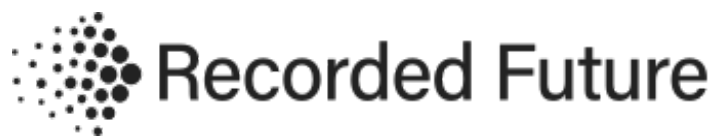


FREE SERVICE: Get trending cyber vulnerabilities delivered to your inbox every day.

SUBSCRIBE



Menu ☰



The Recorded Future Blog

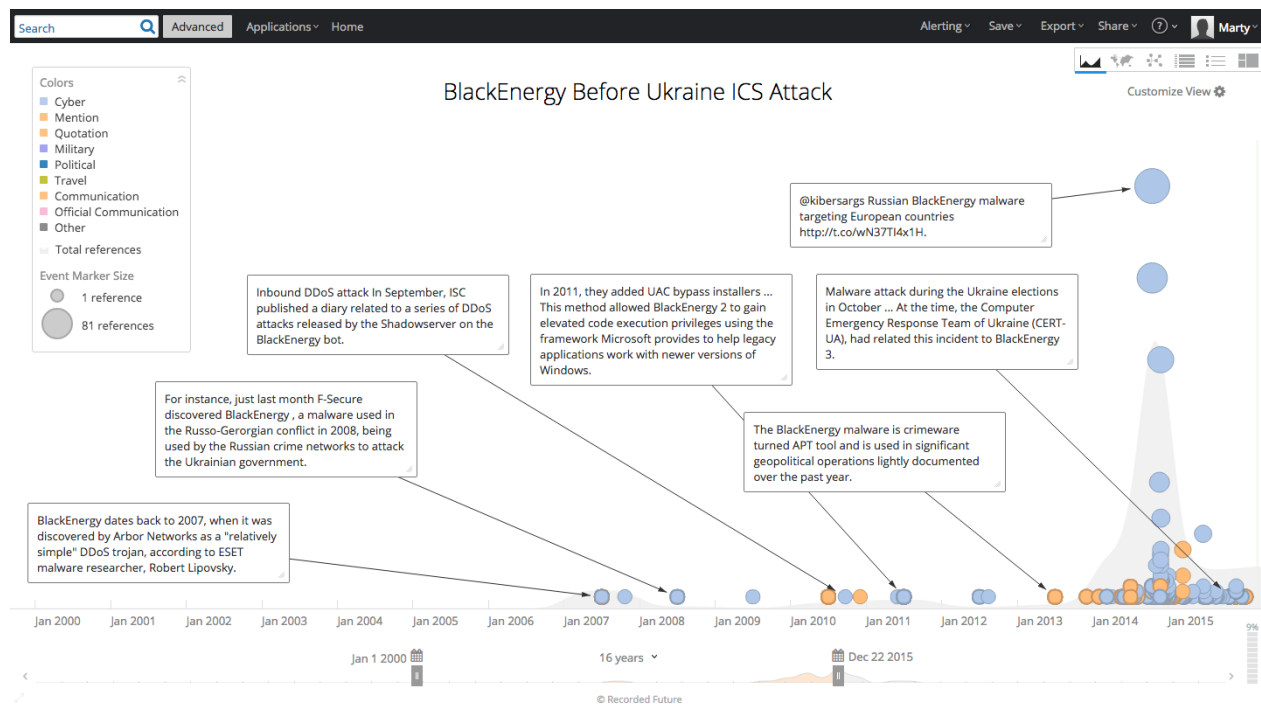


Shedding Light on BlackEnergy With Open Source Intelligence

If you're like me, you don't have access to the malware samples that infected the Ukrainian ICS (industrial control system) networks. You also don't have packet captures or event logs to try to recreate the series of events that lead to over 200,000 people losing power in late December of last year.

What I do have, however, is access to a couple of [open source intelligence tools](#) and a penchant for nerding out over high-profile cyber events.

Chances are, if you're reading this blog, you're familiar with [BlackEnergy](#) and its spot in the limelight due to the recent attacks on Ukrainian infrastructure. For anyone just joining us, I've included a timeline illustrating BlackEnergy's evolution from a "relatively simple" DDoS tool to the multi-capable APT tool it has grown into today.



In 2014, shortly after being picked up by APT groups and becoming more modular, we see a large spike in references to the malware and its increasing usage in European countries, namely Ukraine.

Coincidentally (or maybe not) this spike parallels the growing Russia-Ukraine political tensions of the time and brings us right up to the moment the community as a whole took notice: the power outage of December 23, 2015.

There is [dissention among those reporting](#) on the incident as to the exact role BlackEnergy had in the attack, the other malicious binaries involved, and, rightfully so, where attribution should lie. It is not my intention to provide the smoking gun that answers any of those points; but rather, offer a path other analysts can follow to build upon the information they do have and draw those conclusions for themselves.

Also, whatever the specifics of those questions may be, the implication remains the same: an unauthorized remote user can gain access to a critical infrastructure system and cause far reaching effects in the physical world.

Indicators of Compromise (IOC) Analysis

Shortly after the attack, the experts at ESET [published an excellent article](#) that provided the information used as the jump off point for my analysis. The article abounds with indicators for follow on analysis to include: build ids, command and control (C2) nodes, and hashes for every component from the macro-embedded XLS to the drivers for the malware it dropped. Chief among them (and the avenue that proved most valuable for supplemental intelligence) was the list of C2 nodes*.

In most cases, IP addresses are too fickle for any lasting intelligence to be garnered from them, especially when the analysis is days or weeks post-event. However, because the C2s were hard coded into the exploit, it can be assumed that information about these particular IPs has a little more staying power and is worth

pursuing.

**It should be noted that BlackEnergy has been seen using binaries masquerading as legitimate system processes, so the hashes of the malicious executables are very important for mitigation and system integrity purposes.*

Contrasting Mix of Hardcoded IPs and Tor Nodes

The first course of action was to see what kind of historical information I could surface. Recorded Future data shows five of the six IPs characterized as running Tor services and some appearing on block lists.

C2 Nodes

5.149.254.114

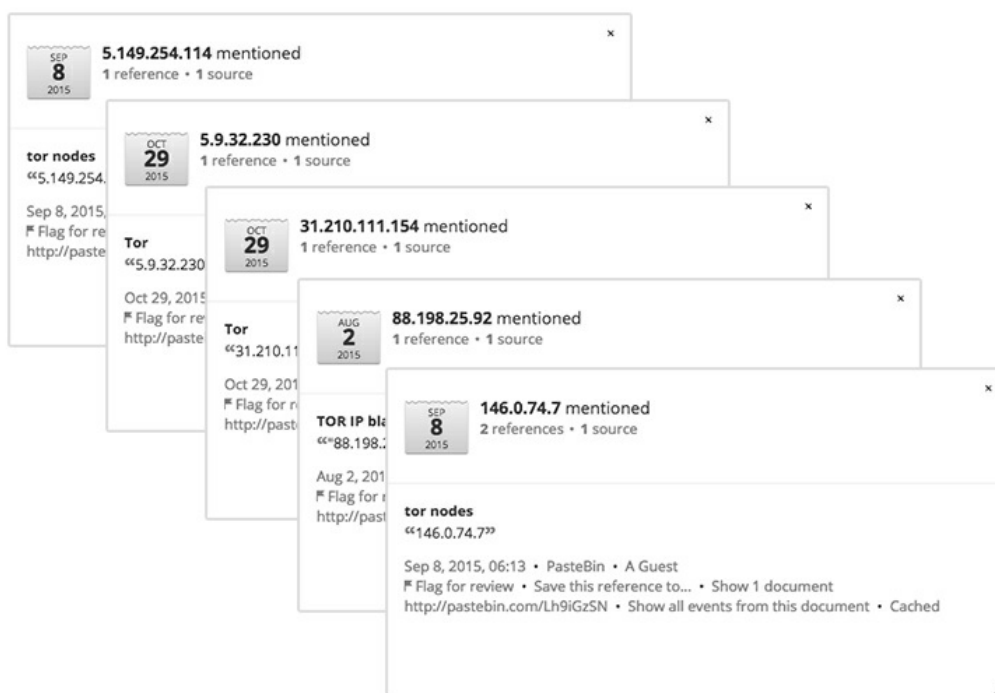
5.9.32.230

31.210.111.154

88.198.25.92

146.0.74.7

188.40.8.72





The combination of hardcoded IPs and Tor exit nodes seems almost counterintuitive. Perhaps the goal was to further the perception of volatility of the IP, or to obfuscate the real purpose of the C2.

“A subnet with only 32 IPs that is part of an attack is immediately more suspicious as a whole than one with 65,536 IPs.”

One IP (188.40.8.72) however, did not appear in Recorded Future data at all (previous to the ICS attack). A general Google search also yielded very little results, none meaningful. This got me curious as to the owner of the IP and the services it was setup to run. I took to DomainTools and Shodan for the answers to my questions.

DomainTools didn't reveal much in the way of registrar information, but that was to be expected. They were leasing the address through a major German service provider. I did find two things interesting about the results though.

First, the unusually small subnet that the IP resided within. Usually we see malware beaconing back to an IP that is part of a large /16 or similar sized subnet to try and get lost in the noise. A subnet with only 32 IPs that is part of an attack is immediately more suspicious as a whole than one with 65,536 IPs. Queries for the other 31 IPs returned as few results as the first, but I would be wary of any traffic originating from that subnet.☒

IP Location	 Germany Nuremberg Hetzner Online Ag
ASN	 AS24940 HETZNER-AS Hetzner Online GmbH (registered Jun 03, 2002)
Resolve Host	static.72.8.40.188.clients.your-server.de
Whois Server	whois.ripe.net
IP Address	188.40.8.72

```
% Abuse contact for '188.40.8.64 - 188.40.8.95' is ' abuse@hetzner.de '
inetnum:          188.40.8.64 - 188.40.8.95
```

The second thing of note is the static subdomain. Static subdomains are used to reliably serve static content to other hosts on a network. Another useful characteristic of static subdomains is that they can be hosted on content delivery networks (CDN) such as CloudFlare or BitTorrent, providing high performance and availability of content. Although not malicious in and of itself, we have seen [many examples](#) of malware using this practice in the past.

Now I wanted to find out what services were running on this box, so I utilized Shodan (a tool used to fingerprint Internet-connected devices). Shodan revealed that the node was running OpenSSH on a Debian platform.

 **188.40.8.72** static.72.8.40.188.clients.your-server.de

Country	Germany
Organization	Hetzner Online AG
ISP	Hetzner Online GmbH
Last Update	2015-12-21T10:59:23.205276
Hostnames	static.72.8.40.188.clients.your-server.de
ASN	AS24940

Ports

22

Services

22

tcp

ssh

OpenSSH Version: 6.6.1p1 Debian 4~bpo70+1

```
SSH-2.0-OpenSSH_6.6.1p1 Debian-4~bpo70+1
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQDpdGAB17/+6L7yK3IT0Spf0Z9PeU7/Cig6utazXX
iLU31I
+UrSh4PFg0J8LrsPVfUVHjLLpQyQ5iVX76RnSrvRX00cTaX4rroEZ+a+QJiViCoYh15Ie2D0ZFT
G
bGJ8jqDy45mptBUMJmpj0tUCLkwRGvf2Kf6KsnzR0bmbb64ZmwbemDf0hSIja0XeXdeuuHf8eUy
i
7sPcKjq7pwvy+P6xZdErAW+y8EXGA3bDFjNKd87JxZwfGczCQ447r384mgBokc3bb297Q3tRS
N
nzGHLN7iKLNUS0hFJqV1vv0N87sD4b/ds80/pzXn18c9YBmuLhit5p//uwvVGfyJIcyl
Fingerprint: 54:0d:23:26:fb:40:ce:13:d8:8d:0d:6c:48:8e:cb:b0
```

According to the ESET article, a previously unknown backdoor in the DropbearSSH protocol was utilized. This box may have been used for development and testing of the exploit. We were also able to gain insight into the structure of the network, which technologies and software versions were present, and possibly what types of files we could expect to be hosted on the machine.

I followed the same workflow for the other command and control nodes listed in the article. The registrar information once again didn't give me much, although we do see another /27 subnet and static subdomain (5.9.32.230). Two of the five remaining IPs were running HTTP and HTTPS (80 and 443) when I fingerprinted them (31.210.111.154 and 146.0.74.7). Two were not responding (88.198.25.92 and 5.9.32.230). The last host (5.149.254.114) however, was interesting.

5.149.254.114 had several open ports for remote administration services including: NetBIOS (135, 137, 139, and 445), Microsoft RDP for virtual machines (2179), WS-Management and Powershell (5985), multiple ephemeral ports, and most notably port 2223. Port 2223 is the assigned port for the protocol "Rockwell CSP2", which

is the client/server protocol used by Rockwell Automation for their ICS devices.

It's possible this host was used to test the exploits used for, or issue commands to, the compromised ICS devices. If neither were the case, and no devices running Rockwell CSP were involved, it is still at least noteworthy that the host was listening on that port, especially given the modular nature of the malware.

5.149.254.114 mail1.auditoriavanzada.info

Ports

```
[+] Nmap scan report for mail1.auditoriavanzada.info (5.149.254.114)
Host is up (0.0083s latency).
Not shown: 91 closed ports

PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

5985

```
5.149.254.114 isn't responding on port 2177 (qwave).
5.149.254.114 isn't responding on port 2178 (bitspeer).
5.149.254.114 is responding on port 2179 ().
```

Services

5985

tcp

http

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 30 Dec 2015 14:44:26 GMT
Connection: close
Content-Length: 315
```

Immediate Takeaways

While an analysis of the attack details is fun and interesting, it won't change the important implications we can draw from this case, namely:

- Whether or not the attack was nation state sponsored, the source code for most of the components that were used is available for purchase and download on the open Web.
- It's no longer far fetched that a similar attack could be conducted by non-nation state sponsored groups for criminal purposes.
- Whatever the events subsequent to the malware being utilized, it was still a method decades old that won the day and enabled the infection: spear phishing.
- User education and, given the ability to erase data with the KillDisk component, data backup and offsite storage practices are still crucial.☒
- This is yet another proof of concept that malware can have tangible effects beyond the cyber landscape.☒

Mitigation and Other Interesting Finds

The open source community is not only fantastic for gathering information about a malware event; it's also a great resource for finding ways to mitigate that malware. Running a simple search in Recorded Future we can quickly uncover a YARA rule that was created shortly after the attack (January 4, 2016) and also one in mid February designed to catch the KillDisk component.

Events

Involving "yara" x Add | v
 AND
 "blackenergy" x Add | v

Event Type Any event type

Event Time Anytime x

Publish Time Anytime

Sources Nothing selected

Exclude Nothing selected

Clear All Options **DONE**

#BlackEnergy and github.com mentioned
 1 reference • 1 source • United States

#Blackenergy YARA sigs https://t.co/CEXPhUZEMe
 "@bry_campbell #Blackenergy YARA sigs https://t.co/CEXPhUZEMe."

Jan 4, 2016, 18:56 • Twitter • @Bry_Campbell
 Flag for review • Save this reference to...
https://twitter.com/Bry_Campbell/statuses/684086032514572289 • Show all events from this document

```

Neo23x0 Change BlackEnergy ruleset to a generic one
1 contributor

172 lines (161 sloc) | 7.27 KB

1 /*
2 Yara Rule Set
3 Author: Florian Roth
4 Date: 2015-02-19
5 Identifier: BlackEnergy Malware
6 */
7
rule BlackEnergy_KillDisk_1 {
  meta:
    description = "Detects KillDisk malware from BlackEnergy"
    author = "Florian Roth"
    reference = "http://feedproxy.google.com/~r/ eset/blog/~3/BXJbnGSvEfc/"
    date = "2016-01-03"
    score = 80
    super_rule = 1
    hash1 = "11b7b8a7965b52ebb213b023b6772dd2c76c66893fc96a18a9a33c8cf125af80"
    hash2 = "5d2b1abc7c35de73375dd54a4ec5f0b06ca80a1831dac46ad411b4fe4eac4c6"
    hash3 = "c7536ab90621311b526aef56003ef8e1166168f038307ae960346ce8f75203d"
    hash4 = "f52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95"

  strings:
    $s0 = "system32\\cmd.exe" fullword ascii
    $s1 = "system32\\liclacs.exe" fullword wide
    $s2 = "/c del /F /S /Q %c:\\*.*" fullword ascii
    $s3 = "shutdown /r /t %d" fullword ascii
    $s4 = "/C /Q /grant " fullword wide
    $s5 = "%08X.tmp" fullword ascii
    $s6 = "/c format %c: /Y /X /FS:NTFS" fullword ascii
    $s7 = "/c format %c: /Y /Q" fullword ascii
    $s8 = "taskhost.exe" fullword wide /* Goodware String - occurred 1 times */
    $s9 = "shutdown.exe" fullword wide /* Goodware String - occurred 1 times */

  condition:
    uint16(0) == 0x5a4d and filesize < 500KB and 8 of them
}

```

Applying the same process to *historical indicators of compromise* attributed to the BlackEnergy malware surfaced a few other notable finds. Among a myriad of hostnames, registrars, and services running, two stood out:

188.128.123.52 which was running a Cisco PIX firewall, secure mail services, and whose hostname resolved to mail1.mil.ru.

🌐 188.128.123.52 mail1.mil.ru

City	Moscow
Country	Russian Federation
Organization	Rostelecom
ISP	Rostelecom
Last Update	2016-02-06T17:31:07.806200
Hostnames	mail1.mil.ru
ASN	AS12389

🗄️ Ports

26	995
----	-----

🗄️ Services

26	Cisco PIX sanitized smtpd
tcp	220 *****
ssh	

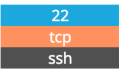
995	+OK Dovecot ready.
tcp	+OK
pop3-ssl	CAPA
	TOP
	UIDL
	RESP-CODES
	PIPELINING
	USER
	SASL PLAIN LOGIN

And 94.185.85.122 which aside from HTTP, DNS, and SSH server ports open, was set up to receive traffic on port 2222, another port assigned to handle Rockwell CSP traffic (among other services such as EtherNet/IP I/O).

City	Stockholm
Country	Sweden
Organization	Netrouting Telecom Sweden
ISP	Netrouting
Last Update	2016-02-18T00:14:56.183163
Hostnames	ip4-94-185-85-122.rdns.netrouting.net
ASN	AS47869



Services



```

OpenSSH Version: 6.0p1 Debian 4+deb7u2
SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQCF9Z0CMNc5ZNu7GcGYbwgkA+by2NQTX
7HTgHpdhe0hUG76
EsbxXWSXiFUo6fw6mxfXU/Cza0BHuTtvADLCMG6JgM/gK9PJd6nP8UckvtZKVHV0Uw
fWeF3Y0am+
t0FTTk0UHVNXzP0quI+mZzHHQ0qnCaqLT6BVvo0TuXiyUaskyLP7WICxnF+FMb1b0
hzVs+Rd1mf
36YnAIUUrKCMVaqZijD0tpa41WKMq2FWfk1LatQco7uINBb+4SStHZy6mnWfPs6nNJ
DYb+EgULcP
i/4i1ycKGkmXMX6bPv3xM2Vz8u2uQtYUqkw1ZX8W72vQtzTP6cCM/0nxGf+qWFCncI
Q7
Fingerprint: 95:d5:17:9f:1d:b5:40:5b:e7:68:24:55:f0:b5:6b:68

```

What You Should Do

As an analyst with a background rooted in network defense, these findings would prompt me to implement and reiterate multiple core concepts:

- End-user education remains paramount to the prevention of unauthorized access to your networks.
- Disallow emails with embedded macros entirely.
- Know what your network is supposed to look like and the processes running on it.
- Conduct regular audits to ensure the integrity of those processes.
- Utilize IP and port whitelisting and blacklisting.
- Adhere to data redundancy and offsite storage best practices.¹
- And finally, continue to monitor the open Web for new developments and stay abreast of mitigations for any changes in the malware.

¹ESET is an IT security company headquartered in Bratislava, Slovakia that was founded in 1992.

Posted by

Zach

March 3, 2016 in [Cyber Threat Intelligence](#)



FREE

**TRENDING
CYBER VULNERABILITIES
DELIVERED TO
YOUR INBOX DAILY**

▼

SUBSCRIBE

OVER **7,000** SUBSCRIBERS



THREAT INTELLIGENCE TWEAKS THAT'LL TAKE YOUR SECURITY TO THE NEXT LEVEL

By Pete Hugh on March 15, 2016

DEFEATING MALWARE COUNTERINTELLIGENCE GUIDE: BUILDING A CHEAP LOCAL WINDOWS/LINUX MALWARE TEST ENVIRONMENT

By Levi Gundert on March 8, 2016

SHEDDING LIGHT ON BLACKENERGY WITH OPEN SOURCE INTELLIGENCE

By Zach on March 3, 2016

3 SIGNS YOUR INFORMATION SECURITY TEAM NEEDS THREAT INTELLIGENCE

By Pete Hugh on March 2, 2016

WANT MORE FROM RSA THAN SEAN PENN? RECORDED FUTURE HAS YOU COVERED

By Amanda on February 26, 2016

Company

About

Jobs

Events

Press

Contact

For Customers

Login

Support Center

Software Status

Developer Code

Copyright © 2016 Recorded Future, Inc.

[Privacy Policy](#)

[Terms of Use](#)

[API Terms of Use](#)