Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Do you know about an emerging new infostealer malware named DockLogs?

Date of Publication	Admiralty Code	TA Number
December 2, 2022	A1	TA2022279

Summary

Active since: 2022
Attack Region: Worldwide
Attack: Stealer, Keylogger, Clipper, Remote access, and many more new features, has C&C servers in the wild

Attack Regions

Attack Details

#1 DuckLogs is a new info-stealing malware variant, which is sold as Malware-as-a-Service (MaaS) product. It captures and exfiltrates data from infected PCs such as credentials, cookies, crypto wallets, browser data, and others. It also has several other features, such as the ability to record keystrokes, execute arbitrary files, block user input devices, and power manage the infected system.

#2 DuckLogs runs with administrative privileges and can avoid UAC (User Access Control). Upon gaining elevated privileges, the intruder can change security settings, steal confidential data, install additional malware, etc., on the victim's system.

#3 This malicious software package is offered for a modest price on cybercrime forums, making this threat harmful to a broader population of potential victims, so the cybersecurity teams need to be always on guard.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion	TA0007 Discovery
TA0004 Privilege Escalation	TA0011 Command and Control	T1204 User Execution	T1059 Power Shell
T1047 Windows Management Instrumentation	T1547 Registry Run Keys / Startup Folder	T1055 Proceed Injection	T1562 Disable or Modify Tools
T1082 System Information Discovery	T1497 Virtualization/Sandbox Evasion	T1057 Process Discovery	T1518 Security Software Discovery
T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1573 Encrypted Channel	T1102 Web Service

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	5bbbef641b0d73309939c16a8bb1621b 58a0f68310f775b4bd4ea251064ed667
URLs	hxxp://lovableduck[.]ru/host/drops/eYjqq6Ezx/ee48v958r[.]exe hxxp://ilovetheducks[.]ru/host/drops/Gh879pKQj/btvM8o8sv[.]exe hxxp://quackquack[.]ru/host/drops/g6tujhiry/hjt50kzbo[.]exe hxxp://quackquack[.]ru/host/drops/Gh879pKQj/btvM8o8sv[.]exe hxxp://quackquack[.]ru/host/drops/jgh1zyoel/fsgrvawrq[.]exe hxxp://smallduck[.]ru/host/drops/ezQEvGqPI/nZAQiWiHm[.]exe hxxp://smallduck[.]ru/host/drops/SrM7WQD2E/7s4udn5F1[.]exe hxxp://smallduck[.]ru/host/drops/20NVT6CUe/9GseGAVEy[.]exe hxxp://lovableduck[.]ru/host/drops/KI2kRAS0x/rrxgKvAJd[.]exe hxxp://lovableduck[.]ru/host/drops/k1rf7fmny/lr2xfd9m9[.]exe hxxp://ilovetheducks[.]ru/host/drops/e563bgj4y/hrldcrajl[.]exe hxxp://ilovetheducks[.]ru/host/drops/JTQ4iHTm3/wT9lPlvPK[.]exe
SHA256	e15bf47074cc31f3445b3efb8ad75fac95ab085b5598cc82075902292ab8276b e9bec9d4e28171c1a71acad17b20c32d503afa4f0ccfe5737171854b59344396

TYPE	VALUE
SHA1	c790ad50365158aecd4599ebab8db004bf9a9091 83c727335125f06b712cf4390bb9d265f77088a0
Domain	Ducklogs[.]com lovableduck[.]ru ilovetheducks[.]ru quackquack[.]ru smallduck[.]ru
IPV4	179[.]43[.]187[.]84

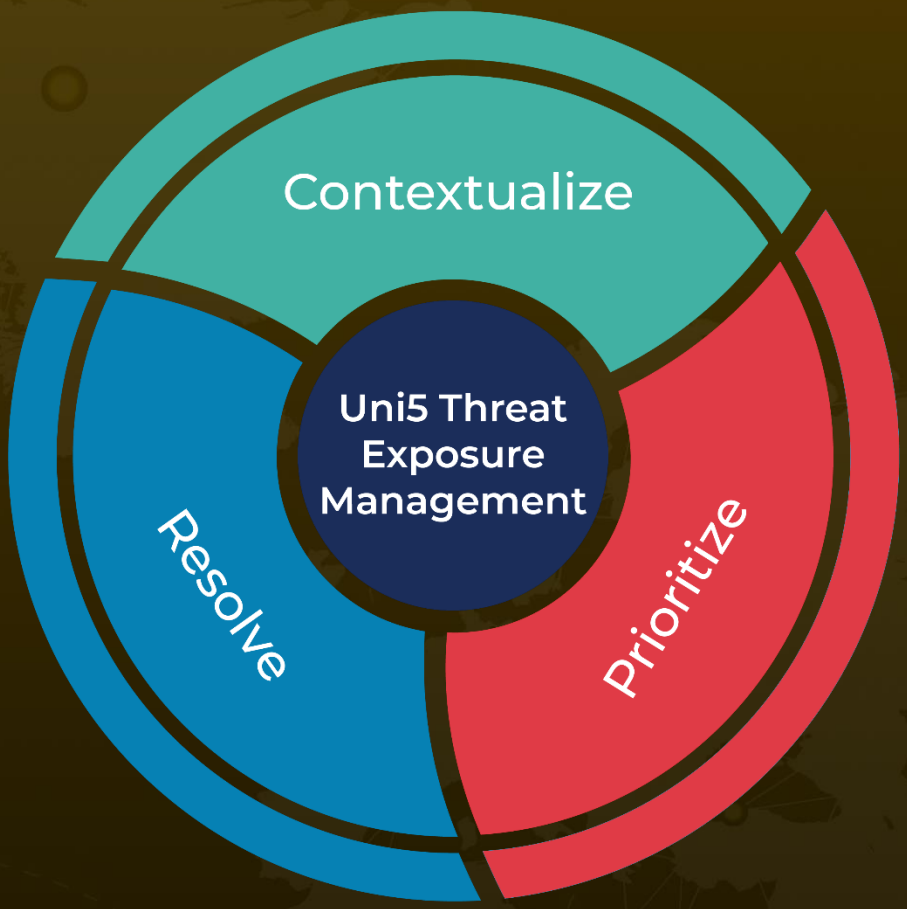
References

https://blog.cyble.com/2022/12/01/ducklogs-new-malware-strain-spotted-in-the-wild/

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

December 2, 2022 • 5:00 AM

More at www.hivepro.com