Backdoor.Winnti attackers have a skeleton in their closet?

New evidence suggests that the skeleton key malware, known as Trojan.Skelky, could be linked to the Backdoor.Winnti malware family.
By: Gavin O GormanSymantec Employee
Created 29 Jan 2015

Contributor: Nikolas Tsapkis

On January 12, 2015, Dell Secureworks blogged about a tool (Trojan.Skelky) that allows attackers to â€œuse a password of their choosing to authenticate as any user.â€ The Skelky (from skeleton key) tool is deployed when an attacker gains access to a victimâ€™s network; the attackers may also utilize other tools and elements in their attack.

Symantec has analyzed Trojan.Skelky and found that it may be linked to the Backdoor.Winnti malware family. The attackers behind the Trojan.Skelky campaign appear to have been using the malware in conjunction with this back door threat. Itâ€™s unclear if the malware family Backdoor.Winnti is used by one attack group or many groups.

During our research, we also found that Trojan.Skelky has been active over the past two years. Within this timeframe, we have seen new variants and a consistent hashed password value.

Where is Trojan.Skelky being used?

Symantec telemetry identified the skeleton key malware on compromised computers in five organizations with offices in the United States and Vietnam. The exact nature and names of the affected organizations is unknown to Symantec. The first activity was seen in January 2013 and until November 2013, there was no further activity involving the skeleton key malware. In November 2013, the attackers increased their usage of the tool and have been active ever since. Four more variants of Trojan.Skelky were discovered as well as additional file names used by the attackers. The complete set of observed file names and hashes are listed as follows

- **msuta64.dll:** 66da7ed621149975f6e643b4f9886cfd
- **ole64.dll:** bf45086e6334f647fda33576e2a05826
- **HookDC64.dll:** bf45086e6334f647fda33576e2a05826
- **HookDC.dll:** a487f1668390df0f4951b7292bae6ecf
- **HookDC.dll:** 8ba4df29b0593be172ff5678d8a05bb3
- **HookDC.dll:** f01026e1107b722435126c53b2af47a9
- **ole64.dll:** f01026e1107b722435126c53b2af47a9
- **olex64.dll:** f01026e1107b722435126c53b2af47a9
- **HookDC64.dll:** f01026e1107b722435126c53b2af47a9
- **ole.dll:** f01026e1107b722435126c53b2af47a9
- **HookDC.dll:** 747cc5ce7f2d062ebec6219384b57e8c
- **ole.dll:** 747cc5ce7f2d062ebec6219384b57e8c

The link between Trojan.Skelky and Backdoor.Winnti
From the first observed use of the tool in January 2013 to the present, the attackers have consistently used the same password. This is the case with three different variants of the tool. The regular use of the same password across multiple variants means itâ€™s likely that only one group of attackers has been using the tool until at least January 2015.

By identifying any other malware active on compromised computers at the same time as Trojan.Skelky, it is possible to learn more about the attackers. There were almost no signs of other malware active at the same time as Skelky in most of the organizations investigated. However, two compromised computers had other malware present, active, and in the same directory, at the same time as Trojan.Skelky.

Two files were discovered on one of the victimâ€™s computers. One file is a variant of Backdoor.Winnti (jqs.exe) and the other is a dropper for Backdoor.Winnti (tmp8296.tmp), which is responsible for creating the Backdoor.Winnti sample. Details on the file names and hashes are as follows:

- **jqs.exe (Backdoor.Winnti dropper):** 600b604784594e3339776c6563aa45a1
- **tmp8296.tmp (Backdoor.Winnti variant):** 48377c1c4cfedebe35733e9c3675f9be

Backdoor.Winnti has been used in the past in a number of different campaigns, most notably against Asian games companies. Given the disparate nature of some victims, itâ€™s unclear if the malware is used by one set of attackers, or many. Symantec is continuing its investigation into this malware familyBackdoor.Winnti and the specific actors behind the combined use of Backdoor.Winnti and Trojan.Skelky.

Symantec and Norton protection
Symantec and Norton products have the following protections against the skeleton key malware:

AV

- Trojan.Skelky

Customers with Behaviour-Based Protection enabled are protected with the signature SONAR.Module!gen3.