Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

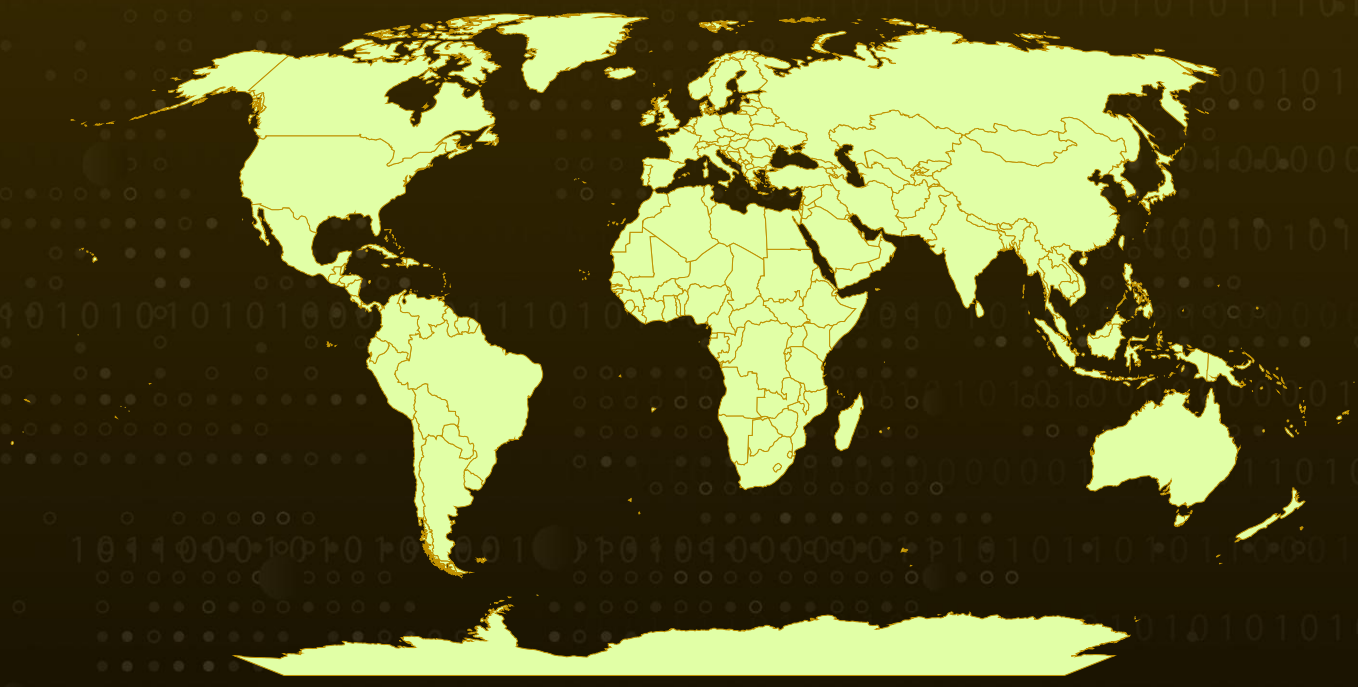
Black Basta's Evolution: Sophisticated Social Engineering Meets Advanced Payloads

Date of Publication	Admiralty Code	TA Number
December 10, 2024	A1	TA2024457

Summary

Attack Discovered: October 2024
Targeted Countries: Worldwide
Affected Platform: Windows
Malware: Black Basta Ransomware, Zbot, DarkGate
Attack: The Black Basta ransomware group has shifted its social engineering tactics, now distributing payloads like Zbot and DarkGate since October 2024. Their approach often involves email bombing, where a victim's email is flooded with subscriptions to numerous mailing lists, creating a distraction or hiding malicious activity. Despite these new methods, the group's objective remains consistent, gain rapid access, enumerate the environment, and extract the victim’s credentials.

Attack Regions



Attack Details

#1 Black Basta ransomware operators have recently revitalized their social engineering campaign, introducing advanced tactics and payloads. Initially observed in May 2024, the campaign underwent a significant update in August, enhancing its malware delivery techniques and evasion capabilities. Threat actors leverage email bombing and impersonation tactics, frequently posing as help desk staff or IT personnel via Microsoft Teams. They utilize genuine-sounding names and profiles to establish credibility, often coaxing victims into downloading remote management tools like AnyDesk, QuickAssist, or TeamViewer.

#2 A notable escalation involves the use of OpenSSH clients for reverse shell creation, along with novel methods like QR codes to bypass MFA after credential theft. Payload delivery mechanisms vary, encompassing compromised SharePoint instances, file-sharing platforms, and direct uploads to targeted systems. In one instance, a customized credential harvester tool, AntiSpam.exe, was used to exfiltrate user credentials, storing outputs in files like 123.txt within the %TEMP% directory. This harvester is often paired with loaders such as Zbot or DarkGate, enabling further payload execution and data theft.

#3 The operators' malware arsenal demonstrates high sophistication. The Zbot variant, SyncSuite.exe, employs advanced techniques like process hollowing and encrypted configurations to evade detection. It establishes persistence through scheduled tasks and registry modifications while encrypting collected system information. Similarly, DarkGate malware deploys randomized keys, have keylogging capabilities, and performs process injection techniques to maintain control over infected systems. It further enhances persistence by exploiting mutex mechanisms and spoofing parent process IDs.

#4 These developments highlight Black Basta's adaptive approach, blending technical innovation with manipulative social engineering. Organizations must bolster their defenses by implementing stringent security protocols, monitoring for unusual activities, and educating users to recognize such sophisticated attacks.

Recommendations

- **Enhanced Email Security:** Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.
- **Secure Platforms:** Enforce stringent policies for platforms like Microsoft Teams and other collaboration tools by restricting communication to verified internal users only. Conduct routine reviews of access permissions and actively monitor for anomalous activities or unauthorized interactions to ensure the integrity of organizational communications.
- **Harden Remote Access Tools:** Limit the use of remote management tools like AnyDesk and TeamViewer exclusively to authorized IT personnel. Implement application whitelisting to block unauthorized installation or execution of these tools, reducing the risk of misuse by threat actors.
- **Implement Behavioral Analysis:** Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.
- **Implement the 3-2-1 Backup Rule:** Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1587 Develop Capabilities
T1587.001 Malware	T1566 Phishing	T1566.004 Spearphishing Voice	T1055 Process Injection

T1055.002 Portable Executable Injection	**T1056** Input Capture	**T1056.001** Keylogging	**T1558** Steal or Forge Kerberos Tickets
T1558.003 Kerberoasting	**T1033** System Owner/User Discovery	**T1572** Protocol Tunneling	**T1219** Remote Access Software
T1218 System Binary Proxy Execution	**T1218.011** Rundll32	**T1649** Steal or Forge Authentication Certificates	**T1055.012** Process Hollowing
T1656 Impersonation	**T1036** Masquerading	**T1053** Scheduled Task/Job	**T1070** Indicator Removal
T1082 System Information Discovery	**T1074** Data Staged	**T1620** Reflective Code Loading	**T1041** Exfiltration Over C2 Channel
T1498 Network Denial of Service	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1140** Deobfuscate/Decode Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	admin[@]youadmin.onmicrosoft[.]com, administracion[@]delparqueflats[.]com , firstlast[@]bilipow.onmicrosoft[.]com , firstlast[@]brandonsupport.onmicrosoft[.]com , firstlast[@]cofincafe[.]com , firstlast[@]cofincafe[.]com, firstlast[@]cofincafe[.]com, firstlast[@]cybersecurityadmin.onmicrosoft[.]com, firstlast[@]cybershieldassist.onmicrosoft[.]com, firstlast[@]databreachsupport.onmicrosoft[.]com, firstlast[@]endpointshield.onmicrosoft[.]com, firstlast[@]eps.udg.edu, firstlast[@]filtrocorp[.]com, firstlast[@]helpadministrator.onmicrosoft[.]com, firstlast[@]itsecurityassistance.onmicrosoft[.]com,

TYPE	VALUE
Domains	firstlast[@]itusaacademy[.]com, firstlast[@]malwareremovalassistance.onmicrosoft[.]com , firstlast[@]networksecuritymonitoring[.]onmicrosoft[[.]]com, firstlast[@]pereirabrito[.]com[.]br, firstlast[@]safesoc[.]onmicrosoft[.]com, firstlast[@]securitypatching[.]onmicrosoft[.]com, firstlast[@]servicedeskadmin[.]onmicrosoft[.]com, firstlast[@]spamprotectionmanager[.]onmicrosoft[.]com , firstlast[@]spamprotections[.]onmicrosoft[.]com, firstlast[@]supporthelper[.]onmicrosoft[.]com , firstlast[@]supporthelpspam[.]onmicrosoft[.]com, firstlast[@]supportteamsservice[.]onmicrosoft[.]com , help__desk[@]llladminllll[.]onmicrosoft[.]com, help_assist[@]llladminllll[.]onmicrosoft[.]com , help_desk[@]hegss[.]onmicrosoft[.]com , help_desk[@]llladminhlpll[.]onmicrosoft[.]com, help_desk[@]llladminllll[.]onmicrosoft[.]com, helpdesk01[@]1helpyou[.]onmicrosoft[.]com, helpdesk1[@]truehalp[.]onmicrosoft[.]com, helpdesk[@]1helpyou[.]onmicrosoft[.]com, helpdesk[@]adminsteams[.]onmicrosoft[.]com, helpdesk[@]asssistingyou[.]onmicrosoft[.]com , helpdesk[@]hegss[.]onmicrosoft[.]com, helpdesk[@]llladminhlpll[.]onmicrosoft[.]com , helpdesk[@]truehalp[.]onmicrosoft[.]com, helpdesk_01[@]asssistingyou[.]onmicrosoft[.]com, helpdesk_1[@]asssistingyou[.]onmicrosoft[.]com, helpdesk_1[@]suporting[.]onmicrosoft[.]com, helpdesk_1[@]youadmin[.]onmicrosoft[.]com, helpdeskmanager[@]hprsynergyengineering[.]onmicrosoft[.]com, quickassist[@]1helpyou[.]onmicrosoft[.]com, technicalsupport[@]bevananda[.]com, sslip[.]io,*[.]doc[.]docu-duplicator[.]com,*[.]doc1[.]docu-duplicator[.]com,*[.]doc2[.]docu-duplicator[.]com ,dns[.]winsdesignater[.]com ,crystallakehotels[.]com,summerrain[.]cloud,mailh[.]org ,file[.]io,bigdealcenter[.]world ,brownswer[.]com ,blazingradiancesolar[.]com ,posetoposeschool[.]com ,arifgrouporg-my[.]sharepoint[.]com ,binusianorg-my[.]sharepoint[.]com,dropmeafile[.]com
IPv4	185[.]130[.]47[.]96, 65[.]87[.]7[.]151, 66[.]78[.]40[.]86 , 184[.]174[.]97[.]32, 212[.]232[.]22[.]140, 8[.]209[.]111[.]227,

TYPE	VALUE
IPv4	8[.]211[.]34[.]166 , 109[.]172[.]88[.]38, 109[.]172[.]87[.]135, 188[.]130[.]206[.]243, 46[.]8[.]232[.]106, 46[.]8[.]236[.]61, 91[.]212[.]166[.]91, 93[.]185[.]159[.]253, 94[.]103[.]85[.]114, 193[.]29[.]13[.]60, 88[.]214[.]25[.]32, 147[.]28[.]163[.]206, 45[.]61[.]152[.]154, 185[.]229[.]66[.]224, 172[.]81[.]60[.]122, 145[.]223[.]116[.]66, 185[.]238[.]169[.]17, 179[.]60[.]149[.]194
SHA256	146494EB276FC4539BFFA6896B958E29A417A5959A5C10D100CAF48514B66864, 67c8bc21bbdcc59f7fd2b0a6f0f6c98f0076a0142e94cb3f158155e0ca9ac71a, ebbe6a9e1188e2ee1651b5c68b6b508fb52b9e8896dbbeb0f4e126961ba94982, 97DAF5E1B2519A655397173FB5AF346F9435FB4ACF097D10AD4FFDE464D21C09, 5E9FBAE0B94F6E36717BBD2C997981BA438D7EFD800E76924F73452A69C04051, 3B7E06F1CCAA207DC331AFD6F91E284FEC4B826C3C427DFFD0432FDC48D55176, EF28A572CDA7319047FBC918D60F71C124A038CD18A02000C7AB413677C5C161, 9a21ec5a25dfe7ca51d4a843a96bfb6e650dc999d3b6d4bd771571359b3bea0a, 1896ab744e436ca52a1c6c64a4608dbb8e5597e35d13be1f3c56bc65eb44e532, 14aad4fcc77e5fd7e7782c9c5714d1a4187e60e75a765b71d5d41b920bbae31a, DB34E255AA4D9F4E54461571469B9DD53E49FEED3D238B6CFB49082DE0AFB1E4, 49405370A33ABBF131C5D550CEBE00780CC3FD3CBE888220686582AE88F16AF7, c4942f989530f09b499978721d282998eaa77be31a4361ac6250f1df721decb9, 22c5858ff8c7815c34b4386c3b4c83f2b8bb23502d153f5d8fb9f55bd784e764,

TYPE	VALUE
SHA256	a9f2c4bc268765fc6d72d8e00363d2440cf1dcbd1ef7ee08978959fc118922c9, 717aed4c123a3cde0695818f7038c1092d9dcd7c910ac5ddba96d5e348e1337f, fb444e7bb7c8f48207ceeba8bad9c2b9ae9c726ac28916c5be5390ba67c2c77c, 2f5301125627331f56db76046d177493d8b0a814cdd9cafad3981aad97383163, C675130390B4EE16EA72DEA30807939B1306D373C5B7FFE0CF1D2AFAFFC402B6, D90AFA08E38C15BB3E48187E436645B42D4D856E219242CB6C33085C4C1611DB, C50271CC3E26651A5B5384894490C7153C56B86435E61B5CA206F8E9C5C5542F, EE79F4E87E0B393C952B478C9A30F35802C09F93E899ECF6B40D8D6625188031, c69ab262ac3f73277c4b9a777a408f57feb618e2e00bc2e66e8d97274083c742, 5fef7a5db4b1c216c9fc37d55143e5b635e8833d82f95004bb4fb47060fdf447, 42ffc3eb728ccc83cf4f115c6a3e32c01ef80869b9f2c4f2d62a7a88c7bf4bc2, 57d8296dd901491d37e7c79d0fe95188f3b7c94affc71c8e732daea8369cfa4f, 729f08249b9f55f17fe7762d6c41c619127e0a7798194b7ff18f06003ff3d041, 95a6c06ac691bec0ac2140b6590c96488feb8bc6c3ca501d1fe8ee7cbf9d0f8b, 71e08a89ecdfac3bb490bec6c4115cfd71de744897fd8b7dd7383646e911858e, 0482dc9c6ed46e247682e1d4ae5c5a037ef0b66f3b22af9ae25ac072028dd7a2, 38ee04ee9d3b3912013d54483d8f822eebd0367408b369bc09f46cb339a54313, 474ba7f2fb18b7b55fc077513cda6f6d36fb79e58065c556724ea049a392e327, 2a8a49d9c25d786a5108a53d0b3281677b299540f54580a7b49aa8de78ec0ee1, ec669387150865b59bbf98b41a770235ba4fd632aab33433c2d493460ef52479, 4f30d975121d44705a79c4f5c8aeba80d8c97c8ef10c86fee011b99f12b173b4, 1656c55c8516bd650fe59b71a5886ecf508deb927ed3c8465cf0ad5923c35958
MD5	a04da51938bb298ff91acd1561f5a32a

TYPE	VALUE
SHA1	92AF977EF07F42607F23FD94E8A790139F910EE1, 9c5235035a40786be22dc11128109ac9d31a1036, b8af3493aa43dc4371f25b8eff349bd774ec179b, 8840AE4BF610BDD0A2D65A246C397AF3F3B3CABA, 5A95B69C11018420B17B469771C8EC07458FDA23, 850C30EF8456EA5EE9DBEECC27959A39DD3FB57D, 577EFD1534DD2C4133EA2E4B16A21672D257AF72, 13b3722483559259c14f69e213aeeb194c7b5718, 516f29bbd64a2661e8770cc76903bfae5aa39f23, 1a404996f1d52d2e2674aa6409d54b8232242d23, 640640d6651c4ac2f66ed8312084849ad9f0124e, ab1271b4316eb4a5d6ea03b4c24d56cef1e8524a, f09804b59a3aac7c1dd47c7e027182fb54f9a277, f1d299336aac1a1314b36064ffa9ae12ebdb3e4c, 6e16e05923be2363b81b235c934b8996a58d3bdf, 8af2eab50e77706cec0f1416a51c171088d26ed6, 52222a8938928d70aa515798c5ba97a2f9932176, 73ceb983d71b42521b13cd9d81657a0857ae3b50, EC446276A337FEE3C51DE2DBD8DF7EBEB3B5EA88, 69FA757349161207E6D07EC3743486285657D013, F2786D1E79C5D1F1876BD171D64A56436465B175, 276C38A5A59BEAB93ABCD33919CBBAA572558AD2, 752b86b58860377d0ed1f9570b1ed1324d3c4f2e, 7b872d6799506ecb1a6a69b0b16cf53a70a337be, 10a3f269d12c41849a052d44ce6855539db91a0b, e600cf9e713f3d5c0bb691c2bdecffd946ff2b35, 0c951a4a4c8a3827832f2d2379f02271e17ff16b, a6d653d2887f0ce4029a94616464ad74c4f770fe, 0cb59b74d87ac56f1aa3269eecee3ad6d01d7915, f8dac4e8b5a11e91640b0277113ad1770e7fc3ef, 966a90baf892a8d1cff1e6ba464e4c29a09b3a3c, 0fbed8d60e2d940882e01a2bf11003f6bd59f883, bccf867716709ce0167cc72f16d4a14f159e459f, 22f10e42683501fb2ea6962e44eefd64848aefe7, 0fdb26c6202acb33eea938da1a492504035ff8c1

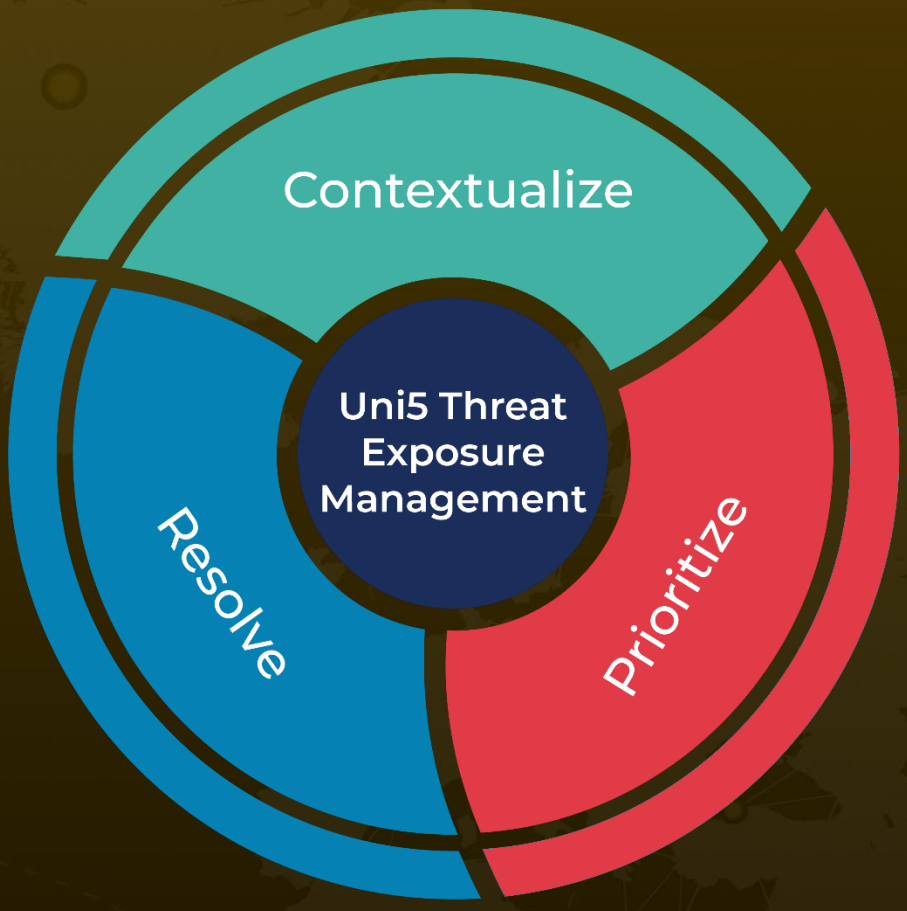
References

https://www.rapid7.com/blog/post/2024/12/04/black-basta-ransomware-campaign-drops-zbot-darkgate-and-custom-malware/

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

December 10, 2024 • 6:00 AM

More at www.hivepro.com