HackBack! Talking with Phineas Fisher

Hacking as Direct Action against the Surveillance State

CrimethInc.

June 5, 2018

Contents

We spoke with the world-famous hacker persona and self-proclaimed anarchist revolutionary Phineas Fisher about the politics behind their attacks on the surveillance industry, the ruling party in Turkey, and the Catalan police. Here follows a retrospective on the exploits of Phineas Fisher, followed by their remarks to us.

Text and interview by BlackBird.

Hacking is often depicted as something technical, a simple matter of attack and defense. Yet motivations are everything. The same technique that builds oppressive tools can be used as a weapon for emancipation. Hacking, in its purest form, is not about engineering: it is about leveraging power dynamics by short-circuiting technology. It is direct action for the new digital world we all live in.

In the shadows of the techno-empire, the hacking scene became a target for cooptation and infiltration. But the underground cannot be eradicated: from time to time, a new action breaks through the surface. Some of the hackers we admire are coders who produce tools for online privacy and anonymity. Other crews create and distribute alternative media. And then there are those who hack back.

The Lost Hacker Circles

It is no secret, for anyone paying attention, that for a long time the hacker underground was also taking sides in the ongoing war. Yet the effervescence that characterized the underground DIY scene of the past few decades has died down, or at least receded to less visible places.

Pessimists mourned the death of hacker communities in a proliferation of individual desertions. It is true that the techno-military complex succeeded in swelling the ranks of the mercenaries: there is a price at which a particular mindset can be bought, whether with money, success, the feeling of power, or the excitement of playing with fancy toys while chasing what state propaganda labels "the enemy."

The underground sought to multiply zones of opacity and resistance, while public perception shifted towards normalizing the relationship between the hacker attitude and technology. Hackers were no longer seen as rebel teenagers producing chaos in a casual game (as depicted by movies from the eighties or nineties like *War Games* or *Hackers*), but as a highly specialized unit of the military occupation forces—or else as their comic-book-level villain counterparts. In the most depoliticized version, the term "hacker" is understood as just another name for the capitalist entrepreneur, a myth you can find in the "hackerspaces" of any gentrified city.

The surveillance industry was so proud of its business that it did not bother concealing it. Representatives of the armed forces and vendors of spy programs showed up regularly at hacker community events, openly recruiting talent. Commercial videos pitching "offensive security" tactics circulated openly, selling products to intelligence agencies, corporations, and governments.

It's an old story: states buy legitimacy in the eyes of the public by portraying themselves as fighting the kinds of crime very few dare to discuss—child pornography, human trafficking, international terrorism. But as soon as they have the surveillance weapons in their arsenals, they direct these weapons against the entire population.

In the middle of this ongoing cooptation of the hacker world, the surveillance complex experienced an important yet invisible blow. An individual—or perhaps a group—fought back by hacking spyware companies and publishing the contents of their secret vaults. When you're fighting an industry that depends on secrecy, publicly disclosing their internal communications and tools can be a very effective strategy.

The GammaGroup Hack

In August 2014, a hack took place against "GammaGroup," an Anglo-German vendor of spy programs. A dump of 40Gb of information followed. After this hack, there were no more secrets about GammaGroup: everything was made public, including their clients, product catalog, price lists, and the programs themselves, along with their training manuals.

The star product of the company, a program named "FinFisher," had been sold to more than 30 government agencies and police forces to spy on journalists, activists, and dissidents. The company had been infecting dissidents in Bahrain and Egypt in the wake of the Arab Spring. They usually used social engineering to trick their targets into installing the software.

A targeted dissident would click on a document attached to an email, or open a link that would install the spyware. From there on, the clients who bought the spyware from the company would have control over the infected computer or cellphone, monitoring microphones, voice and Skype calls, messages, and emails, not to mention continuous location tracking.

Immediately after the hack, someone began tweeting from an account posing as the Gamma PR. The info dump was not enough: a hacker going by PhineasFisher released an old-school text file containing a tutorial with the details of the attack on Gamma:

> "I'm not writing this to brag about what an 31337 h4x0r I am and what m4d sk1llz it took to 0wn Gamma. I'm writing this to demystify hacking, to show how simple it is, and to hopefully inform and inspire you to go out and hack shit… I wanted to show that the Gamma Group hack really was nothing fancy, and that you do have the ability to go out and take similar action."

The name of that phile was "HackBack—A DIY Guide for those without the patience to wait for whistleblowers." For a gravely wounded hacker community, in which the original solidarity, freedom, and open exchange of information was losing ground against the commodification of knowledge by the market and the empire, this action was a breath of fresh air. And—perhaps—the beginning of a movement.

HackedTeam

> "You want more. You have to hack your target. You have to overcome encryption and capture relevant data, being stealth [sic] and untraceable. Exactly what we do."

You can hear these words in the commercial for a product called "Da Vinci," a "remote control system" that was sold worldwide by an Italian company named "Hacking Team."

CrimethInc.
HackBack! Talking with Phineas Fisher
Hacking as Direct Action against the Surveillance State
June 5, 2018

Retrieved on 17th June 2021 from crimethinc.com

theanarchistlibrary.org

Epilogue: Silent Years of Expropriation to Come

Phineas Fisher is dead. It was more than a name: the tip of an underground network of practices and desires. It was not one, but several actions. Cybernetic guerrilla: hit and hide.

However, as anyone who wrote to the hackback email can report, Phineas is still enjoying freedom these days. Engaging in charming conversation, he or she will demonstrate that state does not have absolute control. As he likes to repeat: *it is still possible to attack the system and get away with it.*

Phineas has kept himself busy. He enjoys talking from the shadows about his new occupation. As he told us:

> "Expropriation has some material effects, but it really is an ideological weapon. The rules of this system are not immutable facts, but rules imposed by a minority, and rules that we can question, change, and even break. When someone robs a bank, the State spends huge resources investigating it, not because it makes any economical sense to spend 100k while investigating a 3k robbery, but they spend it because it protects the shared illusion of private property. They try to wipe out that rebel spirit that plays outside of their rules."

He adds:

> "You don't need computer science studies to be able to participate in what the former NSA chief Keith Alexander refers to as responsible for the greatest transfer of wealth in the world's history. In this big project, most of the work is not done by hackers, but by lay people, those who know how to find addresses where to receive post and parcels, how to use a fake ID in a convincing way, and how to use a burner phone. Those are all the skills you need to open a cellphone contract, open bank accounts and ask for loans, make online purchases and receive them. Everyone can learn how to use the Tor Browser and bitcoin, and participate in the darknet markets. Mafia and organized crime acknowledged this change, but anarchists open to illegalism and expropiation did not yet realize that we are not in the pre-internet world anymore, and that there are better tactics than robbing a bank with a gun. We are living an unique moment in history, and we have a great opportunity."

Indeed we do. Long life to hacking, and to all silent expropriations to come.

A company so shamelessly called "Hacking Team" is what results when a local police department approaches two hackers of a mercenary mindset with a request for collaboration. The cybercrime unit of Milan's police force decided that passive monitoring was not enough for their purposes; to fulfill their offensive needs, they asked Alor and Naga, two famous Italian hackers, for help modifying a well-known hacking tool that they had originally authored.

Who their clients were and how they managed to infect and spy on their victims remained a secret until July 5, 2015. That day, the twitter account for the company announced: "As we have nothing to hide, we are publishing all our e-mails, files, and source code," providing links to more than 400 Gigabytes of data. As usual, the company initially claimed that the leak was comprised of false information, but forging such a tremendous amount of data would be an almost impossible feat.

The ones who suspected that the attack had a familiar signature were not wrong: the sarcastic nickname of Phineas Fisher was once again behind the disclosure.

By publishing all the internal information—and, later, another tutorial exploring technical details and political motivations—Phineas Fisher offered the world undeniable evidence about the operations of the 70 customers of Hacking Team. Most of these customers were military, police forces, and federal and provincial governments; the total revenue added up to over 40 million Euros.

This info dump confirmed that there were very good reasons for the global demand for privacy and anonymity. Alongside the Snowden revelations, the ability to peek into HackingTeam's dirty secrets gave us an idea of the magnitude of the campaign of targeted surveillance being carried out by governments and corporations. We know today that there are many other unscrupulous firms profiting from illegal spy operations—such as the Israel-based NSO Group, recently involved in targeted infection of the devices of journalists investigating the Iguala massacre in Mexico, which used base tricks to lure their victims into compromising their own devices.

This anonymous unmasking of HackingTeam was a brilliant operation with global repercussions.

A Market for Secrets

A business like Hacking Team depends on secrecy. To infect their targets, in many of the cases something called a "zero day"[1] is used. A zero day is a vulnerability in a computer program that has not been publicly disclosed yet, which can be exploited by anyone who knows about it to attack computer programs, data, or networks, in many cases offering complete remote control over them. Recently, surveillance capitalism has created a net of companies that act as brokers, buying these vulnerabilities in black and gray markets. The price for a single zero day can range from $10k to $300k or even $1 million.

Spyware companies like Hacking Team "weaponize" these vulnerabilities, gluing several of them together and selling licenses to the forces of repression so they can simply "click and spy," with the added possibility of custom developments for penetrating the systems that belong to chosen victims.

[1] To learn more about software vulnerabilities and government cyberwar, watch the documentary *Zero Days* about the "Stuxnet" affair.

The window of opportunity to take advantage of these "zero days" gets shorter over time. The more you use the knowledge of an unknown vulnerability, the higher the chances that someone will notice the attack and start investigating the holes that allowed it, and the higher the likelihood that other groups will find the same holes. The opportunity to use the vulnerabilities ends when the software in the user's device is patched to fix the errors: this is why it is so important to keep our devices up to date. However, there are cases in which the manufacturers of our devices make the update procedure difficult or even impossible.

Vulnerability brokers and spyware vendors make it possible for technically incompetent people to infect, spy, and exfiltrate data from their targets just by filling forms and clicking around a web application. We saw this when we were able to dissect software like XKeyscore or Hacking Team's Galileo suite.

The irony is that selling dumb-proof spy tools to the cops can give you a false sense of security. Phineas found that the compromised systems were using absolutely lame passwords such as "P4ssword," "wolverine," or "universo." No one is free from the basic rules of operational security!

Hack the Planet! Erdogan and Rojava

Another advantage of cyberspace is that you do not have to travel to attack a target on the other side of the world. You do not even have to get out of bed, although often that is a good idea in order to keep a balanced mind.

"I hacked AKP," Phineas announced in 2016 after having breached the servers of the ruling Turkish party. A dump of more than 100GB of AKP files and emails was passed on to the revolutionary forces in Kurdistan. Phineas had to hurry because Wikileaks published the information before he even finished downloading all the data.

Information is not the only thing that arrived in Kurdistan thanks to hacking actions: Phineas also exploited a vulnerability in the security systems of an undisclosed bank and sent 10,000 euros in bitcoin to Rojava Plan, a group coordinating international solidarity with the autonomous region of Rojava.

Mossos and Scapegoats

In May 2016, after watching the documentary "Ciutat Morta," Phineas thought about trying a simple attack on the Catalan Police Forces. Ciutat Morta is a film about the 4F case, a famous case in the history of the Spanish state in which repressive forces tortured and imprisoned several young people from South America as an act of revenge after a policeman was put into a coma by the impact of a stone following a police charge in downtown Barcelona.

As a result of this new hacking action, using a well-known vulnerability, Phineas defaced the website of the union of the Catalan police with an ironic manifesto declaring that the organization "was refounded as a union in favor of human rights." A data dump with personal details of some 5000 police accounts appeared, along with a 40-minute video tutorial on the techniques used in the hack.

Shortly afterwards, the police carried out several raids on social centers and hacklabs in Barcelona, then claimed to have caught the famous hacker. Only hours later, journalists reported

that the same person had contacted them to say that "he was alive and well" and that the police forces had only imprisoned a scapegoat who happened to have retweeted the info in the dumps.

But Who Is This Phineas Phisher, Really?

One of the most interesting consequences of the Phineas Fisher actions is the look you see in the eyes of your fellow hackers when you discuss the topic with them. Chileans will tell you that Phineas is obviously a Latino. Squatters in Barcelona swear that the tone is familiar. Italians will do the same. US-Americans think she or he speaks like one of them. And then there is the commonsense assumption that, like any good hacker, Phineas must be Russian—one of those Russians who speaks surprisingly good Spanish.

There is indeed something familiar in the actions of this ghost: a deep sense of justice and internationalism, and the feeling that his actions will continue to remain under the radar, because—just as in the past—nobody could believe that a person living an otherwise ordinary life could be the mind behind such deeds.

The truth is, no one cares—except for the cops, who are having a hard time identifying this persona despite all their adversarial modeling paraphernalia and stylistic analysis tools. We don't care about the identity of the person who does these things. It doesn't matter, in the end: when that identity is burned, a new one will appear. Once you ditch the cult of personality, you suddenly gain a lot of freedom.

What we do care about is that, whoever it is, it is one of us, and his actions help us to realize our power.

These direct actions show that, while a lot of effort and dedication might sometimes be needed to cultivate a concrete skillset, most of the time nothing extraordinary is strictly needed. Perhaps you are not particularly technically inclined, but you might be good with people: often, that is the only thing that is needed to pull off an awesome hack. Or you might not come from a technical background, but a determined and playful perseverance can achieve more than any formal training when it comes to making a breach in the realm of cubicle bureaucrats that only care about enforcing policy.

Security is not an absolute quality; there will never be an absolute power in cyberspace. Quoting Phineas: "That's the beauty and asymmetry of hacking: with 100 hours of work, one person can undo years of work by a multi-million dollar company. Hacking gives the underdog a chance to fight and win."

The actions of a humble but motivated hacker can go further than the big, inflated egos of the cyber-security industry, or the academics who do not dare to act outside of the box. It's not always the big hacks that change reality: someone who learns how to stay anonymous, someone who is not afraid and keeps the discipline needed not to leak personal details already has a huge advantage. Not having an ego to feed is also crucial in the business of keeping one's personal freedom.

Eventually, Phineas Fisher went silent. "I killed the accounts because I had nothing else to say." And probably it was enough. Sometimes a little action is all that is needed to shift the collective mood, to render us aware of our own power.