Ransomware Deployed by Adversary with Established Foothold

secureworks.com/blog/ransomware-deployed-by-adversary

Counter Threat Unit Research Team

A threat actor deployed ransomware weeks to months after compromising the system.

During February and March of 2016, SecureWorks analysts responded to several ransomware incidents that appear to have been initiated by the same threat group or threat actor. The analysts determined that the infections did not occur from victims clicking a link or opening an email attachment, but rather from a threat actor accessing the infrastructure through an under-managed, Java-based enterprise application platform, performing reconnaissance of the infrastructure, and then purposefully deploying ransomware to a number of systems (typically servers) within the infrastructure.

The adversary initially accessed the infrastructure through the JBoss enterprise application platform. Log analysis revealed use of various versions of the JBoss exploitation tool known as JexBoss. Figure 1 shows one of the first indicators of compromise discovered in the JBoss application logs (in this case, JBoss version 6.1.0). At a later stage of the incident, the threat actor deployed the REGeorg SOCKS proxy.

```
deploy, url=http://www.joaomatosf.com/rnp/jbossass.war
```

Figure 1. JBoss log excerpt showing indicator of compromise. (Source: SecureWorks)

After gaining system access in one of the incidents, the adversary used the mimikatz tool to collect credentials and then used the compromised credentials to log into user accounts and perform additional actions within the infrastructure. The analysts also observed the threat actor creating a user account named “jboss,” which in most cases was a local administrator account on the compromised JBoss system.

In several of the analyzed incidents, the adversary then performed reconnaissance of the infrastructure by downloading, installing, and executing the SystemTools Hyena network scanning tool. Using appropriate credentials, the threat actor could collect information (e.g., installed software, configuration settings, users, groups) from networked systems. The adversary also used Visual Basic scripts (*.vbs files) to download additional tools, as well as batch files to automate a number of rudimentary tasks. For example, one batch file was used to parse a list of system names and ping each with a single packet, creating separate lists for available and unavailable systems.

Once a list of systems is finalized, the adversary uses several tactics to deploy the Samas ransomware. SecureWorks analysts located this ransomware in files named samsam.exe and sqlsrvtmg1.exe. The analysts also found the batch files used to deploy and execute the ransomware, indications that the threat actor used the PsExec remote process execution tool, and artifacts that indicate that the adversary used the Remote Desktop Client to connect to additional systems within the infrastructure.

The victims engaged SecureWorks shortly after files were encrypted because employees could not access data required for their daily work and operations. In all cases, the adversary had initially compromised the JBoss server several weeks or several months before deploying the ransomware. Endpoint security and detection mechanisms such as the SecureWorks Advanced Endpoint Threat Detection (AETD) service might have detected the malicious activity before the threat actors encrypted the files.