Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 01/2015 – Propagação de Malware relacionado ao Imposto de Renda 2015

1. Descrição do Problema

a. O CTIR Gov alerta para ocorrência de ataques direcionados a usuários dos serviços da Receita Federal. O ataque consiste no recebimento de mensagem fraudulenta com o seguinte teor:

----- --- Mensagem original ----------
De: intimacao@ [mailto:feredal.receita.gov.br alay.guanaes@terra.com.br] Enviada em: segunda-feira, 30 de março de 2015 21:19
Para: xxx@xxx.gov.br
Assunto: Imposto de Renda 2015 com problemas ID:147357
<http://idg.receita.fazenda.gov.br/arquivos-e-imagens/pagina-inicial/logo_receita.jpeg>
Analisamos sua declaração de IR 2015 e achamos varias divergências em informe de rendimentos. Pedimos encarecidamente que confira as divergências encontradas em sua declaração no arquivo em anexo, ou acesse nosso IDENTIFICADOR DE PENDÊNCIAS ONLINE <http://eng-assiut.tk/images/avatar/rec2/get2.php?Receita_Federal_pendencias_IRF2015=PROCESSO_1146379BR_SP> para verificar as informações.
Atenciosamente,
Receita federal - 21:17:51
---------- Fim da mensagem ----------

b. Tal mensagem traz em anexo, ou acessível por "url", um artefato malicioso identificado, até o momento, com as seguintes variantes:

Nome do Malware	Nome de download	Domínio de hospedagem	MD5
get.php	IR_2015_RECEITA.GOV.COM	dl.dropboxusercontent.com	d926e90ac0d265691b115b886bef15e3
get2.php	IR_2015_RECEITA.GOV.COM	dl.dropboxusercontent.com	eb6b7520d0fc4517f523e8305b9ce76d
mcPHZABWMFvf6CVkHm3NpJLVekdqBZ\?dl\=1	IR2015.RECEITA.GOV.COM	dl.dropboxusercontent.com	9xBXOQfk0QwcbKrb3IikciMbpYGw1dX6pnmcPH

c. Os Relatórios do "virustotal" mostram uma baixa taxas de detecção, conforme abaixo:
https://www.virustotal.com/en/file/d14fd38ba9210574deeef2cced8eb9b965a02726ab99a94fecf6befce29dcc86/analysis/1427807128/

https://www.virustotal.com/en/file/38666134c93356bf230faae5cd6ee20c7e612cea9a7a486479dbd9575bbb6169/analysis/1427751833/

https://www.virustotal.com/en/file/38666134c93356bf230faae5cd6ee20c7e612cea9a7a486479dbd9575bbb6169/analysis/1427807144/

2. Possíveis Riscos

a. Durante a análise deste Incidente, este Centro detectou um **repositório** com um volume expressivo de endereços "IP" de Órgãos de governo, que sugere um cadastro de máquinas comprometidas. Tal repositório está acessível em:
" http://eng-assiut.tk/images/avatar/rec2/ver.php"

b. As máquinas comprometidas podem ser usadas para as seguintes ações:

- Passar a integrar uma "botnet";

- Roubo de informações (leaks) das organizações afetadas;

- Porta de entrada para ataques mais sofisticados.

3. Ameaças

Nosso relatório de análise do preliminar trouxe as seguintes informações:

INFORMAÇÕES GERAIS
Nome: 9xBXOQfk0QwcbKrb3IikciMbpYGw1dX6pnmcPHZABWMFvf6CVkHm3NpJLVekdqBZdl1
Data da Análise: 2015-03-30
Tipo: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Tamanho: 3492352
MD5: eb6b7520d0fc4517f523e8305b9ce76d
SHA-1: e6fe1db42735218d9684f093b8ff9ff82b0dc32c
SHA-256: 38666134c93356bf230faae5cd6ee20c7e612cea9a7a486479dbd9575bbb6169
Packer: BobSoft Mini Delphi -> BoB / BobSoft

NÚMERO DE ALTERAÇÕES NO REGISTRO: 1093

REGISTROS LIDOS
registry\machine\system\controlset001\control\computername\activecomputername\computername -> computernamechangeme
\registry\machine\system\controlset001\control\computername\activecomputername\computername -> changeme
---
ESCRITAS NA MEMÓRIA DE OUTRO PROCESSO
Nome: \c:\program files\internet explorer\iexplore.exe

PROCESSOS CRIADOS
"c:\program files\internet explorer\iexplore.exe –nohome"

MUTEXES CRIADOS
1. kb28233240x
2 shell.cmrupidllist
3 wininetconnectionmutex
---

4. Sugestões para Mitigação do Problema

Este Centro não tem como afirmar que tal incidente está direcionado ao Governo. Entretanto, no log de controle do atacante (lista dos equipamentos que acessaram o "link de hospedagem do Malware") consta uma quantidade significativa de endereços IP de redes de órgãos governamentais. Boa parte dos equipamentos que fizeram esse acesso possivelmente está infectada.

Diante disso, recomendamos a divulgação do evento no âmbito dessa organização, bem como orientar os usuários de recursos de TIC a evitar o acesso ao artefato malicioso.

Recomendamos, ainda, a realização de campanhas de conscientização e da aplicação de políticas de segurança eficientes nas Instituições Públicas de modo a conter ou mitigar este tipo de ataque.

Finalmente, sugerimos a adoção de medidas proativas nos "ativos de TI", tais como filtragem de "proxy" e de correio eletrônico (*Email Attachment Filtering*), bem como a inspeção de Logs, de modo a minimizar o risco de propagação deste tipo de artefato dentro do ambiente organizacional.

Brasília-DF, 02 de abril de 2015.

Atenciosamente,

Equipe do CTIR Gov