Risks of boomerangs a reality in world of cyberwar

June 2 2012, by RICHARD LARDNER

In this Wednesday, Sept. 28, 2011 file photo, a part of the Maroun Petrochemical plant is seen, at the Imam Khomeini port, southwestern Iran. Technicians battling a complex computer virus took the ultimate firewall measures shutting off all Internet links to Iran's oil ministry and the terminal that carries nearly all the country's crude exports. (AP Photo/Vahid Salemi, File)

(AP) — The Obama administration is warning American businesses about an unusually potent computer virus that infected Iran's oil industry even as suspicions persist that the United States is responsible for secretly creating and unleashing cyberweapons against foreign countries.

The government's dual roles of alerting U.S. companies about these threats and producing powerful software weapons and eavesdropping tools underscore the risks of an unintended, online boomerang.

Unlike a bullet or missile fired at an enemy, a cyberweapon that spreads across the Internet may circle back accidentally to infect computers it was never supposed to target. It's one of the unusual challenges facing the programmers who build such weapons, and presidents who must decide when to launch them.

The Homeland Security Department's warning about the new virus, known as "Flame," assured U.S. companies that no infections had been discovered so far inside the U.S. It described Flame as an espionage tool that was sophisticated in design, using encryption and other techniques to help break into computers and move through corporate or private networks. The virus can eavesdrop on data traffic, take screenshots and record audio and keystrokes. The department said the origin is a mystery.

The White House has declined to discuss the virus.

But suspicions about the U.S. government's role in the use of cyberweapons were heightened by a report in Friday's New York Times. Based on anonymous sources, it said President Barack Obama secretly had ordered the use of another sophisticated cyberweapon, known as Stuxnet, to attack the computer systems that run Iran's main nuclear enrichment facilities. The order was an extension of a sabotage program that the Times said began during the Bush administration.

Private security researchers long have suspected that the U.S. and Israeli governments were responsible for Stuxnet. But the newspaper's detailed description of conversations in the Oval Office among Obama, the vice president and the CIA director about the U.S. government's responsibility for Stuxnet is the most direct evidence of this to date. U.S. officials rarely discuss the use of cyberweapons outside of classified settings.

Stuxnet is believed to have been released as early as 2009. It was discovered in June 2010 by a Belarusian antivirus researcher analyzing a customer's infected computer in Iran. It targeted electronic program controllers built by Siemens AG of Germany that were installed in Iran. The U.S. government also circulated warnings to American businesses about Stuxnet after it was detected.

The White House said Friday it would not discuss whether the U.S. was responsible for the Stuxnet attacks on Iran.

"I'm not able to comment on any of the specifics or details," White House spokesman Josh Earnest said. "That information is classified for a reason, and it is kept secret. It is intended not to be publicized because publicizing it would pose a threat to our national security."

Cyberweapons are uncharted territory because the U.S. laws are ambiguous about their use, and questions about their effectiveness and reliability are mostly unresolved. Attackers online can disguise their origins or even impersonate an innocent bystander organization, making it difficult to identify actual targets when responding to attacks.

In this Wednesday, Sept. 28, 2011 file photo, an Iranian security guard stands at the Maroun Petrochemical plant at the Imam Khomeini port, southwestern Iran. Technicians battling a complex computer virus took the ultimate firewall

measures shutting off all Internet links to Iran's oil ministry and the terminal that carries nearly all the country's crude exports. (AP Photo/Vahid Salemi, File)

Viruses and malicious software, known as malware, rely on vulnerabilities in commercial software and hardware products. But it is hard to design a single payload that always will succeed because the target may have fixed a software vulnerability or placed computers behind a firewall.

On the Internet, where being connected is a virtue, an attack intended for one target can spread unexpectedly. Whether a cyberweapon can boomerang depends on its state of the art, according to computer security experts. On that point, there are deep divisions over Flame.

Russian digital security provider Kaspersky Lab, which first identified the virus, said Flame's complexity and functionality "exceed those of all other cybermenaces known to date." There is no doubt, the company said, that a government sponsored the research that developed it. Yet Flame's author remains unknown because there is no information in the code of the virus that would link it to a particular country.

Other experts said it wasn't as fearsome.

Much of the code used to build the virus is old and available on the Internet, said Becky Bace, chief strategist at the Center for Forensics, Information Technology and Security at the University of South Alabama. Flame could have been developed by a small team of smart people who are motivated and have financial backing, she said, making it just as likely a criminal enterprise or a group working as surrogates could have been responsible.

"Here's the wake-up call as far as cyber is concerned: You don't have to be a nation-state to have what it would take to put together a threat of this particular level of sophistication," said Bace, who spent 12 years at the National Security Agency working on intrusion detection and network security. "There's no secret sauce here."

Stuxnet was far more complex.

Still, Stuxnet could not have worked without detailed intelligence about Iran's nuclear program that was obtained through conventional spycraft, said Mikko Hypponen, chief research officer at F-Secure, a digital security company in Helsinki, Finland. The countries with the motivation and the means to gather that data are the United States and Israel, he said.

"This is at the level of complexity that very few organizations in the world would even attempt," said Hypponen, who has studied Stuxnet and Flame. "Basically you have to have moles. Most of what they needed to pull this off was most likely collected with what we would characterize as traditional intelligence work."

The more intricately designed a cyberweapon is, the less likely it will boomerang. Stuxnet spread well beyond the Iranian computer networks it was intended to hit. But the collateral damage was minimal because the virus was developed to go after very specific targets.

"When some of these super sophisticated things spread, it's bad but it may not have the same impact because the virus itself is so complex," said Jacob Olcott, a senior cybersecurity expert at Good Harbor Consulting. "It's designed to only have its impact when it finds certain conditions."

Israel is a world leader in cybertechnology and senior Israeli officials did

little to deflect suspicion about that country's involvement in cyberweapons. "Whoever sees the Iranian threat as a significant threat is likely to take various steps, including these, to hobble it," said Vice Premier Moshe Yaalon, a former military chief and minister of strategic affairs.

A senior defense official involved in Israel's cyberwarfare program said Friday that, "Israel is investing heavily in units that deal with cyberwarfare both for defense and offense." He would not elaborate. The official spoke on condition of anonymity because he is not allowed to speak with the media.

Isaac Ben-Israel, an adviser to Israeli Prime Minister Benjamin Netanyahu on cybersecurity issues, declined Friday to say whether Israel was involved with Stuxnet.

It could take years to know who is responsible, which is what is so unsettling about attacks in cyberspace. "We are very good as an industry at figuring out what a piece of malware does," said Dave Marcus, director of advanced research and threat intelligence at digital security giant McAfee. "But we are less accurate when it comes to saying what group is responsible for it, or it came from this country or that organization."

Copyright 2012 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Risks of boomerangs a reality in world of cyberwar (2012, June 2) retrieved 10 May 2024 from https://phys.org/news/2012-06-boomerangs-reality-world-cyberwar.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.