Lumu Advisory Alert

Latinoamérica

Septiembre 7, 2020
Alert Number: L-LATAM-04

Lumu ha encontrado un incremento de contactos relacionados con diversos malware, botnets y Ransomware en la región. Este documento contiene información actualizada y relevante acerca de estos casos.

Antecedentes

Se han encontrado múltiples contactos relacionados con las siguientes familias de Malware:

- Mylobot: Es un malware de diversos usos que es conocido por sus avanzadas técnicas de evasión.
- Andromeda: Distribuye Malware desde su centro de comando y control después de infectar las máquinas objetivo.
- Emotet: Inicialmente lanzado como un troyano bancario, actualmente es uno de las principales herramientas para distribución de ataques adicionales incluyendo los troyanos Trickbot, Qakbot y el ransomware Ryuk. Se propaga principalmente a través de correo electrónico
- Maze: Ransomware descubierto en Mayo de 2019
- Nueva herramienta de malware Lazarus: Malware con capacidad de realizar descarga de nuevos archivos y ejecutar comandos. Lazarus se trata de un grupo de cibercrimen también conocido como Hidden Cobra
- Azolrut: Malware especializado en robo de información descubierto en el año 2016.
- Formbook: Malware con diversas capacidades desde robo de información hasta control del sistema infectado.
- Sodinokibi: Ransomware que tiene como objetivo sistemas Windows.

Lumu ha detectado un incremento de contacto a IoCs relacionados con estos malware en todo latinoamérica lo que puede indicar ataques coordinados para afectar diversas industrias, en caso de estar presentando contactos a esta infraestructura un ataque de robo de información o ransomware puede ser inminente.

URLs/IPs comprometidas

Si su infraestructura contacto a los siguiente IOCs siga las recomendaciones descritas en esta alerta:

50.28.51.143	70.32.84.74	111.67.12.221	hxxp://sac.onecenter.com.br
185.94.252.27	212.71.237.140	hxxp://disorderstatus[.]ru	hxxp://mk.bital.com.br
lavinch[.]firewall-gateway[.]de	hxxp://fywkuzp[.]ru	hxxp://updates.updatecenter[.]icu	hxxp://gestao.simtelecomrs.com.br
hxxp://checksoffice[.]me	hxxp://drivers.updatecenter[.]icu	hxxp://plaintsotherest[.]net	hxxp://co.colnhubplus.com

Lumu Advisory Alert

Latinoamérica

Septiembre 7, 2020
Alert Number: L-LATAM-04

Importante

- **Durante el fin de semana, Banco Estado, uno de los 20 bancos más grandes de latinoamérica, anunció públicamente la detección de un "software malicioso" en sus sistemas, el cual ha afectado gravemente sus operaciones. Esto último resalta la importancia de mantener el nivel de atención al máximo en relación con la actividad de contacto con infraestructura adversaria**

Recomendaciones

- Identificar los dispositivos infectados y eliminar cualquier rastro de malware o ransomware.
- Monitorear de manera continua si su infraestructura está intentando realizar contactos a este dominio o urls.
- Mantener backups actualizados en caso de ser infectado con Ransomware
- Mantener antivirus y sistemas operativos actualizados.
- En caso de estar afectado no es suficiente realizar únicamente la mitigación. Identifique los dispositivos afectados y elimine el ransomware.
- Monitorear los equipos remotos de su organización. Aprenda más como hacerlo con Lumu aquí.

Playbooks

Para los casos contenidos en esta alerta los siguientes playbooks contienen pasos detallados para tomar las acciones correspondientes.

Analizar su metadata de red para medir compromiso es muy fácil. Puede empezar hoy abriendo una cuenta gratuita en www.lumu.io