El grupo de estado-nación iraní conocido como Charming Kitten, está apuntando activamente a múltiples víctimas en Estados Unidos, Europa, Medio Oriente e India, con un nuevo malware denominado Bellaciao, que se suma a su lista en constante expansión de herramientas personalizadas.

Descubierto por Bitdefender Labs, BellaCiao es un *«cuentagotas personalizado»* que es capaz de entregar otras cargas útiles de malware en una máquina víctima en función de los comandos recibidos de un servidor controlado por un hacker.

> *«Cada muestra recolectada estaba vinculada a una víctima específica e incluía información codificada como el nombre de la empresa, subdominios especialmente diseñados o la dirección IP pública asociada»,* dijo la compañía rumana de ciberseguridad, Bitdefender.

Charming Kitten, también conocido como APT35, Cobalt Illusion, Educated Manticore, ITG18, Mint Sandstorm (née Phosphorus), TA453 y Yellow Garuda, es un grupo APT patrocinado por el estado iraní asociado con el Grupo de la Guardia Revolucionaria Islámica (IRGC).

A lo largo de los años, el grupo ha utilizado varios medios para implementar backdoors en sistemas que pertenecen a una amplia gama de industrias verticales.

El desarrollo se produce cuando Microsoft atribuyó al hacker los ataques de represalia dirigidos a entidades de infraestructura crítica en Estados Unidos entre finales de 2021 y mediados de 2022, usando malware a medida como harmPower, Drokbk y Soldier.

Después, a inicios de esta semana, Check Point reveló el uso de Mind Sandstorm en una versión actualizada del implante PowerLess para atacar a organizaciones ubicadas en Israel usando señuelos de phishing como temática de Irak.

> *«El malware desarrollado a medida, también conocido como malware 'a la medida',*

> *generalmente es más difícil de detectar porque está diseñado específicamente para evadir la detección y contiene un código único»,* dijo el investigador de Bitdefender, Martin Zugec.

El modus operandi exacto usado para lograr la intrusión inicial aún no se ha determinado, aunque se sospecha que implica la explotación de vulnerabilidades conocidas en aplicaciones expuestas a Internet como Microsoft Exchange Server o Zoho ManageEngine.

Después de una infracción exitosa, el hacker intenta deshabilitar Microsoft Defender mediante un comando de PowerShell y establece la persistencia en el host por medio de una instancia de servicio.

Bitdefender dijo que también observó a Charming Kitten descargando dos módulos de Internet Information Services (IIS) capaces de procesar instrucciones entrantes y filtrar credenciales.

BellaCiao, por su parte, también se destaca por realizar una solicitud de DNS cada 24 horas para resolver un subdominio en una dirección IP que después se analiza para extraer los comandos que se ejecutarán en el sistema comprometido.

> *«La dirección IP resuelta es como la dirección IP pública real, pero con ligeras modificaciones que permiten a BellaCiao recibir más instrucciones»,* explicó Zugec.

> *«Se comunica con un servidor DNS controlado por un atacante que envía instrucciones codificadas maliciosas a través de una dirección IP resuelta que imita la dirección IP real del objetivo. El resultado es malware adicional que se elimina por medio de instrucciones codificadas en lugar de una descarga tradicional».*

Dependiendo de la dirección IP resuelta, la cadena de ataque conduce a la implementación de un shell web que admite la capacidad de cargar y descargar archivos arbitrarios, así como ejecutar comandos.

También se detectó una segunda variante de BellaCiao que sustituye el shell web por una herramienta Plink, una utilidad de línea de comandos para PuTTY, que está diseñada para establecer una conexión de proxy inverso a un servidor remoto e implementar funciones de backdoor similares.

Se evalúa que los ataques se encuentran en la segunda etapa luego de los ataques oportunistas, en los que BellaCiao se personaliza y despliega contra víctimas de interés cuidadosamente seleccionadas después de la explotación indiscriminada de sistemas vulnerables.

> *«La mejor protección contra los ataques modernos implica implementar una arquitectura de defensa en profundidad. El primer paso en este proceso es reducir la superficie de ataque, lo que implica limitar la cantidad de puntos de entrada que los atacantes pueden usar para obtener acceso a sus sistemas y parchear rápidamente las vulnerabilidades recién descubiertas»*, dijo Zugec.