October 16, 2024

<Topics>

Raising Alarms: New Method to Conceal Cyberattack

NTT Corporation (hereinafter "NTT") and NTT Security Holdings Corporation (hereinafter "NTT Security") have discovered a new cyberattack method for malware to conceal its malicious behavior and verified it would pose real threats in practical situations. With cyberattacks becoming increasingly sophisticated and difficult to detect, it is important for us defenders to proactively find new threats like this before attackers do and start exploiting them. This research was presented at Black Hat USA 2024 Briefings, which took place from August 7 to August 8, 2024 (*1). The acceptance rate of the conference is around 8%, making it one of the most competitive international conferences focusing on the cybersecurity industry. Our acceptance to this prestigious conference shows the research constitutes a world-class achievement. We will help the community defend against the attack we have discovered by sharing its details with security product/tool developers. We will also strive to protect our customers by timely detecting and responding to the new threat through NTT Group's security services and red teaming campaigns.

- Bytecode Jiu-Jitsu: Choking Interpreters to Force Execution of Malicious Bytecode
  Toshinori Usui (Research Scientist, NTT Security), Yuto Otsuki (Senior Researcher, NTT Security)

Research Results

Code injection is a technique used by malware to hide malicious behavior. Traditionally, code injection has had to go through a specific procedure; It allocates a region with execution permission in a benign process's memory, writes malicious code into the region, and executes the code. Security products have used this distinctive chain of operations as an indicator of code injection.

NTT and NTT Security have discovered in our research a new code injection method that only requires memory write operations, without the need to allocate an execution-permissioned memory region or explicitly start execution of the malicious code. One common way for a computer to execute a program is to first convert the source code into intermediate code and then run it. Our new method blends malicious code into a benign process by overwriting the intermediate code (Figure 1).

Our experiment confirms this method successfully bypasses detection of existing security products. We have shared our findings with the developers of security products and tools and are working together to prepare for the threat.

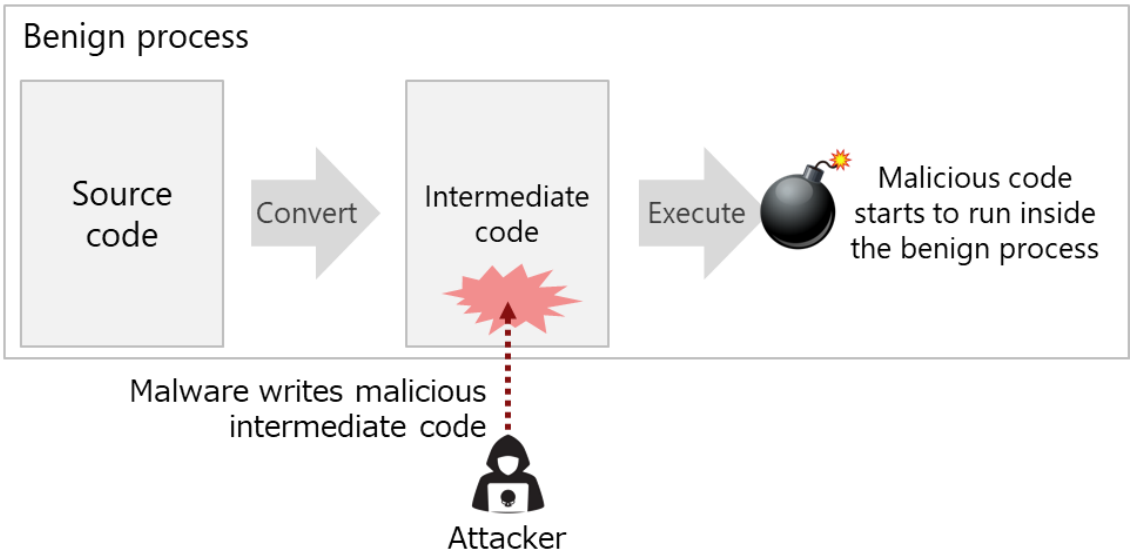

Figure 1　New code injection method

(*1) Toshinori Usui, Yuto Otsuki, Ryo Kubota, Yuhei Kawakoya, Makoto Iwamura, Kanta Matsuura, ”Bytecode Jiu-Jitsu: Choking Interpreters to Force Execution of Malicious Bytecode”, https://blackhat.com/us-24/briefings/schedule/#bytecode-jiu-jitsu-choking-interpreters-to-force-execution-of-malicious-bytecode-38682.

Contact Information

NTT Security Holdings Corporation

makoto.iwamura@security.ntt