Researchers aim to thwart targeted cyberattacks

August 13 2014, by Angela Herring

Professor Engin Kirda and his collaborators have developed advanced malware detection software that can protect against targeted attacks, which represent the growing majority of cyberespionage taking place today. Credit: Brooks Canaday.

When it comes to Internet attacks, hackers have traditionally taken a blanket approach, sending out malware to large, random groups of people and hoping that something would stick. But in recent years, the standard operating procedure has shifted.

"In the past we used to see these opportunistic attacks where people get randomly attacked on the Internet," said Northeastern professor Engin Kirda, a cybersecurity expert who holds joint appointments in the College of Computer and Information Science and the Department of Electrical and Computer Engineering. "But lately we've seen organizations and sometimes even countries specifically targeting an organization with the aim of industrial espionage."

In groundbreaking new research to be presented at the top-tier USENIX Security conference this month, Kirda and his collaborators at the Max Plank Institute in Germany and the University of Singapore analyzed what they called targeted, sophisticated attacks via email against a nongovernmental organization in China called the World Uyghur Congress. The WUC represents a large ethnic minority in China and was the victim of several suspected targeted attacks over the course of several years.

What they found was that "the language and subject matter of malicious emails were intricately tailored to appear familiar, normal, or friendly," in which the sender was impersonating someone else to lure the recipient into opening an attachment or URL. As Kirda put it, "all hallmarks of social engineering."

"People started talking about this five, six years ago, but we didn't see a lot of evidence of targeted attacks," said Kirda, who directs Northeastern's Institute for Information Assurance. "Now we're seeing it a lot. So people know these things are happening but in terms of scientific results, there wasn't much out there because it's difficult to get the data."

For their study, the NGO offered to share data directly with the researchers: Two volunteers from the company offered up more than 1,000 suspicious emails that were also sent to a total of more than 700 unique email addresses, including top officials at the organization as well as journalists, politicians, academics, and employees of other NGOs.

In the new research, the team used software developed at Lastine—a security company Kirda co-founded—as well as other techniques to identify some key features of the WUC attacks. They found that social engineering was critical to the attackers' ability to gain access to victims' accounts; the suspicious emails were sent from compromised accounts within the company or sported email addresses that differed from friendly addresses by a single character or two. Most of the messages sent to WUC and others were in the Uyghur language, and about a quarter were in English.

They also discovered that the vectors through which the malware was delivered were most often attached documents, rather than ZIP files or EXE files, which were recently reported as the most common vectors by recent cyberespionage reports. In addition, the malware that was delivered to the victims was found to be quite similar to that used in other recent targeted attacks, rather than representing so-called "zero-day malware," which is malware that has never been observed before.

Kirda noted that standard malware detection software is insufficient for detecting targeted attacks because it looks at the suspicious documents as static entities after they've performed the attack. As a case in point, the research team analyzed the entire body of existing malware detection software for its ability to detect the malicious attachments in the email corpus from WUC. No single software detected all of the malware used in the targeted attacks and some malware evaded all of the software analyzed. Since targeted attacks utilize sophisticated malware that can adapt to its environment, more sophisticated detection techniques must be used instead, Kirda said.

In an effort to address that problem, his team at Lastline developed software that is able to analyze malware "on the fly"—to observe it in action and see if it behaves suspiciously. While more research must be done to broaden the scope, the current work represents an important first step in analyzing the new wave of targeted attacks taking place around the globe.

Understanding such attacks, Kirda said, is critical to developing software capable of protecting against them. Lastline develops technology to defend against today's evasive and advanced cyberthreats.

"It's very important for high-tech universities like Northeastern to have spin-offs because you get the return on investment and you get to see how the real world actually works," Kirda said. "We get data from the company that we can use in our research."

Provided by Northeastern University

Citation: Researchers aim to thwart targeted cyberattacks (2014, August 13) retrieved 26 April 2024 from https://phys.org/news/2014-08-aim-thwart-cyberattacks.html