University of Oslo Working Session

August 19, 2021

Using STIX2.1 for Modeling

Ransomware Attacks

RaaS Use Case

CYBER THREAT INTELLIGENCE NETWORK

Presented by: Jane Ginn, MSIA, MRP

Jane Ginn

MSIA, MRP

rjg@ctin.us

Co-Founder, CTIN

Co-Secretary, CTI TC @ OASIS

Secretary, TAC TC & OASIS

Secretary/Treasurer,

Cyber Resilience Institute

https://www.linkedin.com/in/janeginn/

sports -ISAO

eosedge Legal

EclecticIQ

TRUSTAR

Reprivata™

OPENCTI

ARIZONA CYBER THREAT RESPONSE ALLIANCE ACTRA

enisa

THE NATIONAL INSTITUTE FOR HOMETOWN SECURITY Research NIHS Solutions

BLUELIGHT THE i2 EXPERTS

IBM X-Force Exchange

MITRE

Wordfence

ELIAS PARTNERSHIP

EC-Council

MERCYHURST UNIVERSITY

GANNON UNIVERSITY

Duke UNIVERSITY

GREAT LAKES INSTITUTE OF MANAGEMENT, CHENNAI

Global Mindset - Indian Roots

CRI CYBER RESILIENCE INSTITUTE

CYBER USA

ThreatConnect

FORSIGHT SECURITY

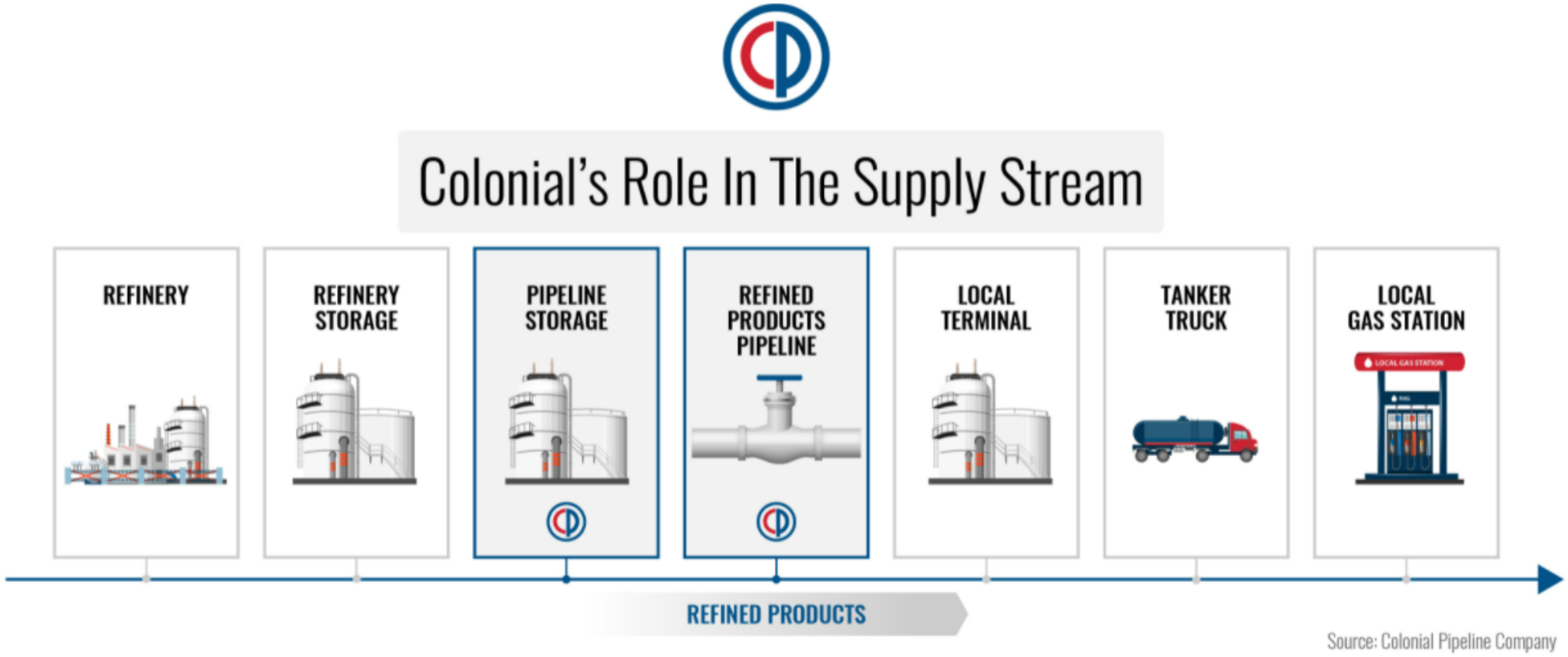
Agenda

- **Colonial Pipeline Background**
  - *Sequence of Events*
- **Darkside RaaS (aka, Black Matter)**
  - *Ransomware as a Service*
  - *FBI/DHS Alert on Darkside*
  - *Affiliate Network*
- **Modeling Attacks with STIX2.1**
  - ***Indicator*** *SDO + Patterning Language*
  - ***Threat Actor*** *SDO*
  - ***Intrusion Set*** *SDO*
  - ***Malware*** *SDO*
- **Importance of Interoperability**

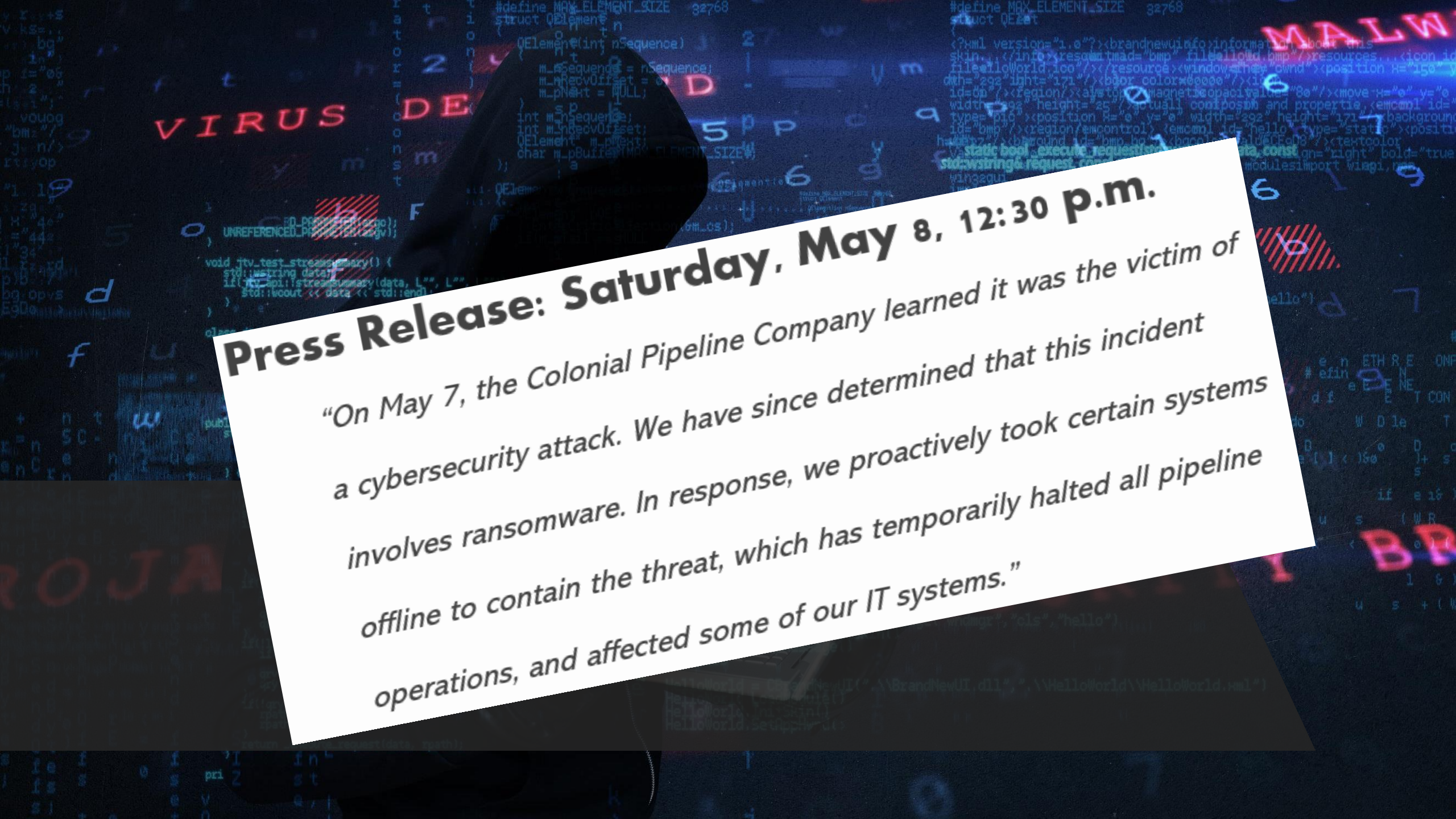
Colonial Pipeline

Infrastructure Attack

Colonial Pipeline: Role in Supply Chain



Linden
SYSTEM ENDS IN LINDEN, NJ
Dorsey
Baltimore
Mitchell
Richmond
Norfolk
Line 4
Line 3
Greensboro
Selma
Knoxville
Charlotte
Nashville
Belton
Spartanburg
Atlanta
Birmingham
Augusta
Macon
Meridian
Oxford
Boligee
Bainbridge
Opelousas
Line 1
Houston
Line 2
Operational
Colonial Pipeline Company


Press Release: Saturday, May 8, 12:30 p.m.
"On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems."

About Colonial Pipeline Hack

- Company transports gasoline, diesel, & jet fuel
- Supplies est. 45% of US East Coast market
- Company transports roughly 2.5 million barrels of fuel daily from the Gulf Coast to the Eastern Seaboard
- Breach from a compromised VPN Password
- The hackers also stole nearly 100 gigabytes of data from Colonial Pipeline and threatened to leak it if the ransom wasn't paid

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Widespread Disruption

4:24 PM · May 12, 2021

Darkside RaaS

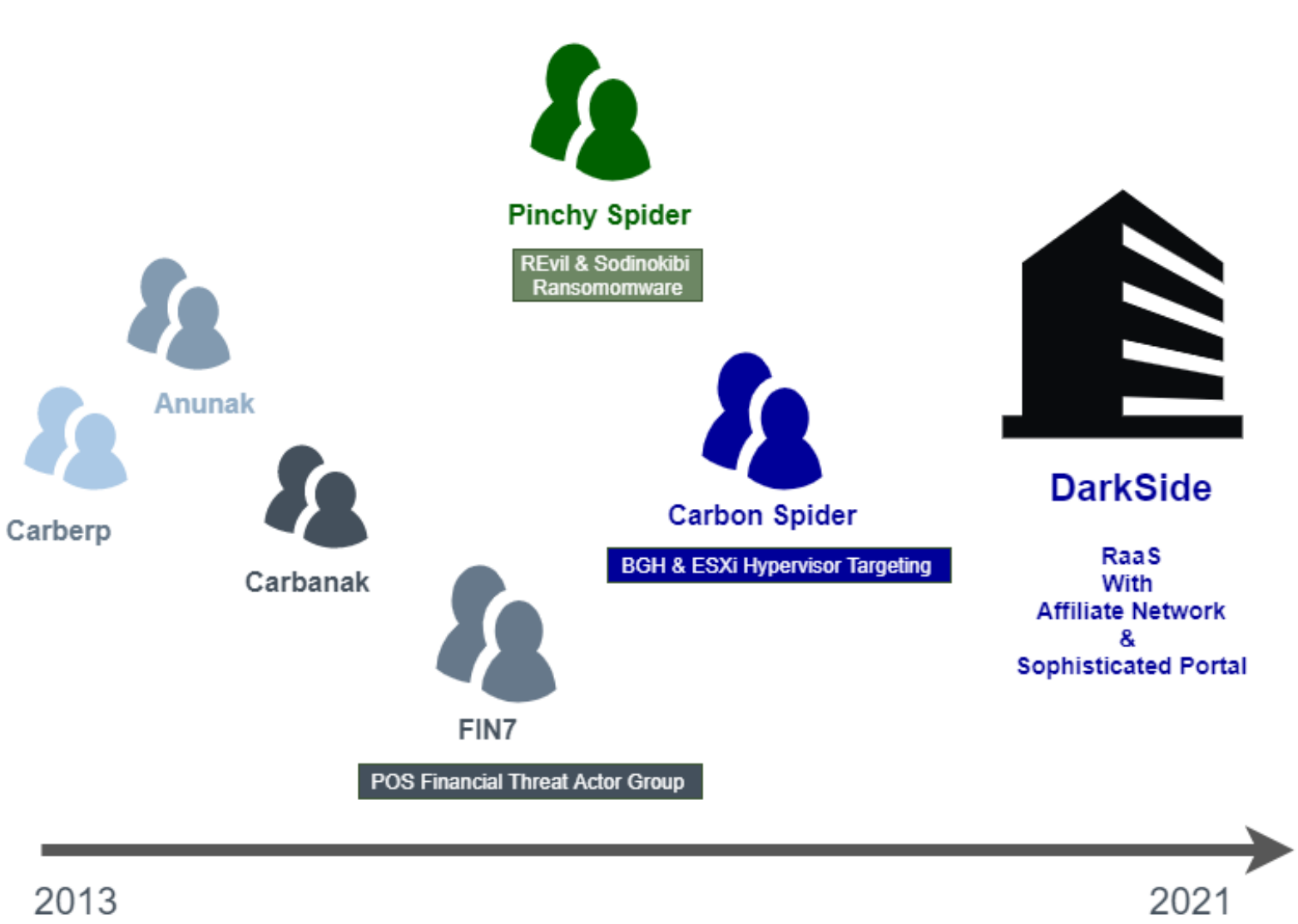
Affiliate Business Model

Geopolitical Context

Ransomware's suspected Russian roots point to a long detente between the Kremlin and hackers

https://wapo.st/35gAj6l

Potential Lineage of Darkside



FIN7 Indictment

THE UNITED STATES ATTORNEY'S OFFICE
WESTERN DISTRICT of WASHINGTON

HOME ABOUT MEET THE U.S. ATTORNEY NEWS DIVISIONS PROGRAMS

U.S. Attorneys » Western District of Washington » News

Department of Justice

U.S. Attorney's Office

Western District of Washington

SHARE

FOR IMMEDIATE RELEASE — Friday, April 16, 2021

High-level organizer of notorious hacking group FIN7 sentenced to ten years in prison for scheme that compromised tens of millions of debit and credit cards

Overall damage to banks, merchants, card companies, and consumers estimated at more than $3 billion

Seattle – The first high-level manager of the notorious hacking group FIN7 was sentenced today in U.S. District Court in Seattle to ten years in prison, announced Acting U.S. Attorney Tessa A. Gorman. Fedir Hladyr, 35, a Ukranian national, served as a high-level manager and systems administrator for FIN7. He was arrested in Dresden, Germany, in 2018 at the request of U.S. law enforcement and was extradited to Seattle. In September 2019, he pleaded guilty to conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking. At today's sentencing hearing, Chief U.S. District Judge Ricardo S. Martinez said, "Cybercrime has become the greatest threat to American's financial health, and to citizens around the globe."

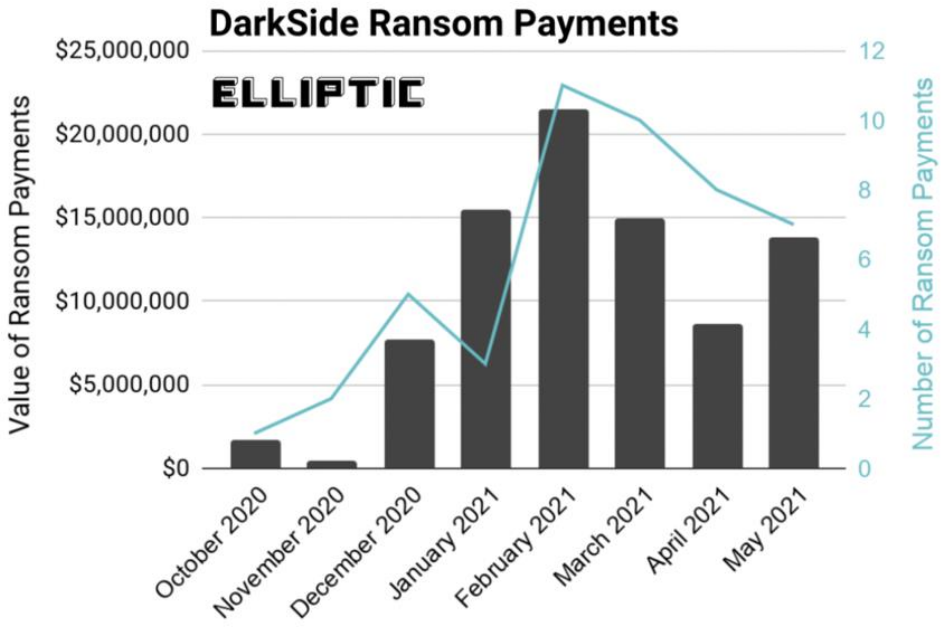
"This criminal organization had more than 70 people organized into business units and teams. Some were hackers, others developed the malware installed on computers, and still others crafted the malicious emails that duped victims into infecting their company systems," said Acting U.S. Attorney Gorman. "This defendant worked at the intersection of all these activities and thus bears heavy responsibility for billions in damage caused to companies and individual consumers."

George Grasso, Attorney for FIN7 CEO Fedir Hiadyr a Ukranian National.

Fedir Hiadyr was sentenced to 10 years in a U.S. Prison on April 16th, 2021

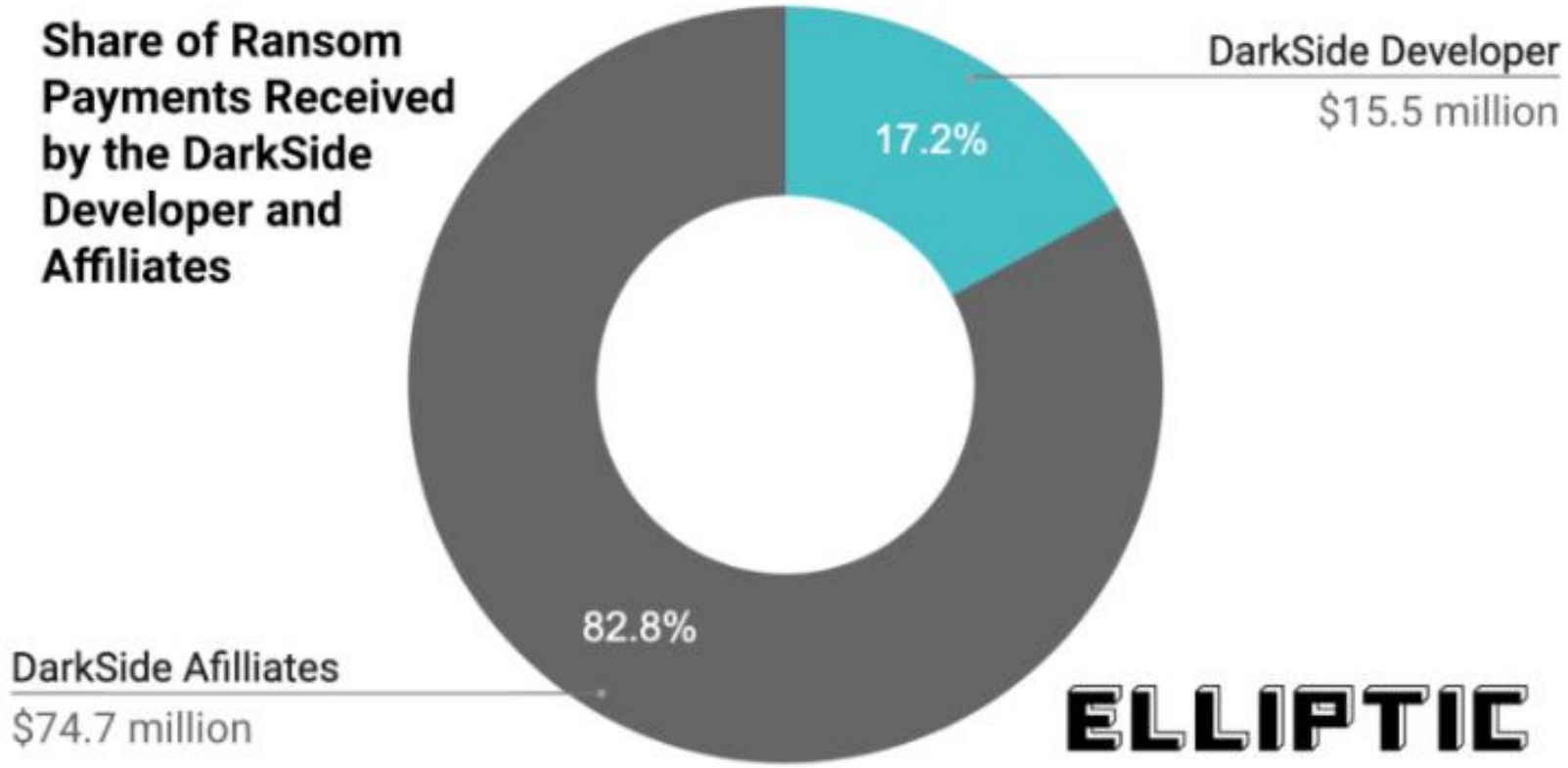
Darkside Profitability

- Darkside grossed US $90M since October 2020
  - (source: Recorded Future)
- Transferred Bitcoins to 47 Bitcoin wallets
  - (source: Elliptic)
- Estimated 99 victims ~ 47% paid ransom
  - (source: Darktrace)
- Bitcoin Wallet Emptied May 13, 2021



https://therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

Darkside Netted Est. US $15.5M



https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

FBI Flash – May 10, 2021

10 MAY 2021

Alert Number
MU-000146-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact
FBI CYWATCH

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA and the Department of Energy.

This FLASH has been released **TLP:GREEN**: Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Indicators of Compromise Associated with Darkside Ransomware

Summary

In May 2021, the FBI received notification that the ransomware variant Darkside had infected a critical infrastructure company in the

Targeting Directives from Darkside

Avoid Targeting Companies In These Sectors:

- Health Care Organizations
- Hospitals
- Educational Organizations
- NGOs

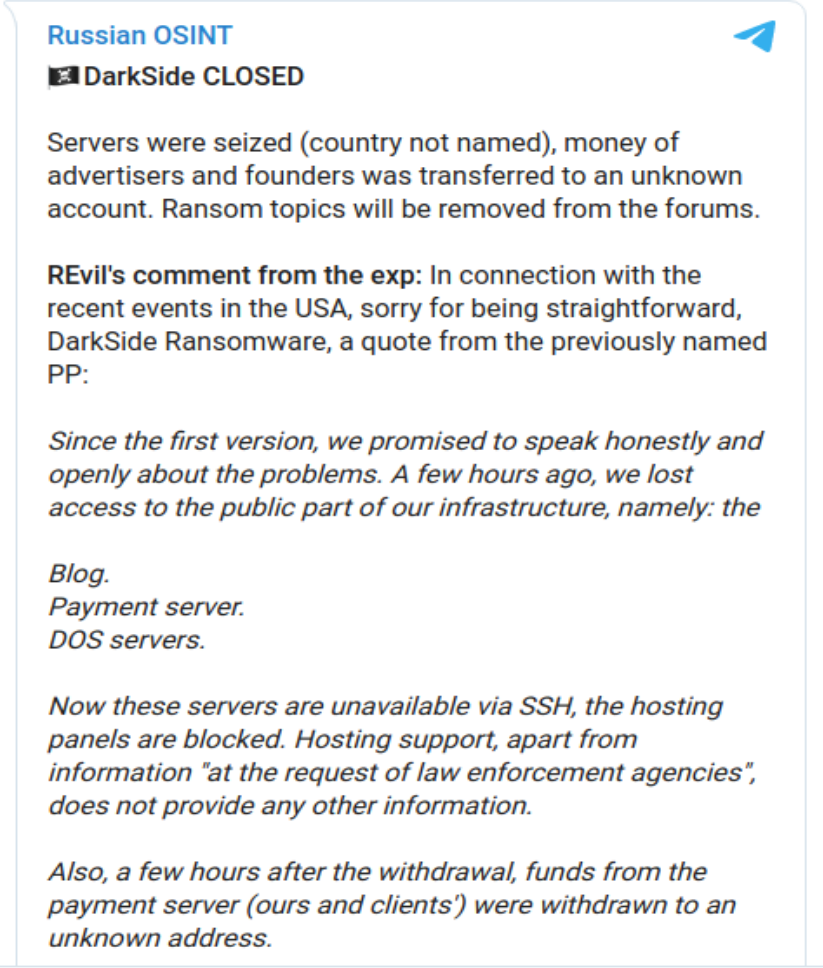
Avoid Targeting Companies Using These Languages:

```
{
  switch(prim_lang_id) {
  case 0x18:     LANG_ROMANIAN
  case 0x19:     LANG_RUSSIAN
  case 0x22:     LANG_UKRAINIAN
  case 0x23:     LANG_BELARUSIAN
  case 0x25:     LANG_ESTONIAN
  case 0x26:     LANG_LATVIAN
  case 0x27:     LANG_LITHUANIAN
  case 0x28:     LANG_TAJIK
  case 0x29:     LANG_PERSIAN
  case 0x2b:     LANG_ARMENIAN
  case 0x2c:     LANG_AZERI
  case 0x37:     LANG_GEORGIAN
  case 0x3f:     LANG_KAZAK
  case 0x40:     LANG_KYRGYZ
  case 0x42:     LANG_TURKMEN
  case 0x43:     LANG_UZBEK
  case 0x44:     LANG_TATAR
    return 1;    If one of the languages, return True
  default:
```

Darkside Servers Seized 05/14/21

- DarkSide Servers “seized”
  - Money of Advertisers & Founders Gone
  - Servers Unavailable via SSH
  - Hosting Panels Blocked

  - Hosting support gone “***at the request of law enforcement does not provide any other information***”



Russian OSINT

DarkSide CLOSED

Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account. Ransom topics will be removed from the forums.

REvil's comment from the exp: In connection with the recent events in the USA, sorry for being straightforward, DarkSide Ransomware, a quote from the previously named PP:

Since the first version, we promised to speak honestly and openly about the problems. A few hours ago, we lost access to the public part of our infrastructure, namely: the

Blog.
Payment server.
DOS servers.

Now these servers are unavailable via SSH, the hosting panels are blocked. Hosting support, apart from information "at the request of law enforcement agencies", does not provide any other information.

Also, a few hours after the withdrawal, funds from the payment server (ours and clients') were withdrawn to an unknown address.

https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/

Еще с первой версии мы обещали честно и открыто говорить о проблемах. Несколько часов назад мы потеряли доступ к публичной части нашей инфраструктуры, а именно:

- Блогу.
- Платежному серверу.
- Серверам СДН.

Сейчас эти сервера недоступны по SSH, хостинг панели заблокированы. Поддержка хостингов, кроме информации "по запросу правоохранительных органов" другой информации не дает.

Так же, через несколько часов после изъятия, средства с платежного сервера (наши и клиентские) были выведены на неизвестный адрес.

Для решения текущей ситуации будут предприняты следующие действия:

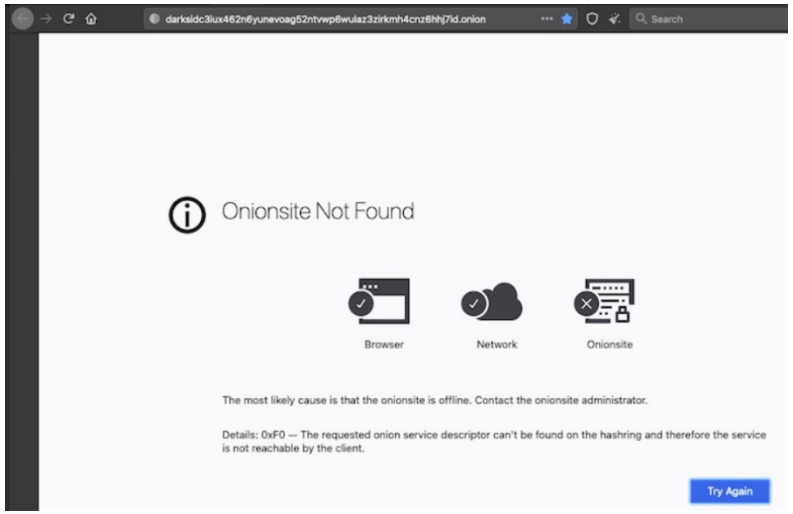
- Вам будут выданы декрипторы ко всем компаниям, кто еще не оплатил. Дальше вы можете общаться как угодно и где угодно. **Пишите саппорту.**
- Мы выведем депозит для закрытия вопросов перед пострадавшими пользователями. Предположительная дата выдачи компенсаций: **23.05** (в связи с холдом вывода депозита на xss в 10 дней).

В связи со всем вышесказанным, а так же давлением со стороны США - **партнерская программа закрыта**.

Мы желаем всем безопасности и удачи.

Лендинг сервера и другие ресурсы будут отключены **в течении 48 часов**.

Darkside Onion Site Down



"On May 13, 2021, the operators of the DarkSide Ransomware-as-a-Service (RaaS) announced they would immediately cease operations of the DarkSide RaaS program. Operators said they would issue decryptors to all their affiliates for the targets they attacked and promised to compensate all outstanding financial obligations by May 23, 2021."

Source: https://www.intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime

DOJ Actions

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | TOPICS | NEWS | RESOURCES | CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Monday, June 7, 2021

Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside

WASHINGTON - The Department of Justice today announced that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation. The seizure warrant was authorized earlier today by the Honorable Laurel Beeler, U.S. Magistrate Judge for the Northern District of California.

"Following the money remains one of the most basic, yet powerful tools we have," said Deputy Attorney General Lisa O. Monaco for the U.S. Department of Justice. "Ransom payments are the fuel that propels the digital extortion engine, and today's announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks. Today's announcements also demonstrate the value of early notification to law enforcement; we thank Colonial Pipeline for quickly notifying the FBI when they learned that they were targeted by DarkSide."

https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

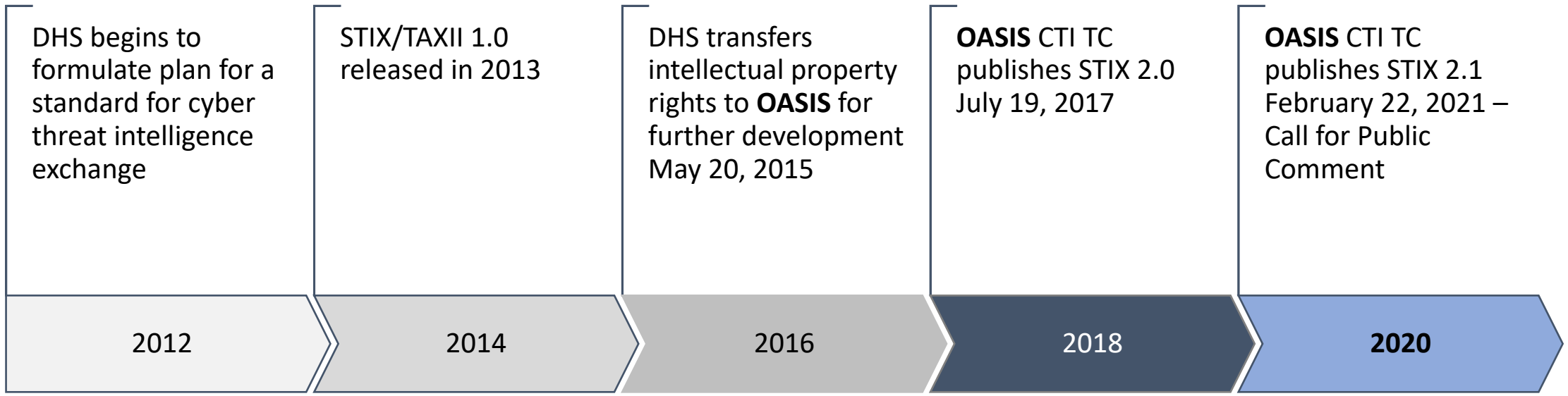
CTI TC Background

OASIS

OASIS CTI TC Public Website

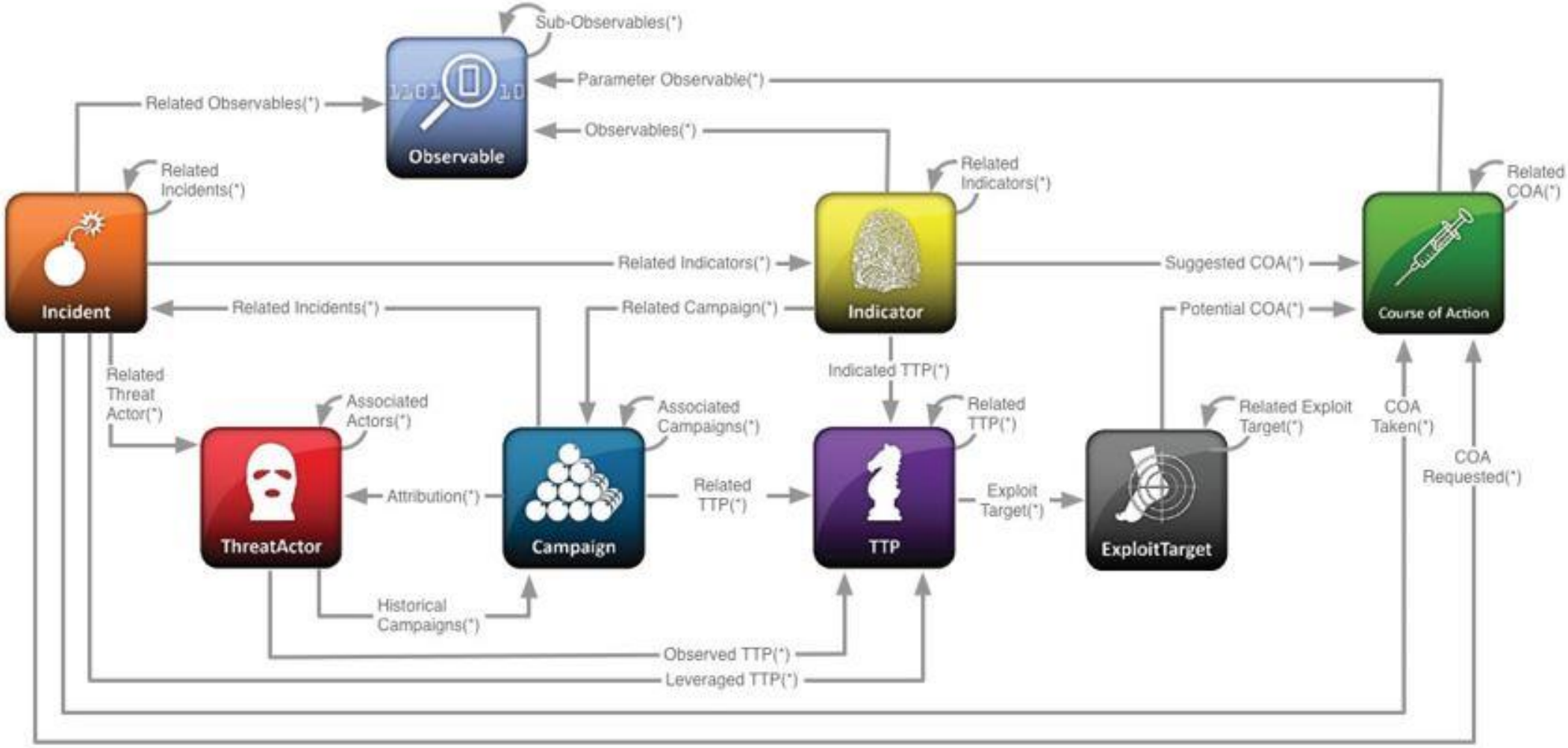
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

Development of STIX Standard




accenture
aetna
AIRBUS
ALIEN VAULT
ANOMALI
AIT
AUSTRIAN INSTITUTE OF TECHNOLOGY
ANZ
Bank of America
BMO Bank of Montreal
BOEING
circl
CISCO
CENTER FOR INTERNET SECURITY
CYBER
THREAT INTELLIGENCE
DELL
difi
eclectic iq
EPRI
ERICSSON
FINANCIAL SERVICES ISAC
FireEye
FORNETIX
FORTINET
FUJITSU
G2
GENIVIA
GEORGETOWN UNIVERSITY
Google
Hewlett Packard Enterprise
HUAWEI
Huntsman
IBM
iboss
情報セキュリティ大学院大学
IJIS Institute
intel
JOHNS HOPKINS APPLIED PHYSICS LABORATORY
JPMorganChase
KAISER PERMANENTE
LOOKINGGLASS
McAfee
MITRE
MTG
NATO OTAN
NC4
NEC
NEW CONTEXT
NORTHROP GRUMMAN
paloalto NETWORKS
PERCH
Phantom
SEMPER FORTIS SOLUTIONS
sFractal Consulting LLC
SIEMENS
SOUTHERN CALIFORNIA EDISON
Symantec.
SYNOPSYS
TELUS
THREATCONNECT
THREATQUOTIENT
TRU/STAR TECHNOLOGY
UNC CHARLOTTE
usbancorp
VERISIGN
ViaSat
XLAB

STIX 1.1 (XML Based)



Lessons Learned from Ver. 1.x

- **JSON, not XML**: Preferred by developers, easier to understand
- **Simplicity and Clarity**: Less flexibility, more standardization
- **Pragmatism**: Fewer, but better-understood objects and properties
- **One Standard**: Merge CybOX into STIX
- **Relationships as first-class objects**: Easier for the community to contribute
- **Leverage existing HTTP features**: Easier to use with existing tooling

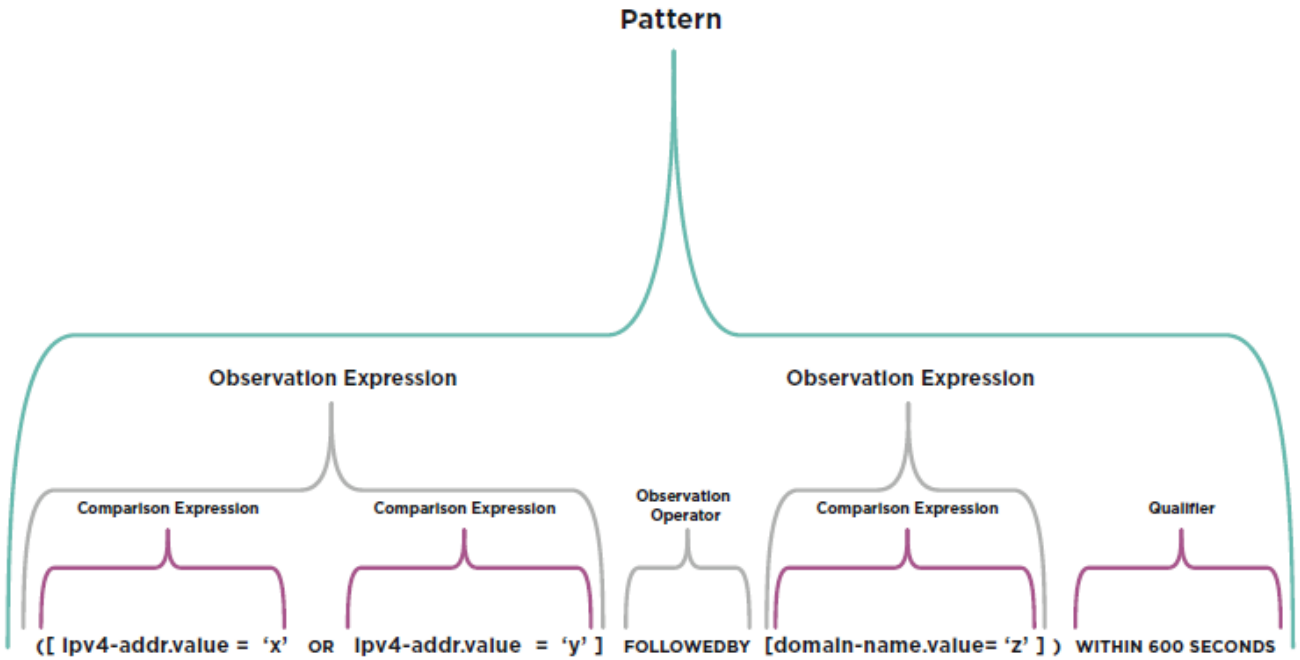
Some Key Design Principles:

- **Vendor** driven; based on real-world use cases
- Understandable by **humans**, but designed for **machines** (JSON)
- There should be **one way** to do any **one thing**
- **Limit optionality** wherever feasible
- **Avoid reinventing wheels**; reference existing standards wherever possible
- Focus on ***interoperability***

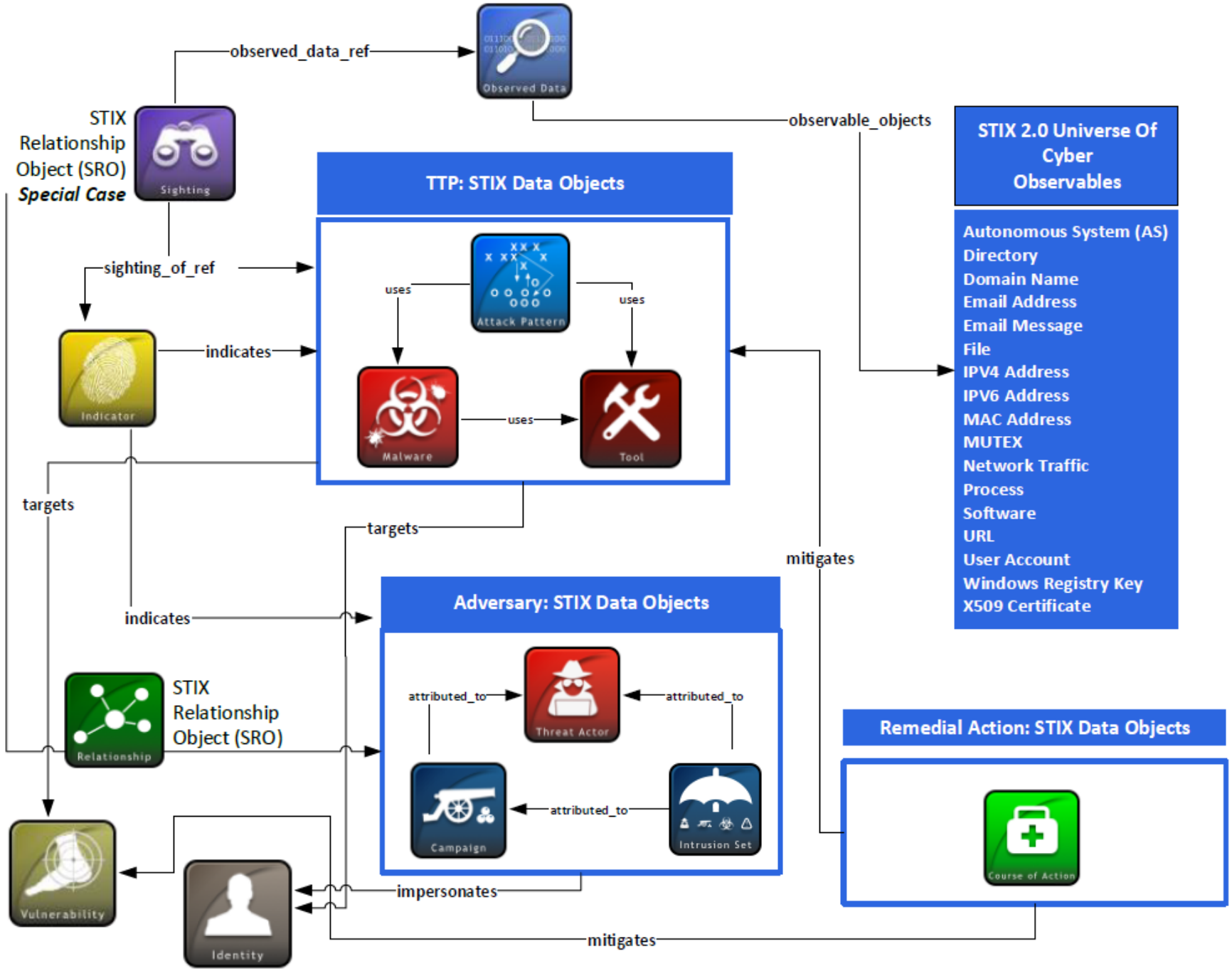
Net Result: **Easier to implement, easier to consume, more foolproof for the end user**

Key Changes from STIX 1.1 to 2.0

- Added Patterning Language



- Adding Self-Certification Program for those that do Interoperability Testing


observed_data_ref
Observed Data
observable_objects
STIX
Relationship
Object (SRO)
Special Case
Sighting
STIX 2.0 Universe Of
Cyber
Observables
TTP: STIX Data Objects
sighting_of_ref
uses
Attack Pattern
uses
indicates
Indicator
Malware
uses
Tool
Autonomous System (AS)
Directory
Domain Name
Email Address
Email Message
File
IPV4 Address
IPV6 Address
MAC Address
MUTEX
Network Traffic
Process
Software
URL
User Account
Windows Registry Key
X509 Certificate
targets
targets
mitigates
indicates
Adversary: STIX Data Objects
attributed_to
Threat Actor
attributed_to
STIX
Relationship
Object (SRO)
Relationship
Remedial Action: STIX Data Objects
Campaign
attributed_to
Intrusion Set
Course of Action
Vulnerability
Identity
impersonates
mitigates

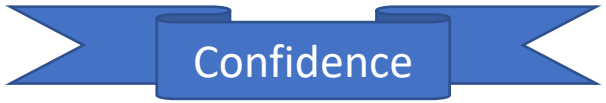
Key Changes from STIX 2.0 to 2.1

- Added ‘Language’ Meta Object

- Added Five SDOs
  - That Provide Significant Support for Human Analyst Activities

- Significantly Improved Malware SDO Plus Added a ‘Malware Analysis’ SDO (Static & Dynamic Capture)

- Added ‘Confidence’ Property to SDOs



- Created Relationships Between SCOs & any SDO

Modeling Attacks

STIX2.1

STIX Domain Objects (SDOs)

- Attack Pattern
- Campaign
- Course of Action
- Grouping
- Identity
- Indicator
- Infrastructure
- Intrusion Set
- Location

Ransomware Attack on Colonial Pipeline

Lineage of Threat Actor Groups

- Malware
- Malware Analysis
- Note
- Observed Data
- Opinion
- Report
- Threat Actor
- Tool
- Vulnerability

Represent Hashes

Darkside Threat Actor Group

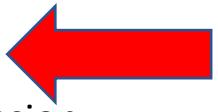
STIX Cyber Observable Objects (SCOs)

- Artifact
- AS
- Directory
- Domain Name
- Email Address
- Email Message
- File
  - Archive Extension
  - NTFS File Extension
  - PDF File Extension
  - Raster Image File Extension
  - Windows PE Binary File Extension
- IPv4 Address
- IPv6 Address
- MAC Address

In FBI Flash

In FBI Flash

- Mutex
- Network Traffic
  - HTTP Request Extension
  - ICMP Extension
  - Network Socket Extension
  - TCP Extension
- Process
  - Windows Process Extension
  - Windows Service Extension
- Software
- URL
- User Account
  - UNIX Account Extension
- Windows Registry Key
- X.509 Certificate

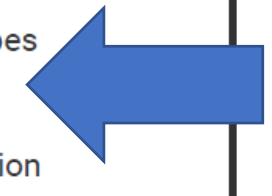


In FireEye/ Mandiant Blog

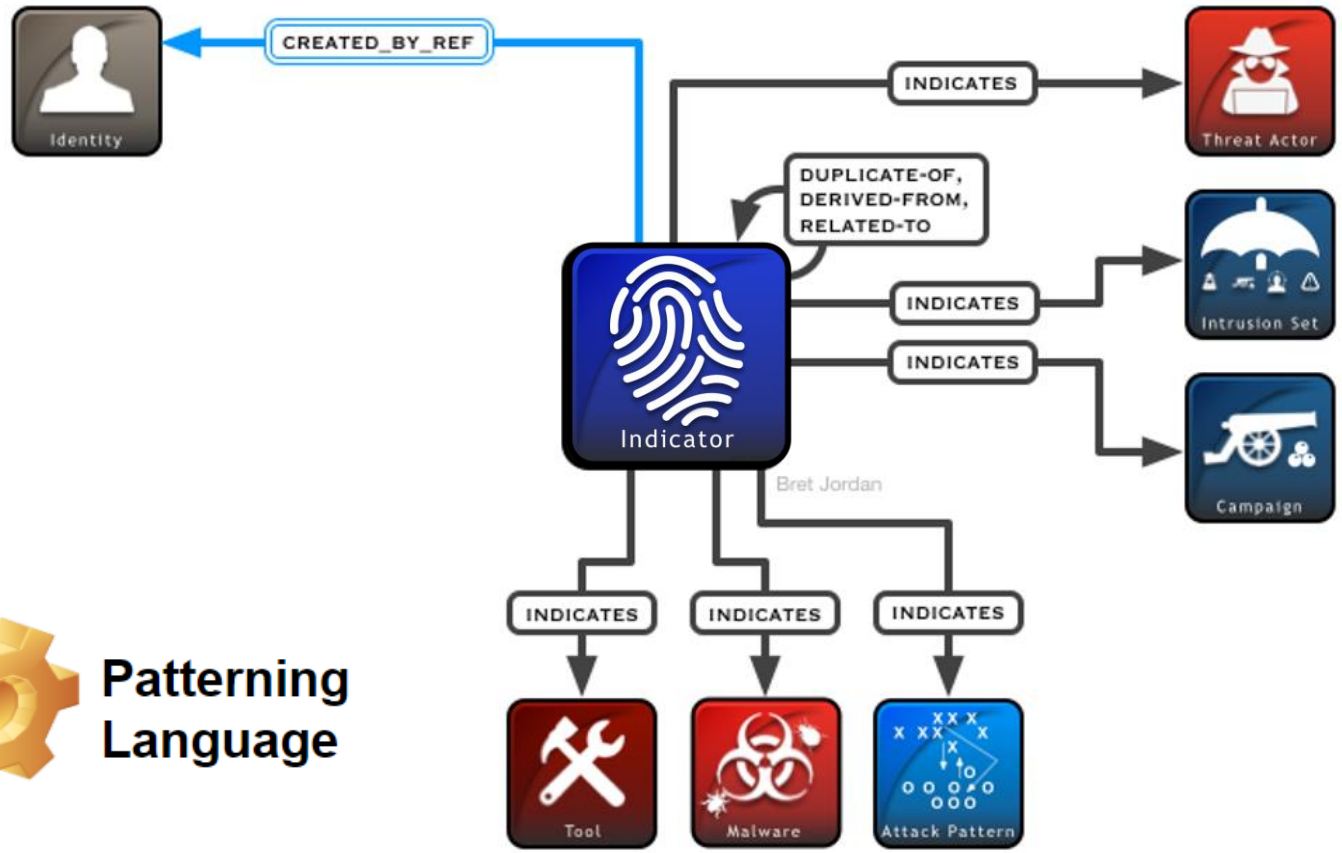
In FBI Flash

Indicator SDO Properties & Relationships

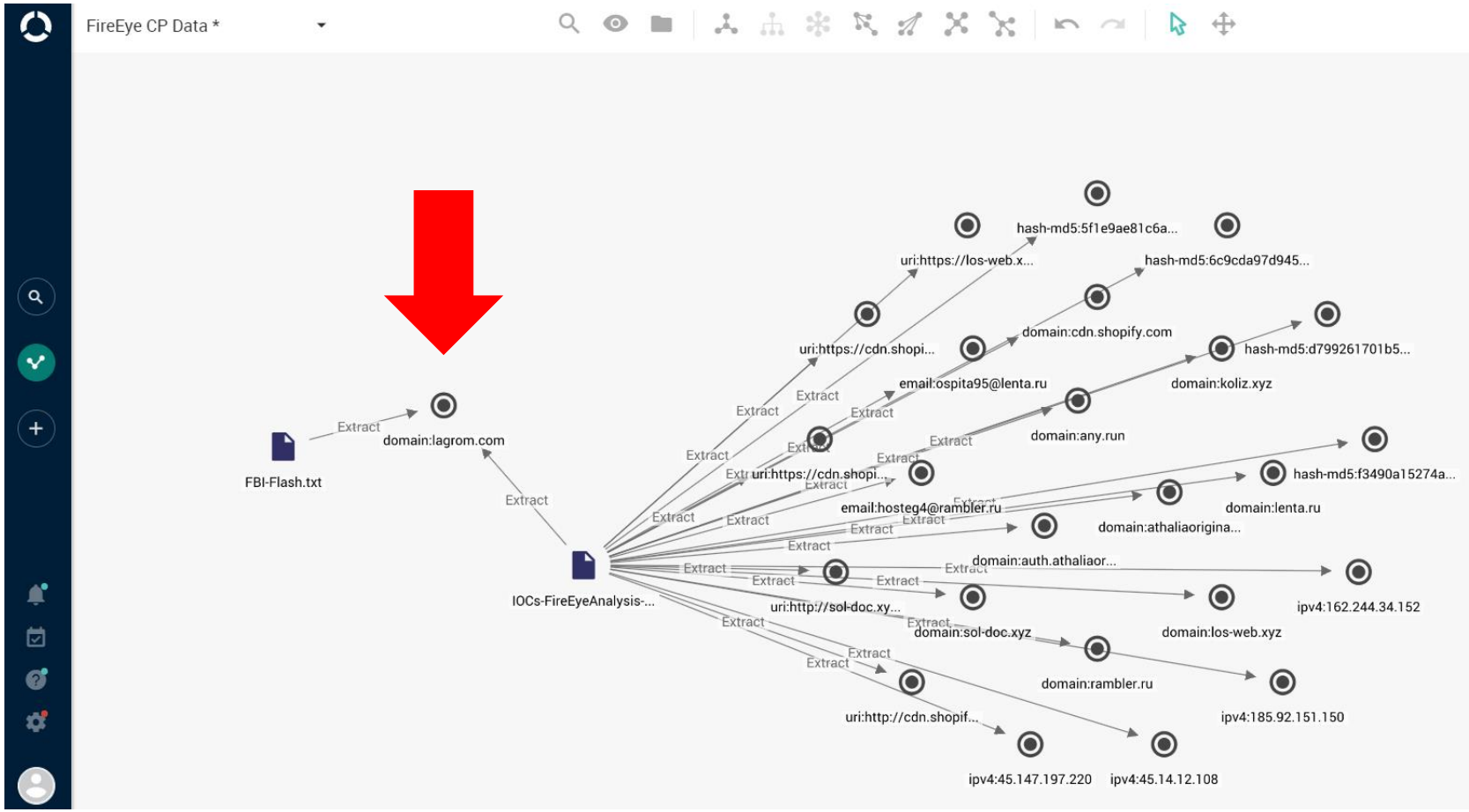
Indicator		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Indicator Specific		name
		description
	R	indicator_types
	R	pattern
	R	pattern_type
		pattern_version
	R	valid_from
		valid_until
		kill_chain_phases



Patterning Language

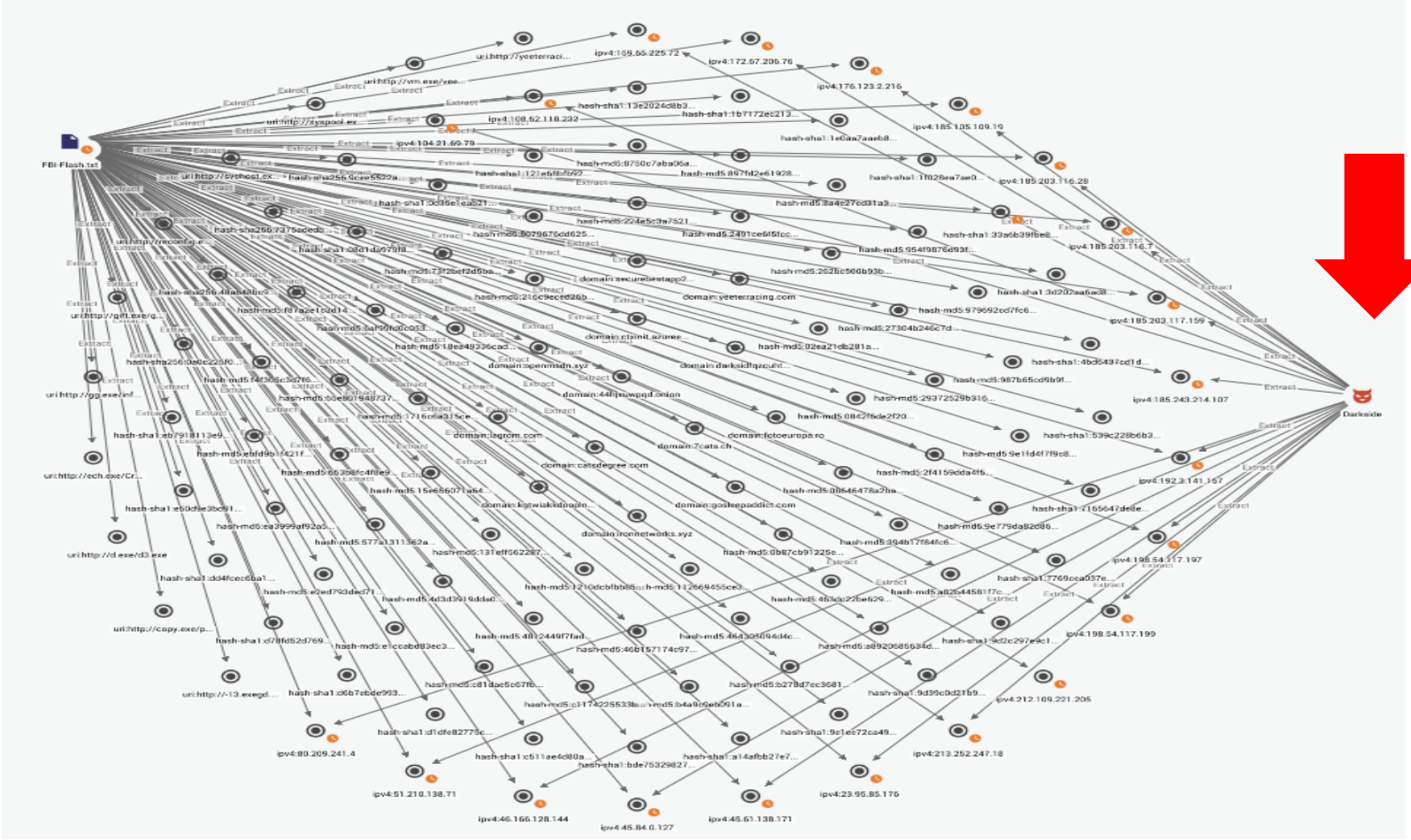


Graph: FBI-FireEye Correlation Point



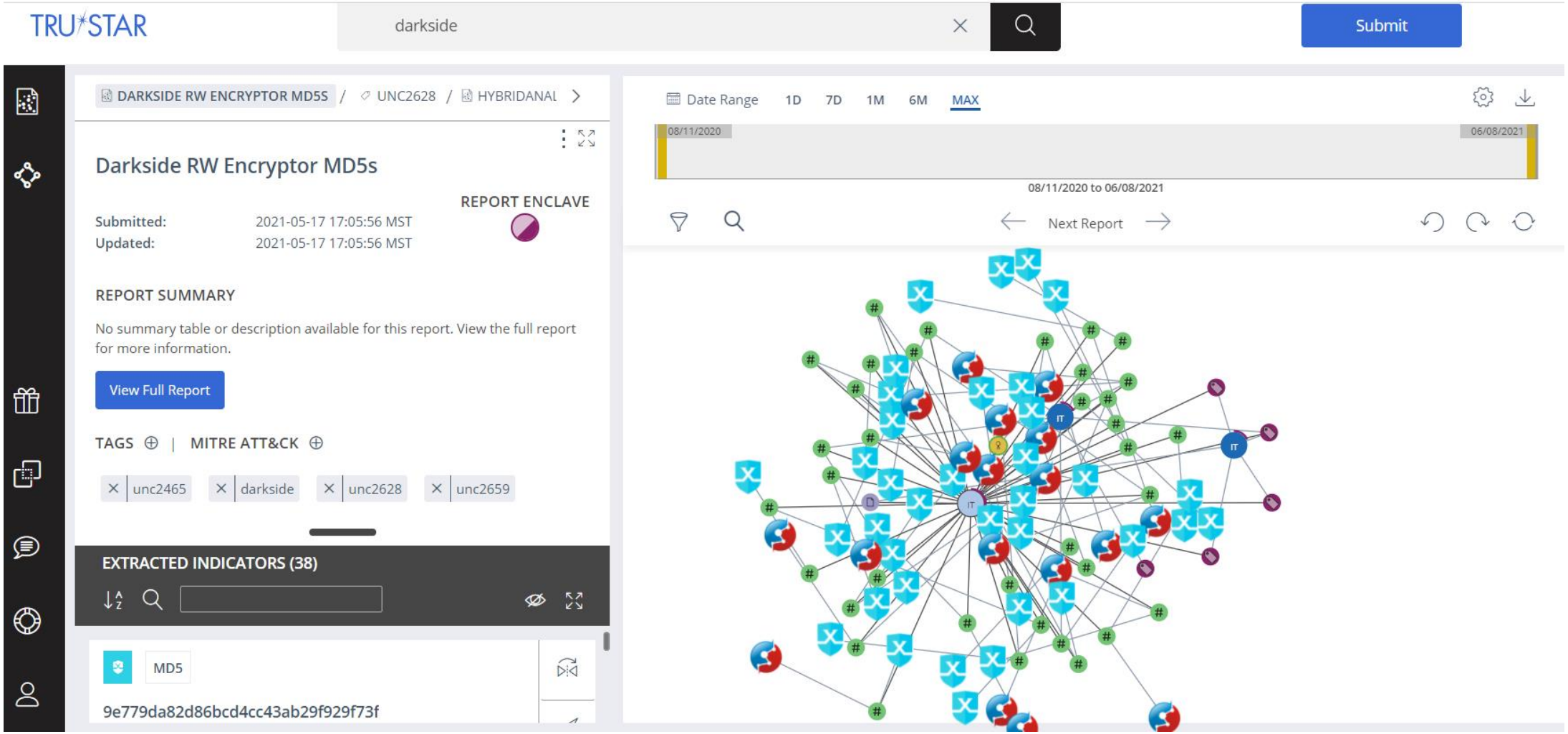
Source: EclecticIQ TIP

Graph: FBI-FireEye Corroborate on DS



Source: EclecticIQ TIP

Property Graph Representation



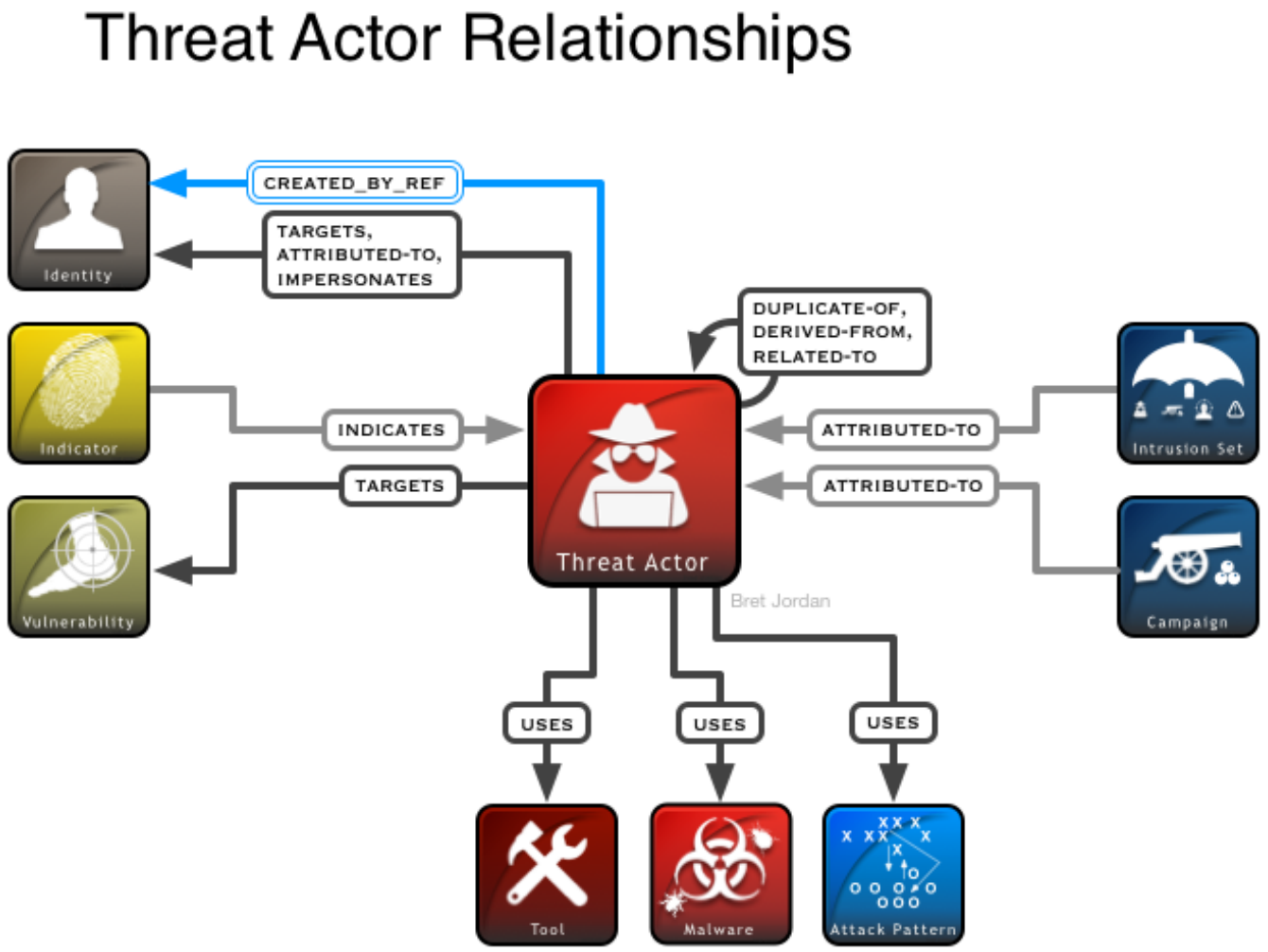
Source: TRUSTAR TIP

Indicator SDO + Patterning Language

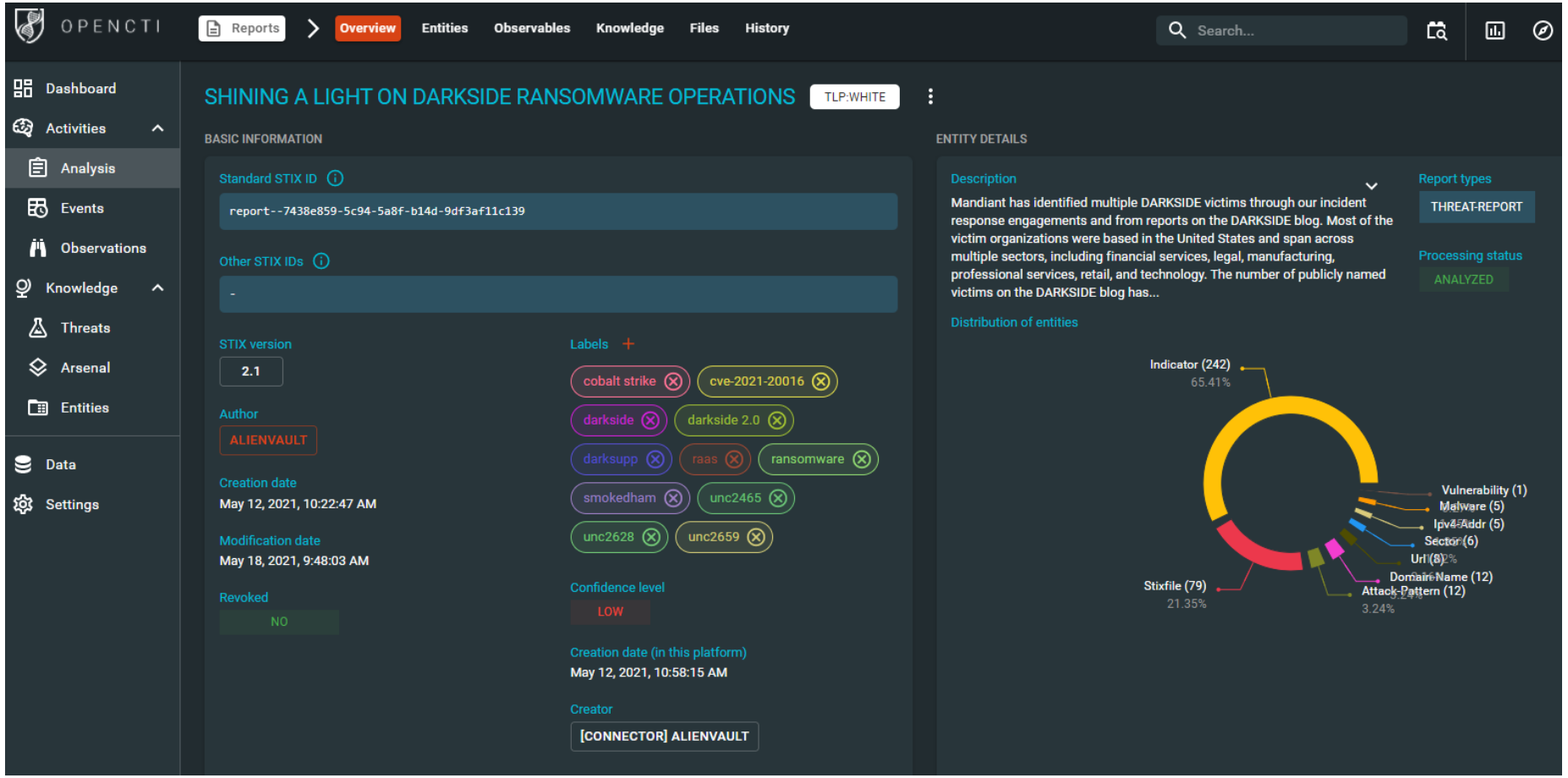

```
{
    "spec_version": "2.1",
    "type": “report",
    "objects": [
        {
            "id": "indicator--73d9cfca-0117-49d2-84f0-2105e00d7660",
            "type": "indicator",
            "created": "2021-06-07T20:39:07.006Z",
            "modified": "2021-06-07T20:39:07.006Z",
            "labels": [ “malicious",],
            "name": "URL Report for lagrom.com",
            "description": "Category: Financial Services",
            "pattern": "[ url:value = ‘http://logram.com' ]",
            "valid_from": "2021-06-07T20:39:07.006Z"
        },
        {
```

Threat Actor SDO Properties and Relationships

Threat Actor	
Required Common	R type
	R spec_version
	R id
	R created
	R modified
Optional Common	created_by_ref
	revoked
	labels
	confidence
	lang
	external_references
	object_marking_refs
	granular_markings
	extensions
Threat Actor Specific	R name
	description
	R threat_actor_types
	aliases
	first_seen
	last_seen
	roles
	goals
	sophistication
	resource_level
	primary_motivation
	secondary_motivation
	personal_motivations

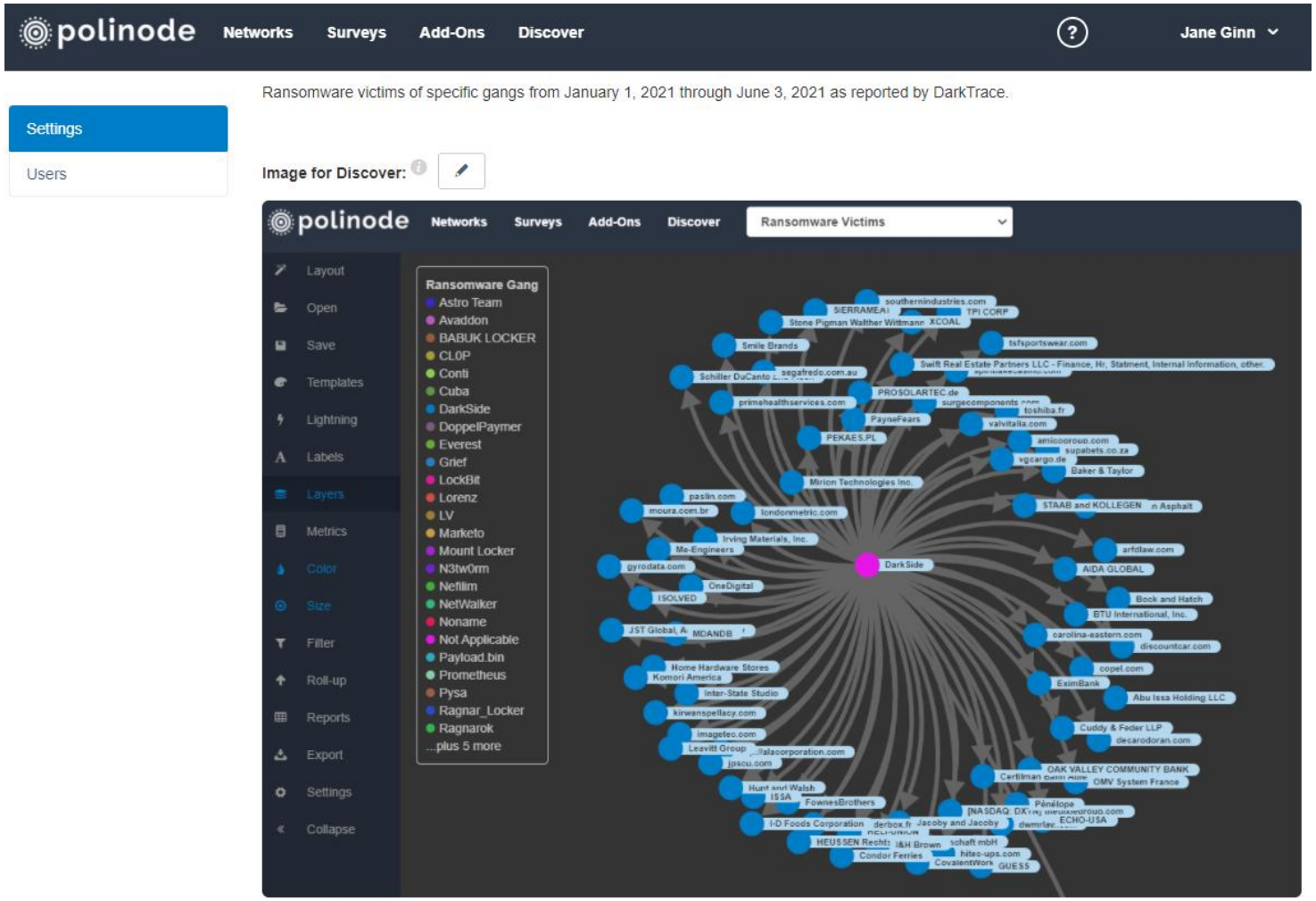


FireEye Cyber Observables (COs)



Source: OpenCTI TIP

Darkside Affiliates' Victims



One Indiana-based manufacturer of a food product was attacked by two different Darkside Affiliates within 10 days of each other.

Data Source: Darktracer https://darktracer.com/

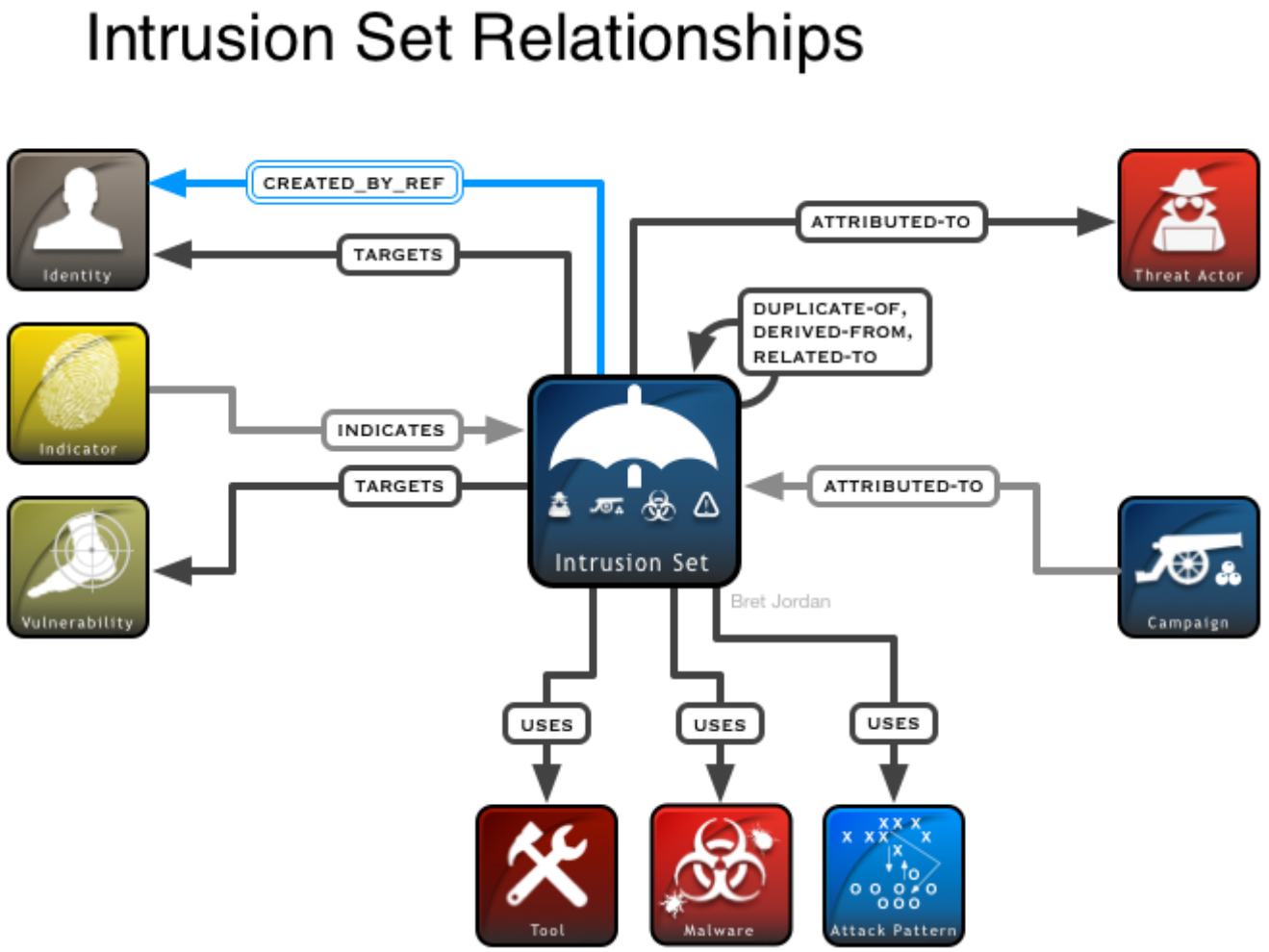
Threat Actor SDO

JSON

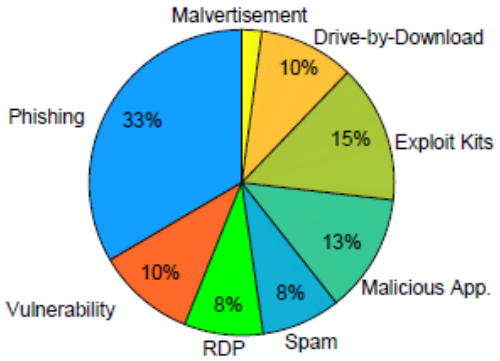

```
{
        "spec_version": "2.1",
        "type": “report",
        "objects": [
                {
                        "id": “threat-actor”--73d9cfca-0117-49d2-84f0-2105e00d7661",
                        "type": “threat-actor",
                        "created": "2021-06-07T20:39:07.006Z",
                        "modified": "2021-06-07T20:39:07.006Z",
                         "roles": [ “infrastructure-operator"],
                         “threat-actor-type": [ “crime-syndicate"],
                        "name": “Darkside Affiliate",
                        "description": “One of at least 47 Affiliates identified",
                        "valid_from": "2021-06-07T20:39:07.006Z"
                },
                {
```

Intrusion Set SDO Properties & Relationships

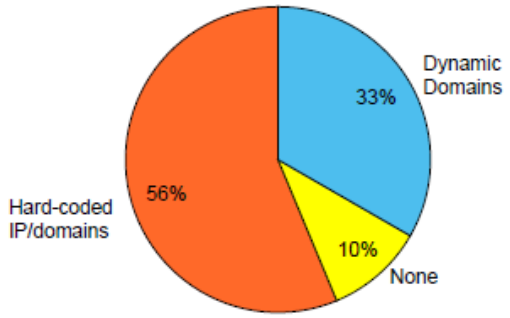
Intrusion Set		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Intrusion Set Specific	R	name
		description
		aliases
		first_seen
		last_seen
		goals
		resource_level
		primary_motivation
		secondary_motivations



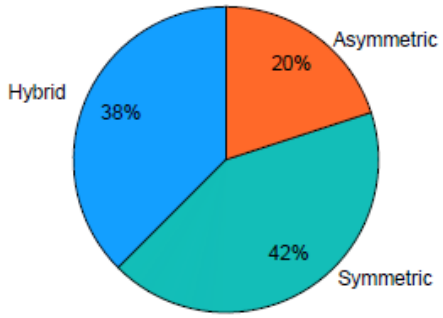
Distribution of Infection Types



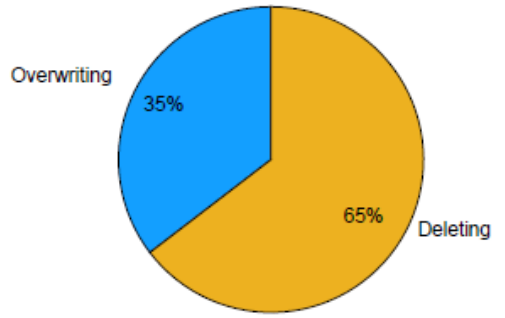
(a) Infection Methods



(b) C&C Communication



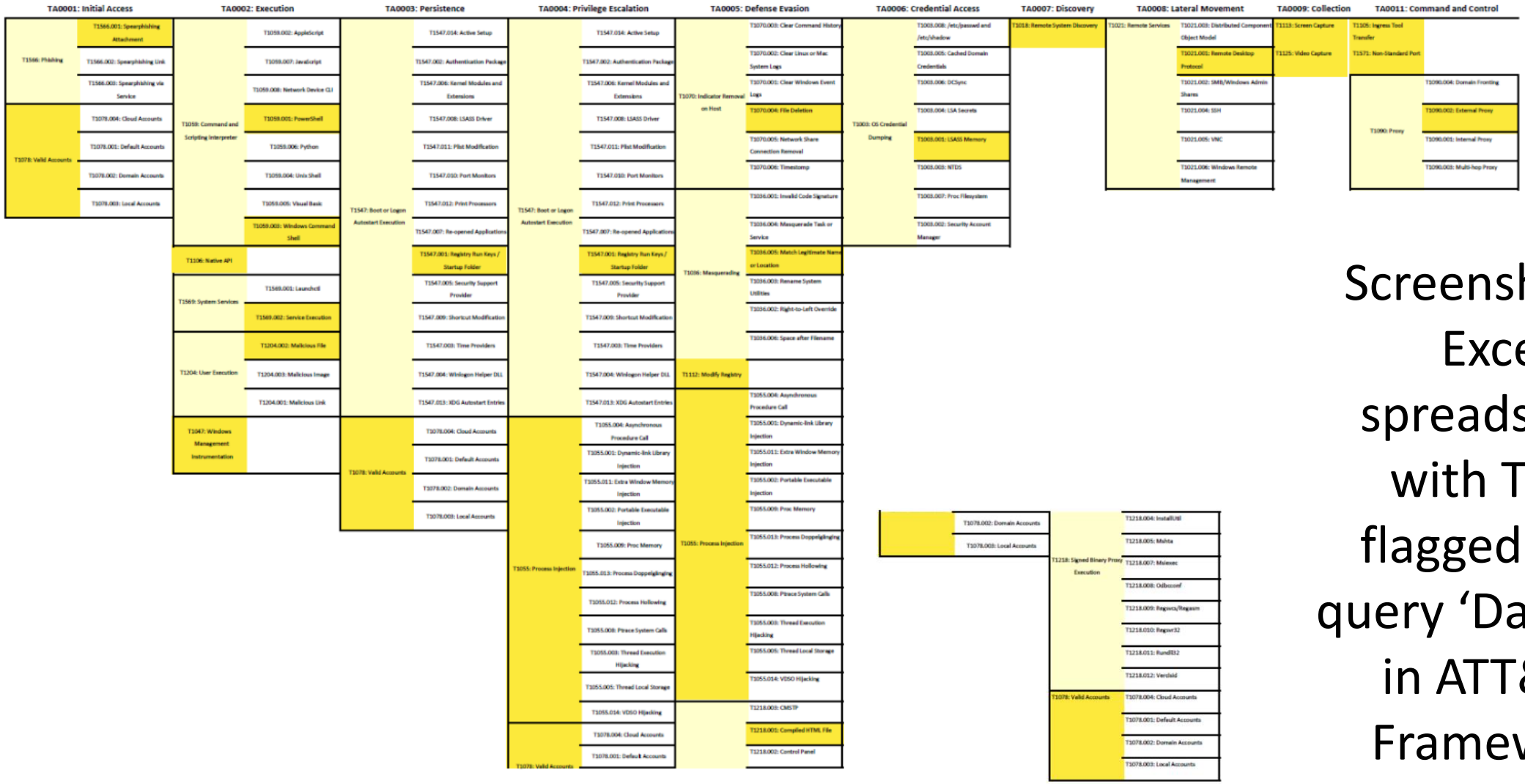
(c) Encryption Techniques



(d) Destruction Methods

Source: Harun Oz, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. 2021.A Survey on Ransomware: Evolution, Taxonomy, andDefense Solutions. ACMComput. Surv. 1, 1 (February 2021), 39 pages

Can Use Deductive Logic to Assign Intrusion Set SDO When Historical Data in MITRE ATT&CK



Screenshot of Excel spreadsheet with TTPs flagged with query ‘Darkside’ in ATT&CK Framework

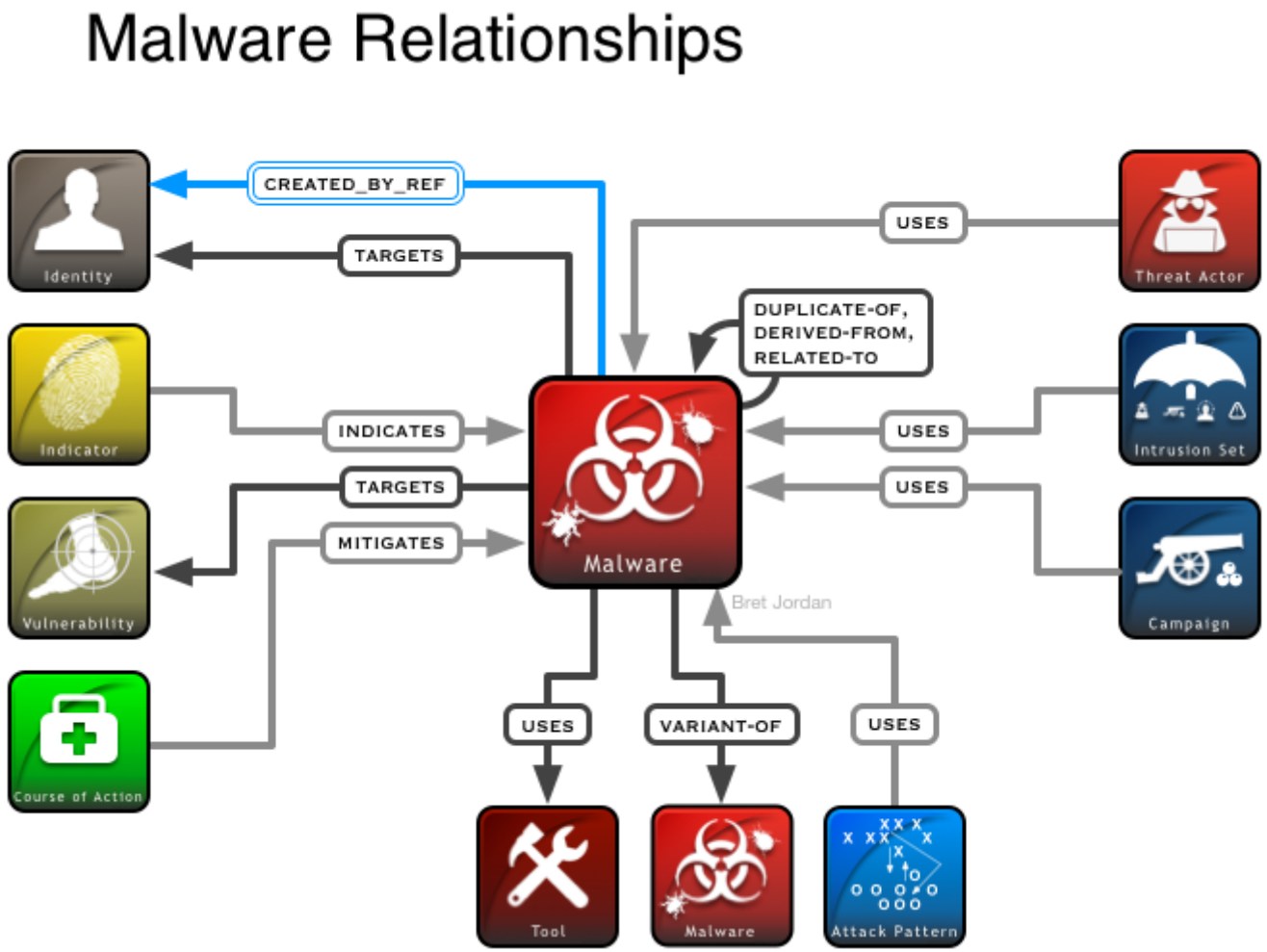
Intrusion Set SDO

JSON

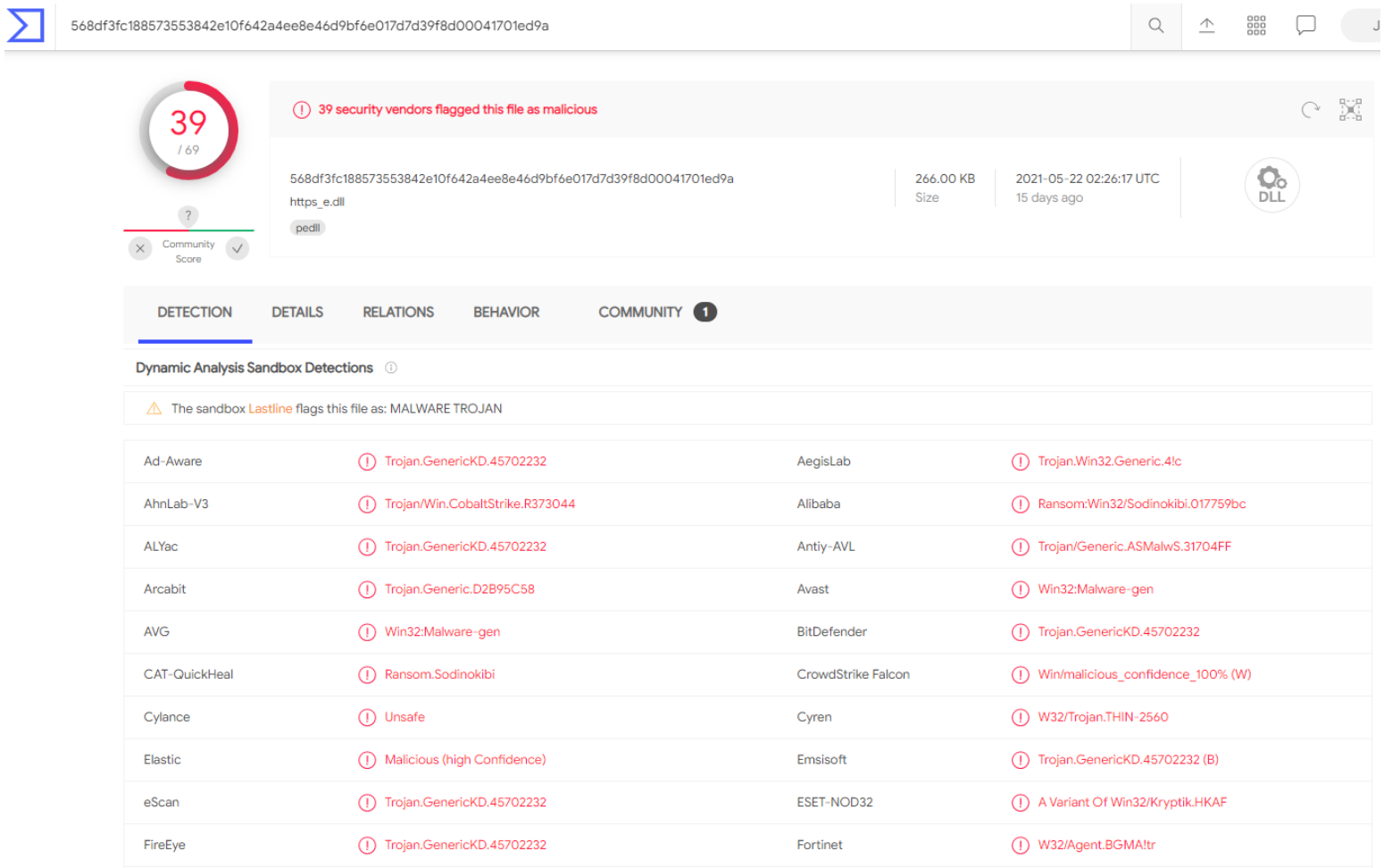

```
{
    "spec_version": "2.1",
    "type": “report",
    "objects": [
        {
            "id": “intrusion-set”--73d9cfca-0117-49d2-84f0-2105e00d7662",
            "type": “intrusion-set",
            "created": "2021-06-07T20:39:07.006Z",
            "modified": "2021-06-07T20:39:07.006Z",
             “labels": [ “FIN7", “Carbon Spider“, “Carbanak” ],
             “primary motivation": [ “financial-gain"],
            "name": “APC-Darkside",
            "description": “Darkside and predecessor crime-syndicates",
            "valid_from": "2021-06-07T20:39:07.006Z"
        },
        {
```

Malware SDO Properties & Relationships

Malware		
Required Common	R	type
	R	spec_version
	R	id
	R	created
	R	modified
Optional Common		created_by_ref
		revoked
		labels
		confidence
		lang
		external_references
		object_marking_refs
		granular_markings
		extensions
Malware Specific		name
		description
	R	malware_types
	R	is_family
		aliases
		kill_chain_phases
		first_seen
		last_seen
		os_execution_envs
		architecture_execution_envs
		implementation_languages
		capabilities
		sample_refs



Malware – Shown on VirusTotal



Domain from CP CO Reporting:
lagrom.com

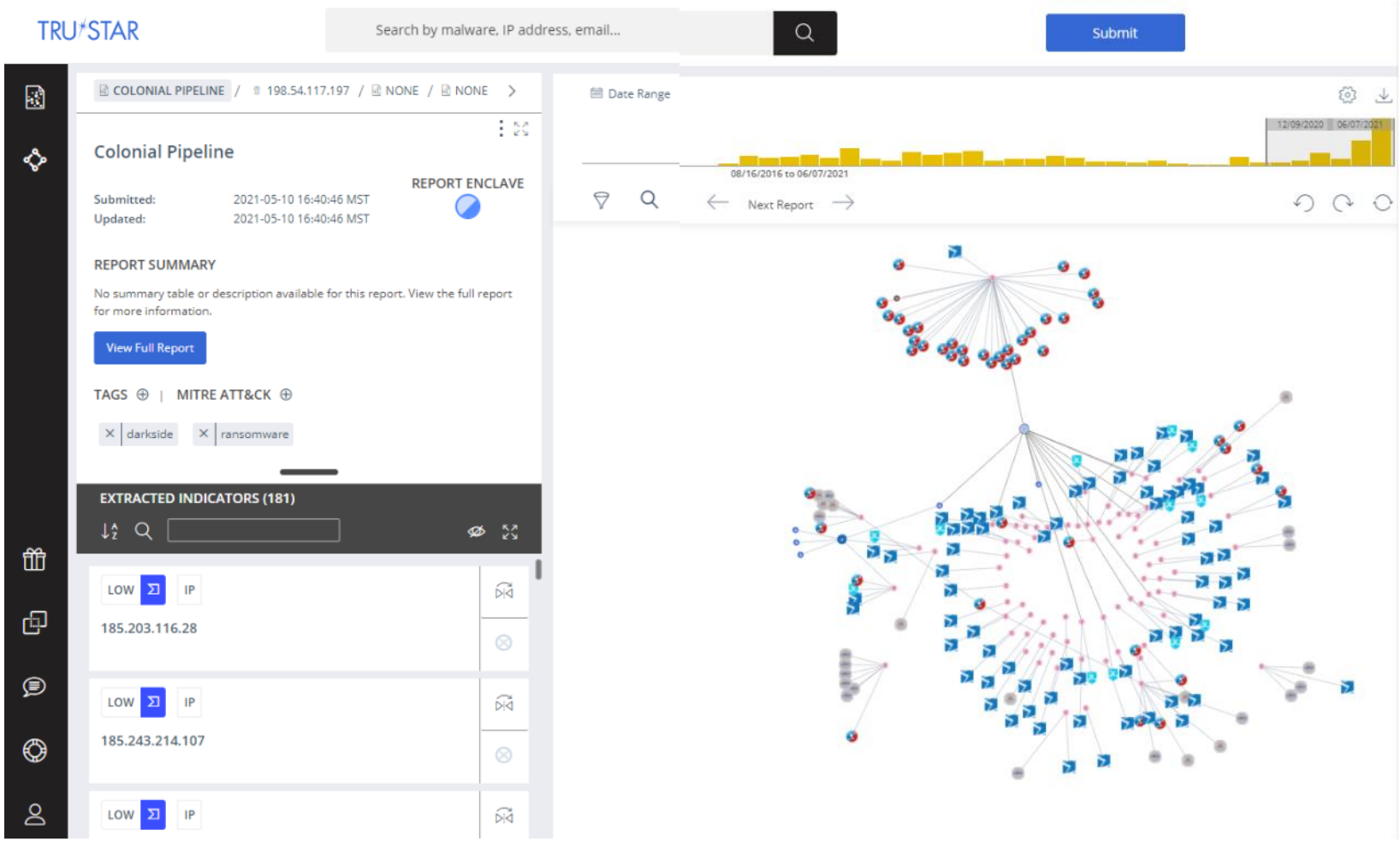
MD5 Hash from CP CO Reporting:
5f1e9ae81c6a3797bf16b9ee469dc66a

File Name:
https_e.dll

Resolves to IPv4:
104.193.252.197

Source: VirusTotal

Overlapping Infrastructure



Domain from CP CO Reporting:
lagrom.com

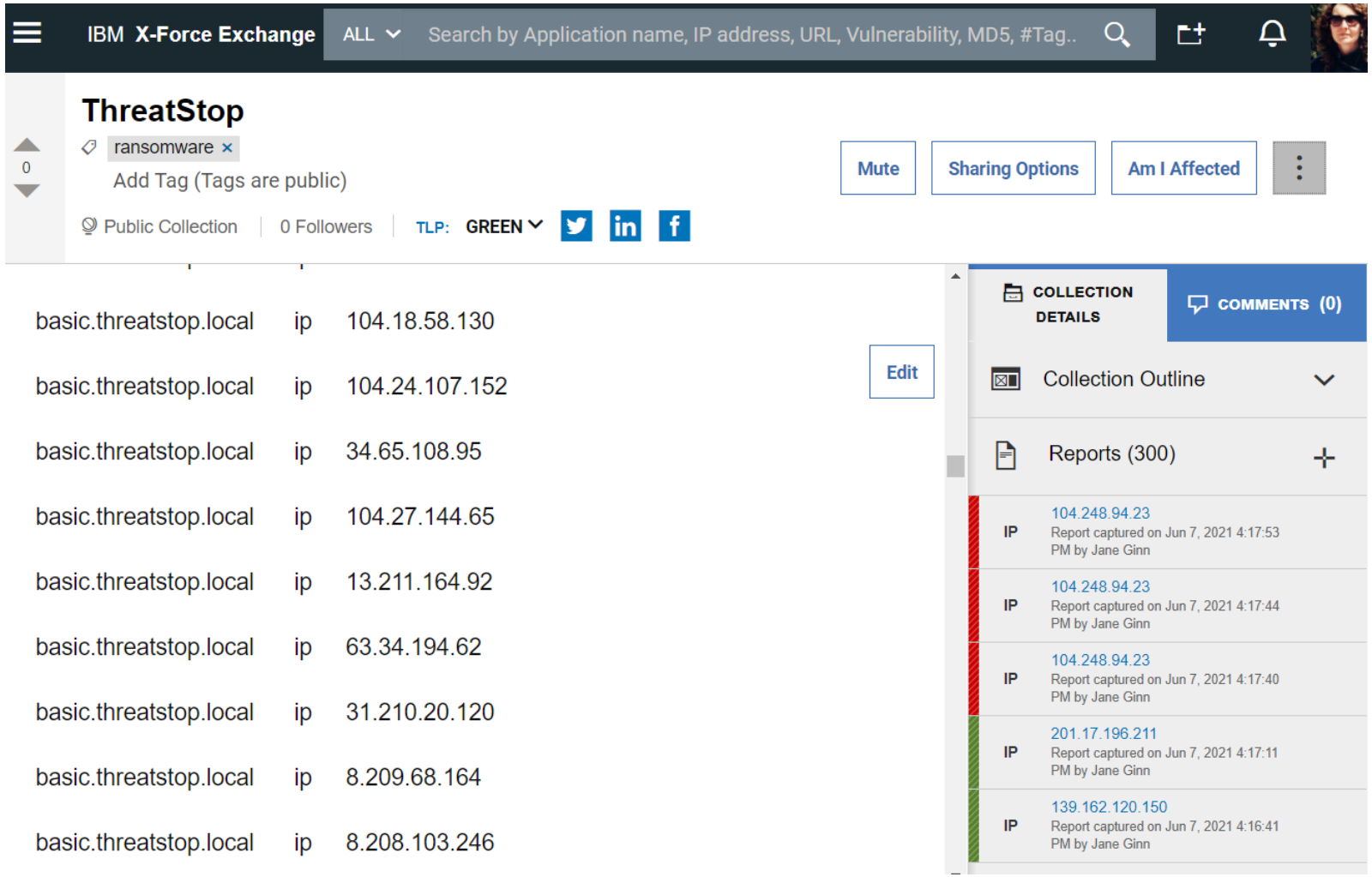
MD5 Hash from CP CO Reporting:
5f1e9ae81c6a3797bf16b9ee469dc66a

File Name:
https_e.dll

Resolves to IPv4:
104.193.252.197

Source: TRUSTAR TIP

Multiple Sightings of COs Shown on XFE



Source: IBM TIP

OSINT Analysis

Malware SDO

JSON


```
{
        "spec_version": "2.1",
        "type": “report",
        "objects": [
                {
                        "id": “malware”--73d9cfca-0117-49d2-84f0-2105e00d7664",
                        "type": “malware",
                        "created": "2021-06-07T20:39:07.006Z",
                        "modified": "2021-06-07T20:39:07.006Z",
                         “malware_types": [ “ransomware"],
                         “is_family": [ “true"],
                        “capabilities": “communicates-with-c2",
                        "description": “Sodinokibi trojan",
                        "valid_from": "2021-06-07T20:39:07.006Z"
                },
                {
```

Access Yara Rules on VirusTotal

```
}

rule HKTL_CobaltStrike_Beacon_Strings {
  meta:
    author = "Elastic"
    description = "Identifies strings used in Cobalt Strike Beacon DLL"
    reference = "https://www.elastic.co/blog/detecting-cobalt-strike-with-memory-signatures"
    date = "2021-03-16"
  strings:
    $s1 = "%02d/%02d/%02d %02d:%02d:%02d"
    $s2 = "Started service %s on %s"
    $s3 = "%s as %s\\%s: %d"
  condition:
    2 of them
}
```

Darkside Re-Emerges as Black Matter

BlackMatter
byte

B

Seller
0
1 post
Joined
07/19/21 (ID: 118280)
Activity
другое / other
Deposit
4.000000 Ƀ

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- THAT.
- TO.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue от 100kk+.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

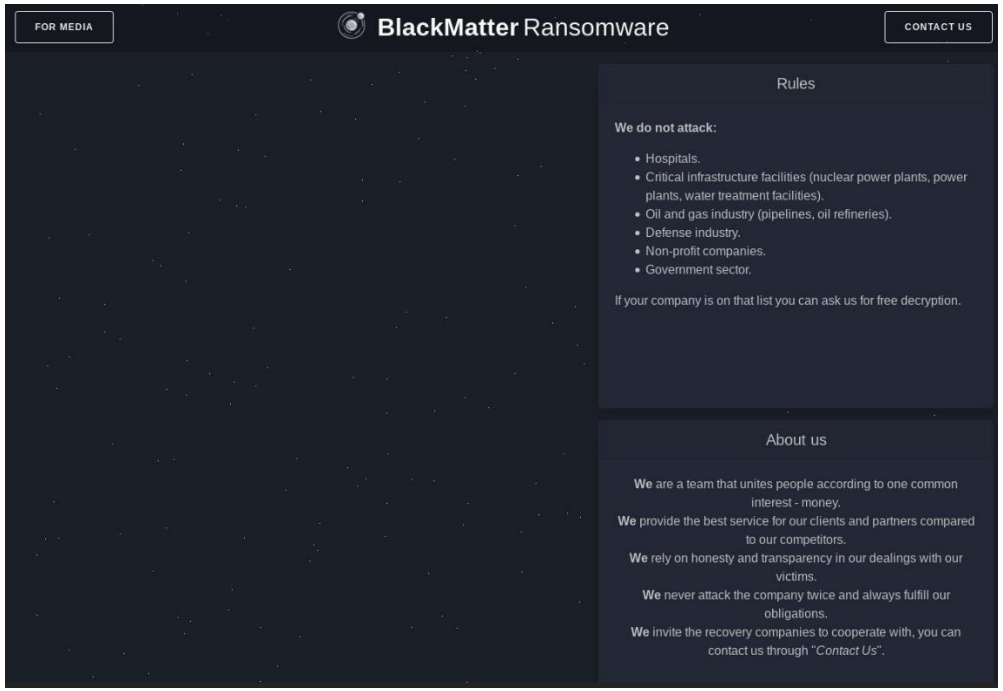
2 options for work:

- We buy: From 3 to 100k.
- We take it to work (discussed individually).

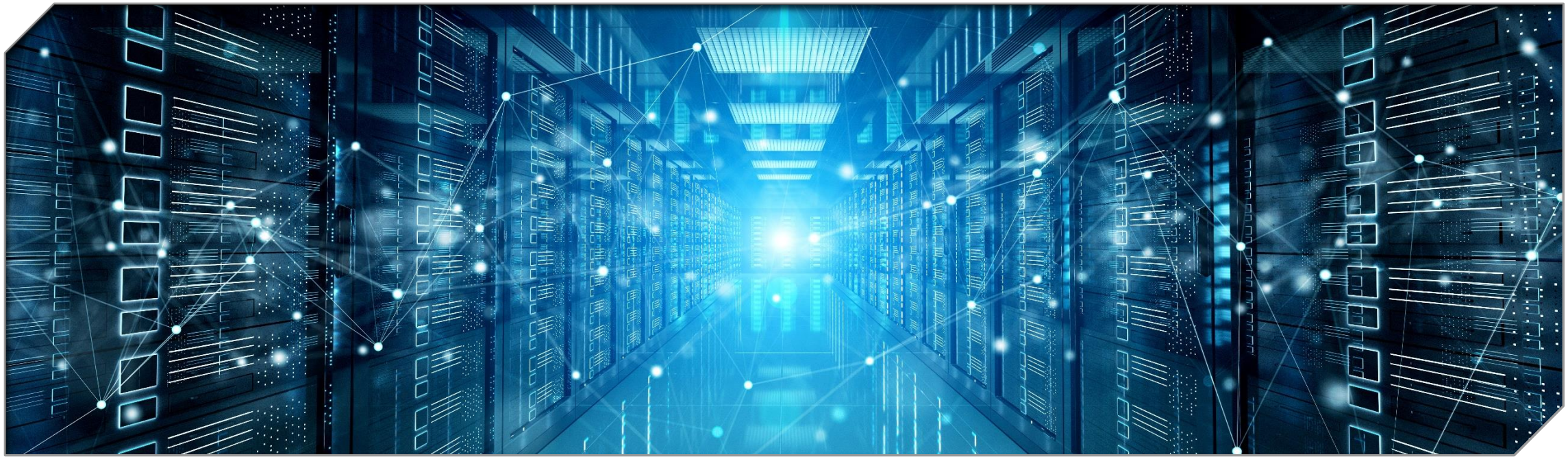
Scheme of work:
Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

Deposit: 120k.

First contact of the PM. We are looking first of all for stable and adequate suppliers.



https://www.recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/



Interoperability

Moving Forward

STIX PREFERRED PROGRAM

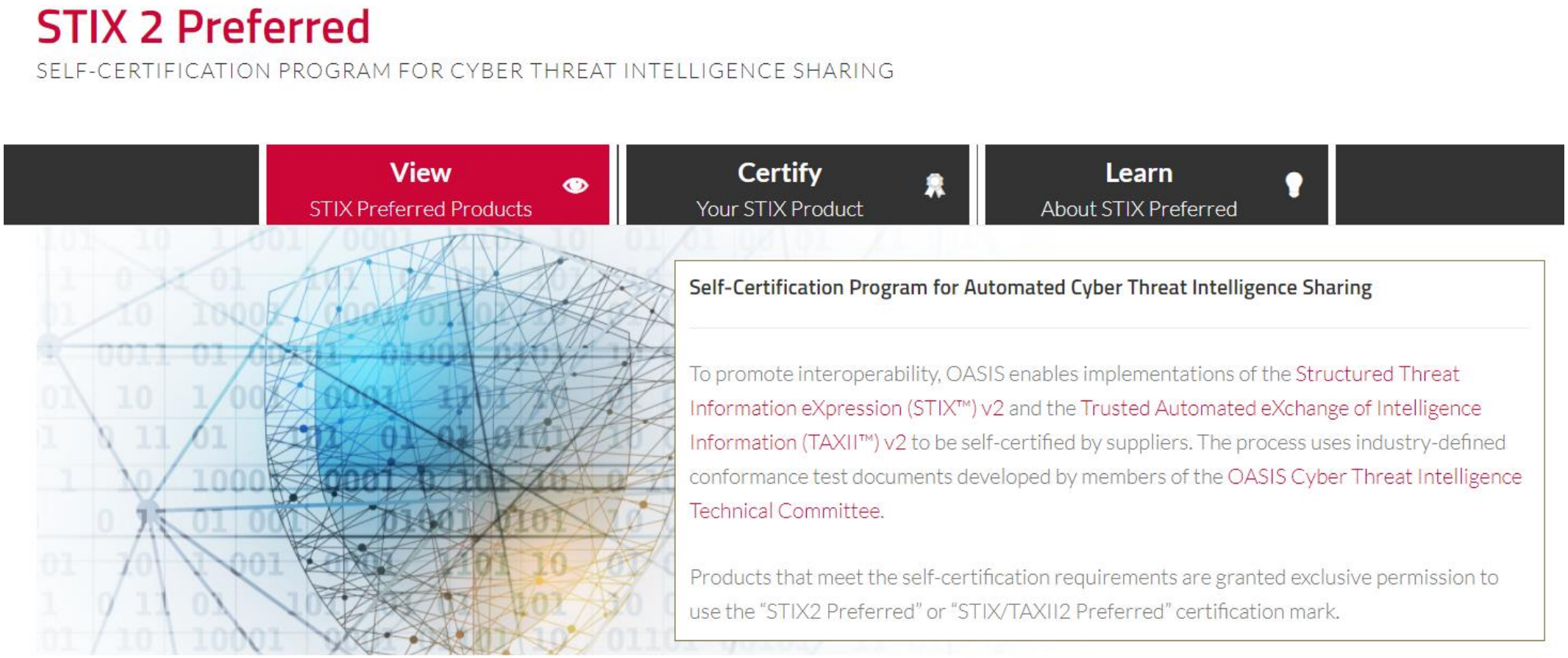
STIX2

- Data Feed Provider (DFP)
- Threat Intelligence Platform (TIP)
- Security Incident and Event Management (SIEM)
- Threat Mitigation System (TMS)
- Threat Detection System (TDS)
- Threat Intelligence Sink (TIS)

STIX2 & TAXII2

- TAXII Server (TXS)
- TAXII Feed Server (TFF)

STIX 2 PREFERRED SELF-CERTIFICATION



https://oasis-stixpreferred.org/

Current Limitations

- Volume and relevance limitations
- Data collection
    - Unique ability to collect from different sources
    - Confidence | Provenance | Reliability | Quality Validation | TTL
- Trust related issues
    - Access Control | Legal & Institutional Features | Culture
- Limited analysis capabilities including analytics & automation
- Diverse data models, formats & ability to handle APIs
- Limited workflow enablement (e.g., potential ticketing system)

Current Opportunities

- Organizations
- TIP Users
- TIP Developers/Vendors
- Intelligence Producers
- CTI Community and Researchers

- Analysis capabilities and TIPs
- Trust modelling functionalities
- Usage of APIs, integration and workflows
- Threat data quality enhancement
- Flexible threat data management

- Enhancing the quality of shared information
- Coherent use of the standards

Summary

- **About Colonial Pipeline Hack**
- **About RaaS Use Case**
- **Modeled SDOs:**
  - Indicator
  - Threat Actor
  - Intrusion Set
  - Malware
- **Importance of Interoperability**

rjg@ctin.us