Fujitsu develops technology to quickly detect latent malware activity in internal networks

April 16 2014

Figure 1: Choke point monitoring method

Fujitsu Laboratories today announced that it has developed technology that quickly detects latent malware activity in a network. This technology monitors an internal network to protect against advanced persistent threats (APT) on specific companies or individuals, an increasingly common problem.

APT employ malicious programs known as malware which cannot always be detected by ordinary antivirus software, so security measures that protect the entryways to internal networks are limited. In addition, with malware infections, it is often the case that the attackers, through remotely controlled operations that are disguised in the flow of ordinary communications from outside the network, can carry out hidden activities for long periods of time. This makes it difficult to discover the

problem at the exit points of internal networks, such as through unauthorized intrusion-detection systems.

As a method to detect the activity of malware designed to remotely control a terminal, Fujitsu Laboratories focused on the typical communications patterns of latent malware activity within a company's network. The company developed technology to analyze and detect the relationships between multiple communications from outside and within the network. Fujitsu Laboratories then developed technology for the high-speed detection of malware in real time that would work using general-purpose servers. Actual application of this method had been a problematic issue to overcome.

In a connected network of approximately 2000 devices, Fujitsu Laboratories tested and verified that the technology could detect simulated malware activity. This technology makes it possible to quickly detect the latent activity of APT malware in an internal network and protect against data breaches before they occur.

Background

In recent years there has been a surge in increasingly sophisticated APT against specific organizations and individuals for the purpose of stealing information. In APT, the target is thoroughly studied in advance, and the attack is persistently carried out through such methods as email messages disguised as regular business communications. It is not always possible for ordinary antivirus software to distinguish between regular software and software used in an attack, so it is difficult to fully protect an internal network from being infiltrated by malware.

To protect against such sophisticated malware activity, in addition to the conventional security protections used at the entry and exit points of internal networks, it is necessary to employ protection methods that

focus inside internal networks.

Issues

The most common type of malware today is known as a Remote Access Trojan (RAT)(1). With a RAT, the intruder outside a network remotely operates an infected PC within a network to collect internal data, disguising activities as routine business communications such as sending or receiving emails. The RAT infiltrates the network in advance through an email message or other means, but does not immediately begin the processing associated with the attack. Afterwards, when the attack begins, the content of the communications does not contain malware itself, and the traffic associated with the remote operations is almost always encrypted. This activity is difficult to discover using conventional antivirus software or unauthorized intrusion-detection systems.

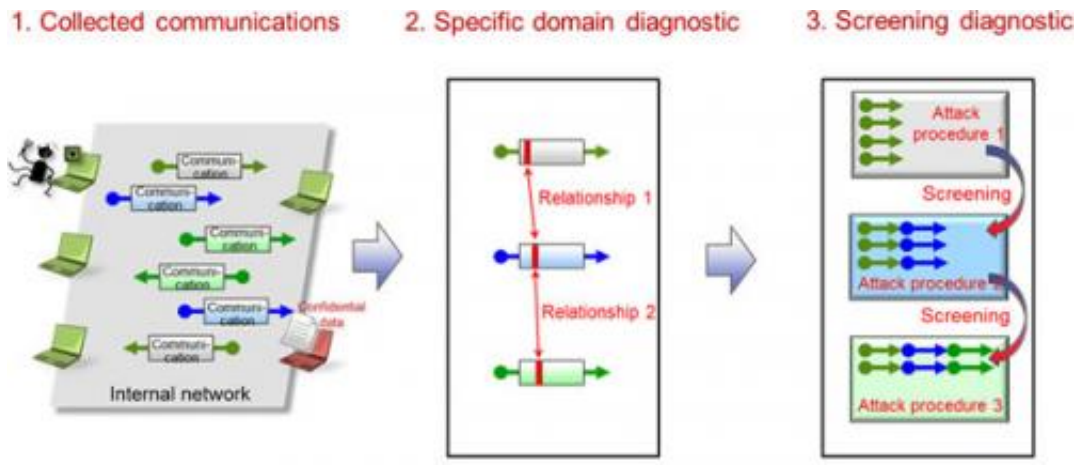

Figure 2: High-speed technology for detecting RAT communication patterns

By analyzing the types of communications flowing over a network and the related communications that precede or follow them, it is possible to

detect latent activity within a network that is characteristic of a RAT, the remote-control type malware. Fujitsu Laboratories conducted research and development on ways to monitor choke points, which are the gateways attackers use in such attacks (Figure 1).

This method, however, requires significant processing time as it is necessary to identify, within a huge stream of work-related traffic, the communications associated with an attack, and then confirm the links between multiple communications. At the same time, to apply this method within a company, it is necessary to configure the detection function to each network domain in the smallest units possible, and, ideally, to use few CPU or memory computing resources.

About the New Technology

By focusing on the communications patterns seen in all latent activity of RATs within an internal network, and by analyzing the relationships between intranet communications, Fujitsu Laboratories developed technology for the high-speed detection of latent activity of RATs within an internal network. This technology enables the choke point monitoring method to be performed at high speeds, and makes it practical to perform with network devices that operate using limited computing resources.

The following two diagnostic technologies were developed to enable the efficient identification of attack-related communications traffic an infected PC sends to its target (Figure 2).

1. Specific domain diagnostic

To determine whether a given communication is associated with an attack, it had been necessary to perform a detailed analysis of the

content of the communication, but now Fujitsu Laboratories has developed a highly precise way to diagnose attack-related communication while reducing the processing load required for analysis. This diagnostic method uses only the relationship between data on the specific domains for multiple communications and the communication sequence.

2. Screening diagnostic

To extract, from an enormous volume of communications, the multiple communications that comprise an attack requires significant processing time. Fujitsu Laboratories has now developed a way to efficiently detect multiple suspicious communications by managing a screening process in which the processing procedures of an attack and communication information are compared in order to screen at each stage of an attack.

The use of these diagnostic technologies enabled an approximately 30-fold increase in the volume of communications that were able to be processed for detection without sacrificing detection performance.

In a connected network environment of approximately 2000 devices on which a large volume of work-related communications was flowing, this technology was verified and evaluated while recreating the latent activity of a RAT. The result was complete detection of the RAT's attack communications, which represented 0.0001% of the overall communication packet volume, with no spillover, even with a Gigabit-class communication line. Moreover, no work-related communications were falsely detected as attack-related communications.

By building this technology into networking equipment and distributively configuring on a local network, it is possible to monitor malicious traffic flowing over a network and detect APT malware, which is difficult to do with firewalls or antivirus software, before data is leaked.

Provided by Fujitsu