Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

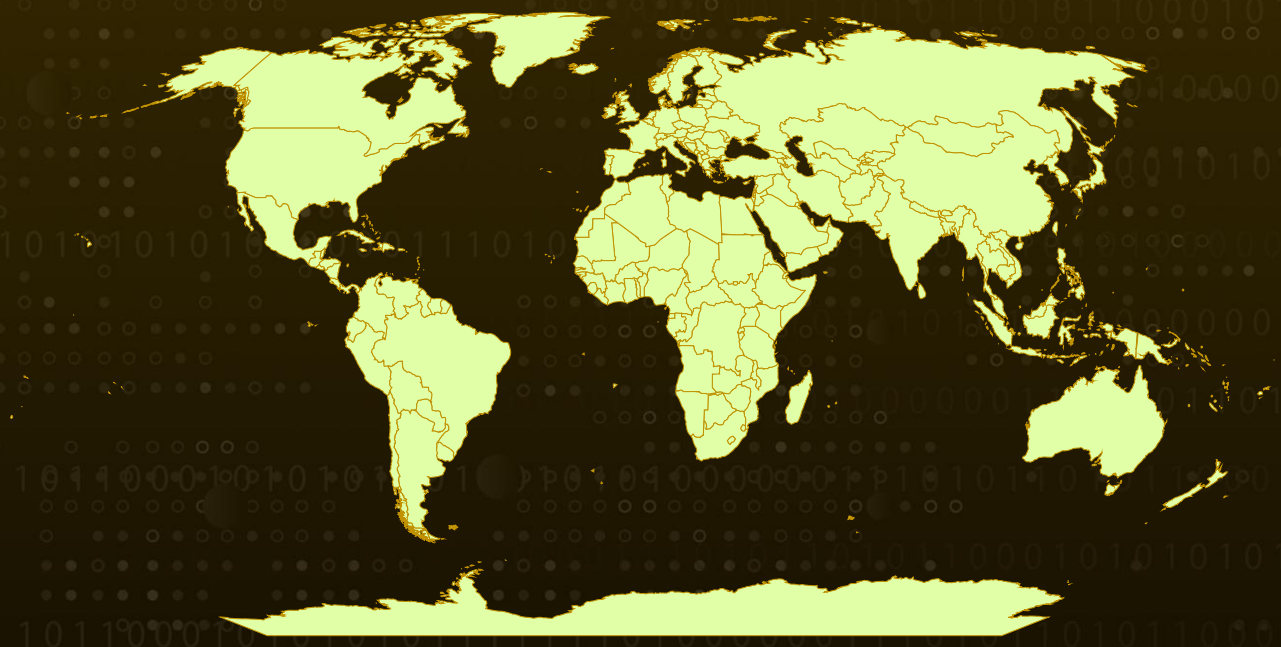
DarkCloud Rising: Spear-Phishing Campaign Targets Manufacturing Sector

Date of Publication	Admiralty Code	TA Number
September 30, 2025	A1	TA2025301

Summary

Attack Discovered: September 2025
Targeted Countries: Worldwide
Targeted Industry: Manufacturing
Affected Platform: Windows
Malware: DarkCloud
Attack: A targeted spear-phishing email disguised as routine banking mail attempted to install DarkCloud, a commercially marketed information stealer, on a manufacturer's machine, aiming to capture browser passwords, keystrokes, FTP logins, and cryptocurrency wallets. DarkCloud's public storefront and feature-rich builder make it easy for criminals to adopt, while its VB6-tied obfuscation, sandbox/VM checks, and multiple exfiltration channels (SMTP, Telegram, FTP, web panel) help it dodge detection and quietly siphon high-value data. The episode is a blunt reminder: even familiar-looking emails can deliver sophisticated, widely available malware, so defence needs simple habits plus strong monitoring to catch and contain data theft early.

Attack Regions



Attack Details

#1 In September 2025, a spear-phishing campaign was identified that delivered DarkCloud, a commercial-grade information stealer, against a manufacturing organisation. The malware was designed to harvest a wide spectrum of sensitive data, including browser-stored passwords, keystrokes, FTP credentials, and cryptocurrency wallet files. Although the intrusion did not lead to a full compromise, it highlights the ongoing threat posed by commodity stealers, which continue to endanger both business operations and financial assets.

#2 The phishing email was crafted to resemble routine banking communication and targeted the address "procure@bmuxitq[.]shop." It carried a malicious ZIP archive containing an older DarkCloud build (version 3.2), disguised as legitimate financial documents.

#3 DarkCloud is openly marketed on platforms such as darkcloud.onlinewebshop[.]net and Telegram, through the handle @BluCoder. Presented with a false veneer of legitimacy, the malware is advertised as supporting a wide range of targets, including web browsers, email clients, FTP tools, and VPN applications. Its feature set, ranging from keystroke logging to targeted file collection, makes it particularly attractive to cybercriminals, encouraging rapid and widespread adoption across underground markets.

#4 The DarkCloud builder carries its own risks. It relies on the outdated Visual Basic 6 (VB6) IDE, tying development to a legacy environment and raising the likelihood of unauthorized versions circulating. Newer builds, such as version 4.2, use a Caesar-style cipher seeded by VB6's Randomize function for string obfuscation. Because this randomization is unique to VB6's msvbvm60 runtime, analysts had to replicate VB6's Randomize and Rnd logic to reverse it. In addition, DarkCloud collects system information, processor type, OS, username, and machine name via WMI queries to adapt its behavior.

#5 DarkCloud integrates both evasion and exfiltration techniques. It checks for sandboxes and virtual machines by scanning blacklisted processes, reviewing hardware specifications, and flagging unusual filenames. Persistence is maintained through RunOnce registry entries, while its file collection rules often prioritize cryptocurrency wallets and other sensitive paths. For data theft, it supports multiple channels, including SMTP, Telegram, FTP, and web panels, often transmitting stolen records in JSON format alongside the victim's IP. DarkCloud ultimately illustrates how accessible, yet advanced, tools empower attackers while raising the stakes for defenders.

Recommendations

- **Be Cautious with Unexpected Emails:** Treat emails with financial subjects or attachments with extra care, especially if you weren't expecting them. Verify the sender through a known, trusted channel before opening attachments or clicking links.
- **Strengthen Email Security:** Use email filtering tools that can flag or block suspicious attachments like packed ZIP files. Training employees to recognise phishing signs also goes a long way in preventing accidental clicks.
- **Monitor for Signs of Compromise:** Watch for unusual logins, file transfers, or registry changes. Network monitoring tools that can detect suspicious outbound traffic (e.g., to Telegram or FTP servers) are especially helpful.
- **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
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1036** Masquerading	**T1056** Input Capture
T1056.001 Keylogging	**T1115** Clipboard Data	**T1027** Obfuscated Files or Information	**T1047** Windows Management Instrumentation
T1082 System Information Discovery	**T1059** Command and Scripting Interpreter	**T1059.005** Visual Basic	**T1497** Virtualization/Sandbox Evasion

T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1048** Exfiltration Over Alternative Protocol	**T1567** Exfiltration Over Web Service
T1555 Credentials from Password Stores	**1555.003** Credentials from Web Browsers	**T1204** User Execution	**T1204.002** Malicious File
T1005 Data from Local System			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e013fb82188cb7ea231183197e12c189b4637e7d92e277793d607405e16da1e2, 6a3b4e62a8262a0bf527ad8ea27eb19a0fcb48a76d6fc2868785362e40491432
Domain	mail[.]apexpharmabd[.]com
Email	procure@bmuxitq[.]shop

References

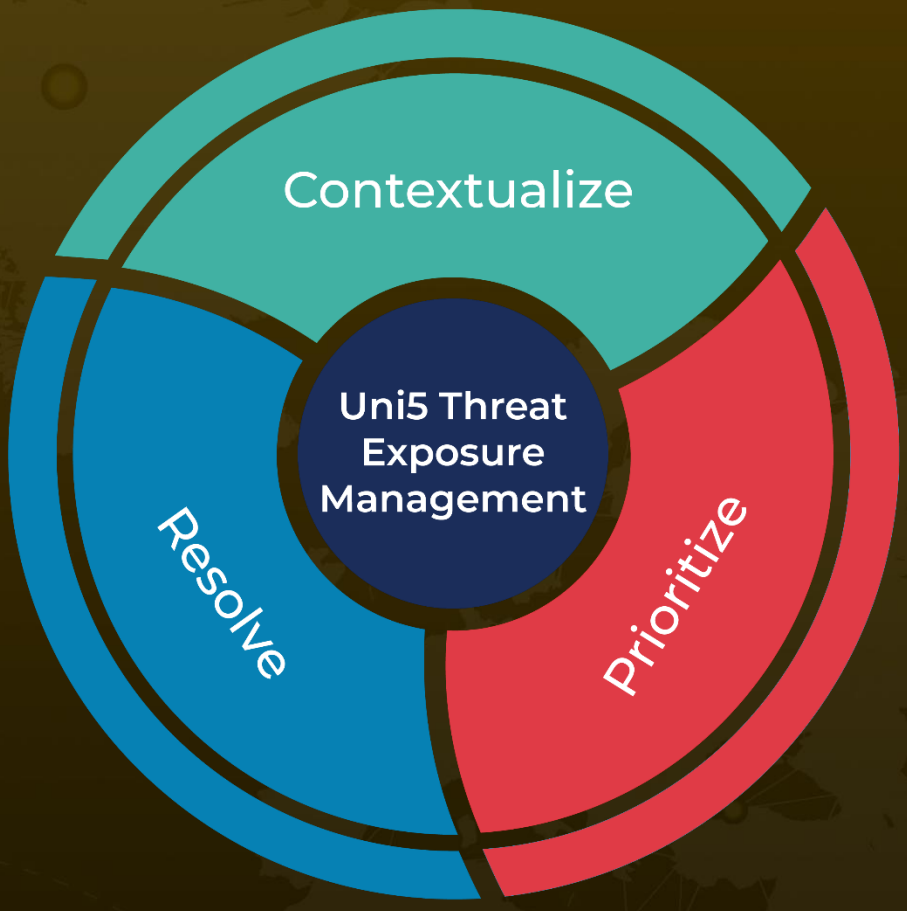
https://www.esentire.com/blog/eye-of-the-storm-analyzing-darkclouds-latest-capabilities

https://hivepro.com/threat-advisory/darkcloud-uses-fileless-techniques-turning-into-a-nightmare-for-windows/

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

September 30, 2025 . 7:30 AM

More at www.hivepro.com