Hive Pro

THREAT ADVISORY

Russia under Attack from New RURansom Wiper	TA2022060

Threat Level	RED	Publish Date – Mar 16, 2022

A series of Wiper Malware attacks have been launched in the continuing cyber war between Russia and Ukraine. Researchers have discovered the RURansom wiper malware, which adds to the current collection of harmful malware.

The RURansom malware traces the IP location of the victim machine and is executed only if it detects an IP belonging to Russia. If the malware does not get Admin privileges, it tries to execute itself in the elevated mode using a PowerShell command. The RURansom wiper malware proceeds to scan the drives, the removable and network drives and then encrypt the victim's system using AES-CBC encryption. The malware renames itself as Россия-Украина_Война-Обновление.doc.exe (Russia-Ukraine_War-Update.doc.exe) and spreads as worm to all connected systems. The files encrypted by the RURansom wiper malware are irreversible.

The Organizations can mitigate the risk by following the recommendations:

- Use multi-factor authentication.
- Keep all operating systems and software up to date.
- Remove unnecessary access to administrative shares.
- Maintain offline backups of data and Ensure all backup data is encrypted and immutable.
- Enable protected files in the Windows Operating System for critical files.

The MITRE TTPs commonly used by **RURansom** are:

T1204: User Execution
T1518: Security Software Discovery
T1087: Account Discovery
T1083: File and Directory Discovery
T1485: Data Destruction
T1486: Data Encrypted for Impact
T1565: Data Manipulation

Indicators of Compromise (IoCs)

Type	Value
MD5	6cb4e946c2271d28a4dee167f274bb80, fe43de9ab92ac5f6f7016ba105c1cb4e, 9c3316a9ff084ed4d0d072df5935f52d, 191e51cd0ca14edb8f06c32dcba242f0, 01ae141dd0fb97e69e6ea7d6bf22ab32, 8fe6f25fc7e8c0caab2fdca8b9a3be89
SHA-1	0bea48fcf825a50f6bf05976ecbb66ac1c3daa6b, 27a16e1367fd3e943a56d564add967ad4da879d8, c6ef59aa3f0cd1bb727e2464bb728ab79342ad32, fbeb9eb14a68943551b0bf95f20de207d2c761f6, c35ab665f631c483e6ec315fda0c01ba4558c8f2, a30bf5d046b6255fa2c4b029abbcf734824a7f15
SHA-256	979f9d1e019d9172af73428a1b3cbdff8aec8fdbe0f67cba48971a36f5001da9, 8f2ea18ed82085574888a03547a020b7009e05ae0ecbf4e9e0b8fe8502059aae, 696b6b9f43e53387f7cef14c5da9b6c02b6bf4095849885d36479f8996e7e473, 610ec163e7b34abd5587616db8dac7e34b1aef68d0260510854d6b3912fb0008, 1f36898228197ee30c7b0ec0e48e804caa6edec33e3a91eeaf7aa2c5bbb9c6e0, 107da216ad99b7c0171745fe7f826e51b27b1812d435b55c3ddb801e23137d8f

References

https://blog.cyble.com/2022/03/11/new-wiper-malware-attacking-russia-deep-dive-into-ruransom-malware/