Slingshot: the spy that came in from the router

Kaspersky Lab researchers have uncovered a sophisticated threat used for cyber-espionage in the Middle East and Africa from at least 2012 until February 2018. The malware, which researchers have called ‘Slingshot’, attacks and infects victims through compromised routers and can run in kernel mode, giving it complete control over victim devices. According to researchers, many of the techniques used by this threat actor are unique and it is extremely effective at stealthy information gathering, hiding its traffic in marked data packets that it can intercept without trace from everyday communications.

The Slingshot operation was discovered after researchers found a suspicious keylogger program and created a behavioral detection signature to see if that code appeared anywhere else. This triggered a detection that turned out to be an infected computer with a suspicious file inside the system folder named scesrv.dll. The researchers decided to investigate this further. Analysis of the file showed that despite appearing legitimate, the scesrv.dll module had malicious code embedded into it. Since this library is loaded by ‘services.exe’, a process that has system privileges, the poisoned library gained the same rights. The researchers realised that a highly advanced intruder had found its way into the very core of the computer.

The most remarkable thing about Slingshot is probably its unusual attack vector. As researchers uncovered more victims, they found that many seemed to have been initially infected through hacked routers. During these attacks, the group behind Slingshot appears to compromise the routers and place a malicious dynamic link library inside it that is in fact a downloader for other malicious components. When an administrator logs in to configure the router, the router’s management software downloads and runs the malicious module on the administrator’s computer. The method used to hack the routers in the first place remains unknown.

Following infection, Slingshot loads a number of modules onto the victim device, including two huge and powerful ones: Cahnadr, and GollumApp. The two modules are connected and able to support each other in information gathering, persistence and data exfiltration.

Slingshot’s main purpose seems to be cyberespionage. Analysis suggests it collects screenshots, keyboard data, network data, passwords, USB connections, other desktop activity, clipboard data and more, although its kernel access means it can steal whatever it wants.

The advanced, persistent threat also incorporates a number of techniques to help it evade detection: including encrypting all strings in its modules, calling system services directly in order to bypass security-product hooks, using a number of Anti-debugging techniques, and selecting which process to inject depending on the installed and running security solution processes, and more.

Slingshot works as a passive backdoor: it does not have a hardcoded command and control (C&C) address but obtains it from the operator by intercepting all network packages in kernel mode and checking to see if there are two hardcoded magic constants in the header. If this is the case, it means that that package contains the C&C address. After that, Slingshot establishes an encrypted communication channel to the C&C and starts to transmit data for exfiltration over it.

The malicious samples investigated by the researchers were marked as ‘version 6.x’, which suggests the threat has existed for a considerable length of time. The development time, skill and cost involved in creating Slingshot’s complex toolset is likely to have been extremely high. Taken together, these clues suggest that the group behind Slingshot is likely to be highly organized and professional and probably state-sponsored. Text clues in the code suggest it is English-speaking. However, accurate attribution is always hard, if not impossible to determine, and increasingly prone to manipulation and error.

So far, researchers have seen around 100 victims of Slingshot and its related modules, located in Kenya, Yemen, Afghanistan, Libya, Congo, Jordan, Turkey, Iraq, Sudan, Somalia and Tanzania. Most of the victims appear to be targeted individuals rather than organizations, but there are some government organizations and institutions. Kenya and the Yemen account for most of the victims observed so far.

“Slingshot is a sophisticated threat, employing a wide range of tools and techniques, including kernel mode modules that have to date only been seen in the most advanced predators. The functionality is very precious and profitable for the attackers, which could explain why it has been around for at least six years,” said Alexey Shulmin, Lead Malware Analyst, Kaspersky Lab.

All Kaspersky Lab products successfully detect and block this threat.

In order to avoid falling victim to such an attack, Kaspersky Lab researchers recommend implementing the following measures:

Users of Mikrotik routers should upgrade to the latest software version as soon as possible to ensure protection against known vulnerabilities. Further, Mikrotik Winbox no longer downloads anything from the router to the user’s computer.

Use a proven corporate grade security solution in combination with anti-targeted attack technologies and threat intelligence, like Kaspersky Threat Management and Defense solution. These are capable of spotting and catching advanced targeted attacks by analyzing network anomalies and give cybersecurity teams full visibility over the network and response automation;

Provide security staff with access to the latest threat intelligence data, which will arm them with helpful tools for targeted attack research and prevention, such as indicators of compromise (IOC), YARA and customized advanced threat reporting;

If you spot early indicators of a targeted attack, consider managed protection services that will allow you to proactively detect advanced threats, reduce dwell time and arrange timely incident response.

A report on the Slingshot advanced persistent threat can be found on Securelist.com