Descubren malware sigiloso para Linux que no fue detectado en 3 años

Autor: I. Stepanenko

Fecha: Friday 14th of May 2021 09:16:15 AM

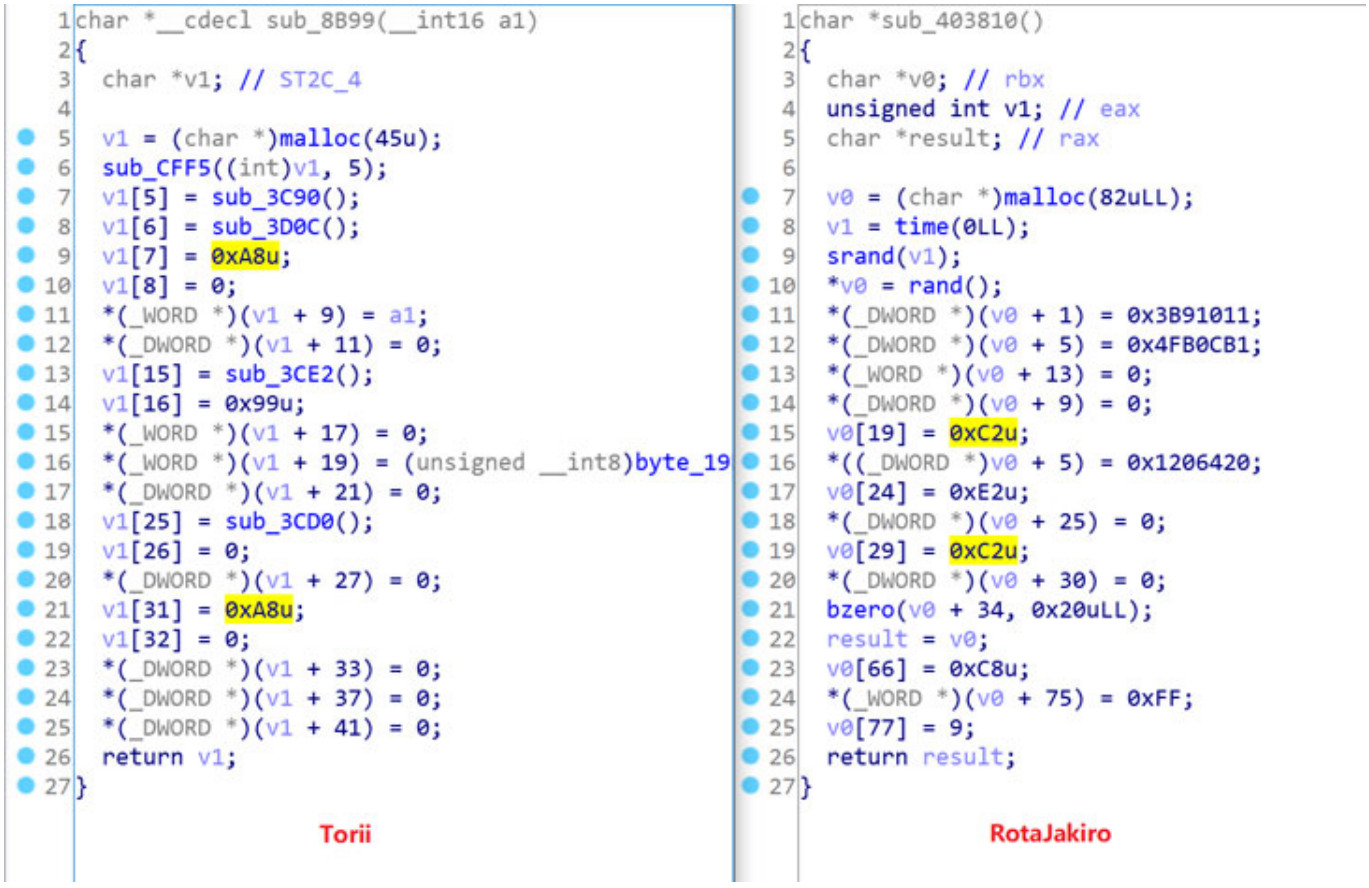
Un malware para Linux previamente indocumentado con capacidades de puerta trasera, ha logrado permanecer bajo el rada durante aproximadamente 3 años, lo que permite a los piratas informáticos detrás de la operación recolectar y exfiltrar información confidencial de los sistemas infectados.

Nombrado RotaJakiro por investigadores de Qihoo 360 NETLAB, la backdoor apunta a máquinas Linux X64 y se llama así por el hecho de que *«la familia usa cifrado rotativo y se comporta de forma deficiente para cuentas root/no root cuando se ejecuta».*

Los hallazgos provienen de un análisis de una muestra de malware que fue detectada el 25 de marzo, aunque las primeras versiones parecen haber sido subidas a VirusTotal en mayo de 2018. Un total de cuatro muestras se han encontrado hasta la fecha en la base de datos, todos los cuales permanecen sin ser detectados por la mayoría de los motores anti malware. Hasta ahora, solo siete proveedores de seguridad señalan la última versión del malware

como maliciosa.

> «A nivel funciona, RotaJakiro primero determina si el usuario es root o no root en tiempo de ejecución, con diferentes políticas de ejecución para distintas cuentas, luego descifra los recursos sensibles relevantes usando AES & ROTATE para la subsiguiente persistencia, protección de procesos y uso de instancia única, y finalmente establece comunicación con C2 y espera la ejecución de los comandos emitidos por C2», dijeron los investigadores.



```
1 char *__cdecl sub_8B99(__int16 a1)
2 {
3   char *v1; // ST2C_4
4
5   v1 = (char *)malloc(45u);
6   sub_CFF5((int)v1, 5);
7   v1[5] = sub_3C90();
8   v1[6] = sub_3D0C();
9   v1[7] = 0xA8u;
10  v1[8] = 0;
11  *(_WORD *)(v1 + 9) = a1;
12  *(_DWORD *)(v1 + 11) = 0;
13  v1[15] = sub_3CE2();
14  v1[16] = 0x99u;
15  *(_WORD *)(v1 + 17) = 0;
16  *(_WORD *)(v1 + 19) = (unsigned __int8)byte_19
17  *(_DWORD *)(v1 + 21) = 0;
18  v1[25] = sub_3CD0();
19  v1[26] = 0;
20  *(_DWORD *)(v1 + 27) = 0;
21  v1[31] = 0xA8u;
22  v1[32] = 0;
23  *(_DWORD *)(v1 + 33) = 0;
24  *(_DWORD *)(v1 + 37) = 0;
25  *(_DWORD *)(v1 + 41) = 0;
26  return v1;
27 }
```

Torii

```
1 char *sub_403810()
2 {
3   char *v0; // rbx
4   unsigned int v1; // eax
5   char *result; // rax
6
7   v0 = (char *)malloc(82uLL);
8   v1 = time(0LL);
9   srand(v1);
10  *v0 = rand();
11  *(_DWORD *)(v0 + 1) = 0x3B91011;
12  *(_DWORD *)(v0 + 5) = 0x4FB0CB1;
13  *(_WORD *)(v0 + 13) = 0;
14  *(_DWORD *)(v0 + 9) = 0;
15  v0[19] = 0xC2u;
16  *((_DWORD *)v0 + 5) = 0x1206420;
17  v0[24] = 0xE2u;
18  *(_DWORD *)(v0 + 25) = 0;
19  v0[29] = 0xC2u;
20  *(_DWORD *)(v0 + 30) = 0;
21  bzero(v0 + 34, 0x20uLL);
22  result = v0;
23  v0[66] = 0xC8u;
24  *(_WORD *)(v0 + 75) = 0xFF;
25  v0[77] = 9;
26  return result;
27 }
```

RotaJakiro

RotaJakiro está diseñado pensando en el sigilo, confiando en una combinación de algoritmos criptográficos para encriptar sus comunicaciones con un servidor de comando y control, además de tener soporte para 12 funciones que se encargan de recopilar metadatos del

dispositivo, robando información sensible, realizar operaciones relacionadas con archivos y descargar y ejecutar complementos extraídos del servidor C2.

Pero sin evidencia que arroje luz sobre la naturaleza de los complementos, la verdadera intención detrás de la campaña de malware sigue sin estar clara. Curiosamente, algunos de los dominios C2 se registraron desde diciembre de 2015, y los investigadores también observaron superposiciones entre RotaJakiro y una botnet llamada Torii.

> «Desde la perspectiva de la ingeniería inversa, RotaJakiro y Torii comparten estilos similares: el uso de algoritmos de cifrado para ocultar recursos sensibles, la implementación de un estilo de persistencia bastante anticuado, tráfico de red estructurado, etc. No sabemos exactamente la respuesta, pero parece que RotaJakiro y Torii tienen algunas conexiones», dijeron los investigadores.