



University of Oslo Working Session
August 19, 2021

Using STIX2.1 for Modeling **Ransomware Attacks**

RaaS Use Case



Jane Ginn

MSIA, MRP

rjg@ctin.us

Co-Founder, CTIN

Co-Secretary, CTI TC @ OASIS

Secretary, TAC TC & OASIS

Secretary/Treasurer,

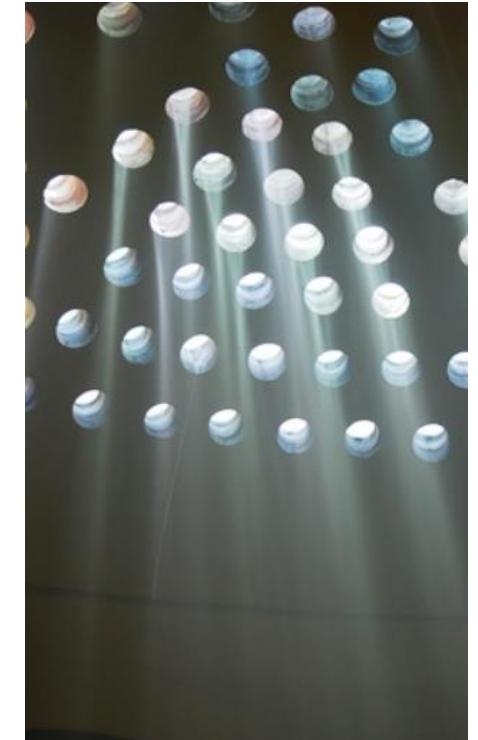
Cyber Resilience Institute

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



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





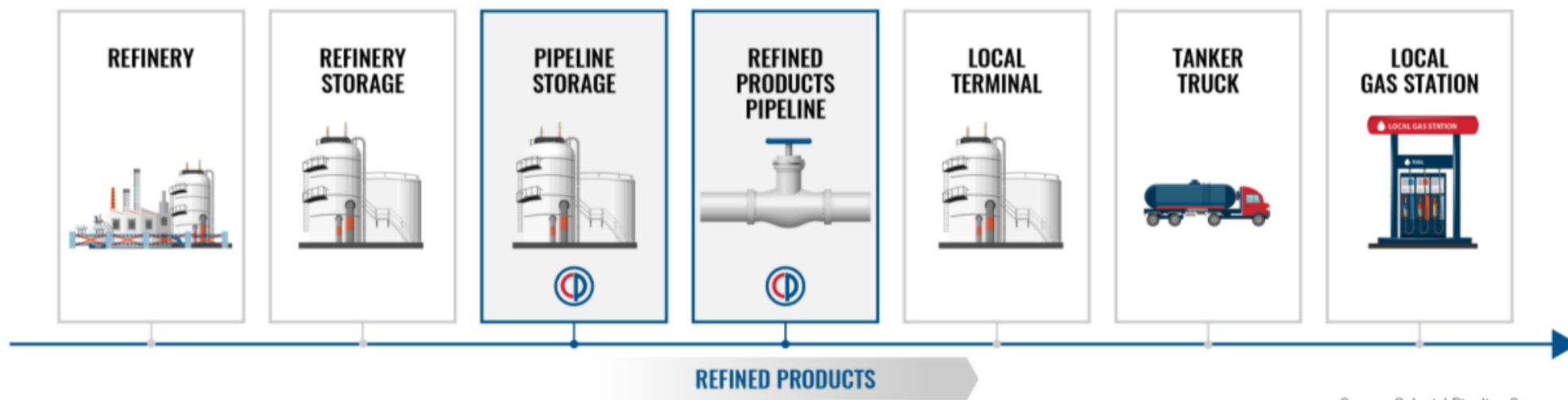
Colonial Pipeline

*Infrastructure
Attack*

Colonial Pipeline: Role in Supply Chain



Colonial's Role In The Supply Stream



Source: 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





Darkside RaaS

Affiliate Business Model

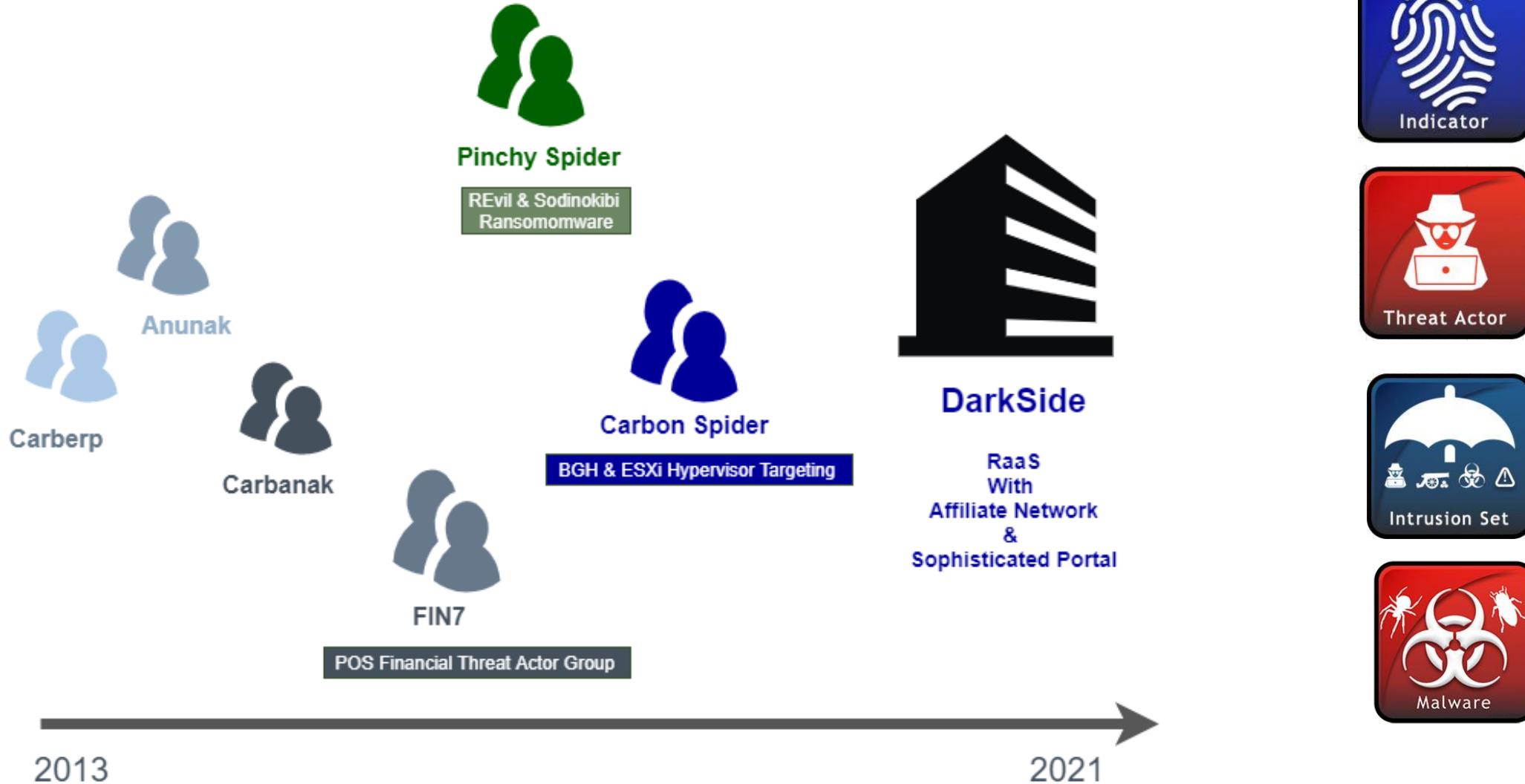
Geopolitical Context

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

SHARE

U.S. Attorney's Office

Western District of Washington

FOR IMMEDIATE RELEASE

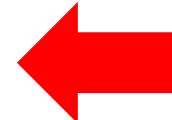
Friday, April 16, 2021

**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 Ukrainian 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."

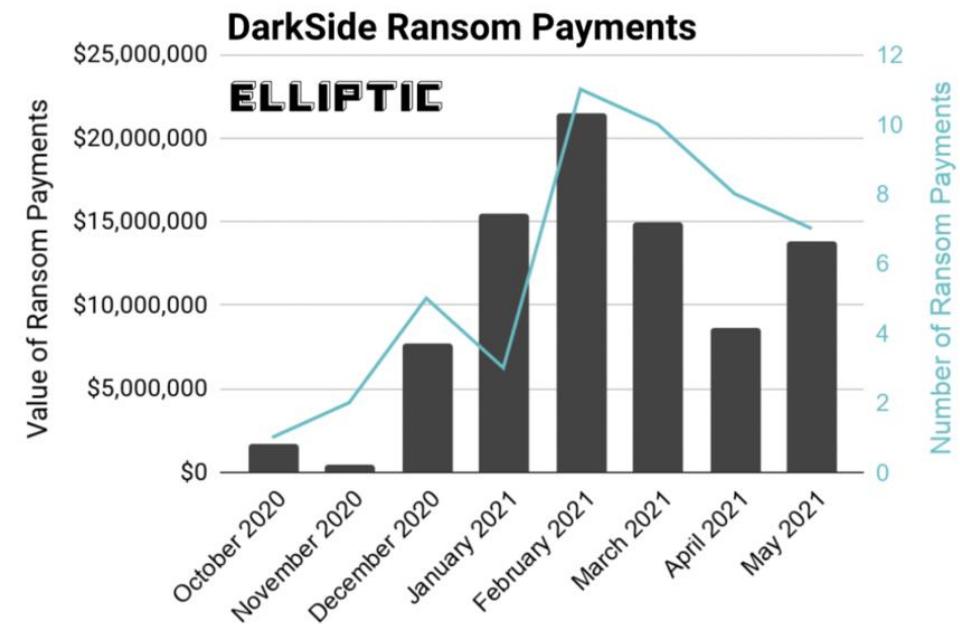


**George Grasso, Attorney for FIN7 CEO
Fedir Hiadry a Ukrainian National.**

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

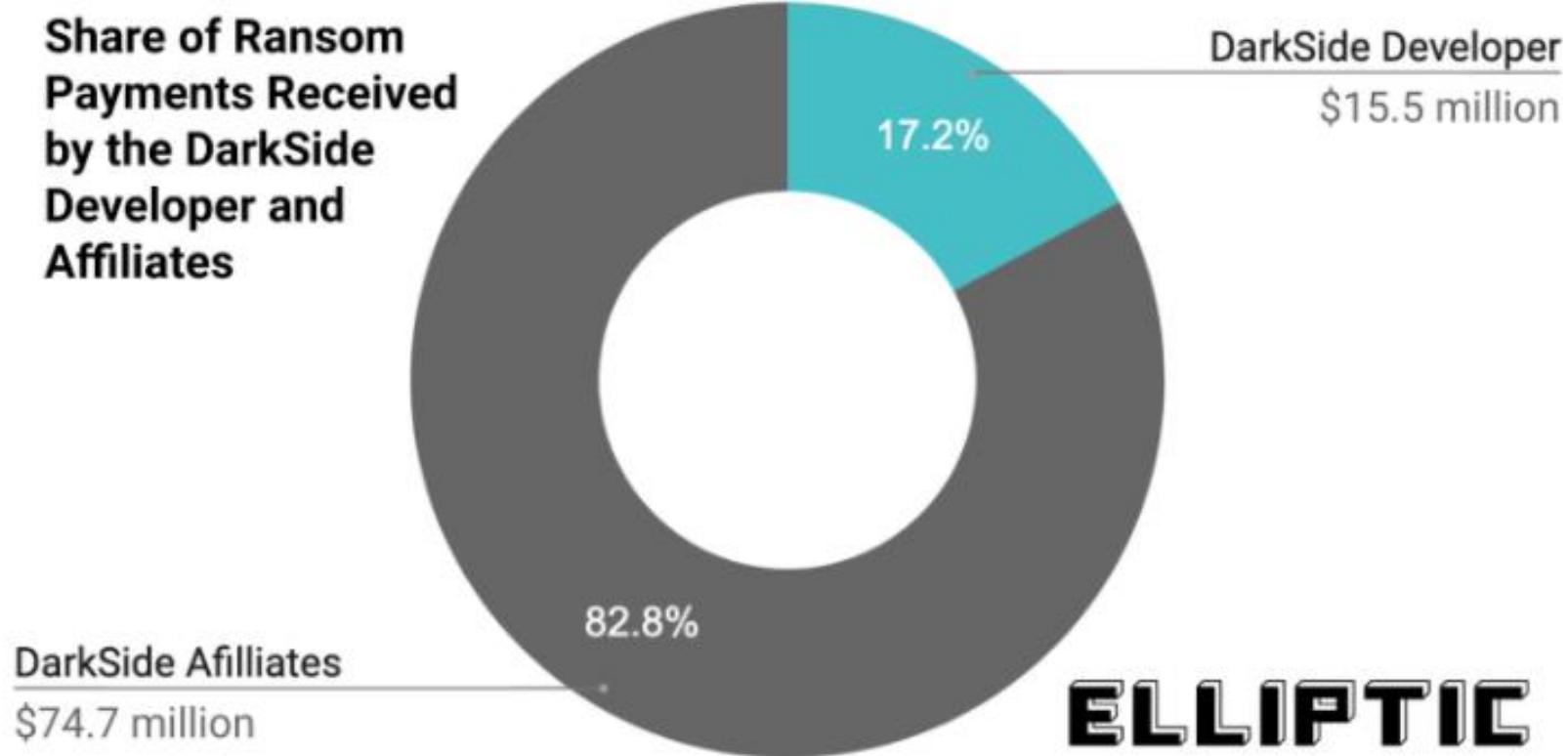
Darkside Profitability

- 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.

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:

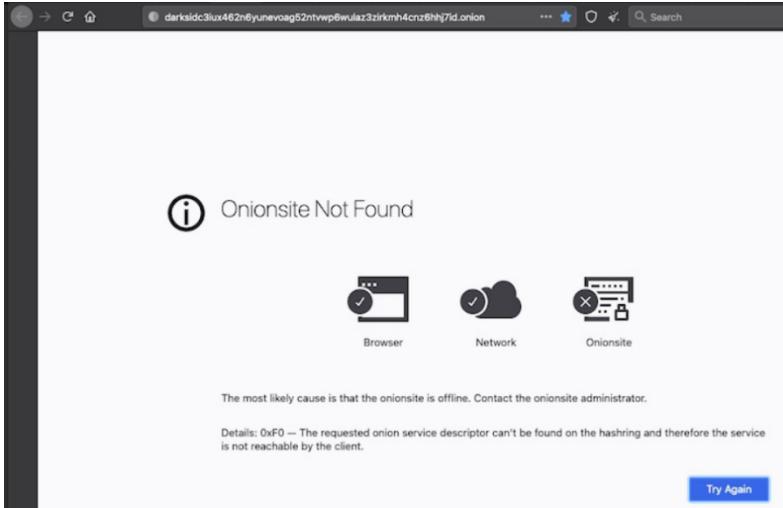
- Вам будут выданы декрипторы ко всем компаниям, кто еще не оплатил. Дальше вы можете общаться как угодно и где угодно. **Пишите саппорту**.
- Мы выведем депозит для закрытия вопросов перед пострадавшими пользователями. Предположительная дата выдачи компенсаций: **23.05** (в связи с холдом вывода депозита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

 **OASIS**
Open standards. Open source.

Other Languages ■ Site Map ■ Member Login

I want to:

[Standards](#) | [Committees](#) | [Join](#) | [News](#) | [Events](#) | [Resources](#) | [Member Sections](#) | [Policies](#) | [About](#)

OASIS Cyber Threat Intelligence (CTI) TC

[Join This TC](#) [TC Members Page](#) [Send A Comment](#)

Supporting automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis

Richard Struse, rjs@mitre.org, Chair
Trey Darley, trey.darley@cert.be, Chair
Jane Ginn, jg@ctin.us, Secretary

Table of Contents

- Announcements
- Overview
- Subcommittees
- TC Liaisons
- TC Tools and Approved Publications
- Technical Work Produced by the Committee
- OASIS TC Open Repositories Sponsored by the Committee
- Expository Work Produced by the Committee
- External Resources
- Mailing Lists and Comments
- Press Coverage and Commentary
- Additional Information

Search

Connect with OASIS
 [RSS](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#) [Google+](#)

Related links

[Charter](#)
[IPR Statement](#)
[Membership](#)
[Obligated Members](#)
[Email Archives](#)
[Comments Archive](#)
[Ballots](#)
[Documents](#)
[Schedule](#)

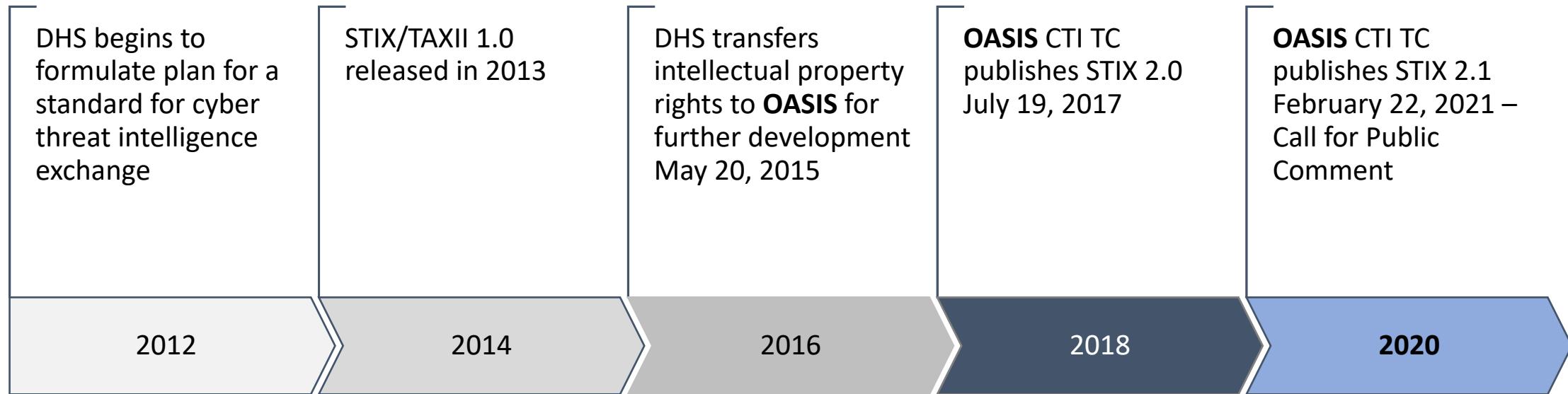
TC Participants

Representing these OASIS Foundamentals and Sponsors:

360 Enterprise Security

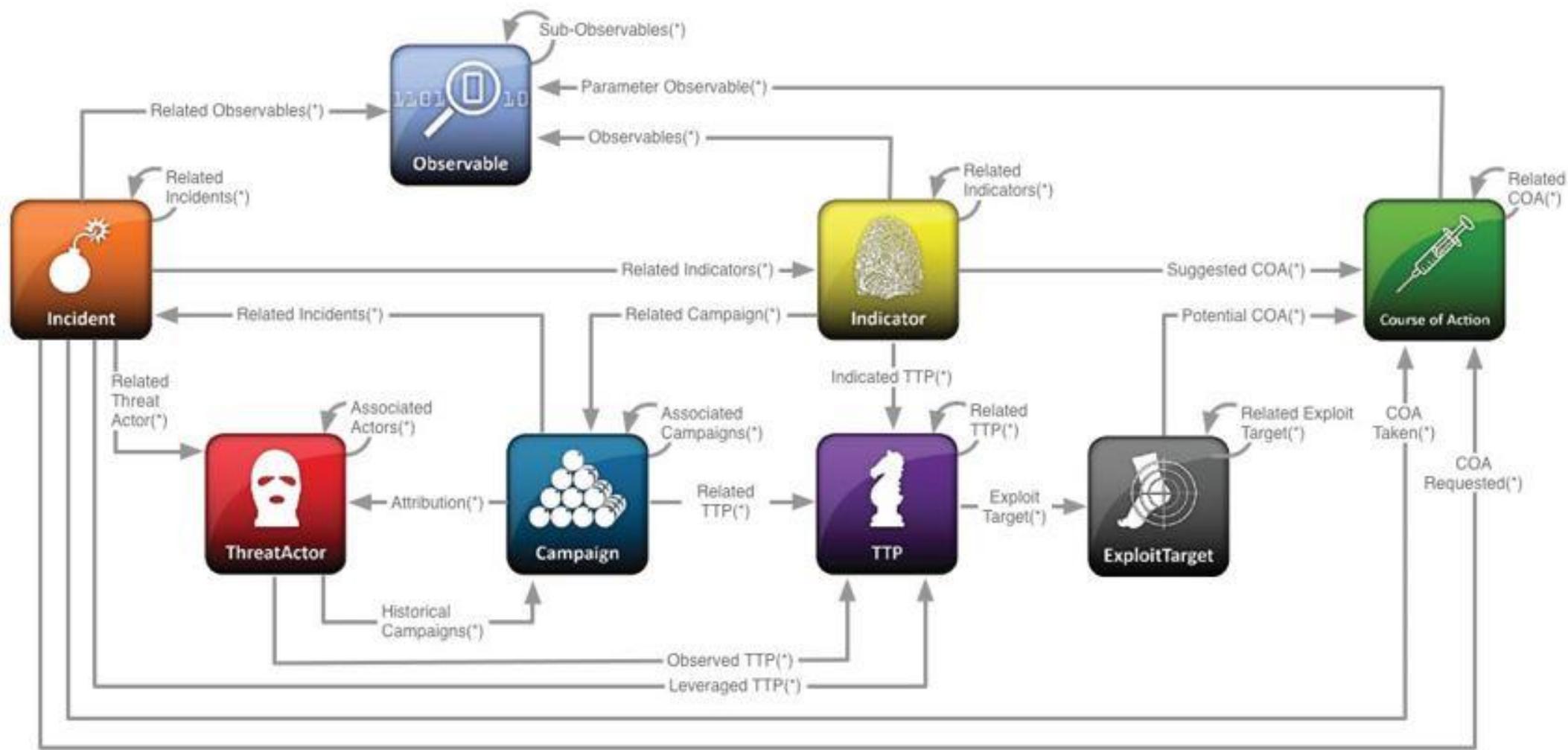
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

Development of STIX Standard



				ANOMALI		
Hewlett Packard Enterprise						

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

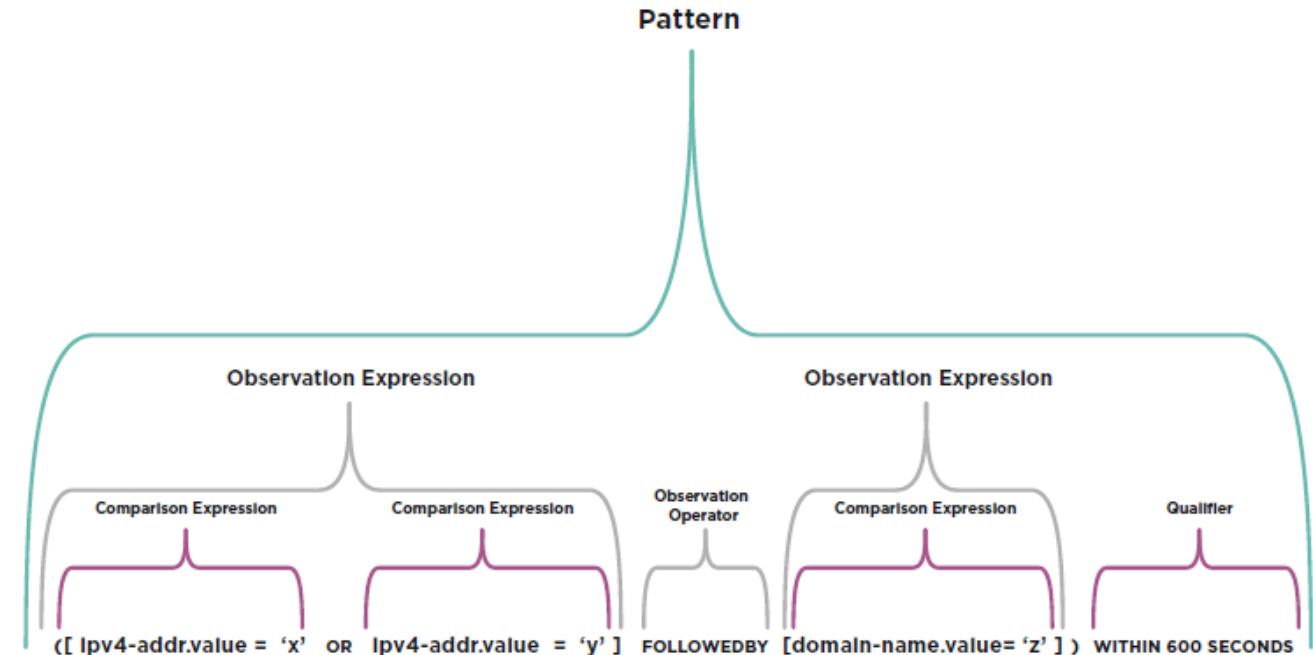
Some Key Design Principles:

- 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**

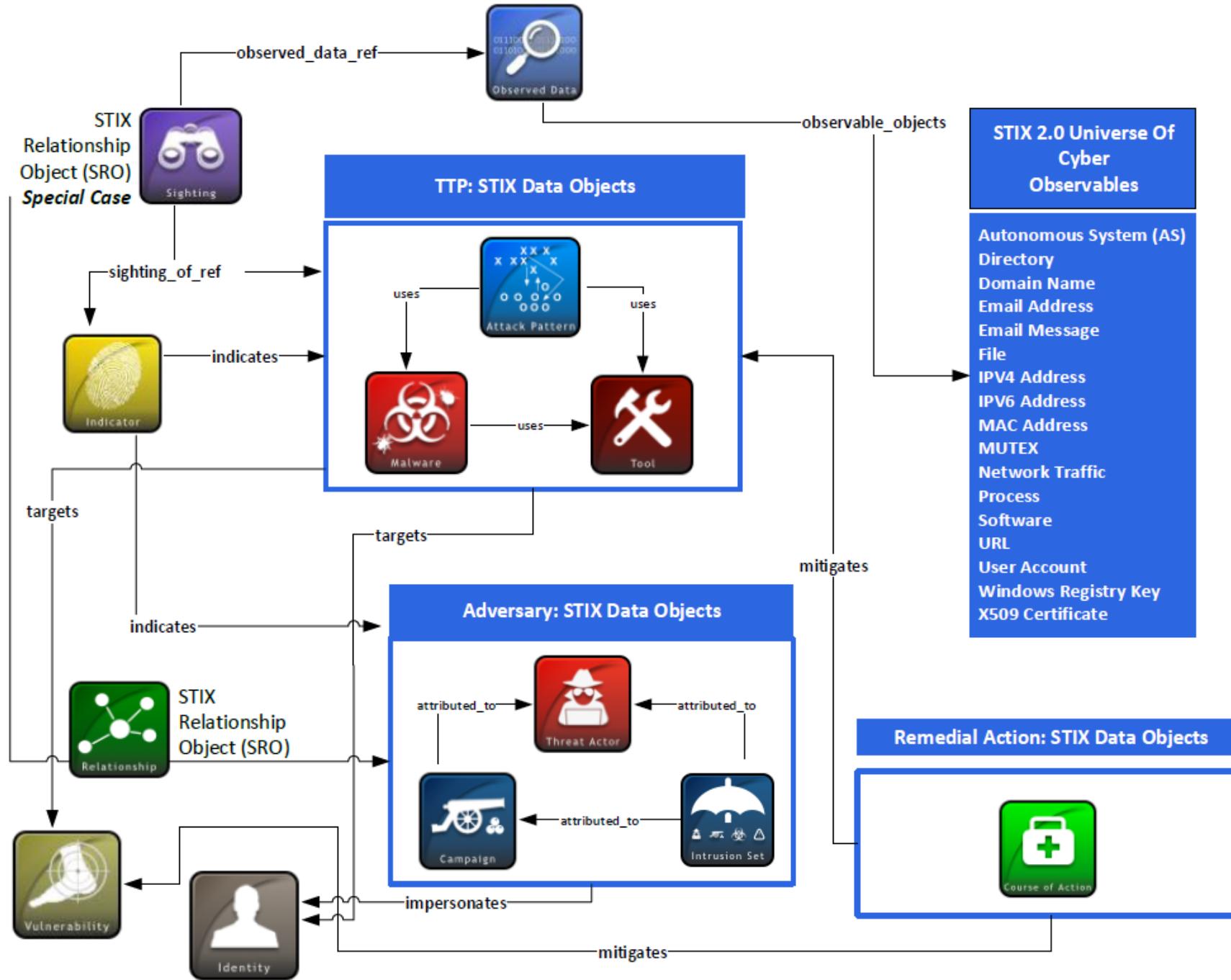
Key Changes from STIX 1.1 to 2.0

- Added Patterning Language



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





Key Changes from STIX 2.0 to 2.1

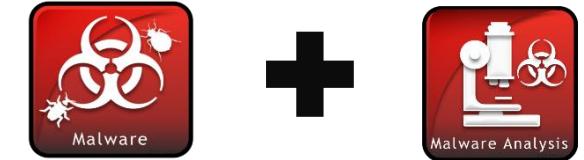
- Added ‘Language’ Meta Object



- 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



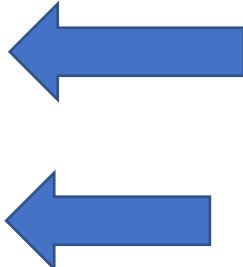


Modeling Attacks

STIX2.1

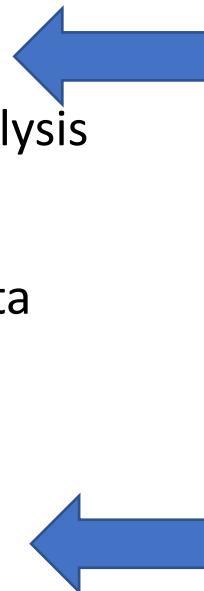
STIX Domain Objects (SDOs)

- 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

- 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

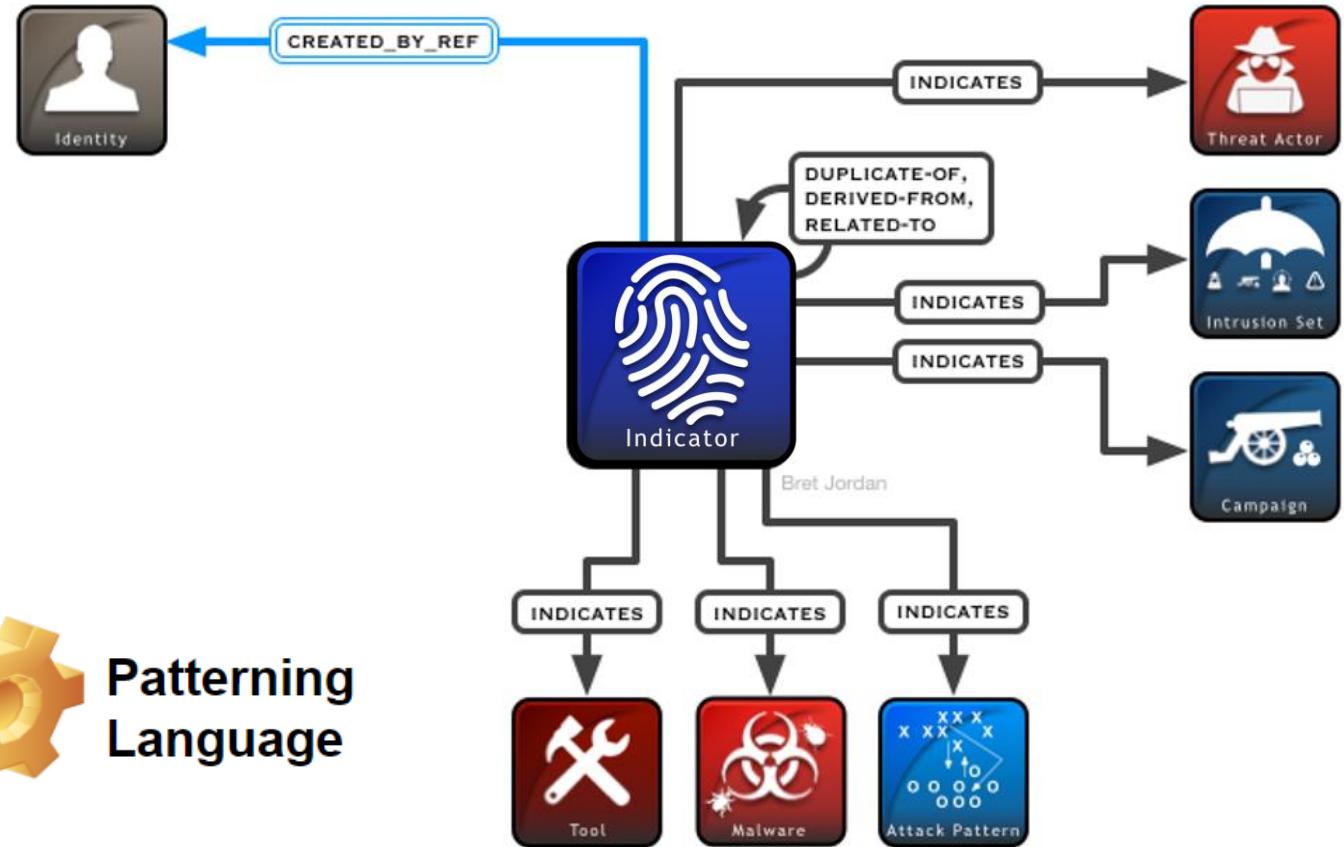
In FBI
Flash

Indicator SDO Properties & Relationships

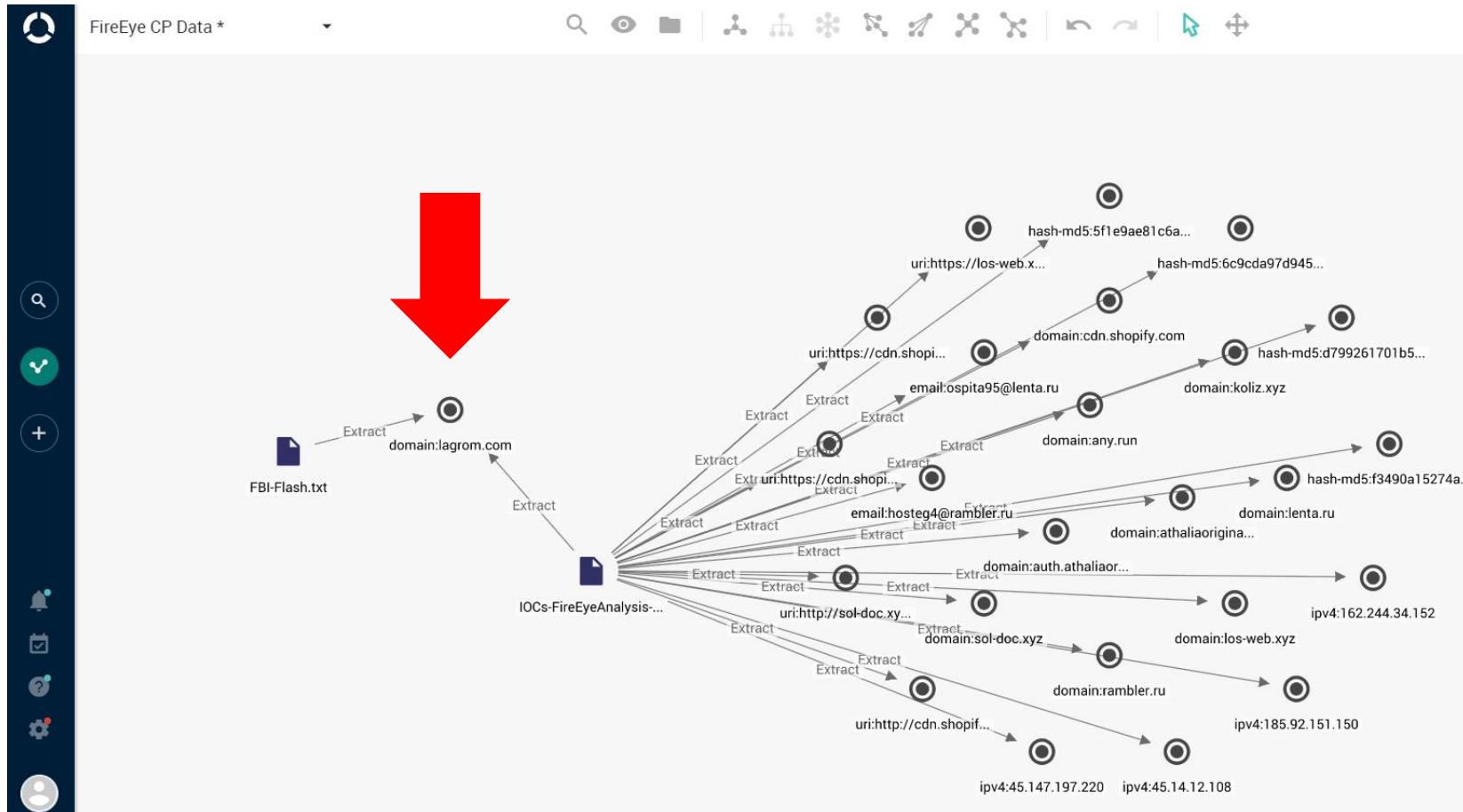
Indicator	
Required Common	R type R spec_version R id R created R modified
Optional Common	created_by_ref revoked labels confidence lang external_references object_marking_refs granular_markings extensions
Indicator Specific	name description R indicator_types R pattern R pattern_type pattern_version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



Patterning
Language

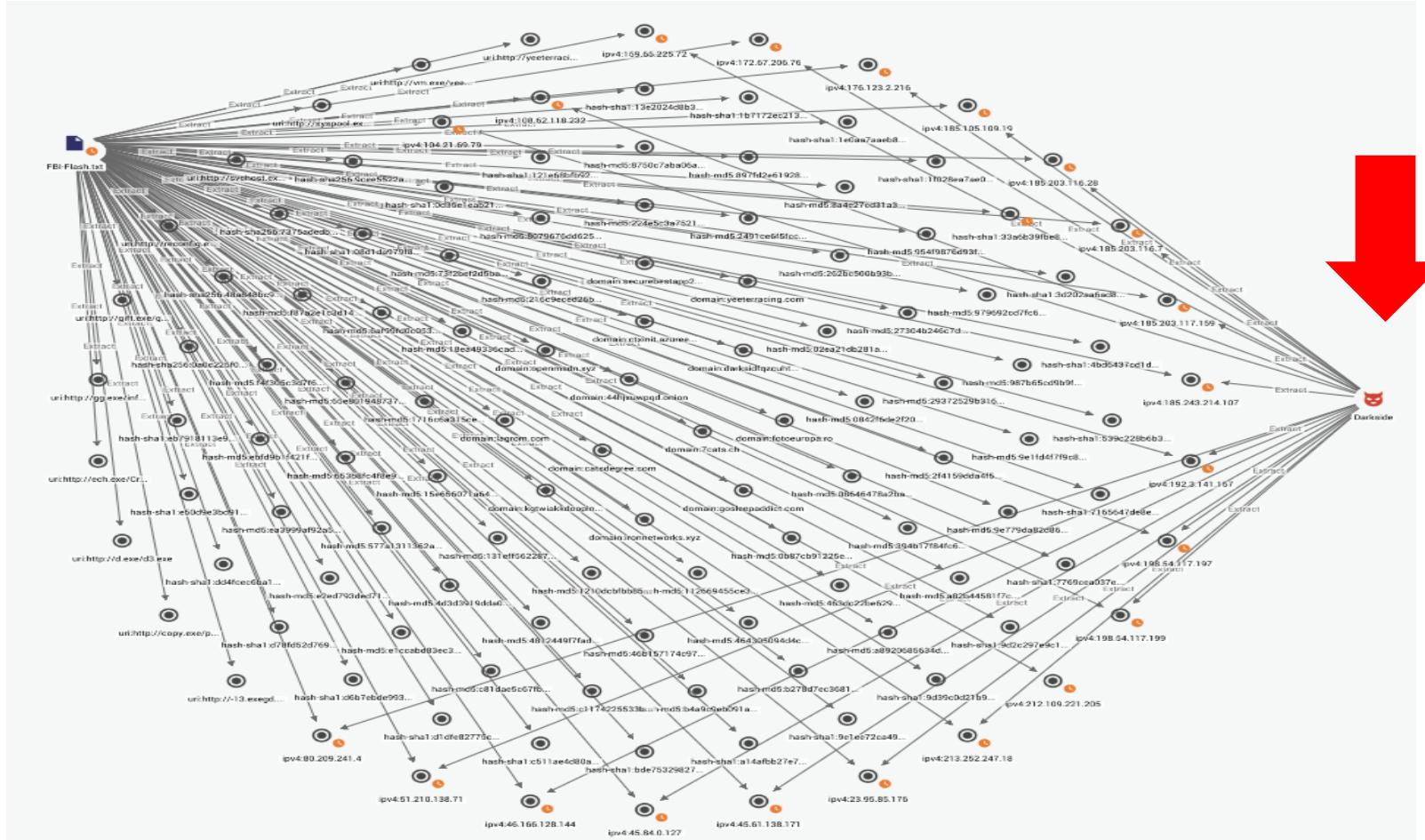


Graph: FBI-FireEye Correlation Point



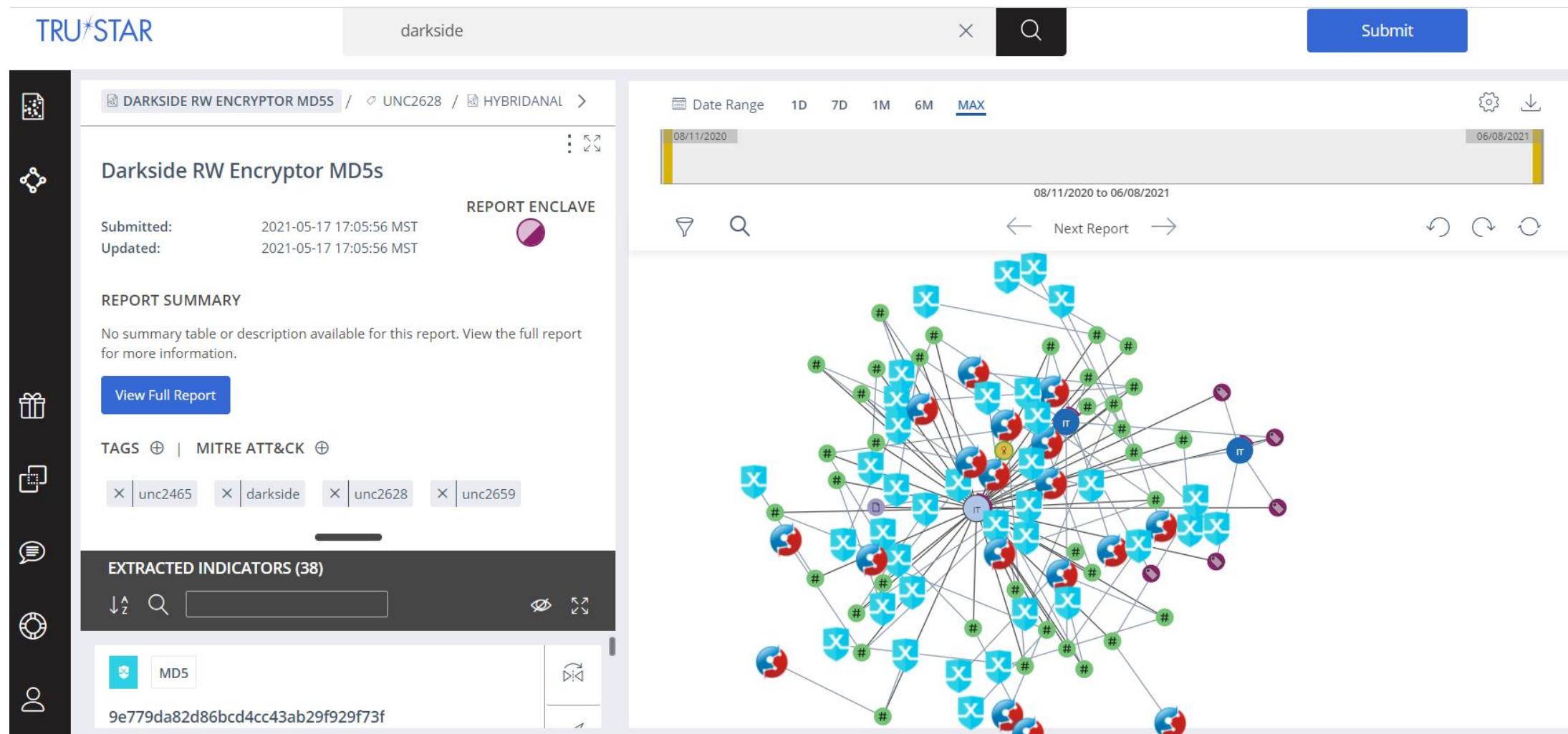
Source: EclecticIQ TIP

Graph: FBI-FireEye Corroborate on DS



Source: EclecticIQ TIP

Property Graph Representation



Source: TRUSTAR TIP

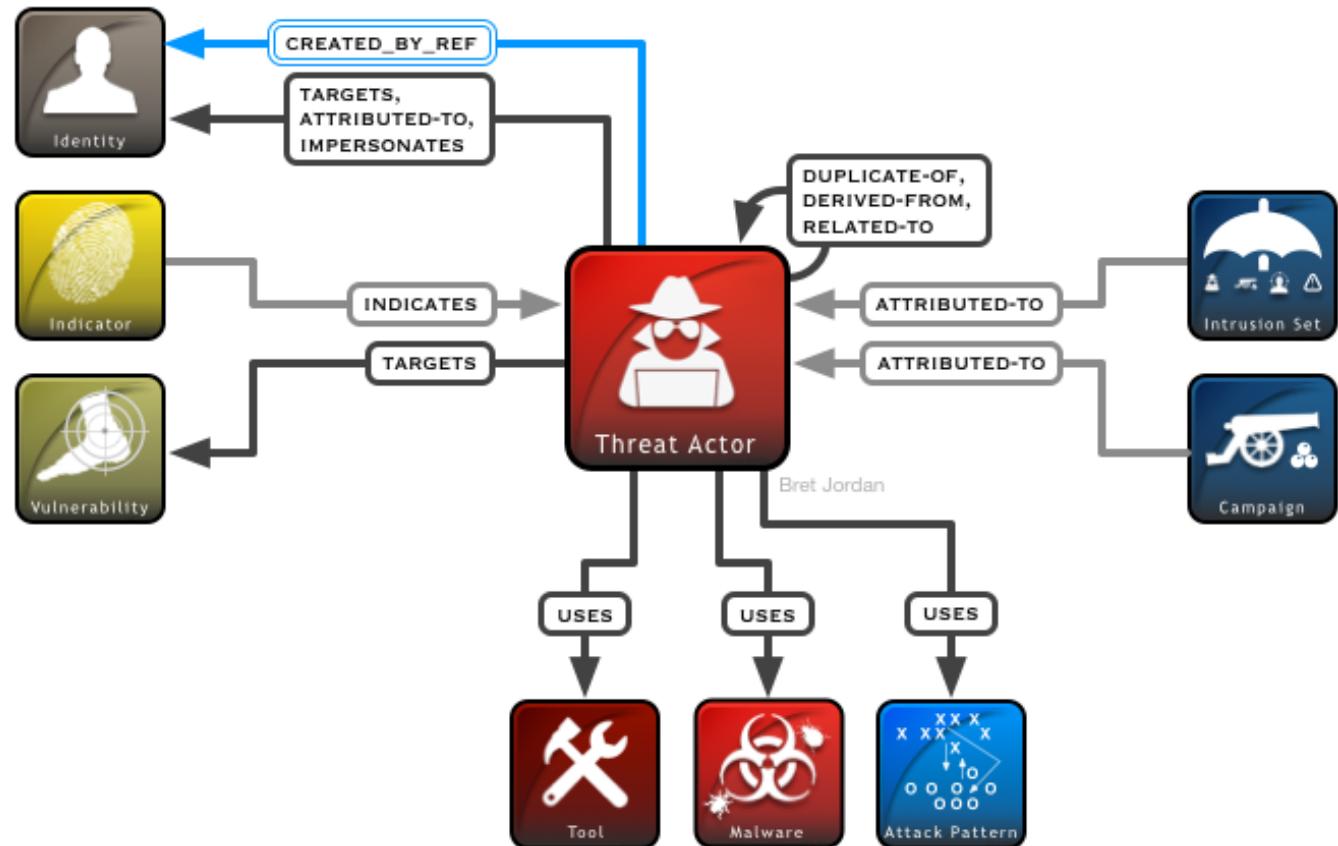
Indicator
SDO +
Patterning
Language

```
{  
    "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://lagrom.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

Threat Actor Relationships



FireEye Cyber Observables (COs)

The screenshot displays the OpenCTI TIP web application interface. The left sidebar shows navigation links for Dashboard, Activities (selected), Analysis, Events, Observations, Knowledge, Threats, Arsenal, Entities, Data, and Settings. The main content area has a title "SHINING A LIGHT ON DARKSIDE RANSOMWARE OPERATIONS" and a TLP:WHITE status. The "BASIC INFORMATION" section includes a Standard STIX ID (report--7438e859-5c94-5a8f-b14d-9df3af11c139), Other STIX IDs (empty), STIX version (2.1), Author (ALIENTAULT), Creation date (May 12, 2021, 10:22:47 AM), Modification date (May 18, 2021, 9:48:03 AM), Revoked (NO), Labels (cobalt strike, cve-2021-20016, darkside, darkside 2.0, darksupp, raaS, ransomware, smokedham, unc2465, unc2628, unc2659), Confidence level (LOW), Creation date (in this platform) (May 12, 2021, 10:58:15 AM), and Creator ([CONNECTOR] ALIENTAULT). The "ENTITY DETAILS" section contains a detailed description of Mandiant's findings on Darkside victims and a donut chart showing the distribution of entities by type. The chart indicates that 65.41% are Indicators (242), 21.35% are Stixfile (79), and 3.24% are other types including Vulnerability, Malware, IPv4-Addr, Sector, Uri, Domain-Name, and Attack-Pattern.

SHINING A LIGHT ON DARKSIDE RANSOMWARE OPERATIONS

TLP:WHITE

BASIC INFORMATION

Standard STIX ID: report--7438e859-5c94-5a8f-b14d-9df3af11c139

Other STIX IDs:

STIX version: 2.1

Author: ALIENTAULT

Creation date: May 12, 2021, 10:22:47 AM

Modification date: May 18, 2021, 9:48:03 AM

Revoked: NO

Labels: cobalt strike, cve-2021-20016, darkside, darkside 2.0, darksupp, raaS, ransomware, smokedham, unc2465, unc2628, unc2659

Confidence level: LOW

Creation date (in this platform): May 12, 2021, 10:58:15 AM

Creator: [CONNECTOR] ALIENTAULT

ENTITY DETAILS

Description: Mandiant has identified multiple DARKSIDE victims through our incident response engagements and from reports on the DARKSIDE blog. Most of the victim organizations were based in the United States and span across multiple sectors, including financial services, legal, manufacturing, professional services, retail, and technology. The number of publicly named victims on the DARKSIDE blog has...

Report types: THREAT-REPORT

Processing status: ANALYZED

Distribution of entities

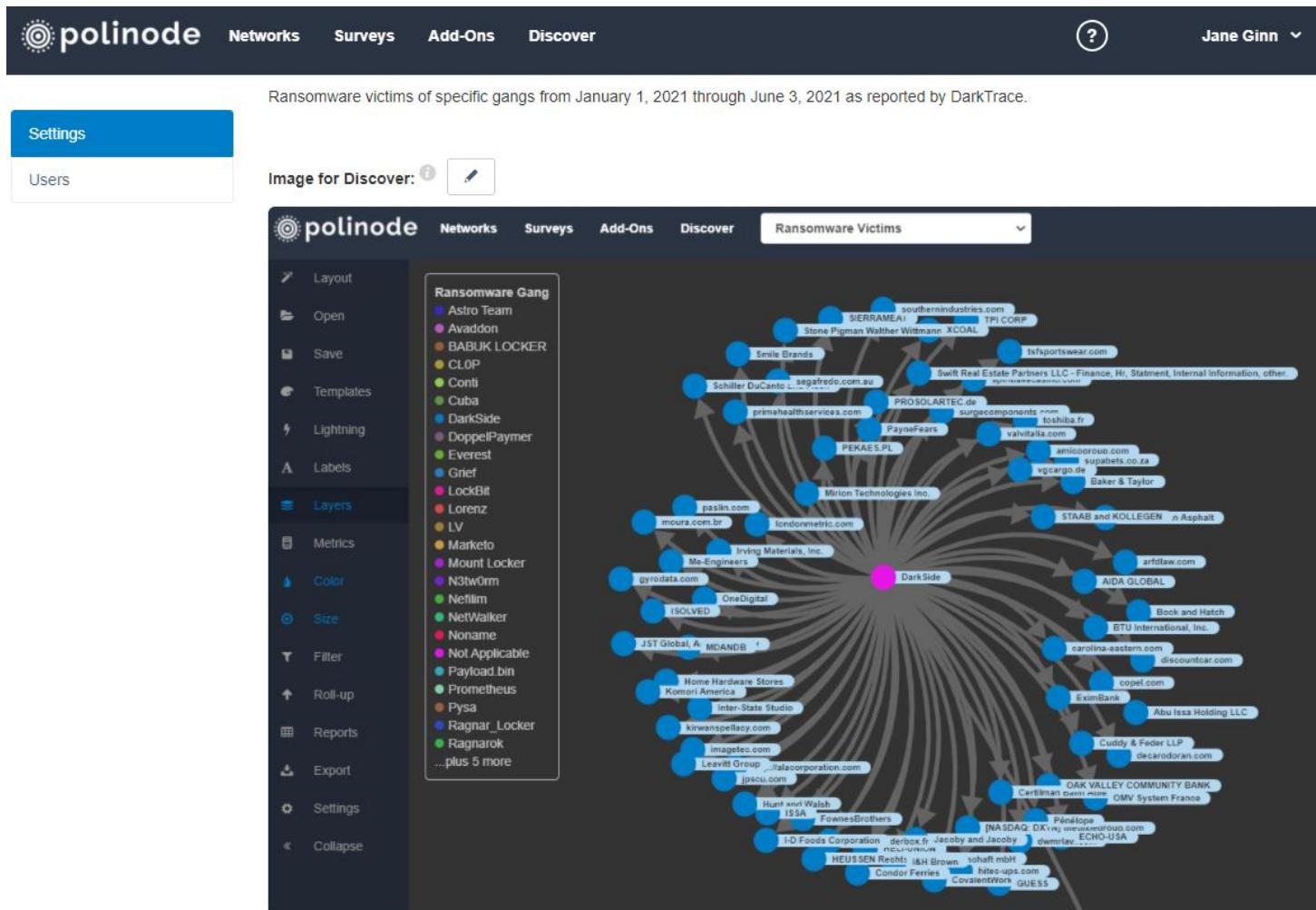
Indicator (242): 65.41%

Stixfile (79): 21.35%

Vulnerability (1), Malware (5), IPv4-Addr (5), Sector (6), Uri (8), Domain-Name (12), Attack-Pattern (12): 3.24%

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

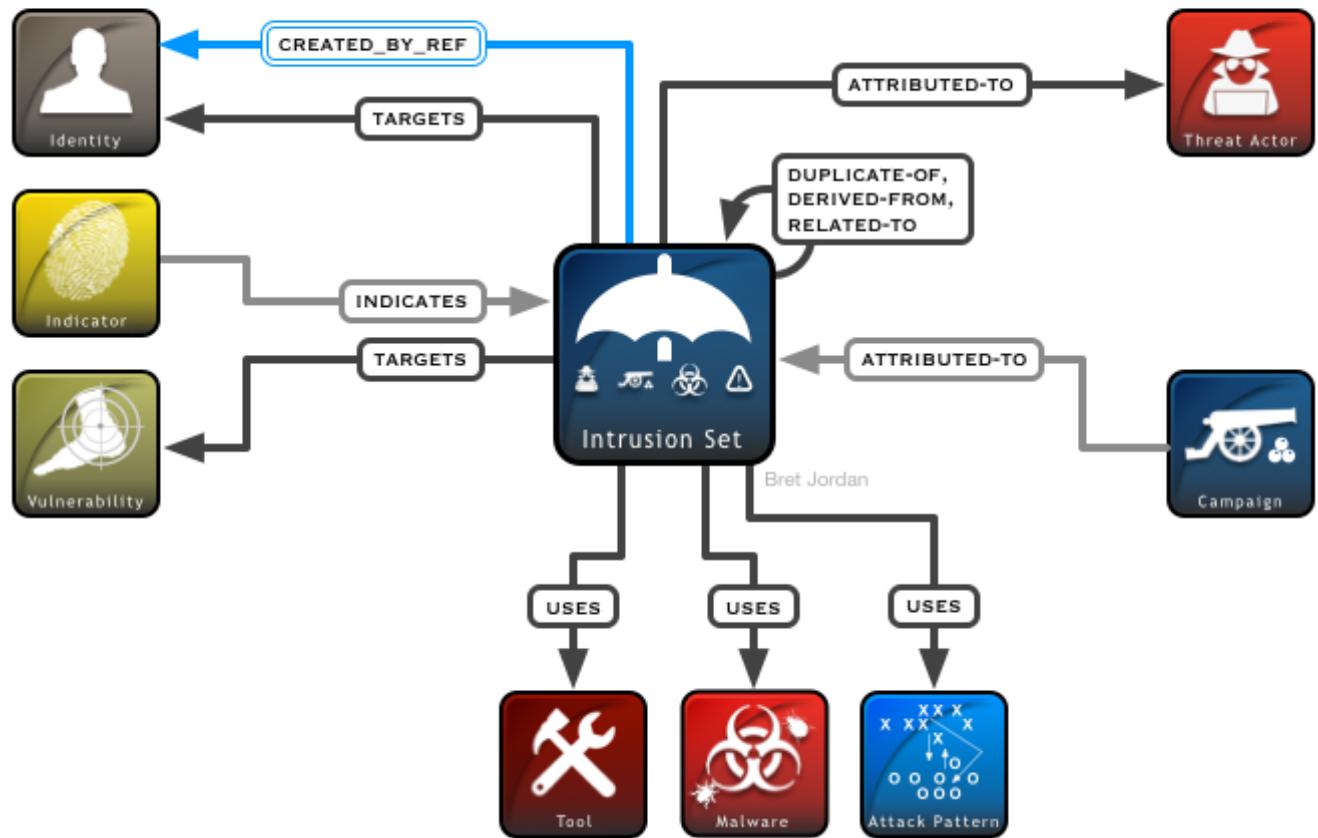
JSON

```
{  
    "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"  
        },  
        {  
        }
```

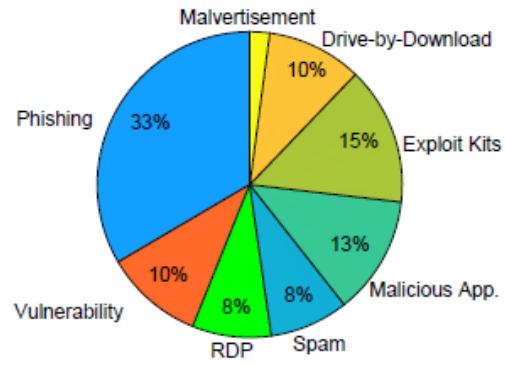
Intrusion Set SDO Properties & Relationships

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

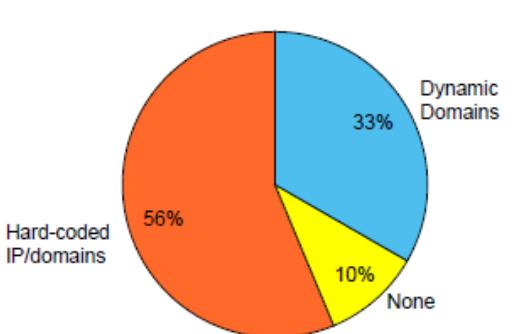
Intrusion Set Relationships



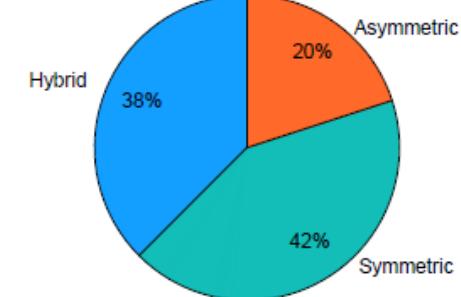
Distribution of Infection Types



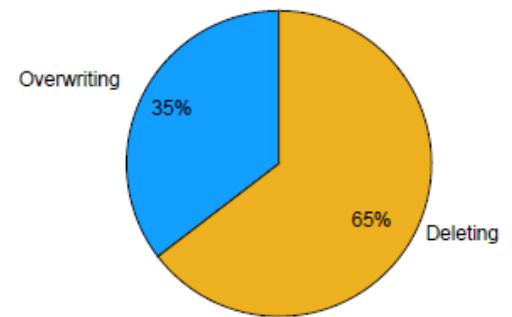
(a) Infection Methods



(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, and Defense Solutions. ACM Comput. Surv. 1, 1 (February 2021), 39 pages

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

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control
T1566: Phishing Attachment T1566.002: Spearphishing Link T1566.003: Spearphishing via Service	T1058.002: AppleScript T1059.007: Javascript T1059.008: Network Device CLI	T1547.014: Active Setup T1547.002: Authentication Package T1547.006: Kernel Modules and Extensions T1547.008: LSASS Driver T1547.011: File Modification T1547.020: Port Monitors T1547.021: Print Processors T1547.027: Re-opened Applications T1547.001: Registry Run Keys / Startup Folder T1547.005: Security Support Provider T1547.009: Shortcut Modification T1547.010: Time Providers T1547.004: Whining Helper DLL T1547.013: XDG Autostart Entries	T1547.014: Active Setup T1547.002: Authentication Package T1547.006: Kernel Modules and Extensions T1547.008: LSASS Driver T1547.011: File Modification T1547.020: Port Monitors T1547.021: Print Processors T1547.027: Re-opened Applications T1547.001: Registry Run Keys / Startup Folder T1547.005: Security Support Provider T1547.009: Shortcut Modification T1547.010: Time Providers T1547.004: Whining Helper DLL T1547.013: XDG Autostart Entries	T3070.005: Clear Command History T3070.002: Clear Linux or Mac System Logs T3070.001: Clear Windows Event Logs T3070.004: File Deletion T3070.005: Network Share Connection Removal T3070.006: Timestamp T3081.001: Invalid Code Signature T3081.004: Masquerade Task or Service T3081.005: Match Legitimate Name or Location T3081.006: Rename System Utilities T3081.007: Right-to-Left Override T3081.008: Space after Filename T3085.004: Asynchronous Procedure Call T3085.001: Dynamic-Link Library Injection T3085.011: Extra Window Memory Injection T3085.002: Portable Executable Injection T3085.009: Proc Memory T3085.013: Process Doppelganging T3085.012: Process Hollowing T3085.008: Proc System Calls T3085.009: Thread Execution Hijacking T3085.001: Thread Local Storage T3085.005: Thread Local Storage T3085.014: VDSO Hijacking T2118.003: CMSIP T2118.001: Compiled HTML File T2118.002: Control Panel	T3005.008: /etc/passwd and /etc/shadow T3005.005: Cached Domain Credentials T3005.006: DCSync T3005.004: LSA Secrets T3005.001: LSAS Memory T3005.002: NTDS T3005.007: Proc Rikyoku T3005.003: Security Account Manager	T1018: Remote System Discovery T3021.001: Distributed Component Object Model T3021.002: Remote Desktop Protocol T3021.003: SMB/Windows Admin Shares T3021.004: SSH T3021.005: VNC T3021.006: Windows Remote Management	T1113: Screen Capture T1125: Video Capture T1371: Non-Standard Port	T105: Ingress Tool Transfer T106: Domain Fronting T109: External Proxy T109: Internal Proxy T209: Multi-hop Proxy	
T1078: Valid Accounts T1078.004: Cloud Accounts T1078.001: Default Accounts T1078.002: Domain Accounts T1078.003: Local Accounts	T1058.001: PowerShell T1059.006: Python T1059.004: Unix Shell T1059.005: Visual Basic T1059.009: Windows Command Shell T1106: Native API T1569: System Services T1569.001: Launchd T1569.002: Service Execution T1304: User Execution T1304.003: Malicious File T1304.004: Malicious Image T1304.005: Malicious Link T1047: Windows Management Instrumentation	T1058.004: Cloud Accounts T1078.001: Default Accounts T1078.002: Domain Accounts T1078.003: Local Accounts	T1058.004: Cloud Accounts T1078.001: Default Accounts T1078.002: Domain Accounts T1078.003: Local Accounts	T1078.002: Domain Accounts T1078.003: Local Accounts	T1228: Signed Binary Program Execution T1228.001: Malicious T1228.002: Malware T1228.003: Odbeconf T1228.004: Regics/Regasm T1228.005: Regser32 T1228.006: Rundll32 T1228.007: Verdad	T2118.004: Install32 T2118.005: Meltix T2118.006: Malware T2118.007: Odbeconf T2118.008: Regics/Regasm T2118.009: Regser32 T2118.010: Rundll32 T2118.011: Verdad	T1078.004: Cloud Accounts T1078.001: Default Accounts T1078.002: Domain Accounts T1078.003: Local Accounts		

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

Intrusion Set SDO

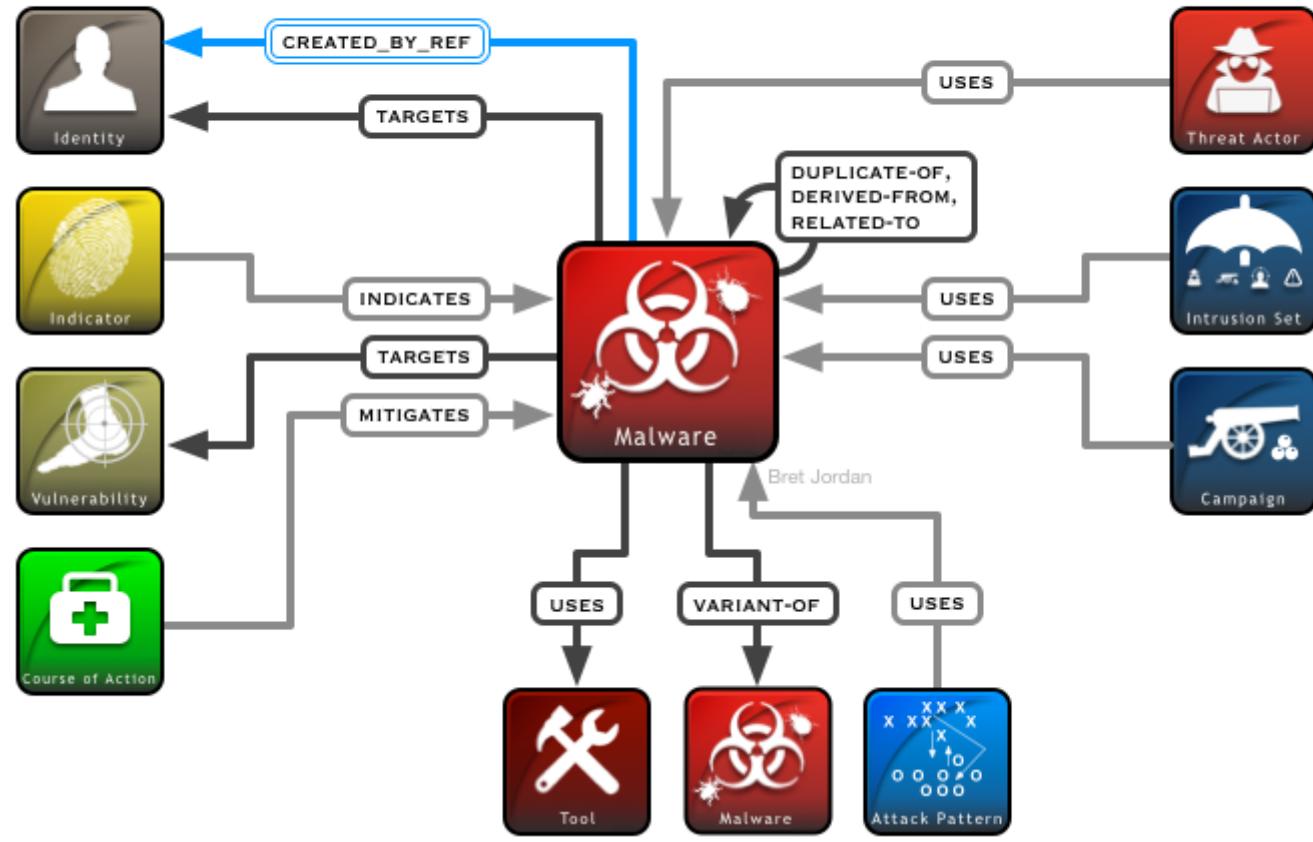
JSON

```
{  
    "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	R name R 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 Relationships



Malware – Shown on VirusTotal

Σ 568df3fc188573553842e10f642a4ee8e46d9bf6e017d7d39f8d00041701ed9a

39 / 69

39 security vendors flagged this file as malicious

568df3fc188573553842e10f642a4ee8e46d9bf6e017d7d39f8d00041701ed9a
https_e.dll
pedll

266.00 KB | 2021-05-22 02:26:17 UTC
15 days ago

DLL

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Dynamic Analysis Sandbox Detections ⓘ
⚠ The sandbox Lastline flags this file as: MALWARE TROJAN

Vendor	Detection	Vendor	Detection
Ad-Aware	Trojan.GenericKD.45702232	AegisLab	Trojan.Win32.Generic.4ic
AhnLab-V3	Trojan/Win.CobaltStrike.R373044	Alibaba	Ransom.Win32/Sodinokibi.017759bc
ALYac	Trojan.GenericKD.45702232	Antiy-AVL	Trojan/Generic.ASMalwS.31704FF
Arcabit	Trojan.Generic.D2B95C58	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	BitDefender	Trojan.GenericKD.45702232
CAT-QuickHeal	Ransom.Sodinokibi	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cyren	W32/Trojan.THIN-2560
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.GenericKD.45702232 (B)
eScan	Trojan.GenericKD.45702232	ESET-NOD32	A Variant Of Win32/Kryptik.HKAF
FireEye	Trojan.GenericKD.45702232	Fortinet	W32/Agent.BGMA!tr

Domain from CP
CO Reporting:
lagrom.com

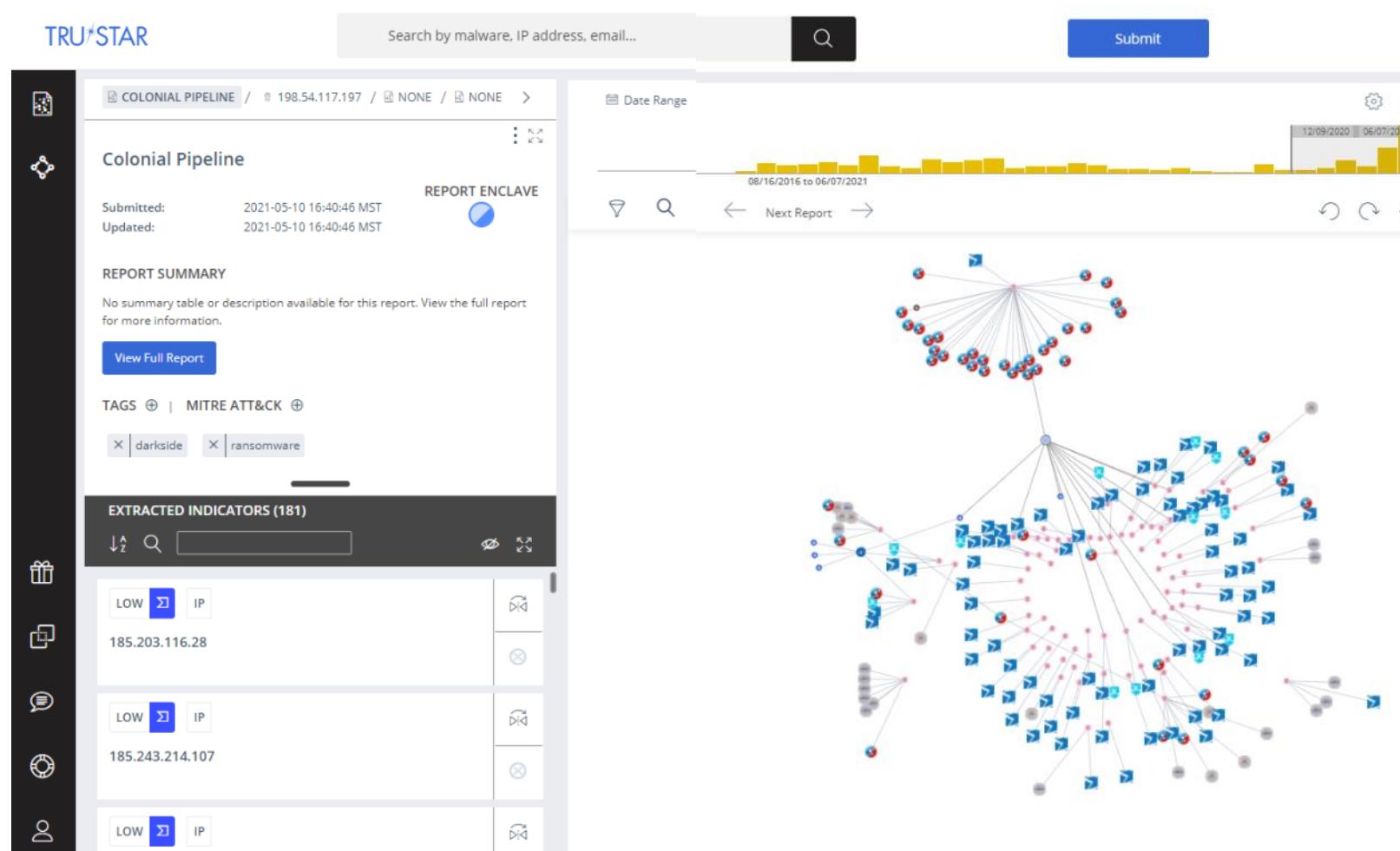
MD5 Hash from
CP CO Reporting:
5f1e9ae81c6a3797bf16b
9ee469dc66a

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:
5f1e9ae81c6a3797bf16b
9ee469dc66a

File Name:
https_e.dll

Resolves to IPv4:
104.193.252.197

Source: TRUSTAR TIP

Multiple Sightings of COs Shown on XFE

The screenshot shows the IBM X-Force Exchange (XFE) interface. At the top, there is a navigation bar with a menu icon, the XFE logo, a dropdown for 'ALL' collections, a search bar, and user profile icons.

The main content area displays a collection titled 'ThreatStop'. It includes a sidebar with a 'ransomware' tag, a 'Public Collection' status, 0 followers, and social sharing links for Twitter, LinkedIn, and Facebook. The main list shows multiple sightings of the IP address 104.18.58.130 under the 'basic.threatstop.local' entry.

A detailed view of one sighting is shown on the right, with tabs for 'COLLECTION DETAILS' and 'COMMENTS (0)'. The details tab shows the collection outline and a list of reports. The first report is for IP 104.248.94.23, captured on Jun 7, 2021, at 4:17:53 PM by Jane Ginn. A red vertical bar highlights this entry.

Sighting	Type	IP Address
basic.threatstop.local	ip	104.18.58.130
basic.threatstop.local	ip	104.24.107.152
basic.threatstop.local	ip	34.65.108.95
basic.threatstop.local	ip	104.27.144.65
basic.threatstop.local	ip	13.211.164.92
basic.threatstop.local	ip	63.34.194.62
basic.threatstop.local	ip	31.210.20.120
basic.threatstop.local	ip	8.209.68.164
basic.threatstop.local	ip	8.208.103.246

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

Posted July 21

byte
●



Seller

● 0
1 post

Joined

07/19/21 (ID: 118280)

Activity

Apyroe / other
Deposit
4.000000 ₿

We are looking for corporate networks of the following countries:

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

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue or 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.

FOR MEDIA

BlackMatter Ransomware

CONTACT US

Rules

We do not attack:

- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Defense industry.
- Non-profit companies.
- Government sector.

If your company is on that list you can ask us for free decryption.

About us

We are a team that unites people according to one common interest - money.
We provide the best service for our clients and partners compared to our competitors.
We rely on honesty and transparency in our dealings with our victims.
We never attack the company twice and always fulfill our obligations.
We invite the recovery companies to cooperate with, you can contact us through "Contact Us".

<https://www.recordedfuture.com/blackmatter-r-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

STIX 2 Preferred

SELF-CERTIFICATION PROGRAM FOR CYBER THREAT INTELLIGENCE SHARING



View STIX Preferred Products 

Certify Your STIX Product 

Learn About STIX Preferred 

Self-Certification Program for Automated Cyber Threat Intelligence Sharing

To promote interoperability, OASIS enables implementations of the Structured Threat Information eXpression (STIX™) v2 and the Trusted Automated eXchange of Intelligence Information (TAXII™) v2 to be self-certified by suppliers. The process uses industry-defined conformance test documents developed by members of the OASIS Cyber Threat Intelligence Technical Committee.

Products that meet the self-certification requirements are granted exclusive permission to use the "STIX2 Preferred" or "STIX/TAXII2 Preferred" certification mark.

<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
 - Analysis capabilities and TIPs
 - Trust modelling functionalities
 - Usage of APIs, integration and workflows
 - Threat data quality enhancement
 - Flexible threat data management
- TIP Users
- TIP Developers/Vendors
- Intelligence Producers
 - Enhancing the quality of shared information
 - Coherent use of the standards
- CTI Community and Researchers

Summary

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





rjg@ctin.us

