Chinese-speaking APT Actor Caught Spying on Pharmaceutical Organizations, including Thailand

Kaspersky Lab's researchers have discovered evidence of an emerging and alarming trend: more and more advanced cyber threat actors are turning their attention to attacks against the healthcare sector. The infamous PlugX malware has been detected in pharmaceutical organizations in Vietnam, aimed at stealing precious drug formulas and business information.

PlugX malware is a well-known remote access tool (RAT). It is usually spread via spear phishing and has previously been detected in targeted attacks against the military, government and political organizations. The RAT has been used by a number of Chinese-speaking cyber threat actors, including Deep Panda, NetTraveler or Winnti. In 2013, it was discovered that the latter – responsible for attacking companies in the online gaming industry – had been using PlugX since May 2012. Interestingly, Winnti has also been present in attacks against pharmaceutical companies, where the aim has been to steal digital certificates from medical equipment and software manufacturers.

PlugX RAT allows attackers to perform various malicious operations on a system without the user's permission or authorization, including – but not limited to – copying and modifying files, logging keystrokes, stealing passwords and capturing screenshots of user activity. PlugX, as with other RATs, is used by cyber criminals to discreetly steal and collect sensitive or profitable information for malicious purposes.

RAT usage in attacks against pharmaceutical organizations indicates that sophisticated APT actors are showing an increased interest in capitalizing on the healthcare sector.

Kaspersky Lab products successfully detect and block the PlugX malware.

"Private and confidential healthcare data is steadily migrating from paper to digital form within medical organizations. While the security of the network infrastructure of this sector is sometimes neglected, the hunt by APTs for information on advancements in drug and equipment innovation is truly worrying. Detections of PlugX malware in pharmaceutical organizations demonstrate yet another battle that we need to fight – and win – with cyber criminals," said Yury Namestnikov, security researcher at Kaspersky Lab.

Other key findings for 2017 in the research include:
• More than 60% of medical organizations had malware on their servers or computers;
• Philippines, Venezuela and Thailand topped the list of countries with attacked devices in medical organizations.

In order to stay protected, Kaspersky Lab experts advise businesses to take the following measures:
• Remove all nodes that process medical data from public and secure public web portals;
• Automatically update installed software using patch management systems on all nodes, including servers.
• Perform network segmentation: refrain from connecting expensive equipment to the main LAN of your organization

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

For more recommendations, please visit Securelist.com.

> Connected Medicine and Its Diagnosis

To learn more about PlugX attacks and healthcare cyber security, read our blogpost on Securelist.com.

> Time of death? A therapeutic postmortem of connected medicine