List of Malicious Samples used in Bee Master: Detecting Host-Based Code Injection Attacks

Thomas Barabosch, Sebastian Eschweiler, Elmar Gerhards-Padilla

Fraunhofer FKIE,
Friedrich-Ebert-Allee 144, 53113 Bonn, Germany
{firstname.lastname}@fkie.fraunhofer.de
www.fkie.fraunhofer.de

This document contains information about the malware samples considered in the evaluation section of the publication *Bee Master: Detecting Host-Based Code Injection Attacks*[1]. All malware families are listed in Table 1. In case we had to pick more than one representative due to compatibility reasons or we could not execute any sample of the mentioned family we explicitly state which sample has been used on what platform. Otherwise the listed sample works on all platforms. Furthermore, we use the labels provided by Microsoft Security Essentials[2] in order to be consistent. Unfortunately, there are few families where we could not determine a Microsoft specific label. These cases are explicitly marked.

Malware family	**MD5 hash**
Bamital	Windows XP/7: b72eae1db843005fb303dc96c4e98593
Bebloh	79ba32519af63486facaa262d88ee4ea
Caphaw	9466be80af54640218fce4351cc19a41
Carberp	02e693a4a66c104541dec55f417d29b9
Citadel	699e84682acdf3304fc79014e30eb11f
Conficker	Windows XP/7: 8c9367b7dc43dadaa3ec9da767c586cf
Cridex	3d919e36029cc92724a7b9915abd8075
Dorkbot	74c7725c2df337cf860990660d63520f
Eyestye	Windows XP/7: 34bd32ff879c86b48e8eaf4d0cfebc8c Windows 8: 02ea29c0b04725f9b9936129de127133
Feodo[1]	557597074df3d3ce0e1674285ef19732
Foidan	991327984cc14474ad4e863a2543bad9
Gamker	Windows XP/7: c9197f34d616b46074509b4827c85675
Gapz[2]	089c5446291c9145ad8ac6c1cdfe4928
Gataka	8d000237aeb45310951185ea895d85ed
Hanthie	Linux: 761b6266c5254513bc1509d0a36becbd
Hesperbot	12bb85fafd5826fb988c2bee03175632
Ice IX[3]	Windows XP/7: e661ff3d8ae16ab40b8638b8a74fff2b
Lolyda	Windows XP: 6f9fc55fc5323704d464794b25dc8a56 Windows 7/8: 235b650a98740db60fefe05a427eda74
Napolar	5418869ee4700f3893ba067109b3bd2e
Neurevt	48048cfbf579c73b9587333d8768c282

Nymaim	628ba5d2ed6ca6df41863057641047ae
Parite	3689dd289c6c00cc6586bb354f8f2530
Poison	Windows XP: 1ab647cd1c08e542d0cf922b3c8432d0
Ramnit	72a792e3d044dbe3db66971501c268b1
Redyms	0044d66e4abf7c4af6b5d207065320f7
Rombrast	Windows XP: dcc8d837dbb6cbfdb49270acf9274e3f Windows 7/8: 33edb276c62afe4aba1f4f1907818135
Sality	5e4f1f1aa595c354413090e172e8fd91
Sazoora[2]	dce968bdae6f1a0ee29046e439b24cd6
Shiotob	01cc26be43086375ff6e6f95318b78b0
Sinowal	007799fc41bc1fb39ff8cff8cb3478b2
Skynet[3]	191b26bafdf58397088c88a1b3bac5a6
Sykipot[1]	Windows XP/7: 4960dd192384469129f0a1bcd2b5ae83
Tinba	6244604b4fe75b652c05a217ac90eeac
Trxa	2a41db8710f165c98f5717818ff3d7be
Ursnif	01ab2ed9e551a9a40c426a826a5a0c9b
Vawtrak	7b05cc5f48c389a53a42ca1a8e4b2957
Virut	ef15ddfb52c443dd2e4698115c4f1a69
Zbot	Windows XP/7: ab0587cd3872e14e3dfbf2503a34e42c Windows 8: 0c5df80b23b7712bc39655d79549b0b4
ZeusP2P[3]	203f031a7d41fb247d0bd55bb8b1f382

Table 1: Representatives of malware families

References

1. Thomas Barabosch, Sebastian Eschweiler, and Elmar Gehards-Padilla. Bee master: Detecting host-based code injection attacks. In *Detection of Intrusions and Malware, and Vulnerability Assessment: 11th International Conference, DIMVA 2014 Egham, England, July, 2014 Proceedings*. Springer, 2014.
2. Microsoft. Microsoft security essentials. `http://windows.microsoft.com/en-us/windows/security-essentials-download`, Last access: April 8, 2014.
3. Trend Micro Incorporated. `http://www.trendmicro.com`, Last access: April 8, 2014.
4. ESET. Eset nod32 antivirus. `www.eset.com/nod32`, Last access: April 8, 2014.

[1] TrendMicro[3]
[2] Eset-Nod32[4]
[3] Zbot derivative, AV vendors commonly assign a Zbot generic label