Análise Estática do Malware Win32.Neshta

Foram analisadas 3 samples do malware Win32.Neshta, das quais, uma era referente à variante A, e outras duas referentes a uma outra variante, a qual pode ser tanto a Win32.Neshta.B ou Win32.Neshta.C, havendo certa discrepância entre as detecções das principais empresas de antivírus(resultados do VirusTotal) sobre qual a verdadeira variante. As samples estão disponíveis no repositório VirusShare e podem ser adquiridas através de uma busca pelos seus hashes.

Virus.Win32.Neshta.a (Kaspersky)

MD5: 221D1F6BF081E4A3E8A4172BBC3F5AEB

SHA1: 44D3AF57B680AAE7D47AB19EBF1740BE1E9C1AE2

SHA 256: A1B2BD603D533A783F9C8122E6951A1D445196DFA2E8FAE6C2385F52F3A6E38A

* Tipo de arquivo: Portable Executable;
* Origem provável: Bielorrússia;
* Linguagem em que foi desenvolvido: Delphi;
* Não comprimido;
* Entropia: 6.30219;
* Há 8 arquivos de seções que compõem esse malware;
* As strings características estão na seção de recurso, enquanto as strings relacionadas às chamadas de funções estão presentes, obviamente, na import data section;
* Arquitetura I386;
* Possui 41,472 bytes.

Strings características:

Tipo: ascii, tamanho:64 bytes, endereço extado da string no arquivo: 0x0000A1A8

*! Best regards 2 Tommy Salo. [Nov-2005] yours [Dziadulja Apanas]*

Tipo: ascii, tamanho: 68 bytes, endereço exato da string no arquivo: 0x0000A0E0

*Delphi-the best. Fuck off all the rest. Neshta 1.0 Made in Belarus.*

Funções suspeitas utilizadas:

*GetCurrentThreadId* Retorna o identificador da thread requisitada.

*WriteFile* Escreve dados em um arquivo.(Função extremamente importante para o funcionamento do malware, dada a sua natureza de infestador de arquivos .EXE)

*RaiseException*

*GetKeyboardType* Essa função retorna o tipo de teclado pela região. (Estaticamente, não é possível concluir se a chamada dessa função tem o fim de roubar informações ou de criar exceções no próprio malware, para evitar a infecção em certos usuários que utilizem algum tipo de teclado definido, como o russo, por exemplo.)

*ShellExecuteA* Faz operações sobre um arquivo