Let’s go

cisco The bridge to possible

The Power of Predictive Attack Analysis in an Offensive-Defensive nexus

Rami Haddad, Product Engineer

cisco Live!

BRKETI-2161

Rami Haddad

- ˜4 years with Cisco
- OutShift
- SRE background
- Amsterdam

Agenda

- Evolving Security Landscape
- Threat Hunting
- Towards Attack Prediction
- Cisco’s activity

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Evolving Security Landscape

Evolving Security Landscape (SoC view)

Availability Monitoring

Network Alerts

NOC

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Evolving Security Landscape (SoC view)

Availability Monitoring	Reactive Monitoring		Proactive Montioring	Automation
Network Alerts NOC	IDS Firewall Antivirus	IPS DPI AntiSpam SIEM	DLP PII detection APT OSINT/TIP	SOAR XDR

Mid
90s

Early
2000s

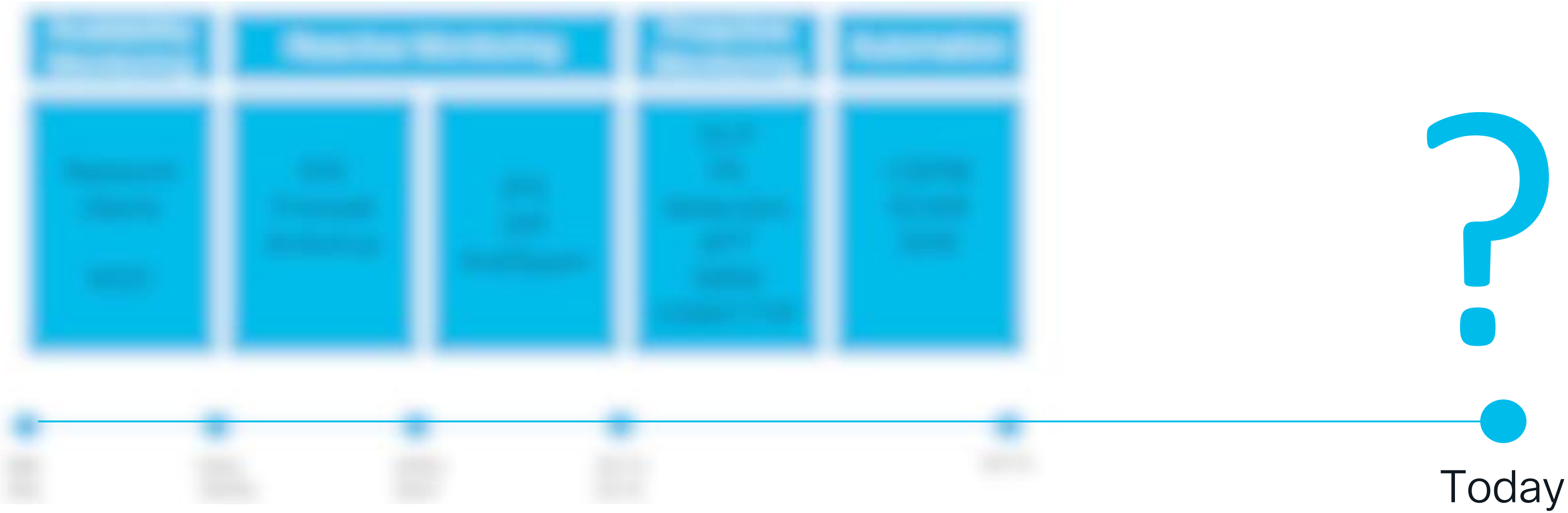
2000-
2007

2013-
2015

2015-

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Evolving Security Landscape (SoC view)



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The state of SOAR and XDR systems

- Unified Security Operations
- MTTD MTTR as primary KPIs
- Addressing Alert Fatigue ‘Information Overload’
- Automation of repetitive tasks
- Visibility/Intelligence

A gap for innovation

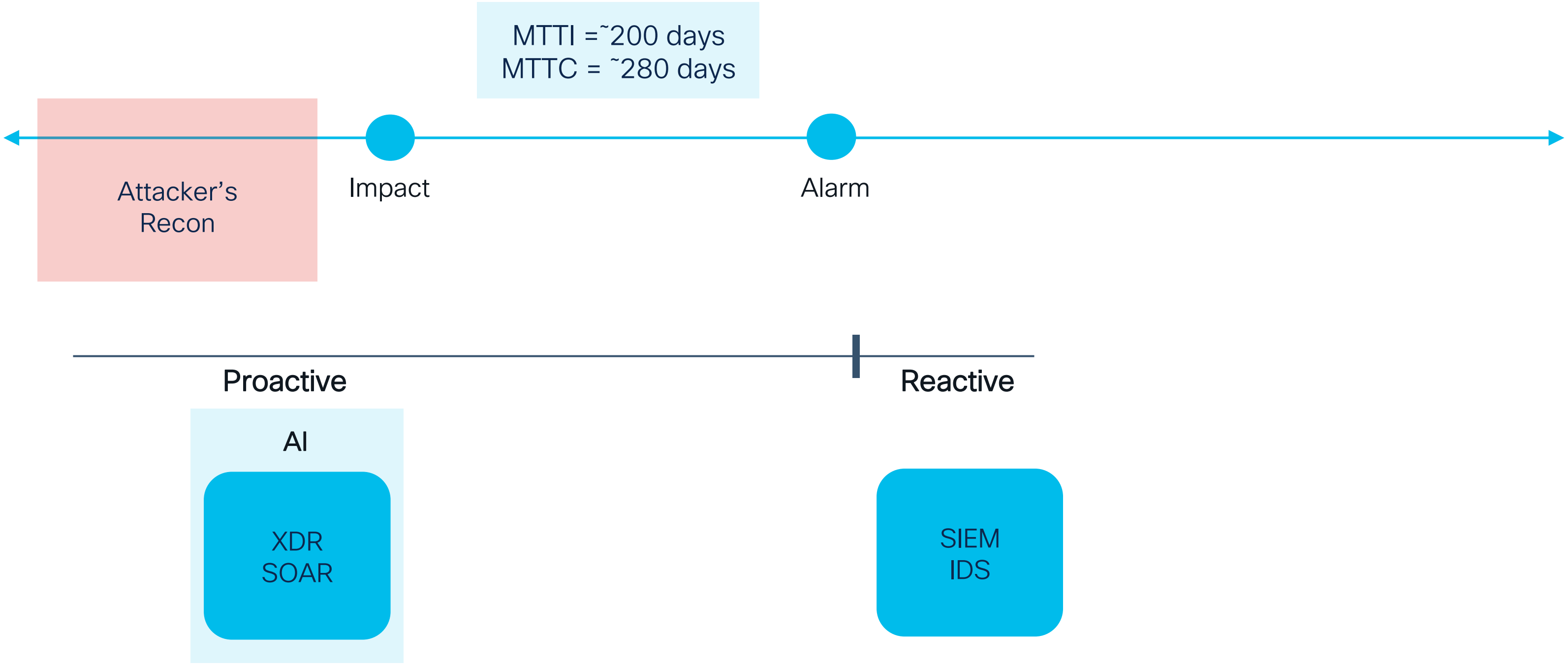
- Contextual enhanced CTI
- Correlation analysis

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Hunting

“Every contact leaves a trace”- Edmond Locard’s

Threat Hunting



MTTI =˜200 days
MTTC = ˜280 days

Attacker’s Recon

Impact

Alarm

Proactive

Reactive

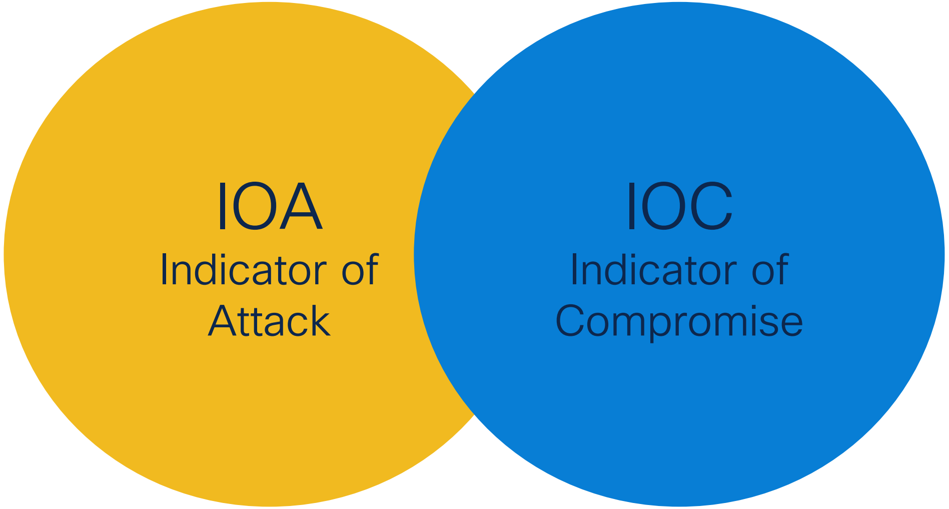
AI

XDR
SOAR

SIEM
IDS

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Indicators of Compromise | Indicators of Attack (IOCs | IoAs)



IOA

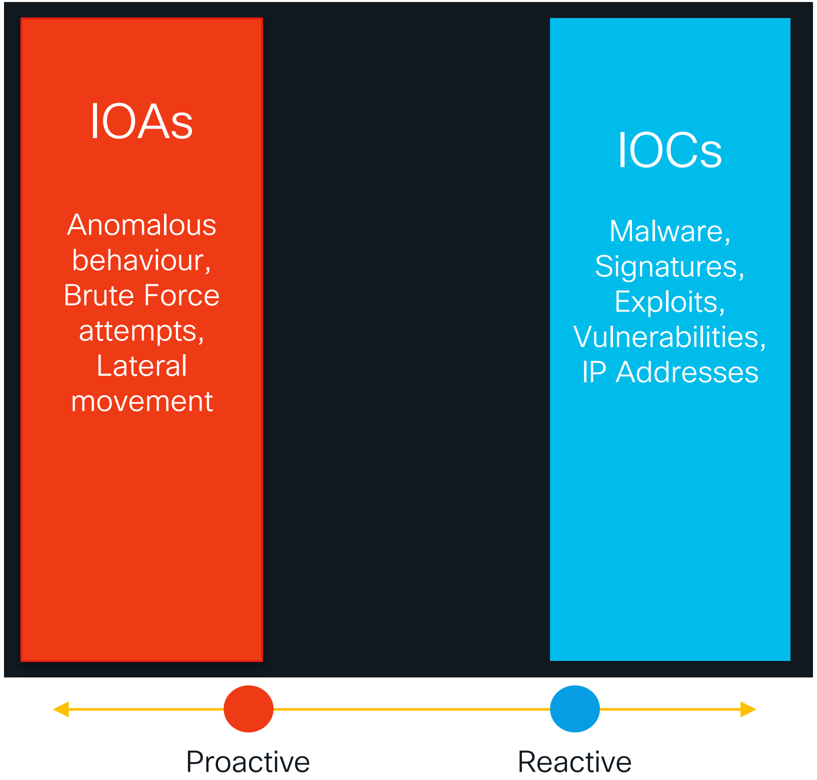
Indicator of Attack

IOC

Indicator of Compromise

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Indicators of Attack



IOAs

Anomalous behaviour, Brute Force attempts, Lateral movement

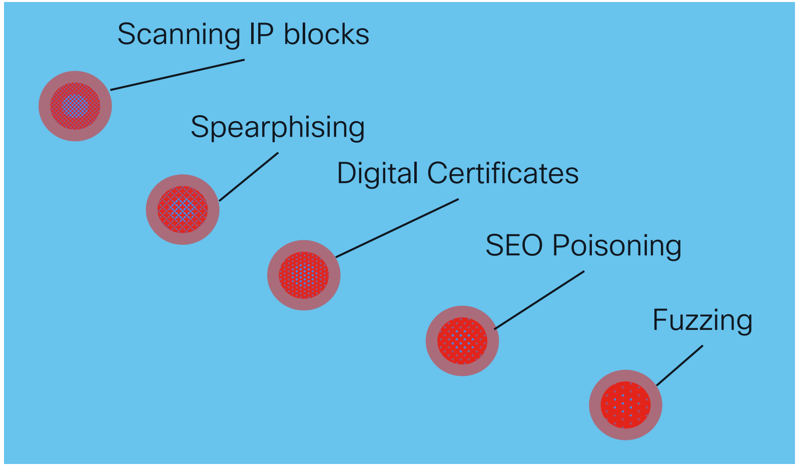
IOCs

Malware, Signatures, Exploits, Vulnerabilities, IP Addresses

Proactive

Reactive

Random indicators



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Hunting – Hunting Models

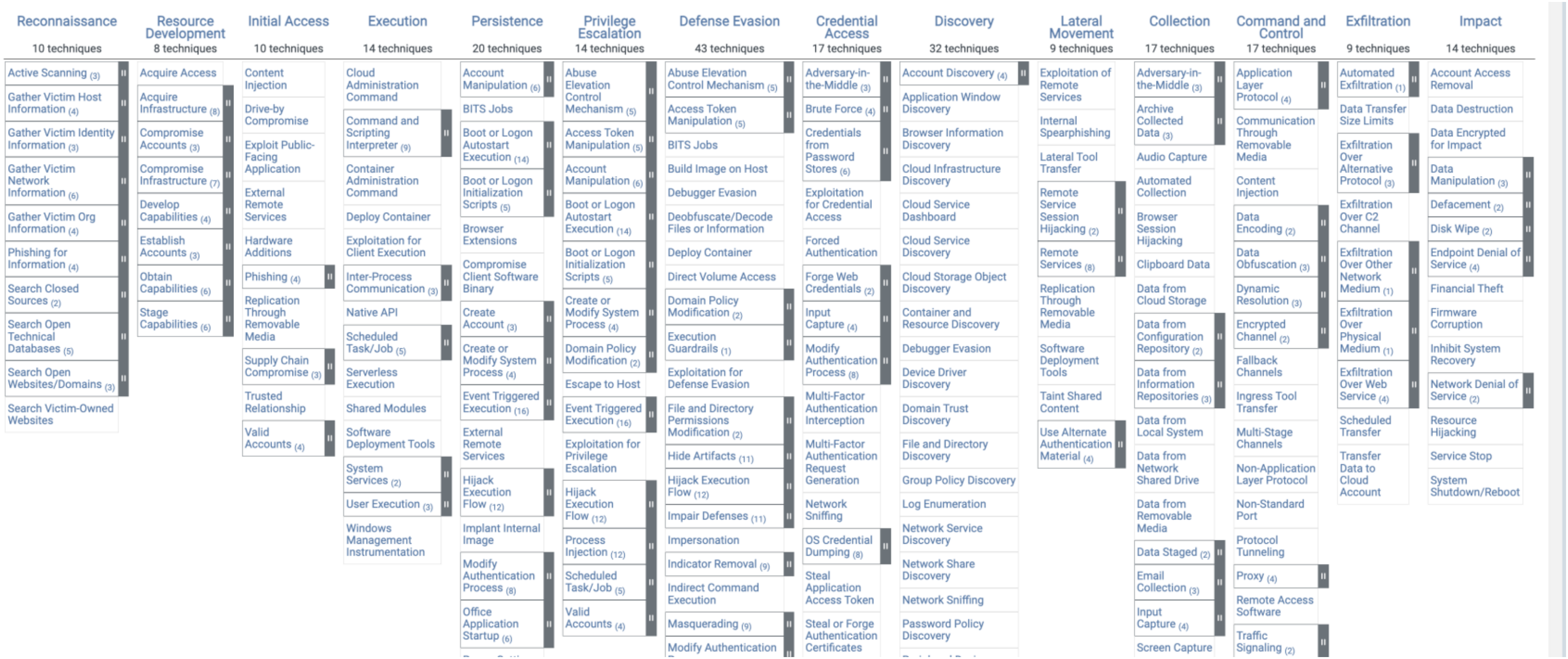
- Structured hunting
- Unstructured hunting
- Situational hunting

Hypothesis hunting

1. Indications of data exfiltrating through a specific port
2. Indications of privilege escalation
3. Lateral movement

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Hunting – Tactics, Techniques, Procedures (TTP)

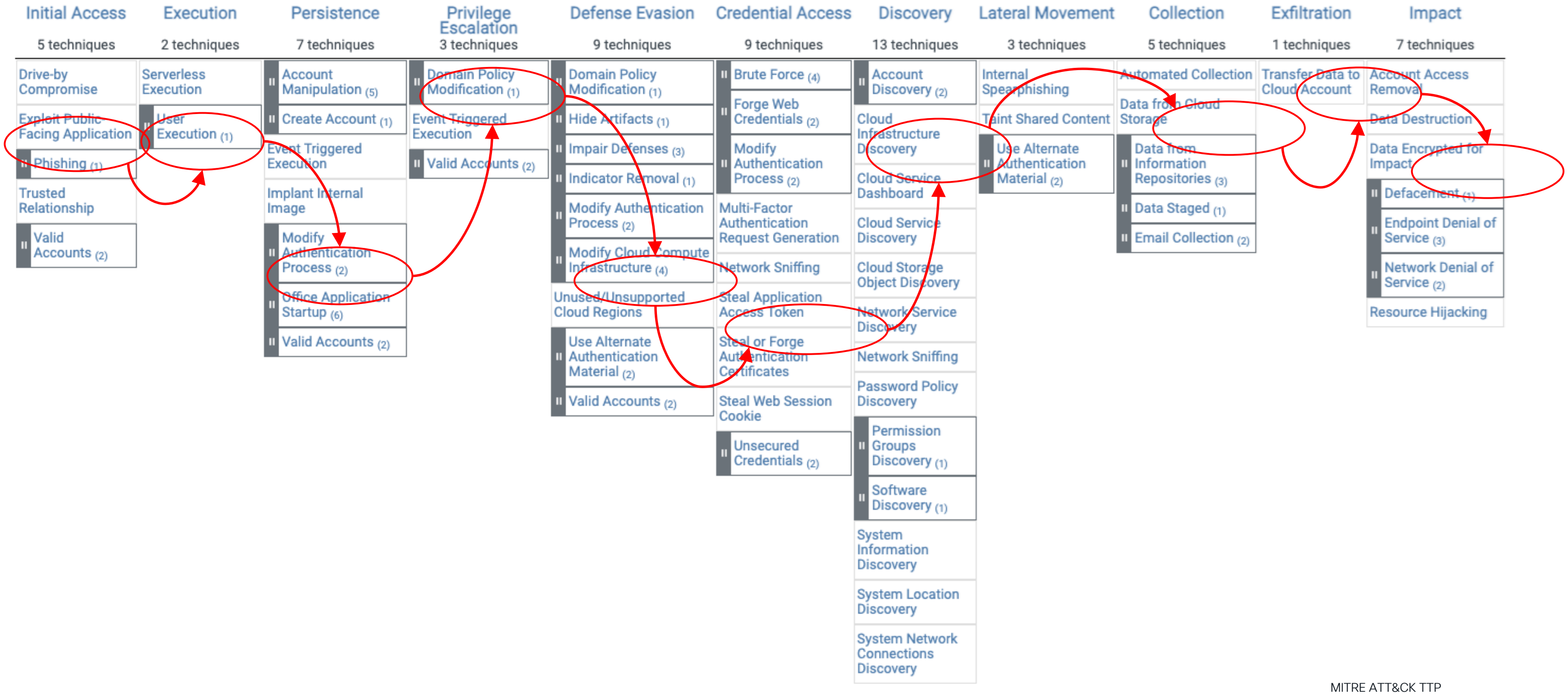


Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution (3)	Modify Authentication Process (8)	Scheduled Task/Job (5)	Hide Artifacts (11)	Steal Application Access Token	Group Policy Discovery		Data Staged (2)	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup (6)	Valid Accounts (4)	Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (3)	Proxy (4)		System Shutdown/Reboot
						Impair Defenses (11)		Network Service Discovery		Input Capture (4)	Remote Access Software		
						Impersonation		Network Share Discovery		Screen Capture	Traffic Signaling (2)		
						Indicator Removal (9)		Network Sniffing					
						Indirect Command Execution		Password Policy Discovery					
						Masquerading (9)							
						Modify Authentication							

MITRE ATT&CK TTP

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threats are becoming more complex

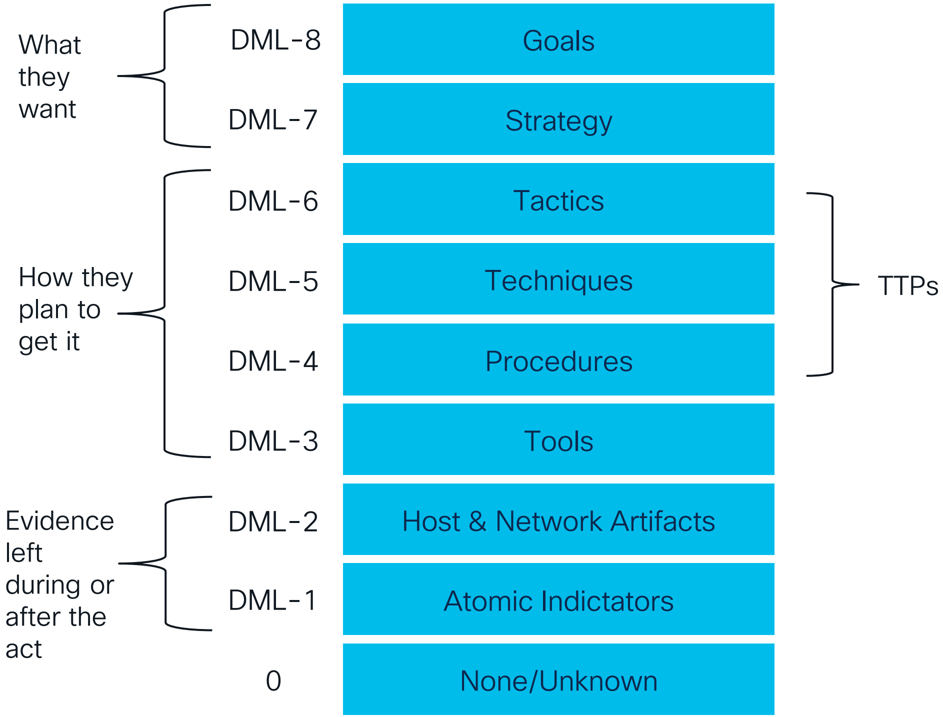


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	2 techniques	7 techniques	3 techniques	9 techniques	9 techniques	13 techniques	3 techniques	5 techniques	1 techniques	7 techniques
Drive-by Compromise	Serverless Execution	Account Manipulation (5)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Transfer Data to Cloud Account	Account Access Removal
Exploit Public-Facing Application	User Execution (1)	Create Account (1)	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery	Taint Shared Content	Data from Cloud Storage		Data Destruction
Phishing (1)		Event Triggered Execution	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (2)	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (3)		Data Encrypted for Impact
Trusted Relationship		Implant Internal Image		Indicator Removal (1)	Multi-Factor Authentication Request Generation	Cloud Service Discovery		Data Staged (1)		Defacement (1)
Valid Accounts (2)		Modify Authentication Process (2)		Modify Authentication Process (2)	Network Sniffing	Cloud Storage Object Discovery		Email Collection (2)		Endpoint Denial of Service (3)
		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Network Service Discovery				Network Denial of Service (2)
		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Steal or Forge Authentication Certificates	Network Sniffing				Resource Hijacking
				Use Alternate Authentication Material (2)	Steal Web Session Cookie	Password Policy Discovery				
				Valid Accounts (2)	Unsecured Credentials (2)	Permission Groups Discovery (1)				
						Software Discovery (1)				
						System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

MITRE ATT&CK TTP

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Hunting – Detection Maturity Level



What they want

DML-8 Goals

DML-7 Strategy

How they plan to get it

DML-6 Tactics

DML-5 Techniques

DML-4 Procedures

DML-3 Tools

TTPs

Evidence left during or after the act

DML-2 Host & Network Artifacts

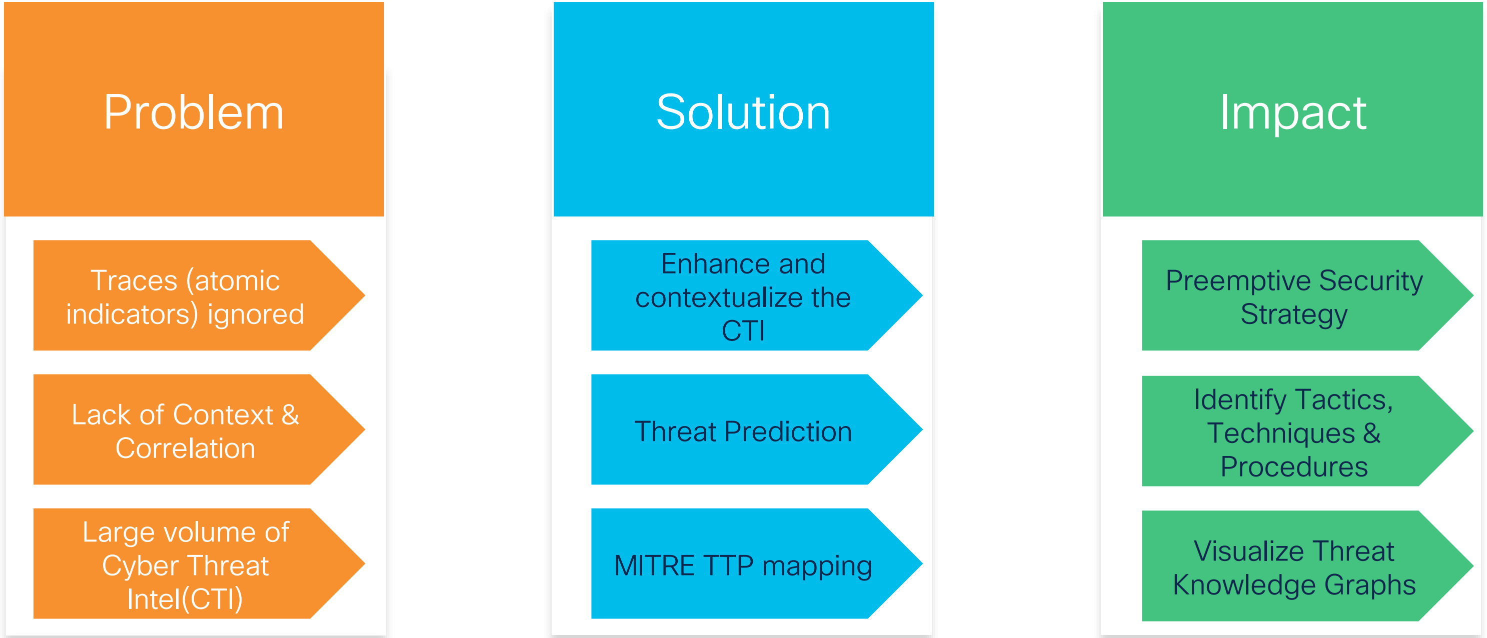
DML-1 Atomic Indictators

0 None/Unknown

© 2024 DML – Ryan Stillions

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

And?



Problem

- Traces (atomic indicators) ignored
- Lack of Context & Correlation
- Large volume of Cyber Threat Intel(CTI)

Solution

- Enhance and contextualize the CTI
- Threat Prediction
- MITRE TTP mapping

Impact

- Preemptive Security Strategy
- Identify Tactics, Techniques & Procedures
- Visualize Threat Knowledge Graphs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Towards Attack Prediction

Attack Prediction Models

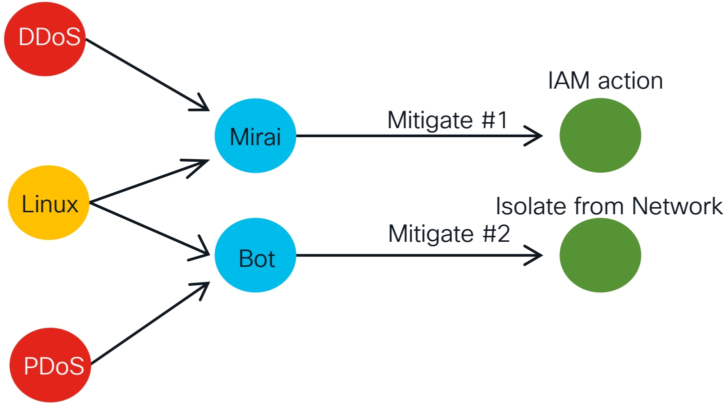
TTPDrill
2017

AttacKG
2021

ThreatKG
2022

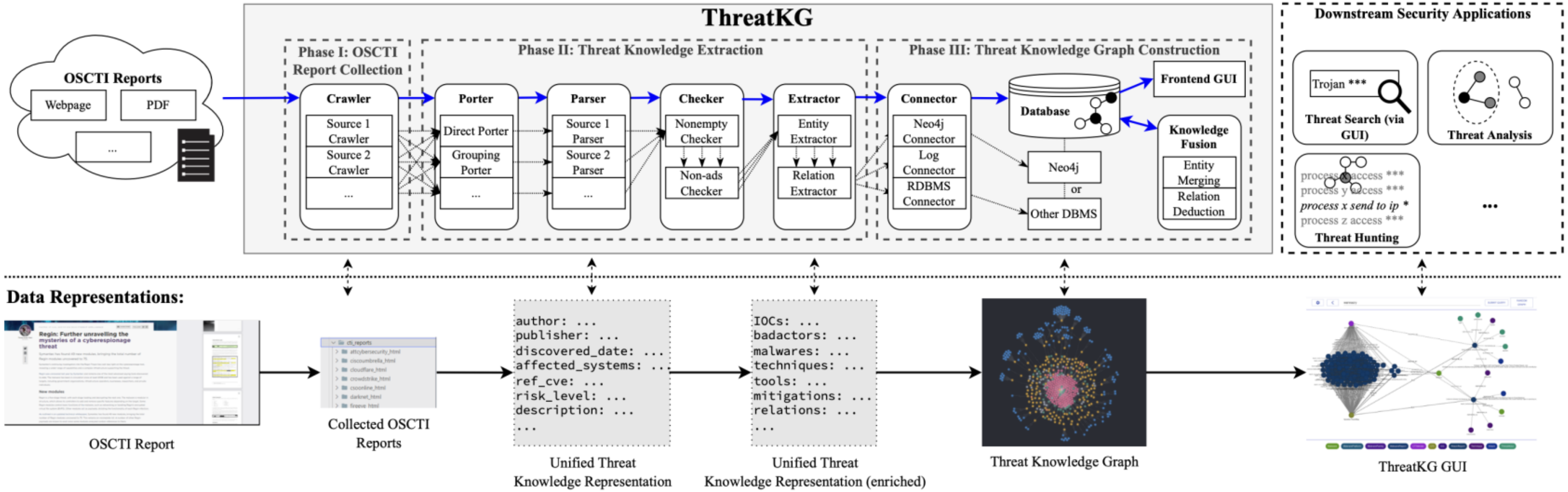
LADDER
2023

Knowledge Graph



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Constructing Knowledge Graphs



ThreatKG

OSCTI Reports

Webpage

PDF

...

Phase I: OSCTI Report Collection

Crawler: Source 1 Crawler, Source 2 Crawler, ...

Phase II: Threat Knowledge Extraction

Porter: Direct Porter, Grouping Porter, ...

Parser: Source 1 Parser, Source 2 Parser, ...

Checker: Nonempty Checker, Non-ads Checker

Extractor: Entity Extractor, Relation Extractor

Phase III: Threat Knowledge Graph Construction

Connector: Neo4j Connector, Log Connector, RDBMS Connector

Database

Neo4j or Other DBMS

Frontend GUI

Knowledge Fusion: Entity Merging, Relation Deduction

Downstream Security Applications

Trojan ***

Threat Search (via GUI)

Threat Analysis

process x access ***
process y access ***
process x send to ip *
process z access ***

Threat Hunting

...

Data Representations:

OSCTI Report

Collected OSCTI Reports

```
author: ...
publisher: ...
discovered_date: ...
affected_systems: ...
ref_cve: ...
risk_level: ...
description: ...
...
```

Unified Threat Knowledge Representation

```
IOCs: ...
badactors: ...
malwares: ...
techniques: ...
tools: ...
mitigations: ...
relations: ...
...
```

Unified Threat Knowledge Representation (enriched)

Threat Knowledge Graph

ThreatKG GUI

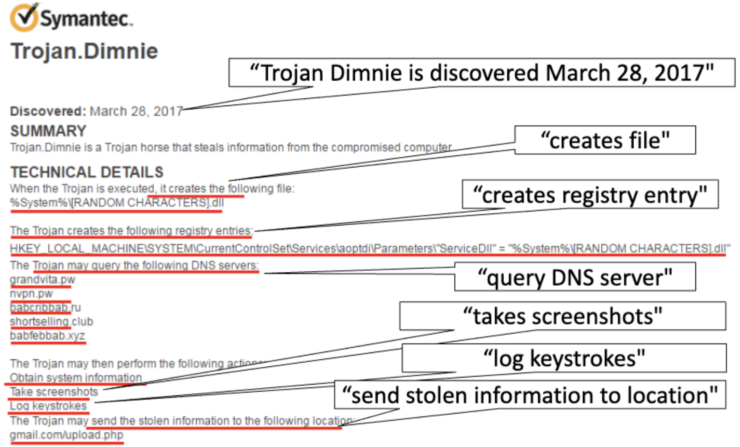
https://arxiv.org/pdf/2211.01753.pdf

Towards Attack Prediction – TTPDrill

- Threat-action ontology
- Text-mining approach (Natural Language Processing & Information Retrieval)
- Construction of complete attack patterns
  - Mapping threat actions to TTP ontology
- Tested with Symantec Threat Reports
  - 82% precision and recall

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Towards Attack Prediction – TTPDrill



Symantec.

Trojan.Dimnie

Discovered: March 28, 2017

SUMMARY

Trojan.Dimnie is a Trojan horse that steals information from the compromised computer

TECHNICAL DETAILS

When the Trojan is executed, it creates the following file:
%System%\[RANDOM CHARACTERS].dll

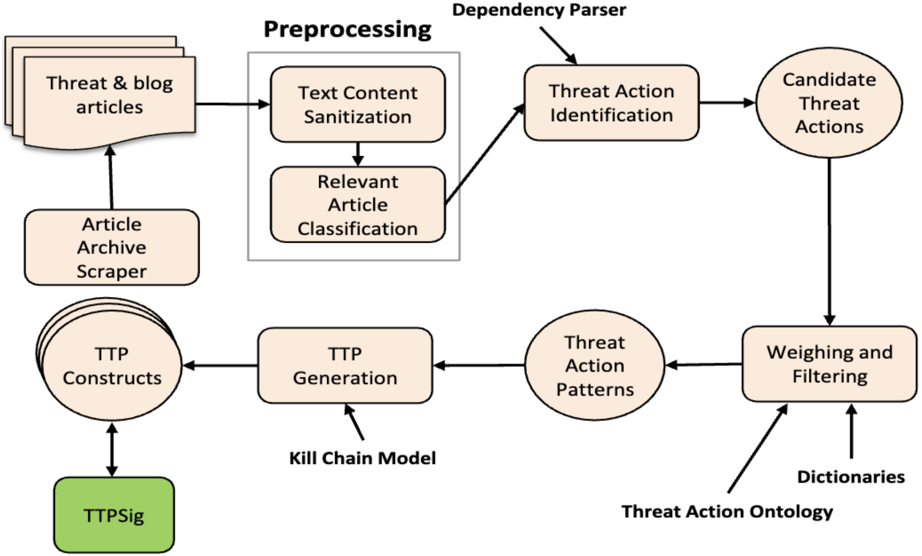
The Trojan creates the following registry entries:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aoptdi\Parameters\"ServiceDll" = "%System%\[RANDOM CHARACTERS].dll"

The Trojan may query the following DNS servers:
grandvita.pw
nvpn.pw
babcribbab.ru
shortselling.club
babfebbab.xyz

The Trojan may then perform the following actions:
Obtain system information
Take screenshots
Log keystrokes

The Trojan may send the stolen information to the following location:
gmail.com/upload.php

https://www.researchgate.net/publication/321503662_TTPDrill_Automatic_and_Accurate_Extraction_of_Threat_Actions_from_Unstructured_Text_of_CTI_Sources



https://www.researchgate.net/publication/321503662_TTPDrill_Automatic_and_Accurate_Extraction_of_Threat_Actions_from_Unstructured_Text_of_CTI_Sources

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

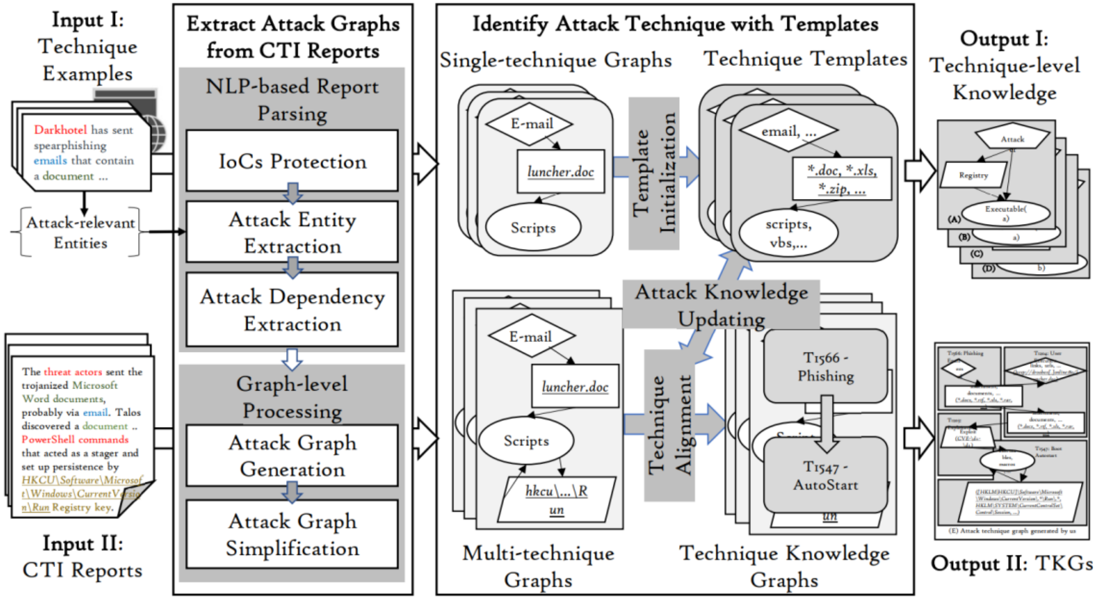
Towards Attack Prediction – AttacKG

- Identifying attack techniques in Cyber Threat Intelligence (CTI) reports
- Constructing Attack/Knowledge graphs
- Correlation | relationships & dependencies
- Attack reconstruction
- Enriched Threat Intelligence

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

AttacKG Architecture

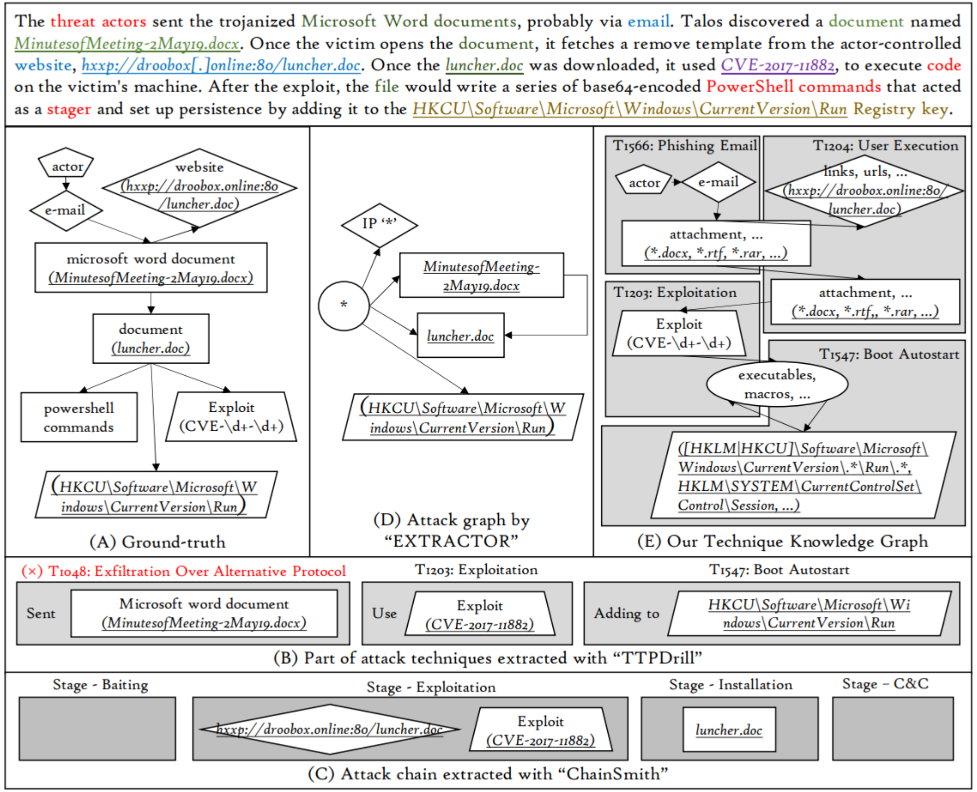
AttacKG: Constructing Technique Knowledge Graph from CTI Reports


Input I: Technique Examples
Darkhotel has sent spearphishing emails that contain a document ...
Attack-relevant Entities
The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document .. PowerShell commands that acted as a stager and set up persistence by HKCU\Software\Microsoft\Windows\CurrentVersion\Run Registry key.
Input II: CTI Reports
Extract Attack Graphs from CTI Reports
NLP-based Report Parsing
IoCs Protection
Attack Entity Extraction
Attack Dependency Extraction
Graph-level Processing
Attack Graph Generation
Attack Graph Simplification
Identify Attack Technique with Templates
Single-technique Graphs
E-mail
luncher.doc
Scripts
Template Initialization
Technique Templates
email, ...
*.doc, *.xls, *.zip, ...
scripts, vbs,...
Attack Knowledge Updating
E-mail
luncher.doc
Scripts
hkcu\...\Run
Technique Alignment
T1566 - Phishing
T1547 - AutoStart
Multi-technique Graphs
Technique Knowledge Graphs
Output I: Technique-level Knowledge
Attack
Registry
Executable(a)
(A)
(B)
(C)
(D)
(E) Attack technique graph generated by us
Output II: TKGs

AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports “https://users.cs.northwestern.edu/~ychen/Papers/ESORICS_AttacKG.pdf”

APT campaign 2019 - Frankenstein

https://blog.talosintelligence.com/2019/06/frankenstein-campaign.html



The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named MinutesofMeeting-2May19.docx. Once the victim opens the document, it fetches a remove template from the actor-controlled website, hxxp://droobox[.]online:80/luncher.doc. Once the luncher.doc was downloaded, it used CVE-2017-11882, to execute code on the victim's machine. After the exploit, the file would write a series of base64-encoded PowerShell commands that acted as a stager and set up persistence by adding it to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run Registry key.

actor
website
(hxxp://droobox.online:80 /luncher.doc)
e-mail
microsoft word document (MinutesofMeeting-2May19.docx)
document (luncher.doc)
powershell commands
Exploit (CVE-\d+-\d+)
(HKCU\Software\Microsoft\Windows\CurrentVersion\Run)
(A) Ground-truth
IP '*'
*
MinutesofMeeting-2May19.docx
luncher.doc
(HKCU\Software\Microsoft\Windows\CurrentVersion\Run)
(D) Attack graph by "EXTRACTOR"
T1566: Phishing Email
T1204: User Execution
actor
e-mail
links, urls, ... (hxxp://droobox.online:80/luncher.doc)
attachment, ... (*.docx, *.rtf, *.rar, ...)
T1203: Exploitation
attachment, ... (*.docx, *.rtf,, *.rar, ...)
Exploit (CVE-\d+-\d+)
T1547: Boot Autostart
executables, macros, ...
([HKLM|HKCU]\Software\Microsoft\Windows\CurrentVersion\.*\Run\.*, HKLM\SYSTEM\CurrentControlSet\Control\Session, ...)
(E) Our Technique Knowledge Graph
(×) T1048: Exfiltration Over Alternative Protocol
Sent
Microsoft word document (MinutesofMeeting-2May19.docx)
T1203: Exploitation
Use
Exploit (CVE-2017-11882)
T1547: Boot Autostart
Adding to
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
(B) Part of attack techniques extracted with "TTPDrill"
Stage - Baiting
Stage - Exploitation
hxxp://droobox.online:80/luncher.doc
Exploit (CVE-2017-11882)
Stage - Installation
luncher.doc
Stage - C&C
(C) Attack chain extracted with "ChainSmith"

AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports
"https://users.cs.northwestern.edu/~ychen/Papers/ESORICS_AttacKG.pdf"

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Towards Attack Prediction – LADDER

- LADDER (**L**earning-Based **A**ttack pattern **D**etection and **D**efens**e**)
  - Knowledge extraction framework (attack patterns)
  - Systematic mapping to MITRE ATT&CK framework
    - Utilized an Ontology and TTPClassifier creating a Knowledge Graph
  - Train future cyberthreat intelligence model
- TTPClassifier
  - Novel ML algorithm for TTP extraction from CTI reports
    - TTPs → MITRE ATT&CK pattern IDs

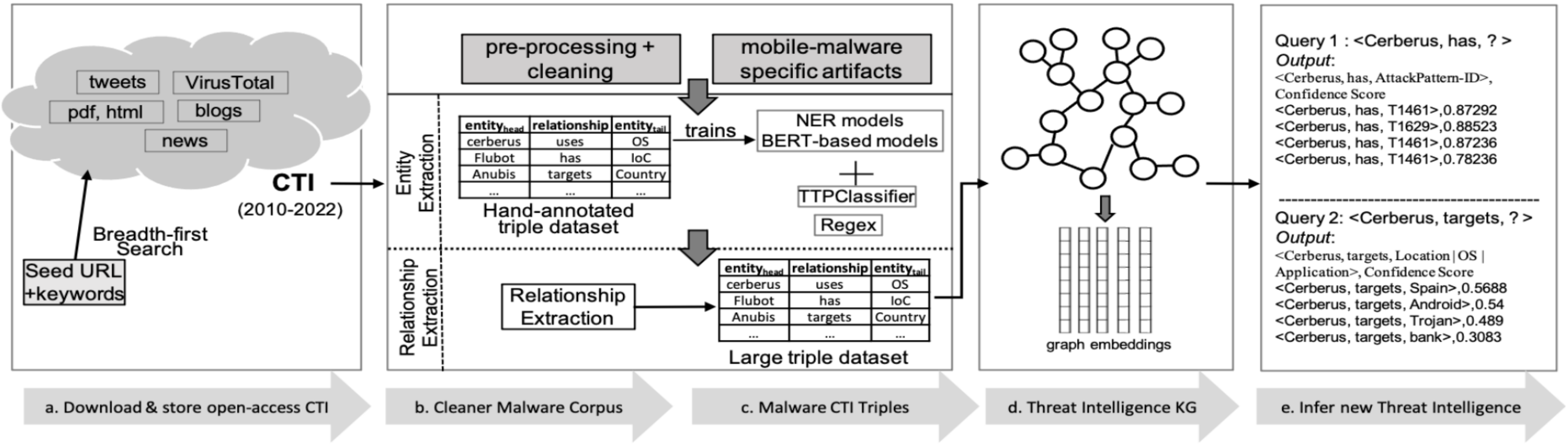
Outcomes

- Predictive Analysis, pre-empt potential attacks
- Learn and analyse attack campaigns
- Automated extraction and analysis of Cyberthreat Intelligence(CTI)
- ML-based Categorization of Tactics, Techniques, and Procedures (TTPs)
- Open benchmark malware dataset to train future cyberthreat intelligence models

https://arxiv.org/pdf/2211.01753.pdf

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Towards Attack Prediction – LADDER



entity_{head}	relationship	entity_{tail}
cerberus	uses	OS
Flubot	has	IoC
Anubis	targets	Country
...	...	...

entity_{head}	relationship	entity_{tail}
cerberus	uses	OS
Flubot	has	IoC
Anubis	targets	Country
...	...	...

Query 1 : <Cerberus, has, ? >
Output:
<Cerberus, has, AttackPattern-ID>, Confidence Score
<Cerberus, has, T1461>,0.87292
<Cerberus, has, T1629>,0.88523
<Cerberus, has, T1461>,0.87236
<Cerberus, has, T1461>,0.78236

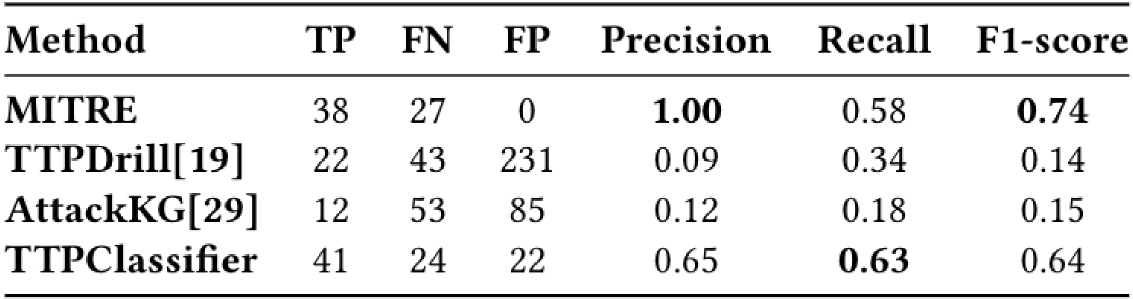
Query 2: <Cerberus, targets, ? >
Output:
<Cerberus, targets, Location | OS | Application>, Confidence Score
<Cerberus, targets, Spain>,0.5688
<Cerberus, targets, Android>,0.54
<Cerberus, targets, Trojan>,0.489
<Cerberus, targets, bank>,0.3083

a. Download & store open-access CTI
b. Cleaner Malware Corpus
c. Malware CTI Triples
d. Threat Intelligence KG
e. Infer new Threat Intelligence

https://arxiv.org/pdf/2211.01753.pdf

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Attack prediction models - Scoring



Method	TP	FN	FP	Precision	Recall	F1-score
MITRE	38	27	0	**1.00**	0.58	**0.74**
TTPDrill[19]	22	43	231	0.09	0.34	0.14
AttackKG[29]	12	53	85	0.12	0.18	0.15
TTPClassifier	41	24	22	0.65	**0.63**	0.64

AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports
"https://users.cs.northwestern.edu/~ychen/Papers/ESORICS_AttacKG.pdf"

1/3

Nearly a third of the top 20 most common MITRE ATT&CK techniques fall under defense evasion tactics

Cisco Talos

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco’s Activity

Cisco Cloud Application Security

panoptica
Cisco Cloud Application Security

Attack Path Analysis

Query graph for security scenarios

Validate and score severity of resources impacted, data at risk, and lateral movement options.

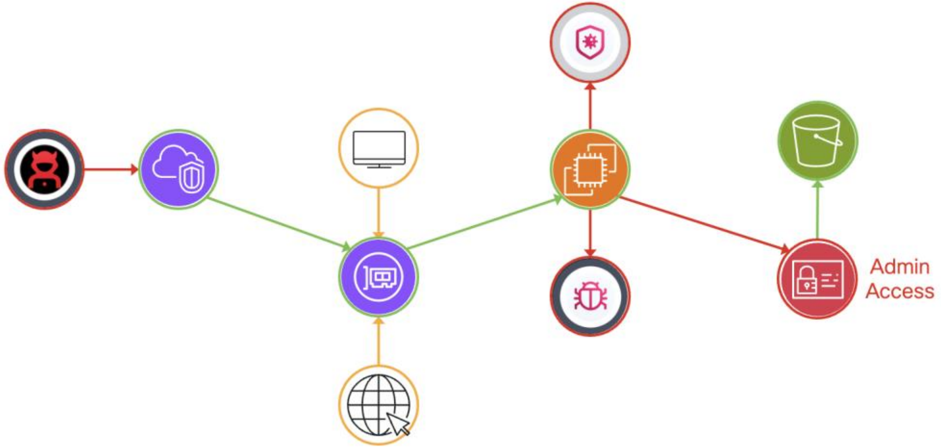
Prioritize the findings and present with relevant context for security investigation

Root Cause Analysis

Identify commonalities across the common attack paths

Comparative health score analysis to identify and prioritize potential root causes

Graph-based Analysis



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Cloud Application Security (Panoptica)

- Currently this solution is undergoing a rebranding from "Panoptica" to "Cisco Cloud Application Security"
- As such, if you see or hear these names throughout the presentation, throughout Cisco Live, or in the near-term after Cisco Live, please note, ***they are the same solution***
- Cisco Cloud Application Security = Panoptica

panoptica
Cisco Cloud Application Security

“In the face of obscured insights, maximize the utility of existing resources and data to compensate for the voids as effectively as possible”

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

Panoptica Technical Breakouts

- **BRKSEC-1585** Application Security in the Cloud Native World
- **BRKETI-2161** The Power of Predictive Attack Analysis in an Offensive-Defensive Nexus
- **BRKETI-2511** Securing Cloud Native Applications with Cisco Cloud Application Security (Panoptica)
- **BRKETI-2512** How to Leverage Generative AI to Protect Your Cloud Applications
- **BRKETI-2903** The Five Biggest Security Nightmares Waiting to Happen to Your Cloud Applications and How to Protect Your Business from Them

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue
your education

Panoptica DevNet Workshops

- **DEVWKS-2255** Security at the speed of cloud - Security as code
- **DEVWKS-2771** Secure Your Kubernetes Runtime and Cloud Posture with Cisco Cloud Application Security (Panoptica)
- **DEVWKS-2774** Securing the Future: Enhancing Application Security with AI and for AI
- **DEVWKS-2780** Prioritise Your Risks with Cisco Cloud Application Security (Panoptica) Attack Path Analysis
- **DEVWKS-3002** Embed Security Practices into DevOps with Cisco Cloud Application Security (Panoptica)
- **DEVWKS-3003** 5G Cloud Native Core Network Security with Cisco Cloud Application Security (Panoptica)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue the Discussion

- Come visit us in the Outshift booth in the Cisco World of Solutions (Booth D10) to see live demos on Panoptica
- Book your one-on-one Meet the Engineer meeting
- See what’s coming in the next releases of Panoptica by meeting with us in the Innovation Forum
- Book a meeting with us for an extended discussion on Panoptica

Visit Outshift in the World of Solutions!

Learn more about Panoptica, Cisco's Cloud Application Security Solution!

outshift
by cisco

- Snap a picture of this slide and visit the Outshift Booth, D10.
- Get your badge scanned to be entered into our daily drawing* for €250 Cisco Store Gift Certificate.

**Winners will be notified via email*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you

cisco Live!

Let's go