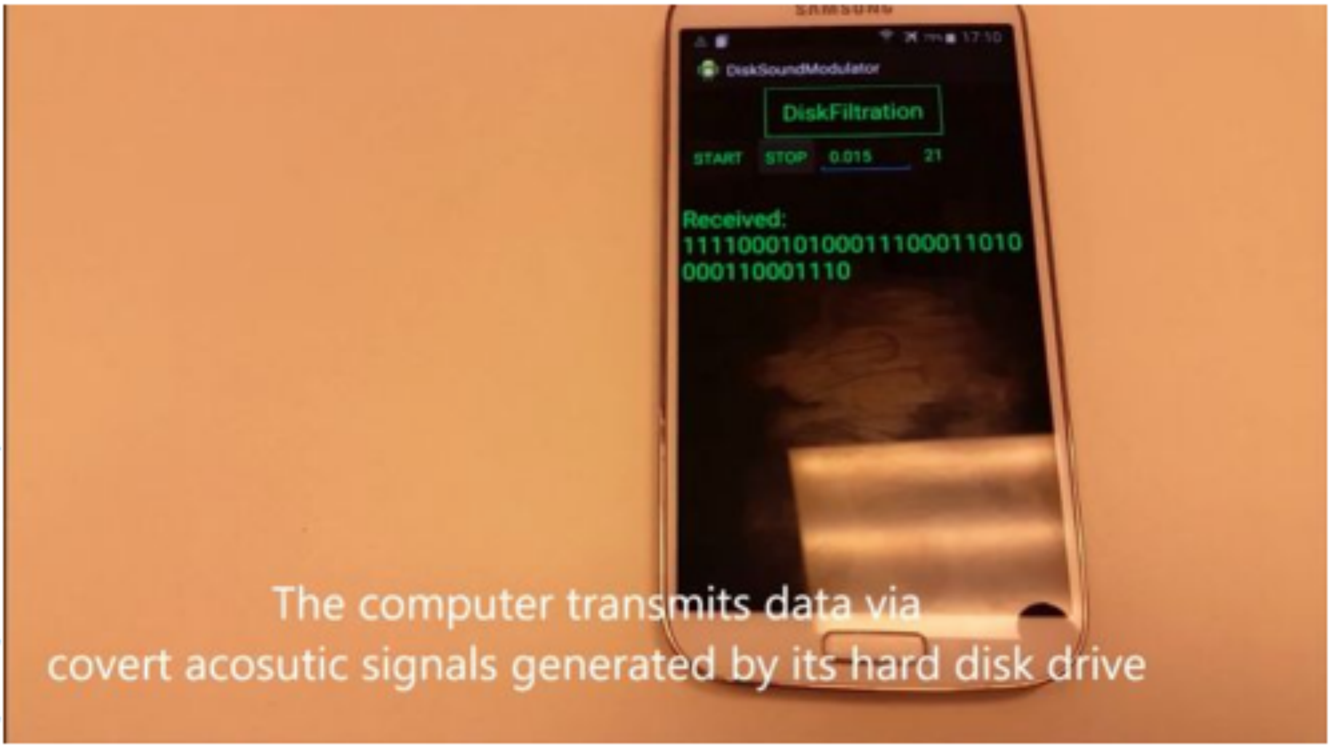
RISK ASSESSMENT —

New air-gap jumper covertly transmits data in hard-drive sounds

"DiskFiltration" siphons data even when computers are disconnected from the Internet.

DAN GOODIN - 8/11/2016, 10:03 PM



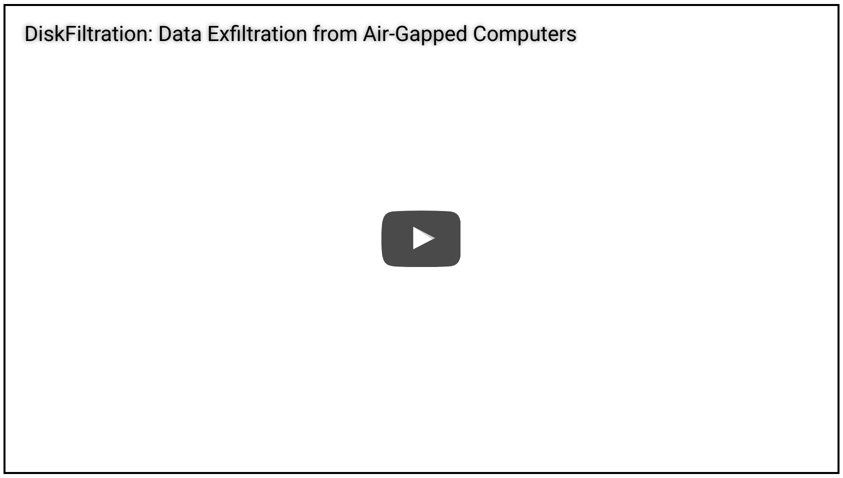
© Cyber Security Labs @ Ben Gurion University

Researchers have devised a new way to siphon data out of an infected computer even when it has been physically disconnected from the Internet to prevent the leakage of sensitive information it stores.

The method has been dubbed "DiskFiltration" by its creators because it uses acoustic signals emitted from the hard drive of the air-gapped computer being targeted. It works by manipulating the movements of the hard drive's actuator, which is the mechanical arm that accesses specific parts of a disk platter so heads attached to the actuator can read or write data. By using so-called seek operations that move the actuator in very specific ways, it can generate sounds that transfer passwords, cryptographic keys, and other sensitive data stored on the computer to a nearby microphone. The technique has a range of six feet and a speed of 180 bits per minute, fast enough to steal a 4,096-bit key in about 25 minutes.

"An air-gap isolation is considered to be a hermetic security measure which can prevent data leakage," Mordechai Guri, a security researcher and the head of research and development in the cyber security labs at Israel's Ben-Gurion University, told Ars. "Confidential data, personal information, financial records and other type of sensitive information is stored within isolated networks. We show that despite the degree of isolation, the data can be exfiltrated (for example, to a nearby smart phone)."

Besides working against air-gapped computers, the covert channel can also be used to steal data from Internet-connected machines whose network traffic is intensively monitored by intrusion prevention devices, data loss prevention systems, and similar security measures. The technique is documented in a technical paper titled DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise, which was published Thursday night. Guri and the other Ben-Gurion University researchers who devised the covert channel created the video demonstration below.



DiskFiltration: Data Exfiltration from Air-Gapped Computers.

DiskFiltration is only the latest method devised by Ben-Gurion University researchers to bridge air gaps. Other techniques include AirHopper, which turns a computer's video card into an FM transmitter; BitWhisper, which relies on the exchange of heat-induced "thermal pings"; GSMem, which relies on cellular frequencies; and Fansmitter, which uses noise emitted by a computer fan to transmit data. In 2013, researchers with Germany's Fraunhofer Institute for Communication, Information Processing, and Ergonomics devised a technique that used inaudible audio signals to covertly transmit keystrokes and other sensitive data from air-gapped machines.

FURTHER READING
Scientist-developed malware prototype covertly jumps air gaps using inaudible sound

The techniques are effective, but their utility in real-world situations is limited. That's because the computers they target still must be infected by malware. If the computers aren't connected to the Internet, the compromise is likely to be extremely difficult and would require the help of a malicious insider, who very well may have easier ways to obtain data stored on the machine. Still, the air-gap jumpers could provide a crucial means to bypass otherwise insurmountable defenses when combined with other techniques in a targeted attack.

Receiving data transmitted by sound generated from a hard drive is generally not efficient. DiskFiltration improves the signal-to-noise ratio by focusing on a narrow range of acoustic frequencies, a feature that effectively strips out background noise. DiskFiltration works even when a hard drive's automatic acoustic management, which reduces acoustic noise, is at its default setting. Still, casual noise emissions from other running processes can sometimes interfere or interrupt the DiskFiltration transmissions.

The most effective way to prevent DiskFiltration-style data exfiltration is to replace hard drives with solid-state drives, since the latter aren't mechanical and generate virtually no noise. Using particularly quiet types of hard drives or installing special types of hard drive enclosures that muffle sound can also be an effective countermeasure. It may also be possible to jam hard-drive signals by generating static noise. Intrusion prevention systems may also be programmed to detect suspicious hard-drive seek patterns used to create the transmissions. Yet another solution is to isolate air-gapped computers from smart phones and other devices with a microphone.

Promoted Comments

Azethoth666 / Ars Tribunus Militum

JUMP TO POST

> Jeremy W wrote:
> So you've got a computer with data valuable enough to require an air gap, or at least some serious outbound data monitoring. You not only allow cellphones near it, but you allow enough access to it that an arbitrary program can be installed and run on it.
>
> You've already failed at the most basic security measures. You deserve to have your data stolen at that point.

By that logic we do not need air gapped computers because apparently there are "basic security measures that prevent offensive software from being on your computer". Just raise some funding for your scheme, you are already a billionaire!

Imagine that cell phones are just one example of an acoustic receiver. Another example would be the entire structure of the embassy the Soviet Union built for us back in the day. Maybe it is a laser picking up the vibrations in a window. Or a tiny drone in a vent. Who knows.

Next, read some of the Snowden revelations and imagine that it is really hard to prevent bad stuff from being on a computer. The NSA tells us they assume their network is compromised and I believe them. The NSA! If your network is compromised how are you creating this miracle clean computer? Did you physically audit all the hardware, somehow without destroying it and somehow verified all code to be correct even though that is hard / impossible? (I am adding the "hard" to cover some trivial code case that can be proven)

As mentioned above, this now mandates SSD use on air gapped computers and I would imagine TEMPEST already covers this as it has dealt with noise for like ever already.

2044 posts | registered 1/20/2011

Statistical / Ars Tribunus Militum / *et Subscriptor*   **JUMP TO POST**

> Jeremy W wrote:
> So you've got a computer with data valuable enough to require an air gap, or at least some serious outbound data monitoring. You not only allow cellphones near it, but you allow enough access to it that an arbitrary program can be installed and run on it.
>
> You've already failed at the most basic security measures. You deserve to have your data stolen at that point.

https://en.wikipedia.org/wiki/Stuxnet

Stuxnet showed getting something onto an air gapped device isn't impossible if you are willing to spend the resources into making it happen. The challenge with security is the defense has to be perfect and the attacker only has to score once to "win".

I agree it is unlikely these types of exotic attacks are going to be useful in the real world but I also think the research is useful. Honestly if two years prior to stuxnet you would have told me the Israelis would infect a good portion of the world's computers with a virus that had a dormant payload just to ensure it would eventually infect the thumb drive of a technician they didn't know working at a plant they didn't have access to so the virus could release the dormant payload without any outside command and control causing the controller to spin centrifuges beyond their design tolerances and destroy them ... well I would have said "cool scifi you should write a techno spy thriller".

7084 posts | registered 9/27/2010

CanadianLibertarian / Smack-Fu Master, in training / *et Subscriptor*   **JUMP TO POST**

> Statistical wrote:
>> Jeremy W wrote:
>> So you've got a computer with data valuable enough to require an air gap, or at least some serious outbound data monitoring. You not only allow cellphones near it, but you allow enough access to it that an arbitrary program can be installed and run on it.
>>
>> You've already failed at the most basic security measures. You deserve to have your data stolen at that point.
>
> https://en.wikipedia.org/wiki/Stuxnet
>
> Stuxnet showed getting something onto an air gapped device isn't impossible if you are willing to spend the resources into making it happen. The challenge with security is the defense has to be perfect and the attacker only has to score once to "win".
>
> I agree it is unlikely these types of exotic attacks are going to be useful in the real world but I also think the research is useful. Honestly if two years prior to stuxnet you would have told me the Israelis would infect a good portion of the world's computers with a virus that had a dormant payload just to ensure it would eventually infect the thumb drive of a technician they didn't know working at a plant they didn't have access to so the virus could release the dormant payload without any outside command and control causing the controller to spin centrifuges beyond their design tolerances and destroy them ... well I would have said "cool scifi you should write a techno spy thriller".

I'm guessing you mean useful on a mass level or for lay people? I don't think the average Joe needs to worry about this type of attack ever being used on them, but I can certainly see it being one of many possible attack vectors being employed on a high-value target.

Just the other day, we read about modular malware, where the creators can seemingly use any array of modules to get access to the data they want. This could simply be one module of many to use when a high-value target computer is compromised.

https://arstechnica.com/security/2016/0 ... r-5-years/

It's potential utility is for high-value targets, which most of us will never have to worry about.

21 posts | registered 7/12/2016

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 73

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS