First technology to detect back-and-forth-type targeted email attacks in real time

January 26 2016

Fujitsu today announced the development of technology that utilizes its artificial intelligence technology to detect targeted email attacks aimed at specific organizations in real time. In recent years, targeted attacks have become more sophisticated, with attackers cleverly camouflaging their contact as a work related matter, then attacking after gaining an employee's trust.

Such an attack makes it difficult to become aware of any suspicious activity. Now, Fujitsu has developed a technology that detects targeted email attacks in real time by detecting suspicious behavior that is different from the normal activity patterns it has learned from the associations found in a collection of operational logs, including users' everyday email habits and the websites they visit before and after using email. With this technology, it is now possible to detect and receive alerts for only those emails that have a high degree of danger, without excessive detection for each suspicious email, even for back-and-forth type targeted email attacks that involve multiple email exchanges between user and attacker. Furthermore, using this technology in tandem with other Fujitsu Laboratories' technologies, security managers can now take proactive countermeasures in response to targeted email attacks, such as temporarily restricting high-risk email and web activities for people targeted by attacks. They can also restrict people and organizations connected to those people from a work-perspective. This technology was developed in part with assistance from the Ministry of Internal Affairs and Communications through the Research and Development Regarding the Detection and Analysis of Cyber Attacks

project.

In recent years, targeted attacks against specific organizations have been increasing in sophistication. The attackers send repeated emails pretending to be customers of the targeted organization, or create traps on websites that users within the organization access frequently, attacking their vulnerabilities and trying to infect them with malware specialized for that organization. In addition, as targeted attacks use emails that are often sent repeatedly to multiple other users within an organization, organizations require ongoing countermeasures.

Targeted attack emails are written so as to be indistinguishable from legitimate inquiries from customers or other related parties, so the malware they use is individually written, and they are difficult for existing spam filters and anti-virus software to detect. It is particularly difficult to respond to exchanges where the attackers carry on emailing and pretending to be customers or other related people for a certain period, building trust before sending an email designed to infect them with malware.

About the Newly Developed Technology

Now, in an industry first, Fujitsu has developed a technology that learns from the associations in a string of operational logs, including users' typical email habits and their website visits before and after using email, and detects suspicious back-and-forth type targeted email attacks in real time. This technology is made up of the two technologies detailed below.

1. Technology that correlates multiple operational user logs, starting with receipt of an email

Fujitsu has developed a technology that correlates a user's unified operational log starting when they receive an email, including receipt of

the email, reading the text of the email, clicking on a URL in the text and accessing the web page in a browser. By correlating operational logs for each person with whom the user exchanges email, including long-term strings of email exchanges and related website access, the system can identify, for example, whether downloads from a particular website occurred in the course of an exchange with a specific person.

2. Real time anomaly detection technology through combined judgement

In order to achieve real time detection of back-and-forth type targeted email attacks in which user and attacker exchange multiple emails, and as the operational log for all of a user's actions over a long period is huge, Fujitsu developed an anomaly detection technology that extracts and combines only the operational log related to a string of emails, compressing it and then learning and comparing it to others to detect anomalies. This can condense the information volume required for anomaly detection to under one-tenth the overall volume, enabling high speed detection processing, even for targeted email attack exchanges that can typically span several days. This machine learning utilizes Fujitsu's proprietary "Human Centric AI Zinrai" technology. These technologies can detect a series of suspicious actions related to a targeted email attack exchange, and exclude unrelated actions, compared with previous technologies that detected individual anomalies in each email or web access. In an experimental testbed, Fujitsu demonstrated that this could reduce the number of events that trigger detection to under one-tenth of previous technologies.

This newly developed technology makes it possible to effectively detect targeted back-and-forth type email attacks from the series of exchanges with a specific person and the related operational log.

Fujitsu has expanded on two other previously developed cyber-attack countermeasure technologies, enabling increased security by combining

them with this newly developed technology.

1. Behavioral characteristic analysis technology: For this technology, which evaluates users' vulnerability to cyber-attacks based on psychological and behavioral characteristics, Fujitsu and Fujitsu Laboratories have added a new IT Risk Dashboard that can display this information in an easy-to-understand format. It can display not only passive risks, such as potential information leaks for individuals and organizations, but also active risks, such as targeted email attacks, as well as display which people have received similar emails.
2. Network detection technology: For this technology, which monitors an organization's internal network and quickly detects malware's concealed activities within a company, Fujitsu and Fujitsu Laboratories have newly connected network sensors, and enabled the precision of monitoring and costs to be adjusted in response to the state of the security risk for each organization.

By combining this newly developed technology with these two other technologies, unusual activity from the initial probes of targeted email attacks can be quickly shared across the organization, enabling preemptive defense with security countermeasures, so that emergency action can be taken for people who receive similar emails, such as restricting access to already received emails, restricting web access, network isolation or strengthened monitoring.

Fujitsu aims to expand the scope of targeted email attacks that can be detected, further improve detection precision, and bring the technology into practical application in fiscal 2016 to counter cyber-attacks and information leaks.

Provided by Fujitsu