Nuevas investigaciones revelan que organizaciones de múltiples sectores sensibles —incluidos gobiernos, telecomunicaciones e infraestructura crítica— están copiando y pegando contraseñas y credenciales en herramientas en línea como JSONformatter y CodeBeautify, usadas comúnmente para dar formato y validar código.

La empresa de ciberseguridad watchTowr Labs señaló que recopiló un conjunto de más de 80,000 archivos alojados en estos servicios, descubriendo miles de nombres de usuario, contraseñas, claves de autenticación para repositorios, credenciales de Active Directory, datos de acceso a bases de datos, credenciales FTP, claves de entornos en la nube, información de configuración LDAP, claves de API para helpdesk, claves de API para salas de reuniones, grabaciones de sesiones SSH y una amplia variedad de datos personales.

Esto incluye cinco años de contenido histórico de JSONFormatter y un año de información almacenada en CodeBeautify, sumando más de 5 GB de datos JSON enriquecidos y anotados.

Las organizaciones afectadas pertenecen a sectores de infraestructura nacional crítica, administración pública, finanzas, seguros, banca, tecnología, comercio minorista, aeroespacial, telecomunicaciones, salud, educación, turismo y, paradójicamente, el propio sector de ciberseguridad.

El investigador de seguridad Jake Knott comentó en un informe que *"estas herramientas son extremadamente populares, suelen aparecer en los primeros resultados de búsqueda para términos como 'embellecer JSON' o 'mejor lugar para pegar secretos' (probablemente, sin comprobar), y las utilizan organizaciones, desarrolladores y administradores en entornos empresariales y proyectos personales"*.

```
$install_params= @{
  'installpath'=$install_path
  'admin.external-username'=[redacted]Planview'
  'admin.external-username-password'=$planview_pass_encrypted
  'collector.external-username'=[redacted]Planview'
  'collector.external-password'=$planview_pass_encrypted
  'external.url.name'=$DNS
  'tomcat.host'=${env:ComputerName}
  'admin.db.host'=$rds_host
  'admin.db.master.url'="jdbc:sqlserver://${rds_host}:1433;selectMethod=direct
    ;sendStringParametersAsUnicode=false;responseBuffering=full;databaseName=master"
  'sa.user'=$rds_user
  'sa.password'=$rds_pass_encrypted
  'admin.db.url'="jdbc:sqlserver://${rds_host}:1433;selectMethod=direct
    ;sendStringParametersAsUnicode=false;responseBuffering=full;databaseName=${ctmdb_name}"
  'admin.db.name'=$ctmdb_name
  'admin.db.user'=$ctmdb_user
  'admin.db.password'=$ctmdb_pass_encrypted
  'admin.db.tidm.url'="jdbc:sqlserver://${rds_host}:1433;selectMethod=direct
    ;sendStringParametersAsUnicode=false;responseBuffering=full;databaseName=${tirs_name}"
  'admin.db.tidm.name'=$tirs_name
  'admin.db.tidm.user'=$tirs_user
  'admin.db.tidm.password'=$tirs_pass_encrypted
}
```

Ambas plataformas también permiten guardar estructuras JSON o fragmentos de código con formato, generando un enlace semipermanente que puede compartirse con terceros, lo que implica que cualquiera con acceso al enlace puede ver la información.

Además, estos sitios no solo ofrecen una práctica sección de Enlaces Recientes donde se listan todos los enlaces guardados, sino que también siguen un patrón de URL predecible para los enlaces compartidos, lo que facilita que un actor malicioso pueda recolectar todos los enlaces mediante un rastreador sencillo:

```
https://jsonformatter.org/{id-here}
https://jsonformatter.org/{formatter-type}/{id-here}
https://codebeautify.org/{formatter-type}/{id-here}
```

Algunos ejemplos del tipo de datos filtrados incluyen secretos de Jenkins, una compañía de ciberseguridad exponiendo credenciales cifradas para archivos de configuración sensibles, información KYC (Know Your Customer) asociada a un banco, credenciales AWS de un importante mercado financiero vinculadas a Splunk y credenciales de Active Directory pertenecientes a una entidad bancaria.

Para empeorar aún más la situación, la empresa señaló que cargó claves de acceso falsas de AWS en una de estas herramientas y detectó que actores maliciosos intentaron utilizarlas 48 horas después de haberse guardado. Esto demuestra que la información valiosa expuesta en estos sitios es recopilada y probada activamente por terceros, generando riesgos graves.

Knott añadió que *"principalmente porque alguien ya lo está explotando, y todo esto es realmente, realmente absurdo"*. También afirmó: *"No necesitamos más plataformas de agentes impulsadas por IA; necesitamos menos organizaciones críticas pegando credenciales en sitios web aleatorios"*.

Al ser consultados por The Hacker News, JSONFormatter y CodeBeautify confirmaron que habían desactivado temporalmente la función para guardar contenido, afirmando que están *"trabajando para mejorarla"* e implementando *"medidas mejoradas de prevención de contenido NSFW (Not Safe For Work)"*.

watchTowr afirmó que esta desactivación probablemente ocurrió en respuesta a su investigación. "Sospechamos que este cambio se implementó en septiembre tras las comunicaciones con varias de las organizaciones afectadas que alertamos", agregaron.