Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

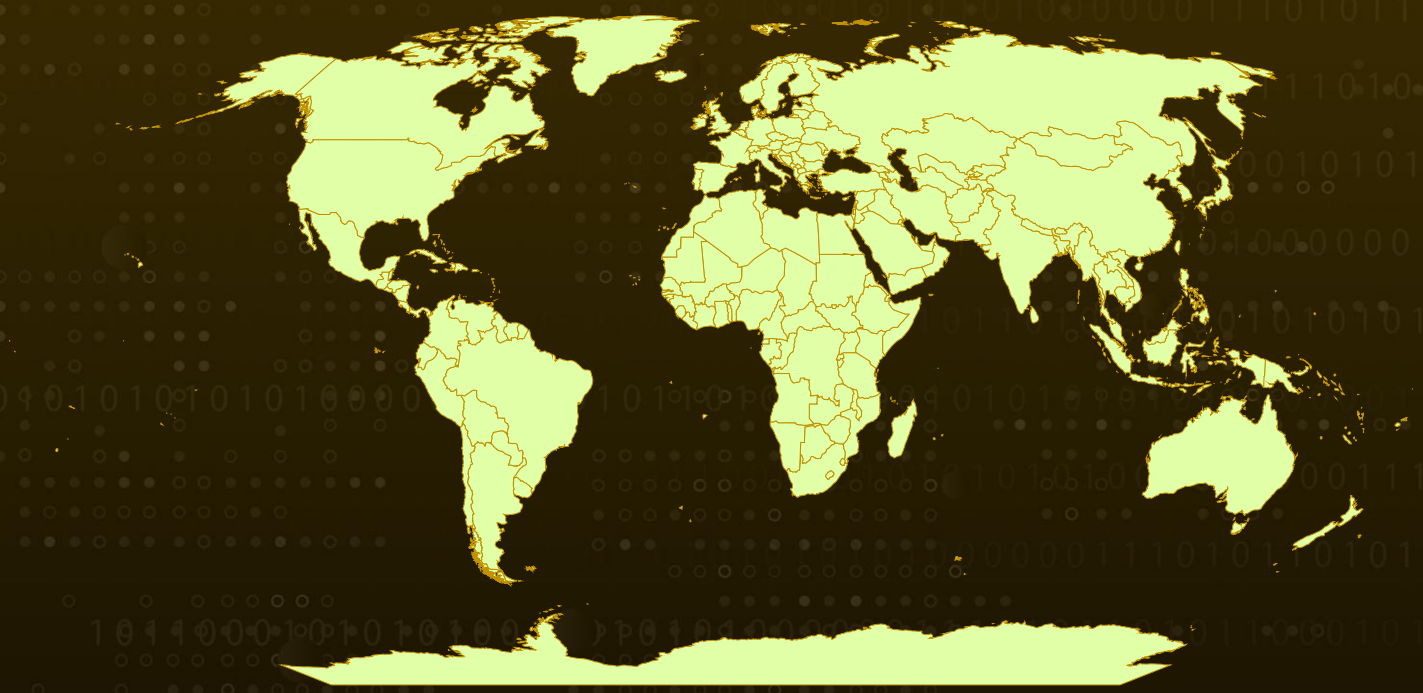
DarkVision RAT That You Can't Afford to Ignore

Date of Publication	Admiralty Code	TA Number
October 17, 2024	A1	TA2024397

Summary

First Seen: 2020
Malware: DarkVision RAT, PureCrypter, Donut
Targeted Region: Worldwide
Attack: DarkVision RAT, a powerful remote access trojan, first emerged in 2020 and quickly gained popularity due to its unique blend of affordability, versatility, and functionality. With its increasing prominence, DarkVision RAT remains a significant threat in the cyber landscape. Initially priced at $40 on Hack Forums, it has now increased to $60, attracting cybercriminals of all skill levels.

Attack Regions



Attack Details

#1 DarkVision RAT is a flexible remote access trojan (RAT) that first appeared in 2020. Originally sold on Hack Forums and its official website for $40, its price has since increased to $60. Written in C/C++ and assembly, this RAT has become popular among cybercriminals for its affordability and powerful features, making it accessible to even less-skilled attackers.

#2 The RAT's capabilities include keylogging, screen capturing, file manipulation, process injection, remote code execution, and password theft. While the exact method for delivering the .NET-protected executable is uncertain, it effectively initiates the infection process.

#3 Once executed, the .NET file decrypts and launches the open-source Donut loader, which activates PureCrypter to unpack and load DarkVision RAT. To ensure persistence on infected systems, DarkVision RAT uses three methods: creating scheduled tasks via the ITaskService COM interface, setting autorun keys, and deploying a batch script that executes the RAT.

#4 The batch script is placed in the Windows startup folder and runs automatically upon reboot. DarkVision RAT also collects system information and can receive additional plugins from a command-and-control (C2) server, expanding its capabilities further.

Recommendations

Monitor Task Scheduler Activity: Implement monitoring tools to track and log all tasks scheduled through the Task Scheduler. This includes regularly reviewing scheduled tasks for unusual or unauthorized entries, especially those utilizing the ITaskService COM interface.

Implement Comprehensive Endpoint Protection: Utilize advanced endpoint detection and response (EDR) solutions to monitor for suspicious activity associated with DarkVision RAT, such as unauthorized file access or unusual process injections.

Implement a Zero Trust Architecture: Adopt a Zero Trust security model that operates on the principle of "never trust, always verify." This approach requires strict identity verification for every person and device trying to access resources on your network, regardless of whether they are inside or outside the network perimeter.

Network Segmentation and Behavioral Analysis: Implement network segmentation to isolate sensitive data and critical systems, minimizing the spread of infections like DarkVision RAT within your organization. Additionally, deploy behavioral analysis tools to detect anomalies and unusual patterns indicative of RAT activities.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0040** Impact
T1053 Scheduled Task/Job	**T1053.005** Scheduled Task	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder
T1055 Process Injection	**T1140** Deobfuscate/Decode Files or Information	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools
T1539 Steal Web Session Cookie	**T1010** Application Window Discovery	**T1057** Process Discovery	**T1082** System Information Discovery
T1123 Audio Capture	**T1125** Video Capture	**T1113** Screen Capture	**T1056** Input Capture
T1056.001 Keylogging	**T1219** Remote Access Software	**T1571** Non-Standard Port	**T1529** System Shutdown/Reboot

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	cd64122c8ee24eaf02e6161d7b74dbe79268f3b7ffb7a8b0691a61ff409f231d, 6e3346d47044d6df85a07aeda745d88f9cd46b20d22028d231add555bf00bf41, 27ccb9f336282e591e44c65841f1b5bc7f495e8561349977680161e76857be5d, 7aa49795bbe025328e0aa5d76e46341a95255e13123306311671678fdeabb617, 0de5f042eb250092454d786b6303dee434202d45dc3fec9e6b39237f9e92514f, 0fa8acdb672f0e6c184fc5d04bb8af92c0bf5db73de096606f23f4c38ef3347b, 10667e9d67706397f7ff96e892d3c0f0ae05d81df5bc17caf85fb356d531c0b8, 1a230bb362cde9ead2d9f867af181ae51292c626a3c9d1d30f5f3751b84ffe85, 201f31c84755a5cd6081c3db30626cc3f17cf84804c2deb66e27866daad259a3, 3295199ba2b4e9cfc448a574cb9e89f3ef131fd19dcf366fe2abb7b3b79eb887, 40d48f5e965a250ac45f2f9c9426743c66fe899f07e16c42339149e30b1956e9, 44de5a248b6e9c24ad547e73c3ba3c8cc9693ba6eaa5190be9b377845844ffb6, 47070e4f6545f9f1308a5aec1e6943e6a29891bce9523db5596544a52f9b3bf4, 478cf5482905fa2ac2a2280a03ad6716f153c372c15cd957a23a67ff3260c867, 5174ef9f7d5420ab4890173792d8aafc50b8bb3191b4c24f6f58ae73bd7212c3, 5cce814cadb4fac6631ff3c988516b4c6618f0c71c7de3588fc0d7038c220f31, 7f97ba9a8e6b70708a001cff8677992fc1e768a62f9f21ddd14fb1c6924281bc, 808680e6761782a7817fd8e3f90463738d17216b3bca51f3ca4e7375458cba1b, a3bd7d3e7006439d1d53cf8db1f403df2162c8f7e8172d6911be203ea58a2d8d, b75354d8ad3f4e0f675ec6a64c82226d75116535198ef4974b17984ccebab63e, bf1c8cf3ab6213c250d1abf8094180fdcf8e871674482fce1930abe9826e61b9,

TYPE	VALUE
SHA256	cb06287e314bf4c684323c7925922cce2932a9e9e9b6aac34634487ac7741afd, e91586b66e6d05e3b118991b72896d37c3e625e4f54ceb4ad6b04f047a31593b, eafa30bac261cc682556812c7c513827f09ef75fc33dbeb61e5d3ff46c9f3808, ee1b2b016b56950986db7b08f451220b91f1d91a70fec0624e289e96c648cb44, f36626f1a71c68c4647347b25eb0000c0e6c5d7700cf16047a3d9967321cf14b, f3b00f34857586056178a56517e4c07effe1182604b11665fb8efb71be78cec4
URL	nasyiahgamping[.]com/yknoahdrv[.]exe
Domain	severdops[.]ddns[.]net[:]8120

References

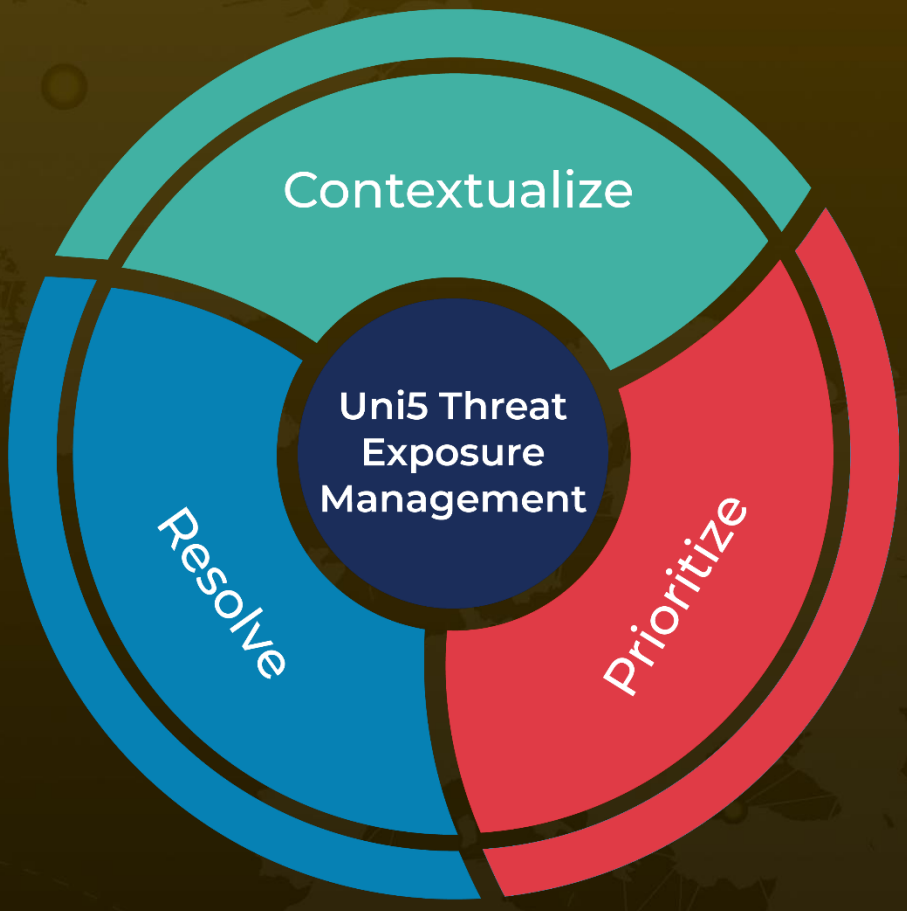
https://www.zscaler.com/blogs/security-research/technical-analysis-darkvision-rat

https://www.deepinstinct.com/blog/new-on-the-scene-darkvision-rat

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

October 17, 2024 • 3:15 AM

More at www.hivepro.com