VirusImmune

http://twitter.com/virusimmune
contato@infovirus.com.br

Malware da NSA encontrado

A empresa de segurança de dados VirusImmune (www.virusimmune.com.br) anuncia a descoberta de três exemplares de malware da NSA (National Security Agency), direcionados exclusivamente ao governo brasileiro e empresas do Brasil:

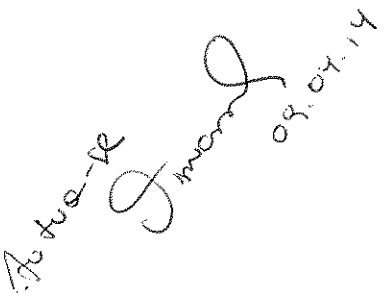
O funcionamento entre eles é muito semelhante e grande parte do código é comum, o que comprova que foram criados pela mesma pessoa ou grupo.

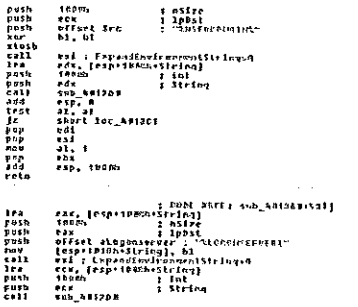
A seguir alguns detalhes:

Informações	Exemplar 1	Exemplar 2	Exemplar 3
MD5	(Disponível para parceiros)	(Disponível para parceiros)	(Disponível para parceiros)
Tamanho do arquivo (em bytes)	102.400	172.032	45.056
Inicialização automática?	Não	Não	Não
Ícone	Não	Não	Não
Possui resources?	Não	Não	Não
Assinatura digital?	Não	Não	Não
Compactado?	Não	Não	Não
Strings criptografadas?	Sim	Sim	Sim
Data de compilação	09/05/2012	10/07/2012	01/08/2012
Leitura do Domínio/Workgroup	petr, org, gov, br	petr, org, gov, br	petr, ong, org, gov, br
Arquivos que captura	*.doc*, *.ppt*, *.xls*, pass*.*, *senha*.*	*.doc*, *.ppt*, *.xls*, *pass*.*, *senha*.*	-
Método de envio dos arquivos	e-mail para NIASC@nsa.gov via porta 587 (email autenticado) Senha do email: ******** (Disponível para parceiros)	POST para um site na Ásia	Grava dados em um arquivo criptografado: %WINDIR%\windowsupdatereport.log
Keylogger	Não	Não	Sim

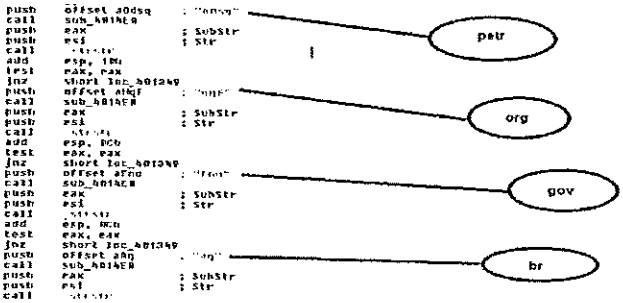
Funcionamento:

- Ao iniciar, o malware tenta ler o conteúdo das variáveis de ambiente: USERDOMAIN e LOGONSERVER, para tentar obter o nome do domínio e/ou workgroup:



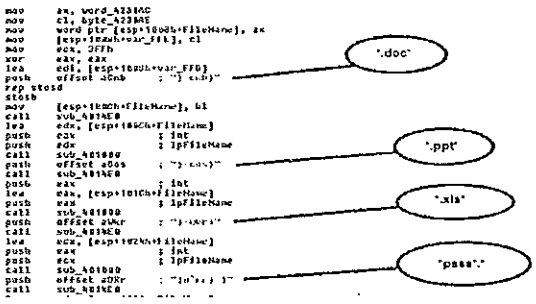


- Em seguida é feita uma checagem por um dos seguintes textos: "petr", "org", "gov" ou "br" (Exemplares 1 e 2) e também por "ong" (Exemplar 3):

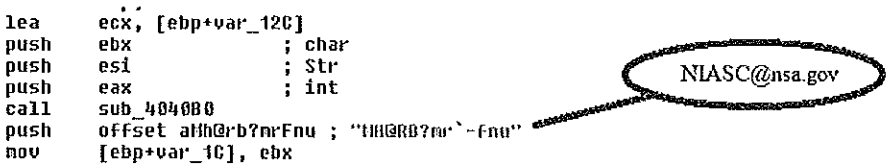


- Caso NÃO encontre nenhum dos textos, ele simplesmente sai do malware (isso dificulta a análise por analisadores automáticos de malware, pois os mesmos teriam que ter os nomes de domínio/workgroup com algum dos textos anteriores).

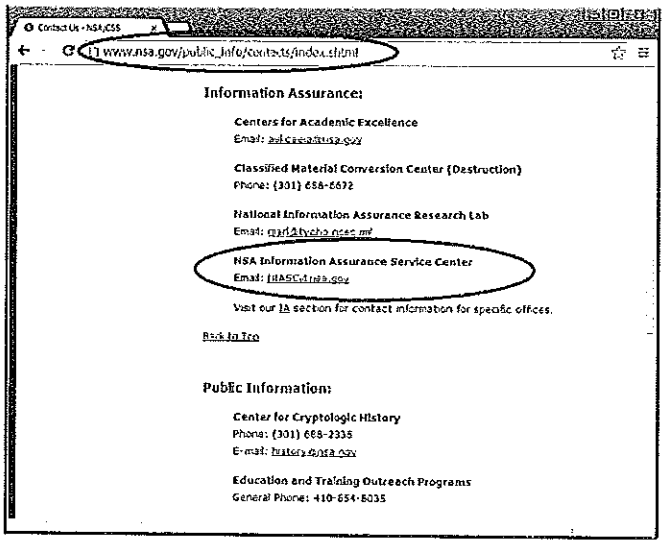
- Caso encontre nomes do tipo GOVerno, ORGanizacao, PETRoleo, PETRobras, BRasil, ele verifica as unidades de disco de C: ate Z: em todas as pastas e subpastas, por arquivos das seguintes máscaras: *.doc*, *.ppt*, *.xls*, *pass*.*, *senha*.* (Exemplares 1 e 2):



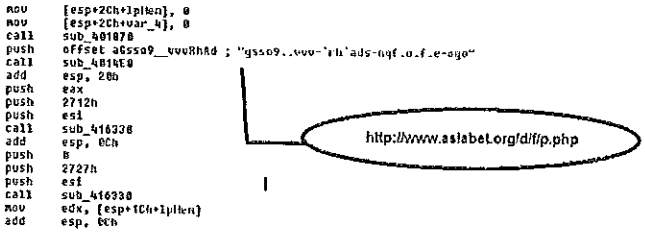
- Se algum arquivo for encontrado, ele faz uma cópia o arquivo para uma extensão .txt e envia para o seguinte email: NIASC@nsa.gov via porta 587 (email autenticado) (Exemplar 1):



- Este email é oficial da NSA (National Security Agency) e pode ser encontrado em seu próprio site:



- Se algum arquivo for encontrado, ele faz o envio via método POST para o site: http://www.asiabet.org/d/f/p.php (Exemplar 2):



- Keylogger (Exemplar 3):

```
call    ds:GetKeyboardLayout
push    eax             ; dwHkl
push    0               ; uMapType
push    ebp             ; uCode
call    ds:MapVirtualKeyExA
lea     ecx, [esp+1008h+String]
push    64h             ; cchSize
shl     eax, 10h
push    ecx             ; lpString
push    eax             ; lParam
call    ds:GetKeyNameTextA
```

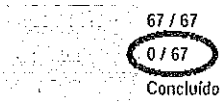
- O keylogger, grava tudo o que é digitado pelo usuário no arquivo %WINDIR%\windowsupdatereport.log em modo criptografado (Exemplar 3):

```
mov     edi, offset aWindowsupdater ; "windowsupdatereport.log"
or      ecx, 0FFFFFFFFh
xor     eax, eax
```

- Como o keylogger (exemplar 3) não possui qualquer tipo de método de envio do arquivo, existe a possibilidade de algum outro módulo ler este arquivo e envia-lo para um site, FTP ou email.

- Após todas as unidades serem checadas, ele encerra o malware.

De acordo com a análise feita pelo site www.virusimmune.com.br, nenhum dos 67 antivírus disponíveis na época detectaram qualquer tipo de infecção no arquivo:



http://www.virusimmune.com.br/virusimmune/analyze

Análise	Informações do arquivo	PE Dump	PE File	ExifTool
Antivirus				**Resultado**
Adobe Malware Classifier				✓
Agnitum				✓
ALYac				✓
Anchiva				✓
Antiy-AVL				✓
ArcaVir				✓
Avast				✓
AVG				✓
Avira				✓
BitDefender				✓
ByteHero				✓

Conclusões:

- Pelas características dos exemplares e pela falta de código de inicialização automática, acreditamos que existam módulos específicos que façam a execução dos mesmos. Possivelmente um módulo central que execute os mesmos através de comandos, controle a segurança, faça o controle dos mesmos contra firewalls e etc;
- Os exemplares foram desenvolvidos com intenção de ataque específico e direcionado, como pode ser determinado pelos textos encontrados: petr, gov, ong, org, br;
- A dificuldade em ter o domínio/workgroup com os textos específicos, reduz a chance de um analisador automático de malware identificar os exemplares, necessitando fazer análise manual;
- Após a identificação dos três exemplares pelas empresas de antivírus, possivelmente serão encontrados outros com padrões semelhantes.
- Os três exemplares foram enviados para o site www.virusimmune.com.br em dias diferentes, mas pela mesma fonte, um IP localizado em Nova York (EUA) - (Disponível para parceiros);
- As redes do Governo e das empresas estatais precisam urgentemente de uma checagem minuciosa para identificar outros possíveis problemas/exemplares que devem existir;
- Lembramos que não basta ter uma solução de antivírus instalada, pois nenhum identificou os exemplares. A solução do problema requer conhecimento profundo de arquivos e análise de malware para que seja feita uma pesquisa avançada.