

Anupam Joshi

Oros Family Professor and Chair  
Director, Center for Cybersecurity  
[joshi@umbc.edu](mailto:joshi@umbc.edu)



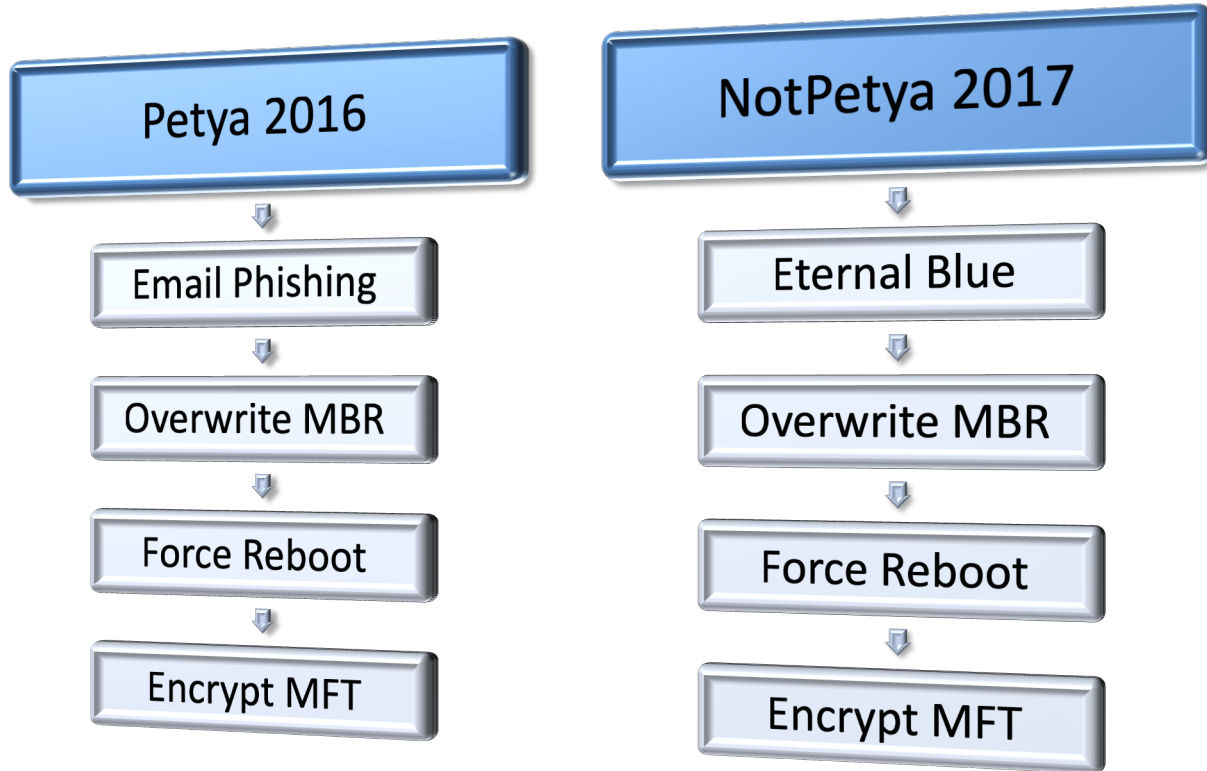
## • Limitations:

- Point based solutions
- Difficulty detecting
  - newly published attacks (zero-day)
  - complex attacks (ex: Advanced Persistent Threats)

## • Watchstanding

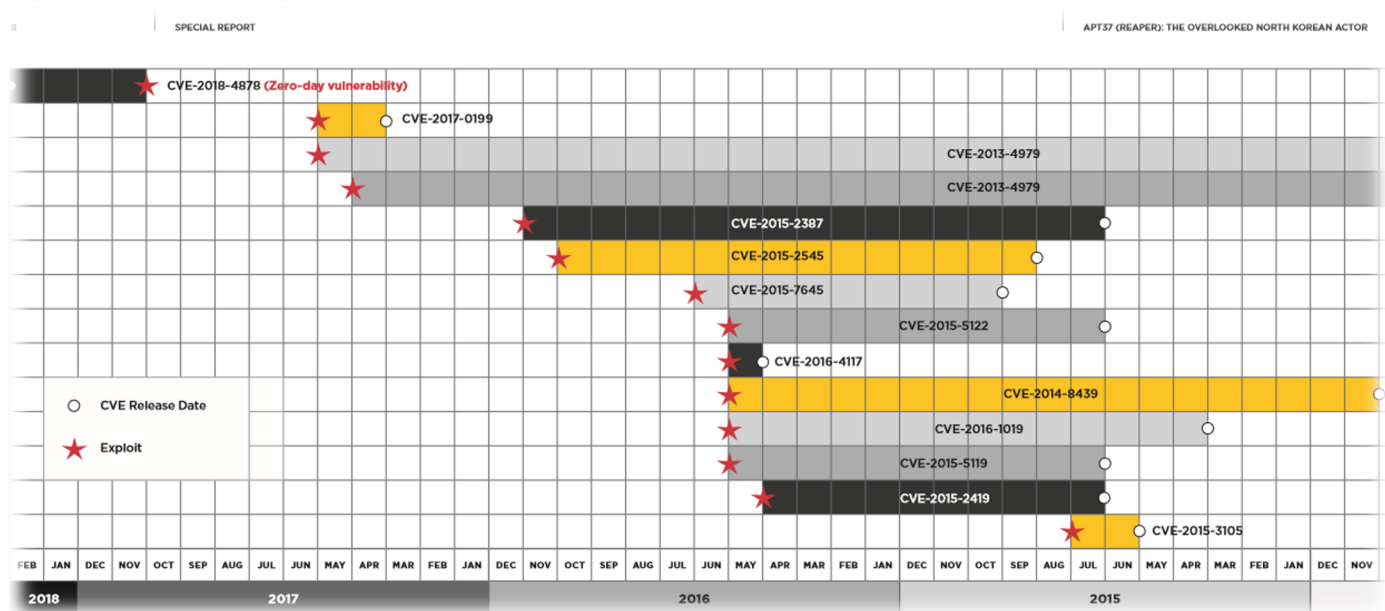
- SIEMs mostly dashboard information
- Forensics



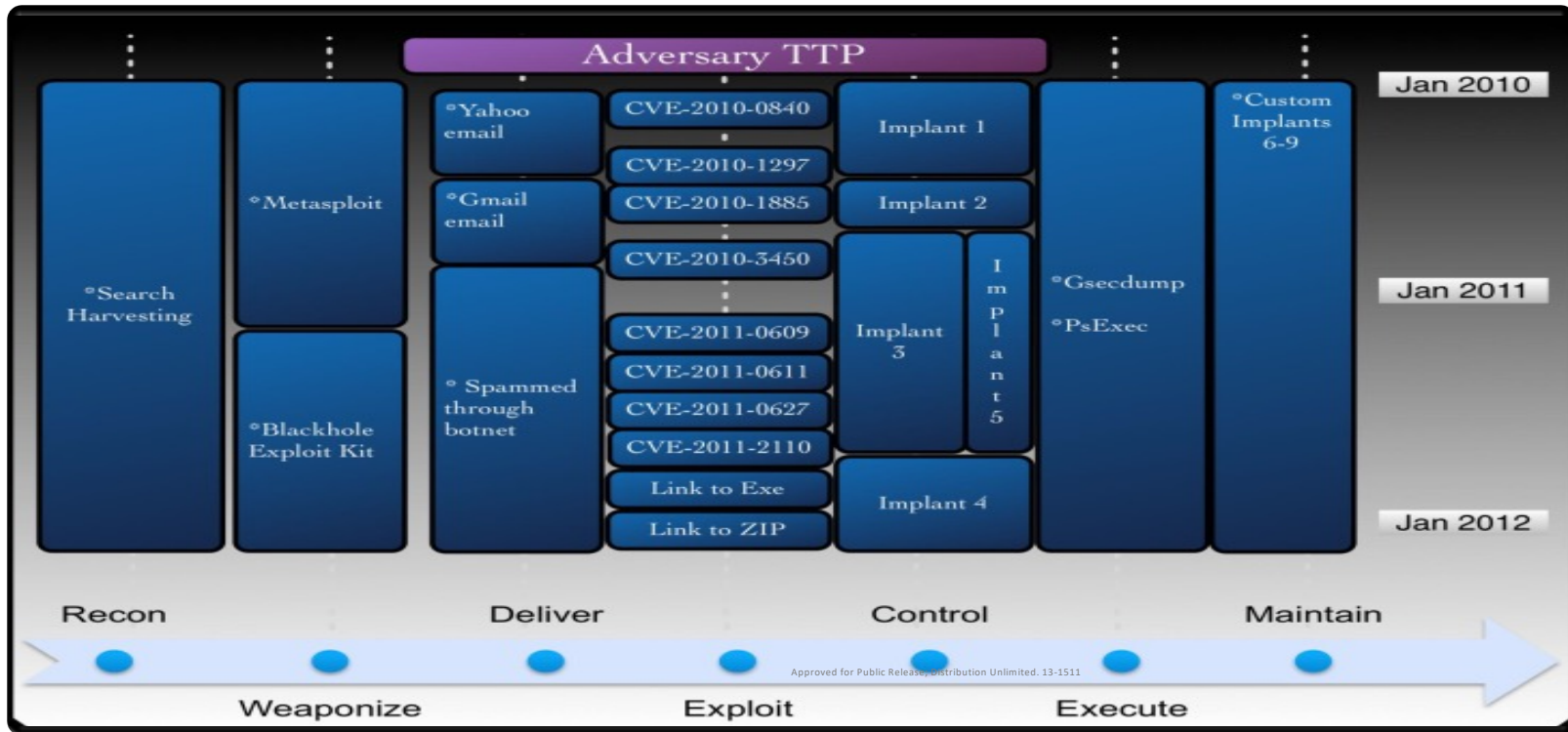


# UMBC Advanced Persistent Threats (APT)

- Long & Multi-step Process - Different vulnerabilities exploited
- APT37 (REAPER)



# UMBC Adversary TTPs and the Kill Chain





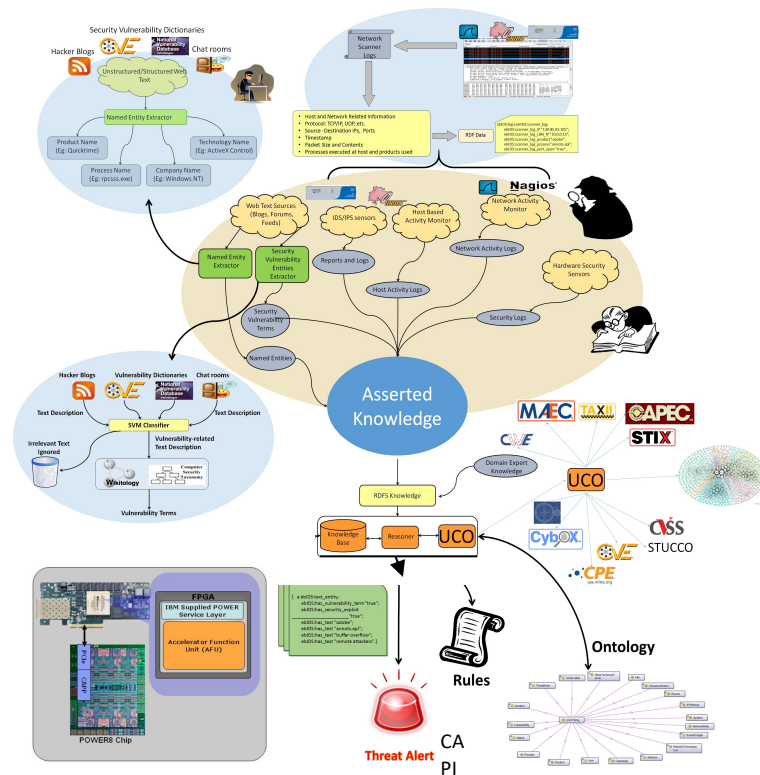
- Focused on our internal systems
- Point Defense solutions
- Assume Flaws are fixable
- Unaware of external environment
- That's not how a good batsman plays

We are too inward looking



- A good player sees the game as it evolves – not just their own actions, but also how others are moving

- Most IDS systems are point-based & driven by known signatures
- Our system maps multiple traditional and novel sensors to a common ontology
- ***Specifically, can extract information from textual sources***
- ***Reasons over the resulting knowledge***
- Detecting possible intrusions missed by standard systems





# UMBC Unified Cybersecurity Ontology

## *Unified Cybersecurity Ontology (UCO)*



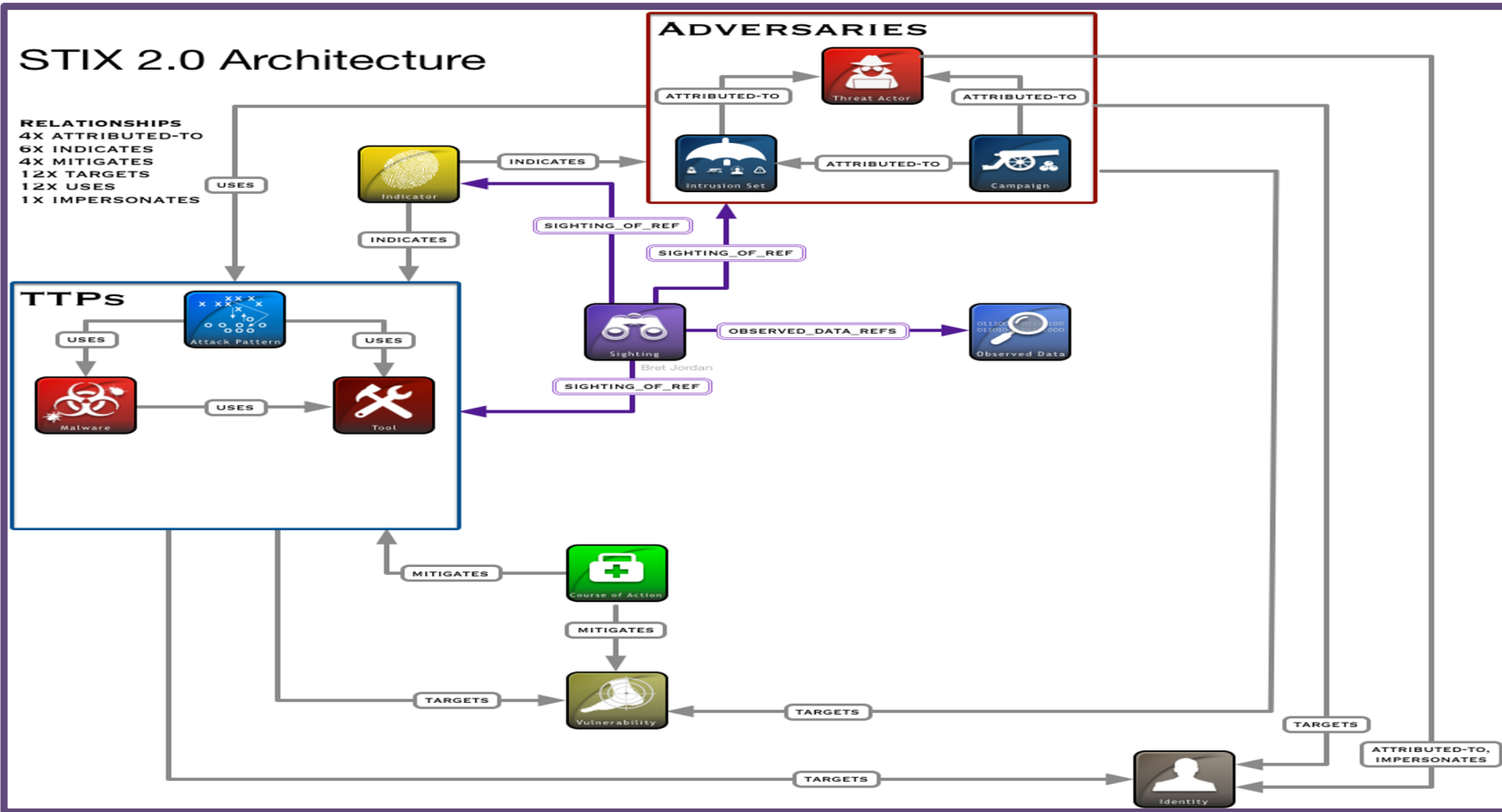
ACCL Architecture



UCO

## STIX 2.0 Architecture

**RELATIONSHIPS**  
 4X ATTRIBUTED-TO  
 6X INDICATES  
 4X MITIGATES  
 12X TARGETS  
 12X USES  
 1X IMPERSONATES



# Detecting Intrusions using Policies, Context, and Reasoning

1. Detect *potential* new vulnerabilities from (Dark) Web descriptions, blogs, tweets, and discussions, extract information and map to CyberSecurity Knowledge Graph (CKG) [\[lebiq.org/p/540\]](http://lebiq.org/p/540)
2. Recognize context of system and *potential* attacks and intrusions in data from low level intrusion detection systems and map to CKG [\[lebiq.org/p/63\]](http://lebiq.org/p/63)
3. Integrate and reason over results of (1) and (2) to identify *actual* attacks [several recent papers]



- Can you represent “rules” in an Analyst’s brain, and reason over them with facts ?
  - Background knowledge/ Intelligence – *New Vulnerabilities have been discovered in a software, Household machines with DHCP addresses are often compromised and used as Zombies, ...*
  - Observed State of the System – *Software installed, processes running, network traffic statistics and connections, ...*
  - Organizational Policies – *People in Group X should generally have no need to receive email’s from contract travel agency, ...*
  - **IF** *an email from travel agency with attachment went to a person in group X and a process is running with their PID where vulnerabilities have been discovered and it makes connections to previously unvisited hosts in the DHCP range of an ISP* **THEN** *an attack might be occurring*

# UMBC Abductive/Inductive Reasoning

## Rule in KB

```
running(IE8, t1) ^ web_site(x) ^ first_visit(X, t) ^  
negative_reputation(x) ^ connection_to(y, t2) ^ zombie(y) ^ t2 > t1  
→ possible_attack(t2)
```

### **Abduction:**

Reason from missing antecedent to possible new vector

Maybe user is running Firefox 45.2.0 but all other conditions are met

Posit vulnerability in Firefox 45.x

### **Induction:**

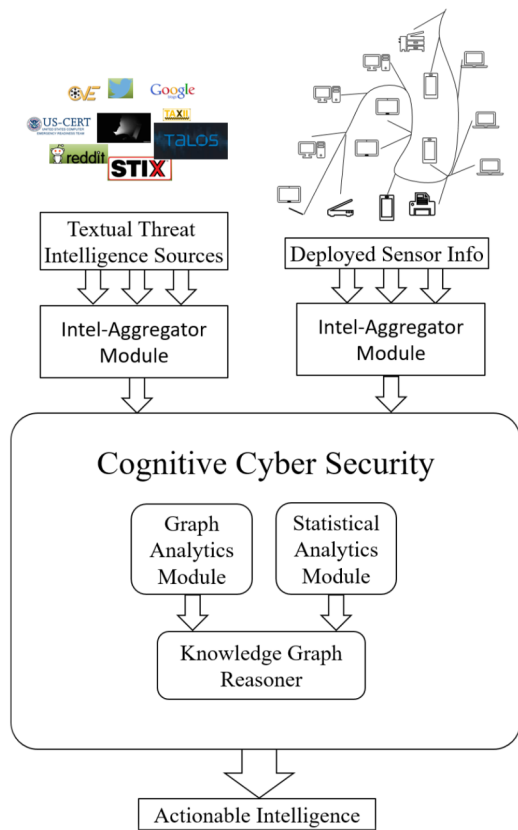
Gather data across enterprise

Measures of certainty (e.g., Firefox 45.x vulnerability is 84% certain)

Establish ranges of previously unknown zombines

# UMBC Collaborative Cognition

- Acquiring Knowledge
  - A new ransomware “Wannacry” uses malformed SMB to get access to a victim
- Representing Experience (about Ransomware)
  - Download/Upload sw/keys from external servers
  - Ransomware modifies sensitive files
- Ingesting Sensed data
  - Malformed SMB network activity, Network download activity, File modification.
- Reasoning
  - In light of what I read and what I know, the sensed data could reflect Wannacry activity
  - Mitigate this by ....



# Test Scenario: Simulated Ransomware



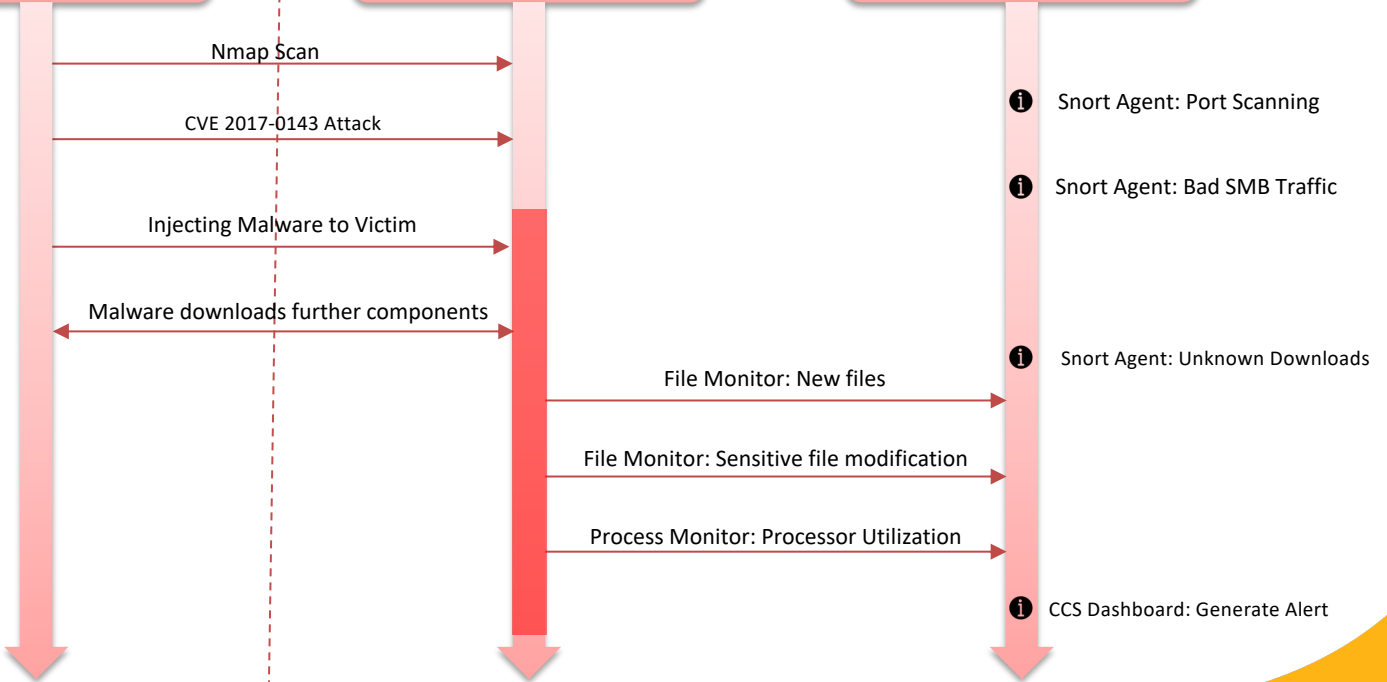
Attacker

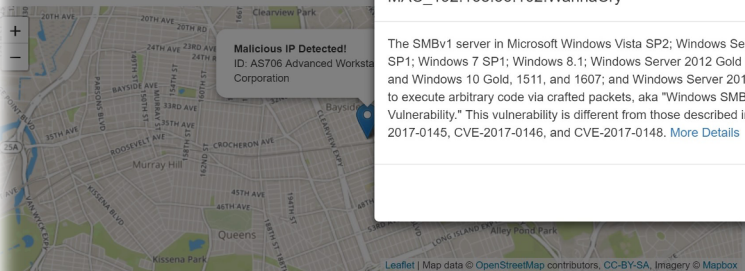


Victim



CCS Monitor





**Malicious IP Detected!**  
ID: AS706 Advanced Worksta Corporation

**MAC\_192.168.56.102:WannaCry**

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148. [More Details](#)

Close

Potential Attackers	
#	Attacker IPAddress
1	192.168.56.102
2	192.168.56.101

Network Alerts				
#	Time	ID	Message	Class
1	2017-09-18T10:55:56.001250	1:5000002:1	Windows BAT file Download	Executable_code_was_detected
2	2017-09-18T10:55:55.931395	1:5000002:1	Windows BAT file Download	Executable_code_was_detected
3	2017-09-18T10:55:55.862413	1:5000002:1	Windows BAT file Download	Executable_code_was_detected
4	2017-09-18T10:56:20.767527	1:5000002:1	Windows BAT file Download	Executable_code_was_detected
5	2017-09-18T10:55:56.024865	1:5000002:1	Windows BAT file Download	Executable_code_was_detected
6	2017-09-18T10:56:55.929123	1:5000002:1	Windows BAT file Download	Executable_code_was_detected

System Alerts		
#	File	Action
1	c:\Users\attack\Thunderbird\config.txt	isDeleted
2	c:\Users\attack\Thunderbird\config.txt.enc	isModified
3	c:\Users\attack\Thunderbird\EmailBackup_mail.enc	isCreated
4	c:\Users\attack\Thunderbird\config.txt.enc	isCreated

Inferred Warnings	
IP Address	Notes
192.168.56.102	SuspiciousDownloadExecute
192.168.56.102	SuspiciousExecute
192.168.56.102	SuspiciousDownload
192.168.56.102	SuspiciousProtocol
MAC_192.168.56.102	SuspiciousFileModification

**About us**

Accelerated Cognitive Cybersecurity Lab (ACCL)  
University Of Maryland Baltimore County (UMBC)

Copyright © 2017 @ UMBC

**Information**

The project is part of UMBC's cybersecurity research to leverage cognition to improve threat detection. UMBC is part of IBM's Cognitive Horizon's Network and the project



We are developing systems that can extract cybersecurity relevant information from text

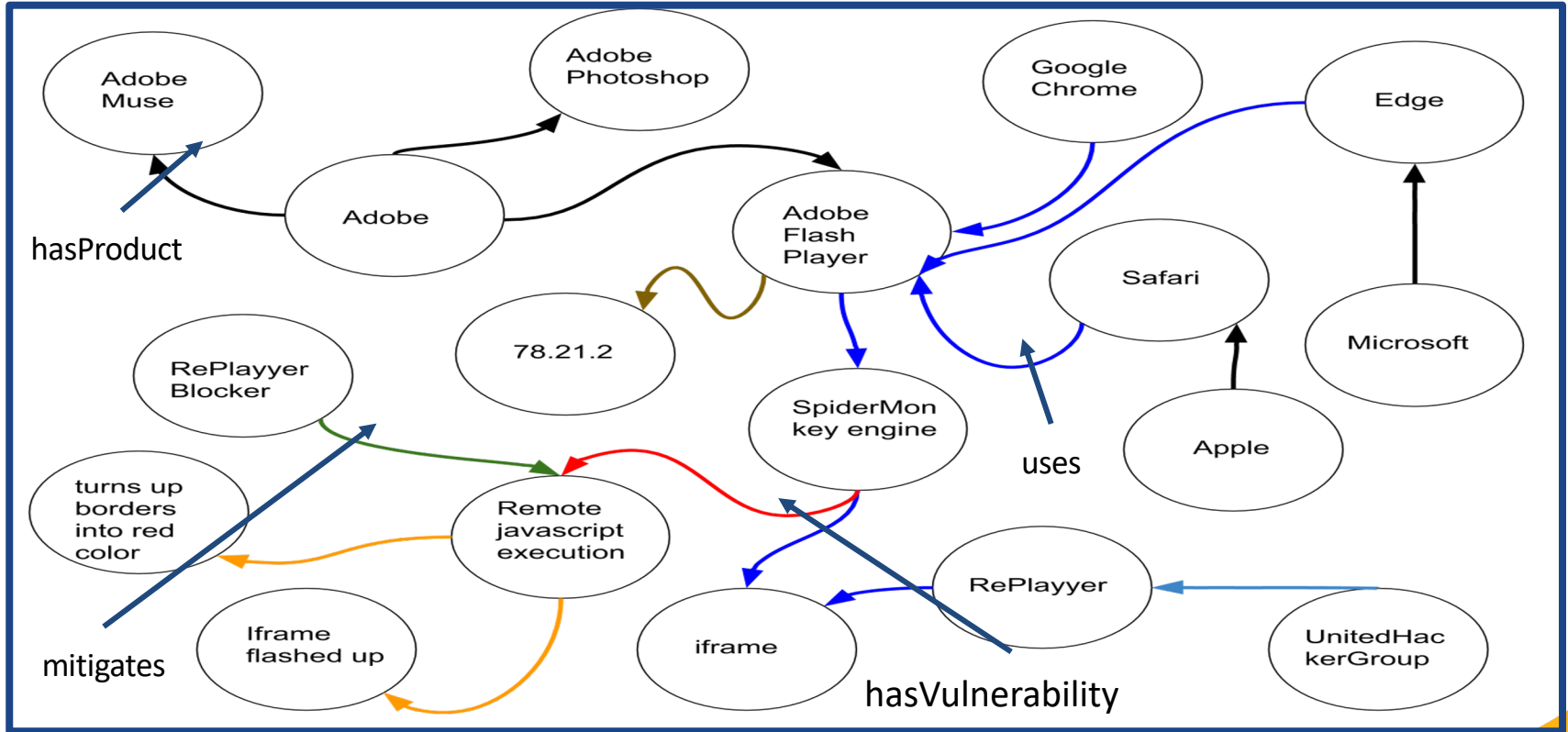
- **Find** entities and their properties, relations & events
- **Represent** in a generic knowledge base with *proven-ance* and *probabilities*
- **Group** entities & events referring to the same things
- **Link** these to external background knowledge bases (e.g., Wikipedia) where possible
- **Reason** over results to improve and assess accuracy, coherence and trustworthiness

- Structured & unstructured
  - “The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets”
- From a human security Analyst
  - “Ransomwares try to encrypt files”
  - “They might download some encryption software”
  - “They might upload/download keys”

## Intelligence Sources



# UMBC Illustration of a Cybersecurity KG



The Naikon group used mostly spear-phished documents for the attacks, with CVE-2012-0158 exploits that dropped the group's signature backdoor.

While many of these attacks were successful, at least one of the targets didn't seem to like being hit, and instead of opening the documents, decided on a very different course of action.

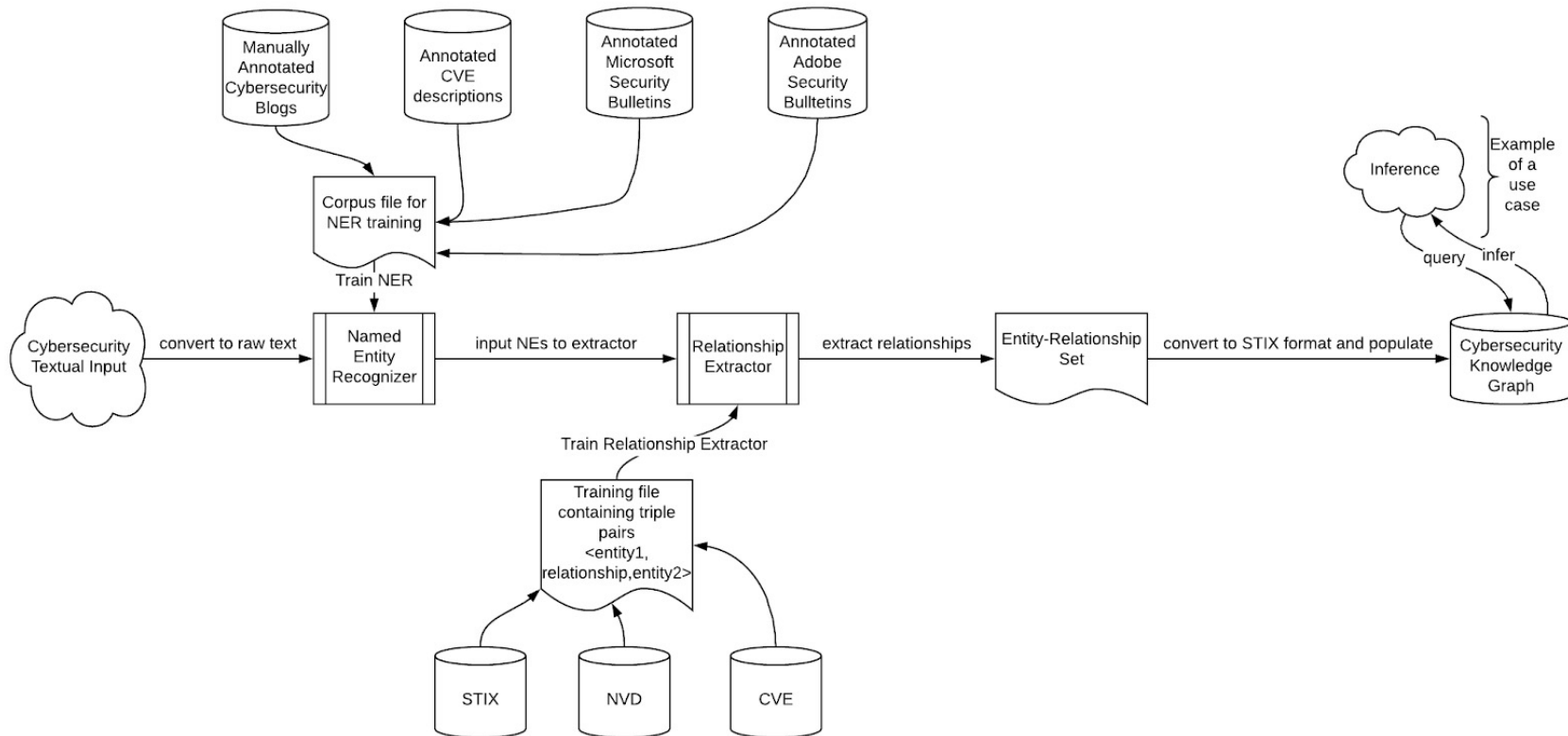
### The empire strikes back

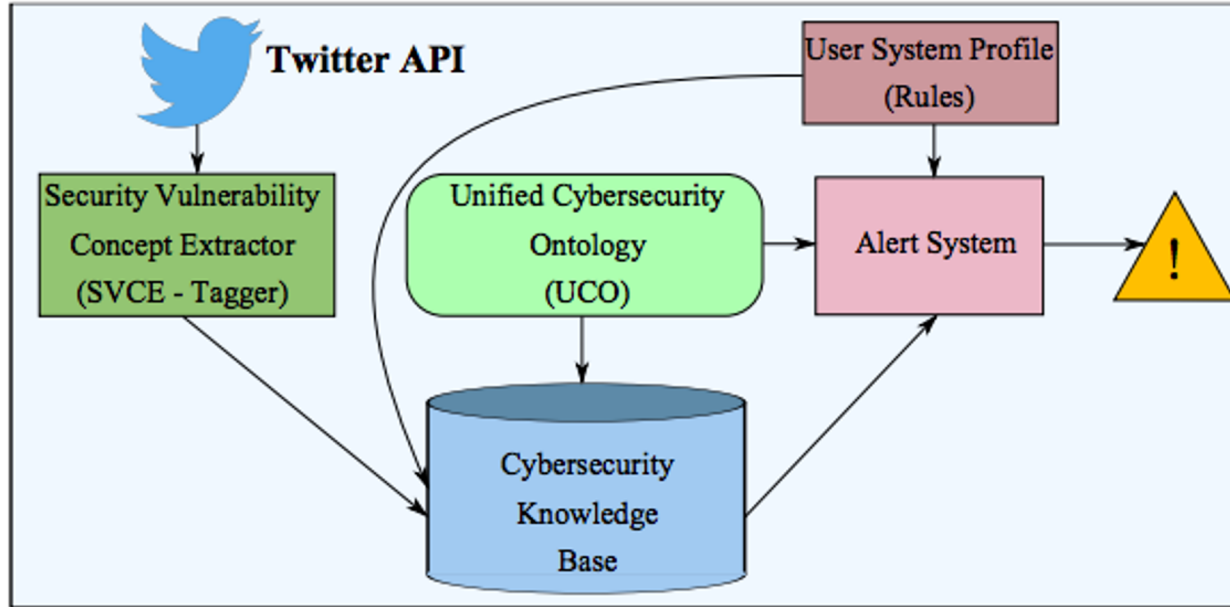
Here's a question - what should you do when you're receiving a suspicious document from somebody you don't know, or know very little? Choose one:

- Open the document
- Don't open the document
- Open the document on a Mac (everybody knows [Mac's don't get viruses](#))
- Open the document in a virtual machine with Linux

Based on our experience, most people would say 2, 3 or 4. Very few would open the document and even fewer would actually decide to test the attacker and verify its story.

But this is exactly what happened when one of the Naikon spear-phishing targets received a suspicious email. Instead of opening the document or choosing to open it on an exotic platform, they decided to check the story with the sender:





# Why can't we use an NLP toolkit out of the box

Remote Login Service (RLS) 1.0.0 does not properly clear account information when switching users, which might allow physically proximate users to obtain login credentials.

Remote **Login Service** (RLS) 1.0.0 does not properly clear account information when switching users, which might allow physically proximate users to obtain login credentials.

	ORGANIZATION
--	--------------

- Remote Login Service (RLS) 1.0.0 does not properly clear account information when switching users, which might allow physically proximate users to obtain login credentials.



- Remote Login Service (RLS) 1.0.0 does not properly clear account information when switching users, which might allow physically proximate users to obtain login credentials.

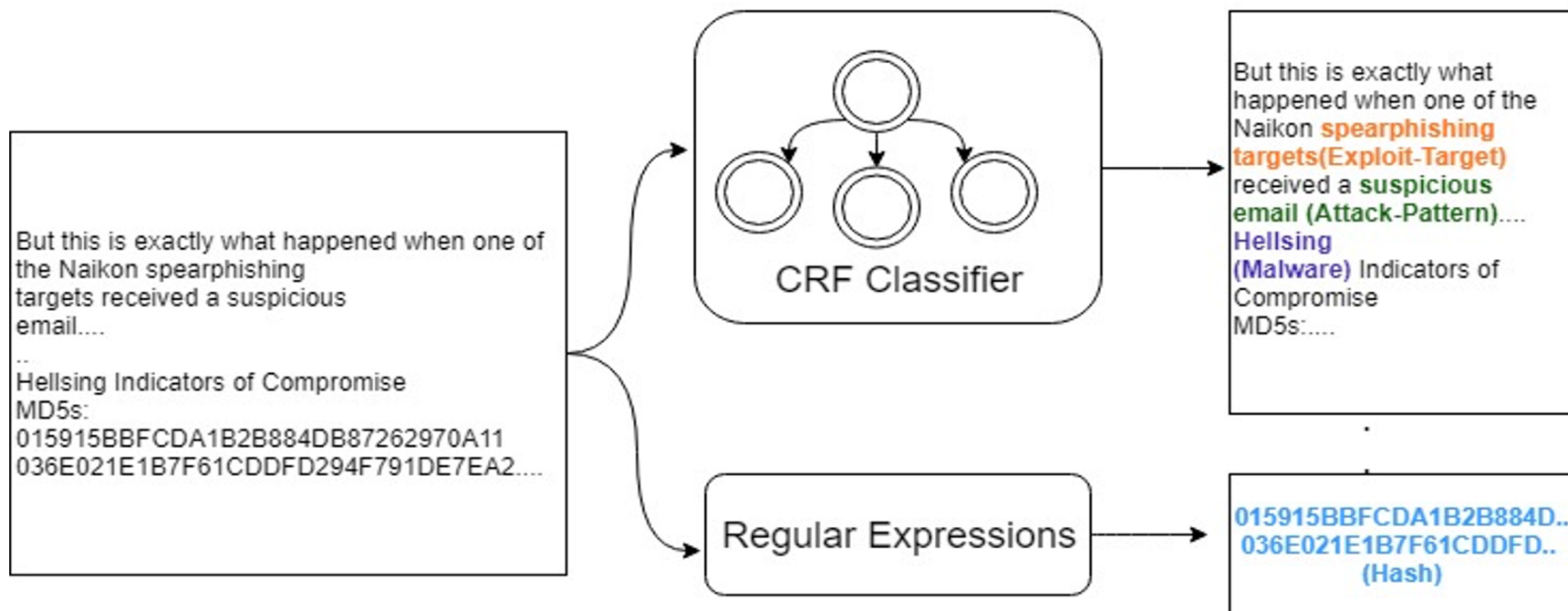
	Product
	Version
	Exploit Target
	Weakness





Classes in  
NER

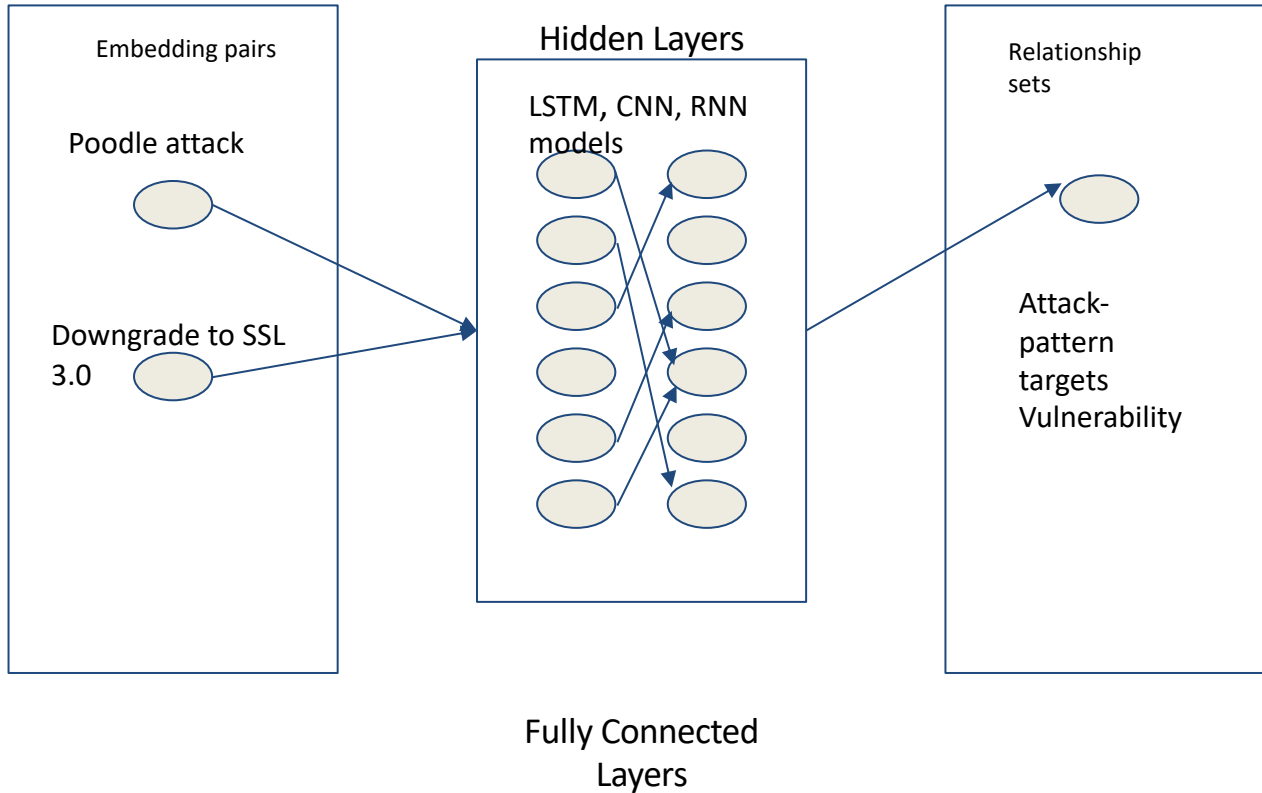
Named Entities	
Exploit Target	Attack Pattern
File Names	Campaign
Version	Course-of-Action
Weakness	Indicator
Software	Intrusion-Set
Vulnerability	Malware
IP Addresses	Observed Data
SHA encryptions	Tool



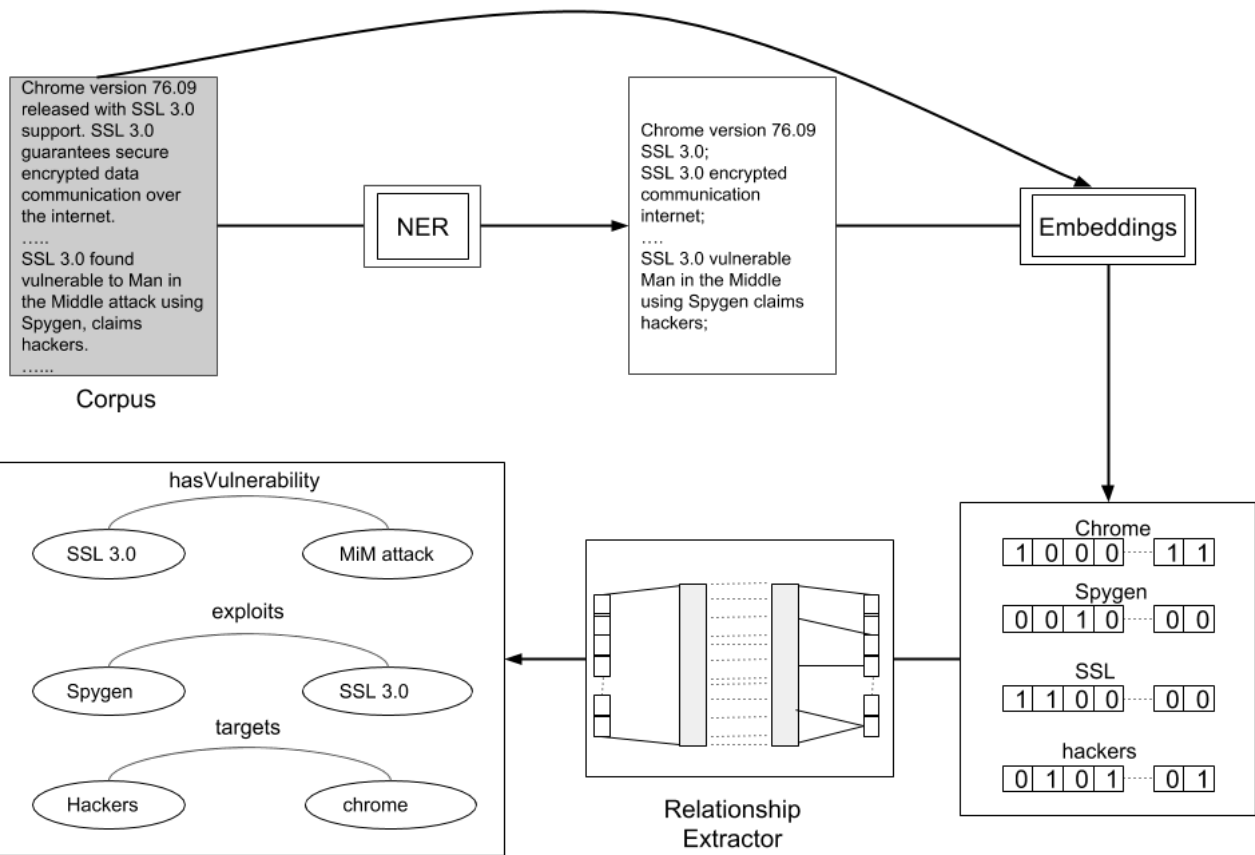
- We have annotated 54,240 words from CVE, Microsoft Security Bulletin, Adobe Security Bulletin, and blogs
- Training set - 48,959
- Test set - 5281
- Average precision - 0.91
- Average recall - 0.92
- Average F-1 0.91

# Relationship Set

- CourseOfAction **hasCost** StatementType
- Vulnerability **hasMitigation** CourseOfAction
- Attacker **hasRelatedIncident** Incident
- Attack **isLaunchedBy** Attacker
- System **isUnderAttack** Consequence
- Attack-pattern **targets** Vulnerability
- And so on ...



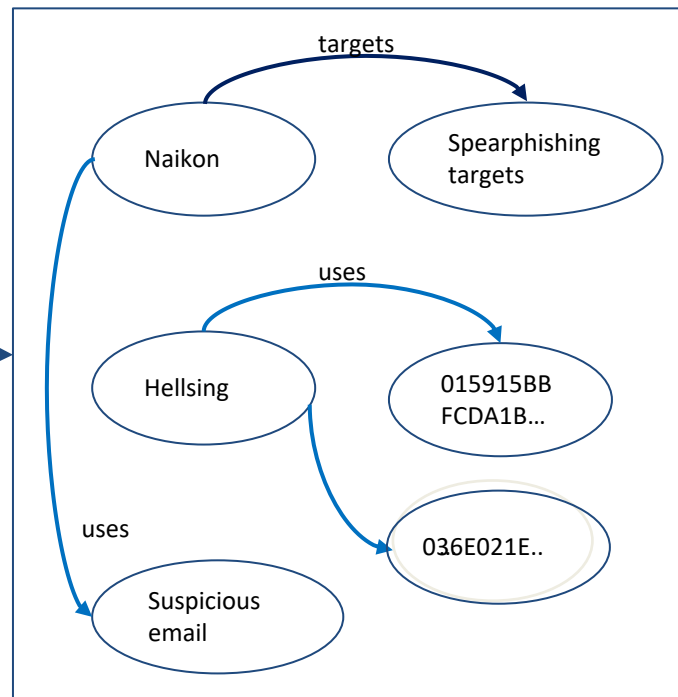
# UMBC Relationship Extractor



But this is what exactly happened when one of the Naikon spearphishing targets received a suspicious email  
.....

Helsing Indicators of Compromise  
**MD5s:** 015915BBFCDA1B2B884DB87262970A11  
036E021E1B7F61CDDFD294F791DE7EA2

Corpus



Prediction

NER is evaluated by averaging on annotated After Action Reports of about 50 sentences per set, 10 times. RelExt is evaluated on CVE, After Action Reports and Triples hosted on our stardog server

	NER	RELEXT
Average precision	0.76	0.89
Average recall	0.76	0.92
Average F-1	0.75	0.90



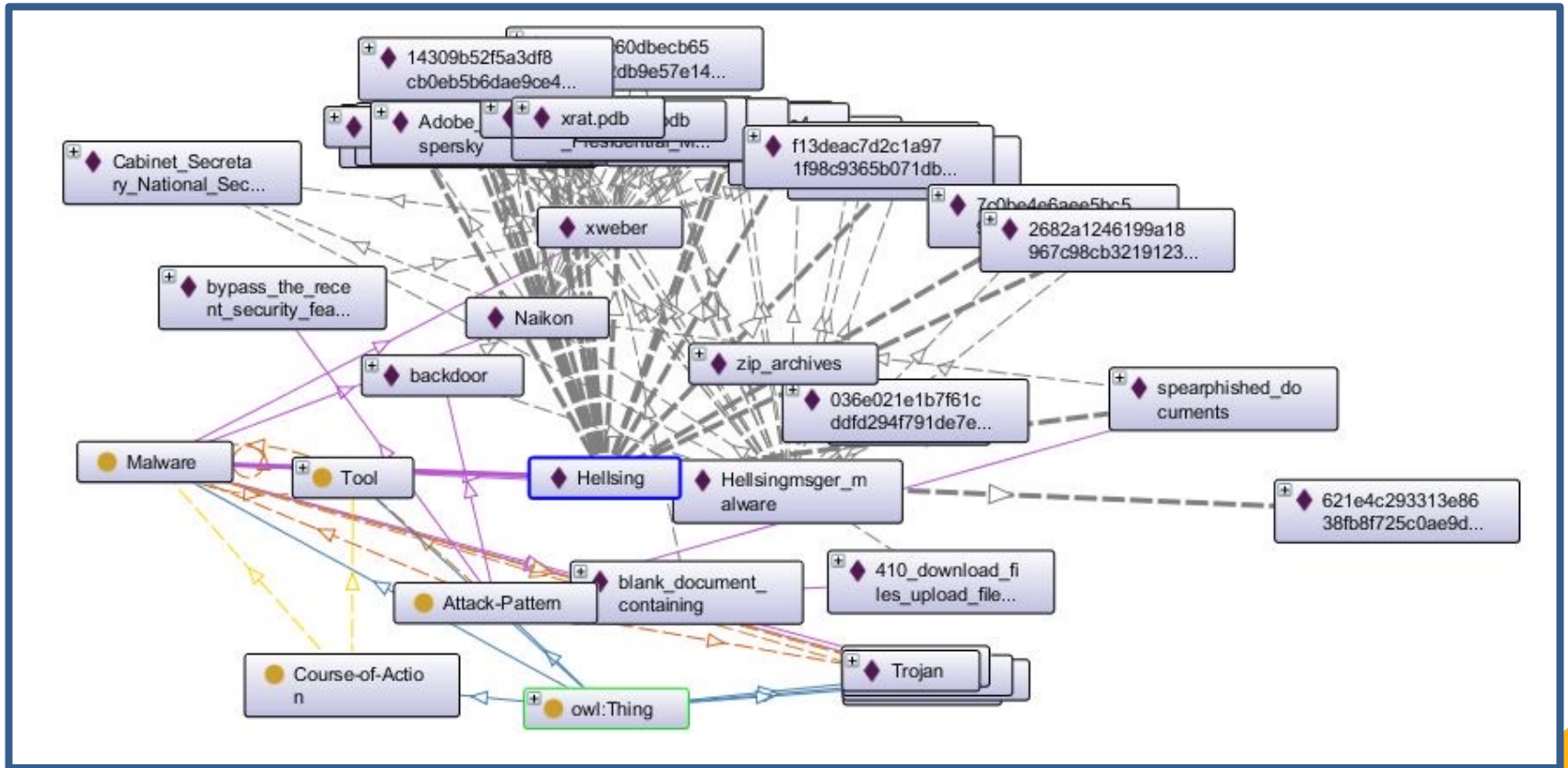
The **Hellsing** series chronicles the efforts of the mysterious and secret Hellsing Organization, as it combats [vampires](#), [ghouls](#), and other [supernatural](#) foes; which makes it perhaps an appropriate name for our group.

In addition to the Hellsing/msger malware, we've identified a second generation of Trojan samples which appear to be called "xweber" by the attackers:

```
etModuleFileNameW 0@LoadLibraryW 0@ExpandEnvironmentStringsW 0vsprintfA USER32.dll
AllocateAndInitializeSid M CheckTokenMembership 0FreeSid ADVAPI32.dll A SHGetFolder
PathW f@GetConsoleCP 0@GetConsoleMode ,0WriteConsoleA 0@GetConsoleOutputCP 0WriteCo
nsoleW 0SetStdHandle A@FlushFileBuffers Z0RaiseException 0SetEndOfFile 0j0
Q \40 0 0 0 H40 P40 X40 0 0 s40 B40 0 xweber_install_uac.exe ?test1@@YAXX
Z ?test2@@YAHXZ
```

"Xweber" seems to be the more recent Trojan, taking into account compilation timestamps. All the "msger" samples we have seen appear to have been compiled in 2012. The "Xweber" samples are from 2013 and from 2014, indicating that at some point during 2013 the "msger" malware project was renamed and/or integrated into "Xweber".

During our investigation we've observed the Hellsing APT using both the "Xweber" and "msger" backdoors in their attacks, as well as other tools named "xrat", "clare", "irene" and "xKat".



## Helsing Indicators of Compromise

### MD5s:

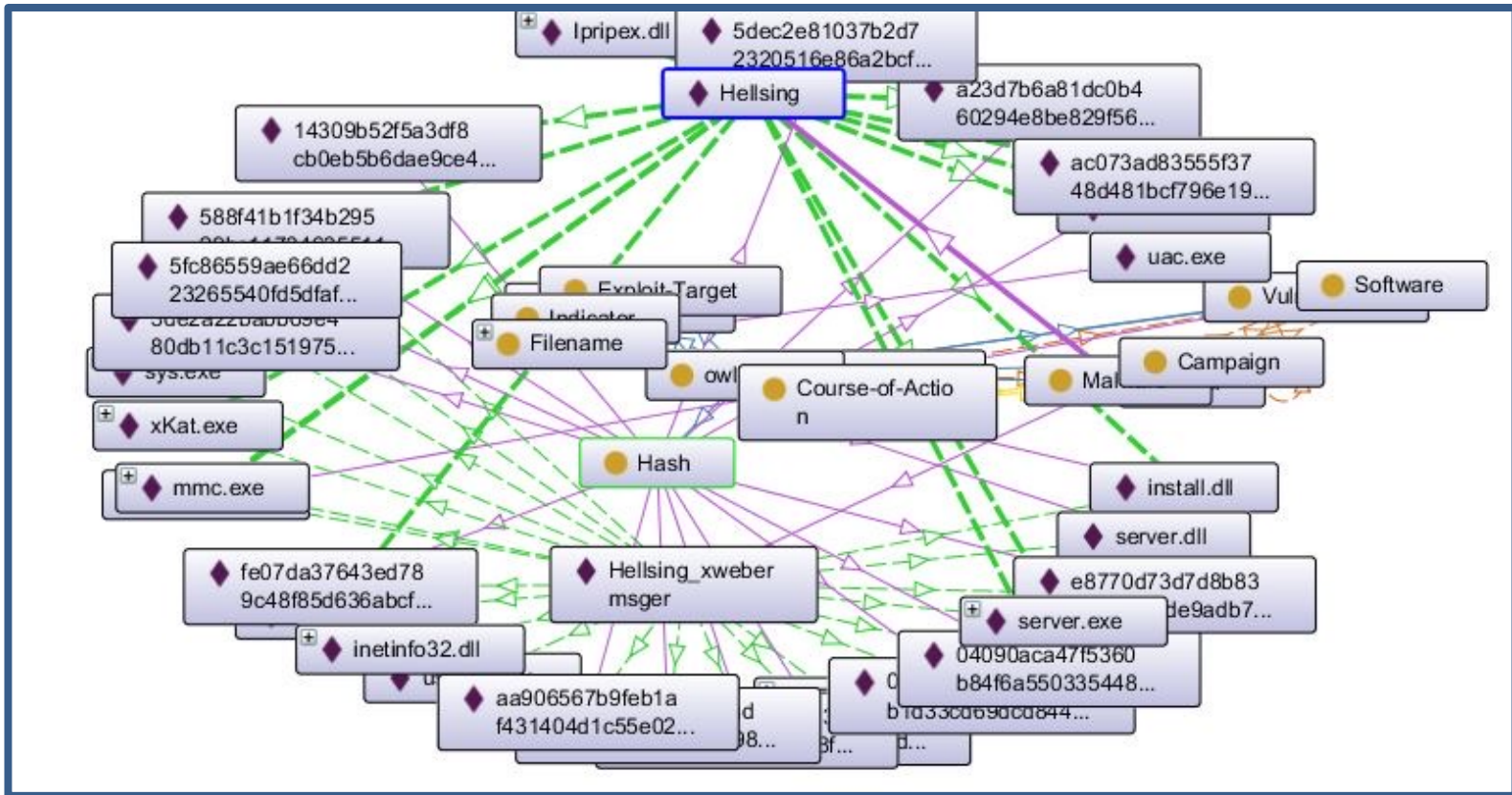
```
015915BBFCDA1B2B884DB87262970A11
036E021E1B7F61CDDFD294F791DE7EA2
04090aca47f5360b84f6a55033544863
055BC765A78DA9CC759D1BA7AC7AC05E
085FAAC21114C844529E11422EF684D1
0BA116AA1704A415812552A815FCD34B
0CBefd8CD4B9A36C791D926F84F10B7B
0CC5918D426CD836C52207A8332296BC
0dfcbb858bd2d5fb1d33cd69dcd844ae
0F13DEAC7D2C1A971F98C9365B071DB9
0FFE80AF4461C68D6571BEDE9527CF74
13EF0DFE608440EE60449E4300AE9324
14309b52f5a3df8cb0eb5b6dae9ce4da
17EF094043761A917BA129280618C1D3
2682A1246199A18967C98CB32191230C
2CCE768DC3717E86C5D626ED7CE2E0B7
```

### Domain registrations:

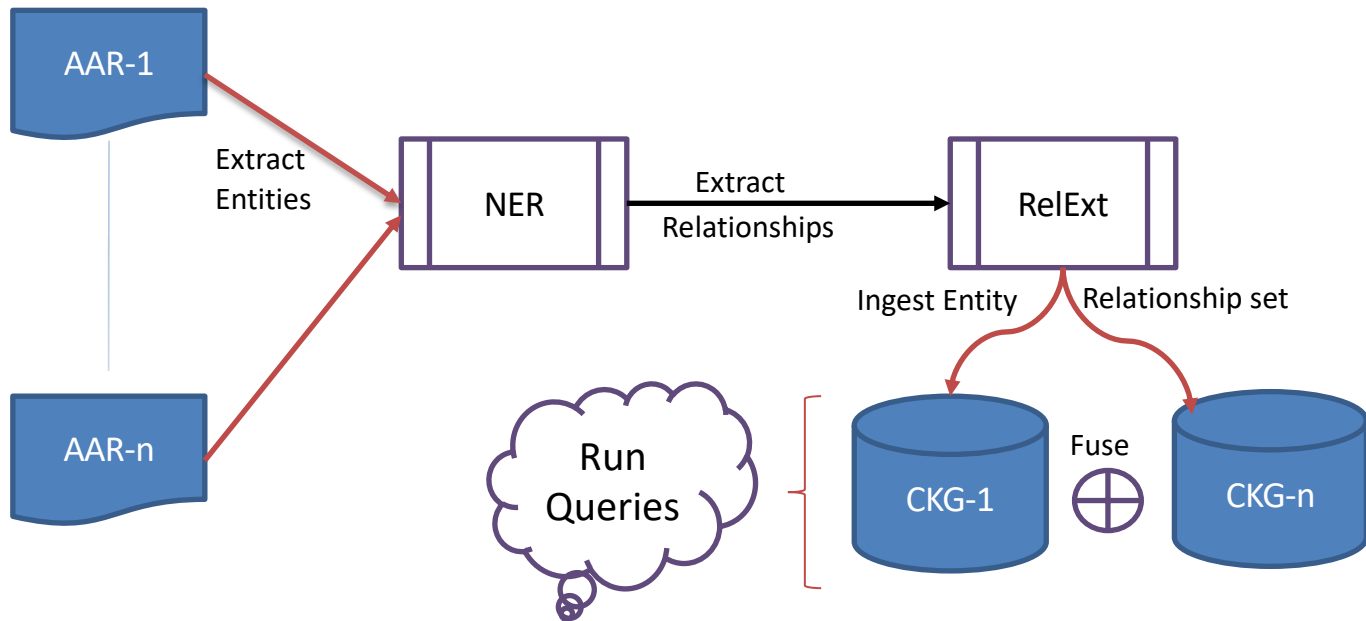
- huntingtomingalls[.]com - [ssdfsdfs@qsdfsq.com](mailto:ssdfsdfs@qsdfsq.com)
- philippinenewss[.]com - [sambieber1990@yahoo.com](mailto:sambieber1990@yahoo.com)
- philstarnotice[.]com - [sambieber1990@yahoo.com](mailto:sambieber1990@yahoo.com)

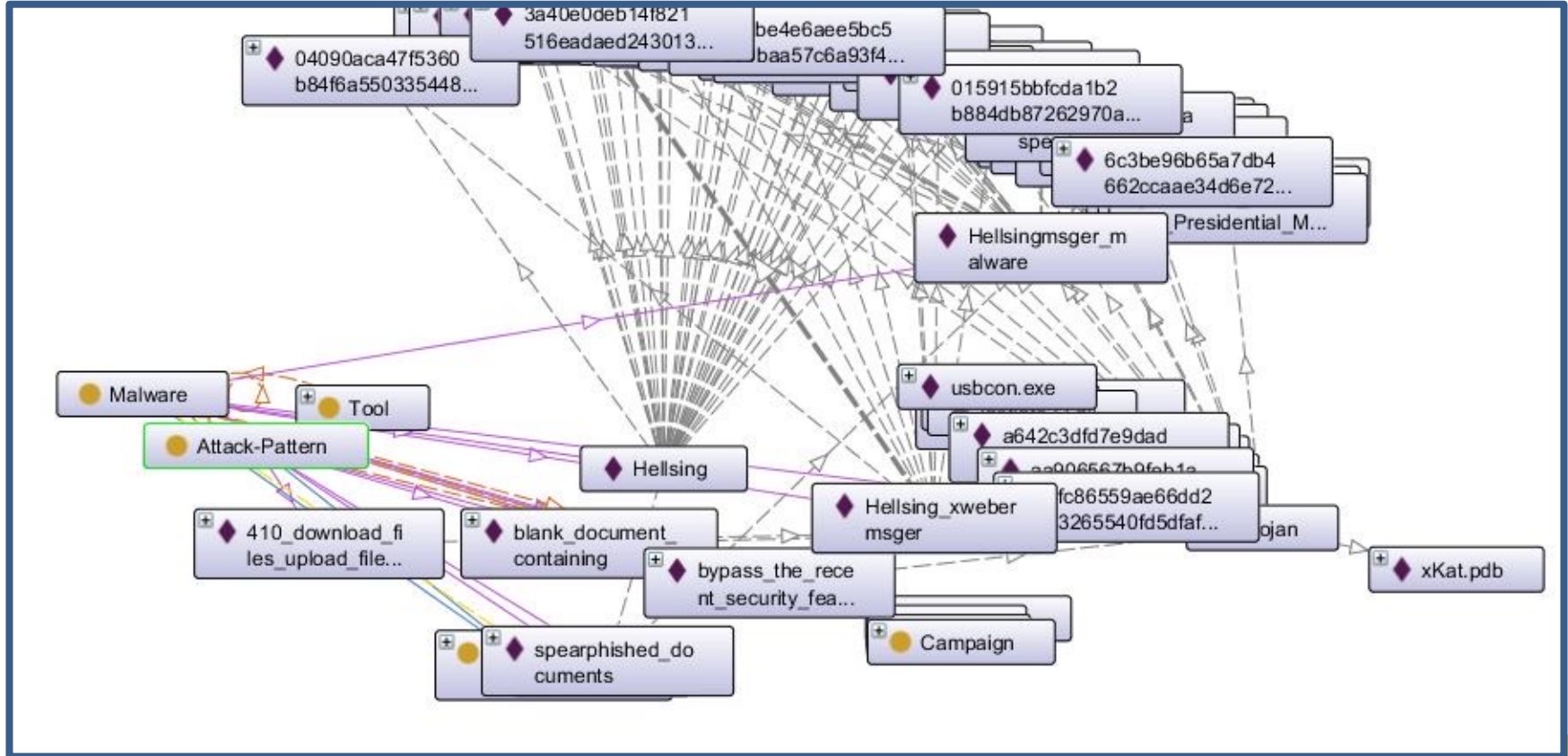
### Filenames:

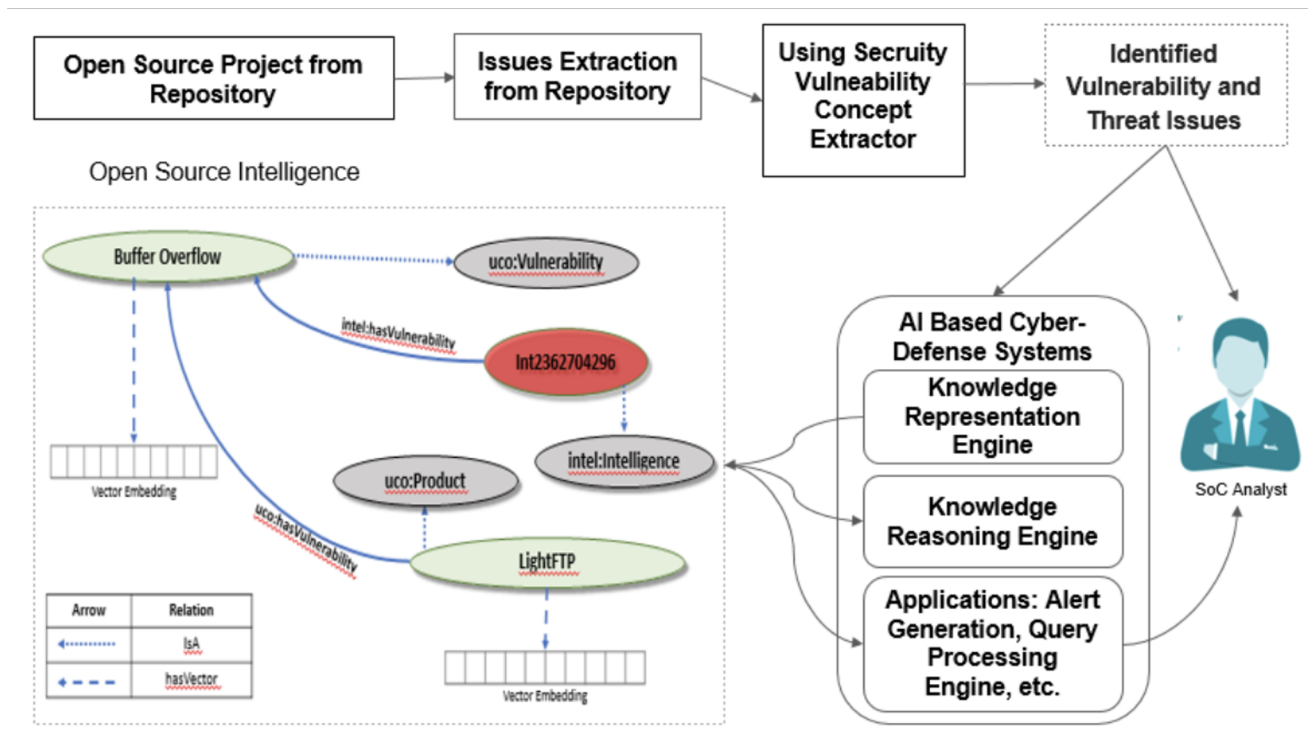
- %systemroot%\system32\irmon32.dll
- %systemroot%\system32\FastUserSwitchingCompatibilityex.dll
- %systemroot%\system32\inetinfo32.dll
- %systemroot%\system32\drivers\drivers\diskfilter.sys
- %systemroot%\system32\usbcon.exe
- %windir%\temp\xKat.exe
- %systemroot%\system32\drivers\drivers\usbmgr.sys
- %appdata%\Microsoft\MMC\mmc.exe
- %systemroot%\system32\lasex.dll
- %systemroot%\system32\lpripex.dll



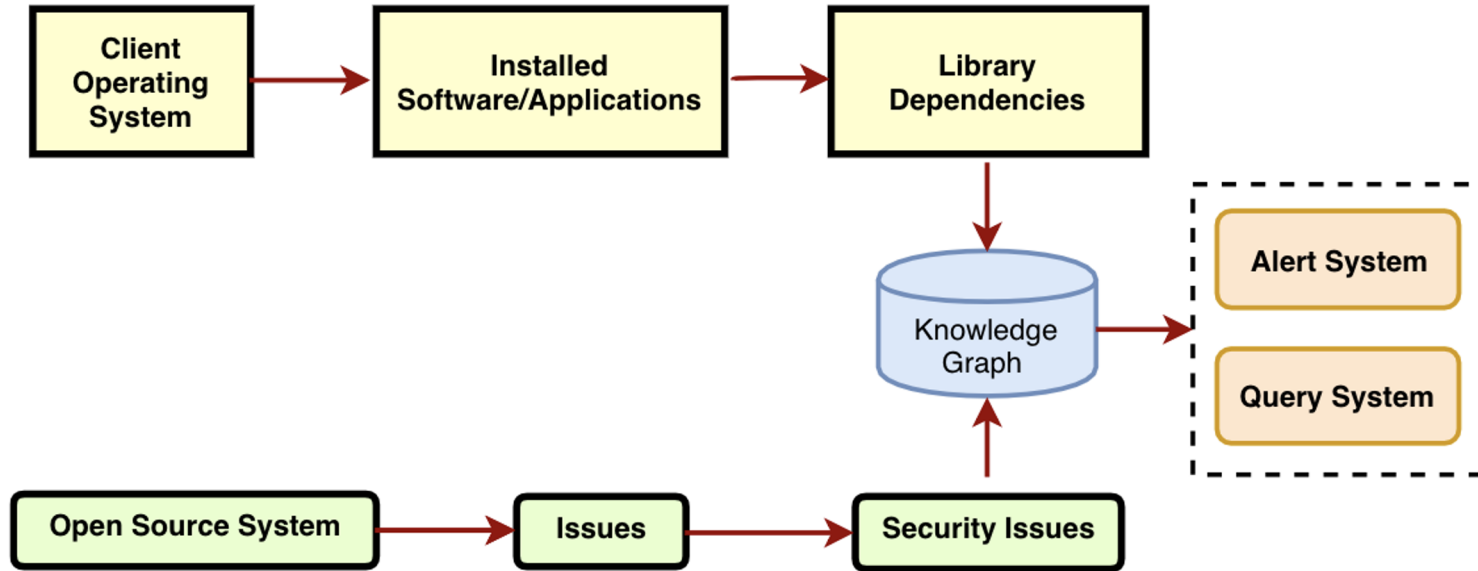
# UMBC Fusing the Extracted Knowledge!





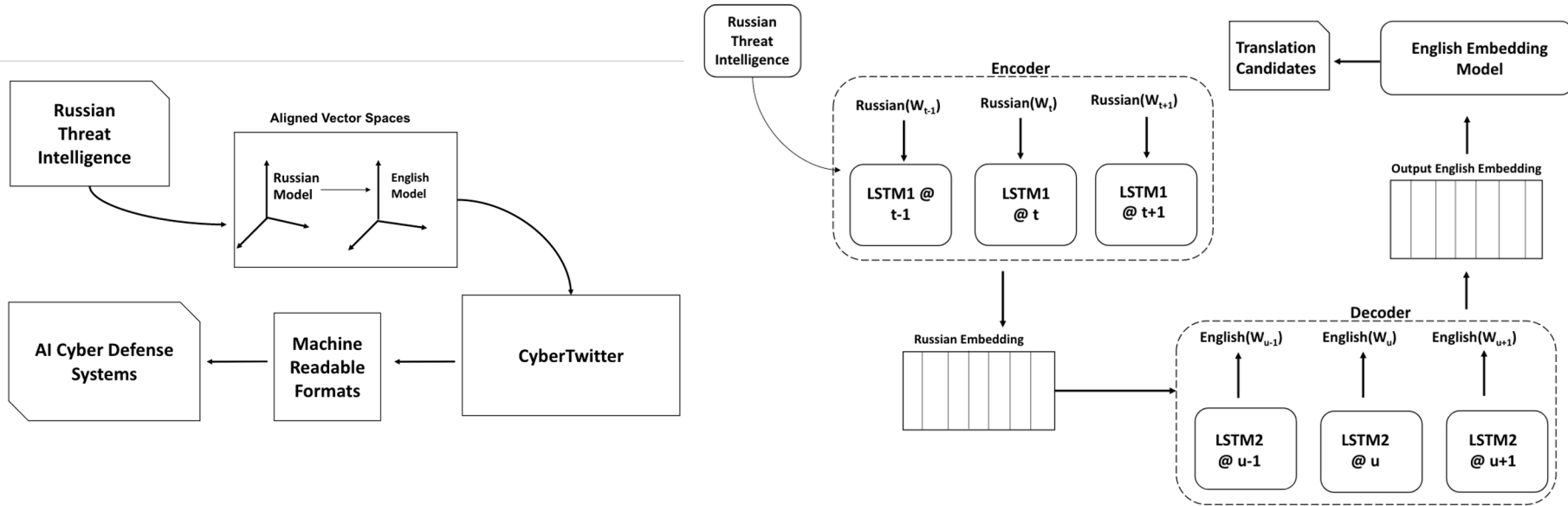


# Tracking vulnerability inheritance during development – Software supply chain attacks!





# Multi-lingual Threat Intelligence



# Multi-lingual Threat Intelligence

Original Russian Tweet	Intelligence Translation System	Google Translate
Вредоносные программы установлены на устройствах китайских производителей	Malware installed on devices of Chinese manufacturers	Malicious programs are installed on devices of Chinese manufacturers
Разработчики убирают шпионское приложение из-за протестов игроков	Developers clean spyware application because of player protests	The spyair was cleaned due to the protests of the players
Positive Technologies: хакнуть процессоры Intel можно через USB порт и отладочный интерфейс	Positive Technologies: Intel processors can be hacked via a USB port and a debug interface	Positive Technologies: Hacked Intel processors with USB port and debugging interface
При открытии сайта Минэнерго высвечивается только красная страница, на которой написано что сайт зашифрован	Council of Defense displays Red page, which says that the site is encrypted	When the website of the Ministry of Energy is opened, only the red page is displayed, on which it is written that the site is encrypted

Developing support for SOC integration.

# UMBC Detecting Information Poisoning

World Events:

Poisoning/  
Mis-information  
propagation  
on Social Media

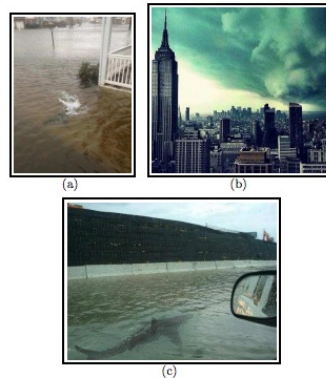


Figure 1: Some of the fake pictures of Hurricane

Cybersecurity Intelligence:

(Under Development)

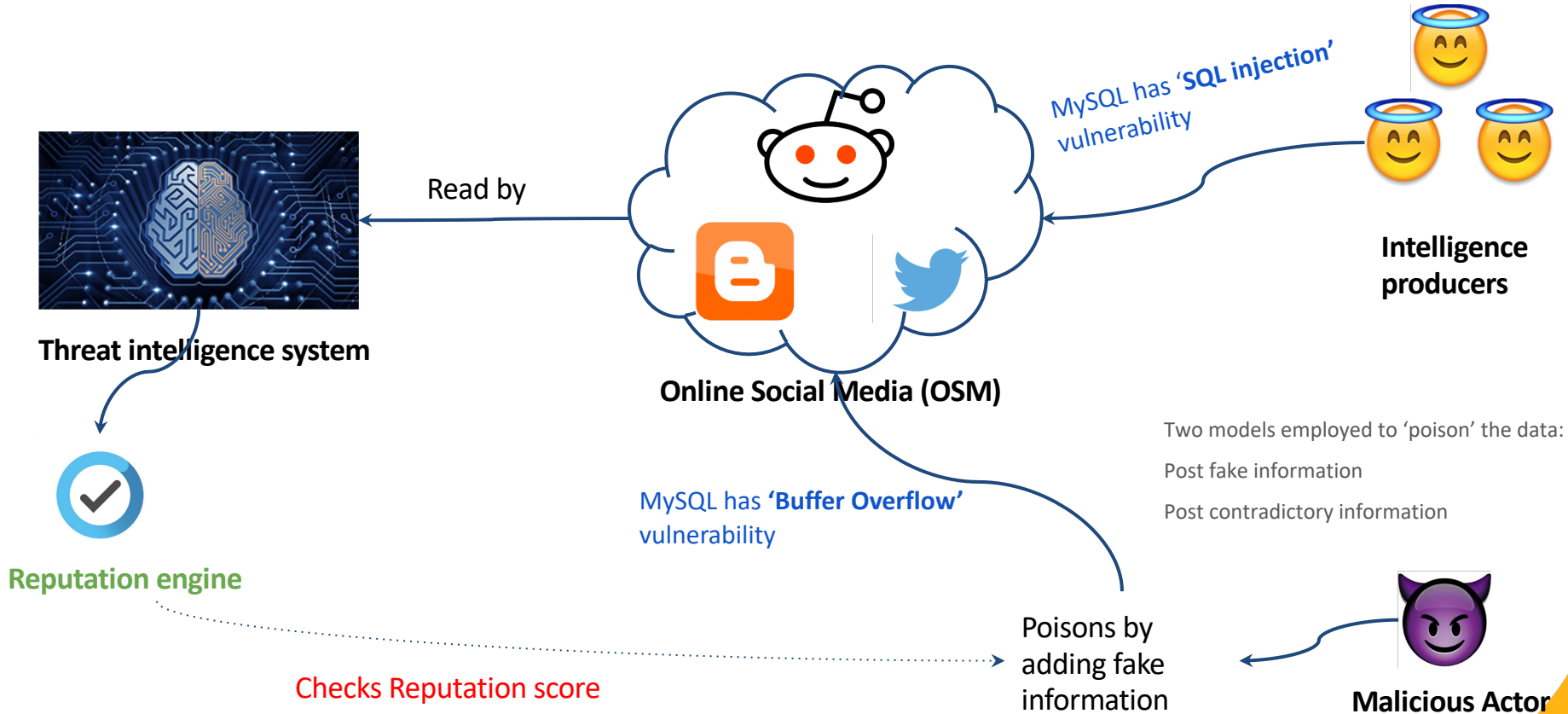
Poisoning of Threat Intelligence  
cultivated from OVERT  
intelligence sources

Starting with Reddit



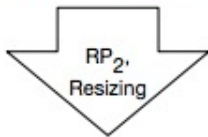
Gupta, Aditi, Hemank Lamba, Ponnurangam Kumaraguru, and Anupam Joshi. "Faking sandy: characterizing and identifying fake images on twitter during hurricane sandy." In Proceedings of the 22nd International Conference on World Wide Web (workshop), pp. 729-736. ACM, 2013.





## Robust Physical Perturbation

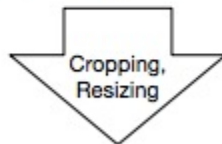
Sequence of physical road signs under different conditions



Different types of physical adversarial examples

## Lab (Stationary) Test

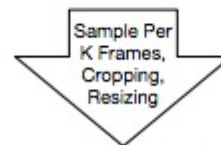
Physical road signs with adversarial perturbation under different conditions



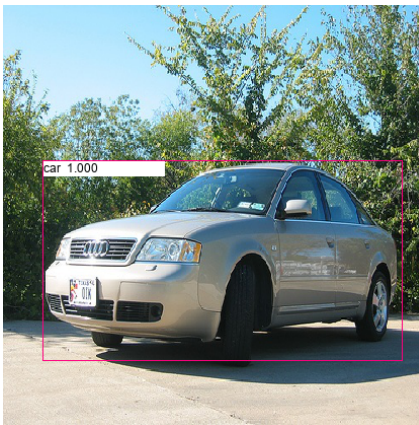
Stop Sign → Speed Limit Sign

## Field (Drive-By) Test

Video sequences taken under different driving speeds



Stop Sign → Speed Limit Sign



(e) Prediction: "car"



(f) Prediction: "dining table"

Akshayvarun Subramanya, Koninika Patil, Hamed Pirsiavash, "Adversarial patches for object detection", submitted to European Conference on Computer Vision (ECCV) 2018.

# Thank You

Questions: [joshi@umbc.edu](mailto:joshi@umbc.edu)