Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

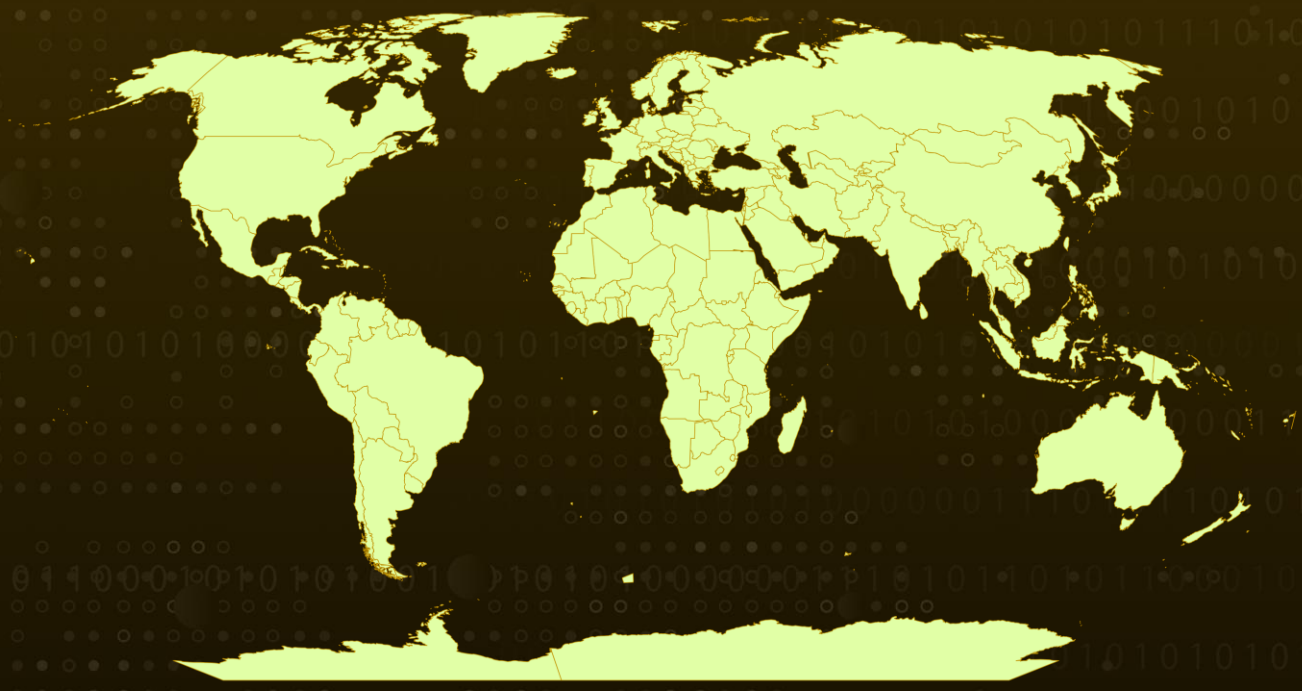
Unveiling Lu0Bot Malware A Node.js-Based Threat

Date of Publication	Admiralty Code	TA Number
October 10, 2023	A1	TA2023406

Summary

First appeared: February 2021
Attack Region: Worldwide
Affected Platform: Windows
Malware: Lu0Bot
Attack: Lu0Bot Malware, a Node.js-based threat, surfaced in February 2021 as a secondary payload in GCleaner attacks. This malware acts as a bot, responding to C2 server commands and transmitting encrypted system data while employing intricate obfuscation techniques for stealth.

Attack Regions



Attack Details

#1

Lu0Bot Malware, which emerged in February 2021 as a second-stage payload in GCleaner attacks, operates as a Node.js-based bot. It patiently awaits commands from a C2 server and transmits encrypted system information to this server. Despite its relatively low activity, Lu0Bot stands out due to its inventive use of Node.js, offering versatile capabilities.

#2

The analysis of Lu0Bot unfolds in two segments. Firstly, the malware is compressed within an SFX archive. Inside this archive, a BAT file compiles various files into an EXE file. This interpreter receives both bytes and a numeric key for encryption. Files like eqnyiodbs.dat and lknidtnqmg.dat play integral roles in the malware's functions.

#3

In the second part of the analysis, Lu0Bot's JavaScript code constructs its communication domain from multiple components. It collects system data via WMIC and secures persistence by copying itself to the startup folder. The malware endeavors to establish connections and exchange data with a C2 server.

#4

Lu0Bot employs advanced obfuscation techniques using JavaScript, merging traditional malware traits with web technologies, rendering it a formidable challenge for detection and analysis.

#5

Static analysis of the source file reveals the presence of an SFX packer and various files, including a BAT file, a Node.js interpreter, and encrypted data files. The malware is engineered to retrieve comprehensive system information, encompassing processes and execution locations, and maintains persistence by copying itself to the startup folder.

#6

Although heavily obfuscated, the JavaScript code employed by Lu0Bot can be deobfuscated to unveil its core functionality. The code incorporates AES-128-CBC encryption, with an identified decryption key. The malware persistently seeks an address for transmitting data to the C2 server.

Recommendations

Regular Software Updates: Ensure that all operating systems, software applications, and security solutions are kept up-to-date with the latest patches and updates. This helps eliminate vulnerabilities that adversaries can exploit.

Endpoint Security: Use endpoint security solutions that can detect and prevent the execution of malicious files and scripts. These solutions can help stop malware like Lu0Bot from infecting endpoints.

Network Monitoring: Implement robust network monitoring and intrusion detection systems to detect unusual network traffic patterns. Pay special attention to DNS requests and communication with external IP addresses.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0002 Execution	TA0011 Command and Control	T1573 Encrypted Channel
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1132.002 Non-Standard Encoding	T1132 Data Encoding
T1573.002 Asymmetric Cryptography	T1053.005 Scheduled Task	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1047 Windows Management Instrumentation	T1573.001 Symmetric Cryptography		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	6181206d06ce28c1bcdb887e547193fe
SHA1	8eb65b4895a90d343f23f9228e0d53af62de3dab
SHA256	169b23f45787a0213143bdbb4125658b4bee18e74cb9899c09c29233807bcd21, 4a6ff95b69e3af76e8b36ec5de23b7dd5f8edb72f86a98a710da1dc08f41d799, e6bf861332a771e037a76546d095dd752db63ba0e9fec254a69e0864ae248921, 31fa43d98ac742905cf04735033e154fd103bc67c255cec63a7448ad138df0cf, ca09a22afb6d9a1853fe4fc4d36089900d24d7178642ec7ca86789cd0dbc5c67, 8ee274b430932f7e8068229a7f32c2bbaead31bf6c18dd13194a1126f5cbfb33, 3a1f00f2d35eb2fbab05c0543eaf32d29b12b856c64809393c873474a4a27083, 95fad71ca5df4eb7e390f6795d4a02d117524e9432d118a5213a484e211e1480, 7b4055eb9d72b5e5cd10c846497cb538bc366f8993198b680d195c98987d74e6, e2c630adb97cc041c5ce1835add03841493ae95223d43c9e415e26e6c4c418e2, fb808be98b583a2004b0af7b6f4bf5e3419d8b6a385c5ce4e8fab4ddc0b48428, f4b15f591e0138a46f1f5fd157f31a78b360624d72a18136a5269a05ba8b987c, 22b643071879895cd947cf37c75c71b23af5fe4228f36b49571b1a47df137d06, 28eb3941dee1a78351ee18596be6445d4fb10332d002f85aee675f672cf2fd1c, ea596ff0c0802b85cc304447799c91907ae1016283152ba5ba5dc4cb50ca8712, 9837727bf67f4a49655b5f2230fa7dad235b025c9af377e559df6fab0f4ff36a, a4a0e26bb4aa352f66952902cc9704d130593adacb46017c0b2a1be2b7a9269d, 863c612734f5ff0ff0ea3fed7fd790dfb43c47eecdc1417bcd82c0ad866419af, 9c5898b1b354b139794f10594e84e94e991971a54d179b2e9f746319ffac56aa,

TYPE	VALUE
SHA256	f17694550f57c6605f37588e37f55898bbc969c1f24b18f0be8ce416c95ab91c, 0296a426d47abf467c431db1e126b8763eac7d062e731193eccd15a51c52da7c, 149ca091b02aafdeff15610c639b442a61e0dfcd461d9bec7f8c38998a390575, 6f7ab51e9f0d382c650743cb3c06b42708cd06d64170a458864e89ad6480a237, fd746c51486e5ccb2bd801f4cffbeefaf77e7844ef1dd5d211a4c183ec26f52d, cb96ceb0b26fc150baaa7fe1cc2a65af42c7db902f54839578b3235a7d12d25c, bfc050b80ad15c6bf86ea0dce49089c56ed9ffccf5dae2b8e3b78b59dd36e0bb, 956610a72b5e5aaf220b861aec44e08dda7b6a97ccae3d2fea0181e3a6b37228, 09a2d8ab4c255b6f78ca7534e3105014a21613cd3c6b07cbb92eb2c82b553483, 24c0997ec70f23963598b59df453f28ffcc1e8b356898d5ddc4b2cbf06f6f2ac, 0718b209bd95315b8347d3f006b7da387f9807153ebe8b2788285296e19b5973, 0739718c03bd39daad459142116b886d6138cfe887d30b02942e01b9d238dd13, b13633b31e8704b63d977921d1c9a4284bfd4780c3f35a5bee372816d7beb005, 242467ea19694c0e6cd76dcff901f5af6a309c2c999971b1dc4cd9bad253ea19, f5f8716486cab2d9b866a1e19e4f25d64d070262ce32d2ff79db283ac7fd1b05, 0bdaa27e390c5e15c3b27ae4f4168fbf97693f5d03fa0f70487c63c13030ffd8, 5920894ae997b61f27b53c9f6e598df5f928acb11a5dc09f4fa0627747f1312d, 6d265ec945dfd70f60e5a016ec26276f3d460076e9320a3c11c7a76b638da9ab, 5a2283a997ab6a9680b69f9318315df3c9e634b3c4dd4a46f8bc5df35fc81284, 742eb714457c3646f7f5dee44aaf0d57d5fa076ee294de6755818132402b06f5, 70657b04b2da77f8019be49fa3043898874bebb385317a6c91246f9e3858bf16, 858bafe27080124fc1560894b00cf8c0c672df0bd0a66dbd08cf28b4cf9e1ee5, 7374cce760bf018df8c602b12e475a66114747d96848168cb939f27afafb29e0,

TYPE	VALUE
SHA256	d5069d544f3ff1efe1851688b9625cd44fe45c6f1a9792b30f5f28c74af1d6d6, 5de7148d727fec09a0597b5f64cf1719968372a21c6ded90c51cae3f42b4c26d, 0f2c35b80a36f70ab923b56c495ea6fe9ebdd48b3d5a4ff404fec3b99ff010d9, d189c35ecd1b9665741e7e08f9d9029c307e07870cf57832426d8bfce1c48fa6, 8264e723a411381a9d837458ec39cbb36c8d582bcba14f7ed7fc45f8154c479d, 4547dab867404fa6e5cebc5794ae58c4d365355372d26e6bcd01c1aea0f91e1b, 45964a7afb9d41eb319161c26215c5bea0334b388ecfb1520b83bb2d6984ad5e, 02e4898e0a4cc85c406996e5e60274082746eb45d77a18a24eb545074a56ab3c, 418a860f2f7f5d415ffa2c7b2662c6fde7c35e2bdafd45e378bdf7c95579fde8, fce3d69b9c65945dcfbb74155f2186626f2ab404e38117f2222762361d7af6e2, f186c2ac1ba8c2b9ab9b99c61ad3c831a6676728948ba6a7ab8345121baeaa92, 5a2264e42206d968cbcfff583853a0e0d4250f078a5e59b77b8def16a6902e3f, c88e27f257faa0a092652e42ac433892c445fc25dd445f3c25a4354283f6cdbf, 2d721df670fdb63c643b3de2dcdd46311b8d94d2753b47ad0035392644dee77a, 4c31eccb460bef397e6100e1ecd85c3a2b823b893a9a9add4bb83fde8f9b122b, 0297bbb0f00b3f591894ebcf042f2c6b0ed52e6662def1a9dbca0f8d20133cee, cb23aeac6382ff99608a71e3b416c1ca22f5f301474840239e4c319db31cef25, 9db5c02ac4e161369160fe13719a212e55377dd57ffc9f98b7141bce3b9df26c, 4c99457625e752a03693aab64e2b5129eff89872c649194e81bd87809ed1ae13, 22934e006b3f1b8225c51a93ce0acaa1874c4f1dc895fa1664bdf16b0065d2e7, 7c37b8dd32365d41856692584f4c8e943610cda04c16fe06b47ed2d1e5c6415e

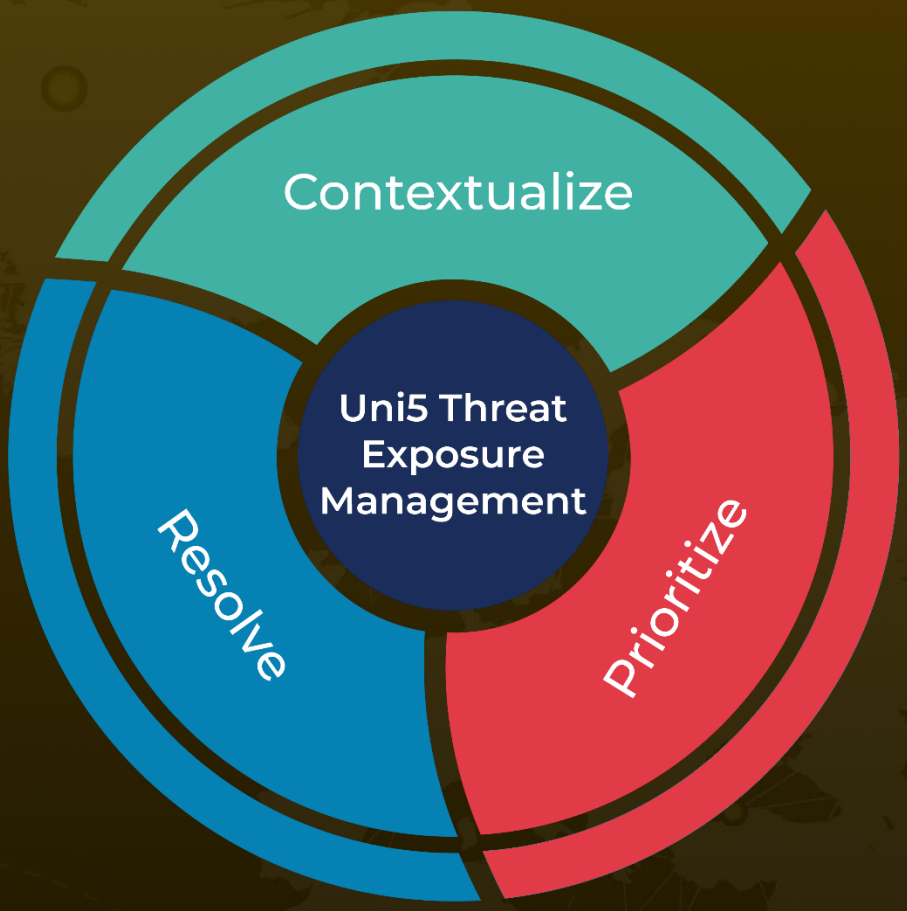
References

https://any.run/cybersecurity-blog/lu0bot-analysis

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 10, 2023 . 7:30 AM

More at www.hivepro.com