MNEMO CERT

Mnemo-CERT

Aviso de seguridad MVN-2017-1030

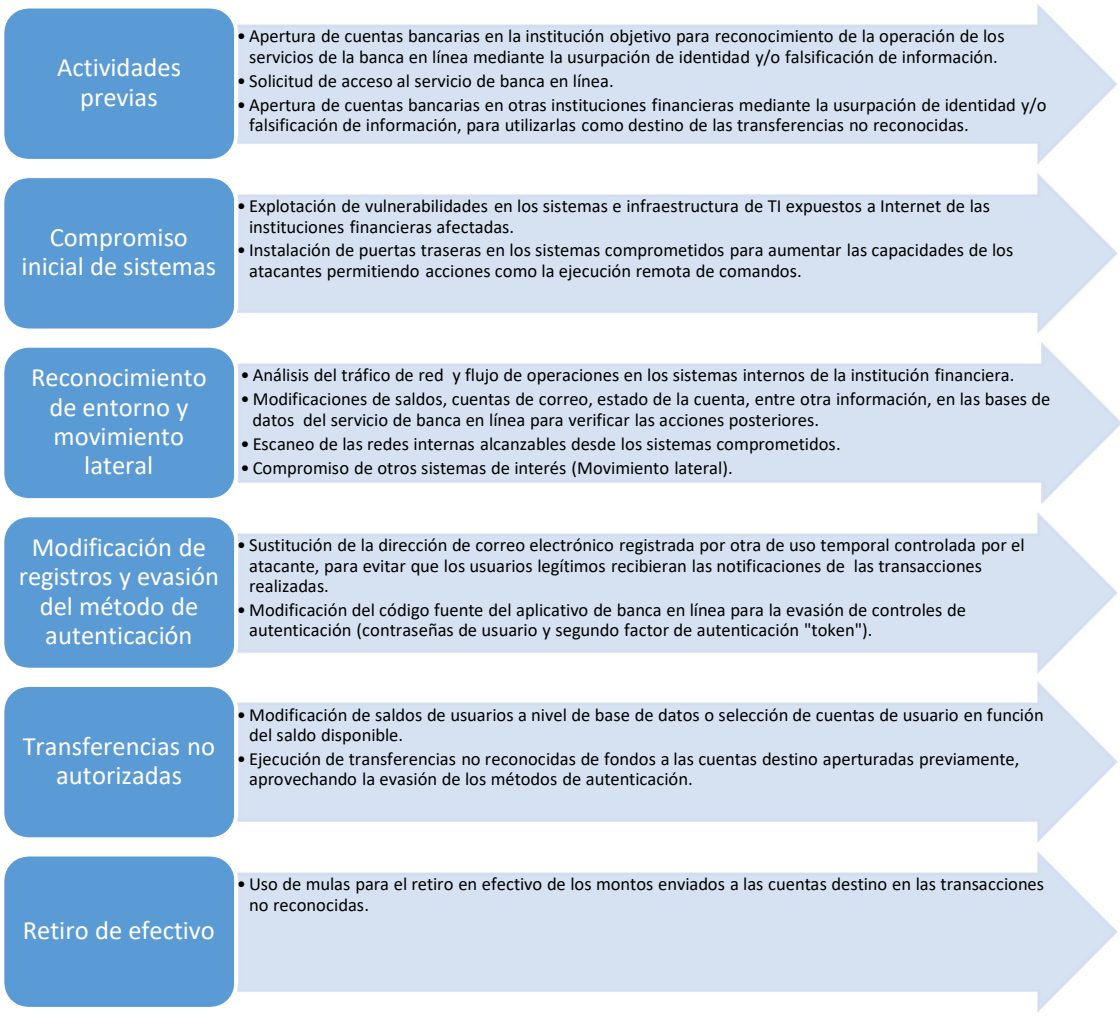
Campaña de ciberataques dirigida a instituciones del sector financiero mexicano

Martes, 30 de Octubre de 2017

Descripción

La Unidad de Inteligencia de Amenazas de Mnemo-CERT (Equipo de Respuesta a Incidentes Cibernéticos) analizó una nueva campaña de ciberataques en contra de instituciones financieras, presentada a inicios del segundo semestre del año 2017.

A continuación, se describe el modo de operación identificado en la campaña:



Información adicional:

- El periodo de tiempo que se identificó desde el compromiso inicial hasta la realización de transferencias de fondos no reconocidas es de aproximadamente 6 meses.
- Las direcciones de correo electrónico temporales se caracterizan por ser de uso gratuito, no requerir registro para su uso, no solicitar credenciales de acceso para visualizar la bandeja de entrada y el tiempo de vida de la bandeja de entrada es de 12 a 24 horas.
- Para que estos ataques sean exitosos debe conocerse el detalle de los siguientes aspectos:
    - Procesos y procedimientos de apertura de cuentas en la institución financiera objetivo.
    - Operación interna de procesos de verificación de cuentas de la institución financiera.
    - Vulnerabilidades en la infraestructura de TI de la institución financiera.
    - Conocimientos avanzados de aplicativos de banca en línea, programación y base de datos.
    - Operación de los sistemas de transferencias interbancarios.

El análisis realizado por Mnemo-CERT ha permitido identificar indicadores de compromiso (IoC) relacionados con esta nueva campaña de ciberataques sobre instituciones financieras, los cuales pueden auxiliar a las instituciones financieras a detectar comportamientos sospechosos en sus aplicativos e infraestructura tecnológica.

Principales indicadores de compromiso

Dominios de cuentas de correo electrónico temporales			
mailinator.com yopmail.com maildrop.cc dropmail.me getnada.com dispostable.com sharklasers.com guerrillamail.info grr.la guerrillamail.biz guerrillamail.com guerrillamail.de guerrillamail.net	guerrillamail.org guerrillamailblock.com pokemail.net spam4.me harakirimail.com boun.cr inboxbear.com armyspy.com cuvox.de einrot.com fleckens.hu gustr.com jourrapide.com	rhyta.com superrito.com teleworm.us mailnesia.com mt2015.com tempr.email discard.email discardmail.com spambog.com spambog.ru 0815.ru hulapla.de pfui.ru	0815.su zaktouni.fr freelance-france.eu webcontact-france.eu fast-mail.fr mail-easy.fr instantmail.fr dispostable.com cd.mintemail.com
Contraseñas			
133700	991377	M4g1cP4ssw0rd	
Nombre de puertas traseras (backdoors)			
123c 124c Application clx m4 newsgroupz probe tesrx testsx ultima up_lo xtestsx xxas	uy144 x114 x122 x12 x132 x144 x222 x322 x333 x433 x443 x444 xx144	xxas xy144 2x bak cm-nix defaultp defaultx defaultxz defaulty defaultz defaultzz ndex pro	proxy-jsp safe sw sw3 sw4 sw5 xase xase2 xasf xffd xffdu xffdx xndex

MD5 de puertas traseras (backdoors)	
a5241e41a4b9151ae80f297adc5c1b63 ddb2c574e4fd3ad64c027c74d0f382c8 2dcb13e75e9b58b9546154e00a0b9665 3cba29c805261e91715e473f62d55c60 3869ca35ced71188e367b1e75282c8a6 9e0563caa00582c3aa4bf6c41d9f9c46 6c8f822588c0bf9810b2d573bca27812 92287b484365c6cf21234eb5b382e4e6 cc187f69fcfb943284f90e4d9815aef7 df93c950f349321289cbc9422b75b4ed 5137c9160e605d8c03878fdc593d0063 81083a956264d87834ec0daea3e93d1f 8fd88f8ddaf879c2b2d0f73d670bb389 4e3caa1070aa7046cdfe5c55a64e5099 b487b63162e6ed3e797c3ae1c5771345 a40a765fa4570606175831182e126270	0f883acee8228740039b58212eb4ac0a 9ab4ac91df35dcb771dfc3879a213ec2 34e69c44c714d08fdcbd20249d8d528b ba01998510acf24730afbcdee872411c eb4a8090b571eef8ed35319b8edee7d0 4e5d9a9b28b63f0bdfc689d89a451cbf c164953898ae8262f955144633a4b578 7bad2c69b0874a19d56f59f3e2469188 27de8aca21be426e60305fbb94ac8fef a08ee1f9c35b6c11099c55409c245788 a0202e00c32555574e30bf406a545b6e dc62b6746dcd26b5af472ae598e0e053 1ff3094144a5e0cbede2800e3584b480 ee4a50a94db19c8f9dbd626ef89c4598 23a73d5cf2e858cec326d020827e086a
SHA1 de puertas traseras (backdoors)	
ef488cbf66c3450dbe1ea14aacf2ecc914a5466b 9fd8bd767d1b89d46bdea0229b65b6701cdcabd4 d8c00ad08868c6e20bd4f1e36f9e766771463724 8d9eaa20232a57c102f52e95b90de219bf4abe68 2a6d4da2057cd983902e2ae9a41fcf5710c33898 880f72a3651704affb3ef32102b69d7c7617dfd2 797dc40a6a243ec948ad5ae3e957a9ee861078e9 1b48c44ce349e6cd5549512ab06fa5504a3cc33e 6fe1dc3bb3cd22b9b068de10acc36811d8d5944a 050e29b654dd7b124f254c24545cd24ca3a961eb 4d0c7a4d201117e193f8af2e2b20cf8119ba6b0a 88cfd74d9ed2b79c20b85bfb2114b592fff57548 c8dcd4ba03162fea0cb8bc7f716741da679e96b7 4d9d72803ab01effe4820d15065fac6b683ad2d9 6c7d66bd886161574f8e5a0af90cbd4997ba8e7c d8114e2d3e1a4ebca810b86baaa3d1e9a10b3b43	4e90aadef0c1caf1b45a57d9a3cfcde19380878e c937d8b8f7be5f61b5b8037b2e2b87c97393c014 2c8b6230d3e80ebdbc4b8957f59d0d93d979915a 1b5f9251b2da917be72e0414170f1d909b17692a 4291c4620ca7a0f08917ae9e9425517cf15b82ff 98a01a80f8f7d5f47fd90746b4d229590a98311c 81750a58ccbf40331f8e18774ed1799ae2888e29 4716aeb3076a6b0fd00ec9f5144747270407dcc1 eeb91310fb67178599128963ba67c8339182976f 510633e5f8e8f5b0b94c6bf649ceddebb65bd15a 75b99a04d7bb8f347e47fb5ac9b3eb6df9cef3d6 aa4b788bc72081d8cac2d4773d2d3f3cccdc3d31 f15a2eb77ccbde93b4db2e9e83d3374eeee19928 4de191ce55fff9e77f9f1dbca74d934690665ac2 8b089c24cf75cb123917249f68b0360afd3b4331

Sistemas afectados

- Aplicativos e infraestructura de TI que dan soporte a los servicios de banca en línea de algunas instituciones financieras.

Recomendaciones

- Evaluar el impacto de las amenazas cibernéticas en los procesos operativos y de negocio.
- Implementar un esquema de seguridad por capas, desde el perímetro hasta el host, considerando mecanismos de monitoreo de integridad.
- Realizar periódicamente pruebas técnicas para evaluar el estado de la seguridad en los sistemas e infraestructura de TI.
- Establecer un plan de mitigación de los hallazgos obtenidos durante las pruebas técnicas.
- Identificar en sus sistemas e infraestructura de TI el registro de alguno(s) de los indicadores de compromiso listados previamente.
- Mantener registros tanto de la infraestructura como de los aplicativos que permitan realizar la trazabilidad y facilitar la respuesta a incidentes.
- Desarrollar un plan de Threat Hunting, es decir, la búsqueda de actividad maliciosa de forma periódica al interior y exterior de la institución.