no alert is sent.

Later, Smart Protection Network receives another data log indicating a detection of a CobaltStrike beacon on a different Windows server machine within the customer's network. TAD identifies this as another noteworthy IoC and determines that the attack progressed further.

TAD : Noteworthy lateral movement event trigger via a malicious CobaltStrike beacon detection log



Malicious CobaltStrike beacon file

- File Meta
- File Hash
- Detection Meta

Similarity to target attack deploy model

- File naming
- File path
- File landing protocol
- Machine role

Abnormal Process Chain Identifier

- Process name
- Process image hash
- Process command line

Smart Protection Network

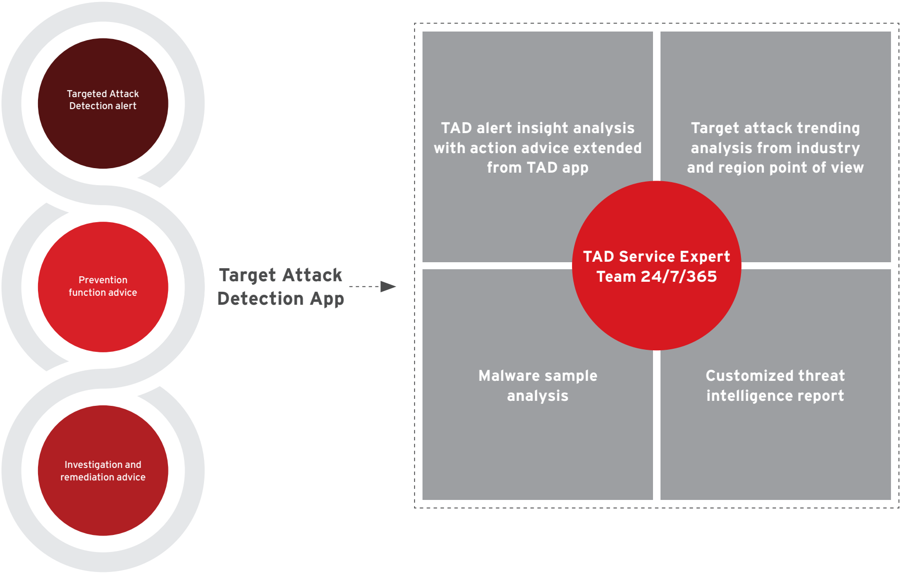
TAD analysis of a CobaltStrike beacon detection log.

An alert is sent to the customer, notifying them of the attack and that it is on the lateral movement phase now. The alert from TAD also provides a prediction that it will lead to a serious ransomware attack. To prevent similar attacks from occurring in the future, TAD will continuously analyze and consolidate other related data, like any communication the attacker's command and control (C&C) site, from the same server or other endpoints within the customer's network.

Initial Access	Persistance	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact and Exfiltration
Insecure RDP	Registry AutoRuns	Domain/ Local Admin Compromise	4 Termination of Security Softwares	5 Mimikatz	Arp, Net, NsLookup	7 Cobalt Strike	Ransomware Encryption
BazaarLoader, Qakbot, etc.	2 Powershell / WMI Scripts	3 Create new Admin Account	Disable System Firewall	Lazagne	Sharphound, Bloodhound, NLBrute	PowerShell Empire	Data Exfiltration
1 External Applications Vulnerability	Scheduled Tasks	Fileless UAC bypass	Hide in ADS	PwDump	6 AdFind	Psexec	
Spear Phishing	Logon Scripts						

GAME OVER

Actual attack chain from initial access to the end


Targeted Attack Detection alert
Prevention function advice
Investigation and remediation advice
Target Attack Detection App
TAD alert insight analysis with action advice extended from TAD app
Target attack trending analysis from industry and region point of view
TAD Service Expert Team 24/7/365
Malware sample analysis
Customized threat intelligence report

TAD Service Expert Team alerts users of the attack and provides threat remediation guidance and customized threat intelligence.

TAD provides customers with an early warning of an impending target attack as well as threat remediation guidance from threat experts. By leveraging internal and external threat intelligence reports, threat intelligence feeds, and/or malware analysis, our threat experts help the user understand how to eliminate the ongoing attack.

SUMMARY

TAD is available for both tiers of Trend Micro Service One. By providing qualified, high-risk alerts and a detailed action plan, TAD extends your security team, providing more proactive prevention, detection, and response across your entire infrastructure/

With insight into the movement of an attack, TAD provides security teams with essential and precious threat response.

Prevention function optimization:

- To reduce further risks, TAD leverages alert context to suggest corresponding prevention function implementation. For example, if TAD finds that company users continuous clicking a malicious email attachment, it will recommend deploying the email pre-filter with attachment detonate capability.

Investigation and remediation

- To help limit the scope of an attack, especially for those in the late stages, TAD will determine the “hot zone” and guide users to deploy XDR sensors for further investigation of the attacker’s footprints. This will also validate if the threat is eliminated.

Securing Your Connected World

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1408.257.2003