Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

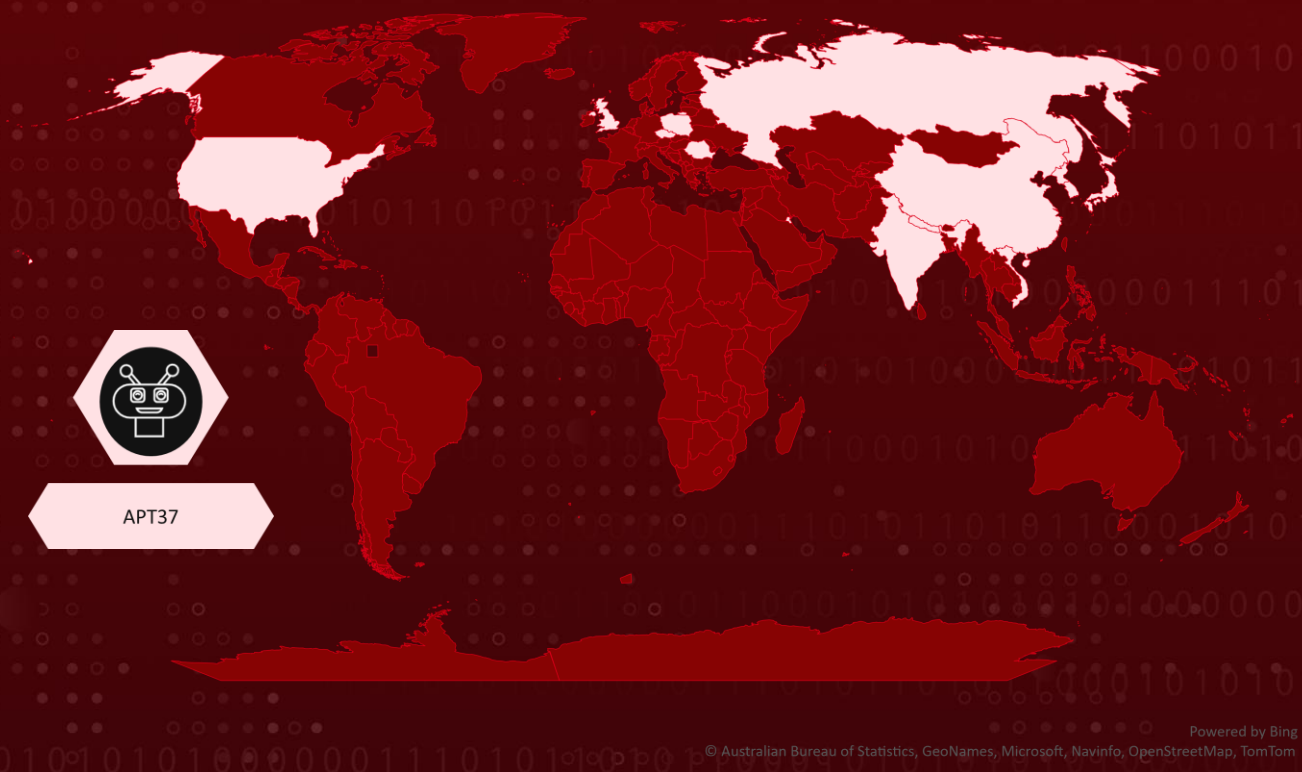
APT37 employs Konni malware to target high-level organizations.

Date of Publication	Admiralty code	TA Number
July 29, 2022	A3	TA2022160

Summary

The Konni remote access trojan, which is widely used malware by the APT37, is used in the attack campaign to take advantage of high-value targets from countries like the Czech Republic, Poland, and many others. The malware includes a built-in functionality to maintain persistence and privilege escalation on the target system.

Actor Map



Potential MITRE ATT&CK TTPs

T1560.003 Archive via Custom Method	**T1113** Screen Capture	**T1119** Automated Collection	**TA0011** Command and Control
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1132** Data Encoding	**T1132.001** Standard Encoding
T1105 Ingress Tool Transfer	**TA0010** Exfiltration	**T1020** Automated Exfiltration	**T1041** Exfiltration Over C2 Channel

TA0001 Initial Access	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**TA0002** Execution
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell	**T1059.005** Visual Basic
T1053 Scheduled Task/Job	**T1053.005** Scheduled Task	**T1569** System Services	**T1569.002** Service Execution
T1204 Malicious File	**T1204.002** User Execution	**TA0003** Persistence	**T1543** Create or Modify System Process
T1543.003 Windows Service	**TA0004** Privilege Escalation	**T1134** Access Token Manipulation	**T1134.001** Token Impersonation/Theft
TA0005 Defense Evasion	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control	**T1070** Indicator Removal on Host
T1070.004 File Deletion	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools	**TA0006** Credential Access
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1606** Forge Web Credentials	**T1606.001** Web Cookies
T1539 Steal Web Session Cookie	**TA0007** Discovery	**T1082** System Information Discovery	**T1057** Process Discovery
T1007 System Service Discovery	**T1033** System Owner/User Discovery	**TA0009** Collection	**T1560** Archive Collected Data

Technical Details

#1 The threat actor targets victims through phishing emails that contain a malicious attachment archive containing the files "missile.docx" and "_weapons.doc.lnk.". Once opened, the code gets executed to run a base64-encoded PowerShell script in the DOCX file to establish C2 communication and download two files, 'weapons.doc' and 'wp.vbs'.

#2 In the background, a VBS file keeps running to establish a scheduled task called "Office Update." The intruder eventually launches the RAT, capable of exfiltrating captured screenshots, state keys, and saved credentials from the victim's web browsers.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
APT 37 (Reaper, TEMP.Reaper, Ricochet Chollima, ScarCruft, Thallium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)	North Korea	Information theft and espionage	China, Hong Kong, India, Japan, Kuwait, Nepal, Romania, Russia, South Korea, UK, USA, Vietnam, Czech Republic, Poland, North Korea	Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation, Defense, Education

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	07b10c5a772f6f3136eb58a7034bcb5ce71c0c740aaa528d3bae318d939b2242, 5d28072d76bd6af944fcec8045cbc24410a58fe70eef6f83c50934245ec92e60, b9727fb553894d857900c0a18f82723659d136329ef56bbe9388905a666f1197, 12df9753abd867118ce97e6570c2bde780c7913ecab4b91ef7f540c4fede2772, 6f325fb0a7de6f05490f1eb3c0e5826a44a11ed2dee4c17f486b8200f539d49e, 35d38eed9168c16d2dd595fa9542a411080d12de971ea3d3c12dd5c44e454049, 31a9801e5e2e5fd7f66f23bc8456069b6a958e03838e431ccf7d84867f88c840, 5fce9f27326549cc6091ba1f806e7c161878a2642411a941ba484b0c1c7adb8f, 9f27430ed919e74c81b0487542fe29a65a0b860a6a290e3b032f3a5ba7c691bc, b6987a717741329d5b64f769c9d3f1f572b42c7375dd841aecbf2b6d4096d6de, dee7826f5b7f0cbc97a81de8f6844a011cc836269bc5d00a0594dfec5386613c, 44566d506e0348c999a66ee5158b0014a74bdd3f038e40ca76e5b069b8991f85, 9c82477eac14abfb7f507806a941e4e5633dd07c4b73a44b10296ec28e3df162, 5f3483823342318c4154bbef806cec2187a0360f079237a456603896ff7f5473
IPV4	185[.]176.43.106

References

https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a 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

July 29, 2022 • 4:00 AM

More at www.hivepro.com