

# Threatpost | The first stop for security news

- [Categories](#)
  - [Category List](#)
    - [Cloud Security](#)
    - [Critical Infrastructure](#)
    - [Cryptography](#)
    - [Government](#)
  - [Category List](#)
    - [Hacks](#)
    - [Malware](#)
    - [Mobile Security](#)
    - [Privacy](#)
  - [Category List](#)
    - [SAS](#)
    - [Vulnerabilities](#)
    - [Web Security](#)
  - [Authors](#)
    - [Michael Mimoso](#)
    - [Christopher Brook](#)
  - [Additional Categories](#)
    - [Slideshows](#)
  - [The Kaspersky Lab News Service](#)
- [Featured](#)
  - [Authors](#)
    - [Michael Mimoso](#)
    - [Christopher Brook](#)
  - [The Kaspersky Lab News Service](#)

## Featured Posts

[All](#)[‘Deliberate’ Backdoor Removed From Secure Conferencing...](#)[Threatpost News Wrap, January 22, 2016](#)[Apple Fixes Cookie Theft Bug in...](#)

- [Podcasts](#)

## Latest Podcasts

[All](#)



[Threatpost News Wrap, January 22, 2016](#)



[Threatpost News Wrap, January 15, 2016](#)



[Threatpost News Wrap, January 8, 2016](#)



[Threatpost's 2015 Year in Review](#)



[Threatpost News Wrap, October 30, 2015](#)



[Gary McGraw on BSIMM6 and Software...](#)

## Recommended

[The Kaspersky Lab Security News Service Videos](#)

## Latest Videos

[All](#)



[Kris McConkey on Hacker OpSec Failures](#)



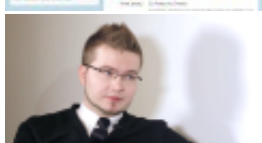
[Trey Ford on Mapping the Internet...](#)



[Christofer Hoff on Mixed Martial Arts,...](#)



[Twitter Security and Privacy Settings You...](#)



[The Biggest Security Stories of 2013](#)



[Jeff Forristal on the Android Master-Key...](#)

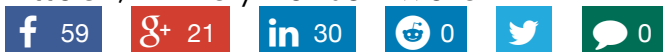
## Recommended

[The Kaspersky Lab Security News Service](#)

- [Twitter](#)
- [Facebook](#)
- [Google](#)
- [LinkedIn](#)
- [YouTube](#)
- [RSS](#)



[Welcome](#) > [Blog Home](#) > [Malware](#) > Israeli Electric Authority Hit by ‘Severe Cyber Attack,’ Likely Ransomware



## Israeli Electric Authority Hit by ‘Severe Cyber Attack,’ Likely Ransomware

by [Chris Brook](#) January 27, 2016 , 12:55 pm

Earlier this week Israel's Electric Authority mitigated what officials there are calling a "severe cyber attack."

The Electric Authority is in charge of regulating and overseeing the distribution of electricity in Israel.

## Related Posts

[Dridex Borrows Tricks From Dyre, Targets U.K. Users](#)

January 20, 2016 , 11:00 am

[Apple's 'Targeted' Gatekeeper Bypass Patch Leaves OS X Users Exposed](#)

January 15, 2016 , 8:00 am

[13 Brain Test Malicious Apps Booted From Google Play](#)

January 6, 2016 , 4:01 pm

The State of Israel's National Infrastructure, Energy and Water Resources Minister Yuval Steinitz disclosed the incident, calling it a virus Tuesday, during closing remarks at the [Cybertech Conference](#) in Tel Aviv.

Details around the incident are a little hazy. Some reports are contesting the attack, insisting the agency was hit by ransomware instead.

According to Steinitz, the incident occurred on Monday, coinciding with rapidly plunging temperatures across Israel. The Minister claims as a result of the attack workers at the Authority powered down parts of the system to prevent the virus from spreading after it struck their computer network on Monday.

[According to Haaretz](#), Israel's oldest newspaper, Steinitz told a thinning crowd that Authority had the "right software" to tackle the issue.

"The virus was already identified and the right software was already prepared to neutralize it," Steinitz told the crowd, "We had to paralyze many of the computers of the Israeli electricity authorities. We are handling the situation and I hope that soon, this very serious event will be over."

According to [The Times of Israel](#) he claims the event was "a fresh example of the sensitivity of infrastructure to cyberattacks, and the importance of preparing ourselves in order to defend ourselves against such attacks."

Conflicting reports on Wednesday argue the Authority wasn't hit by an attack per se, but by ransomware.

Some reports, including one from the [Israeli news site Ynet](#), states the Authority wasn't hit by an attack, but instead with malware that prevented access to data "in exchange for ransom." The article claims the malware locked computers, spread to others on the corporate computer network, and that as of Wednesday afternoon, Israel Standard Time, many machines were still "paralyzed."



The article cites an unnamed government source, who expressed disbelief the Authority's networks weren't properly secured.

"It's just unbelievable the authority's computer system was not properly protected."

The Israeli National Cyber Defense Authority [warned last summer](#) the State could be targeted by cyber attacks and that security officials should "prepare for any possible scenario."

A report in [The Media Line](#) on Wednesday talked to Yosi Shneck, SVP of Information & Communication at Israel Electric Corporation, a power supplier in Israel separate from Israel's Electric Authority. Shneck claims ransomware has hit the IEC's systems "in recent months" and that he faces "between 4 to 20 million" cyber events in an average month and that he "maybe" knows where the malware originated from, but can't officially say.

Regardless of whether it's an attack or ransomware, details around the incident remain scant. It's unclear who's behind the malware, or triggered the attack. Steinitz claims there are no suspects and that the National Infrastructure, Energy and Water Resources Ministry and Israel's National Cyber Bureau are investigating the incident however.

The incident is the latest to affect a nation's electricity infrastructure.

A cyber attack hit Western Ukraine power company Prykarpattiaoblenergo last month, leaving hundreds of thousands of residents in the Ivano-Frankivsk region in the dark.

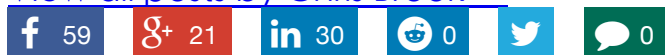
Attackers peddling BlackEnergy malware have demonstrated an affinity for targeting power facilities, generation operators, and power sites [in the past](#) and are believed to have had a hand in the attack.



## About Chris Brook

"Distrust and caution are the parents of security" - Benjamin Franklin

[View all posts by Chris Brook →](#)



Categories: [Malware](#), [Vulnerabilities](#)

## Leave A Comment

Your email address will not be published. Required fields are marked \*


Comment

You may use these HTML tags and attributes: <a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>

Name

Email

☐ I'm not a robot

  
reCAPTCHA  
[Privacy](#) - [Terms](#)

Post Comment

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

## Recommended Reads



January 20, 2016 , 11:00 am

Categories: [Malware](#), [Uncategorized](#)

### [Dridex Borrows Tricks From Dyre, Targets U.K. Users](#)

by [Chris Brook](#)

Attackers behind the Dridex Trojan have narrowed their sights on banks based in the United Kingdom frequented by high-value business accounts, researchers claim.

[Read more...](#)



January 15, 2016 , 8:00 am

Categories: [Hacks](#), [Malware](#), [Vulnerabilities](#), [Web Security](#)

## [Apple's 'Targeted' Gatekeeper Bypass Patch Leaves OS X Users Exposed](#)

by [Michael Mimoso](#)

Two separate Apple patches for Gatekeeper bypasses have been incomplete, and leave users exposed to attacks.

[Read more...](#)



January 6, 2016 , 4:01 pm

Categories: [Uncategorized](#)

## [13 Brain Test Malicious Apps Booted From Google Play](#)

by [Michael Mimoso](#)

Researchers at mobile security company Lookout found 13 malicious apps on Google Play that are related to the Brain Test malware family.

[Read more...](#)

## Top Stories

### [Government Agencies Audit for Juniper Backdoor](#)

January 26, 2016 , 9:59 am

### [Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47](#)

December 2, 2015 , 11:18 am

[Cisco Patches Hardcoded Password, DoS Vulnerabilities in Software, Devices](#)

January 14, 2016 , 11:15 am

[Time Warner Cable Urges 320,000 Customers to Change Passwords](#)

January 7, 2016 , 1:54 pm

[Denial-of-Service Flaw Patched in DHCP](#)

January 13, 2016 , 10:00 am

[Inexpensive Webcam Turned into Backdoor](#)

January 12, 2016 , 10:39 am

[New JavaScript Ransomware Sold as a Service](#)

January 4, 2016 , 11:04 am

[Curious Tale of a Microsoft Silverlight Zero Day](#)

January 13, 2016 , 9:01 am

[New RAT Trochilus Skilled at Espionage, Evading Detection](#)

January 12, 2016 , 12:14 pm



## TIP #3



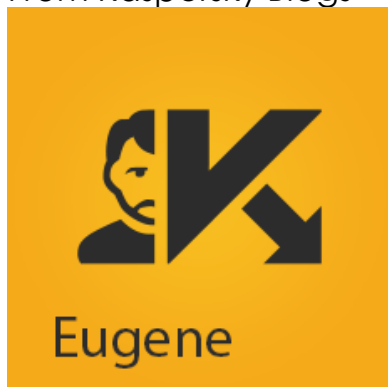
**Security policies  
should work  
everywhere**

even outside the workplace

[Click to learn more](#)

## The Final Say

From Kaspersky Blogs



[Three questions for physicists....](#)

I did a fair bit of walking in Tanzania on our Kilimanjaro expedition – a whole week’ s worth, in fact. That meant I had plenty of time – besides chatting to my companions – to ponder, contemplat...

[Read more...](#)



### [The Asacub Trojan: from spyware to banking malware...](#)

We were recently analyzing a family of mobile banking Trojans called Asacub, and discovered that one of its C&C servers is also used by CoreBot, a Windows spyware Trojan. This prompted us to do a...

[Read more...](#)



### [Twitter Star or Identity Fraud? A scary case of pu...](#)

So your social media photos are public, great. Ever wonder what could happen when they get stolen?...

[Read more...](#)



### [Hyatt hotel chain hit by financial malware; how to...](#)

The Hyatt hotel chain has revealed recently that 250 of 627 of its properties worldwide

were infected with money-stealing malware. Customer financial data may have been compromised, as well. The malwa...

[Read more...](#)



[Watching your account being hacked...](#)

Sometimes it happens ... yes, your account is subjected to a hacker attack. And you get a firsthand view of what happens next – the password change requests, notifications or text messages about unautho...

[Read more...](#)

[Threatpost | The first stop for security news](#) The Kaspersky Lab Security News Service  
Categories [Black Hat](#) | [Cloud Security](#) | [Critical Infrastructure](#) | [Cryptography](#) | [Featured](#)  
| [Government](#) | [Hacks](#) | [Malware](#) | [Mobile Security](#) | [Podcasts](#) | [Privacy](#) | [Security](#)  
[Analyst Summit](#) | [Slideshow](#) | [Uncategorized](#) | [Videos](#) | [Vulnerabilities](#) | [Web Security](#)

- [RSS Feeds](#)
- [Home](#)
- [About Us](#)
- [Contact Us](#)

## Authors

[Michael Mimoso](#)  
[Christopher Brook](#)

Copyright © 2016 [Threatpost | The first stop for security news](#)

- | [Terms of Service](#)
- | [Privacy](#)