Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Ukraine Hit by Cyber Attack: 2,000+ Computers Infected by DIRTYMOE

Date of Publication	Admiralty Code	TA Number
February 7, 2024	A1	TA2024045

Summary

First appeared: January 31, 2024
Attack Region: Ukraine
Malware: DIRTYMOE (also known as PURPLEFOX)
Threat Actor: UAC-0027
Impact: Over 2,000 computers infected
Affected Platform: Windows
Attack: The UAC-0027 group executed a sophisticated cyber attack against Ukrainian organizations. Their weapon of choice was the notorious DIRTYMOE (PURPLEFOX) malware. This modular malware has been active for over half a decade and poses a serious threat.

Attack Regions

Attack Details

#1 The cybersecurity landscape in Ukraine faces increasing threats from various hacking groups, including the notorious UAC-0027, along with others attempting to breach Ukrainian systems. A recent extensive cyber attack led to over 2,000 computers being infected with DIRTYMOE (PURPLEFOX) malware, attributed to the UAC-0027 group. CERT-UA issued a warning on January 31, 2023, outlining the cyber attack and the infiltration of Ukrainian systems by DIRTYMOE (PURPLEFOX).

#2 The DIRTYMOE malware, also known as PURPLEFOX, is modular and has been a prominent player in the cyber threat landscape for over half a decade. primarily used for remote access, DDoS attacks, and mining. It utilizes a rootkit to hinder removal and self-propagates by exploiting vulnerabilities and using authentication data.

#3 The malware ensures fault tolerance by employing multiple communication methods with control servers, often located in compromised equipment in China. To detect infections, network connections, registry values, event logs, and specific directories are inspected. The malware persists through service creation and hides its files using a rootkit.

#4 Removal options include using antivirus softwares or manually deleting files and services. Steps for manual removal involve booting from LiveUSB or connecting the affected disk to another computer and deleting specific files and registry entries. A firewall should be enabled before removal to prevent re-infection via self-propagation mechanisms, with rules blocking incoming traffic on specific ports.

Recommendations

Software and System Updates: Regularly update operating systems, software, and applications to patch vulnerabilities. Implement automatic updates to ensure timely patching and security improvements. Vulnerabilities in outdated software can be exploited by malware like DIRTYMOE (PURPLEFOX) for infiltration.

Network Segmentation: Implement network segmentation strategies to isolate critical systems and separate computers running outdated operating systems. This helps contain potential infections and limits the spread of malware within the network

Monitor Network Traffic: Implement robust network monitoring solutions to detect and analyze suspicious network traffic. Continuous monitoring can help identify unusual patterns or behaviors associated with malware infections and enable a timely response.

Continuous Monitoring and Threat Detection: Deploy intrusion detection and prevention systems (IDS/IPS) to continuously monitor network traffic for suspicious activities and potential signs of malware infections. This proactive approach can help detect and respond to threats like DIRTYMOE (PURPLEFOX) in real-time.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0011** Command and Control
T1569.002 Service Execution	**T1569** System Services	**T1218.007** Msiexec	**T1218** System Binary Proxy Execution
T1014 Rootkit	**T1027** Obfuscated Files or Information	**T1055** Process Injection	**T1071.004** DNS
T1071 Application Layer Protocol	**T1059** Command and Scripting Interpreter		

Indicators of Compromise (IOCs)

TYPE	VALUE
Hostname	kew[.]1qw[.]us, kew[.]8df[.]us, nk[.]1qw[.]us, ret[.]6bc[.]us, rpc[.]1qw[.]us

TYPE	VALUE
MD5	135605de47aaad4140bdce443b24b24d, 191a5e1c2fab01634748e6f30c097fbd, 1c17d105e0ad36459ac40fbf1aec6f95, 75540c21874be37b2087de213b2f55c2, 80ea4b5ada49ae2f18a62aa16665e060, 843b9a7dac964a9d242b8174e8d16227, 9620e0d47aa20f31ac21a2fc2de21f46, a240accad68ced374b9e90bb0b642d9f, a7f8fa8f44034ab8176e02f15ebae504, ae5fa12b6862cf49f5f44a4bfcdbfd0a, b5f85c26d7aa5a1fb4af5821b6b5ab9b, c12241be2c41ae69187ca9faf83494ff, c6a26ec425627730c0e17c5e68ad7ee8, f12332acf2b94bda02eabb5a5d24d179, f6284c8a22be3be7bc57e14533295584, f9eac6143f31bdb4ea5bf8cc8017c7bf, fde752850864fc4dde67f5da7e44b176
SHA1	27c4599a2cf7ce739ba967d03c308bac217e2ee8, 31a14bce84bd89133dfba392f161a5ec640c544e, 54b64205f29cdc5b3e9f0a157ea357a08073b9dc, 5b1de649f2bc4eb08f1d83f7ea052de5b8fe141f, ad4861583851fc7730987197f68ebb681f5481e2
SHA256	29db0e21d078018f85bea7c0906a7894a4b78e74707f1cbac8f9f462eaecad23, 3184ecf43310e2487be0073a6041d292dab1f176560edf2e8e60d594ad5d2ab2, 31f50cb8ae6d41a410a39efd020ea0ed05add98df48c4257dfb8441bc6c57856, 326bb4222a2f42d4f4ca455fbe97c7ae0784fb14538b0f5d4f5088acb981fbe9, 395a3bd57246241f2c2b5efc427afbf5083facbde30b0199335f4102f73b8ae6, 3eea47b22bc68089440a40b3f899665e3584c845d8c302872e1d93b62fa59fab, 43eef76fa966395bde56b4e3812831ca75ad010e3b8216103358deb09bdc14d1, 6d817e8cd54c3a21f6d4aa437b16663a2a40b726014a8de1cbf9343101a0ab62, 6dc323456042048bdd0260c87e0deea082c855c53b6f948dbb5be27a3d721ded, 937e0068356e42654c9ab76cc34cf74dfa4c17b29e9439ebaa15d587757b14b0,

TYPE	VALUE
SHA256	aaba7db353eb9400e3471eaaa1cf0105f6d1fab0ce63f1a2665c8ba0e8963a05, b3b5fff57040c801a4392da2af83f4bf6200c575aa4a64ab9a135b58aa516080, c4c6f2c4452a540b2c69dc6164887d6014f6ab02d203bb56753c89863e840e46, d627d4b6b8e15c4538776d8dcb03c4029b461144f921589655509b9f4aab4c65, ea4c2f895f7b1c46aa8de559e7a6d8201b49437332d6d5e859052276db50c6c4, eb29edd6211836e6d1877a1658e648beb749091ce7d459dbd82dc57c84bc52b1, f957af223174a135b23c48e40a4de50494737f3d6e10e193510446e27ebb7595,
URLs	hxxp://103[.]39[.]232[.]29:18601/C558B828[.]Png, hxxp://103[.]73[.]161[.]184:17487/C558B828[.]Png, hxxp://103[.]97[.]202[.]40:11592/08388E25[.]Png, hxxp://110[.]45[.]196[.]155:14753/C558B828[.]Png, hxxp://112[.]26[.]121[.]7:19139/C558B828[.]Png, hxxp://113[.]161[.]145[.]95:19153/C558B828[.]Png, hxxp://114[.]244[.]48[.]11:19650/C558B828[.]Png, hxxp://118[.]97[.]59[.]84:18079/C558B828[.]Png, hxxp://121[.]201[.]103[.]253:18101/C558B828[.]Png, hxxp://121[.]22[.]124[.]78:17535/C558B828[.]Png, hxxp://123[.]192[.]32[.]191:18102/C558B828[.]Png, hxxp://138[.]68[.]78[.]116:11016/08388E25[.]Png, hxxp://138[.]68[.]78[.]116:11016/C558B828[.]Png, hxxp://144[.]172[.]122[.]165:15673/C558B828[.]Png, hxxp://149[.]88[.]77[.]33:19566/C558B828[.]Png, hxxp://159[.]89[.]31[.]59:16801/08388E25[.]Png, hxxp://160[.]3[.]221[.]54:15591/08388E25[.]Png, hxxp://160[.]3[.]221[.]54:15591/C558B828[.]Png, hxxp://170[.]246[.]224[.]162:15427/08388E25[.]Png, hxxp://170[.]246[.]224[.]162:15427/C558B828[.]Png, hxxp://172[.]93[.]220[.]105:20127/08388E25[.]Png, hxxp://172[.]93[.]220[.]105:20127/C558B828[.]Png, hxxp://173[.]230[.]225[.]13:11843/C558B828[.]Png, hxxp://178[.]128[.]103[.]246:17880/08388E25[.]Png, hxxp://178[.]128[.]103[.]246:17880/C558B828[.]Png, hxxp://187[.]189[.]218[.]211:16789/C558B828[.]Png, hxxp://187[.]39[.]137[.]14:12399/C558B828[.]Png, hxxp://187[.]84[.]208[.]218:17009/C558B828[.]Png, hxxp://190[.]111[.]12[.]242:17742/C558B828[.]Png,

TYPE	VALUE
URLs	hxxp://192[.]250[.]197[.]178:16932/08388E25[.]Png, hxxp://195[.]154[.]237[.]3:20175/C558B828[.]Png, hxxp://195[.]189[.]28[.]244:17807/C558B828[.]Png, hxxp://201[.]230[.]62[.]167:15840/C558B828[.]Png, hxxp://212[.]233[.]205[.]81:17849/08388E25[.]Png, hxxp://212[.]233[.]205[.]81:17849/C558B828[.]Png, hxxp://219[.]150[.]217[.]124:11825/08388E25[.]Png, hxxp://219[.]150[.]217[.]124:11825/C558B828[.]Png, hxxp://220[.]194[.]177[.]52:14975/C558B828[.]Png, hxxp://221[.]199[.]171[.]174:16543/08388E25[.]Png, hxxp://221[.]199[.]171[.]174:16543/C558B828[.]Png, hxxp://221[.]230[.]11[.]85:18156/C558B828[.]Png, hxxp://222[.]186[.]134[.]123:11700/08388E25[.]Png, hxxp://222[.]92[.]147[.]235:17538/C558B828[.]Png, hxxp://36[.]7[.]175[.]92:18879/08388E25[.]Png, hxxp://36[.]7[.]175[.]92:18879/C558B828[.]Png, hxxp://41[.]33[.]183[.]69:19811/C558B828[.]Png, hxxp://60[.]223[.]244[.]12:11053/C558B828[.]Png, hxxp://61[.]146[.]235[.]242:17770/C558B828[.]Png, hxxp://61[.]160[.]233[.]68:19583/C558B828[.]Png, hxxp://64[.]227[.]152[.]193:18336/08388E25[.]Png, hxxp://64[.]227[.]152[.]193:18336/C558B828[.]Png, hxxp://74[.]96[.]232[.]10:19408/C558B828[.]Png, hxxp://8[.]137[.]17[.]159:15066/C558B828[.]Png, hxxp://85[.]191[.]122[.]242:17756/C558B828[.]Png, hxxp://89[.]111[.]243[.]60:17320/08388E25[.]Png, hxxp://91[.]135[.]200[.]114:10872/C558B828[.]Png

References

https://cert.gov.ua/article/6277422

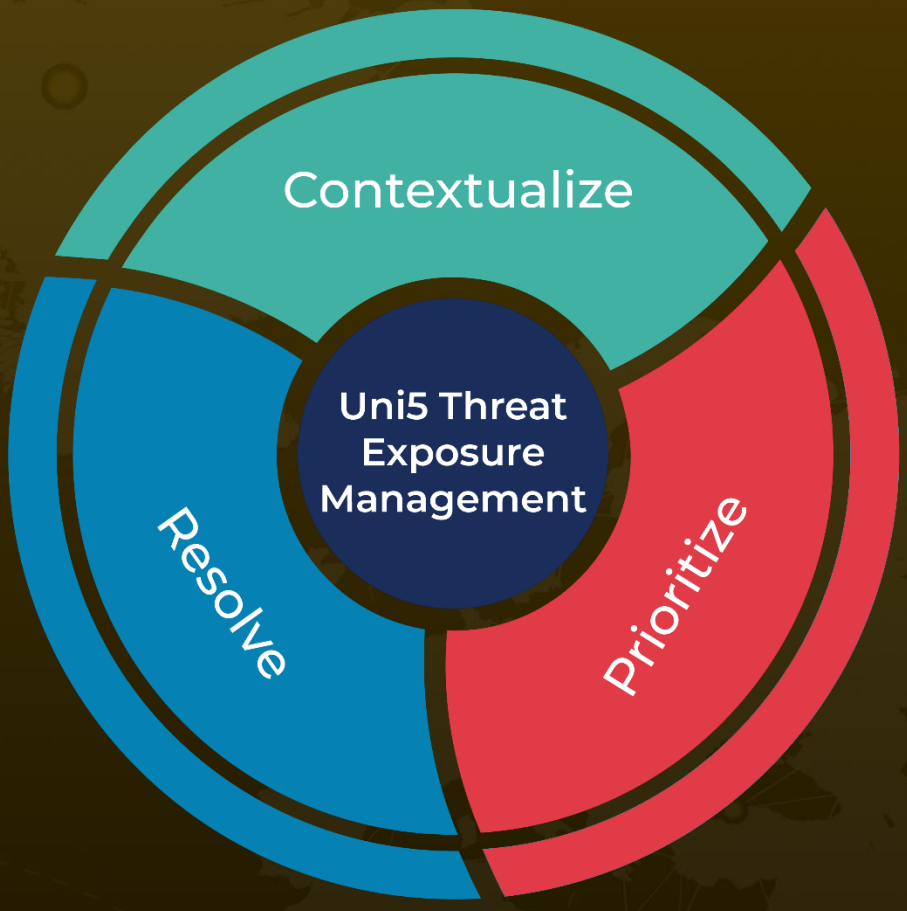
https://www.trendmicro.com/en_us/research/21/l/a-look-into-purple-fox-server-infrastructure.html

https://decoded.avast.io/tag/dirtymoe/

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

February 7, 2024 • 2:30 AM

More at www.hivepro.com