INFORME DEL ADVERSARIO

APT38

ÍNDICE

RESUMEN EJECUTIVO

APT38 es un grupo de ciberdelincuentes financiado por el régimen de Corea del Norte con el objetivo principal de consumar ataques contra los recursos económicos de instituciones y empresas, son responsables de los robos cibernéticos más prolíferos de todo el mundo.

Su modus operandi es similar a una operación de espionaje, donde una vez dentro de la institución comprometida realizan un reconocimiento de la misma para monitorear y aprender de los sistemas internos, para posteriormente cometer un desfalco catastrófico.

Este grupo ha logrado comprometer más de 16 organizaciones en al menos 13 países diferentes, desde al menos 2014.

Desde la detección de su actividad sus operaciones se han vuelto mas sofisticadas y destructivas, esto lo han logrado afinando sus técnicas, tácticas y procedimientos (TTPs) logrando evadir su detección temprana.

PAÍSES ATACADOS

Los países donde han realizado ataques son

1. Estados Unidos
2. Mexico
3. Chile
4. Brazil
5. Uruguay
6. Polonia
7. Turquia
8. Malasia
9. Bangladesh
10. Rusia
11. Vietnam
12. Taiwan
13. Filipinas

ORGANIZACIONES AFECTADAS

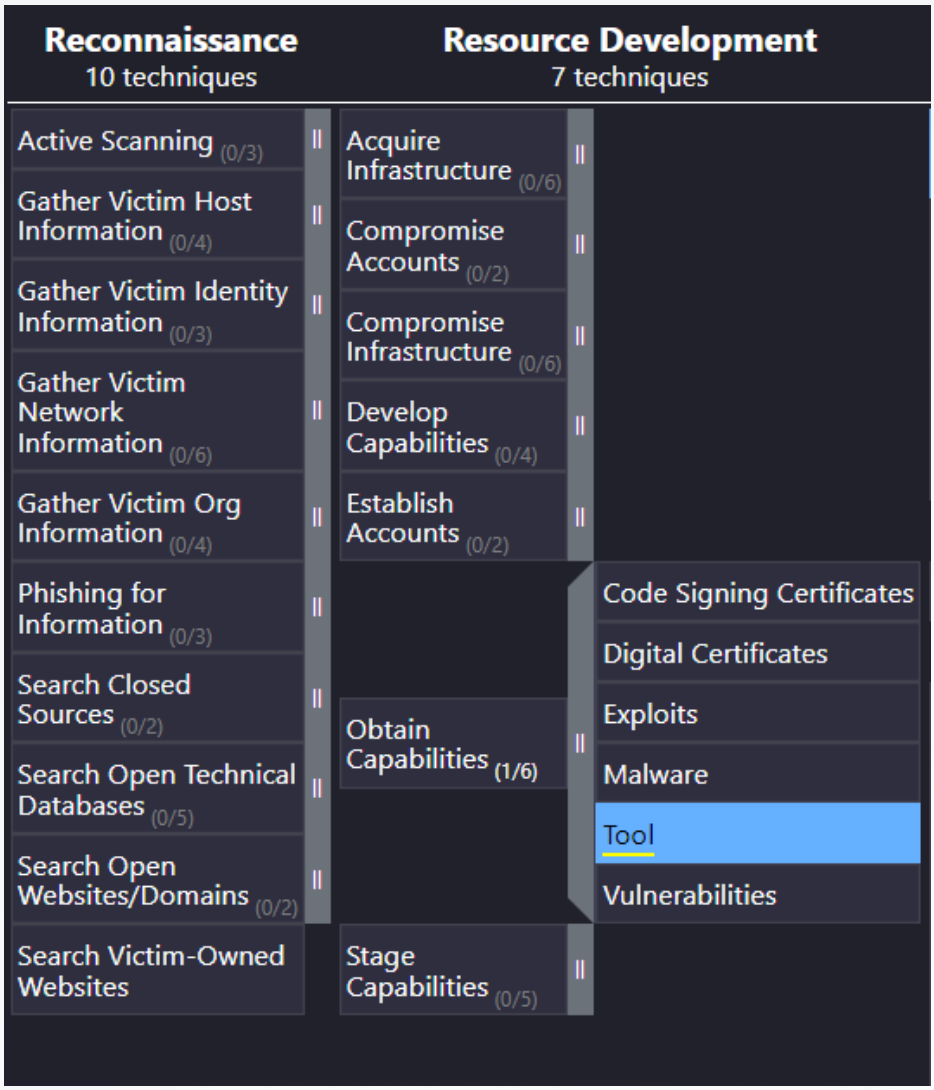
Basado en su actividad las organizaciones que el APT38 tiene como objetivo son instituciones bancarias y financieras, dentro de sus victimas tenemos:

- Vietnam TP Bank - Diciembre 2015
- Bangladesh Bank - Febrero de 2016
- Far Eastern International Bank Taiwan - Octubre 2017
- Bancomext - Enero 2018
- Banco de Chile - Mayo 2018

TTPS MITRE ATT&CK

Podemos ver un extracto del mapeo de sus TTPs a continuación, puede consultar el mapeo completo en el siguiente enlace.

TTPS MITRE ATT&CK APT38



HERRAMIENTAS Y TÉCNICAS USADAS

A continuación se listan herramientas y técnicas empleadas según el ciclo de vida del ataque.

Initial compromise

- Comprometer sitios web
- Acceso a servidores linux, con vulns de Apache Struts2

Establish foothold

- Quickcafe
- Nestegg
- Rawhide
- TightVNC

Escalate privileges

- Sorrybrute
- Mimikatz

Internal recon

- Keylime
- Mapmaker
- Sysmon

Mission complete

- Dyepack
- DarkComet
- Hermes
- Cleantoad
- Clear Windows event log and Sysmon logs

CONCLUSIONES

APT38 es sin duda un adversario letal, con el financiamiento de un régimen autoritario como el de Corea del Norte ha llevado acabo desfalcos importantes a lo largo del mundo, así como mejorado sus técnicas de ataque con procedimientos mas sofisticados con el fin de hacer el mayor daño posible a las entidades financieras del planeta.

Gracias al esfuerzo de empresas que se dedican a cazar este tipo de adversarios en todo el mundo podemos hoy saber la forma en la que opera este grupo delictivo.

RETO 3

Pueden consultar el reto 3 en el siguiente enlace

RETO 3