Hive Pro

THREAT ADVISORY

MoonBounce: New malware deployed by APT41 in UEFI firmware

TA2022017

Threat Level RED

Publish Date – Jan 25, 2022

MoonBounce is a new type of malware that hides in the most complex part of an Operating System (OS), the Basic Input Output System (BIOS) chip, and thus persists even after reinstalling your OS or formatting your hard drive.

MoonBounce is the most advanced malware up till today that implants malicious code into the motherboard's Serial Peripheral Interface (SPI) Flash and has a complicated attack surface as well as greater technical sophistication. It can also execute remotely. MoonBounce belongs to the famous Chinese actor APT41.

Organizations are recommended to take these actions:

- Keep UEFI firmware updated directly from the manufacturer,
- Verify that BootGuard is enabled when available
- Enable Trust Platform Modules
- Run regular scans on system firmware for issues

The TTPs used by MoonBounce includes:

TA0040 - Impact
TA0009 - Collection
TA0006 - Credential Access
TA0002 - Execution
TA0005 - Defense Evasion
TA0004 - Privilege Escalation
TA0011 - Command and Control
TA0007 - Discovery
TA0008 - Lateral Movement
T1495 - Firmware Corruption
T1056 - Input Capture
T1059 - Command and Scripting Interpreter
T1014 - Rootkit
T1055 - Process Injection
T1496 - Resource Hijacking
T1102 - Web Service
T1049 - System Network Connections Discovery
T1007 - System Service Discovery
T1021 - Remote Services
T1047 - Windows Management Instrumentation
T1070 - Indicator Removal on Host
T1140 - Deobfuscate/Decode Files or Information

Actor Detail

Name	Known As	Origin	Target Locations	Target sectors
APT41	Double Dragon, TG-2633, Bronze Atlas , Red Kelpie, Blackfly, Earth Baku, SparklingGoblin, Grayfly	China	Australia, Bahrain, Brazil, Canada, Chile, Denmark, Finland, France, Georgia, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Myanmar, Netherlands, Pakistan, Philippines, Poland, Qatar, Saudi Arabia, Singapore, South Korea, South Africa, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	Construction, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Hospitality, Manufacturing, Media, Oil and gas, Petrochemical, Pharmaceutical, Retail, Telecommunications, Transportation, Online video game companies

Indicators of Compromises(IoCs)

Type	Value
MD5	D94962550B90DDB3F80F62BD96BD9858, C3B153347AED27435A18E789D8B67E0A, 4D5EB9F6F501B4F6EDF981A3C6C4D6FA, E7155C355C90DC113476DDCF765B187D, 899608DE6B59C63B4AE219C3C13502F5, 4EF90CEEF2CC9FF3121B34A9891BB28D, CFF2772C44F6F86661AB0A4FFBF86833, 5F9020983A61446A77AF1976247C443D, 0603C8AAECBDC523CBD3495E93AFB20C, 8C7598061D1E8741B8389A80BFD8B8F5, F9F9D6FB3CB94B1CDF9E437141B59E16, 5FE6CE9C48D0AE98EC2CA1EC9759AAD9, 50FF717A8E3106DDBF00FB42212879C5, D98614600775781673B6DF397CC4F476, C9B250099E2DD27BB4170836AC480FE0, 97EF7B8FCDCB0C0D9FBB93D0F7E6E3B6, 4E4388D7967E0433D400C60475974D50, 5F1C7602688E67F299F5BD533FA07880, 45E862964EF4EFDEA181F3927D20E96D, 4BC82105403974AA24BF02CFB66B8F7C
File Names	wbwkem.dll, wkbem.dll , wmiwk.dll , C_20344.nls, C_20334.nls, compwm.bin , pcomnl.bin , wmipl.dll , Microsoft.Service.Watch.targets, MstUtil.exe.config , System.Mail.Service.dll , schtask.bat , CmluaApi.dll
Domain	mb.glbaitech.com, ns.glbaitech.com, dev.kinopoisksu.com, st.kinopoisksu.com, m.necemarket.com, holdmem.dbhubspi.com
Mutexes	Global\GouZUAkmtdpUmves, Global\PtUojBxCOZGVmQQn, Global\EGuUCpyYIJRTQJAV, Global\YCtiqMgRrpLGbfDo
URL	http://mb.glbaitech.com/mboard.dll

Type	Value
IPV4	188.166.61.146, 172.107.231.236, 193.29.57.161, 136.244.100.127, 217.69.10.104, 92.38.178.246, 172.105.94.67, 5.188.93.132, 5.189.222.33, 5.183.103.122, 5.188.108.228, 45.128.132.6, 92.223.105.246, 5.183.101.21, 5.183.101.114, 45.128.135.15, 5.188.108.22, 70.34.201.16

References

https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/
https://otx.alienvault.com/pulse/61ea8f0fe72ea3d1783f483a/
https://www.tomshardware.com/news/moonbounce-malware-hides-in-your-bios-chip-persists-after-drive-formats