Babuk Ransomware Variant Delta Plus Used in Live Attacks After Source Code Leaked

zerofox.com/blog/babuk-ransomware-variant-delta-plus/

October 1, 2021

BLOG

October 1, 2021 | by Stephan Simon

5 minute read

On September 28th, the ZeroFox Threat Intelligence team discovered a Babuk ransomware variant calling itself Delta Plus 2.3. The operator behind Delta Plus has recently made use of multiple other ransomware variants under the name Delta Plus as well. While no notable changes were made to the Babuk variant aside from modifying the file extension, the sample's build date was just 10 days after the leak, highlighting how low the barrier to entry for running a ransom operation can be when given a complete solution.

Babuk Ransomware Explained

Babuk ransomware was first discovered in early January 2021. In its early days, victim leaks were published on underground criminal forums while the group worked to create their website. January to April 2021 saw several organizations fall victim to the group, including the Metropolitan Police Department of the District of Columbia. The attention from attacking the Metropolitan Police Department allegedly caused disagreements within the group over those who wanted to publish the leak and those who felt it went too far, eventually leading to a retirement announcement and split. Payload.bin, a site focused solely on extortion, was launched as a direct result of the fallout.

By the end of June, a compiled version of the Babuk ransomware builder had been published online by "biba99," the same account responsible for publishing early victims to underground forums. Finally, on September 2nd, a user going by the handle "dyadka0220"

published the full source code for the ESXI, NAS and Windows versions of the ransomware, decryptors and builder application.

Figure 1. *Actor dyadka0220 posts a link to Babuk's source code hosted on a public file sharing platform.*
Source: ZeroFox Threat Intelligence

Babuk Ransomware Delta Plus Variant

On September 28th, the ZeroFox Threat Intelligence team retrieved a malware sample tagged as Babuk ransomware. It matched several publicly available YARA signatures created to detect Babuk, but the sample was changing file extensions of encrypted files to ".delta" rather than ".babyk" like the group was known for. Because of the builder application getting published in June, anyone could generate new "Babuk" payloads with a custom ransom note. Even with this builder, however, the user was stuck with the .babyk file extension unless they modified the compiled binaries.

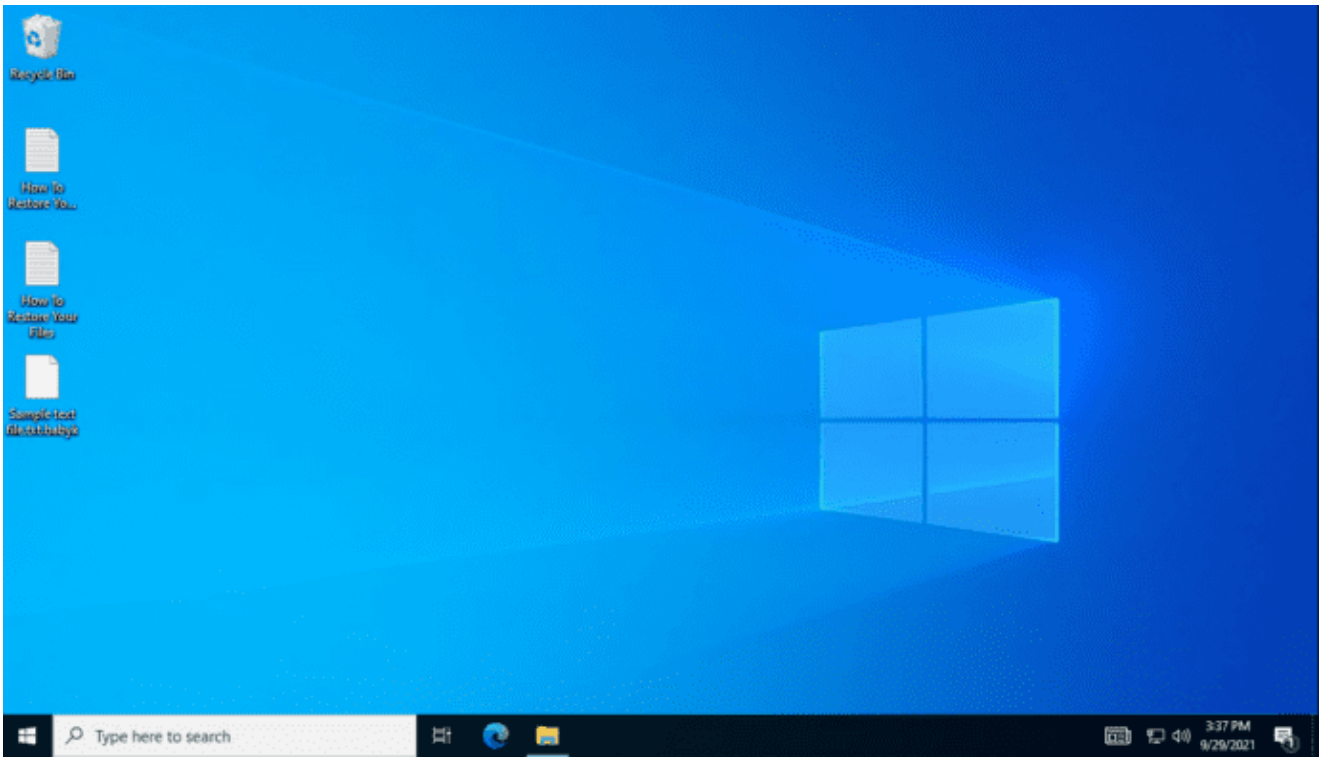

Figure 2. *A virtual machine that was encrypted using the Babuk builder-generated payload. Encrypted files still used the .babyk file extension.*
Source: ZeroFox Threat Intelligence

The second clear difference was the compilation timestamp. When using binaries from the leaked builder, all generated payloads appear to be built on March 23, 2021. The new sample had a compilation date of September 12, 2021.

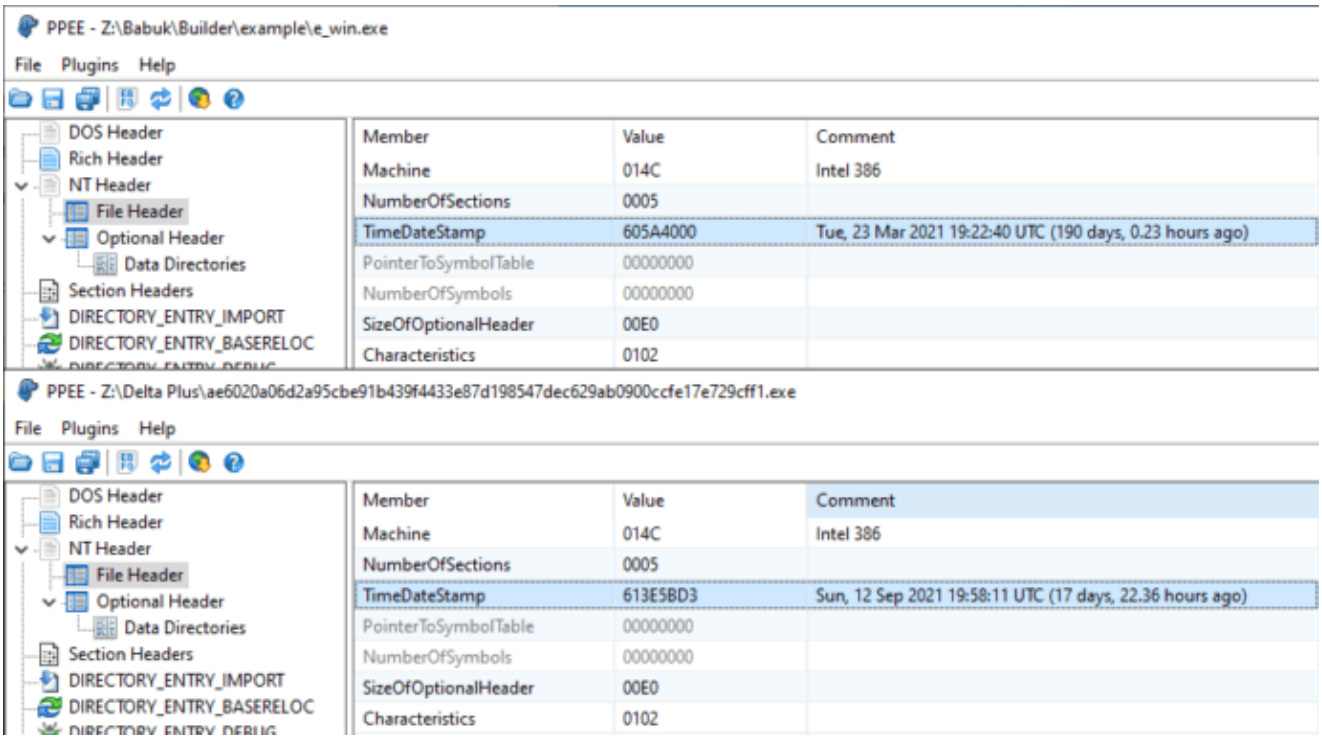

Figure 3. *Compilation timestamps of a payload using the builder (top) and Delta Plus*

(bottom).
Source: ZeroFox Threat Intelligence
Looking at the dropped ransom note, we can see that the actor decided to brand this ransomware as Delta Plus.The ransom demand is significantly smaller than the six and seven figure ransom amounts regularly demanded by the larger groups. In this case, the potential victim is demanded to pay $6500 US dollars in Bitcoin. If the victim contacts the provided email within 72 hours, the amount is halved to $3250.

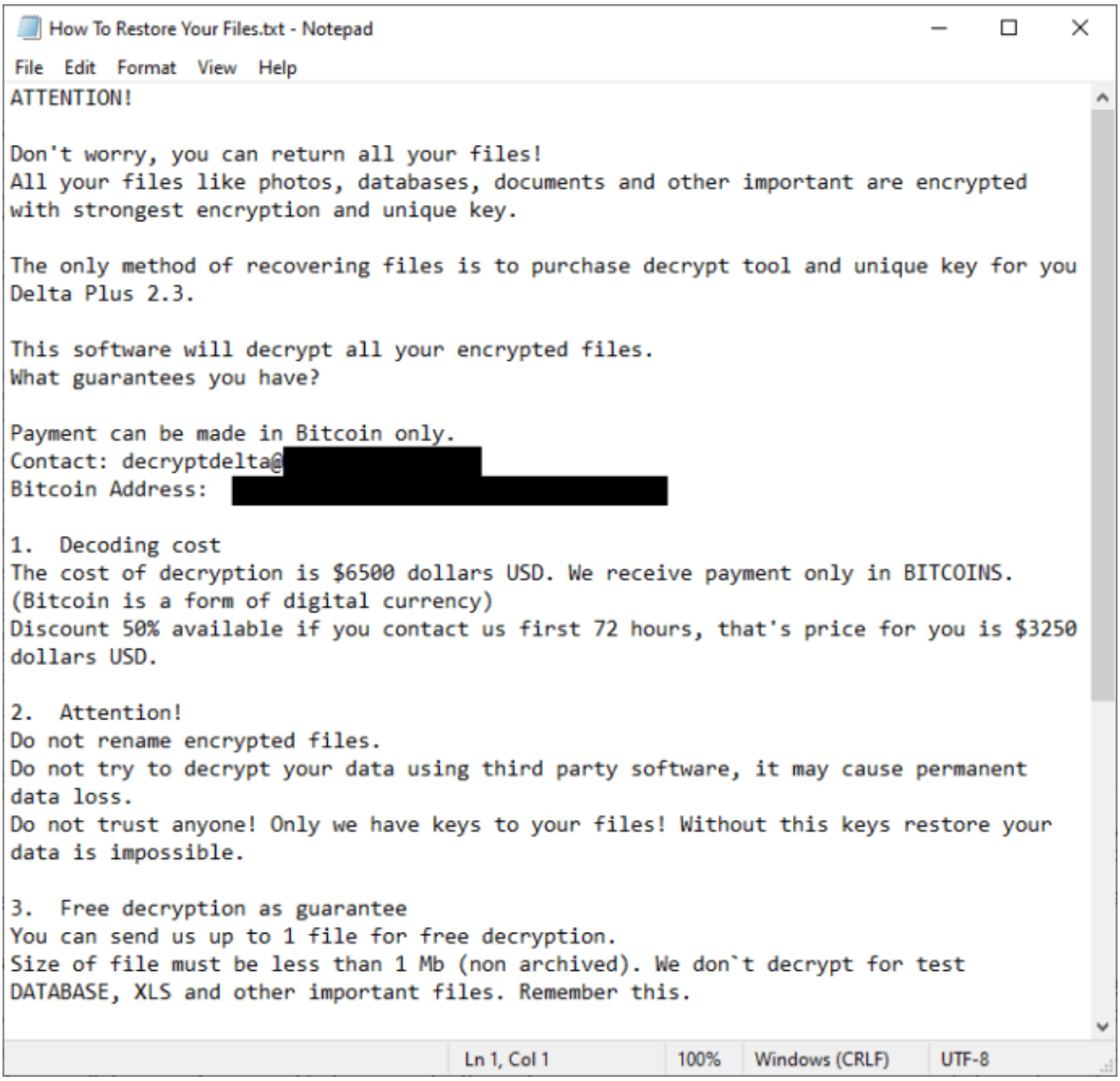

Figure 4. *Ransom note dropped by Delta Plus 2.3.*
Source: ZeroFox Threat Intelligence
By following the email address and Bitcoin wallet given in the ransom note, the ZeroFox Threat Intelligence team was able to discover more related samples. The actor behind Delta Plus did not appear to be attached to any one ransomware solution, as we discovered binaries compiled from .NET, and Delphi as well, while Babuk is written in the C

programming language. Various notes dropped by these samples had ransom demands from $300 to $10,500 and mostly stuck to the Delta Plus name, though one sample was referred to as “Doydo.” Multiple email addresses and Bitcoin wallets were discovered to be in use by this actor.

Recommendations

As with the identification of any new ransomware variant or digital attack technique, it’s imperative that security teams have proactive protections in place to detect and respond to cyber attacks. The ZeroFox Threat Intelligence team recommends that all security teams:

- Ensure antivirus and intrusion detection software is up-to-date with all patches and rule sets
- Enable 2-factor authentication for all of your organizational accounts to help mitigate phishing and credential stuffing attacks
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks
- Avoid opening unsolicited attachments and never click suspicious links
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity
- Review network logs for potential signs of compromise and data egress

Conclusion

The actor behind Delta Plus appears to be using various freely available ransomware products with the ability to drop custom ransom notes. With freely available ransomware builders and full source code to projects like Babuk available for anyone to download, the barrier to entry has been lowered. Skilled and low-skilled actors alike now have the ability to repackage ready-made solutions with minimal changes needed.

Indicators of Compromise

Hashes

MD5: 093f098e70cc57a17d02323cbe6cd484

SHA-1: 134239f63291d00a604e619ffafb0bf3a05e5a80

SHA-256: ae6020a06d2a95cbe91b439f4433e87d198547dec629ab0900ccfe17e729cff1

MD5: 1dfba6ad901aa33ef1622e980192aa82

SHA-1: 495f1014ff21be916de257775bedbebc5526016e

SHA-256: ca0d9c8e8b2ed05fcf10178e1d194f5e484892dbe59ede4ae9549d27a5c8fd75

MD5: 00d0b2073d8dec2da0dd6a05af2533ec

SHA-1: aeb61462a038e2ee5d52be1bee9af57b0deb7672

SHA-256: 13ccf6c512823f7d30f14d06fd50e00bce8dd03ca331dd5c5d9fee64c340c92d

MD5: 36a16c31c3da7e55ba52c54083d67a3a

SHA-1: ffdbdb2ae899589f7f73a969c5561a1353457e90

SHA-256: 60d1145c0827d5065bc0e99da1d80b041973fc959d9c143ac06eb268e8740d10

MD5: 7540d846032fd69dcf7a863213e8befa

SHA-1: 0cf8025ed457b54a7430f6c604e9f8b6e204087f

SHA-256: a52267dc795a51404cbf2a7e8e7875929783bcc62abd6b7cfd1921c938cf2756

MD5: b647e513448a7ad0aeb214818b7f3acf

SHA-1: d255e18a0dd872edcf0064c11cb99eefcbb798a0

SHA-256: c9133320766a0b1ccee6a6af10077694fb19b7dda538525749749e26b493f852

MD5: 1dfba6ad901aa33ef1622e980192aa82

SHA-1: 495f1014ff21be916de257775bedbebc5526016e

SHA-256: ca0d9c8e8b2ed05fcf10178e1d194f5e484892dbe59ede4ae9549d27a5c8fd75

MD5: a22ca06bb3a58d4ca2bca856434b96f3

SHA-1: 4a12e232b2442746334ef5d94fab4c3577b33de7

SHA-256: 63b6a51be736d253e26011f19bd16006d7093839b345363ef238eafcfe5e7e85

MD5: b43e8b865d3339eeb8b8b11f900f6c89

SHA-1: 52538e17d4dc85c22f6a01acbbc8caa7447a50b0

SHA-256: 106118444e0a7405c13531f8cd70191f36356581d58789dfc5df3da7ba0f9223

MD5: 3e7ff21d849455dd604af1d48b61ad98

SHA-1: c40904f865e04265c4ed6bcf03622e8822a36d1c

SHA-256: c8d97269690d3b043fd6a47725a61c00b57e3ad8511430a0c6254f32d05f76d6

MD5: 01d8a481d1e98eaed43af57e9c0dd2a4

SHA-1: b90eed3c354307808f0121cfc6207ece3e2068c5

SHA-256: eb180fcc43380b15013d9fe42e658fc6f6c32cf23426ef10b89bc6548d40523b

MD5: c5ef4a503cd7bfc90f966bbb2f910c3e

SHA-1: 4a83e408711713de3163cf160eaf48a60b05b85f

SHA-256: 94fe0825f26234511b19d6f68999d8598a9c21d3e14953731ea0b5ae4ab93c4d

MD5: 1f302220fb993a9a219db6dd0558fa71

SHA-1: b52016083e27d7e6a0a96ff3d031aacc2d3d8c8b

SHA-256: c3776649d9c0006caba5e654fa26d3f2c603e14463443ad4a5a08e4cf6a81994

ITW Links

- hxxp://atualziarsys.serveirc[.]com/Update3/Update.exe.rar
- hxxp://atualziarsys.serveirc[.]com/Update4/Update.exe.rar
- hxxp://atualziarsys.serveirc[.]com/Update4/Update.exe2.rar
- hxxp://services5500.sytes[.]net/Update6/Update.exe.rar
- hxxp://suporte01092021.myftp[.]biz/update/WindowsUpdate2.rar
- hxxp://suporte01928492.redirectme[.]net/AppMonitorPlugIn.rar
- hxxp://suporte01928492.redirectme[.]net/Update5/Update.exe.rar
- hxxp://suporte01928492.redirectme[.]net/Update6/Update.exe.rar
- hxxp://suporte01928492.redirectme[.]net/Update7/Update.exe.rar
- hxxp://suporte20082021.sytes[.]net/Update3/Update.exe.rar
- hxxp://suporte20082021.sytes[.]net/Update5/Update.exe.rar