Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

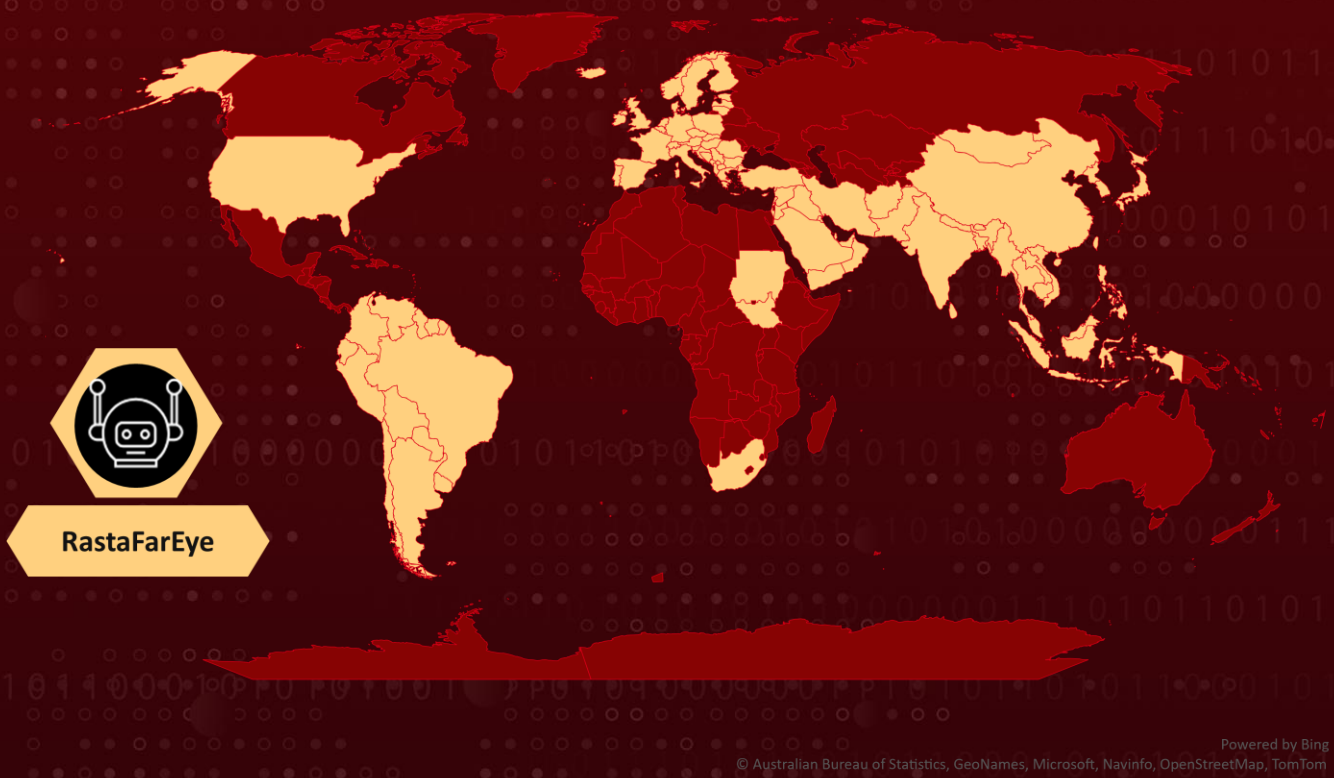
The Lethal Advancement of DarkGate Malware-as-a-Service

Date of Publication	Admiralty Code	TA Number
November 22, 2023	A1	TA2023472

Summary

Active Since: 2021
Malware: DarkGate (aka Meh, MehCrypter)
Threat Actor: RastaFarEye
Attack Region: United States, Europe, Regions in Asia, South America, and Africa (excluding CIS countries).
Attack: DarkGate, a formidable Remote Access Trojan (RAT), functions as a Malware-as-a-Service (MaaS) and is masterminded by the elusive RastaFarEye within the underground cybercrime landscape. The latest iteration, DarkGate 5.0.19, advances upon its predecessors with sophisticated evasion techniques and a comprehensive toolkit for credential theft, keylogging, and screen capture.

Attack Regions



Attack Details

#1 DarkGate is a powerful Remote Access Trojan (RAT) that enables the thorough compromise of targeted systems. Marketed as Malware-as-a-Service (MaaS), this insidious software is the creation of an entity known as RastaFarEye, operating within the covert realms of cybercrime forums.

#2 The latest iteration, DarkGate version 5.0.19, expands on its predecessors by integrating advanced evasion techniques, commanding control capabilities, and a suite of modules dedicated to credential theft, keylogging, and screen capture. This comprehensive toolkit provides malicious actors with the means to exert complete control over victimized systems.

#3 Offered through a subscription-based model by RastaFarEye, the pricing for DarkGate's malevolent services can reach up to $15,000 per month. To stay ahead of security measures, RastaFarEye consistently issues incremental updates to DarkGate, aimed at thwarting antivirus detection, introducing novel features, and rectifying identified vulnerabilities.

#4 DarkGate typically dessimated via phishing campaigns, where malicious links embedded in emails serve as the initial infection vector. These links lead to either a Visual Basic Script (VBS) or a Microsoft Software Installer (MSI) file. Upon execution of the VBS dropper, obfuscated code initiates the download and execution of a Windows batch script from the command and control (C&C) server.

#5 This script, in turn, is responsible for executing a PE file that functions as the DarkGate loader module. Versions of DarkGate post-v4.13 incorporate mechanisms to circumvent endpoint security and antivirus solutions. DarkGate v5 introduces an innovative shellcode loader, responsible for downloading, decrypting, and executing the final payload.

#6 Furthermore, RastaFarEye actively monitors threat reports, swiftly adapting DarkGate's features to elude detection. The malware's adaptability, rapid iteration pace, and the depth of its evasion strategies underscore the sophisticated nature of contemporary malware threats.

Recommendations

Network Traffic Monitoring: Implement robust network traffic monitoring tools to detect and respond to unusual or malicious activities, especially those associated with DarkGate's command and control infrastructure.

Employee Training and Awareness: Conduct regular cybersecurity training for employees, emphasizing the risks associated with phishing emails and the importance of not clicking on suspicious links or downloading unfamiliar attachments.

Email Filtering and Security: Strengthen email security measures, including advanced filtering to detect and block phishing attempts. Educate users to recognize and report suspicious emails promptly.

Zero Trust Architecture: Implement a Zero Trust architecture, where trust is never assumed, and strict access controls are enforced. This mitigates the risk of lateral movement and unauthorized access in case DarkGate gains a foothold.

Blockchain for Threat Intelligence: Enhance your cybersecurity strategy by incorporating blockchain technology to build a resilient infrastructure for securely storing and safeguarding the integrity of threat intelligence data. Organizations can achieve this by embracing a decentralized storage model, implementing smart contracts, employing cryptographic hashing, and adopting permissioned blockchain architecture. These measures collectively contribute to the creation of an immutable and trustworthy ledger.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact	T1566.001 Spearphishing Attachment

T1566.002 Spearphishing Link	T1204.002 Malicious File	T1059.001 PowerShell	T1059.003 Windows Command Shell
T1547.001 Registry Run Keys / Startup Folder	T1055.012 Process Hollowing	T1543.003 Windows Service	T1027.002 Software Packing
T1027.007 Dynamic API Resolution	T1027.009 Embedded Payloads	T1055.002 Portable Executable Injection	T1574.002 DLL Side-Loading
T1622 Debugger Evasion	T1036.008 Masquerade File Type	T1555.003 Credentials from Web Browsers	T1056.001 Keylogging
T1528 Steal Application Access Token	T1010 Application Window Discovery	T1217 Browser Bookmark Discovery	T1083 File and Directory Discovery
T1497.001 System Checks	T1614.001 System Language Discovery	T1518.001 Security Software Discovery	T1005 Data from Local System
T1113 Screen Capture	T1115 Clipboard Data	T1071.001 Web Protocols	T1132.002 Non-Standard Encoding
T1573.001 Symmetric Cryptography	T1219 Remote Access Software	T1041 Exfiltration Over C2 Channel	T1489 Service Stop

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	83037a444567a6d47b6221288cdad4e9, 3f2ae21059230fd9d7e72a1558cd81eb, 9bf2ae2da16e9a975146c213abd7cd4f, 63f9b76e4bf4983e13eba7e22dd22781
SHA1	7cf2487dc111a590f9db5c041f9f3ad84622e044, b4124a0428b45bf73b97095cc9a453306f0337bf, b4850a42227dc43d4079392eb3a449e8a3f6312d, a25081cf2da611b827f11f653ddcc2f18647ff93

TYPE	VALUE
SHA256	6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e, 73c0d0f220a30b541e0855e8039b8050d1332ff03c3e0c8a35671bd5eb9d30be, 74729d4569691daf72e23849e91461471411f551639663e11e1091a48790611e, bec37877e3bffa222efb5c5680c7defd2d917317293d7fa70e0882ad45290a40, a448c4abbb2f1844a8fa0c929cd84c2f6f57a4af0442a6a4b5307af89c35cef6, bc80b13b639ee4b4a6a79555cb4daf3ec360682322ffae68c1272b5aed8b1593, 5b608a6729343cf8b6752d5bb201f906920fcb472f5949e04173b907f65ceff1, 6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70, 394ee7c88a0925698ce1a2e0268ca49404591eb5cdd961d657d785993212cd86, aa92f9692dfa98ba9ee991156612f2015c10a5ecf02b605b0b6d528827430601, de2064d4363a3ccbda5518c619f1c803393b0876e349530583a72b1d1643c16a, 54f52ef506f6649c09838b9935aed223f0f320798e13fdb9541ffd1db3e08816, 9f48b63528a24a1241f0bc793e960d420314d595c9927e2294f4475c4be143cd, 9a7db0204847d26515ed249f9ed577220326f63a724a2e0fb6bb1d8cd33508a3, 23885818c2a665d5a57ba16acfe46db68258da619a8db3df8f069c0205ac648e, 9b9514d5af8a9c92e7596dc15aadba0defaedd9f08ec50a588279aa6f6b8ea80, 0e01bad874c61d09d09ce06f76f5e46f6648a1fc943644874c8e1a53a93af9a7, c9b3e70c459be9643f764afd535976f9d308d098e1476013de431e7aea22b3e9, bb37b05a34b2547941efdceee54ec8745e2ce7a7d5d0968c3b5c10274dc81880, 5be83d13f20b4a044a8c8281d13723a808555cdd73a7ddcec37422a4e44fbd4e, 4e48d4c355ceb58267a29fd3337b101722c805a7e53662816b73ce9b756ae321, bde8e0c4bc687ea485fd4a00c86bd25ab14a04edf9b2bbc03808e9b86074717b, cde0f0b6a29a11aa8a5a4ee543fd632cb460bc11927c7153c1f5f8664e474d23,

TYPE	VALUE
SHA256	3a5e7ce24fc5a18843e4f877f5c704bf95eb90c039bc8d791273c191e4ca3242, 4325d78175a803fb6a1d235e8255816a07283501087e1b115f28c38b6b542856, 22933b3ae7d125f312b6d1fe6356092cdcd1def6dca3ad128de65ba7986266ae, f8fcf37ab1e391d1809c4b5baf00d669c4263682d99230432c5199bde5914a60, a3fc0ef279b5717d0b0dcbe25f8e543efee252cc116336a744968279ce9d3c29, 1776dcbc4a3f430dd5ace833aac80b0954a050e5a7dec164b53b62fbe72feab3, 59c026ed7f98aff21521b7a76845821aa5f1ce1a978d1c90404c073bd6310a1d, acad12dd611551ee4cdfd9fba7dd06c1f6a7c4d8cd8619cbbafa3d8f88bde910, 659733a584c52078ac6b568dfb34a089bef2b3835a5ea737d32c1623a468b743, 7c6fa5cec54bc8afa51376db19c9c83d7c17f6e21ce761bfb1daeb7ad31d898d, 6610e152e07225c91a723f3b65e33af4b0df0d816dd69fe73f9d25dc0fc975d4, b7874a778f21b2d21a2a2ab2c2ec4a7ae5042443e1d3f20a070424d628079056, 00dbb5f6bbb9c230fc0c7f7526b46d697850587b30d0b4f4d54106eb3a3d5410, fa0a47360f68f211413d582d2c73035594a9191c2399c52612c940b45402065f, 2caa6b5e92ad4c772166860d428d388a4fa376c5adc439b10ee2f045e0a1b003, 2bf6b1dcb11e7e32b353e0c135aca9c979177d14aa9834119cd8e4c1a5b08562, 2d08809875f2cfcbe4538d11ee5537768beba0b7740e1785ac35fd90d32e5c25, 6bc0a512fa3d69c724c2a0aaea8f915795f9c0ef68617dbd32d3b78ee5cddc06, 70e79ddbcc5bb1f9d40133e4f3dbcea6362794854d47b6a2081f1439ff795dcd, 37ea8a57e3d3964448238aff31125381c7063b98e1fe0d83a20b315b70546c94, 6a81b3d6606bd5c4f9d3484719ec35fc6d2dedb902a85553705a71a6e1273104, b2db96bae6065dbea52711c6f732a29bd39cbb4e81dde9e7d854d52cfb1970f0, 8458a43245c6ff9e3d688a8393f692d3088bf5338ae810ff78b8b3a1d751a87e,

TYPE	VALUE
SHA256	09bf1b88716c49a62cb4ff708f7ff4f09cb7c3ff42e58661802cd66f1a2a0311, 7999c9ba66c57b8f2932f54db723feeef411295f8ed6a6d403376278153745c6, 2ffb2a102df381c9688cc78c2cba4faa6a561d5aa78a9163888ebf7c73bdc8d0, 453e7fabfa2d6fca1f9a5b9edc456e46417d8fb76332d397a39fcc8e76ccf54f, 96c84918db77c8bc7d5080aca1b618f7ea7c824d27f67b2346364756f04b3226, 20cd543224dc3229dece35f018678a52fc98e533596e4995a5534bde0e7e161f, f02928ec21ad8c600eef3e3a006581a3af858975cbc2ad29ba3dfdd1a78d3cb9, c6bce64cf86ff6f6b52b9ffa8b8dc2283645b9f0cea7391117d5dd80c2092ce6, b7c6b567eab740efa575826c94f4c9c552ed5894b8b3ef57e77959b740d8bec8, 1af981d9c5128b3657cdb5506d61563e0d1908b957e5dd6842059d6d3cfdc622, b68736ce13dd44a60e7c462b4f451a4132187a0b76adf9cc201a1468379e7601, b6b2b1773fbd354cc7fcf409f4b4208e570be077658c2a92ea59319c250d9f8c, bd8fc787abfebba8d167e9979c2ec692f861ab21ea138c3381daa852a58677be, fffa5abebf578cfc2200b4856889e397e412e56c5bff0032d2d7565d9286685f, 22d5fdd23ff4302517d5652375ee5ec3bfb28cb964015b3e9902d2398c908fd9, 684b3445349d8e08e2f2d33f3b30d509a3fde82cb798ccbad2726105301a9470, da27475894815900fefb9d383de0d255bfa3b7a22927b2912a2d614742b3109c, 2b49ceb658da03b30d38ee2dc46bcf2bb85af728cece29f8c30d7c1a92c1ad09, af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b, 063ea8cd25e166182ef68ab1b1157e6448caccaa89cf0f0166c08c21501bf273, 9a19aa451bb9974c05e616bf02762ee001cc02669aca15150199415e5e190f01, 3c520028ad9dbf10e5a94023fbbd5ca7134802a6def3fae427f70620c12f8988,

TYPE	VALUE
SHA256	bd9426beaee1c5908b0f71b31539ae4fe3ffed155ab00041b543d48fda3f1654, 6345b02dc1606522232ac853a0e2599d166aef91ae1d7f4d4104d184273dc1e8, feeddfb2a7cc4945eaedd8f75907c42ff097252c3e38d7ef2006bd7a191f09ae, b15e4b4fcd9f0d23d902d91af9cc4e01417c426e55f6e0b4ad7256f72ac0231a, 7d2c98c8d667891c33119d314d1945c285e2a28701970532f6272cad91f59028, f1fa42c3d50d4468b9ac3f7e5cdb1160c8f7ed7bbb6e4017859b837dac7e8d93, a2be457dc7fc5d5662e5db1b51b77094898449fedab7b1a9f837c093c249c5ba, cb93d34f34e5e999705fd5d17d6725b452c57bc799fc835899e4af9330f4169f, d2b24a51e7e12fded160344bbac9ee1a9082b690d0c6f326170ea8a224038215, aa5cb7f6ccb5470ff643cfcba9254263c9db9e7a84984d30166cc14945e219f2, 3b271f7f34255146366ab7c7d916fa5ab3b1accfc4b0f3d727e16690cfb7ad3a, 2f342c83cc564e0110f2c0a32a3259f0ef624cd47c50d82000b308411a402c17, 8ff356af97443bd2b028eb57f160a92c2a1ecab2d227977a87a221ae6409c4be, 1239ab2c5b8f4445353eacba276938c9cce9711a643851db8979728defc5a3ee, a63bce69103155accf3c836e7bedf155bee789276624def8713a4431d6562883, 1d256c2fd442e69120cdf8d12d7bd865f058ec667e2119a66259fc9052dbaa36, 9e398fb049ae1cf95976ba1c80280cb3f78833569fe7fc5c1ba93c7e57c00fac, 284458ee75b1d1c2f07ad9fe3a811589360c23092852b2b80a67d2e25e06b269, 2d8f91bb2359c13abf0ff31af101fc6ecb39849350fbfde015b549e97c8877d5, 7837e71f9bf00f48ab5336ed8647b116471561181069b79d29dbaee0e951ded7, 6a9e7b47bec075225861d61cf20555c38a17b7b9ff46ff85de7f6791c548cc2e, cefc06b2bec8d175eaa9bf3f91c8246731811a8ad7b52af336478655dbc70039, 4aea930309b590d34488187a8c9cb31b83ff1faa2ff4d27606e50fac3a0db742,

TYPE	VALUE
SHA256	975d1510380171076b122cd556a1a05bd1eca33b98a9fd003fb3662cb8c83571, 92372f91137114704b5c7cc10882eced9636997486832c5504551e2ba894cb34, 3a543dbe70ef5fc78e2fd8b2752e36892f705fc56c54837e248611941dea49c1, 6311ed9b17dfee292dcdc9dabbde47a1148e384c33d8ee8294b3e32111ce80a4, 07e7ce324773077d571c026405790fe61209008017e71313a3713e9d9095fc4d, 1da4bf9ef73b820612e493877ccd3dd065763d161d03586e189b21732fe09db4, 209c9c9bf25a922e62163f8d2d525b046b345d14c29bdfac0a05c837060052d93, 8b7f551954d4f474b4265aa56b5ad93c7a0d08774ecfd25c2d6b63dfb9052889, 965f2a99685f9777da6c5d21cd4654357e34c7abd7c0c8190c19815d21d9be29, ad36b909721d64a3c32678f4c2ca758d81661088ba1ed57bec50ef0ac4d4a871, 00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df, 0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2, 10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896, 2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4, 74f21cf5ab72aad0f7f3cf3274a167c20e787f9513019510561f39d4230f3c4b, bc5ad215876055a8a6a097579e16d24e233a323a6157afbb6db49705ac12a1f1, E7b76e11101e35c46a7199851f82c69e819a3d856f6f68fa3af0636c3efde0ca
IPv4	107[.]181[.]161[.]200, 149[.]248[.]0[.]82, 167[.]114[.]199[.]65, 179[.]60[.]149[.]3, 185[.]39[.]18[.]170, 185[.]8[.]106[.]231, 45[.]89[.]65[.]198, 5[.]188[.]87[.]58, 5[.]34[.]178[.]21, 80[.]66[.]88[.]145, 89[.]248[.]193[.]66

TYPE	VALUE
Domains	bikeontop[.]shop, drkgatevservicceoffice[.]net, msteamseyeappstore[.]com, naserviceebaysmman[.]shop, positivereview[.]cloud, private-edinmarketing[.]com, reactervnamnat[.]com, sanibroadbandcommunicton[.]duckdns[.]org, xfirecovery[.]pro

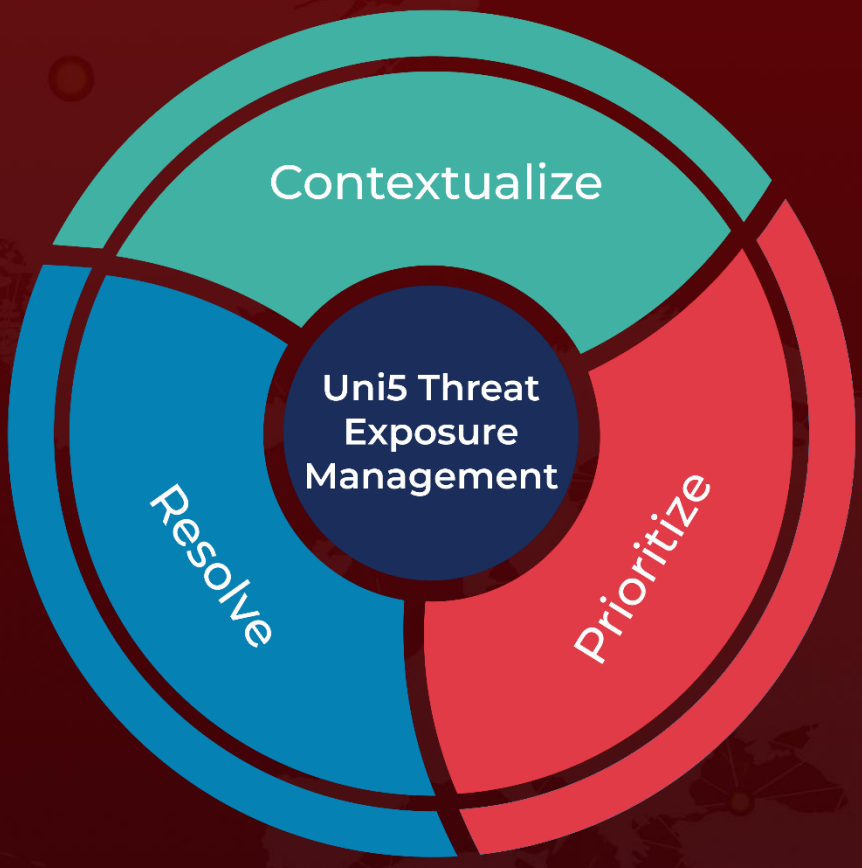
References

https://www.trellix.com/about/newsroom/stories/research/the-continued-evolution-of-the-darkgate-malware-as-a-service/

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

November 22, 2023 . 4:00 AM

More at www.hivepro.com