Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

DotRunpeX Novel Injector Delivers Multiple Malware Strains

Date of Publication	Admiralty Code	TA Number
March 17, 2023	A1	TA2023144

Summary

First appeared: October 2022
Malware: DotRunpeX Malware Injector
Attack Region: Worldwide
Attack: DotRunpeX malware attack vectors have been linked to dozens of campaigns. The DotRunpeX is a second-stage infection used to deploy a variety of malware families, most notably stealers, RATs, loaders, and downloaders.

Attack Regions

Attack Details

#1

DotRunpeX is a novel injector written in.NET that employs the Process Hollowing technique to infect systems with malware from a range of renowned families. This new threat gained popularity primarily between November 2022 and January 2023. The first-stage loaders are typically distributed as malicious attachments in phishing emails.

#2

The latest iteration of DotRunpeX features protection from the KoiVM virtualizer. Clicking on fraudulent links results in the download of the DotRunpeX injector, which is then employed to distribute a variety of malware. DotRunpeX is capable of deploying several malware strains, including AgentTesla, ArrowRAT, AsyncRAT, AveMaria, BitRAT, Formbook, Lokibot, NetWire, PrivateLoader, LgoogLoader, QuasarRAT, Remcos, Vidar, and numerous others.

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	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1106 Native API	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1055** Process Injection
T1027 Obfuscated Files or Information	**T1027.002** Software Packing	**T1036** Masquerading	**T1055** Process Injection
T1003 OS Credential Dumping	**T1497** Virtualization/Sandbox Evasion	**T1005** Data from Local System	**T1105** Ingress Tool Transfer
T1573 Encrypted Channel	**T1095** Non-Application Layer Protocol	**T1071** Application Layer Protocol	**T1018** Remote System Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1e7614f757d40a2f5e2f4bd5597d04878768a9c01aa5f9f23d6c87660f7f0fbc,68ae2ee5ed7e793c1a49cbf1b0dd7f5a3de9cb783b51b0953880994a79037326,317e6817bba0f54e1547dd9acf24ee17a4cda1b97328cc69dc1ec16e11c258fc,65cac67ed2a084beff373d6aba6f914b8cba0caceda254a857def1df12f5154b,81763d8e3b42d07d76b0a74eda4e759981971635d62072c8da91251fc849b91e,0e11704fcc3c36832ba98b80ea44a3013660d1ed3fb48158b982fed9f9050391,0f9e27ec1ed021fd7375ca46f233c06b354d12d57aed44132208cd9308bfee11,881a337aa85a4b01c08706ab941573c5dc9b76ea0e4e1c2693a9b4aa4453ec8c,feae44d8927dd41feaed997b3dbf7b41933496d6285b79554b83e72ae8a045c4,1c1fcc4133af77f07d0c0299d0320aa9f447748ebead74b429f73c44d950e38b,35c11f7315d2e5d04d783de4314d8cde2def382f1e3fc49ccc555337c54d63cc,4068637c121888476533a3bbb16bec6bc3b4f81f7b9de635ef3576d56dc54c75,40df5a6e6dcadbe576ce4a8b01cfb82bf3f56a87bae674200e60814eab666c6d,8a0d6e40e545d40956194230f03608859f2a47420a9b11b199142641bc6419ee,7c3803c09a0370aa6484d8ad2f5690b96212d98e45fc8f9cb6022f87dff637fc,93e2ea6f021951369028b73637d9558c8baf3c99d9de1a2a60c1461cb9d571bf,d95298befdde567b31571d16f327840fa0f0dd9c54bf876531820910418a52b6,149af913afd7eb2773386d14e88a46449cbc9096e0748cfbaa2e061b59525bf0,a73f134ab62a5c23a8c8bafabbfbd5e0408c826ba5418488639724708ec5ef28

TYPE	VALUE
SHA256	aca4d6278f31f374262e0388d16ee6fdcdbbad8257374f1feaabf75b0ec23157,50451fda27fd8569c7b32bfe82197b82a8637cac928164e1b091a389060e957e,9ed8eeb1db8909c96a958d91213093d2488dc172a8d22ba62657b9bfeb044fec,6c08c0654726c2f793b5191d5e7c74fdf3a2461118a45aa8527a0a30e3f256fd,283cd48dc1368b6852c2f3168bf7a78ad593df010d9a67ed1c938508da5de783,b019a0535ca7466d7884825542ac6910fe037913118e1136dcac7e9ef3dc0dc9,b1c9b356c50230629c4697b0527fd7a0fa8d6f0e8342a1eb5b5a4f90d8f0eb86,5bbd9513f0872d23ca43dd553a63a12882be274fef983fab427721257d60eaec,9d9940b60809e3c10cd4540f8e589626a293244a999bea16c259f9712969a742,cd4c821e329ec1f7bfe7ecd39a6020867348b722e8c84a05c7eb32f8d5a2f4db,cddf8b8da972cb2e560c70d01366f582445441864fcff884b8194eb6c21a768c,6c367333c677c2268df9deaff6ad4e711e73e53504aa1aa845bebfbfe635f1d2,5e3588e8ddebd61c2bd6dab4b87f601bd6a4857b33eb281cb5059c29cfe62b80,244f2d4f3c34d00babef5f1765e91c0abda9dbd1d131fc93ecb48c91ecc801a8,95793df9284fe35c0491e5cfa36bc8f49fd426ccdf35f5fe2f098e07d160a4dc,55ee7efcb3d1d2e0eac0ecadd651d6a299de82d94347ef9862bc981ae619532b,13081992c0ef5c52c2b6224f3ff1ab38160bca9424e7c0470e0c175c920bdc9d,0daef2c2bf086312037ebc91beec0302a7e4d1750f260d02bf815bd13c611559,331ad58c524100da7e459e5c3943e970414617f60b3ed0f1a74f3bf189aafea7,44a11146173db0663a23787bffbb120f3955bc33e60e73ecc798953e9b34b2f2,03fcbab82603df2858f7d6fefdb6ae3cc8e17393af6d44f24634d28fccf3f181,373a86e36f7e808a1db263b4b49d2428df4a13686da7d77edba7a6dd63790232,50ec8a9e59e1bcb0a41477e20f5bb809a80329d56e20cf99e93d756b9e0ceefc,41ea8f9a9f2a7aeb086dedf8e5855b0409f31e7793cbba615ca0498e47a72636,76e129552a30fa5c914d9f946f40b2ec2bbbbeb4e5e2f324e70455725030e157,8fa81f6341b342afa40b7dc76dd6e0a1874583d12ea04acf839251cb5ca61591,ae4f3b6c43d5ea8ee68d862362d4e8d7b317889eb9abead948a9b791ad9d7071,b4c876d1797efbef614b44e52482c835c32e8ee020975a30fa2d25ed9cf8aa2b,d5eda02ff2f05d1e0d06a69018de463ab36497048a1ef2b69af93aa76ccfc07d,fa3a9fc2adf9d1ca812e0951e21bf72ba3ec9ceb1c0cf0bfc0171b6d4adadf83,1f2ffabb3b89e6083ca5de70f5d718295c7a633c2d957da7c4469de059efde2c,bd133efea4b865f42eb05e0c92e3ab3b58ac087c0682ea9112b96596a7111ff6,e6da2d860bd2d0e8b56737b4c8c47cdeea78a404cd0d6fa5a26cbb5ac7682d1d,d87a200a26d07a64272e93fb3ae8f8d9e4d34bdfedb0cf7c685a6c97912e967f,7120cf1ad3fdcae7ba6956749a8988e8181837a05948b432cec6ae11229b1d12,304847c69875ec59995fbb453f8d1106f80c5eb380ae6b8676e76f5372290194,25fbe0ff3274b4bc981fa6ec0459e9b95cec6397194e10ea6287bf4b899a9b07,1bc7fc0a4796f7780223b4f0bf8d6816b3721f0b52eedc0df9a32dc4ea4829e8

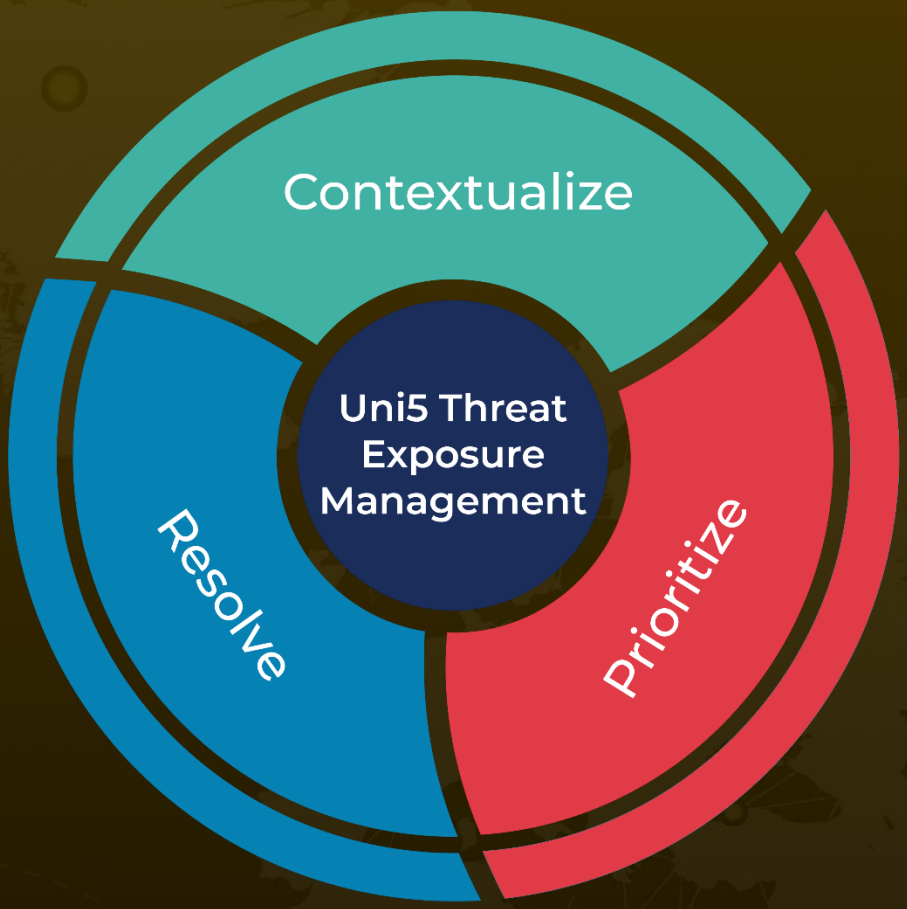
References

https://research.checkpoint.com/2023/dotrunpex-demystifying-new-virtualized-net-injector-used-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

March 17, 2023 • 5:49 AM

More at www.hivepro.com