MUST READ Experts revealed that security camera vendors lack of security by design

iSight Partners says the Sandworm APT is involved Ukrainian power outage

January 8, 2016 By Pierluigi Paganini

The Russian Sandworm APT group if the first suspect for the Ukrainian power outage, states experts at eiSight Partners.

According to a report published by experts at eiSight Partners the cyber attack against a Ukraine power station has been managed by a Russian group called Sandworm.

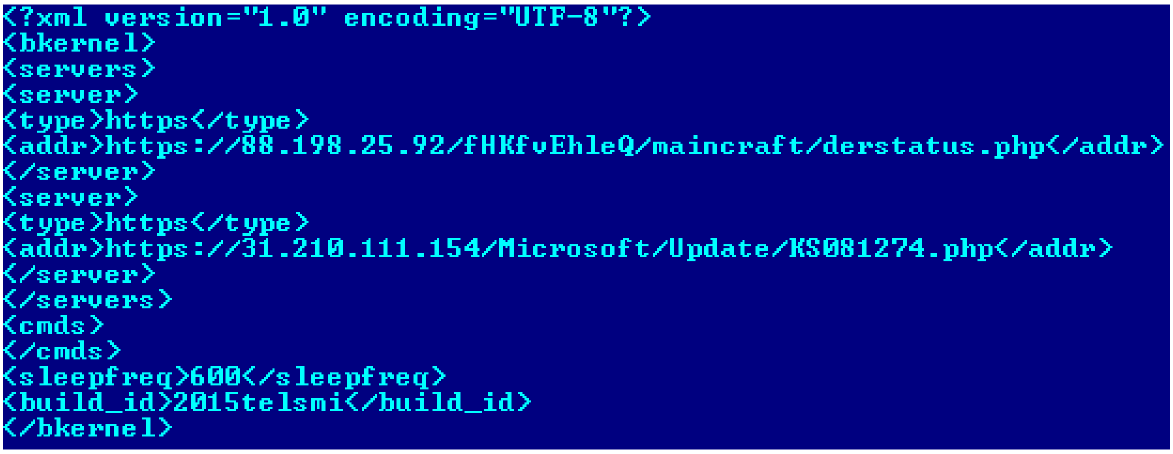
A few days ago experts at ESET reported the existence of a new component in the BlackEnergy trojan, the KillDisk module which is capable of destroying some 4000 different file types and rendering machines unbootable.

"ESET has recently discovered that the BlackEnergy trojan was recently used as a backdoor to deliver a destructive KillDisk component in attacks against Ukrainian news media companies and against the electrical power industry. " states the blog post published by ESET.

Now experts at iSIGHT's linked the KillDisk to the BlackEnergy 3 used by Sandworm in the past.

"Last week iSIGHT's sources provided us with the same KillDisk malware published by Rob Lee of SANS and Dragos Security. As ESET has, we place this malware within the greater context of activity tied to BlackEnergy

3, which we believe is Sandworm Team. We believe this KillDisk malware is related to the destructive malware leveraged during Ukrainian elections in October. At the time, CERT-UA connected that incident to BlackEnergy 3. Symantec has since verified those claims. Furthermore, iSIGHT's own sources indicate that BlackEnergy 3 malware was deployed on at least one of the Ukrainian power systems affected by KillDisk." wrote John Hultquist, director of cyberespionage analysis at iSight Partners.



```
<?xml version="1.0" encoding="UTF-8"?>
<bkernel>
<servers>
<server>
<type>https</type>
<addr>https://88.198.25.92/fHKfvEhleQ/maincraft/derstatus.php</addr>
</server>
<server>
<type>https</type>
<addr>https://31.210.111.154/Microsoft/Update/KS081274.php</addr>
</server>
</servers>
<cmds>
</cmds>
<sleepfreq>600</sleepfreq>
<build_id>2015telsmi</build_id>
</bkernel>
```

The hackers used the highly destructive malware to compromise the systems at three regional power authorities in Ukraine. The attacks caused blackouts across the Ivano-Frankivsk region of Ukraine on 23rd December.
According to a Ukrainian media TSN, the power outage was caused by a destructive malware that disconnected electrical substations.
Also in this case, hackers launched a spear-phishing campaign across the Ukrainian power authorities to spread the destructive variant to the BlackEnergy leveraging on Microsoft Office documents.

The attribution of the attack is not simple, we are only aware that the BlackEnergy malware has a Russian origin and that Russian has a political dispute with the Ukraine that had repercussion also on the cyberspace.

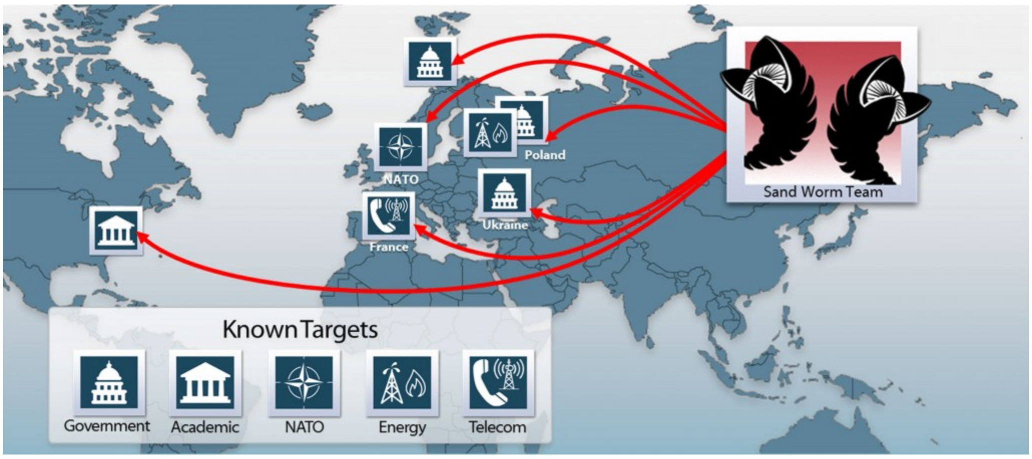
My readers have already read about Sandworm, according to a previous report issued by iSIGHT, the APT has been active since at least 2009. In 2014, the Russian group targeted a Polish energy firm, a Western European government agency and also a French telecommunications firm.

The experts began the investigation in late 2013 when the NATO alliance was targeted by the SandWorm hacking team with exploits other than the zero-day, but they discovered the critical zero-day in August 2104, when the group targeted the Ukrainian government, in the lead-up to the NATO summit in Wales.

> *"In late August, while tracking the Sandworm Team, iSIGHT discovered a spear-*

> ***phishingcampaign targeting the Ukrainian government and at least one United States organization. Notably, these spear-phishing attacks coincided with the NATO summit on Ukraine held in Wales." states the report published by iSIGHT.***

Security experts speculated that the intensification of the cyber dispute between Russian and Ukraine could have increased the likelihood to discover operations that went under the radar for so long.



Below chronological details provided by the researchers on the Sandworm activity:

- *The NATO alliance was targeted as early as December 2013 with exploits other than the zero-day*
- *GlobSec attendees were targeted in May of 2014 with exploits other than the zero-day*
- *June 2014*
    - *Broad targeting against a specific Western European government*
    - *Targeting of a Polish energy firm using CVE-2013-3906*
    - *Targeting of a French telecommunications firm using a BlackEnergy variant configured with a Base64-encoded reference to the firm*

The SandWorm hacking team sent spear-phishing emails with malicious attachments to compromise the victim's machine, the threat actors mentioned a global security forum on Russia and a purported list of Russian terrorists.

Another element that suggests Russia is responsible for the cyber espionage campaign are codes discovered on the C&C server, located in Germany, that had not been properly secured and that contains Russian-language computer files that had been uploaded by the hackers.

“

“They could have closed it off, and they didn’t,”

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence |
Laws and regulations | Malware | Mobile | Data Breach | Security | Social Networks |
Reports | EXTENDED COOKIE POLICY | Contact me |
Mobile Data Breach Security Social Networks
Reports EXTENDED COOKIE POLICY Contact me

ing the

hackers.”

lanned order to show the ability of abnormal function compromised corporate media networks by using a tool such hackers as ***Black Energy*** *(Win32 / Rootkit.BlackEnergy, Backdoor.Win64.Blakken), which is used to conducting APT-attacks.”*

Stay Tuned!

Pierluigi Paganini

(Security Affairs – Black Energy, Sandworm)

Share it please …

APT | BlackEnergy | Hacking | Information Warfare | Russia | Sandworm | Ukraine

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and

MORE S

Expert camera by desi

When it c business

ly named
e Hacker

privileged
exposing

News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Experts revealed that security camera vendors lack of security by design

YOU MIGHT ALSO LIKE

Experts revealed that security camera vendors lack of security by design

January 8, 2016 By Pierluigi Paganini

Time Warner Cable security breach may have exposed 320K customers

January 8, 2016 By Pierluigi Paganini