Declaraciones de Kaspersky Lab acerca del ataque WannaCry

- El 12 de mayo, un ataque de ransomware masivo fue desencadenado, afectando a organizaciones de todo el mundo. Los investigadores de Kaspersky Lab han analizado los datos y pueden confirmar que los subsistemas de protección de la compañía detectaron al menos 45.000 intentos de infección en 74 países, la mayoría de ellos en Rusia.

  Este ransomware infecta a las víctimas explotando una vulnerabilidad de Microsoft Windows descrita y corregida en el Boletín de Seguridad de Microsoft MS17-010. El exploit utilizado, "Eternal Blue", fue revelado por Shadowbrokers el 14 de abril.

  Una vez dentro del sistema, los atacantes instalan un rootkit, que les permite descargar el software para cifrar los datos. El malware cifra los archivos. Una solicitud de $ 600 en Bitcoin se muestra junto a una billetera - y la demanda de rescate aumenta con el tiempo.

  Los expertos de Kaspersky Lab están actualmente tratando de determinar si es posible descifrar los datos bloqueados en este ataque con el objetivo de desarrollar una herramienta de descifrado tan pronto como sea posible.

  Las soluciones de seguridad de Kaspersky Lab detectan el malware utilizado en este ataque por los siguientes nombres de detección:

- Trojan-Ransom.Win32.Scatter.uf
- Trojan-Ransom.Win32.Scatter.tr
- Trojan-Ransom.Win32.Fury.fr
- Trojan-Ransom.Win32.Gen.djd
- Trojan-Ransom.Win32.Wanna.b
- Trojan-Ransom.Win32.Wanna.c
- Trojan-Ransom.Win32.Wanna.d
- Trojan-Ransom.Win32.Wanna.f
- Trojan-Ransom.Win32.Zapchast.i
- Trojan.Win64.EquationDrug.gen
- Trojan.Win32.Generic (el componente System Watcher del sistema debe estar habilitado)

  Recomendamos tomar las siguientes medidas para reducir el riesgo de infección:

  • **Instale el parche oficial de Microsoft que cierra la vulnerabilidad utilizada en el ataque**
  • Asegúrese de que las soluciones de seguridad estén habilitadas en todos los nodos de la red

• Si utiliza la solución de Kaspersky Lab, asegúrese de que incluya el System Watcher, un componente de detección proactivo de comportamiento y que esté habilitado
• Ejecute el Scan de Área Critica en la solución de Kaspersky Lab para detectar una posible infección lo antes posible (de lo contrario, se detectará automáticamente dentro de 24 horas, si no se deshabilita).
• Reinicie el sistema después de detectar MEM: Trojan.Win64.EquationDrug.gen
• Utilice los servicios de Reportes de Inteligencia de Amenazas específicos para clientes

Una descripción detallada del método de ataque de WannaCry y los Indicadores de Compromiso se pueden encontrar en Securelist:
https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/