

Casting a Light on BlackEnergy

 threatconnect.com/blog/casting-a-light-on-blackenergy/

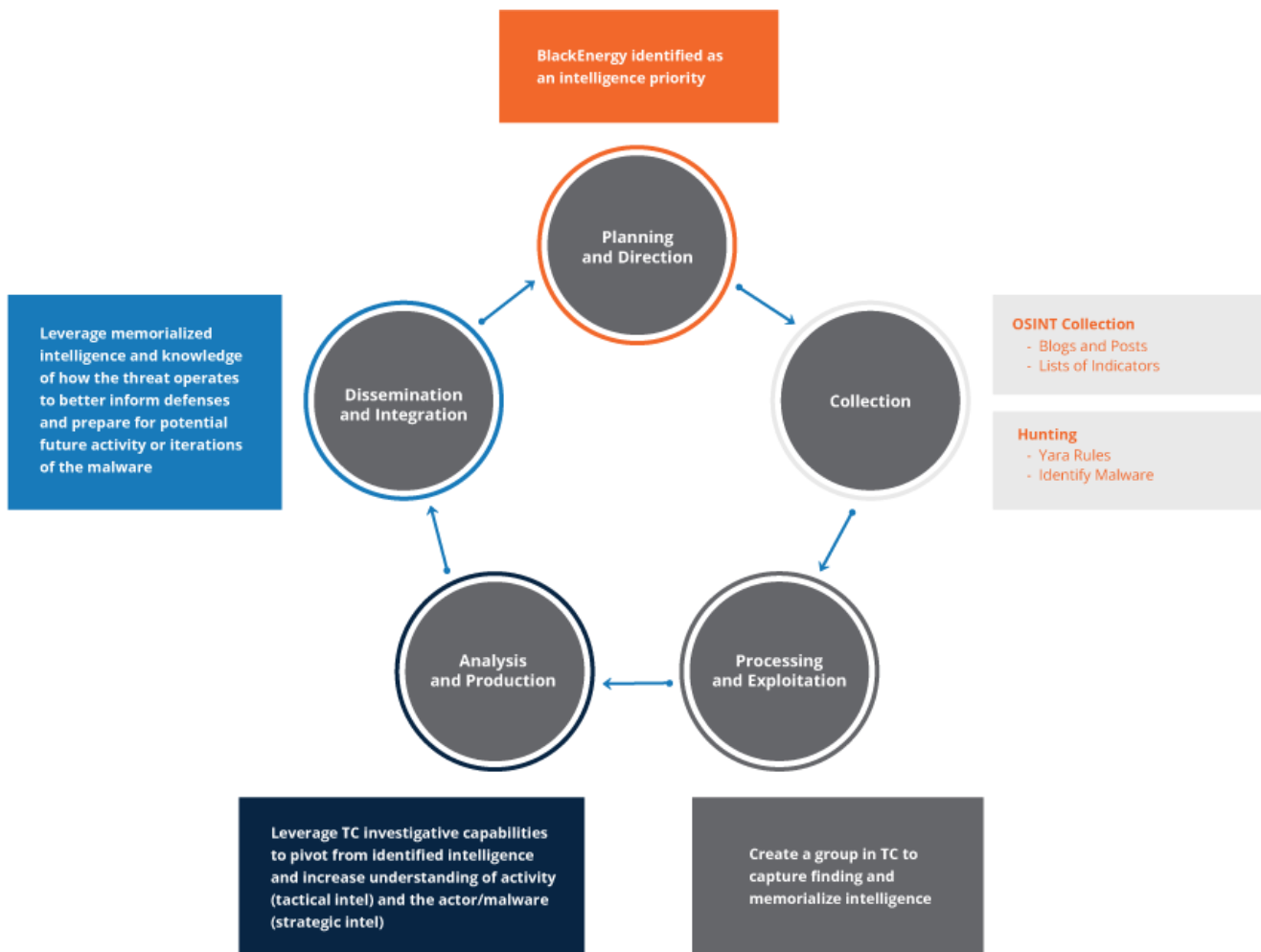
September 18, 2017

A look into BlackEnergy malware and using ThreatConnect to aggregate and memorialize the identified intelligence.

As workers prepared to head home on December 23, 2015, an attack against Ukraine's energy sector left 230,000 without electricity (or heat) for six hours. The attackers demonstrated a variety of capabilities, including spearphishing emails and variants of the BlackEnergy 3 malware to gain a foothold into the Information Technology (IT) networks of the electricity companies. The December 2015 incident was the first known instance where a cyber attack disrupted electric grid operations. And BlackEnergy 3 malware was key to enabling it.

This blog post will:

- Examine how we used the ThreatConnect platform as part of the intelligence cycle when reviewing the BlackEnergy malware.
- Review the BlackEnergy malware, related incidents, and methods for gathering indicators related to the malware.
- Discuss how researchers can use ThreatConnect to sort through and pull these indicators together.

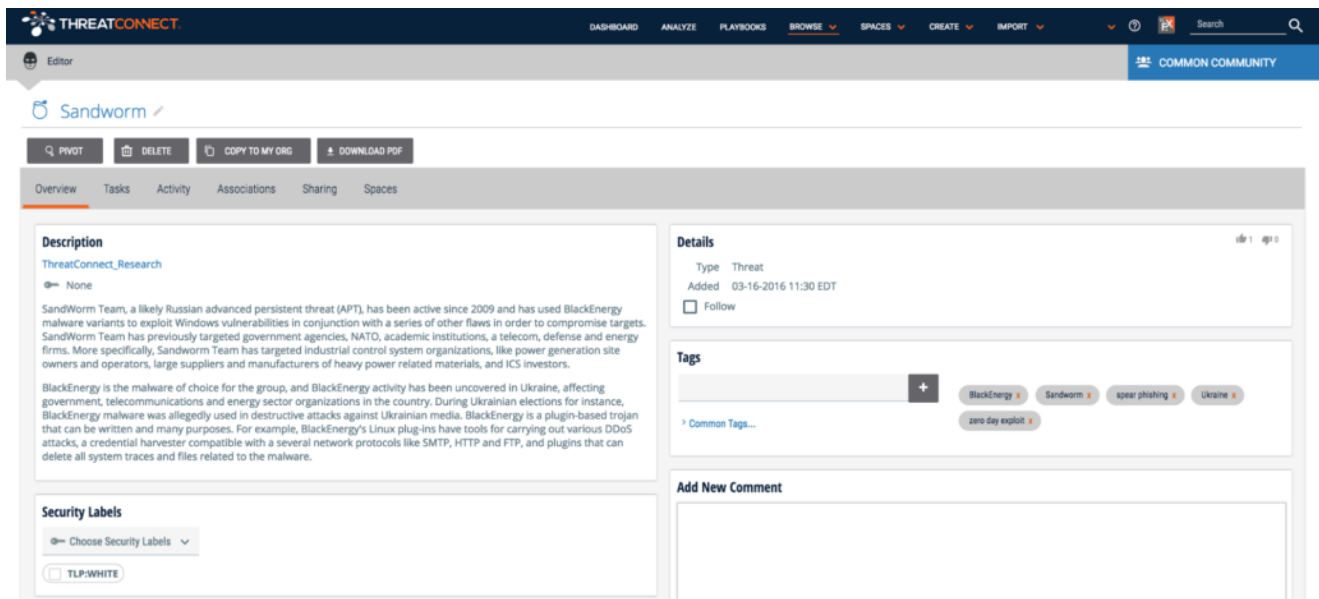


This graphic captures how we incorporated ThreatConnect into the intelligence cycle to aggregate and memorialize intelligence on BlackEnergy. We started off by identifying background information on BlackEnergy and the actors behind it, which ultimately drove our later research efforts.

Planning and Direction – BlackEnergy Background

Since it was first found in the wild in 2007, the BlackEnergy malware family has grown to include three variants, the third of which was used in the Ukraine cyber attacks. The first variant is a simple Trojan that runs distributed denial of service (DDOS) attacks against targeted servers. The second variant –also known as BlackEnergy 2– marked a major change to the malware’s capabilities and an almost complete code rewrite from the first variant. BlackEnergy 2 added support for 64 bit drivers and implemented UAC Bypass Installers to give the malware elevated code execution privileges on Windows. The third variant (BlackEnergy 3) was also a big change from BlackEnergy 2 with the addition of a wider variety of plugins and anti-analysis techniques.

The Russian APT Sandworm Team, also known as Quedagh and BE2 APT, is associated with BlackEnergy attacks targeting various organizations in Ukraine. Since at least 2009, Sandworm Team has also previously attacked government, telecommunications, defense, and energy organizations.



The screenshot displays the ThreatConnect web interface. At the top, there is a navigation bar with options like DASHBOARD, ANALYZE, PLAYBOOKS, BROWSE, SPACES, CREATE, and IMPORT. Below this, the main content area is titled 'Sandworm' and includes a toolbar with actions like PIVOT, DELETE, COPY TO MY ORG, and DOWNLOAD PDF. The interface is divided into several sections: 'Description' with a detailed text block about the Sandworm Team's activities and BlackEnergy malware; 'Details' showing the threat type and date added; 'Tags' with a list of related terms like BlackEnergy, Sandworm, spear phishing, and Ukraine; and 'Security Labels' with a dropdown menu. The overall layout is clean and professional, typical of a security information system.

The consistent use of BlackEnergy malware against the energy and industrial sectors means those organizations should consider BlackEnergy an intelligence requirement. Identifying and memorializing strategic intelligence on when BlackEnergy was used, what it targeted, what it can do, and how it has evolved can ultimately inform those organizations' higher level defensive efforts. The next step in the intelligence cycle is to collect intelligence on the threat itself.

Intelligence Collection

OSINT Baseline

One method ThreatConnect uses when researching a threat, is collecting indicators from openly available sources. These collections often include network and file indicators including hashes, hostnames, IP addresses, and email addresses. ThreatConnect also has a free intelligence feed collecting over 75 cybersecurity reports and blogs that automatically captures indicators so organizations and researchers can incorporate them into their investigative and defensive efforts.

Type	Summary	Owner	Tags	Added
Incident	Security Alert: Locky Ransomware Cha...	Technical Blogs and R...	BLOG: Heimdal Security Security alerts	09-07-2017
Incident	Back to Basics: Worm Defense in the R...	Technical Blogs and R...	Ransomware BLOG: Talos WannaCry +3 more...	09-07-2017
Incident	The Cybersecurity Canon: Cybersecurit...	Technical Blogs and R...	BLOG: Palo Alto Cybersecurity cybersecurity canon +5 more...	09-07-2017
Incident	Booters with Chinese Characteristics: ...	Technical Blogs and R...	BLOG: Talos DDoS DDoS-as-a-Service	08-16-2017
Incident	IT threat evolution Q2 2017. Statistics	Technical Blogs and R...	Mobile Malware large thumbnail +10 more...	08-15-2017
Incident	DefPloreX: A Machine-Learning Toolkit ...	Technical Blogs and R...	BLOG: Trend Micro Open source DefPloreX	07-28-2017

Technical Blogs and Reports Intelligence Source Browse Screen, Filtered for ICS related Incidents

One good starting point was a 2014 Kaspersky report detailing BlackEnergy use that contained five MD5 hashes associated with the BlackEnergy 3 malware. After identifying these openly available reports and indicators, we imported them into ThreatConnect and associated them with their respective BlackEnergy Incidents.

The screenshot shows the ThreatConnect interface for an incident titled "20170828C: SecureList BlackEnergy 3 Report". The interface includes a navigation bar with options like DASHBOARD, ANALYZE, PLAYBOOKS, BROWSE, SPACES, CREATE, and IMPORT. Below the navigation bar, there are tabs for Overview, Tasks, Activity, Associations, Sharing, and Spaces. The main content area is divided into several sections:

- Description:** Shows the incident title and a description: "ThreatConnect_Research says: None. SecureList Report on the BlackEnergy 2 and 3 Malware Variants, containing MD5 Hashes associated to the Threat."
- Security Labels:** Includes a dropdown menu for "Choose Security Labels" and a label "TLP:WHITE".
- Associations:** A section for managing associations.
- Details:** Provides metadata such as Type (Incident), Added (08-31-2017 16:07 GMT), Event Date (08-28-2017), and Status (None). It also includes a "Follow" checkbox and a "Status" field.
- Tags:** Displays a list of tags including "Advanced Persistent Threat", "BlackEnergy", "Blackenergy3", "Energy", and "Sandworm".

Malware Hunting

Another method that can be used to identify and gather indicators is hunting using [YARA](#) rules. We used the ThreatConnect YARA hunting integration to deploy a YARA ruleset of five BlackEnergy signatures and identified samples submitted to a public malware scanning site that matched those YARA rules. The matching file results identified all three variants of the malware and associated the file indicators with YARA signature groups in the Platform.

The screenshot shows the ThreatConnect platform interface. At the top, there is a navigation bar with the ThreatConnect logo and menu items: DASHBOARD, ANALYZE, PLAYBOOKS, BROWSE (selected), SPACES, CREATE, and IMPORT. A search bar is on the right. Below the navigation bar, there is a filter section with 'BlackEnergy' selected. A table displays search results for 'BlackEnergy'.

Type	Summary	Owner	Tags	Added
Incident	20170827 057892 BlackEnergy2	[Redacted]	α RU	08-27-2017
Incident	20170826 057689 BlackEnergy2	[Redacted]	α RU	08-26-2017
Incident	20170825 057537 BlackEnergy2	[Redacted]	α RU	08-25-2017
Incident	20170825 057532 BlackEnergy2	[Redacted]	α RU	08-25-2017
Incident	20170825 057531 BlackEnergy2	[Redacted]	α RU	08-25-2017
Incident	20170825 057524 BlackEnergy2	[Redacted]	α RU	08-25-2017
Incident	20170825 057502 BlackEnergy2	[Redacted]	α RU	08-25-2017

Hunting for BlackEnergy in the ThreatConnect Platform

Above is an image of the output from hunting for BlackEnergy using ThreatConnect. The YARA hunting integration automatically imports file indicators that match deployed YARA rules. These indicators are organized into groups based on the date of identification, the associated rule, and sample. This integration helped us identify hundreds of files related to this specific threat. Additionally, it helped us organize the data so that it can be enriched and associated with other BlackEnergy intelligence in the platform.

Processing and Exploitation – Building Out Intelligence With ThreatConnect

After we've collected intelligence from a variety of sources, we can leverage ThreatConnect's various integrations, Spaces apps, and investigation links to build out our understanding of the identified activity. This iterative process helps organizations identify tactical intelligence that may inform their incident response efforts in the wake of experienced activity.

For example, we can use our investigation links for a BlackEnergy 3 malware hash identified in an [RSA forum](#) to query VxStream for the given file.

The screenshot displays the ThreatConnect interface for a specific threat indicator. The top navigation bar includes options like DASHBOARD, ANALYZE, PLAYBOOKS, BROWSE, SPACES, CREATE, and IMPORT. The main content area is divided into several sections:

- Indicator Analysis:** Shows a 'ThreatAssess' gauge with a value of 850 and 'Priority 1'. It includes filters for 'Recent False Positive Reported', 'Recent Observation', and 'Multiple Sources'. A 'CAL Insights' section lists 'False Positives' and 'Observations' for 'All Time' and 'Previous 7 Days'.
- Description:** Identifies the sample as 'ThreatConnect Research' and notes it is likely a sample of 'BlackEnergy 3 Malware'.
- Source:** Lists the source as 'ThreatConnect Research' with a URL: <https://community.rsa.com/thread/186012>.
- Security Labels:** Shows a 'TLP:GREEN' label.
- Additional Owners:** Lists 'Common Community' with a 'Threat Rating' of 80.
- Details:** Provides metadata such as 'Type: File', 'Added: 07-20-2017 08:48 EDT', and 'Modified: 08-22-2017 10:20 EDT'. It also shows an 'Overall Threat Rating' of 'High' and an 'Overall Confidence Rating' of '70 - Probable'.
- Observations/False Positives:** A table showing the number of observations and false positives reported by different users.
- Tags:** Includes tags for 'BlackEnergy 3', 'Blackenergy 3', and 'Energy 3'.
- Investigation Links:** A grid of links to external analysis services, including Google MDS, Hybrid Analysis, Recorded Future, VirusTotal, and others.

We can then use VxStream to find similar samples to the queried hash. Many public malware scanning sites associate similar files to the sample being scanned, which researchers can use to find associated samples related to the incident they are investigating.

These similar samples have already been scanned, making it easier for us to identify the variant of the malware. This decreases the amount of time an analyst needs to spend analyzing the sample.

PAYLOAD SECURITY Home Submissions Resources Contact Search ... English

Search results for *similar-to:07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660*

Download all DNS Requests (CSV) Download all Contacted Hosts (CSV)

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
April 1 2016, 15:06 (CEST)	vba_macro.exe PE32 executable (GUI) Intel 80386, for MS Windows f2678590508471085a91570b01e196ba4274bd96903cd94033713860f80fabbb	malicious	Threat Score: 76/100 AV Multiscan: 66% Trojan.BlackEnergy Matched 7 Signatures Intelligence: Show Similar Samples	-	Windows 7 32 bit - Usermode Monitor	
March 29 2016, 16:25 (CEST)	vba_macro.exe PE32 executable (GUI) Intel 80386, for MS Windows f2678590508471085a91570b01e196ba4274bd96903cd94033713860f80fabbb	malicious	Threat Score: 76/100 AV Multiscan: 66% Trojan.BlackEnergy Matched 7 Signatures Intelligence: Show Similar Samples	-	Windows 7 32 bit - Usermode Monitor	
February 19 2016, 21:16 (CET)	virus_04.exe PE32 executable (GUI) Intel 80386, for MS Windows ca7a8180996a98e718f4278379d52453b78d0a307e06e1866db4d4ce969d525	Sample (70KB) malicious	Threat Score: 100/100 AV Multiscan: 78% Backdoor.Fonten Matched 38 Signatures Intelligence: Show Similar Samples		Windows 7 32 bit - Kernelmode Monitor	
February 19 2016, 21:16 (CET)	virus_04.exe PE32 executable (GUI) Intel 80386, for MS Windows ca7a8180996a98e718f4278379d52453b78d0a307e06e1866db4d4ce969d525	Sample (70KB) malicious	Threat Score: 100/100 AV Multiscan: 78% Backdoor.Fonten Matched 30 Signatures Intelligence: Show Similar Samples		Windows 7 32 bit - Usermode Monitor	
January 19 2016, 22:05 (CET)	03.exe PE32 executable (GUI) Intel 80386, for MS Windows 1fcbb6e0a1a530b5ed82ed961e9c76c353ac6c14781f13002abdb2ff53b9b59	Sample (70KB) malicious	Threat Score: 100/100 AV Multiscan: 54% Gen:Trojan.Heur.TDss Matched 28 Signatures Intelligence: Show Similar Samples		Windows 7 32 bit - Usermode Monitor	
January 19 2016, 22:05 (CET)	03.exe PE32 executable (GUI) Intel 80386, for MS Windows 1fcbb6e0a1a530b5ed82ed961e9c76c353ac6c14781f13002abdb2ff53b9b59	Sample (70KB) malicious	Threat Score: 100/100 AV Multiscan: 54% Gen:Trojan.Heur.TDss Matched 29 Signatures Intelligence: Show Similar Samples		Windows 7 32 bit - Kernelmode Monitor	

Hybrid Analysis BlackEnergy Malware Associated Samples

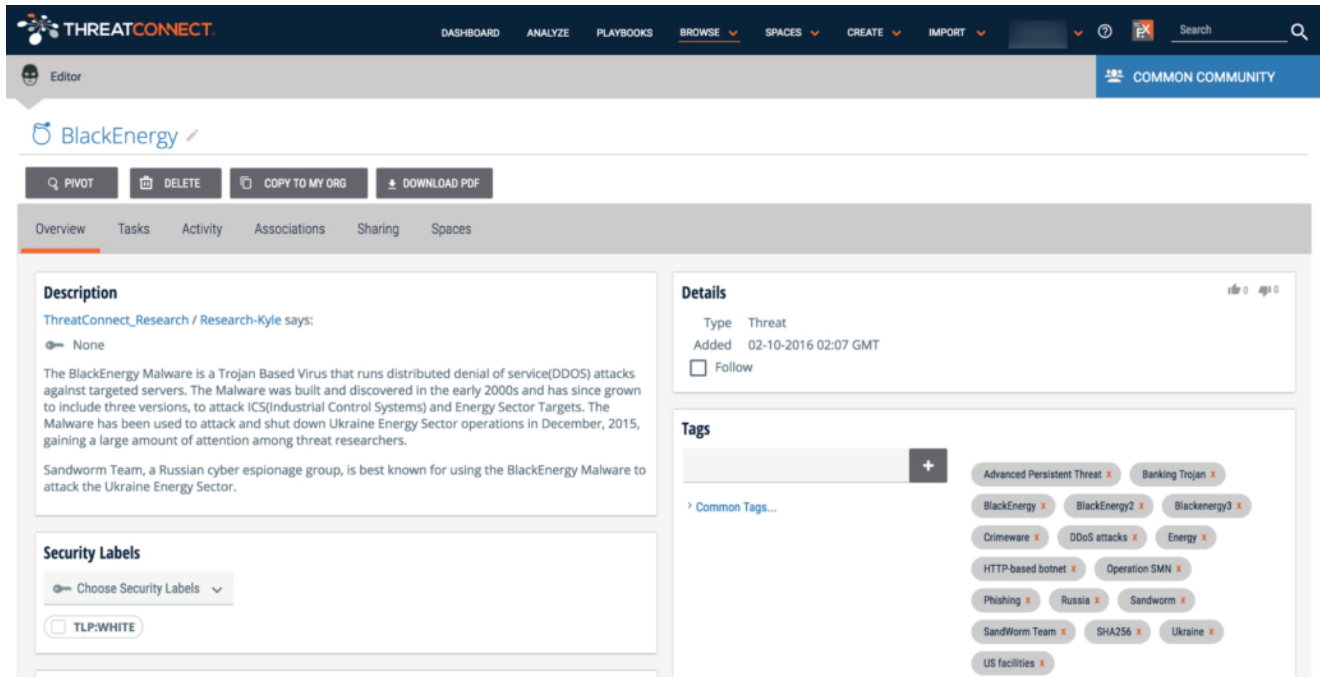
This newly identified information that augments findings from intelligence collection efforts, is then imported into ThreatConnect and associated with the BlackEnergy threat to further increase visibility into the malware activity.

Analysis and Production – Using ThreatConnect to Associate Indicators

Next we began grouping the indicators according to the three variants of BlackEnergy in ThreatConnect, where we can easily and efficiently associate indicators and show relationships using incidents, threats, and campaigns. Here’s how:

BlackEnergy Threat

The first thing that we did to start pulling BlackEnergy indicators together was create a BlackEnergy malware threat. Threats in the Platform are made up of incidents and activity groups defined by common infrastructure, common malware, and carried out by a common adversary or team. Our BlackEnergy Threat captured the information we learned about BlackEnergy during the prior phases of the intelligence cycle.



Screenshot of the BlackEnergy Threat in the ThreatConnect Common Community

We also applied a few relevant tags such as the names of the malware variants, targeted industry, and type of activity, and then associated the BlackEnergy malware threat group to the preexisting Sandworm threat actor group. Tags provide another useful way to pivot through information of interest in ThreatConnect.

BlackEnergy Incidents

After building the BlackEnergy threat, we began compiling incidents for each variant of the malware. These incidents have indicators associated to them, and allow us to organize our work as we enrich those indicators. We started with a BlackEnergy 2 Malware Samples incident, BlackEnergy 3 Malware Samples incident, and a BlackEnergy Malware incident. Shortly thereafter we pulled together a Ukraine BlackEnergy 3 Attacks incident so that we could move all of the indicators of compromise from that attack into one group.

BlackEnergy Malware Incidents





We also associated two incidents that were already associated with the Sandworm threat actor and the CVE-2014-4114 vulnerabilities, as they had similar indicators and characteristics to the BlackEnergy 3 malware. From there, we began gathering BlackEnergy related indicators to associate to each incident.

BlackEnergy 3 Campaign

After building the Threat and Incidents, we created a BlackEnergy 3 Campaign to organize all of the BlackEnergy 3 related Incidents including the Ukraine BlackEnergy 3 Attacks, and BlackEnergy 3 Samples Incidents. We chose to create a campaign for this variant because

Associations

▲ Associated Groups (4) +

Type	Owner	Date Added	
 Incident 20170106B: BlackEnergy 2 Malware Sa...	ThreatConnec t Research	01-06-2017	...
 Incident 20170731A: BlackEnergy Malware Samp...	ThreatConnec t Research	07-31-2017	...
 Campaign BlackEnergy 3	ThreatConnec t Research	08-01-2017	...
 Threat SandWorm Team	ThreatConnec t Research	10-24-2014	...

▼ Associated Indicators (0) +

▼ Associated Victim Assets (0) +

we found several reports with different indicators, that we felt needed individual Incidents.

Generally, the purpose of creating a campaign in ThreatConnect is to associate together related incidents, or other campaigns.

Associations

▲ Associated Groups (6) +

Type	Owner	Date Added	
 Incident 20141016A: Sandworm to Blacken: The ...	ThreatConnec t Research	10-24-2014	...
 Incident 20141029A: ICS-CERT Ongoing Sophistic...	ThreatConnec t Research	10-29-2014	...
 Incident 20170719G: BlackEnergy 3 Malware Sa...	ThreatConnec t Research	07-19-2017	...
 Incident 20170804A: Ukraine BlackEnergy 3 Attac...	ThreatConnec t Research	08-04-2017	...
 Threat BlackEnergy	ThreatConnec t Research	07-19-2017	...
 Threat SandWorm Team	ThreatConnec t Research	10-24-2014	...

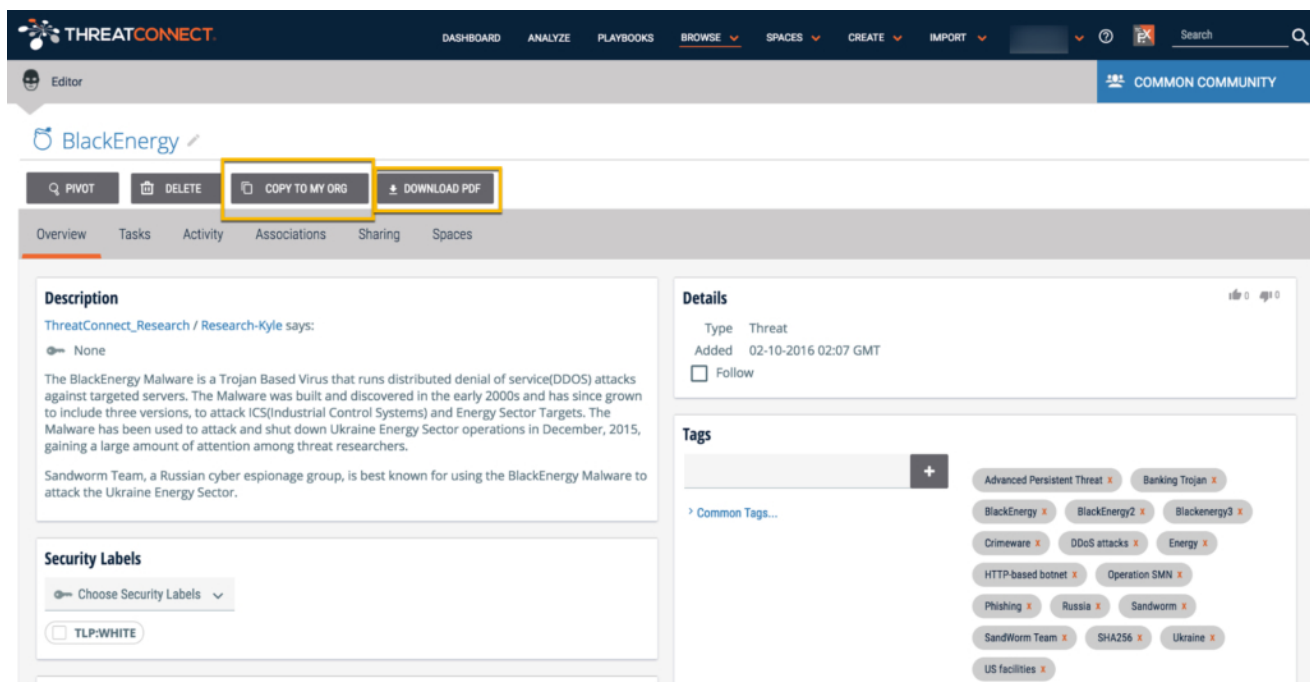
The screenshot shows the ThreatConnect interface for an incident titled "BlackEnergy 3". The top navigation bar includes the ThreatConnect logo and menu items: DASHBOARD, ANALYZE, PLAYBOOKS, BROWSE, SPACES, CREATE, and IMPORT. A search bar is located on the right. Below the navigation bar, the user is identified as "Editor" and the "COMMON COMMUNITY" is selected. The incident page features a header with the title "BlackEnergy 3" and action buttons: PIVOT, DELETE, COPY TO MY ORG, and DOWNLOAD PDF. The main content area is divided into several sections:

- Description:** A text block stating "ThreatConnect_Research says: None" and a detailed paragraph about the BlackEnergy 3 malware, mentioning its use in the Ukraine Energy Sector in late 2015 and its capabilities to protect itself from virtual environments and anti-debugging methods.
- Details:** A table-like section showing:
 - Type: Campaign
 - Added: 09-18-2017 13:56 GMT
 - First Seen: 08-01-2017
 - A "Follow" checkbox.
- Tags:** A section with a "+" button and a list of tags: Advanced Persistent Threat, BlackEnergy, Blackenergy3, Energy, Russia, and Sandworm.
- Security Labels:** A section with a "Choose Security Labels" dropdown and a "TLP:WHITE" checkbox.

BlackEnergy 3 Campaign in the ThreatConnect Common Community

Dissemination and Integration

Information and data you found in ThreatConnect can be shared out to other users and other communities that you have access to. This includes our Common Community, which is available to all of our wonderful users as well as the ThreatConnect Intelligence source, reserved for our paying customers. You can also download your Incidents, Indicators, and Threats as a PDF and copy other incidents to your research organization using the “Copy to My Org” function to show to individuals that may not have access to ThreatConnect, so that they can make informed decisions using ThreatConnect data. You are also able to follow incidents from other organizations and get immediate or summarized reports on changes made to those incidents.



Making it Actionable

Now that we have identified and pulled all of this information together in ThreatConnect and shared with appropriate parties, what happens next? As we like to say, intelligence doesn't exist for its own sake: it exists to inform decisions. Using the ThreatConnect Platform, the information gathered can be used to make informed decisions about the threat posed by BlackEnergy, and prevent and respond effectively to incoming threats. ThreatConnect has numerous integrations that make it easy to take action on information pulled together in the Platform. The added functionality of ThreatConnect Playbooks further simplifies these processes allowing users to quickly send indicators to be blocked, further analyzed by an automated malware analysis service, or even assigned to an analyst.

Looking beyond ThreatConnect, recommendations like these from the ICS-CERT are other ways to protect ICS (Industrial Control Systems) and energy sector systems:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Remove, disable, or rename any default system accounts wherever possible.
- Apply patches in the ICS environment, when possible to mitigate known vulnerabilities
- Implement policies requiring the use of strong passwords.
- Monitor the creation of administrator level accounts by third-party vendors.
- Limiting remote systems or unmanned stations with sensitive information or computer systems.