Endpoint Protection

symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware

Oct 14, 2014 12:00 PM

A L Johnson

A coordinated operation involving Symantec and a number of other security companies has delivered a blow against Backdoor.Hikit and a number of other malware tools used by the Chinese-based cyberespionage group Hidden Lynx. Dubbed Operation SMN, this cross-industry collaboration has seen major security vendors share intelligence and resources, resulting in the creation of comprehensive, multi-vendor protection which may significantly blunt the effectiveness of this malware. The organizations involved in this operation include Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Symantec, ThreatConnect, Tenable, ThreatTrack Security, Novetta, and Volexity.

The Hikit back door has been used in cyberespionage attacks against a range of targets in the US, Japan, Taiwan, South Korea, and other regions. Attackers using Hikit have focused their energies against organizations associated with the government, technology, research, defense, and aerospace sectors among other targets.

Operation SMN is the first time a cross-industry group has come together to disrupt an advanced persistent threat (APT) group. Previous collaborations, such as operations against the gangs behind the Gameover Zeus and Shylock Trojans, have usually been focused on cybercriminal gangs.

Coordinated by security firm Novetta under Microsoft's new Coordinated Malware Eradication program, Operation SMN has resulted in a significant amount of intelligence being shared among vendors, leading to the rollout of more effective protection against Hikit and a number of other associated pieces of malware, including one previously unknown malware tool.

Hikit

The main target for this operation was Backdoor.Hikit, a sophisticated and stealthy remote access Trojan (RAT) which has been used in high profile attacks since 2011. Hikit provides the attackers with a back door on the victim's computer. It enables them to download information from the infected computer and upload commands and other malware.

Network-tunneling capabilities allow the threat to create proxies, while an ad-hoc network generation feature allows it to connect multiple compromised computers to create a secondary network. Hikit comes in 32-bit and 64-bit versions, which are deployed depending on the target's infrastructure.

Hikit has been used by at least two Chinese-based APT groups to launch cyberespionage attacks: Hidden Lynx and Pupa (also known as Deep Panda). Whether the groups are related in some way or whether they simply have access to the same malware tools is currently unknown.

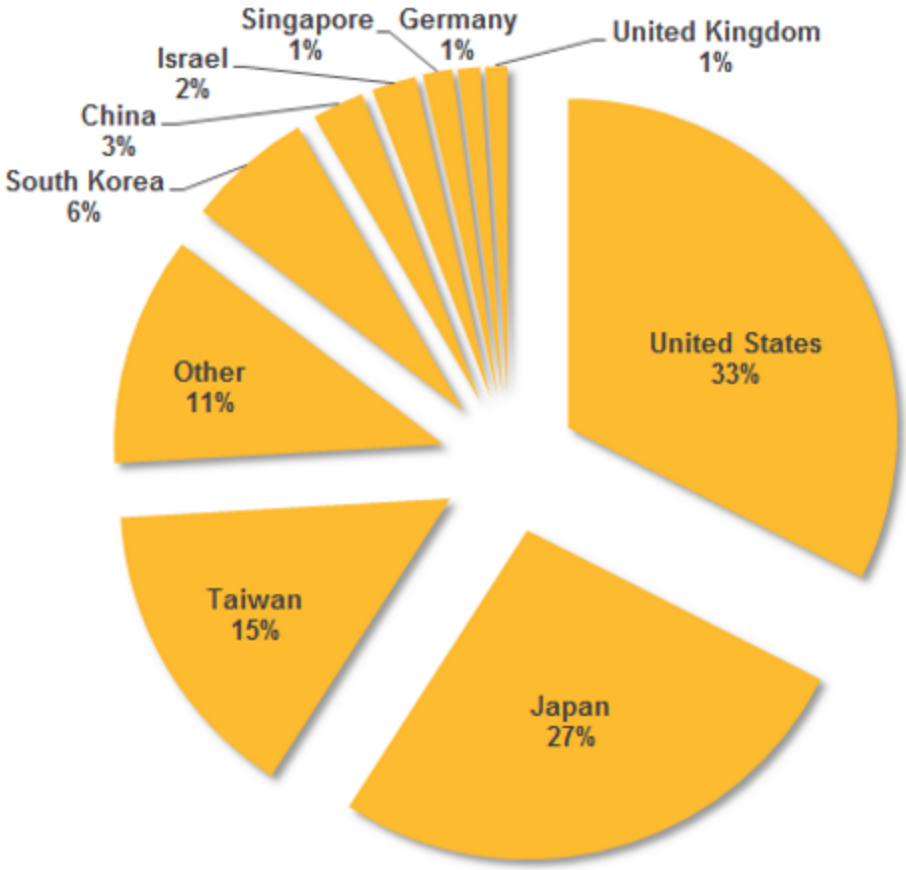

Figure 1. Hikit infections by region

Hidden Lynx

Hidden Lynx, also known in the industry as Aurora, is a highly capable and well-resourced group of attackers that is based in China. The group has a track record of mounting relentless and persistent attacks against a broad range of targets.

Symantec has carried out extensive research on Hidden Lynx and has concluded that the group has between 50 and 100 operatives at its disposal and is capable of carrying out hundreds of simultaneous attacks against diverse targets. Given its broad focus, the group appears to operate as a "hackers for hire"-type operation, mounting attacks on demand as directed by its paymasters.

Hidden Lynx is regarded as one of the pioneers of the “watering-hole” attack method and it appears to have early access to zero-day vulnerabilities. If it cannot mount direct attacks against a target, Hidden Lynx has the capabilities and the patience to work its way up through the supply chain, compromising the security at companies that are suppliers to the target organization and using them a stepping stone towards the ultimate goal.

Hidden Lynx used Hikit during its compromise of Bit9’s trusted file-signing infrastructure in 2012. This attack was then leveraged to mount the VOHO campaign in July 2012 using Bit9-signed malware. The ultimate target of this campaign was US companies whose computers were protected by Bit9. Hikit once again played a key role in this attack campaign.

Since then, Hidden Lynx has continued to use Hikit in its attacks against organizations predominantly in Taiwan, the US, Japan, and South Korea. In 2013, Hidden Lynx underwent a significant re-tooling effort, introducing two new malware tools, Backdoor.Fexel and Backdoor.Gresim, which it continues to use in conjunction with Hikit. Backdoor.Gresim was undiscovered prior to this collaboration effort.

This is the first time that a significant effort to disrupt the activities of an APT has been made. Symantec welcomes the work between industry partners to share intelligence and coordinate efforts to provide the maximum impact against APT groups. Through effective collaboration, we can help ensure that any organization likely to be targeted by these groups will be better protected in the future.

Symantec protection
Symantec has the following detections in place for the malware used in these attacks:

AV

IPS