Fox Kitten - Campaña de grupos Iraníes para explotar Vulnerabilidades en VPN Servers

Durante el último trimestre de 2019, se descubrió una campaña ofensiva Iraní generalizada, que atacaba servidores VPN para implantar puertas traseras, con principales objetivos las VPN de Pulse Secure, Fortinet, Palo Alto Networks y Citrix, dirigida contra empresas y organizaciones en todo el mundo.

Publicación:
20/02/2020
Importancia:
Alta
Riesgo de explotación:
Media
Tipo de explotación:
Remoto

Campaña ofensiva de espionaje Iraní generalizada

Fuentes:

DigiCSIRT

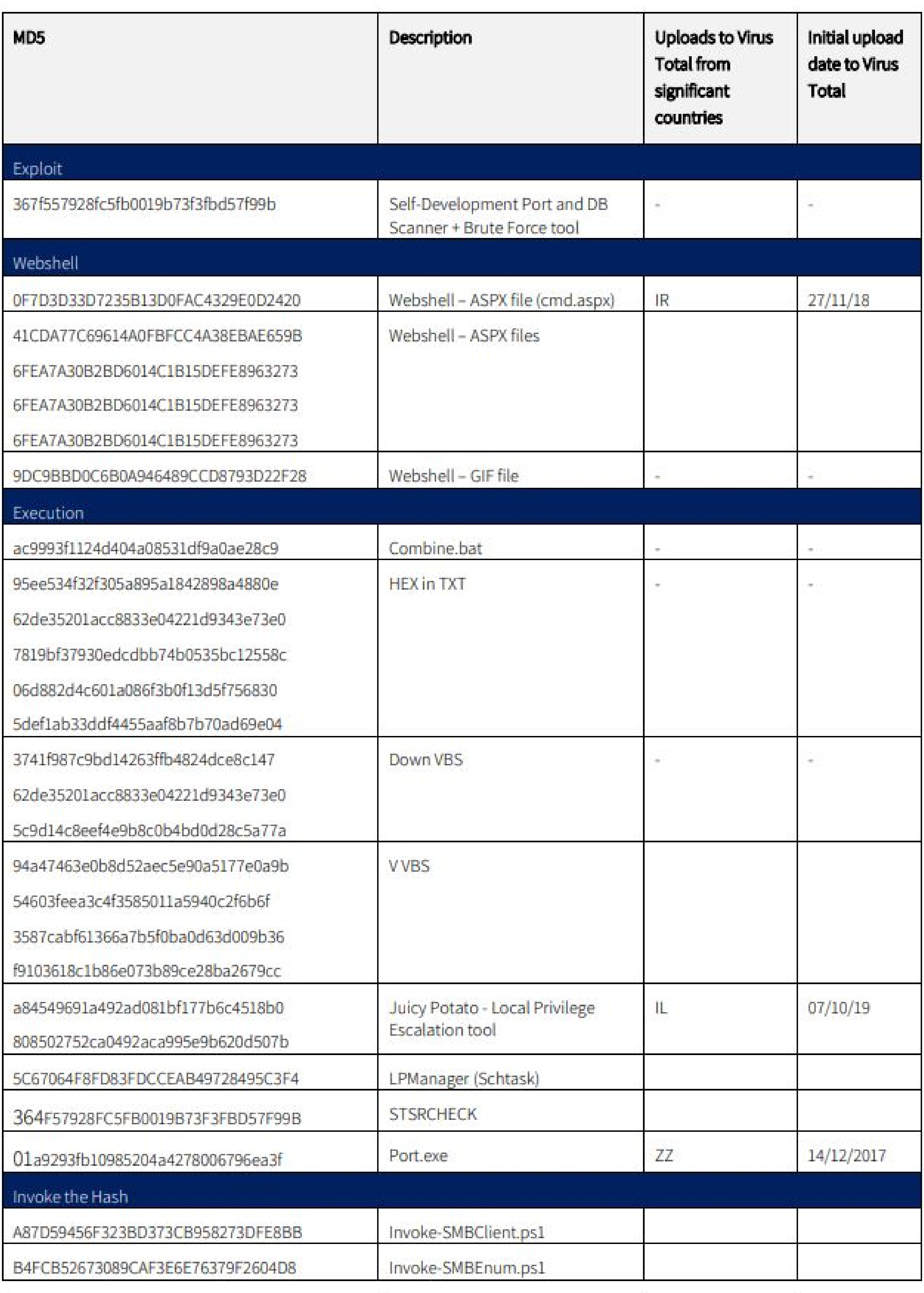
Según investigadores de ClearSky durante el último trimestre de 2019 grupos Iraníes habrían explotado vulnerabilidades de día 1 en servicios de VPN y RDP. La campaña estaba dirigida a empresas y organizaciones en todo el mundo y de diferentes sectores incluidos TI, Telecomunicaciones, Petróleo y Gas, Aviación, Gobierno y Seguridad.

Los ataques fueron llevados a cabo por grupos APT vinculados a Irán, entre ellos APT34, APT33 y APT39 mediante el desarrollo de exploits para aumentar la capacidad de intrusión. Desde finales de agosto de 2019, los grupos vinculados a Irán han explotado las vulnerabilidades en las VPN Pulse Secure (CVE-2019-11510), Fortinet FortiOS VPN (CVE-2018-13379) y Palo Alto Networks "Global Protect" VPN (CVE-2019-1579).

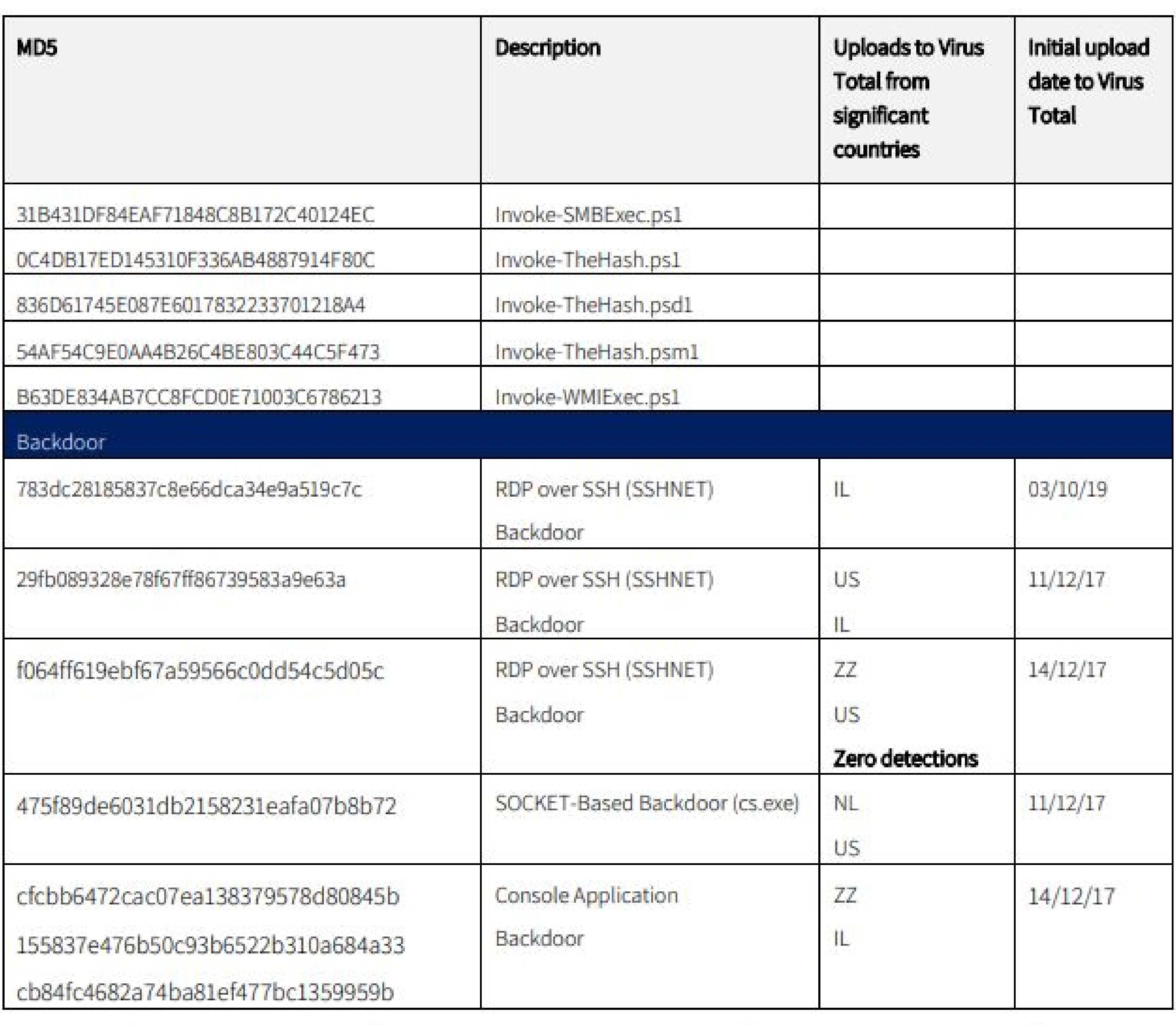
Recientemente, los atacantes también emplearon exploits para aprovechar la vulnerabilidad en Citrix "ADC" VPN (CVE-2019-19781).

Los atacantes explotan las fallas de VPN para acceder a las redes empresariales, infectan los sistemas mediante una puerta trasera y desde ellos se mueven lateralmente para comprometer otras computadoras en la red interna. Después de que los atacantes han explotado las vulnerabilidades en los sistemas VPN para alcanzar la red objetivo, realizan varias acciones y utilizan múltiples herramientas para mantener su posición en la red con altos privilegios.

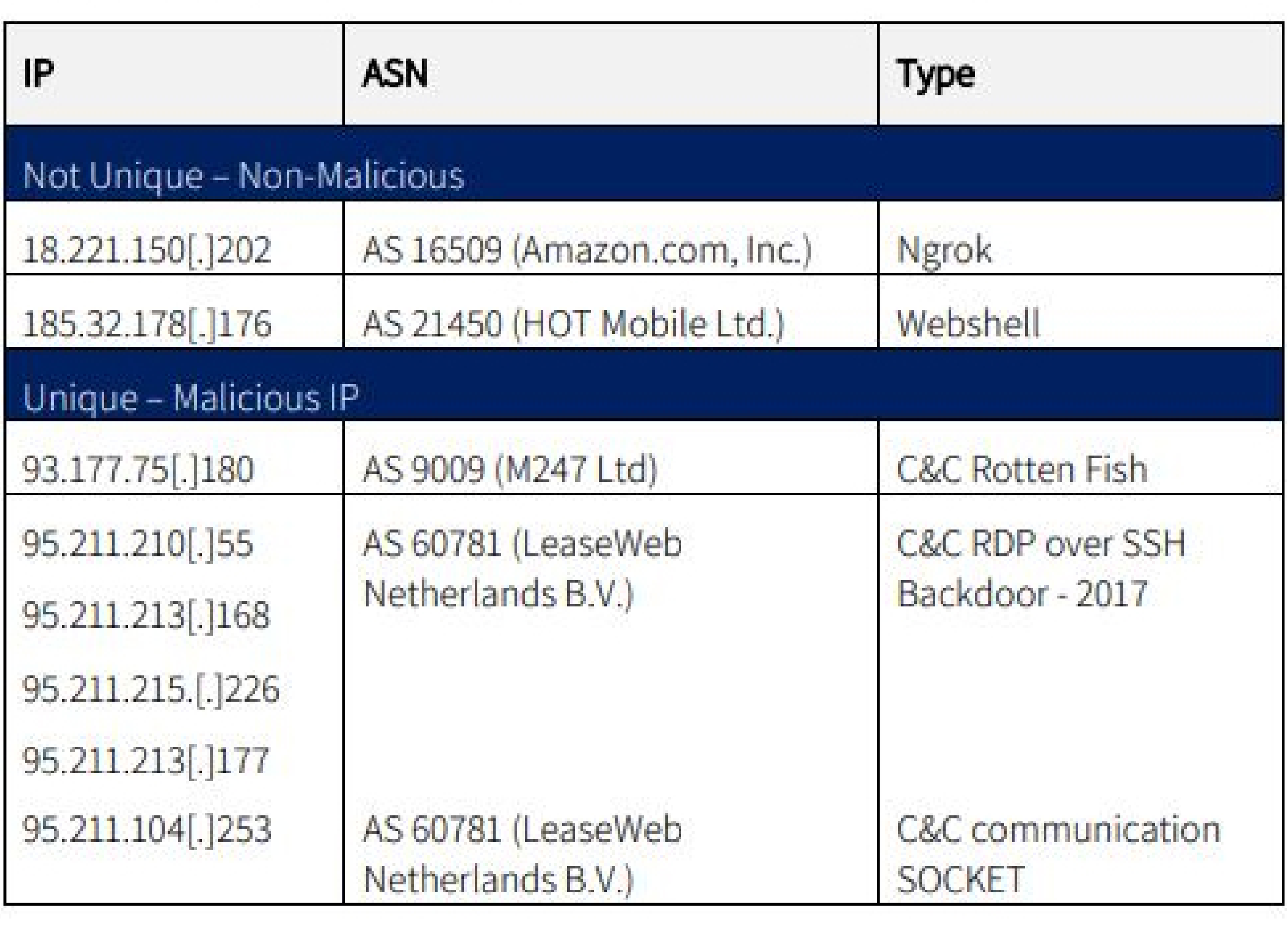
IoC



MD5	Description	Uploads to Virus Total from significant countries	Initial upload date to Virus Total
Exploit			
367f557928fc5fb0019b73f3fbd57f99b	Self-Development Port and DB Scanner + Brute Force tool	-	-
Webshell			
0F7D3D33D7235B13D0FAC4329E0D2420	Webshell – ASPX file (cmd.aspx)	IR	27/11/18
41CDA77C69614A0FBFCC4A38EBAE659B 6FEA7A30B2BD6014C1B15DEFE8963273 6FEA7A30B2BD6014C1B15DEFE8963273 6FEA7A30B2BD6014C1B15DEFE8963273	Webshell – ASPX files		
9DC9BBD0C6B0A946489CCD8793D22F28	Webshell – GIF file	-	-
Execution			
ac9993f1124d404a08531df9a0ae28c9	Combine.bat	-	-
95ee534f32f305a895a1842898a4880e 62de35201acc8833e04221d9343e73e0 7819bf37930edcdbb74b0535bc12558c 06d882d4c601a086f3b0f13d5f756830 5def1ab33ddf4455aaf8b7b70ad69e04	HEX in TXT	-	-
3741f987c9bd14263ffb4824dce8c147 62de35201acc8833e04221d9343e73e0 5c9d14c8eef4e9b8c0b4bd0d28c5a77a	Down VBS	-	-
94a47463e0b8d52aec5e90a5177e0a9b 54603feea3c4f3585011a5940c2f6b6f 3587cabf61366a7b5f0ba0d63d009b36 f9103618c1b86e073b89ce28ba2679cc	V VBS		
a84549691a492ad081bf177b6c4518b0 808502752ca0492aca995e9b620d507b	Juicy Potato - Local Privilege Escalation tool	IL	07/10/19
5C67064F8FD83FDCCEAB49728495C3F4	LPManager (Schtask)		
364F57928FC5FB0019B73F3FBD57F99B	STSRCHECK		
01a9293fb10985204a4278006796ea3f	Port.exe	ZZ	14/12/2017
Invoke the Hash			
A87D59456F323BD373CB958273DFE8BB	Invoke-SMBClient.ps1		
B4FCB52673089CAF3E6E76379F2604D8	Invoke-SMBEnum.ps1		



MD5	Description	Uploads to Virus Total from significant countries	Initial upload date to Virus Total
31B431DF84EAF71848C8B172C40124EC	Invoke-SMBExec.ps1		
0C4DB17ED145310F336AB4887914F80C	Invoke-TheHash.ps1		
836D61745E087E6017832233701218A4	Invoke-TheHash.psd1		
54AF54C9E0AA4B26C4BE803C44C5F473	Invoke-TheHash.psm1		
B63DE834AB7CC8FCD0E71003C6786213	Invoke-WMIExec.ps1		
Backdoor			
783dc28185837c8e66dca34e9a519c7c	RDP over SSH (SSHNET) Backdoor	IL	03/10/19
29fb089328e78f67ff86739583a9e63a	RDP over SSH (SSHNET) Backdoor	US IL	11/12/17
f064ff619ebf67a59566c0dd54c5d05c	RDP over SSH (SSHNET) Backdoor	ZZ US **Zero detections**	14/12/17
475f89de6031db2158231eafa07b8b72	SOCKET-Based Backdoor (cs.exe)	NL US	11/12/17
cfcbb6472cac07ea138379578d80845b 155837e476b50c93b6522b310a684a33 cb84fc4682a74ba81ef477bc1359959b	Console Application Backdoor	ZZ IL	14/12/17



IP	ASN	Type
Not Unique – Non-Malicious		
18.221.150[.]202	AS 16509 (Amazon.com, Inc.)	Ngrok
185.32.178[.]176	AS 21450 (HOT Mobile Ltd.)	Webshell
Unique – Malicious IP		
93.177.75[.]180	AS 9009 (M247 Ltd)	C&C Rotten Fish
95.211.210[.]55 95.211.213[.]168 95.211.215.[.]226 95.211.213[.]177	AS 60781 (LeaseWeb Netherlands B.V.)	C&C RDP over SSH Backdoor - 2017
95.211.104[.]253	AS 60781 (LeaseWeb Netherlands B.V.)	C&C communication SOCKET

Recomendaciones

- Mantener al día la remediación de vulnerabilidades en sistemas de acceso remoto, VPN, mediante la actualización de plataformas.
- Aplicar acciones de bloqueo para los diferentes IoC relacionados el presente informe, bajo validación previa.

Referencias:

- https://securityaffairs.co/wordpress/97957/apt/fox-kitten-campaign-vpn-bugs.html
- https://www.clearskysec.com/fox-kitten
- /https://www.zdnet.com/google-amp/article/iranian-hackers-have-been-hacking-vpn-servers-to-plant-backdoors-in-companies-around-the-world/?__twitter_impression=true
- https://threatpost.com/iranian-apts-fox-kitten-global-spy-campaign/152974/
