Serviço Federal de Processamento de Dados SERPRO

ESP REC
000045

OFÍCIO: DP - 038775/2013

Brasília, 26 de dezembro de 2013

A Sua Excelência a Senhora
Senadora VANESSA GRAZZIOTIN
Presidente da CPI da Espionagem do Senado Federal
Anexo II - Ala Senador Alexandre Costa, sala 15 - subsolo
Brasília - DF

Assunto: Presta informações.

Senhora Senadora,

Em atendimento à requisição de Vossa Excelência, informamos que o SERPRO tem como clientes alguns dos mais importantes órgãos da adminstração pública federal, estadual e municipal, dentre os quais podemos destacar o Ministério da Fazenda, a Receita Federal do Brasil, o Ministério do Planejamento, Orçamento e Gestão, a Presidência da República, o Departamento de Polícia Federal dentre outros, para os quais atua nas seguintes linhas de negócio: desenvolvimento de soluções, integração e interoperabilidade, rede multiserviços, segurança, serviços ao cidadão e serviços de datacenter.

A proteção dos dados que estejam sob nossa responsabilidade e gestão, como ocorre nos casos da Receita Federal, do Ministério da Fazenda, ou do Ministério do Planejamento, por exemplo, se dá com observância do dever de sigilo previsto no art. 8º da Lei 5.615/1970 e com a adoção de todos os meios de proteção em matéria de rede, manipulação, armazenamento disponíveis no atual estado da arte: mediante o uso de *firewalls*, IPSs, roteamento, criptografia, controle de acesso, segregação de ambientes, aplicação de *antimalware*, atualização de *patches*, correlação de eventos, monitoração constante, proteção contra negação de serviços pontual ou distribuída, adoção de técnicas de desenvolvimento seguro, análise de vulnerabilidade de código, análise de vulnerabilidade às escuras, aplicação de políticas de segurança, regras de rede e gestão de continuidade, além de uso de ferramentas de alta disponibilidade para serviços considerados "de missão crítica".

Os ataques havidos em 2009 e 2013 são inúmeros. Podemos dizer que por dia são sofridos milhares de ataques vindos de toda parte do mundo e que esse nível de tentativa de ataque cresce bastante em momentos críticos (grandes eventos, pico de produção do imposto de renda em março/abril etc.).

Subsecretaria de Apoio às Comissões Especiais e Parlamentares de Inquérito
Recebido em 27/12/2013
Às 16h26 horas
www.serpro.gov.br
Rogério Faleiro Machado
Analista Legislativo
Mat. 256101

SERPRO - SEDE
SGAN Quadra 601 - Módulo V - CEP 70836900 - DF-Brasil
CNPJ:33.683.111/0001-07
Telefone:(61) 2021-8000

A listagem de ataques havidos mais importantes e evidenciados nos dois referidos anos consta da tabela anexa. É importante destacar que a "origem" ali detectada representa o ponto último de referência, razão pela qual não podemos excluir a possibilidade de o verdadeiro atacante estar operando aquela unidade de *Internet Protocol* a partir de outro país, encoberto por recursos de *proxy, botnet* e *quetais*.

Essa listagem inclui todos os ataques tentados e detectados por nossa monitoração.

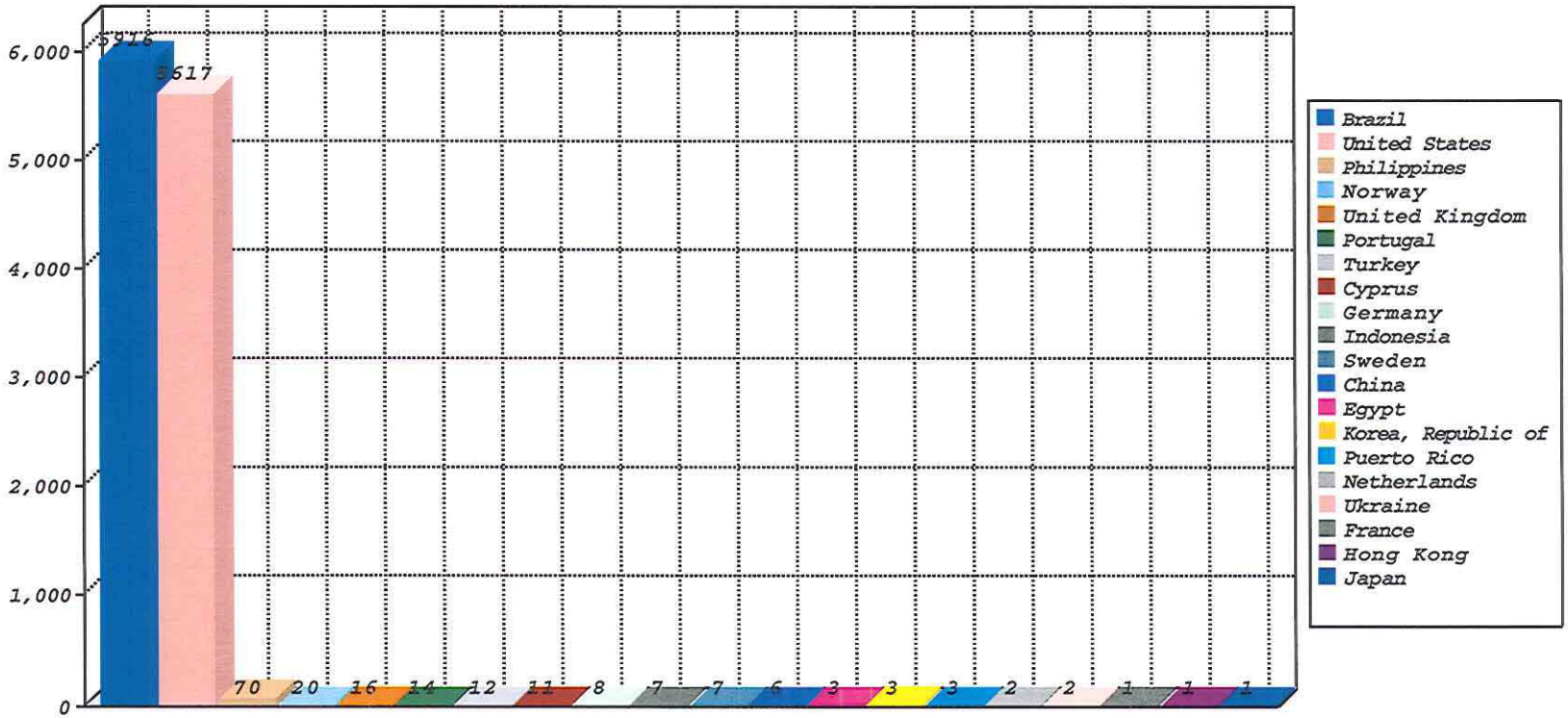
Respeitosamente,

MARCOS VINICIUS FERREIRA MAZONI
Diretor-Presidente

SERPRO - SEDE
SGAN Quadra 601 - Módulo V - CEP 70836900 - DF-Brasil
CNPJ:33.683.111/0001-07
Telefone:(61) 2021-8000

SERPRO
Serviço Federal de Processamento de Dados

Relatório_Ataques_Identificados



ASSINATURA IDENTIFICADA	PAÍS DE ORIGEM	QTD. DE ATAQUES
HTTP: Microsoft Windows HTTP.sys Denial of Service	Brazil	3296
HTTP: IIS3 ASP Dot Bug	Brazil	1911
HTTP: IIS3 ASP Dot Bug	United States	1852
HTTP: Microsoft Windows HTTP.sys Denial of Service	United States	1691
HTTP: Possible HTTP GET LOIC Denial-of-Service Attack Detected	United States	441
TCP: Small Window DoS	United States	343
HTTP: Internet Media Tunneling through HTTP	Brazil	263
HTTP: Internet Media Tunneling through HTTP	United States	258
IPv4: TCP Session Hijacking Attempt Detected	United States	195
HTTP: Microsoft Multiple Products HTML Sanitization Cross-site Scripting Vulnerability	United States	143
HTTP: Attempt to Read Password File	United States	125
HTTP: Xitami If-Modified-Since Header Buffer Overflow I	United States	87
TCP: Small Window DoS	Philippines	70
HTTP: Xitami If-Modified-Since Header Buffer Overflow I	Brazil	68
HTTP: Microsoft IIS Multiple Extension Processing Security Bypass Vulnerability	Brazil	67
TCP: Small Window DoS	Brazil	62
P2P: Shareaza Alive	Brazil	58
HTTP: OS Command Execution Unix	United States	55
HTTP: Microsoft Multiple Products HTML Sanitization Cross-site Scripting Vulnerability	Brazil	37
HTTP: SQL Injection - Exploit II	Brazil	36
HTTP: SQL Injection - Exploit	United States	36
HTTP: SQL Injection - Exploit	Brazil	29
HTTP: phpBB Viewtopic.php Remote Command Execution	United States	28
HTTP: IIS cmd.exe Execution	United States	26

ASSINATURA IDENTIFICADA	PAÍS DE ORIGEM	QTD. DE ATAQUES
HTTP: SQL Injection - Exploit II	United States	25
P2P: Shareaza Alive	United States	24
HTTP: Detect PHP-CGI Remote code Execution vulnerability	United States	23
HTTP: CRLF Injection	United States	22
HTTP: ZmEu Exploit Scanner	Brazil	19
HTTP: RedHat JBoss Enterprise Application Platform JMX Console Security Bypass	United States	17
HTTP: Possible HTTP GET LOIC Denial-of-Service Attack Detected	Brazil	17
HTTP: Trojan Shell Script	United States	14
HTTP: IIS3 ASP Dot Bug	Portugal	14
HTTP: IIS Index Sever idq Read File	United States	14
SHELLCODE: Shellcode Detected for MIPS Family CPUs	Turkey	12
HTTP: Detect PHP-CGI Remote code Execution vulnerability	United Kingdom	11
HTTP: IIS iisadmpwd Proxied Password Attack Attempt	United States	11
HTTP: Detect PHP-CGI Remote code Execution vulnerability	Brazil	10
HTTP: Detect PHP-CGI Remote code Execution vulnerability	Cyprus	10
HTTP: SqlMap SQL Injection - Scanning I	Brazil	9
TCP: Fin with Zero Window and Payload	United States	9
TCP: Small Window DoS	Sweden	7
HTTP: ZmEu Exploit Scanner	Germany	7
HTTP: Apache mod_isapi Denial of Service	United States	7
TCP: Small Window DoS	Indonesia	7
HTTP: Microsoft IIS hit-highlighting Remote Security Bypass	United States	7
HTTP: ZmEu Exploit Scanner	United States	7
HTTP: Abyss Web Server Malicious HTTP Request Information Disclosure Vulnerability	United States	7
HTTP: IIS cmd.exe Execution	Norway	6
HTTP: IIS JET VBA Run Command Attempt	United States	6
HTTP: BadBlue Unencrypted Password File Read Attempt	United States	6
HTTP: Apache Win32 PHP.EXE Remote File Disclosure	United States	6
TCP: Fin with Zero Window and Payload	Brazil	6
HTTP: Firefuzzer SQL Injection Scanning III	Brazil	5
P2P: BitTorrent Meta-Info Retrieving	United States	5
HTTP: ColdFusion Sample Application Usage	United States	5
HTTP: Microsoft IE Remote .lnk/.url Vulnerability	Brazil	5
TCP: Bare Push Probe	United States	5

ASSINATURA IDENTIFICADA	PAÍS DE ORIGEM	QTD. DE ATAQUES
HTTP: PHP Include - PHP Includedir Include Code Execution	United States	5
HTTP: Allaire JRun WEB-INF Disclosure	United States	5
HTTP: phpSecurePages secure.php cfgProgDir Parameter PHP File Include	United States	4
HTTP: RedHat JBoss Enterprise Application Platform JMX Console Security Bypass	Norway	4
HTTP: SQL Injection - Exploit II	Norway	4
HTTP: Apache Tomcat Sensitive Information Disclosure	United States	4
HTTP: Attempt to Read Password File	Norway	4
HTTP: iPlanet Remote File Viewing Vulnerability	United States	4
HTTP: IIS root.exe Execute Command	United States	4
HTTP: VBulletin Forumdisplay PHP Code Execution	United States	3
HTTP: Lotus Domino Directory Traversal Vulnerability	United States	3
TCP: Small Window DoS	China	3
HTTP: Apache Tomcat Servlet Path Disclosure	United States	3
HTTP: Apache mod_isapi Denial of Service	Brazil	3
HTTP: Trojan Shell Script	Brazil	3
HTTP: Faxsurvey Execute Command	United States	3
TCP: Bare Push Probe	Brazil	3
HTTP: Trojan Shell Script	Egypt	3
HTTP: gwweb Access File	United States	3
HTTP: PDGSoft Shopping Cart Orders Exposure	United States	3
HTTP: Apache HTTPD mod_proxy_ajp Denial Of Service	Brazil	3
HTTP: Detect PHP-CGI Remote code Execution vulnerability	Puerto Rico	3
HTTP: WEBactive HTTP Server File Disclosure	United States	3
HTTP: PHP Include - PHP Includedir Include Code Execution	Korea, Republic of	2
HTTP: Selena Sol Webstore Order Log Exposure	United States	2
HTTP: Microsoft SharePoint ws asmx Denial of Service Vulnerability	United States	2
HTTP: Sun AnswerBook2 Administrative Script Access Vulnerability	United States	2
HTTP: RaQ Bash History Read	United States	2
HTTP: Read UNIX History File	United States	2
HTTP: Cisco HTTP Admin Authentication	United States	2
HTTP: PCCS MySQL Database Obtain Sensitive Infomation	United States	2
HTTP: Nginx ngx_http_parse_complex_uri() Buffer Underflow Vulnerability	United States	2
HTTP: Apache Win32 Directory Listing	United States	2
HTTP: MailStudio Design Error	United States	2

ASSINATURA IDENTIFICADA	PAÍS DE ORIGEM	QTD. DE ATAQUES
HTTP: Siteserver site.csc File Read	United States	2
HTTP: WebSpeed Sensitive Info Disclosure	United States	2
HTTP: EZMall Information Disclosure	United States	2
ORACLE: 9iAS OracleJSP Information Disclosure Vulnerability	United States	2
SSL: OpenSSL Client Hello Cipher Length Overflow	Brazil	2
HTTP: php.cgi Buffer Overflow	United States	2
HTTP: Cisco Catalyst Remote Arbitrary Command Execution	United States	2
HTTP: Apache Win32 .Bat Exploit	United States	2