FireEye Intel Center
FireEye, Inc. · Security. Reimagined.
1440 McCarthy Blvd · Milpitas, CA 95035

What Goes Around Comes Around—Hacking Team Becomes the Victim

Date: July 8th, 2015 **Tags:** hacktivisim, italy, disruption-destruction

The eponymously named Italian firm Hacking Team was recently breached, and over the Independence Day holiday saw a massive tranche of internal information released to the public. This incident is a watershed for Hacking Team, and potentially for the entire private hacking industry. The company's response to this latest breach will serve as a guide as to the resiliency and survivability of private surveillance and hacking firms worldwide.

Outing the Spies

On July 5, 2015 details began to surface surrounding the leak of 400GB of data from the private Italian surveillance software firm Hacking Team. In addition to the stolen data, the perpetrators also managed to compromise and deface the company's website and main Twitter account, as well as that of its founder, Christian Pozzi. Privacy and human rights activists have decried the firm's alleged lack of conscience in doing business with countries where dissidents or journalists are tracked down, arrested, and often interrogated. The list of customer countries included Azerbaijan, Ethiopia, Nigeria, Saudi Arabia, Sudan, and the United States.

In the hours and days since the breach, the security community has pored over many of the documents, discovering contracts, product descriptions, pricing information, and troves of internal emails. In his response to news of the company's breach, Pozzi accused the perpetrators of spreading "lies" about his company, and noted his firm was working with law enforcement to identify those responsible. Pozzi's account was later deleted after it too was compromised.

Roughly 11 months prior, another private hacking firm, Gamma International, also had its systems breached and troves of documents leaked to the public. In both cases, the companies were found to be selling their services to authoritarian regimes with poor human rights records in violation of national and international arms embargos. Supporters of increased transparency and regulation of the private surveillance industry have called this latest incident the “equivalent of the Snowden leaks.”

Cyber Mercenaries

Many of the countries that purchased products or services from Hacking Team were small developing nations with authoritarian-style governments. Because they lack either the funding or manpower to develop indigenous cyber capabilities, many of these nations have turned to private suppliers who are happy to provide whatever tools or services these regimes may need to achieve their goals. Other nations that have more open or democratic political systems may use the company’s tools for law enforcement purposes to uncover wrongdoing, rather than to monitor those perceived to be a threat to the state. Luxembourg, Mexico, and the U.S. more likely used Hacking Team’s capabilities to combat money laundering, uncover narcotics trafficking, and investigate terrorism suspects.

While recent history with regard to hacking has largely focused on state sponsored cyber activity, the gaze of both the security community and the public is shifting toward private firms like Gamma International and Hacking Team that operate in a realm practically devoid of regulation or standardization. Several activists have questioned the legality of Hacking Team’s $480,000 of business with the government of Sudan, which is under a UN weapons embargo, and the backlash over allegations of global spying revealed by the Snowden leaks has heightened the public’s sensitivity to any perceived threats to its online freedoms. While private firms will undoubtedly argue that surveillance software does not constitute a weapon, human rights campaigners may see it differently if such software is used to identify and detain suspected dissidents or facilitate the harassment of journalists reporting information counter to regime narratives.

The U.S. Commerce Department is currently debating expanding its arms control regulations, and we could see certain software added to the list. According to the leaked documents, Hacking Team offers its products in the U.S. through two businesses in California and Maryland. The Commerce Department’s ruling could still have an effect on Hacking Team’s offerings to U.S. organizations. A pilfered Excel sheet revealed the Drug Enforcement Agency and Federal Bureau of Investigation to be customers of Hacking Team. Any additions to international arms control regimes would also affect private hacking firms’ operations in many other countries around the world. U.S. campaigners have called for Congressional action to establish acceptable use standards for such software, believing that private firms are capable of—and are currently—operating outside legal guidelines implemented to restrain law enforcement and intelligence organizations.

Is Recovery Possible?

For nations that would have preferred to keep their affiliation with the company a secret, Hacking Team has almost certainly lost their business. The release of such a large trove of information, including source code for malware, stockpiled zero day exploits, passwords, and—most importantly—customer details, has dealt a significant blow to Hacking Team's operations and reputation. Its malware can eventually be reverse-engineered, signatured, and mostly neutralized. The zero days can be patched. With the company's techniques revealed, current and future targets now know how to best protect themselves from surveillance, and in which countries they more likely to face increased scrutiny of their digital lives.

Hacking Team will have to spend significant time and money building new tools and doing its best to win back customers. Hacking Team may never recover if enough of its customers decide too much trust has been destroyed by this breach, coupled with a public and regulatory backlash that could see its products and services more strictly controlled, reducing profit margins.

When the private security services contractor Blackwater encountered public outrage after four of its employees were convicted of criminal acts after killing 17 civilians during a 2007 firefight in Iraq, it rebranded itself several times in order to distance itself from its previous iterations. Hacking Team may find this strategy effective in a market where demand for its services will probably remain strong, but where governments will also be eager to rid themselves of association with a company that has attracted too much negative attention.

Seller's Market

Both the security community and the public will carefully observe how Hacking Team decides to begin to recover from this breach, and whether other private firms also alter their tactics in response. As the viability, favorable cost ratios, and anonymity of cyber activity become more apparent and attractive, nations and groups that cannot afford their own programs will increasingly turn to private firms all too happy to sell their wares at a premium price. If the demand for defensive cyber security services is any guide, private hacking companies may decide the risks are worth the rewards expected from such a booming market. The phenomenon will have come full circle once a private offensive cyber firm hires one specializing in cyber security to prevent such damaging breaches in the future.

FireEye™