# BlackEnergy and the Ukraine: Signals vs. Noise

## Introduction

Fear of hackers causing real-world damage has long been part of Hollywood's history. We've watched these movies for decades and become almost numb to it. But what if the fiction derived for the big screen had a foothold in reality? What if our world could be impacted by an attacker halfway around the world, and it happened today, right in front of our eyes?

As we continue to connect systems and networks together around the world, and ignore the warnings to prevent access to cybercriminals, today's physical world can come under attack from almost anyone.

In this white paper we will discuss the cyber community's latest fear: the ever-evolving BlackEnergy family of malware. We'll delve into how it works, how it has evolved and how it may have laid the groundwork for a far bigger impact on the world than it was ever originally designed to have.

## Why Your Security is only as Strong as Your Least Secure Endpoint

The recent flurry of Ukrainian electricity and power distribution attacks perfectly illustrate both the sophistication of today's attack landscape, as well as the undeniable need for intelligent, predictive, and preventative controls.

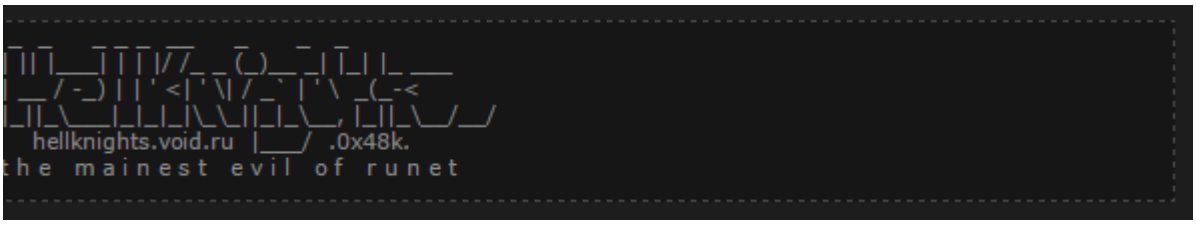
On December 23, 2015, around half a million homes in the Ivano-Frankivsk region of Ukraine lost power in a blackout that lasted for several hours. Initial reports from Ukrainian news outlets reported the cause was a 'virus' spread by 'hackers'; the truth is far more sinister. The cybercriminal group involved hit electricity distribution companies with a trojan called BlackEnergy. BlackEnergy infects systems and runs malicious tasks, such as creating a backdoor which gives the attackers direct access to core system files so they can examine the system and see if the machine does indeed belong to the company they are targeting. If this is confirmed, they may then drop a destructive payload, such as the Win32/KillDisk component, which overwrites valuable company files that have certain extensions and/or uses a plugin named dstr to delete system files to make the system unbootable.

An infection by malware such as BlackEnergy on any vital infrastructure system has the potential to be catastrophic. Predictive and preventative mitigations are the only method to truly thwart the constant evolution of these threats and their ongoing attempts (both automated and human-controlled) to evade traditional controls.

A note here: BlackEnergy is not a new threat framework. It is in fact almost a decade old, and upon direct inspection there are numerous signatures or hallmarks that are specific to any "BlackEnergy" artifact. Yet, we still see traditional (aka signature-based) AV/endpoint controls fail to protect against it. We'll touch on how the mathematical approach from Cylance® excels in this area, but first let's step back and review the history of BlackEnergy.

## History of BlackEnergy

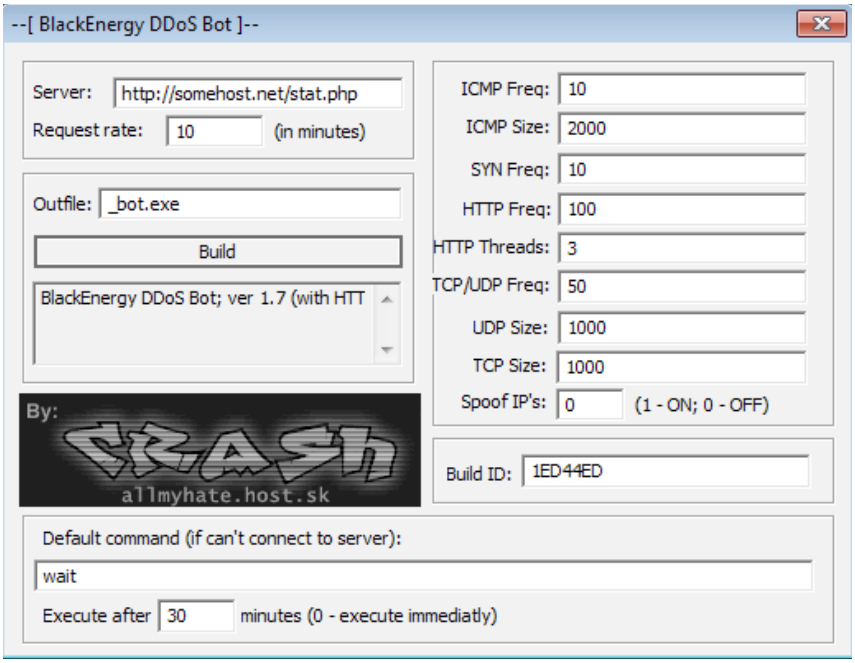
To understand our future, we must know our past. So let's take a look at BlackEnergy, which started life in 2007 as a very straightforward DDoS tool. The original tool was authored by "Cr4sh", who was associated with the 'Hellknights Crew'.







Early versions of BlackEnergy (as seen below) contained very few options. All configurable items were in a single 'page' of the builder application.




Over time, various components (and source code) of BlackEnergy emerged in forums and other dark and seedy corners of the net. This includes leaked source, cracked/leaked builder and panel components, and outright deviations/hijacks of the tool.

Versions 2 and 3 of BlackEnergy have expanded into fully-fledged and highly modular bots. BlackEnergy v2 fully introduced the modular (and updatable) plug-in feature, which made it very simple to expand functionality beyond DDoS, while retaining the core 'ease of use' for admins/bot-herders. Amongst the highly publicized new features were plug-ins for hijacking banking sessions and/or stealing banking credentials. In 2010, this functionality was widely observed as it was leveraged in attacks against Russian and Ukrainian banking customers[1].

The BlackEnergy tool excels in another cyber arena as well, the targeting of critical infrastructure. This was observed in 2015 in conjunction with Operation Sandworm. In 2014 and 2015 we saw hundreds of individual targets, including previous incidents in the Ukraine and Poland. Similar strains (with the KillDisk wiper) were observed in late 2015 when used against Ukrainian media outlets, which overwrote valuable media files with random data, targeting over 400 file extensions on company computers.

[1] http://www.darkreading.com/vulnerabilities---threats/new-blackenergy-trojan-targeting-russian-ukrainian-banks/d/d-id/1133120

## Interpreting Information from Ongoing Open Investigations

**Caveats: Are we looking at the right pile of 'noise'? If so, what's the right signal?**

There is currently a vast amount of Open Source Intelligence (OSINT) related to the latest campaign within the Ukraine, which targeted power distribution entities. Any security company or individual researcher can post and provide analysis data on these items, but any such post MUST come with the following caveat:

This is an ongoing and open investigation. Current OSINT, Indicators of Compromise and any other publically available artifacts should be considered incomplete. There is no current consensus that the long list of samples (provided by a number of prominent entities over the last few days) is truly and unquestionably associated with the latest round of attacks against the utility providers in the Ukraine.

As with any active investigation, only the specific parties directly involved in this investigation have the true indicators. So until those parties release or confirm the current crop of OSINT, we are only able to speculate and take a best-effort stab to connecting the dots and establishing provable relationships between these artifacts.

## Why Traditional AV is Unable to see in the Dark

Now, understanding the caveat above, we can confirm that the well-circulated list of artifacts is indeed BlackEnergy-related. Like previous generations, these are kit-based artifacts that are typically generated via the known and predictable builder apps. One would hope that modern AV with cloud-based detection features and hyper-paranoid heuristics would excel at detecting these artifacts and preventing such compromises, but they would be ultimately wrong.

Let's look at the primary dropper binaries and their traditional AV detections when first observed.

SHA256:

07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660

07a76c1d09a9792c348bb56572692fcc4ea5c96a77a2cddf23c0117d03a0dfad

When these samples were first publicly available, 07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660 was only detected by 30 of 55 vendors tested. Similarly we saw that sample 07a76c1d09a9792c348bb56572692fcc4ea5c96a77a2cddf23c0117d03a0dfad was detected by only 20 of 57 vendors tested.

Similar results can be observed with the destructive wiper (KillDisk) components.

SHA256:

11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80

5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6

c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d

f52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95

Upon initial release, sample f52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95 was only detected by 7 of 53 tested products! Only 7 detections, despite a very visible and observable level of 'badness'.

As you can see on the next page, the strings embedded in the f52869 sample show numerous potentially malicious commands available to the malware:

```
/c format %c: /Y /Q

/c format %c: /Y /X /FS:NTFS

kernel32.dll

InitiateSystemShutdownExW

InitiateSystemShutdownW

system32\cmd.exe

shutdown /r /t %d

/c del /F /S /Q %c:\

__Wow64DisableWow64FsRedirection
```

## Machine Learning = Night Vision

Machine learning powers Cylance's flagship product, CylancePROTECT®, and with that power comes amazing visibility in the dark, and even insight into the future. CylancePROTECT doesn't waste time analyzing a piece of software, downloading endless lists of malware updates or waiting for the malware to give away its position and 'do something' before it blocks it; the moment CylancePROTECT 'sees' a piece of malware, it 'knows' what it is and instantaneously blocks it from ever executing – even if the world has never seen that sample before.

When we first obtained the samples currently considered to be related to the major Ukrainian power outages, we found our detection was near perfect. Like many times before, without having previously observed the malware, CylancePROTECT was able to successfully classify the samples as malicious, while the majority of the products currently available from the rest of the AV industry struggle to catch up.

Let's take a look at our results:

| Category | SHA256 | Cylance Score |
|---|---|---|
| BlackEnergy Dropper | 07a76c1d09a9792c348bb56572692fcc4ea5c96a77a2cddf23c0117d03a0dfad | -0.997481544946 |
| BlackEnergy Dropper | 07e726b21e27eefb2b2887945aa8bdec116b09dbd4e1a54e1c137ae8c7693660 | -0.99949615696 |
| BlackEnergy Driver | 90ba78b6710462c2d97815e8745679942b3b296135490f0095bdc0cd97a34d9c | -1.0 |
| BlackEnergy Driver | cbc4b0aaa30b967a6e29df452c5d7c2a16577cede54d6d705ca1f095bd6d4988 | -1.0 |
| BlackEnergy Driver | 32d3121135a835c3347b553b70f3c4c68eef711af02c161f007a9fbaffe7e614 | -1.0 |
| BlackEnergy Driver | cfb20e7516b42486d11c59021a8be8a457ee1fa0d0be6d5d958e80b3cfeb04ae | -1.0 |
| BlackEnergy Driver | 1ce0dfe1a6663756a32c69f7494ad082d293d32fe656d7908fb445283ab5fa68 | -1.0 |
| BlackEnergy Driver | 3432db9cb1fb9daa2f2ac554a0a006be96040d2a7776a072a8db051d064a8be2 | -1.0 |
| BlackEnergy Driver | 5111de45210751c8e40441f16760bf59856ba798ba99e3c9532a104752bf7bcc | -1.0 |
| BlackEnergy Driver | 97be6b2cec90f655ef11ed9feef5b9ef057fd8db7dd11712ddb3702ed7c7bda1 | -1.0 |
| BlackEnergy Driver | 166ba02539d3ea8cd1298d916fad1264a815f55798df5477698b7d775542b696 | -0.999807341704 |
| BlackEnergy Driver | b73777469f939c331cbc1c9ad703f973d55851f3ad09282ab5b3546befa5b54a | -0.9999460447 |
| BlackEnergy Driver | edcd1722fdc2c924382903b7e4580f9b77603110e497393c9947d45d311234bf | -0.999993369412 |
| BlackEnergy Driver | 7874a10e551377d50264da5906dc07ec31b173dee18867f88ea556ad70d8f094 | -0.999996451234 |
| BlackEnergy Driver | 244dd8018177ea5a92c70a7be94334fa457c1aab8a1c1ea51580d7da500c3ad5 | -0.995401048757 |
| BlackEnergy Driver | 405013e66b6f137f915738e5623228f36c74e362873310c5f2634ca2fda6fbc5 | -0.999306684666 |
| BlackEnergy Driver | 7a393b3eadfc8938cbecf84ca630e56e37d8b3d23e084a12ea5a7955642db291 | -0.999865875218 |
| BlackEnergy Driver | edb16d3ccd50fc8f0f77d0875bf50a629fa38e5ba1b8eeefd54468df97eba281 | -0.999484358249 |
| BlackEnergy Driver | ac13b819379855af80ea3499e7fb645f1c96a4a6709792613917df4276c583fc | -0.999008357757 |
| Dropbear | 0969daac4adc84ab7b50d4f9ffb16c4e1a07c6dbfc968bd6649497c794a161cd | -0.999904036122 |
| KillDisk | f52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95 | -0.985950844972 |
| KillDisk | 11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80 | -1.0 |
| KillDisk | 5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6 | -1.0 |
| KillDisk | c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d | -0.998064124691 |

The only exception here was the modified version of Dropbear, which by itself is not malicious, as it would require the use of malicious software to be installed on a target's computer. As the malicious software itself would be caught by CylancePROTECT, Dropbear would be rendered harmless in this case.

## Winning the Digital Arms Race

As cybercriminals come up with ever more sophisticated malware, the digital arms race between humans and machines continues to play out in our seemingly most secure locations, many of which are under attack every minute of every day. As a race, humans are alarmingly shortsighted and naive; as we go about our daily lives, we don't like to think about the fact that the private and government entities designed to keep us safe may themselves be vulnerable to attack from the inside out.

Whether it is supplying our homes with heat and power during a blizzard, keeping our hard-earned money securely in our banks or keeping airplanes up in the air, software is used everywhere, every day to keep the wheels of civilization turning. All the while, adversaries constantly develop new attacks from all corners of the globe to conduct more ambitious and heinous acts.

Cylance was built with the notion that prevention is truly possible. Using artificial intelligence and machine learning to block threats before they cause us (and our infrastructure) harm, we are proud to be a disruptive force in the cybersecurity industry through our revolutionary, preventative approach that provides unprecedented levels of detection. And with detection comes freedom.

## About Cylance:

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated machine learning and artificial intelligence with a unique understanding of a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com

+1 (877) 973-3336
sales@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700, Irvine, CA 92612

CYLANCE