Security

25

'Adversarial DNA' breeds buffer overflow bugs in PCs

Boffins had to break gene-reading software but were able to remotely exploit a computer

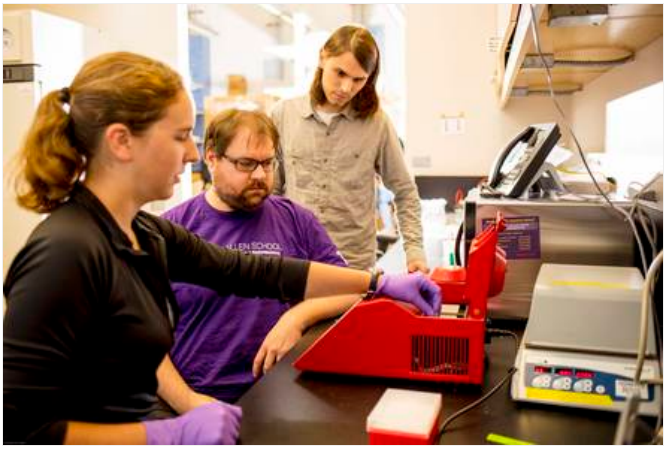
By Simon Sharwood and Andrew Silver 11 Aug 2017 at 03:57 SHARE ▼

Scientists from the University of Washington have created synthetic DNA that produced malware of a sort.

Detailed in a paper titled “Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More”, the authors explain that they decided to “synthesize DNA strands that, after sequencing and post-processing, generated a file; when used as input into a vulnerable program, this file yielded an open socket for remote control.”

Lead author computer scientist Tadayoshi Kohno admits that malware-laced DNA isn't a realistic threat, but suggests there's "potential" in the future for it to be used by hackers planning to steal developing drug IP or ransom off sensitive genomic data.

"It's important to understand the security risks before they manifest," Kohno told *The Register*. "There aren't bad guys knocking at the door to compromise the software systems developed by this community."



From left, Lee Organick, Karl Koscher and Peter Ney prepare the DNA exploit for sequencing. Credit: Dennis Wise/University of Washington

To make it work, the authors got their hands on the source code of open-source DNA compressor `fqzcomp` and “inserted a vulnerability into version 4.6 of its source code; a function that processes and compresses DNA reads individually, using a fixed-size buffer to store the compressed data.”

Biologists use fqzcomp to compress digital files containing strings of A, C, T, G. A simple computer command was translated into 176 DNA letters and, after ordering copies of this DNA from a vendor, the researchers fed it to a sequencing machine. After some processing, this digital file is fed

Most read


Salesforce sacks two top security engineers for their DEF CON talk


Revealed: The naughty tricks used by web ads to bypass blockers


Can GCHQ order techies to work as govt snoops? Experts fear: 'Yes'


Hell desk to user: 'I know you're wrong. I wrote the software. And the protocol it runs on'


So you're thinking about becoming an illegal hacker – what's your business plan?

to the compression program.

They manually modified the code to decrease the size of the DNA sequence input it was expecting, allowing the command in the DNA to spill over (a buffer overflow attack) and execute a program connected to a remote server with complete control over the machine. About 37.4 per cent of all reads ended up pulling off the buffer overflow.

Readers may at this point think that it's pretty easy to break software when you feed it data that you know in advance will cause it problems. The researchers recognise this, writing that they know their crocked code is “in many ways the 'best possible' environment for an adversary.”

But they also note that “`fqzcomp` already contains over two dozen static buffers. Our modifications added 54 lines of C++ code and deleted 127 lines from `fqzcomp`.” *The Register* imagines that kind of modification could go unnoticed in many-a-lab.

For example, the researchers also evaluated 13 open-source programs for DNA processing and found the same kind of insecurities.

But the paper also points out that synthesising any DNA, never mind stuff designed to disrupt bioinformatics software, is hard and prone to error. Even if you can do the job, you need to get the right sample into the right lab, and need to know what software that lab is running. Or get malformed software into that lab.

All of which is hard. But so was getting Stuxnet across an air-gap into an Iranian centrifuge.

Pass the password

Yaniv Erlich, a computer scientist at Columbia University in New York City who has studied DNA storage but was not involved in the study, told *The Register* that the exploit "is basically unrealistic". He says a hacker would have to precisely time the DNA exploit to when a sequencing center runs a new compression tech with longer reads for the very first time, but any centre would "rigorously test" a pipeline when any new tech arrives "so short buffers are likely to be detected ahead of time."

He said he's more worried about academic centres using default passwords on their internet-connected DNA sequencers, which could be targets for ransomware.

But Christophe Dessimoz, a computational biologist at University of Lausanne in Switzerland who was also not involved in the study but has studied DNA storage, told *The Register* that the authors are correct that the "general security hygiene of bioinformatics programs is very low".

"Current tools have been developed to handle natural DNA sequences, which are not expected to contain code executable by computers," he added. Although not surprising, "The work is a nifty stunt."

Someone needs to be thinking about security in the DNA sequencing ecosystem

The authors' main recommendation is that bioinformatics software just hasn't been written with this kind of attack in mind, but seeing as DNA is information encoded in chemicals the authors of such software should wise up to the risks they've demonstrated.

Kohno, who is next studying regulations around DNA sequencing and analysis pipelines, believes it's possible there are other exploits that

could take advantage of DNA. He said that while some researchers might not find it surprising now, "hindsight is always 2020".

You can find the paper here [PDF] and the University's explainer and FAQ here. The team will present their peer-reviewed research at next week's annual USENIX Security Symposium in Vancouver, British Columbia, Canada

The second document tries hard to point out that this is all theoretical. “We have no evidence to believe that the security of DNA sequencing or DNA data in general is currently under attack,” the primer says. “Instead, we view these results as a first step toward thinking about computer security in the DNA sequencing ecosystem.” ®

Bootnote

Here, the University of Washington's interdisciplinary team of biologists, computer security and DNA processing pipeline experts used synthetic DNA to take down a system. But is it possible that natural human DNA could also accidentally take down a biological research computer system someday?

We asked some of the researchers if it would be possible.

They thought about it and said it's "unlikely"...

Tips and corrections 25 Comments

MORE Malware Dna

collared by FBI on way home from DEF CON

UPDATED Chap who stopped malware spread cuffed in Vegas

138 Comments

cache for world+dog

Daaaamn, these exploits are old-school

33 Comments

rallies around suspected banking malware dev

WannaCry ransomware killer due in court August 14

86 Comments

and helpdesk for crims

Lad cuffed after worldwide manhunt leads cops to parents' home in Stockport, UK

23 Comments

Whitepapers

Serving Over 30 Million Mailboxes with Greater Flexibility and Resilience

Comcast Cable is one of the world's largest video, high-speed Internet and phone providers to residential customers and businesses.

How to audit the 5 most important active directory changes

Active Directory is the central identity store and authentication provider for most networks today making it hugely critical to security.

Hewlett Packard Enterprise cloud is at the center of Deutsche Bank's digital transformation

HPE is deploying a range of private and public cloud services to Deutsche Bank as part of a long-term digital transformation project.

BigTwin - The Industry's Highest Performing Twin Multi-Node System

A breakthrough modular multi-node server system that eliminates traditional modular vs rack computing design trade-offs.