Backdoor Multi Propósito Amenaza Los Sistemas Windows

Nuevas variantes de malware son mas frecuente últimamente, pero algunos son mas preocupantes que otras versiones.

El último componente de software viene de los investigadores de la empresa de seguridad **Doctor Web,** quienes han descubierto un nuevo troyano llamado **BackDoor.Yebot,** el cual es capaz de llevar a cabo una amplia gama de acciones destructivas en una máquina infectada.

Se ha extendido a través de otro componente de malware, **Trojan.Siggen6.31836**. Cuando se lanzó en la máquina objetivo, este inyecta su código en los **procesos svchost.exe, csrss.exe, lsass.exe y explorer.exe**. Después de enviar una solicitud al servidor remoto, descarga y descifra BackDoor.Yebot y transfiere el control a la misma. Algunas características de Trojan.Siggen6.31836 se cifran y se pueden descifrar sólo mientras se está ejecutando. También incorpora mecanismos para verificar la máquina virtual en un sistema objetivo y el Control de cuentas de usuario, y todo esto afectando los sitemas Windows.

Una vez activo en un sistema, BackDoor.Yebot tiene una gama de capacidades. Puede **ejecutar un servidor FTP** o un servidor proxy SOCKS 5 en un equipo infectado, también puede modificar el protocolo RDP para proporcionar acceso remoto a la máquina.

Tiene la capacidad de registrar las pulsaciones de teclado y puede interceptar actividad de navegación mediante la captura (Perl Compatible Regular Expressions) de Patrones PCRE. Es capaz de inyectar contenido arbitrario en páginas web cargadas en las ventanas del navegador.

Así como el seguimiento e interfiriendo con su navegación puede interceptar varias funciones del sistema, modificar el

código del proceso en ejecución, interactuar con los plug-ins, tomar capturas de pantalla, y la búsqueda en el sistema infectado para claves privadas.

BackDoor.Yebot se comunica con sus servidores C & C utilizando el protocolo HTTP estándar, así como el protocolo binario nativo y tiene la capacidad de usar una lista negra de direcciones IP, con la cual decide cuales están disponibles para conseguir mas trafico.

Analistas de Doctor Web sugieren que BackDoor.Yebot está siendo utilizado como un troyano bancario, pero su gama de habilidades sugiere que ha sido diseñado como una pieza de malware de usos múltiples. Ya se ha añadido a la base de datos de virus Dr.Web y más detalles técnicos sobre la infección se puede encontrar en el sitio web de la compañía.