Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

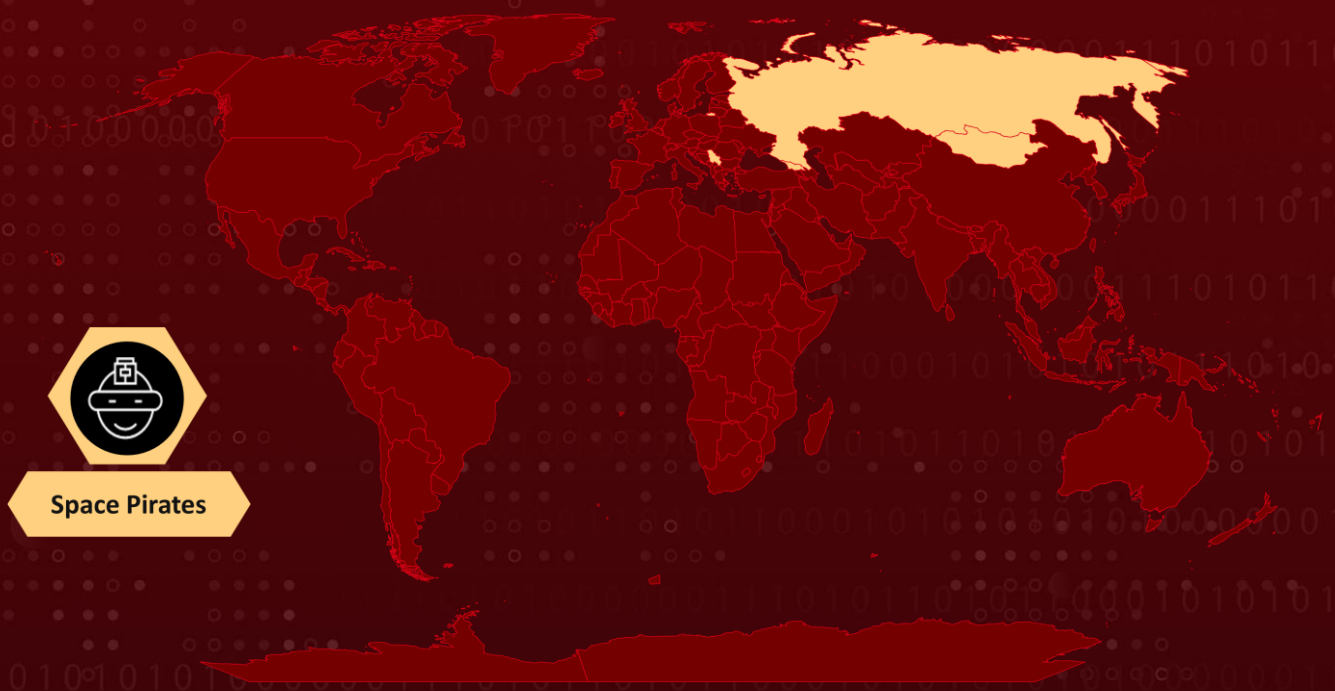
A Deep Dive into Space Pirates' Unconventional Cyber Arsenal

Date of Publication	Admiralty code	TA Number
July 20, 2023	A1	TA2023307

Summary

First Appearance: 2017
Actor Name: Space Pirates (aka Webworm)
Target Industries: Government, Educational Institutions, Private Security Companies, Aerospace Manufacturers, Agricultural Producers, Defense, Energy, and Infosec Companies
Target Region: Georgia, Mongolia, Russia, Serbia
Malware: Deed RAT, Voidoor, ShadowPad, and PlugX

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-0213	Microsoft Windows Privilege Escalation Vulnerability	Microsoft Windows	✗	✓	✓

Actor Details

#1

Since 2017, the menace of Space Pirates (aka Webworm) has persistently haunted the digital world. This infamous group has intensified its attacks, targeting at least 16 organizations in Russia and one in Serbia. While their methods have mostly remained the same, they constantly evolve, developing new tools and refining the old ones.

#2

Their primary cyber warfare goals continue to revolve around espionage and the theft of sensitive information. Notably, the threat actors deployed an Acunetix on one of the Space Pirates' command-and-control (C&C) servers unveiling their penchant for exploiting vulnerabilities such as CVE-2017-0213, which enables privilege escalation.

#3

Furthermore, their significant interest in PST email archives came to light, providing valuable insights into their deceptive activities. Space Pirates have scarcely altered their tactics; nevertheless, they have pioneered novel tools and enhanced their existing arsenal.

#4

Unlike ShadowPad and PlugX, Deed RAT is exclusively associated with the Space Pirates group. A new malware, Voiddoor, is delivered by Deed RAT. The Voidoor sample initiates the Preparatory phase by attempting to access port 27015. Should this endeavor fail, the process is promptly terminated.

#5

Furthermore, apart from deploying backdoors, the hackers have employed a plethora of publicly accessible network tools, such as Stowaway, CHAOS, Mimikatz, and numerous others. Additionally, there have been observations of Space Pirates strategically utilizing their tailor-made malware to target select Russian firms, evidently driven by financial motives, hinting at a potential dual function within the threat group.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Space Pirates (aka Webworm)	China **MOTIVE** Information theft and espionage	Georgia, Mongolia, Russia, and Serbia	Government, Educational Institutions, Private Security Companies, Aerospace Manufacturers, Agricultural Producers, Defense, Energy, and Infosec Companies

Recommendations

Ensure prompt **patching** and updating of Microsoft Windows systems to address the vulnerability CVE-2017-0213, a Privilege escalation flaw. This proactive measure will effectively thwart Space Pirates' attempts at unauthorized command execution and enhance overall system security.

To bolster defenses against the Voidoor malware deployed by Space Pirates, block unnecessary ports, and closely monitor any communication attempts on port 27015. Employ robust firewall rules to restrict traffic to this port and continuously monitor network activity for any suspicious attempts to establish communication with it.

Strengthen cybersecurity defenses by enhancing network security measures to protect against publicly available tools like Stowaway, CHAOS, and Mimikatz. Simultaneously, implement robust monitoring and detection mechanisms to identify and mitigate Space Pirates' custom malware, which poses a targeted financial threat to specific Russian and Serbian firms.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control	T1595 Active Scanning
T1595.002 Vulnerability Scanning	T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1059.003 Windows Command Shell
T1059.005 Visual Basic	T1053.002 At	T1053.005 Scheduled Task	T1106 Native API
T1036.004 Masquerade Task or Service	T1036.005 Match Legitimate Name or Location	T1197 BITS Jobs	T1569 System Services
T1569.002 Service Execution	T1543 Create or Modify System Process	T1543.003 Windows Service	T1546 Event Triggered Execution
T1546.015 Component Object Model Hijacking	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1548 Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	T1068 Exploitation for Privilege Escalation	T1027 Obfuscated Files or Information	T1027.001 Binary Padding
T1027.002 Software Packing	T1036 Masquerading	T1055 Process Injection	T1055.001 Dynamic-link Library Injection
T1078 Valid Accounts	T1078.002 Domain Accounts	T1112 Modify Registry	T1140 Deobfuscate/Decode Files or Information
T1218 System Binary Proxy Execution	T1218.011 Rundll32	T1553 Subvert Trust Controls	T1553.002 Code Signing

T1572 Protocol Tunneling	**T1571** Non-Standard Port	**T1090.001** Internal Proxy	**T1105** Ingress Tool Transfer
T1564.001 Hidden Files and Directories	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1620** Reflective Code Loading
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1095** Non-Application Layer Protocol	**T1003.001** LSASS Memory
T1040 Network Sniffing	**T1102.002** Bidirectional Communication	**T1087.001** Local Account	**T1087.002** Domain Account
T1082 System Information Discovery	**T1614.001** System Language Discovery	**T1016** System Network Configuration Discovery	**T1069.002** Domain Groups
T1083 File and Directory Discovery	**T1033** System Owner/User Discovery	**T1057** Process Discovery	**T1021.002** SMB/Windows Admin Shares
T1119 Automated Collection	**T1560.001** Archive via Utility	**T1056.001** Keylogging	**T1071.001** Web Protocols
T1071.004 DNS	**T1132.001** Standard Encoding	**T1573.001** Symmetric Cryptography	**T1008** Fallback Channels

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	b6860214fcc1ef17937e82b1333672afa5fcf1c1b394a0c7c0447357477fe7c9, 212f750a1d38921b83e68e142ee4ae1c7b612bf11c99210da60775f17c85a83e, aafb0a46610064cd88ba99672e0f18456ed827cf46b2d3064487c45bac75637a, 50c34013472f3848abb0fb280254d0514e83a65c1ce289ae199389795dcfb575, f3f122aee9cd682074cdc757844dfd4e65d6268c2a71430d77265cf369deb774

TYPE	VALUE
SHA256	6cfa8ce876c09f7e24af17bbe9baa97f089e9bf478a47d18417e399e64a18d40, b7bb9b41298420d681d1a79765d7afb7ecf05d6f0baf0b29a07b8b1af20a8c97, f554ff7eb069f0ea5ebc49e015bde1e88d4cf83f6df21e4de2056716e83fedc6, 7ee776272f7c51e41e10f5ffbd55c8c24ddb332e8c376e132e5a8cb72abd7397, ece771ab5ae8372078c378fa0cf0a1ac055ea5cbe6091f890185c02caf0edc19, 87a2176d8839e087100530ee79aa169f5078173acac2a5652527a35924ebf15e, 5c7f727c852819ae60182c4406c233f5b86962c1da3b933953058985d9f90722, ceca49486dd7e5cf8af7b8f297d87efe65aba69124a3b61255c6f4a099c4a2ab, 4f84f4333dc9c42ae4ed55c4550ebb14c8079235ae7de9fef4191251537454fc, 8c3e0fdddc2c53cf7961f770080e96332592c847839ccf84c280da555456baf0, 85d190304accb34422d3e1d603c33b86b6b8c4e88cc4713b0e0c6d4fdee9d93e, a3df5eb54f0a77cb52beccf1b2aa2caa427f80fcd047fc6be4c7aa849649e1b5, f9e97776826f83278c63cda59910c49920b7316433d9d95570dd187e154fed0b, 74ac74ea85118fe3686f9d6774de2d63db7870dadb4f0ba0d119a77d6c11323a, 057a16008ce50c3d02c910eac697748eb157afb8a6e8573adefa4b75b495a778, 66bca22ba5fbd01758fde8e57e1e251191cd1c7bb599f0beb8dd0ffd661464ac, 10d122833af8b8fec97ebdd843942bfc2bf237e3b8c01ae9f852eaca2e9cddc7, f0b8bf55a3e23379aefd9a95c556430e073ad206b4c39e0086f0a17d00ae64fe, 8a3aefd75501137f601d4b802959fb50b7cba2b135ce2ab2f1f5fa65b1a86159, 3a1e67006fb1e761e0188a04361cb7a57329346e7d0a78ef909fbc5469e3c08b, e88c7dd128c456a34804a36459f32cdf97fe30a5642caa3072ff31cda07f29e2, a2d7255cf7c8710cdec62c01b3e2c9d22600441b20914d73eb8f8af3245a9806, bfa3c91767c333a97d6849a3f885f4ed2205f24882bffbbfc916624b2601a9b7,

TYPE	VALUE
SHA256	241d1ab6a0da9dfcbc9c565d1ff948743cd7673ed334e5906a1428055cab6c82, c8c3b639c6e880d7e01cba8cb019087f0c4d2cf4dcdfa712a18054b78e525a47, 5e712e78736bde2d3ed507fb730be3a9d55d2b4ee3f7ff827f961fcada4e4e0b, c4e023110216481d0ccb09787ccc5ea46879fdf331f5d2fda2b1f33719a35104, ef17d44cde003c17c28137c6d4692eb4a1b42f86e5d6995f2f06a05e363f044a, 42ef77391f20ffc1751ded79da25376bc20a007d03e501049fff37f781df5403, cae7622a5f1ed791d317db0b3bc791a8ab71a9c68837282435f5db6bab540615, 2707602481a025da29438d01e894cfc9742389d419a5b08aa96ddc76bde38cba, 5311e4fd3329945496962c6417b74da919f5e50ae20ba7ab0d5983012c956f4b, dc3c1df20d73a62e8219ed6193ecf1229845dd0a6e42d32eb11cbaee04cfa7df, 70e43da5c5b6a8cfea8fcad768a2e5cfdf532b49b5ac87ec8ca9d05d83e0e915, 1473fcf2297376a819b6cccd50dc709fb61f48f70dc9a0eaff741c893b33d670, 67f7faf0161fdac7ebb619a2aa0c73a4a08def05d7752dfdd698d24410d9989e, 7c11eecc2fef6a2ad2e5d80156946d7bdcb9c345d542781c3116141f10eb490f, e2735841dd8ae66a825182d6d06629821c49aca44357e5980c3bfb97ace7ebf0, 374fff9a48949254d72bfe34b9b62129da1cfafb74623d187791ada09d976e7d, 86c17c549433223f3b59f5ee3e4f2694ebf4e6aabd66508a9a6fec1bdf830c61, 22c6d07b64d40811ef31113faac7293348845ab6a06f7319a653ca694c26e94a, 8c8f9fd17d1c28b471bcc4c870ab53a3b4b260ae2fd123b0ef2a2a819ce1cc78, ff9a833d34ff89660c1c5f3fa71d4d88c287c183235f714e03ccbdec7a3a6b17, 87d36c48bf6d1d9a3b157aaab45ae162b78b79b0c956383a670dcc7d9d7c14e8, 0992aa7f311e51cf84ac3ed7303b82664d7f2576598bf852dbf55d62cb101601, 8756f0619caff132b0d4dfefad4387b8d5ea134b8706f345757b92658e6e50ff,

TYPE	VALUE
SHA1	3f8ee1e875cbb01e145a09db7d857b6be22bdd92, f99f5f397fe1abb3fc25cc99fe95952fe24b6123, 1fb924ec4f0ab73a952f2a3cb624b94933275d1b, 2910415d483972cc17c76548e2b2aa5afd5bc59a, 067ca2d961b913cb2e6d6aaa92595345125d6683, 1a6e675d82e67cc41493ff991f99da70316848c4, c055f30523028037f51cc62d25ce6d38334a531e, 2404ac00114cd2481099c52b879e1776dedb2d24, ced02716f59a9a70c37eaf373c42796e6f3e93b0, e986b238cb5fe037718172d965a41c12c85bbdd0, 59239f73996a3f5a6260228cf7ca3c01e3a00822, 84ca568879ca62448d035d56bec816a11188b831, ac499c86012858f40eb78ecf3bcefae779527d73, 99cc3349b64188aae1c986afbcee7e776aa4b349, 30ad2f4a758ab2c526b6439772c7cd7cee66ffc4, 0d0c026a1661923cd184b6d0fde647128be75488, 20c83bcfd9fb45a8ba5922dbefb74d47cb361db7, e50dc750e7697ba5e28d6dde12e9a4d370076c0c, 491248fdf1141e81d5ff23eb1e44d58b50339fe2, c58d5d36201cee88a01c9913d771723edde302e4, 0912822548e5983f8a2b6d77848994f6d929ffed, af71956b59b9c05acdcd7badecc232ca6237cc8d, bfe05003730d79f0004cc41e09f48944df6f68fe, 19da36d73e0a72f65c8a9f6fc2e2504ed599b57d, 6e0c406d07206b588652729a271e054c416b5c90, 338881ff10434b523feb63a8a66370f444378cc7, f4a5778b74b73745a533f22d33a65880f2968705, 57792f875625fec78bea22af46010bd34dff863a, a24d306d0ed0061485cb05901cf9fc9d5f07c097, c321233155af13a53ecd746eaab84cc6ac69d510, 6f8cc7abbf3185a085aa43186c5da332b04c3156, a7de9de3774ad507e7d1ddfcce4924625a600434, 493e89a70c4176dcec50f34b79eaa4f910e50800, ab64d32da52a1e516b0c874aad006db404f9c21e, a3225a0bbb66b5babf52466ae23a1538407f0cef, c5c844582c0590cdc901c253a1215682511 54c61, e49d21f1e66268715efc6003c4e2d3b98cee666a, 28ed17b046e0bed3d1cde67eccf241ecf01fe3c4, aa42f3758dc599e6184894a2911e774c2e16b92d, 57b138f2bb4731b1c50a034aff3013bce735267c, f95deea8d824ee681341f9457e0a86129ec4eb91, 1749f99443b345860dd037940505421c45156950, a8808089c37faacebc19bafd2677ba011afffc49, 154da55173f97c50e41e48157bc94515cc6146ec, 89375a28a96286584e321401915bff2860190470, 3caf909e6590a4ae2db99ae577d5585d854ad15e, 7abf05ccdf0709aacae2ebe07b7104c81b19abe1,

TYPE	VALUE
SHA1	fc6b59571353c74d4d8cbd254ea7b216f8449208, b85fec5a965785830af1cf5534ef6a3b437542c2, 8ef130998044df15395dcf50123e5a1d8f6ce208, Ec5394b93c376e359a8a2c380622e3a9d033d0de
MD5	972a1a6f17756da29d55a84d7f3f23a4, 51ca39e3700e9ed16d90302dd31f3a1d, b0b438bcb2a71233721a2ddcdb765a68, 0fa4a2b8210500427bb23d2d92502964, 804824203f31ebfb56e580e73e932d26, 38c43e589e3dc65258322d91b58e2e15, ef6264abe296357100e2db48820b13f6, 24ec73b4e1845088a28dde0007c2d6bd, d217fe96c7737ac318321deafc4cd261, 633ccb76bd17281d5288f3a5e03277a0, 77ef4bc2f23ef97add7ec0ad229396a4, 8002cd74e579a44a78b2c8e66f8f08a4, d4e51120c368ee4ef5f5571756803fd3, 66e8f82a418923b92bef57ad61bcebf3, fb23fc47484150250cfd7b1260e23524, 99b86ad9bf6193b044076df373534fad, 4db33e5390bfebd84e38cbb85b75c006, dbb5995037745e04d03dc7f2985f017f, a94277fad94ca6fbdb2b8eeb716bac90, 7aa890406a74a44f17fe665653bd92e2, 9faf04fc6e522050527e71dea5918d01, 1a04af6c3abe8f67bf98adc588c46736, 6d52d0e7f49817c6315b308cb973d405, 8e3217391e11cabf6f9a62a35c636835, 97c00cee887279f12f309a86e7bc3638, 5d0aa944ce19e0a70adad562ce0e7880, 1d07e53969cd1cb34db944bfdfa5bf6f, 81a93165b338dd5ebb59841e199e0460, a2221a72d42b978c0f295557a100d574, c1be341ffc0f58bafdf4e5210b881106, 9a6b1bd3b7f13d30d1595b874f513744, ab6a57e40ba74135de9fc6b8f37efa7b, 7949b560ecf60644e2b537199589d67b, 81de205ac5e44e1167c0c01c7207c6c4, 4fdb78de4da91c06e5778feb560750f4, 2ec55245fbe57cae1a045f9106ca709a, ffc18496b2b1563e081beefc9e884769, ef4d35b1780cb1799eadb648f4e7b5b5, 01b596051d1fa4785ef4e73dc3f08ec0, 54c7f04fc5418553812910db8adc6995, 824fbfa8b35f19152a834a1bfff9ef54,

TYPE	VALUE
MD5	48097e614cdf1f9c908b7449cd1119c5, 3cf999dd950af82cad3f8c6eb5430bd5, 6d3ce5d4003ce4c9af3048826638ab82, b33e5e2e14b0fbe319f6a8b719c43c1a, 8ec966f8b441fa20225e08ffd5e83f94, 3381df84cf05826aff084002ba323774, 8a7b4985db84e9093e169c237b853adc, 5e25310d2ada344715cf8edd5e64a848, 0c19d2e8bc1429fac245dd6c870afbe0, D0ea84204096109f18a2201fae1c4f30
Domains	0077.x24hr[.]com, alex.dnset[.]com, amazon-corp.wikaba[.]com, api.microft.dynssl[.]com, apple-corp.changeip[.]org, as.amazon-corp.wikaba[.]com, asd.powergame.0077.x24hr[.]com, bamo.ocry[.]com, chdsjjkrazomg.dhcp[.]biz, comein.journal.itsaol[.]com, elienceso.kozow[.]com, eset.zzux[.]com, fgjhkergvlimdfg2.wikaba[.]com, findanswer123[.]tk, freewula.strangled[.]net, fssprus.dns04[.]com, ftp.microft.dynssl[.]com, goon.oldvideo.longmusic[.]com, journal.itsaol[.]com, js.journal.itsaol[.]com, lck.gigabitdate[.]com

Patch Link

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213

References

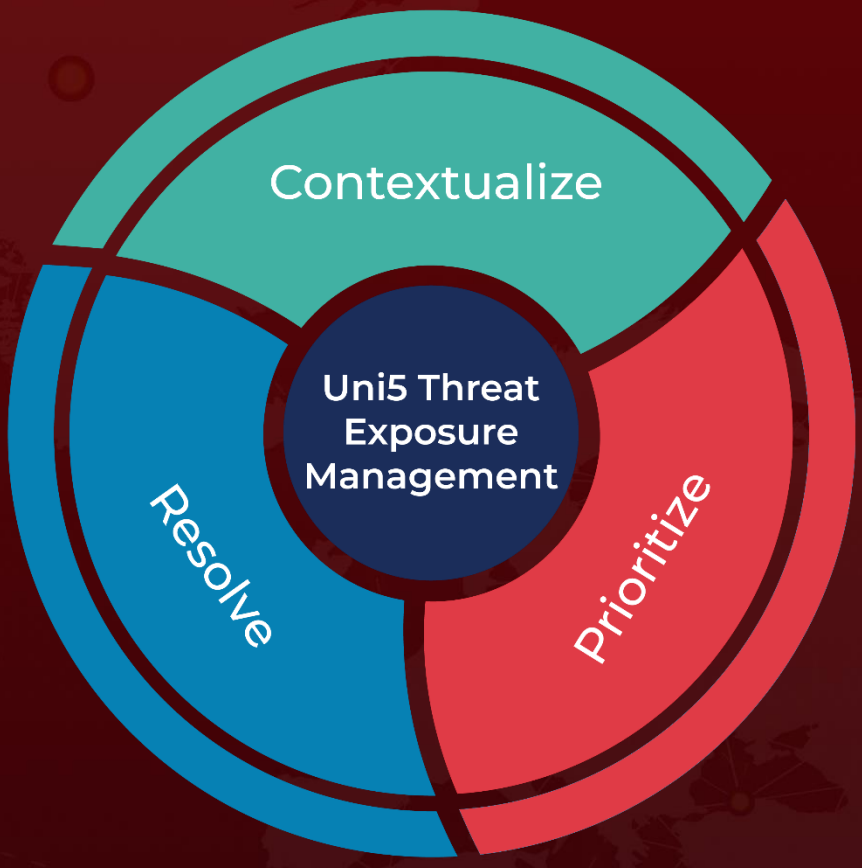
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/#id4

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/webworm-espionage-rats

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

July 20, 2023 • 8:00 AM

More at www.hivepro.com