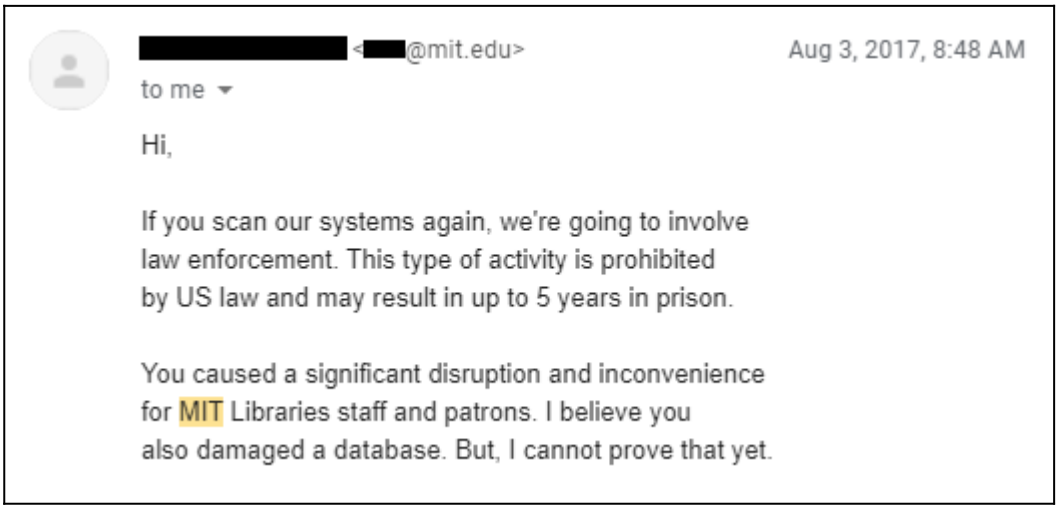
Bill Demirkapi @D4stiny

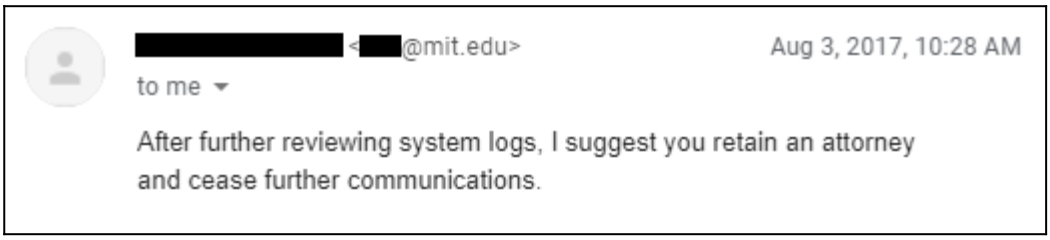
Experience Submitted: Apr 25, 2021, 11:50 PM UTC

https://github.com/disclose/research-threats/issues/27

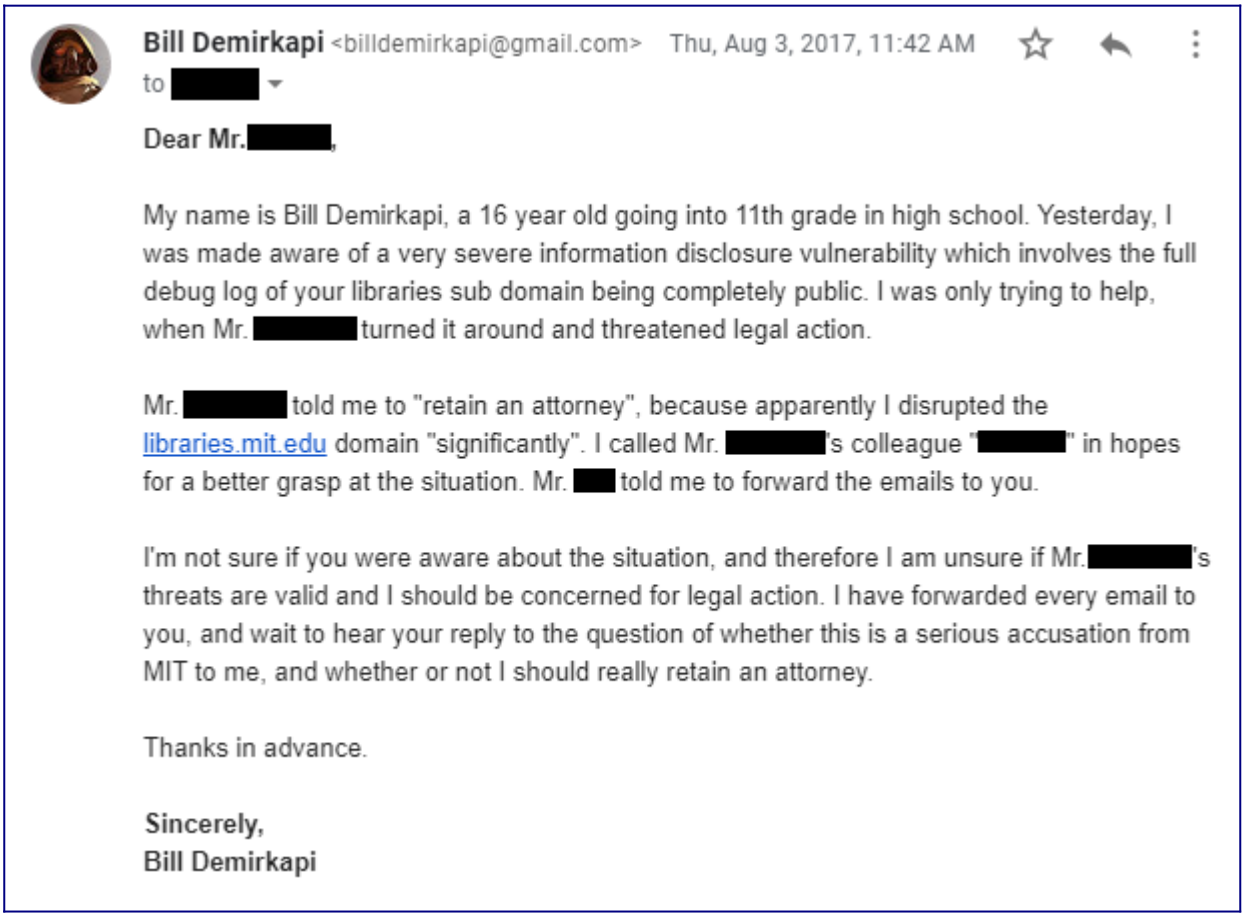
Thought I'd open a new issue regarding my experiences with the Massachusetts Institute of Technology four years ago. I had found an exposed WordPress debug log that had been recording for about a year when I found it (4GB+ of data). All PII has been removed except my own, which is already publicly available.

The legal threat:





My email to the head of MIT's IT department:



Bill Demirkapi <billdemirkapi@gmail.com> Thu, Aug 3, 2017, 11:42 AM

to [redacted]

Dear Mr.[redacted],

My name is Bill Demirkapi, a 16 year old going into 11th grade in high school. Yesterday, I was made aware of a very severe information disclosure vulnerability which involves the full debug log of your libraries sub domain being completely public. I was only trying to help, when Mr. [redacted] turned it around and threatened legal action.

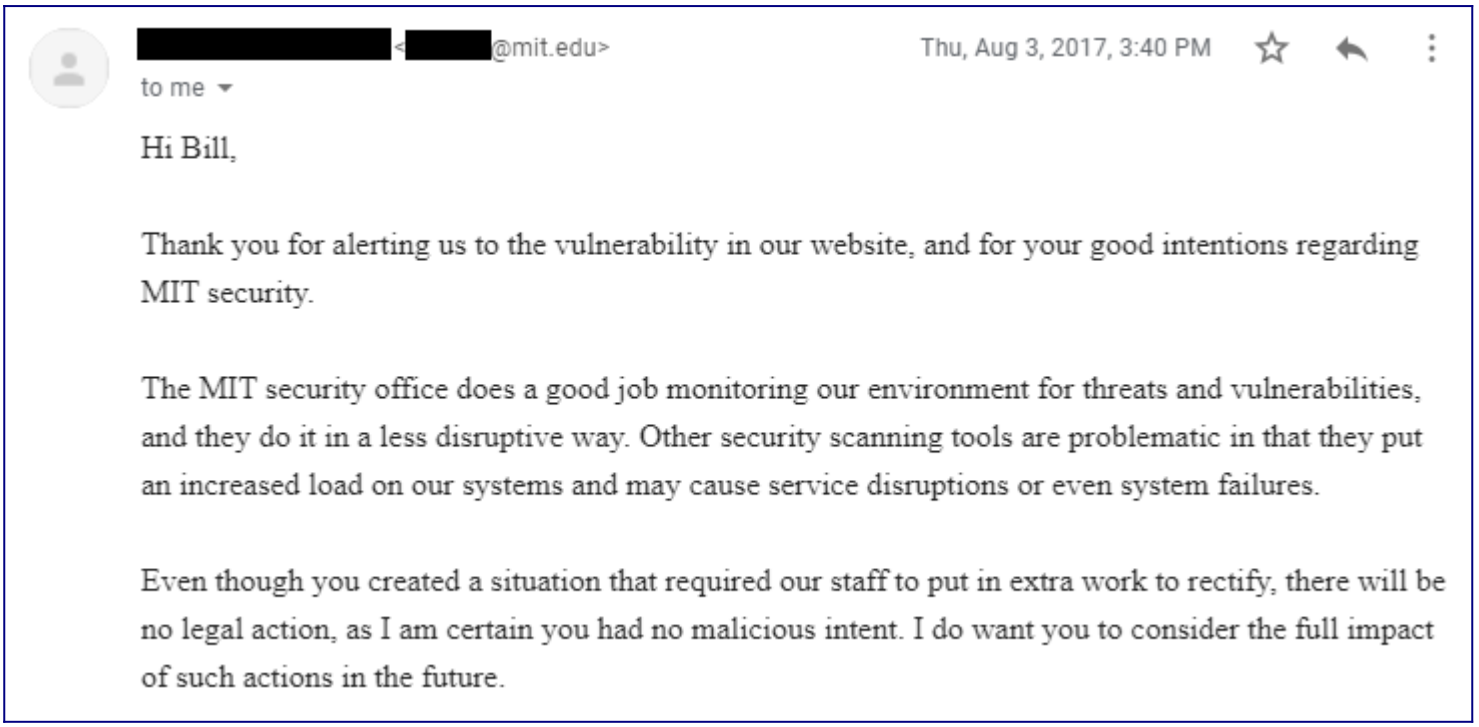
Mr. [redacted] told me to "retain an attorney", because apparently I disrupted the libraries.mit.edu domain "significantly". I called Mr. [redacted]'s colleague "[redacted]" in hopes for a better grasp at the situation. Mr. [redacted] told me to forward the emails to you.

I'm not sure if you were aware about the situation, and therefore I am unsure if Mr.[redacted]'s threats are valid and I should be concerned for legal action. I have forwarded every email to you, and wait to hear your reply to the question of whether this is a serious accusation from MIT to me, and whether or not I should really retain an attorney.

Thanks in advance.

Sincerely,
Bill Demirkapi

MIT's IT Head response:



[redacted] <[redacted]@mit.edu> Thu, Aug 3, 2017, 3:40 PM

to me

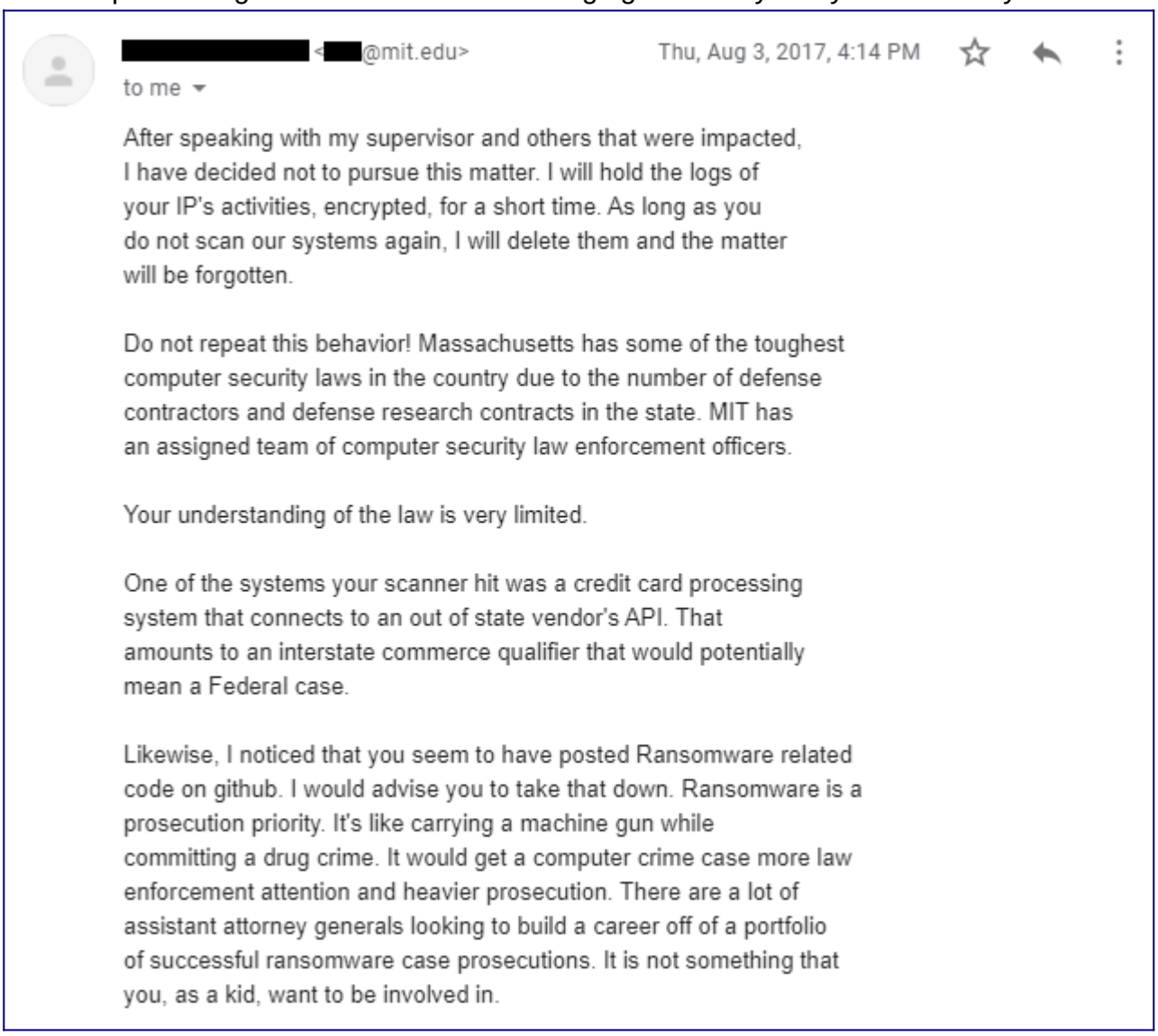
Hi Bill,

Thank you for alerting us to the vulnerability in our website, and for your good intentions regarding MIT security.

The MIT security office does a good job monitoring our environment for threats and vulnerabilities, and they do it in a less disruptive way. Other security scanning tools are problematic in that they put an increased load on our systems and may cause service disruptions or even system failures.

Even though you created a situation that required our staff to put in extra work to rectify, there will be no legal action, as I am certain you had no malicious intent. I do want you to consider the full impact of such actions in the future.

Follow-up from original staff member encouraging that I stay away from security:



[redacted] <[redacted]@mit.edu> Thu, Aug 3, 2017, 4:14 PM

to me

After speaking with my supervisor and others that were impacted, I have decided not to pursue this matter. I will hold the logs of your IP's activities, encrypted, for a short time. As long as you do not scan our systems again, I will delete them and the matter will be forgotten.

Do not repeat this behavior! Massachusetts has some of the toughest computer security laws in the country due to the number of defense contractors and defense research contracts in the state. MIT has an assigned team of computer security law enforcement officers.

Your understanding of the law is very limited.

One of the systems your scanner hit was a credit card processing system that connects to an out of state vendor's API. That amounts to an interstate commerce qualifier that would potentially mean a Federal case.

Likewise, I noticed that you seem to have posted Ransomware related code on github. I would advise you to take that down. Ransomware is a prosecution priority. It's like carrying a machine gun while committing a drug crime. It would get a computer crime case more law enforcement attention and heavier prosecution. There are a lot of assistant attorney generals looking to build a career off of a portfolio of successful ransomware case prosecutions. It is not something that you, as a kid, want to be involved in.

You are headed down the wrong path. If you do get arrested, not even convicted - but just arrested, for some future vulnerability scanning or computer hacking activity it will most likely end any chance for a technology career. Good computer security jobs almost all require a Top Secret Clearance, now. While a felony can fall off a person's record after 7 years and no longer impact regular background checks, that is not the case for a TSC background check. Such a situation would make even programming and administration jobs difficult to acquire.

If you want to build your computer skills, I would advise that you stay away from security and instead learn lower level programming and infrastructure software like web servers and databases. There are open source projects that you can involve yourself such as the Apache Foundation's software projects. IRC and project mailing lists are a good way to learn the capabilities need and opportunities available. After learning low level programming and associated concepts, it is easy to developing meaningful knowledge about security topics and technology in a benign way.

The people in the computer security community performing similar actions to your own are taking measures to protect themselves that you are not. Many, if not most of them, will face much less severe consequences than you would if you were caught breaking computer security related laws as a resident of Massachusetts.