Alerta de seguridad informática	2CMV22-00374-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de noviembre de 2022
Última revisión	07 de noviembre de 2022

NOTA SOBRE EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO

La información contenida en este informe fue procesada por el CSIRT de Gobierno analizando múltiples fuentes. La información puede ser modificada o actualizada a partir de nuevos antecedentes y análisis.

Las personas y organizaciones víctimas de suplantación, en los casos que corresponda, no tienen responsabilidad sobre esa acción ejecutada por el atacante. El uso de la imagen de los suplantados en este informe tiene el específico propósito de evitar que terceras partes sean afectadas por atacantes.

Las alertas de seguridad cibernéticas del CSIRT de Gobierno contienen información sobre incidentes y acciones maliciosas que podrían impactar en las organizaciones. Los receptores de esta información tienen la responsabilidad de evaluar la eventual aplicación de cuarentenas preventivas sobre los indicadores de compromiso (IoC) que se comparten en este documento, teniendo presente los impactos que pueda tener en la entrega de sus servicios o en la continuidad operativa de sus negocios. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa sobre los IoC compartidos, se debe evaluar la posibilidad de levantar el bloqueo.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) comparte una serie de indicadores de compromiso pertenecientes a nuevas campañas que distribuyen el peligroso malware Emotet.

Emotet es uno de los malware más peligrosos del mundo. Ha evolucionado de ser un troyano bancario a a servir como puerta trasera para todo tipo de delitos. Cualquier ciberdelincuente puede comprarlo para ingresar a los sistemas de sus víctimas y realizar distintos ataques, como ransomware o robo de datos.

Advertencia sobre gestión de IoC

Los patrones expresados en forma de hash de un archivo pueden ser administrados con herramientas centralizadas y distribuidas, como firewall y antimalware. Las organizaciones deben tomar resguardo de incorporar un hash que pudiere estar vinculado a un archivo o DLL válida dentro de un sistema.

Al gestionar patrones potencialmente maliciosos con nombres de host o IP, se debe considerar que la relación entre nombre FQDN e IP puede cambiar en el tiempo, y que una dirección IP específica puede estar siendo usada por un proveedor de web hosting que puede tener más de un dominio asociado a dicha IP.

En consecuencia, se recomienda tener un orden de prioridades a la hora de ejecutar un bloqueo, considerando al menos:

- El uso de un dispositivo WAF que pueda discriminar el nombre FQDN potencialmente malicioso por sobre la IP.
- El uso de un firewall que permita integrar listas de bloqueo FQDN sin necesitar la conversión a IP.
- El uso de sistemas proxy que permitan bloquear el FQDN sin necesitar la conversión a IP.
- En última instancia, incorporar el bloqueo de la IP verificando que no corresponda a un esquema de web hosting, porque existe la posibilidad de bloquear los restantes dominios implementados que utilizan la misma dirección IP.

Indicadores de Compromiso asociados

Archivos que se encuentran en la amenaza

Tipo	Indicador	Relación
SHA256	33c1a387b8118c12cea6fc5c2673c94a52403e945ba76ac3dbb3a8c4649035f0	documentación-131862.xls
SHA256	f794589c2b118c53894a21943813b43d95b5f9bef158dbda283a8859a7246254	66.xls
SHA256	cf2ca104cce3798296b220e3ea0b749c089dc10011531e0012c0a41a95c7b5d3	DOCUMENTO_02112022.zip
SHA256	b07e769f7508a2e1d35f7d4835893051a08586d33192e4b933d36b0ecb4887f1	Archivo-0411.zip
SHA256	ce868c3cd85acb99df28599fec809e3af99292f996755dbad8038118201bedd0	lista_7491.xls
SHA256	b9eee623a848474899bf25709dc654346c764143d45038ef055220da70119f0f	FAB819888270MC.xls
SHA256	b56305f0d32be944614288f8c27c4410d242eebcf87259cddcf687a37d179f1d	doc_0411.zip
SHA256	d86e1e56338a16cc1789ce68ed1996c2188cc4764f431e16390c46aef791c569	699_9566099.zip
SHA256	370c9603bb9b454372070ee671a62772a69729cb08ac7b58aee51583d7b7f3f0	INFO_8956593.xls
SHA256	ce1df5f23e6126202dc5c2e20b47168c6a06ecab2bebfb71a545d1a800cf0a43	ARCHIVO_6273223699.xls
SHA256	0740ce43cd29acaf8cb96fdbfe414c5a614d953552a5c5cc1faa040465def06e	VIM_8.zip
SHA256	55501764c7388762cb3621027575be215529a78e2d296d6405e24dfccf16c29e	CORREO 0411.zip
SHA256	197a43730f3ff494f025bdd4435a3f92138cb1a85e488507f3f7a31bac368573	comentarios-83686.zip
SHA256	6fc6e50b0d7bedc713908a49db41b4157b6a4016c2be073aa1cbdda824b18643	sC8waWXyWVkP8OOUQSDExaGhXNrIhEpUnPY.dll
SHA256	25fce5f66196997fbbd2991df77a1b035aeef47b7d7f3139aa078b46b000bcbf	uvVpdDj0Fxl99g3c80y.dll
URL	http://www.detertecnica.com/var/azLISfW/	Malware Config
URL	http://demo.cansunoto.com/lYqTuQ0qe5r2Y/	Malware Config
URL	http://cybertech.freeoda.com/ct/go6hL733p4vjEnuu/	Malware Config
URL	http://danoblab.com/wordpress_4/Fw/	Malware Config
URL	http://eznetb.synology.me/@eaDir/7ks2a6g9TV/	Malware Config
URL	http://www.chawkyfrenn.com/icon/BzGzSWFZIZGaTK/	Malware Config
URL	http://royreid.co.uk/wp-content/UIa3o/	Malware Config
URL	http://www.muyehuayi.com/cmp/Vtm2m7z88g/	Malware Config
URL	http://ly.yjlianyi.top/wp-admin/NRAdJ/	Malware Config
URL	http://ftp.agir-santeinternationale.com/doctors/KAacngW97n4ApzVBDdGy/	Malware Config

Recomendaciones

- Los usuarios deberían procurar:
  - No abrir correos ni mensajes de dudosa procedencia.
  - Desconfiar de los enlaces y archivos en los mensajes o correo.
  - Solicitar que sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras) estén actualizadas.
  - Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
  - Prestar atención en los detalles de los mensajes o redes sociales.
  - Solicitar que todas las plataformas de tecnologías y de detección de amenazas estén actualizadas.
  - Siempre intentar verificar que los sitios web que se visitan sean los oficiales.
  - No descargar software que no cuente con la autorización del equipo de informática (cracks, antivirus, utilitarios, juegos, aplicaciones de oficina, etc.).
  - Notificar oportunamente a sus encargados de ciberseguridad para que investiguen el incidente, comprueben si ha llegado a otros usuarios y apliquen las mitigaciones pertinentes. Algunas señales que debieran gatillar un informe inmediato:
    - Mi equipo presenta alto consumo de CPU y de memoria.
    - Accedí a un portal y entregué mis credenciales, y luego me percaté que no era un sitio institucional u oficial.
    - Mis archivos están inaccesibles (parece que están encriptados).
    - En mi computador aparece una nota o mensaje que solicita un rescate por recuperar mis archivos.
    - Mi ejecutivo de finanzas u otras personas dicen que desde mi correo les he enviado un mail y no he sido yo.
- Los administradores deben:
  - Implementar controles anti spoofing (DKIM, SPF y DMARC).
  - Revisar la información que se expone de sus usuarios en sus sitios y sistemas web.
  - Filtrar o bloquear los correos entrantes que sean clasificados como phishing.
  - Evaluar el bloqueo preventivo de los indicadores de compromisos.
  - Revisar los controles de seguridad de los antispam y sandboxing.
  - Instruir a sus usuarios sobre el phishing y ayudarlos a reconocerlos. Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
  - Crear mecanismos amistosos para el reporte y el feedback, en un entorno donde no se busque la culpabilidad, sino que la solución.
  - Implementar 2FA.
  - Proteger a sus usuarios de sitios maliciosos usando proxy servers y manteniendo actualizados sus browsers.
  - Proteger sus dispositivos del malware.
  - Tener un protocolo de respuesta rápido ante estos incidentes.
  - Detectar rápidamente estos incidentes instando a los usuarios a que reporten rápidamente cualquier actividad sospechosa.