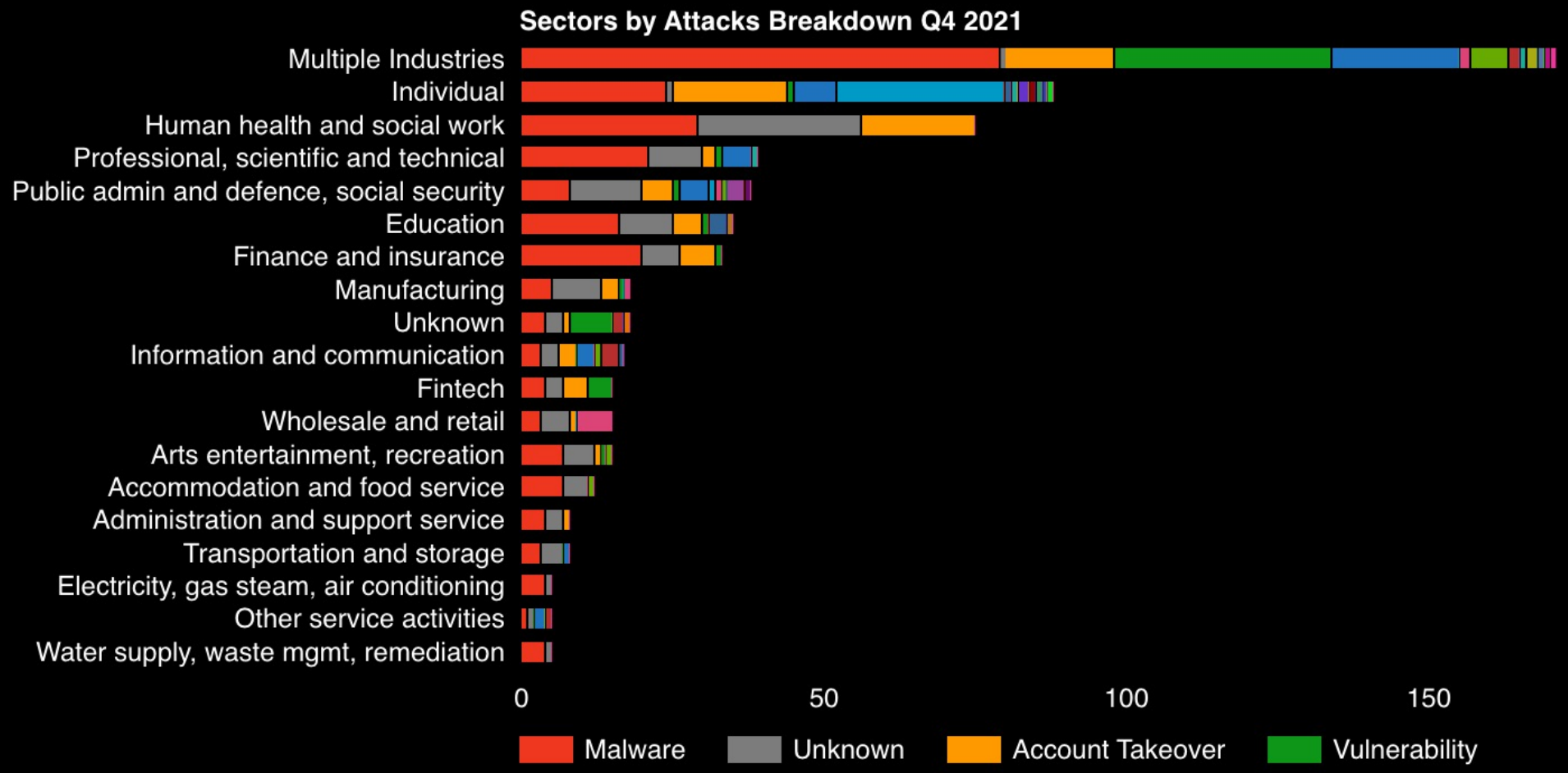
Contextual Security

need for a critical shift in threat intelligence

Nidhi Rastogi
Assistant Professor,
Rochester Institute of Technology, NY

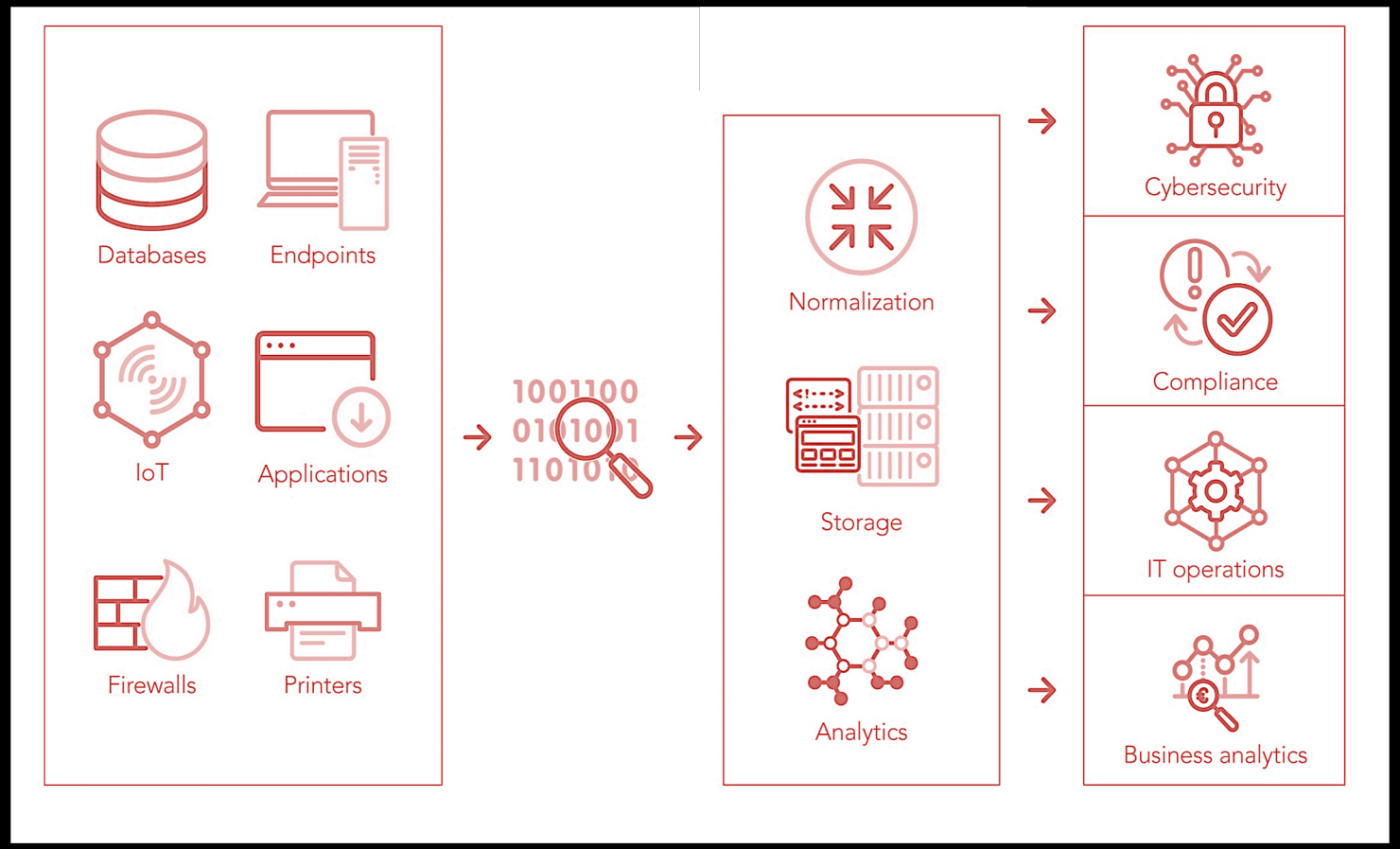
02.02.2022

internet <> cybersecurity

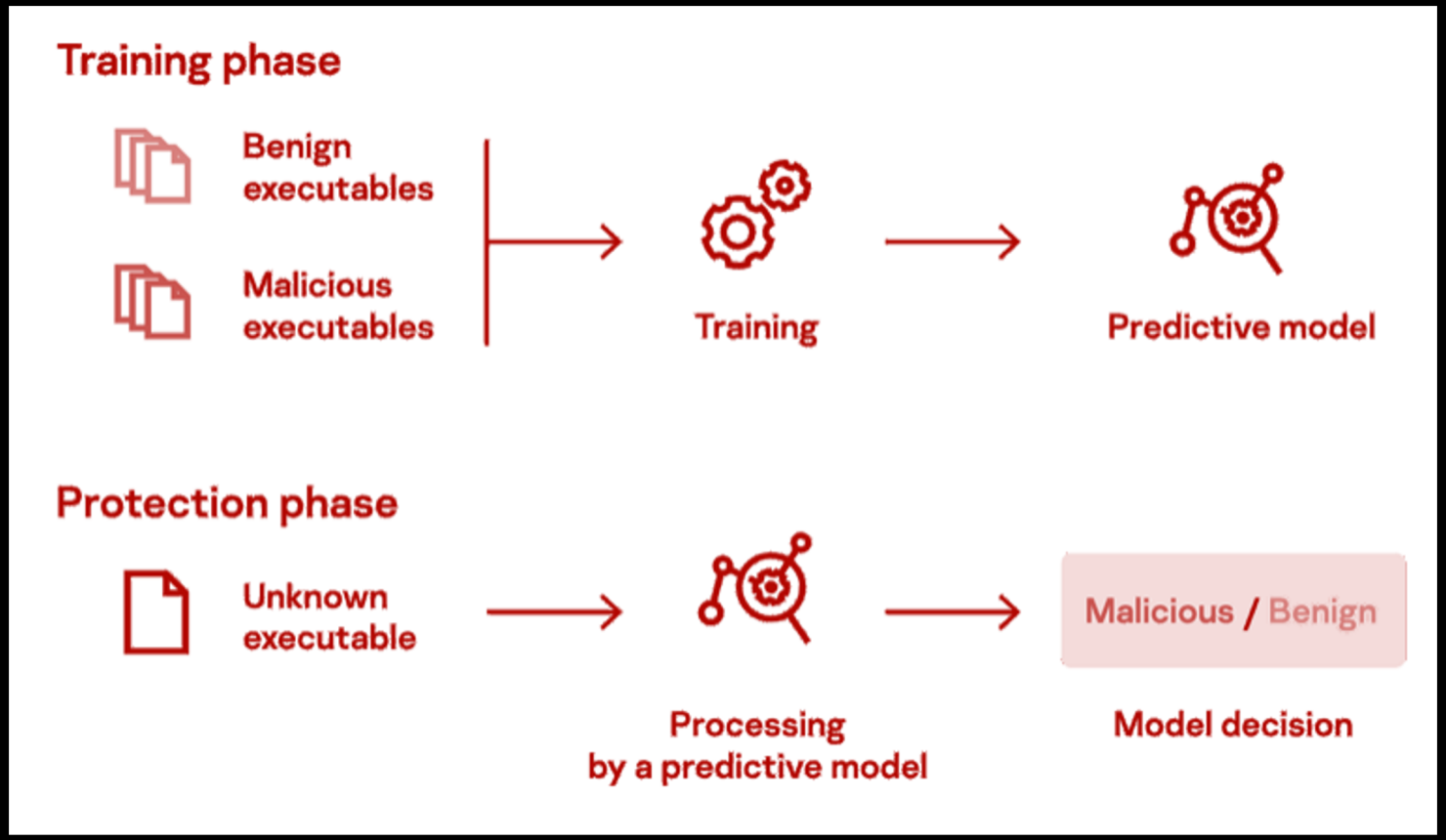


malware is everywhere

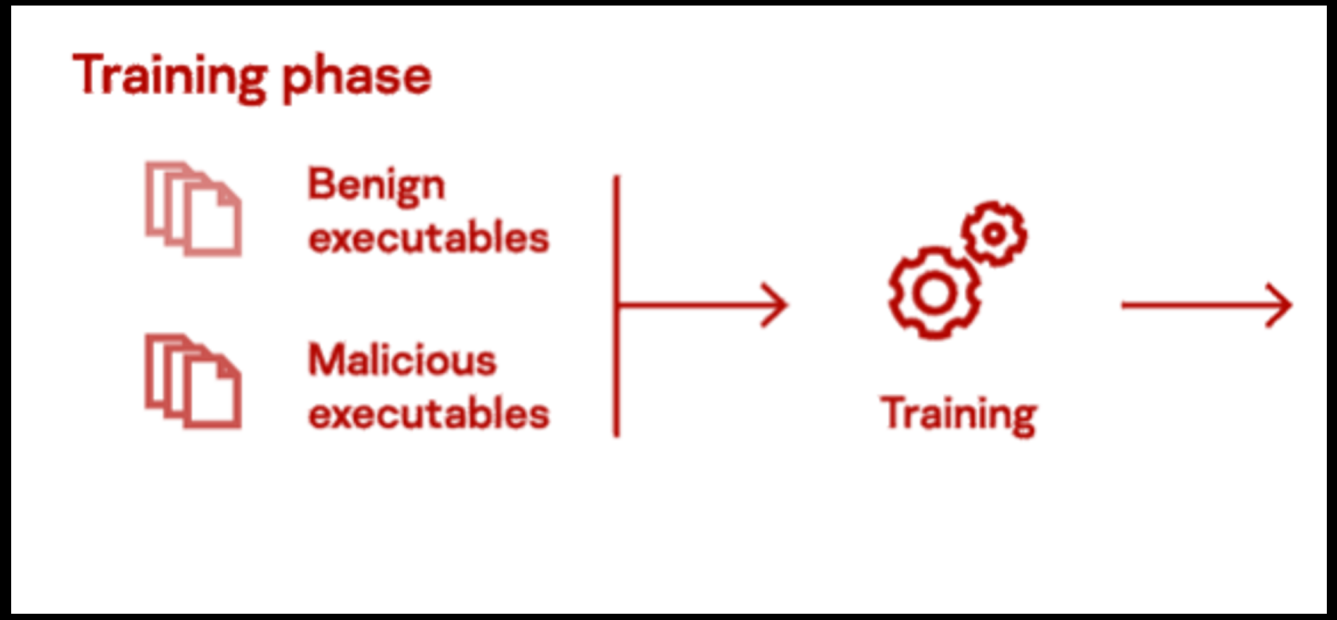
Credit: https://www.hackmageddon.com/2022/01/13/2021-cyber-attacks-statistics/



SIEM – at a glance



ml widely used for securing systems



data drives ml

challenges with ml

unmanageable false positives

p1 – lack of good data to test rules

p2 - deluge of fp – even high priority

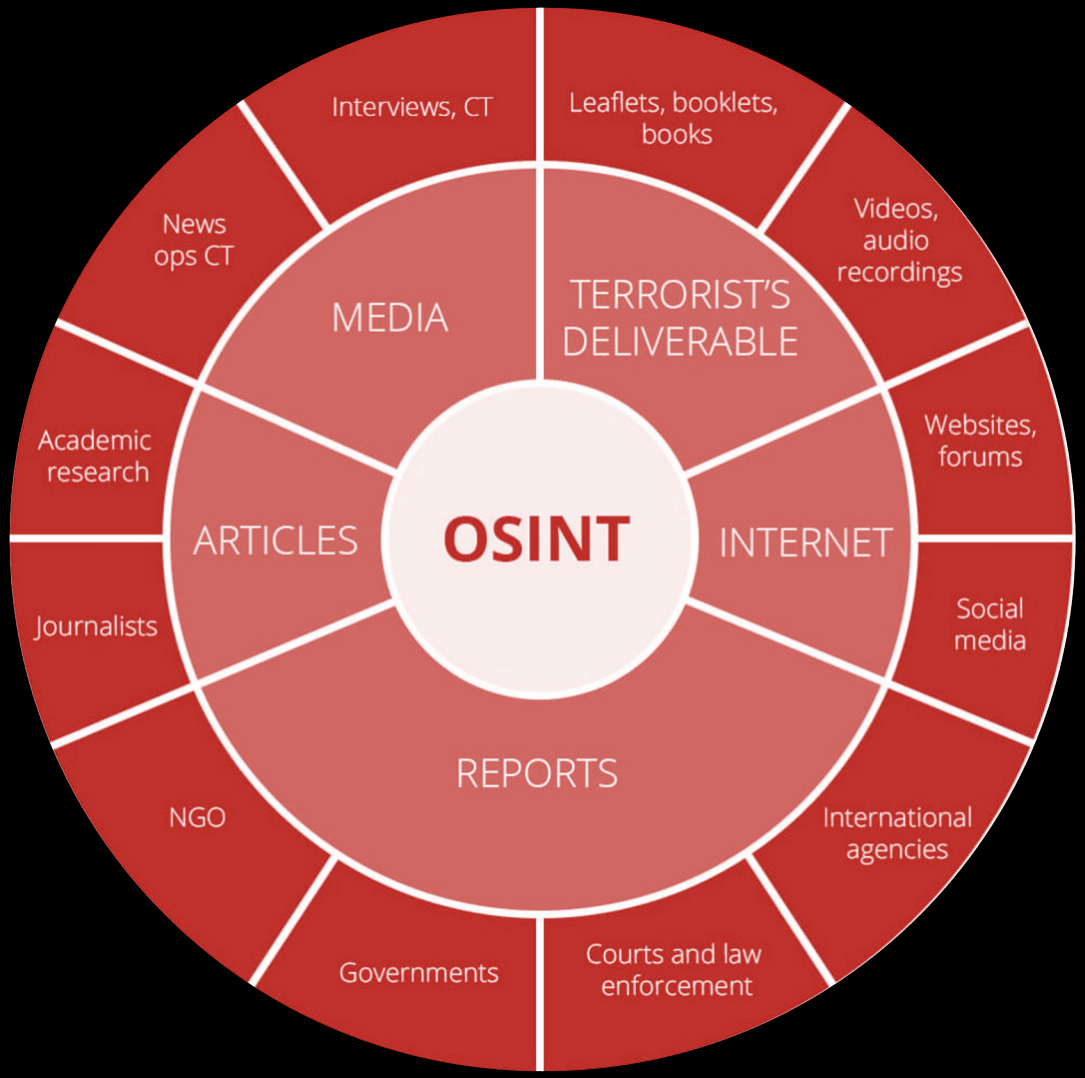
dealing with fp - reality

p1 – lack of good data to test rules
improve learning. add most recent data

p2 - deluge of fp – even high priority
triage alerts. providing more information - > “context”

dealing with fp - reality

continuous learning



data aggregation

McAfee Labs Threat Advisory

Trojan-Sunburst

McAfee™ Together is power.

December 23, 2

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL: https://www.mcafee.com/enterprise/en-us/sns/preferences/sns-form.html.

Summary

Trojan-Sunburst is an http backdoor. Upon execution, it communicates with a C2 server whose subdomain is partially generated based on the domain of the infected computer. Once executed, the backdoor has the ability to idle for extended periods of time, collect system information, upload system information, execute arbitrary code from the attacker, collect running process information, write files to the system, delete files, modify the registry, and reboot the machine. This backdoor was distributed to consumers using a supply-chain attack on SolarWinds Orion platform where the backdoor code was hidden in an update for product version 2019.4.

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

- Infection and Propagation Vectors
- Mitigation
- Characteristics and Symptoms
- Restart Mechanism
- McAfee Foundstone Services

The minimum DAT versions required for detection are:

Detection Name	MD5 of samples	DAT Version	Date
Trojan-Sunburst	2C4A910A1299CDAE2A4E55988A2F102E	V2: 9836 V3: 4288	20/12/15
Trojan-Sunburst	B91CE2FA41029F6955BFF20079468448	V2: 9836 V3: 4288	20/12/15
Trojan-Sunburst	56CFB6D0011D87B6F4D7023D7FF85676	V2: 9836	20/12/15

```
// Token: 0x06000057 RID: 87 RVA: 0x000089C4 File Offset: 0x00008BC4
private static ulong GetHash(string s)
{
    ulong num = 14695981039346656037UL;
    try
    {
        foreach (byte b in Encoding.UTF8.GetBytes(s))
        {
            num ^= (ulong)b;
            num *= 1099511628211UL;
        }
    }
    catch
    {
    }
    return num ^ 6605813339339102567UL;
}
```

This figure represents the hashing code used to check strings against the hardcoded hashes.

Backdoor Functionality

Backdoor functionality for this threat is standard, and its intentions and purposes are not obfuscated.

```
private enum JobEngine
{
    Idle,
    Exit,
    SetTime,
    CollectSystemDescription,
    UploadSystemDescription,
    RunTask,
    GetProcessByDescription,
    KillTask,
    GetFileSystemEntries,
    WriteFile,
    FileExists,
    DeleteFile,
    GetFileHash,
    ReadRegistryValue,
    SetRegistryValue,
    DeleteRegistryValue,
    GetRegistrySubKeyAndValueNames,
    Reboot,
    None
}
```

Idle – Idle for a randomized amount of time, scaled by SetTime.
Exit – Exit this execution
SetTime – Sets the idle scale time
CollectSystemDescription - Domain Name, Domain Admin SID, Hostname, Username, OSVersion, SystemDirectory, TotalDays uptime, as well as the following attributes from Win32_NetworkAdapterConfiguration: Description, MACAddress, DHCPEnabled, DHCPServer, DNSHostName, DNSDomainSuffixSearchOrder, DNSServerSearchOrder, IPAddress, IPSubnet, DefaultIPGateway
UploadSystemDescrption – Upload information collected from previous command to CNC.
RunTask – Creates a process from a file on disk, and will accept arguments.
GetProcessByDescription – Returns process information matching specified pattern
KillTask - Kill process by PID.
GetFileSystemEntries – Returns directory contents matching specified pattern
WriteFile – Write file to disk.
FileExists – Check for existence of specified file.
DeleteFile – Delete specified File
GetFileHash – Retrieve MD5 Hash of File
ReadRegistryValue – Read indicated Registry Value
SetRegistryValue - Set indicated Registry Value
DeleteRegistryValue - Delete indicated Registry Value
GetRegistrySubKeyAndValueNames – Retrieve Subkey and Value names from specified key
Reboot - Reboot the machine.

Command and Control

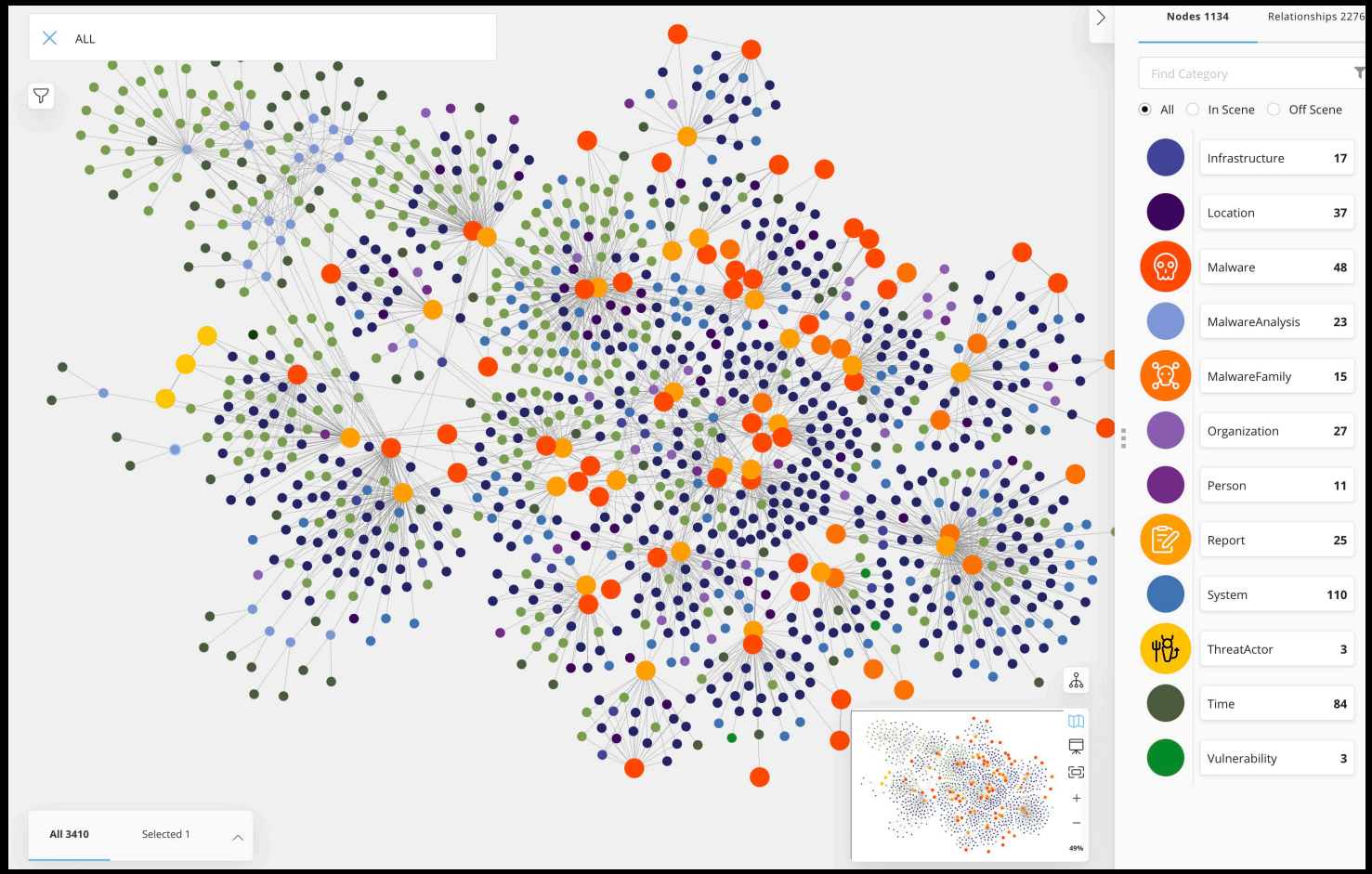
Trojan-Sunburst uses a DGA (Domain Generation Algorithm) to create part of the subdomain for communication with the command and control infrastructure. The DGA takes into account the domain name of the infected computer and a generated UID to prepend to a hardcoded list of subdomains.

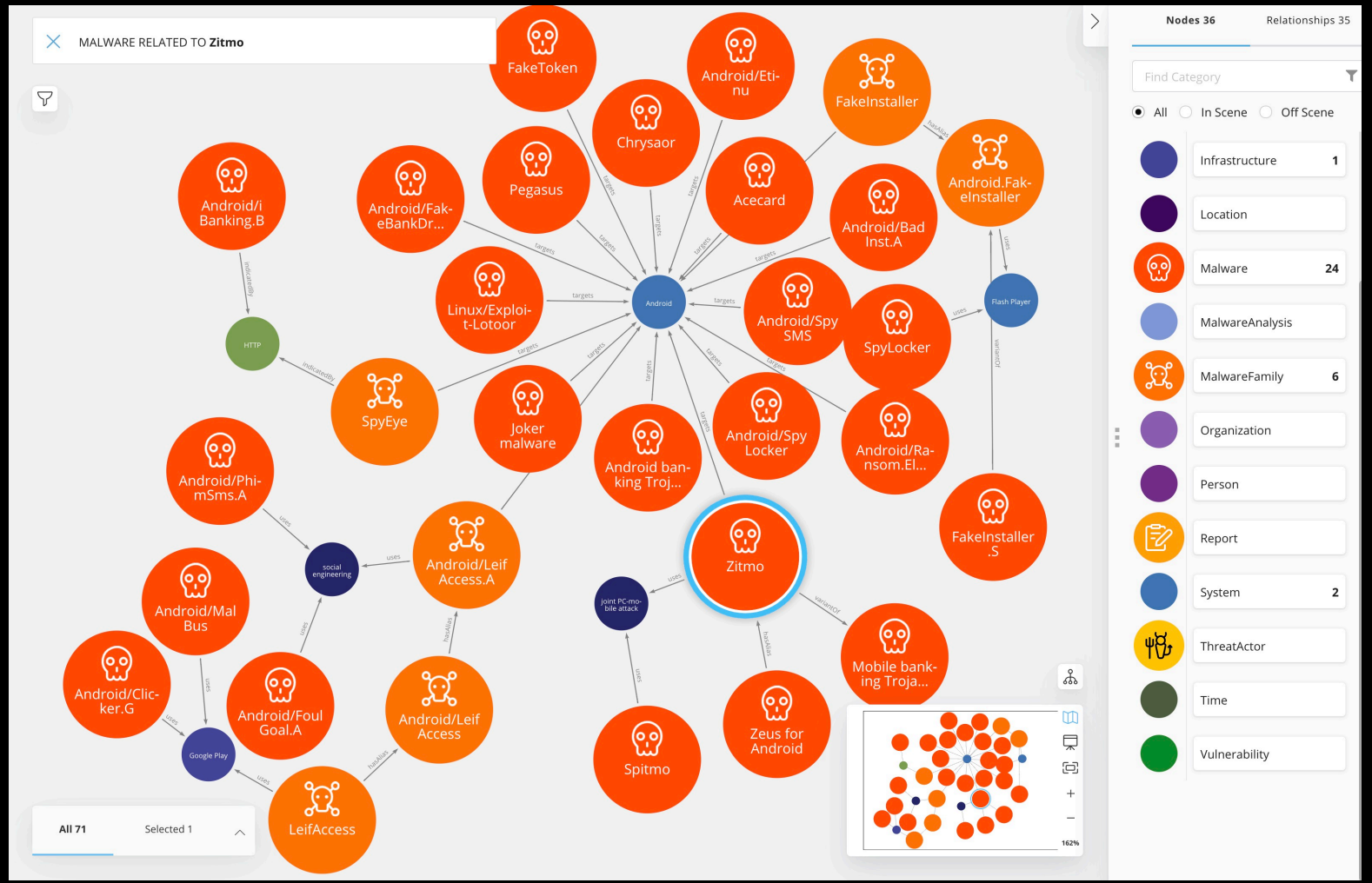
%generateddomain%.appsync-api.eu-west-1.avsvmcloud.com
%generateddomain%.appsync-api.us-west-2.avsvmcloud.com
%generateddomain%.appsync-api.us-east-1.avsvmcloud.com

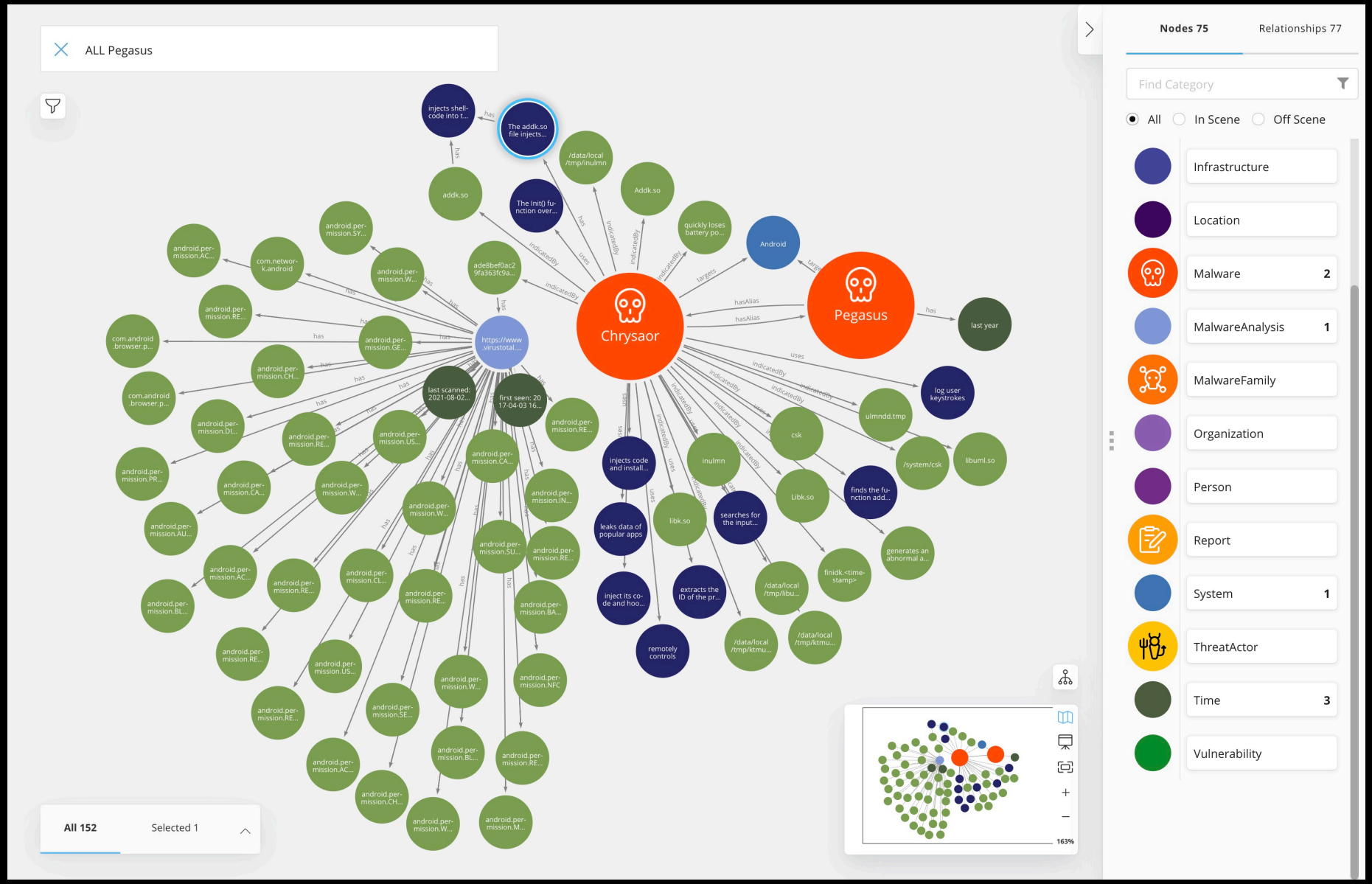
OpenCTI

knowledge graph generation

Ongoing Research
Knowledge Graphs for capturing Threat Intelligence



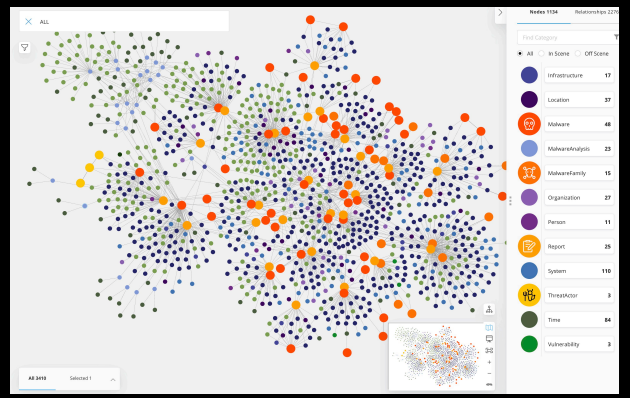

MALWARE RELATED TO Zitmo
FakeToken
Android/Eti-nu
FakeInstaller
Chrysaor
Pegasus
Acecard
Android.Fak-eInstaller
Android/i Banking.B
Android/Fak-eBankDr...
Android/Bad Inst.A
Linux/Exploi-t-Lotoor
Android
Android/Spy SMS
SpyLocker
Flash Player
HTTP
SpyEye
Joker malware
Android ban-king Troj...
Android/Spy Locker
Android/Ra-nsom.El...
FakeInstaller .S
Android/Phi-mSms.A
social engineering
Android/Leif Access.A
Zitmo
Android/Mal Bus
Joint PC-mo-bile attack
Mobile bank-ing Troja...
Android/Clic-ker.G
Android/Foul Goal.A
Android/Leif Access
Google Play
Spitmo
Zeus for Android
LeifAccess
All 71
Selected 1
Nodes 36
Relationships 35
Find Category
All
In Scene
Off Scene
Infrastructure 1
Location
Malware 24
MalwareAnalysis
MalwareFamily 6
Organization
Person
Report
System 2
ThreatActor
Time
Vulnerability
162%


ALL Pegasus
Nodes 75
Relationships 77
Find Category
All
In Scene
Off Scene
Infrastructure
Location
Malware 2
MalwareAnalysis 1
MalwareFamily
Organization
Person
Report
System 1
ThreatActor
Time 3
Vulnerability
Chrysaor
Pegasus
Android
Addk.so
The addk.so file injects...
injects shell-code into t...
addk.so
The Init() function over...
/data/local /tmp/inulmn
quickly loses battery po...
ade8bef0ac2 9fa363fc9a...
https://www .virustotal....
last scanned: 2021-08-02...
first seen: 2017-04-03 16...
last year
log user keystrokes
ulmndd.tmp
/system/csk
libuml.so
csk
inulmn
Libk.so
libk.so
injects code and install...
leaks data of popular apps
inject its code and hoo...
extracts the ID of the pr...
searches for the input...
finds the function add...
generates an abnormal a...
finidk.<time-stamp>
/data/local /tmp/libu...
/data/local /tmp/ktmu...
/data/local /tmp/ktmu...
remotely controls
All 152
Selected 1
163%


Vultur
reached thousands of dow...
connect to the same
android trojan
Alien
data leakage
MITRE T1475
collecting contacts
banking trojan
Toddler
Anatsa
Gustuff
Teabot
READ_CONTA...
sends bots the comm...
command
redirects the target
verify if new bots can send
sending SMS
convinces
botnet
smishing SMS ca...
access to a consid...
FluBot gang
typically sent by some...
spreading
Dutch
FedEx
German
Correos
Deutsche Telekom
late 2020
Flubot
Polish
German
Android
Steal contacts
applicati...
SMS spammi...
spamming
increase the spr...
SMS exfiltrati...
hash busting
convince targets to
utilizes social engin...
query the comm...
Polish texts to Polish
social enginee...
sending of smishi...
informati...
acquire new bots
circumv...
access to hundr...
sent SMS with Dutch texts
Flubot operators
changing their sm...
mechani...
switch the theme of their
hacked websites
change the links in these
keep out security rese...
changing their sm...
change the links in these
switch the theme of their
implement
smishing SMS ca...
malware
Teabot
Toddler
C2 server
forward the target to the
host a heavily obfusc...
contact another server
generate the lure
convince victim in
accessib...
payload is downl...
Google Play dropper
PDF scanners
target only regions of th...
not every device that
100, 000 install...
RAT and semi-...
keyloggi...
possess the claimed
asks the victim to grant Acc...
dropper will decide whether
making their apps look le...
January 2021
installed on the device
perform classic overlay
Anatsa
June 2021
6
perform actions on the vic...
app for scanning doc...
updating its list of
steal credenti...
sending informa...
makes a request towards
large numbers of posi...
upon the start of inst...
after installat...
QR code scanners
moving from region
service is started to che...
cryptocu...
spreading
Europe
Accessi...
Cabass...
dropper campai...
automate and inst...
Google Play
introduci...
download and inst...
sporting a dropper C2 ba...
decides whether to pro...
C2
Brunhilda
Ermac
sends a registra...
gRPC protocol
Hydra,
device ID, device name,
QR code creator app.
Gymdrop
website is design...
payload is posed as a n...
the user clicks OK
convince victims to
request the permi...
gets its configur...
dropper
November
small malicious footprint
avoid downlo...
requests permiss...
does not request Acc...
focusing on load...
promise to install new w...

RIT

1 2 3



adding context

context in < > context out

adding context

Provenance
Reasoning
Trust

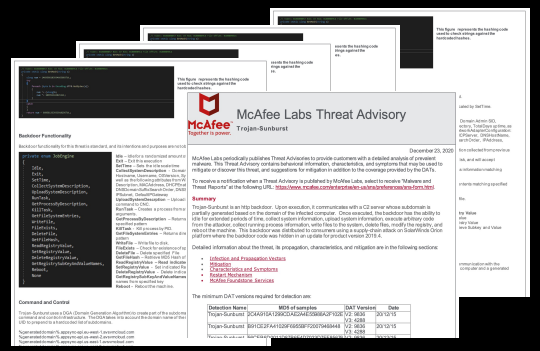
adding context

Provenance – wikidata, dbpedia
Reasoning
Trust

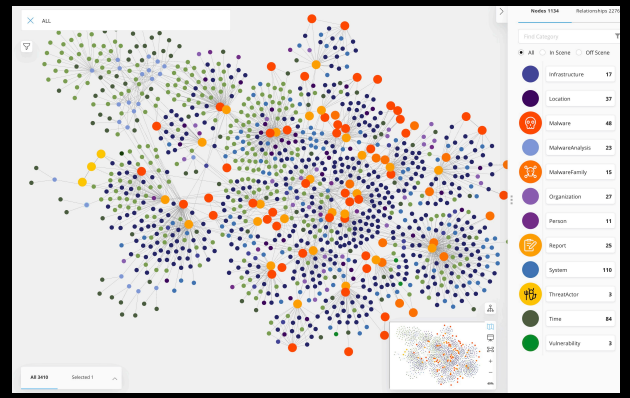
adding context

Provenance – Wikidata, dbpedia
Reasoning – Ontology, KG
Trust

RIT



1 2 3

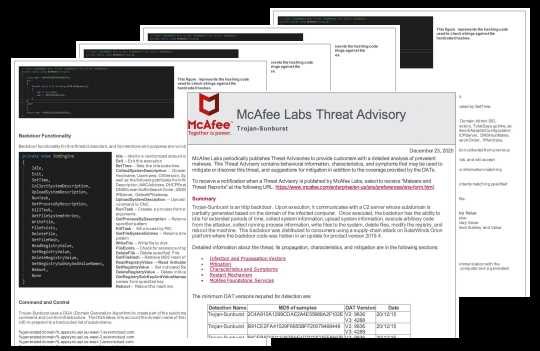


1. ontology

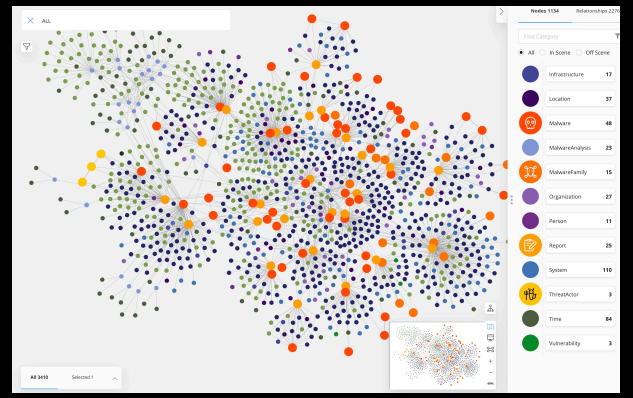
2. named entity recognition (ner), relation extraction (re)

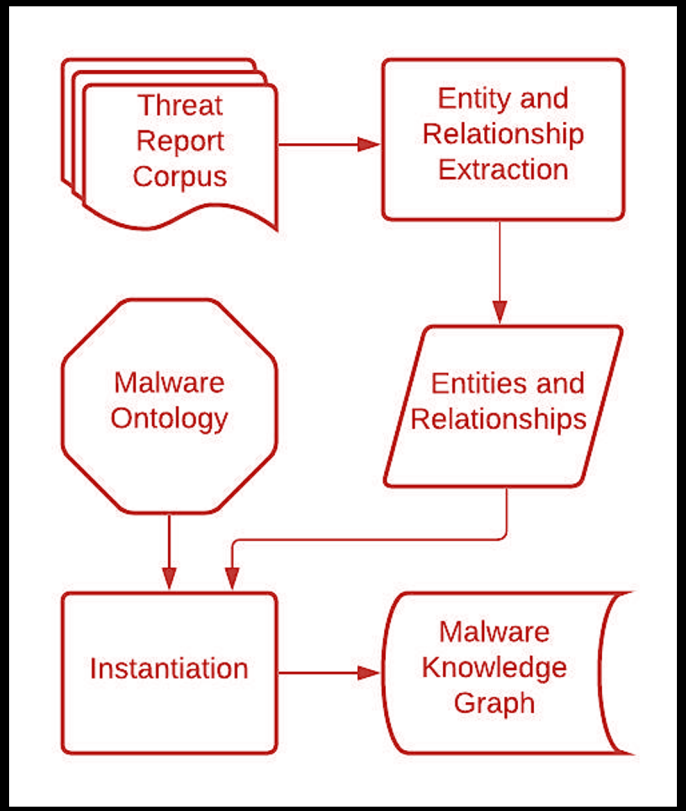
3. disambiguation, co-referencing, de-duplication

RIT

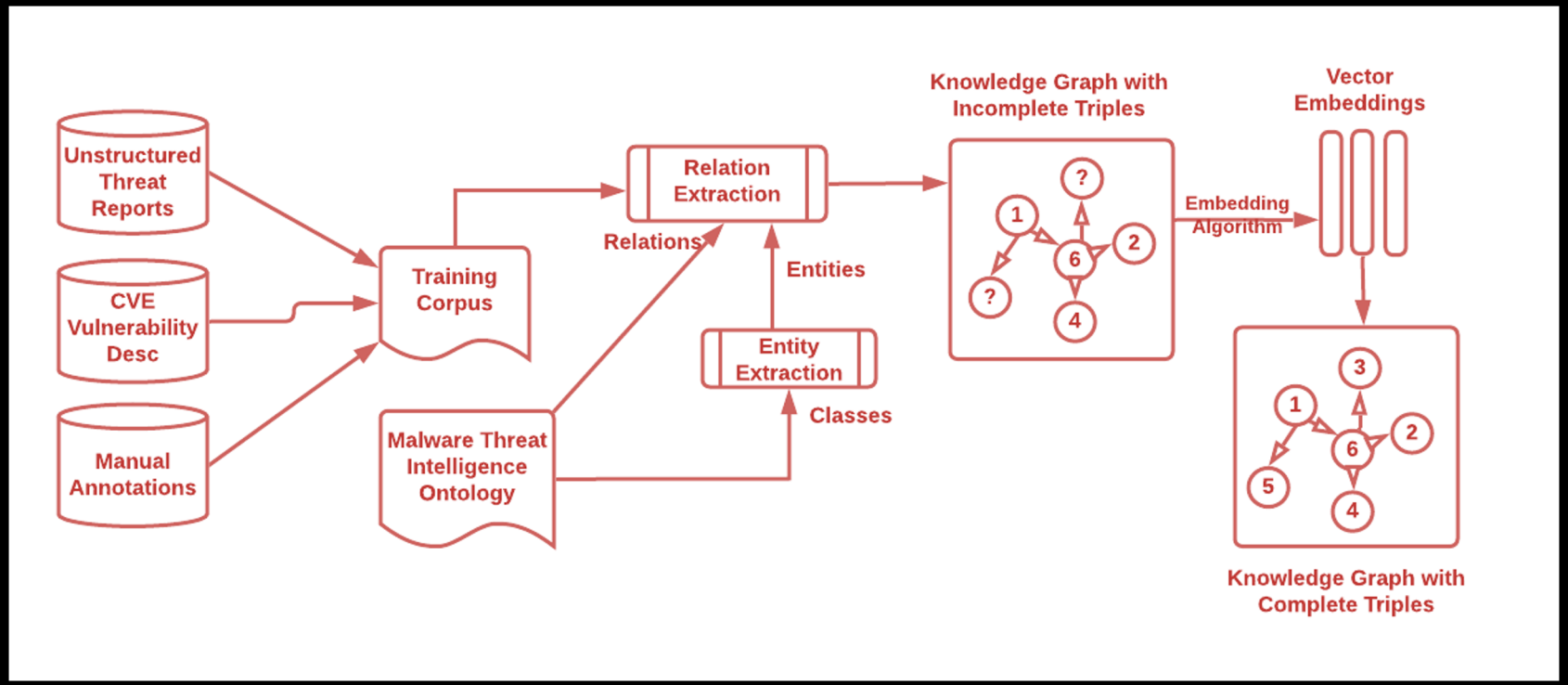

McAfee Labs Threat Advisory
Trojan-Sunburst

1 2 3




Threat Report Corpus
Entity and Relationship Extraction
Malware Ontology
Entities and Relationships
Instantiation
Malware Knowledge Graph

MalKG for triaging Threats



MalKG for triaging Threats

Table 6: Detailed result of Entity prediction case studies

	Case study 1: Predicting a malware family $\langle intel-update[.]com, indicates, ? \rangle$		Case study 2: Predicting attack target $\langle$"coronavirus-themed attacks", $targets, ?\rangle$	
Rank	Predicted entity	Confidence score	Predicted entity	Confidence score
1	A malware hash[13]	0.5769	**India**	**0.8683**
2	**Stealer**	**0.5694**	recorded future	0.8634
3	A malware hash[14]	0.5679	issuemakerslab	0.2972
4	Gholee	0.5679	google	0.1873
5	200.63.46.33	0.5668	China	0.1662
6	26978_ns2._aeroconf2014[.]org	0.5662	maas	0.1316
7	A malware hash[15]	0.5620	United Arab Emirates	0.1173
8	Capstone Turbine	0.5602	Kaspersky	0.0836
9	2012/06/06	0.5592	italy	0.05486
10	Google Hack Attack	0.5566	portugal	0.04999

Bold text denotes the true entity for the corresponding test triple

Parting Notes

Key Take Away – Context is next

Automating Context while using ML is challenging.

Next Research Frontier