+44 345 094 0945
www.waterstons.com

Article

Aug 2023

Another Day On The Watch: Hacking On The Blue Team

"Mr. Eccles requests that anyone working or hacking on the electrical system turn the power off to avoid blowing a fuse."







"Mr. Eccles requests that anyone working or hacking on the electrical system turn the power off to avoid blowing a fuse."

In our current climate, this quote may have you picturing the morning meeting of a nation state threat group, hell bent on infiltrating the critical infrastructure of another sovereign nation but the reality of it is far more benign. This innocuous memo from Bill Eccles in 1955 to the MIT Tech Model Railroad Club was the birth of the term "Hacker". It wasn't till the 1960s that this term began doing the rounds in computer circles.

Today, hardly a day goes by that the term "hacker" is not in the headlines. The image we conjure up is usually that of a hoodie clad individual dwelling in a dark basement, shaping the world around them with the sheer force of their digital will.

Driven by greed and/or malcontent for a system that has somehow wronged them. While this image is great for selling newspapers and generating clicks and hype while providing a focal point for the faceless digital fear that is coursing through our collective consciousness, in 99% of cases it also couldn't be further from the truth.

I am a hacker, yet you won't see me donning a Guy Fawkes mask, spitting venom and threats at this government or that. You'll never receive a communication from me asking for bitcoin to unencrypt your network or live in fear that I've stolen your identity and am currently sunning myself on a beach in a non-extradition country, courtesy of the loan I've taken out in your name. Yet, a hacker I am.

There is a common misconception when "hackers" are labelled white, grey or black hat, as the skill set is identical. The only differentiation is intent and consent. I HAVE lied to and manipulated people to extract their credentials, breached systems, stolen sensitive data and deployed devastating malware. I HAVE acted on numerous occasions with malicious intent, but the difference is – I have always done so with consent. Only with consent.

Yes, if my life had taken another direction, one could easily imagine me as one of those hoodie-clad basement dwellers, but I have chosen to get up every day and do what I can, with the skillset I have, to make this world a better place. In the cybersecurity industry, this is not a unique tale.

My day starts like many of yours. I wake up, make my wife breakfast in bed, then take the arduous 12-step commute to my office. I check the news feeds and my inboxes for anything that might have occurred during the night and start my day. I work for a global Managed Security Service Provider (MSSP), on the blue team, running their security operations centre, using my knowledge of offensive techniques to better defend our clients and the public at large.

It's a challenging role, with little downtime. The ever-evolving cyber threat landscape and exponentially increasing sophistication of attacks means one needs to be constantly upskilling to face the next challenge, contain the next breach, or help a client recover from a major incident. While you won't see any Hollywood blockbusters featuring Hugh Jackman as a Rockstar SOC analyst, the blue team are the true heroes of cybersecurity. "Attackers only need to be lucky once. Defenders must be lucky all the time."

As it turns out, today has been a more interesting day than most, requiring the team to lean on a wider skill set than would usually be required of a SOC analyst. Part of our day-to-day duties is to triage the constant flow of spam and phishing emails that are received en masse by our clients. Automated tools take care of the majority of the low-hanging fruit; for the rest, we rely on the keen eyes of our analysts. Today, a particularly eagle-eyed end-user picked up something interesting.

The email submitted passed all the checks and balances an email must pass to be deemed legitimate, but like all things, this can be faked. Digging into the content of the email, it explained how the author, a vendor of a building security product, was planning on dropping by the recipient's office to deliver some hardware that needed to be installed. A casual once-over could have missed what could have ended up in a major incident, but fortunately, our offensive Spidey sense started to tingle, and we decided to dig a little deeper.

Initially, it all seemed for naught. The sender legitimately worked at the company he claimed to be from. In fact, he was one of the founders. The investigation would have concluded there if it wasn't for one tiny detail. This gentleman was based in the US, while the recipient was in the UK. Now, while it is possible that he may be swinging by our client in ol' London town, the sender's socials did not reflect the fact that this gentleman was anywhere near the UK. As a precaution, we sent our client an image of the real sender of the email to confirm if and when this meeting was to take place. This is a perfect example of where OSINT or open-source intelligence, a skill set valuable to every facet of cybersecurity, is integral in keeping our clients safe.

Another aspect of our role is to interpret the slew of alerts created by the day-to-day operations of an enterprise network that our automated tools mark as suspicious. A skilled, modern attacker will use seemingly innocuous applications to hide their nefarious actions. Known as living off the land, an attacker will manipulate these well-known applications available on every PC, such as Notepad, Google Chrome, or Microsoft Word, to hopefully slip under the radar.

Today's attacker was not so lucky. Why? Inexperience, probably. A script kiddie. This is the title given to a hacker who uses only pre-made tools with no understanding of what they do. A point and click attacker. These tools are widespread, well-known, and easy for an experienced analyst to detect. Today was such a day.

99% of attacks end this way, with the blue team and the tools at their disposal shutting down attacks before they become an issue, but this is slowly changing due to the AI arms race. While it's true this is happening in a more serious way at the nation-state level, it's also lowering the bar to entry on the cyber-crime front. AI, the proliferation of AI-assisted tools, and tool creation mean that operators with only rudimentary technical skills can unleash relatively sophisticated attacks with little investment in time, talent, or money.

Sometimes it can feel like a game of whack-a-mole, one that much of the public is unaware of, but it's not a thankless job. The cybersecurity community is just that, a community. A collection of like-minded individuals working every day to make this world a better place. Think of us like Castle Black. We are the first and often the last line of digital defence against the unnamed terrors out there, and, as we all know, "Winter is Coming".

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members - 24/7

info@waterstons.com.au | 02 9160 8430