Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

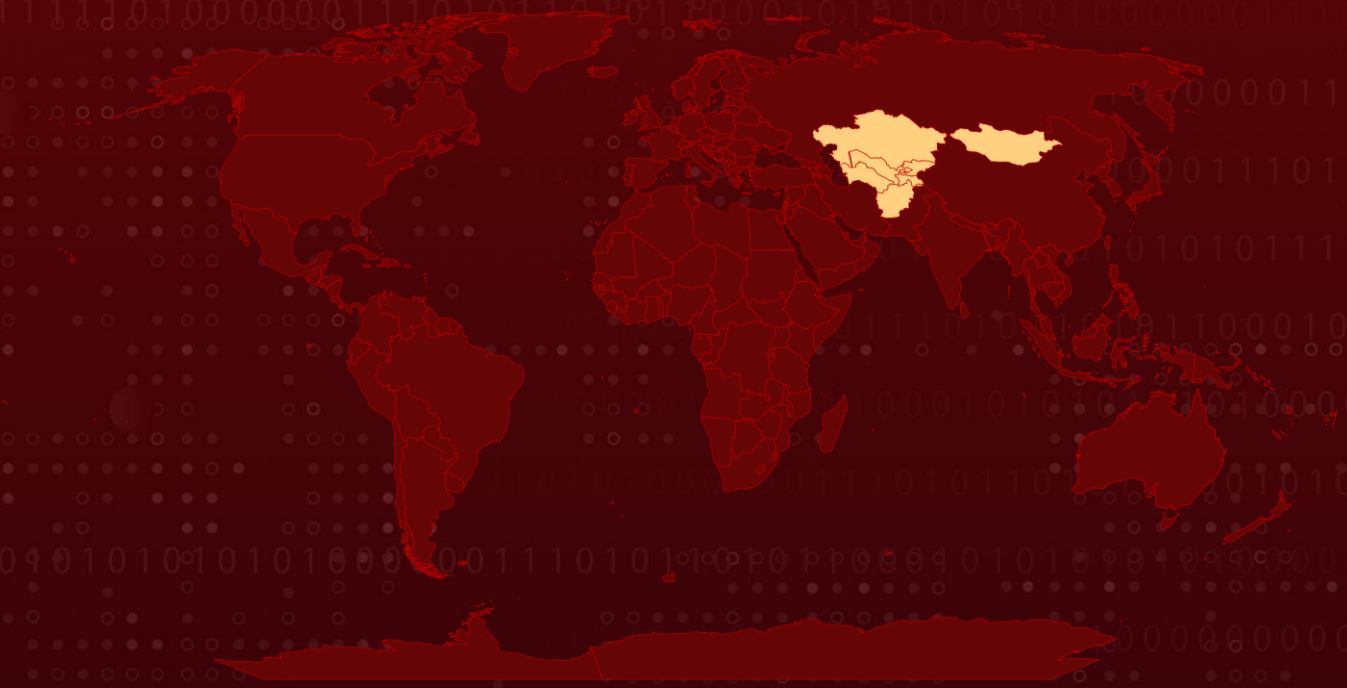
New DownEx Malware Campaign Targets Foreign Government Institutions in Central Asia

Date of Publication	Admiralty Code	TA Number
May 11, 2023	A1	TA2023224

Summary

First Appearance: February 15, 2022
Malware: DownEx
Targeted Countries: Central Asia
Affected Platforms: Windows
Attack: The DownEx malware was discovered in a cyberattack on government institutions in Kazakhstan and Afghanistan in 2022, likely with state sponsorship. The attackers used spear-phishing emails to infiltrate systems with a malicious payload.

Attack Regions



Attack Details

#1 In late 2022, a targeted cyberattack on foreign government institutions in Kazakhstan. Upon further investigation, it was determined that this was a highly targeted attack aimed at exfiltrating data. The malware used in this attack is a new family named DownEx, and there is some evidence pointing to a state-sponsored group based in Russia as the attacker, but attribution remains unclear.

#2 The initial infection vector was most likely a spear-phishing email with a malicious attachment that masqueraded as a Microsoft Word document. Once executed, the malware extracted a Word document as a disguise and a HTA file with embedded VBScript code that served as a loader for the main payload. Although the download of the next stage failed, the attackers used other tools and scripts located on the victim's machine to establish a connection with their command and control infrastructure.

#3 Two tools written in C/C++ designed to enumerate all the resources on a network were discovered, along with a Python-based backdoor that was protected by PyArmor and Themida software protection tools. The script generated an RSA public/private key pair of 2048 bits, and the public key was shared with the C2 server using a POST method.

Recommendations

Spear-phishing emails with malicious attachments are a common initial infection vector for DownEx. The attackers disguise the attachment as a legitimate Microsoft Word document to trick the victim into executing the malware.

Deploying multiple layers of security controls such as antivirus, firewalls, and intrusion detection systems can help detect and block malicious activity. Implementing application whitelisting can also help prevent the unauthorized execution of unknown programs

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
T1574.002 DLL Side-Loading	T1106 Native API	T1569 System Services	T1027 Obfuscated Files or Information
T1204.002 Malicious File	T1140 Deobfuscate/Decode Files or Information	T1086 System Information Discovery	T1113 Screen Capture
T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1106 Native API
T1190 Exploit Public-Facing Application	T1059.006 Python	T1574 Hijack Execution Flow	T1552.004 Private Keys
T1566 Phishing	T1566.001 Spearphishing Attachment	T1036 Masquerading	T1204 User Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	net-certificate[.]services
IPV4	139.99.126[.]38 84.32.188[.]123 206.166.251[.]216

TYPE	VALUE
MD5	1e46ef362b39663ce8d1e14c49899f0e bb7cf346c7db1c518b1a63c83e30c602 a45106470f946ea6798f7d42878cff51 3ac42f25df0b600d6fc9eac73f011261 14a8aad94b915831fc1d3a8e7e00a5df 457eca2f6d11dd04ccce7308c1c327b7 d310a9f28893857a0dc1f7c9b624d353 d20e4fffbac3f46340b61ab8f7d578b1 5602da1f5b034c9d2d6105cdc471852b 89f15568bc19cc38caa8fd7efca977af ae5d4b9c1038f6840b563c868692f2aa c273cdfcfd808efa49ec0ed4f1c976e0 d11fcd39a30a23176337847e54d7268c 70e4305af8b00d04d95fba1f9ade222d 1492b0079b04eb850279114b4361f10c

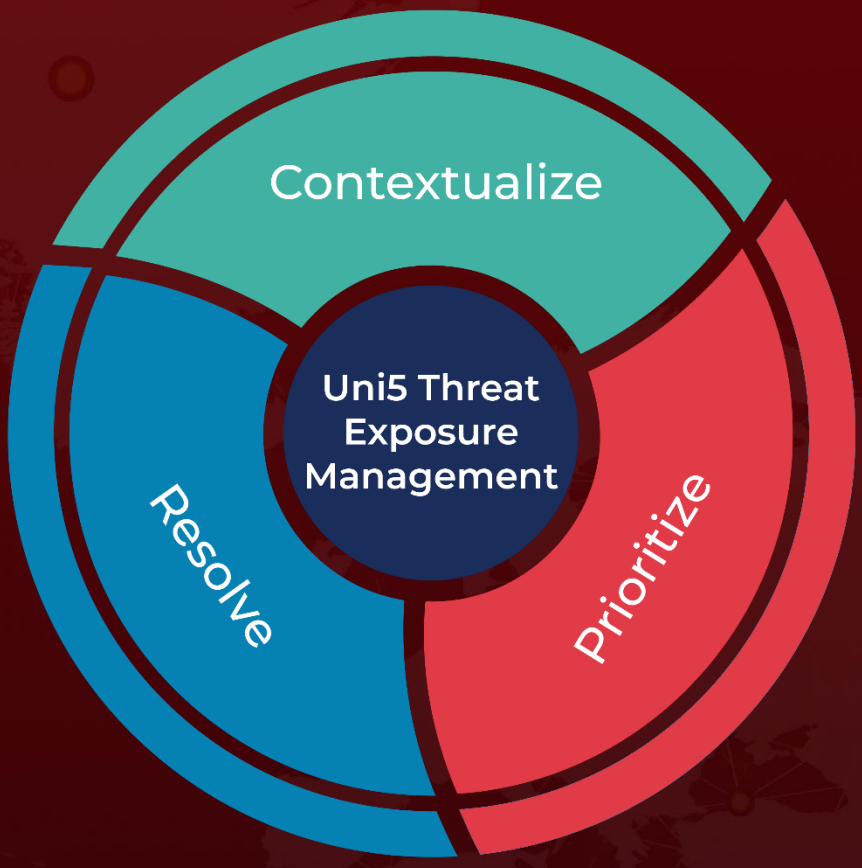
References

https://www.bitdefender.com/blog/businessinsights/deep-dive-into-downex-espionage-operation-in-central-asia/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 11, 2023 • 5:30 AM

More at www.hivepro.com