Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

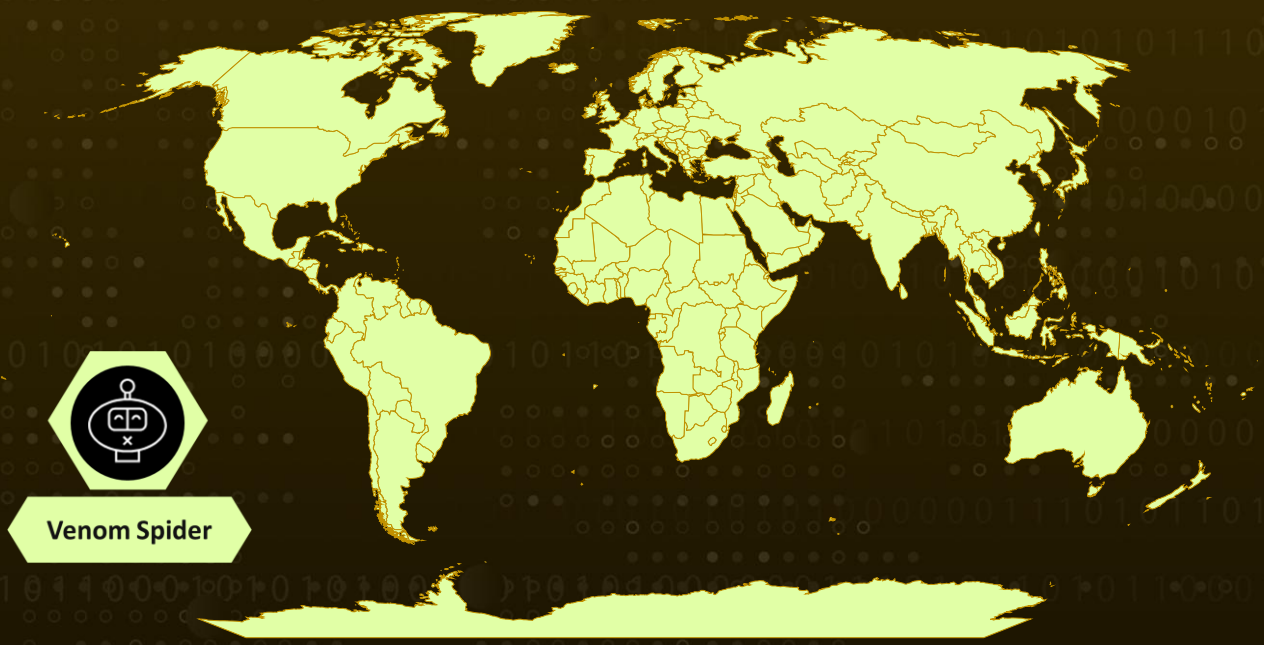
Hiring Trap: Threat Actors Exploit Job Portals to Breach Corporate Systems

Date of Publication	Admiralty Code	TA Number
May 7, 2025	A1	TA2025138

Summary

Actor: Venom Spider (aka Golden Chickens, badbullz, badbullzvenom)
Malware: More_eggs
Affected Industry: Hiring Managers
Targeted Countries: Worldwide
Attack: Venom Spider is launching a phishing campaign targeting HR departments. The attackers disguise emails as job applications, delivering an updated version of their More_eggs backdoor malware. The attack tricks HR professionals into downloading a ZIP file containing a malicious shortcut, which uses "living-off-the-land" techniques to execute a hidden JavaScript payload. This malware creates multiple files, evades detection, and opens a backdoor for long-term system access. The attack is difficult to trace due to the use of anonymous cloud services and multi-layered URLs.

Attack Regions



Attack Details

#1 Venom Spider, a known cybercriminal group, is running a new campaign that targets human resources (HR) departments and recruiters. They're using phishing emails disguised as job applications to deliver an updated version of their More_eggs backdoor malware. Attackers often see recruiters and hiring managers as easy targets since they regularly open emails and attachments from unknown senders, like job applicants or recruitment agencies.

#2 The attack begins with a spear-phishing email sent to an HR professional, asking them to download a resume from an external website. To bypass automated scanners, the victim is prompted to complete a CAPTCHA. Once that's done, a ZIP file downloads containing a malicious Windows shortcut (.LNK) file and an image. Each download comes with a slightly different malicious file to help it avoid detection. When the shortcut file is opened, it triggers a hidden batch script that creates and runs a file with hidden commands using a legitimate Windows tool. This method, known as "living-off-the-land" (LOTL), helps the malware blend in with normal system activity. This leads to the execution of the main JavaScript payload.

#3 This JavaScript sets up a library called More_eggs_Dropper, which includes a time delay to avoid being spotted by security tools. It creates multiple files, including a real Windows tool (msxsl.exe) used to execute JavaScript inside XML files. A smaller JavaScript script then launches the main malicious payload. The payload changes with each execution, making it more difficult for security tools to detect. It's encrypted and includes layers of protection that require specific system information like the computer's name to unlock the next stage.

#4 Once running, the malware sends information about the victim's system to a remote server and checks back every few minutes for instructions. The attackers can then send more JavaScript or other files to run on the victim's machine. This backdoor gives them long-term access and control of the infected system, allowing them to steal data or install more malware.

#5 To hide their activity, Venom Spider uses cloud services and domains registered anonymously. They build multi-layered URLs and reuse previously registered domains to avoid being detected by scanning tools. This makes tracking their infrastructure extremely difficult.

#6 Interestingly, another threat actor known as TA4557 has also been observed targeting recruiters by pretending to be job applicants. This actor also uses the More_eggs backdoor, showing overlaps with Venom Spider's tactics, techniques, and tooling. While it's unclear whether TA4557 and Venom Spider are directly connected, their shared use of the same malware and similar social engineering methods.

Recommendations

Strengthen Email Security: To strengthen email security, use advanced filtering to block spear-phishing, sandbox attachments for safe analysis, and enable DMARC, DKIM, and SPF to prevent spoofed emails. These measures help protect against malicious threats.

Train HR and Recruitment Staff: Regularly train HR staff to recognize phishing emails, especially those with urgency or suspicious attachments. Be cautious with file types like .LNK, .ISO, .VBS, and unexpected .ZIP files. Conduct simulated phishing exercises to test their awareness.

Secure Web Downloads: Block access to file-sharing sites and untrusted download links in corporate networks. Apply strong web filters to limit access to potentially malicious domains.

Validate Applicants Through Secure Channels: Avoid downloading resumes from unverified third-party sites or cloud storage. Encourage applicants to use secure portals for submitting applications and resumes.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**T1566** Phishing	**T1566.002** Spearphishing Link
T1204 User Execution	**T1204.002** Malicious File	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell
T1059.007 JavaScript	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1497** Virtualization/Sandbox Evasion

T1497.003 Time Based Evasion	T1027 Obfuscated Files or Information	T1027.010 Command Obfuscation	T1027.013 Encrypted/Encoded File
T1027.014 Polymorphic Code	T1105 Ingress Tool Transfer	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1573 Encrypted Channel	T1573.001 Symmetric Cryptography	T1518 Software Discovery	T1518.001 Security Software Discovery
T1016 System Network Configuration Discovery	T1016.001 Internet Connection Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	ec103191c61e4c5e55282f4ffb188156, c16aa3276e4bcbbe212d5182de12c2b7, ebb5fb96bf2d8da2d9f0f6577766b9f1, 2da2f53ffd9969aa8004d0e1060d2ed1, 17158538b95777541d90754744f41f58, 46f142198eeeadc30c0b4ddfbf0b3ffd, b1e8602e283bbbdf52df642dd460a2a2
SHA256	f7a405795f11421f0996be0d0a12da743cc5aaf65f79e0b063be6965c8fb8016, bd49b2db669f920d96008047a81e847ba5c2fd12f55cfcc0bb2b11f475cdf76f, 2fef6c59fbf16504db9790fcc6759938e2886148fc8acab84dbd4f1292875c6c, 0af266246c905431e9982deab4ad38aaa63d33a725ff7f7675eb23dd75ca4d83, f873352564a6bd6bd162f07eb9f7a137671054f7ef6e71d89a1398fb237c7a7b, 184788267738dfa09c82462821b1363dbec1191d843da5b7392ee3add19b06fb, ccb05ca9250093479a6a23c0c4d2c587c843974f229929cd3a8acd109424700d
File Name	ikskck.htm

TYPE	VALUE
File Path	C:\Users\%username%\AppData\Roaming\Adobe\d{9}.txt, C:\Users\%username%\AppData\Roaming\Adobe\hex{17}.txt, C:\Users\%username%\AppData\Roaming\Adobe\msxsl.exe, C:\Users\%username%\AppData\Roaming\Adobe\d{5}.dlll, C:\Users\%username%\AppData\Roaming\Adobe\fCore.txt
URLs	hxxp[:]//doefstf[.]ryanberardi[.]com/ikskck, hxxp[:]//doefstf[.]ryanberardi[.]com, hxxps[:]//tool[.]municipiodechepo[.]org/id/243149, hxxp[:]//dtde[.]ryanberardi[.]com, hxxp[:]//dtde[.]ryanberardi[.]com/ikskck, hxxps[:]//tool[.]municipiodechepo[.]org/id/243149, hxxps[:]//beta[.]w3[.]org[.]kz/release/info, hxxps[:]//host[.]moresecurity[.]kz/host/info, hxxps[:]//developer[.]master[.]org[.]kz/api/v1, hxxps[:]//ssl[.]gstatic[.]kz/ui/v2, hxxps[:]//report[.]monicabellucci[.]kz/295693495/info, hxxps[:]//cast[.]voxcdn[.]kz/yui/yui-min[.]js, hxxps[:]//blog[.]jasonlees[.]com/latestnews/info, hxxps[:]//contactlistsagregator[.]com/j2378745678674623/ajax[.]php, hxxps[:]//onlinemail[.]kz/version44/info, hxxps[:]//stats[.]wp[.]org[.]kz/license[.]txt, hxxps[:]//api[.]incapdns[.]kz/v1

References

https://arcticwolf.com/resources/blog/venom-spider-uses-server-side-polymorphism-to-weave-a-web-around-victims/

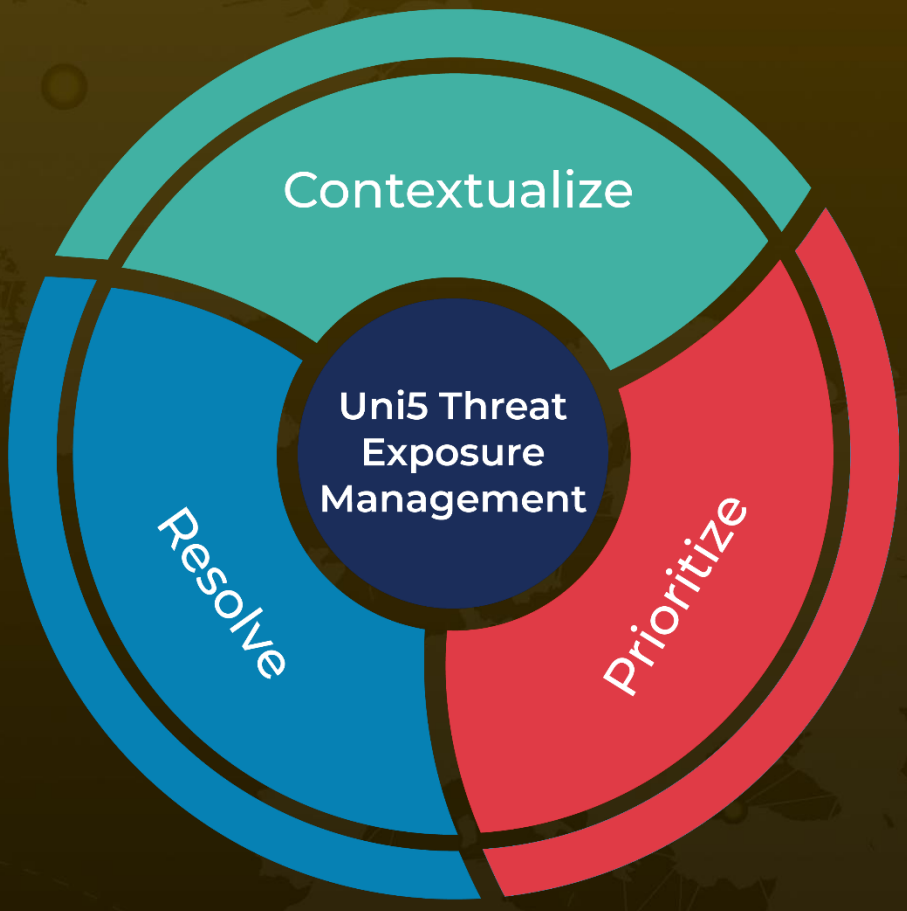
https://hivepro.com/threat-advisory/venom-spiders-victim-specific-malware-tactics-decoded/

https://www.hivepro.com/threat-advisory/ta4557-targets-recruiters-by-delivering-malware-disguised-as-job-applicant/

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 7, 2025 • 6:50 AM

More at www.hivepro.com