Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

Worok cyber-espionage gang preys on high-profile Asian businesses and governments

Date of Publication	Admiralty code	TA Number
September 8, 2022	A1	TA2022195

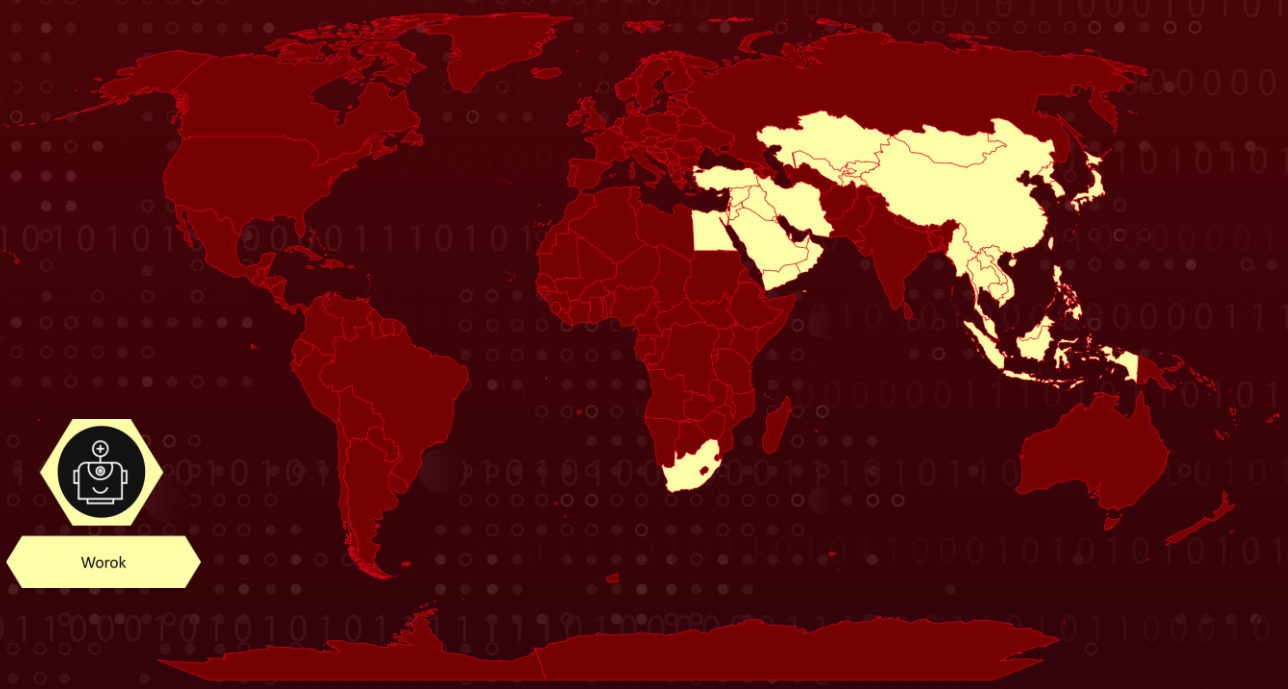
Summary

Worok, a newly uncovered cyber-espionage gang, has been targeting governments and high-profile companies in Asia since at least 2020 using a combination of unique and existing harmful tools. This group of attackers has attacked companies in Asia from the energy, banking, maritime, and telecommunications industries, as well as a government agency in the Middle East and a private firm in South Africa.

CVE Table

CVE	NAME	PATCH
CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability	✓

Actor Map



Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**T1592** Gather Victim Host Information	**T1592.002** Software	**T1592.001** Hardware
T1590 Gather Victim Network Information	**T1590.005** IP Addresses	**TA0042** Resource Development	**T1583** Acquire Infrastructure
T1583.004 Server	**T1583.001** Domains	**T1588** Obtain Capabilities	**T1588.002** Tool
T1588.005 Exploits	**T1587** Develop Capabilities	**T1587.001** Malware	**T1587.003** Digital Certificates
TA0002 Execution	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**TA0003** Persistence
T1505 Server Software Component	**T1505.003** Web Shell	**TA0005** Defense Evasion	**T1140** Deobfuscate/Decode Files or Information
T1036 Masquerading	**T1036.005** Match Legitimate Name or Location	**TA0006** Credential Access	**T1003** OS Credential Dumping
T1003.001 LSASS Memory	**TA0007** Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1046 Network Service Discovery	**T1124** System Time Discovery	**TA0009** Collection	**T1005** Data from Local System
T1560 Archive Collected Data	**T1560.002** Archive via Library	**TA0011** Command and Control	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1090** Proxy	**T1090.001** Internal Proxy	**T1001** Data Obfuscation
T1001.002 Steganography	**T1573** Encrypted Channel	**T1573.002** Asymmetric Cryptography	**T1095** Non-Application Layer Protocol
T1132 Data Encoding	**T1132.001** Standard Encoding	**T1132.002** Non-Standard Encoding	**TA0010** Exfiltration
T1041 Exfiltration Over C2 Channel			

Technical Details

#1

The initial screening into the target network required the employment of ProxyShell exploits (CVE-2021-34523) in certain instances, accompanied by the deployment of additional tailored backdoors for persistent access. Worok's arsenal includes a C++ loader, a PowerShell backdoor, and a C# loader that employs steganography to extract concealed malicious payloads from PNG files.

#2

Once access is gained, a variety of publicly available reconnaissance tools such as Mimikatz, EarthWorm, ReGeorg, and NBTscan are employed. After which a customized implant is deployed: a first-stage loader is a PowerShell backdoor called "PowHeartBeat" that is masked with techniques like compression, encoding, and encryption.

#3

The second stage loader called "PNGLoad" creates a payload to execute using bytes from PNG files. It is a 64-bit .NET executable that is obfuscated using .NET Reactor and masquerades as legitimate software to communicate with a remote server through HTTP or ICMP to execute arbitrary instructions, send and receive files, and perform associated file operations

Actor Detail

NAME	ORIGIN	TARGET LOCATIONS	TARGET INDUSTRIES
Worok	Unknown	Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen, China, Hong Kong, Macau, Japan, Mongolia, North Korea, South Korea, Taiwan, BruneiCambodia, East Timor, Indonesia,Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam, Kazakhstan, Kyrgyzstan, Tajikistan , Uzbekistan, South Africa	energy, financial, bank, maritime, government, public sector and Telecommunications
	MOTIVE		
	Information theft and espionage		

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2021-34523	Microsoft Exchange Server: 2013,2016 and 2019,	cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*	CWE-287

Indicator of Compromise (IOC)

TYPE	VALUE
SHA1	3A47185D0735CDECF4C7C2299EB18401BFB328D5 27ABB54A858AD1C1FF2863913BDA698D184E180D 678A131A9E932B9436241402D9727AA7D06A87E3 757ABA12D04FD1167528FDD107A441D11CD8C427 54700A48D934676FC698675B4CA5F712C0373188 C2F53C138CB1B87D8FC9253A7088DB30B25389AF C2F1954DE11F72A46A4E823DE767210A3743B205 CE430A27DF87A6952D732B4562A7C23BEF4602D1 EDE5AB2B94BA85F28D5EE22656958E4ECD77B6FF 4721EEBA13535D1EE98654EFCE6B43B778F13126 728A6CB7A150141B4250659CF853F39BFDB7A46C 864E55749D28036704B6EA66555A86527E02AF4A 8DA6387F30C584B5FD3694A99EC066784209CA4C AA60FB4293530FBFF00D200C0D44EEB1A17B1C76 B2EAEC695DD8BB518C7E24C4F37A08344D6975BE CDB6B1CAFEE098615508F107814179DEAED1EBCF 4F9A43E6CF37FF20AE96E564C93898FDA6787F7D F181E87B0CD6AA4575FD51B9F868CA7B27240610 4CCF0386BDE80C339EFE0CC734CB497E0B08049C 5CFC0D776AF023DCFE8EDED5CADA03C6D7F9C244
File Path	C:\Program Files\VMware\VMware Tools\ C:\Program Files\VMware\VMware Tools\VMware VGAuth\readme.txt C:\Program Files\VMware\VMware Tools\VMware VGAuth\VMWSU_V1_1.dll C:\Program Files\WinRar\ C:\Program Files\WinRar\rarinstall.log C:\Program Files\WinRar\des.dat C:\Program Files\UltraViewer\ C:\Program Files\UltraViewer\CopyRights.dat C:\Program Files\UltraViewer\uvcr.dll

TYPE	VALUE
IPV4	118.193.78[.]22 118.193.78[.]57 5.183.101[.]9 45.77.36[.]243
Mutex	aB82UduGX0EX ad8TbUIZI5Ga Mr2PJVxbIBD4 oERiQtKLgPgK U37uxsCsA4Xm Wo0r0KGWhYGO xBUjQR2vxYTz zYCLBWekRX3t 3c3401ad-e77d-4142-8db5-8eb5483d7e41 9xvzMsaWqxMy
Domains	airplane.travel-commercials[.]agency central.suhypercloud[.]org

Patch Links

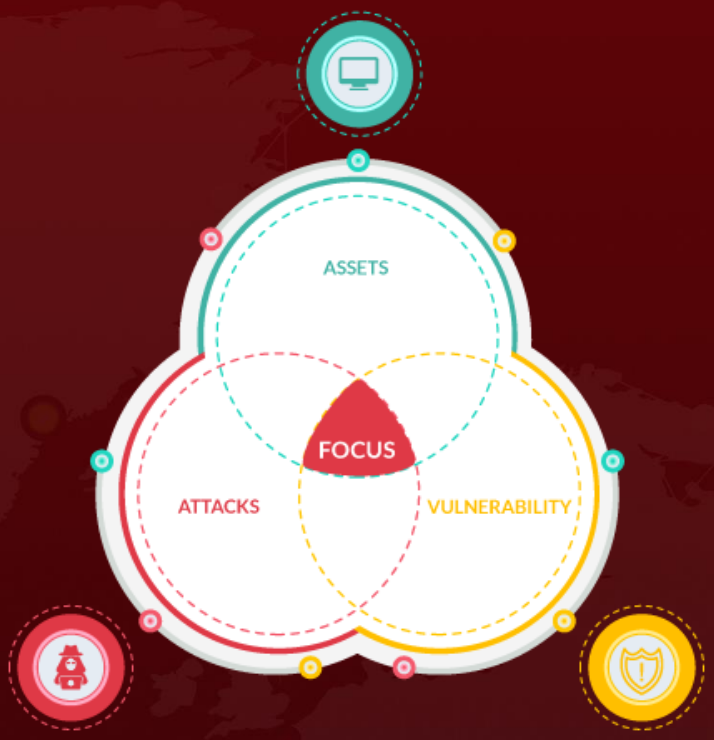
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523

References

https://www.welivesecurity.com/2022/09/06/worok-big-picture/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 8, 2022 . 3:04 AM

More at www.hivepro.com