BlackEnergy infected also Ukrainian Mining and Railway Systems

February 13, 2016 By Pierluigi Paganini

Experts at Trend Micro discovered strains of BlackEnergy malware involved in the recent attacks against Ukrainian Mining and Railway Systems.

BlackEnergy was in the headlines when the security industry examined the power outage occurred in Ukraine in December 2015.

The BlackEnergy malware is a threat improved to target SCADA systems, the latest variant includes the KillDisk component developed to wipe the disks and make systems inoperable.

The Ukrainian government accused Russia of being involved in the attack that caused the power outages, but further analysis revealed that the BlackEnergy malware was not directly responsible for the outages.

Now Trend Micro announced that have spotted operator.

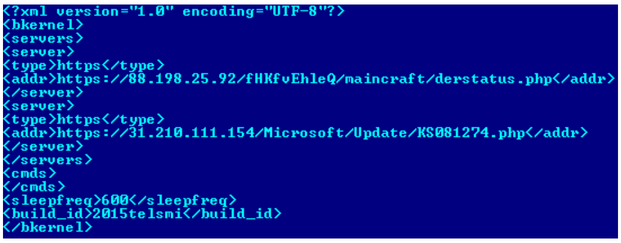
The experts noticed that the systems at the mining company were also infected with multiple variants of KillDisk, these samples implements the same features observed in the KillDisk component that infected the power utilities in Ukraine.

The security researchers believe that the threat actors behind them is the same that targeted the Ukrainian power companies.

The researchers noticed many similarities between the samples, naming conventions, control infrastructure, and the timing of the attacks.

TrendMicro spotted several samples similar to the BlackEnergy variant that infected the Ukrainian power utility, the malware used the same command and control (C&C) servers.

"Like the attacks against the Ukrainian mining company, we also witnessed KillDisk possibly being used against a large Ukrainian railway company that is part of the national Ukrainian railway system. The file tsk.exe (SHA1:□ f3e41eb94c4d72a98cd743bbb02d248f510ad925) was flagged as KillDisk and used in the electric□ utility attack as well as against the rail company. This appears to be the only spillover from the Ukrainian power utility infection. However, we have no proof showing that BlackEnergy was present on the railway systems, it could be assumed that it was likely present somewhere in their network." states a blog post published by Trend Micro.



```
<?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 experts elaborated several theories about the attack, one of the most plausible is the offensive of a politically motivated persistent attacker that intends to hit Ukrainian critical infrastructure to destabilize the country.

"One is that the attackers may have wanted to

destabilize Ukraine through a massive or persistent disruption involving power, mining, and transportation facilities," Wilhoit said. "Another possibility is that they have deployed the malware to different critical infrastructure systems to determine which one is the easiest to infiltrate and□ subsequently wrestle control over. A related theory is that the infections in the mining and train companies may have just been preliminary infections, where the attackers are just attempting to test the code base."

Whichever is the case, cyber attacks against critical infrastructures represent a serious threat against any government.

Pierluigi Paganini

(Security Affairs – BlackEnergy, critical infrastructure)

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 awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker 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

UK police arrested teenage hacker who allegedly hacked CIA and FBI officials

NEXT ARTICLE

The IPT ruled that GCHQ spies can legally hack any electronic devices

YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini

- +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) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top ^