Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

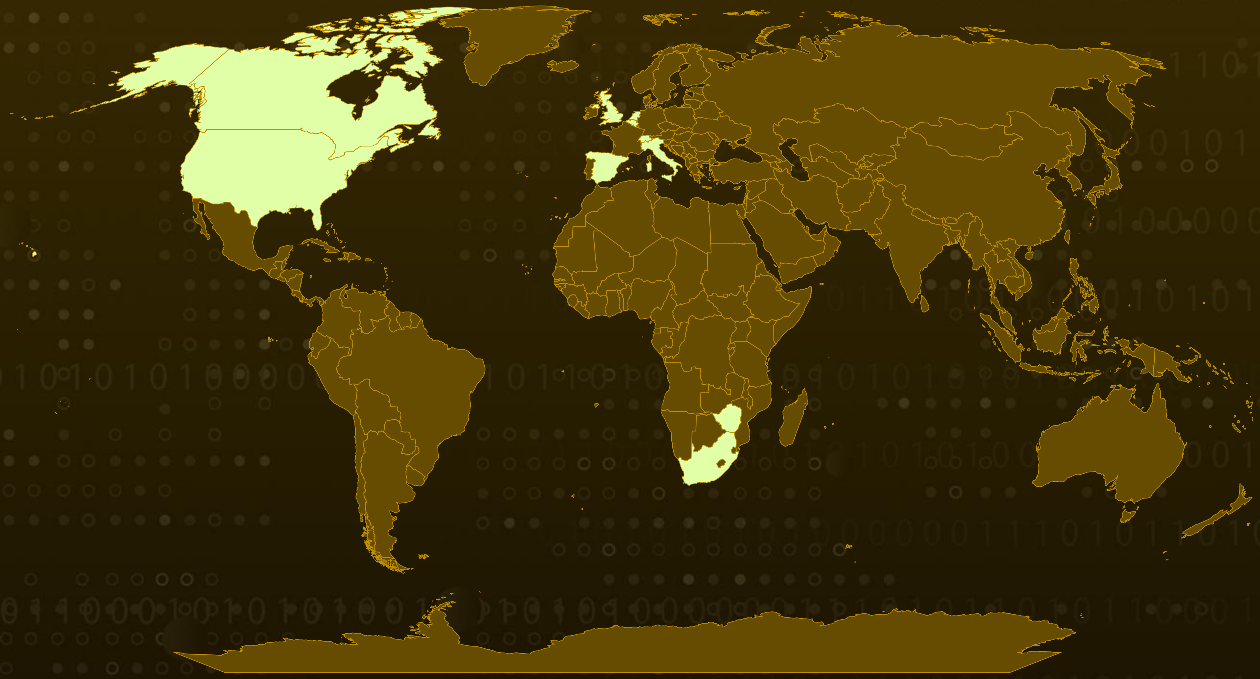
Mad Liberator Uses AnyDesk to Pull Off Data Heists

Date of Publication	Admiralty Code	TA Number
August 19, 2024	A1	TA2024317

Summary

First Seen: July 2024
Malware: Mad Liberator Ransomware
Targeted Countries: Belgium, Canada, Italy, Netherlands, South Africa, Spain, Switzerland, United Kingdom, United States, Zimbabwe
Targeted Industries: Agriculture, Banking, Finance, Government, Healthcare, Legal, Manufacturing, Medicine, Nonprofits, Retail, Technology, Transportation
Attack: Mad Liberator, a newly identified ransomware group, emerged in July 2024, utilizing the popular remote-access tool AnyDesk to execute its attacks. Unlike typical ransomware operations, Mad Liberator's attack method does not rely on social engineering tactics such as phishing emails or phony websites.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 A new extortion gang known as Mad Liberator has emerged, utilizing the remote-access tool AnyDesk to infiltrate organizations, exfiltrate data, and demand ransom payments. First identified in July 2024, the Mad Liberator ransomware specifically targets AnyDesk users by deploying a fake Microsoft Windows update screen to distract victims while siphoning data from their systems.

#2 The method by which Mad Liberator selects its victims remains unclear. However, it is speculated, though unproven, that the threat actor may randomly test potential AnyDesk connection IDs until a connection is accepted. Notably, the attack strategy lacks the typical social engineering tactics, such as phishing emails or direct contact, commonly used by other ransomware groups.

#3 The attack begins with an unsolicited AnyDesk connection request. Upon approval, the attackers deploy a binary file named "Microsoft Windows Update" on the compromised system, displaying a counterfeit Windows Update screen. This disables the victim's keyboard, preventing any interruption to the data exfiltration process.

#4 Using AnyDesk's File Transfer tool, Mad Liberator extracts data from OneDrive accounts, network shares, and local storage. Following the data theft, the attacker employs an Advanced IP Scanner to identify additional vulnerable devices but does not engage in lateral movement.

#5 The attack concludes with the deployment of a program that leaves numerous ransom notes across a shared network. These notes contain threats of reputational and regulatory harm, instructing the victim on how to pay the ransom to avoid the public disclosure of the stolen data.

Recommendations

Enforce Rigorous Access Controls: Configure AnyDesk Access Control Lists (ACLs) to permit connections only from authorized devices. This measure substantially mitigates the risk of unauthorized access, a vulnerability exploited by the Mad Liberator ransomware group. Adhere to the comprehensive security guidelines provided by AnyDesk to ensure effective ACL configuration.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Establish and Communicate Clear IT Policies: Develop and disseminate a well-defined IT policy outlining the procedures for initiating and managing remote sessions. Ensure that staff are aware that IT departments will never request unscheduled or unsolicited AnyDesk sessions, thereby decreasing the risk of falling prey to attacks disguised as routine operations.

Conduct Regular Security Audits and Monitoring: Consistently perform security audits and monitor logs related to AnyDesk to maintain vigilance. Focus on key files such as connection_trace.txt, which records Address IDs of recent connections, and ad_svc.trace and ad.trace, which provide detailed logs of connections, file transfers, source IP addresses, and user actions.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**TA0040** Impact	**T1133** External Remote Services	**T1204** User Execution
T1203 Exploitation for Client Execution	**T1543** Create or Modify System Process	**T1036** Masquerading	**T1036.004** Masquerade Task or Service
T1082 System Information Discovery	**T1135** Network Share Discovery	**T1563** Remote Service Session Hijacking	**T1005** Data from Local System
T1071 Application Layer Protocol	**T1213** Data from Information Repositories	**T1018** Remote System Discovery	**T1491** Defacement

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f4b9207ab2ea98774819892f11b412cb63f4e7fb4008ca9f9a59abc2440056fe
File Name	readme.txt, restore_files.txt
TOR Address	k67ivvik3dikqi4gy4ua7xa6idijl4si7k5ad5lotbaeirfcsx4sgbid[.]onion
Email	mad[.]liberator[@]onionmail[.]org

Recent Breaches

https://www.awsag.com
https://www.suandco.com
https://www.coinbv.nl
https://www.orbinox.com
https://www.vrd.be
https://www.vitaldent.com
https://www.crosswear.co.uk
https://www.governo.it
https://www.zb.co.zw
https://www.sacities.net
https://www.msprocuradores.es

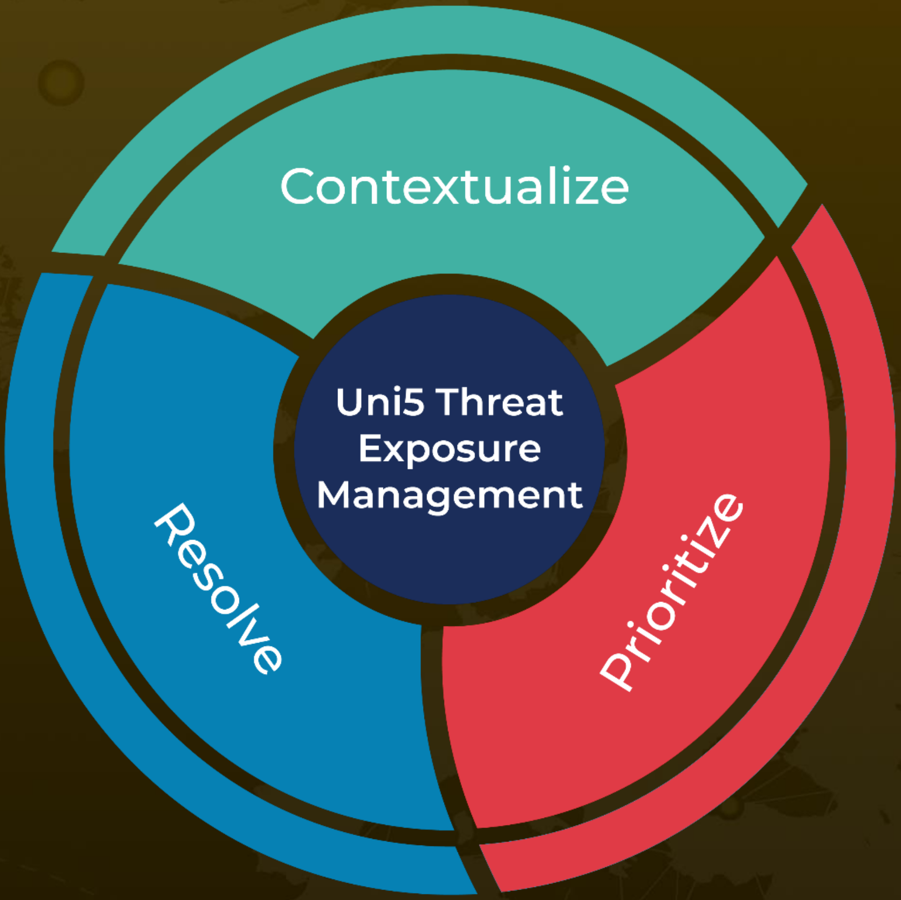
References

https://news.sophos.com/en-us/2024/08/13/dont-get-mad-get-wise/

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

August 19, 2024 • 8:30 PM

More at www.hivepro.com