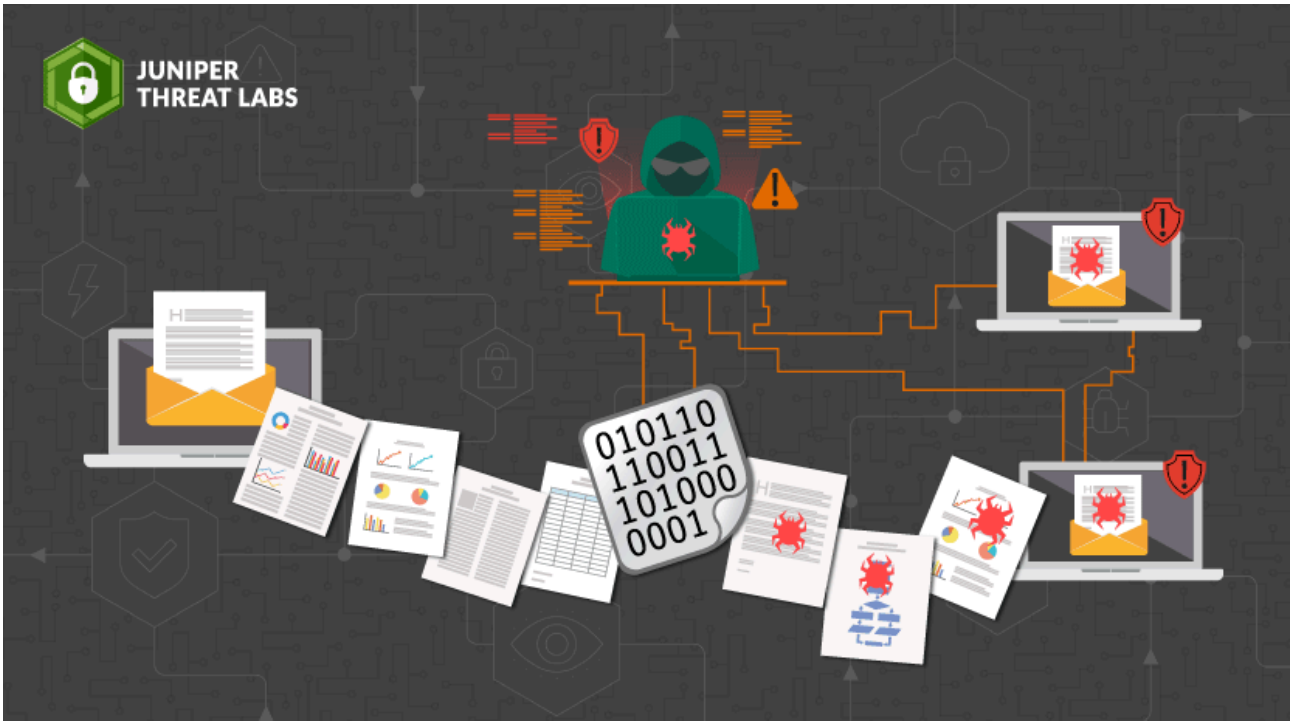
New pastebin-like service used in multiple malware campaigns

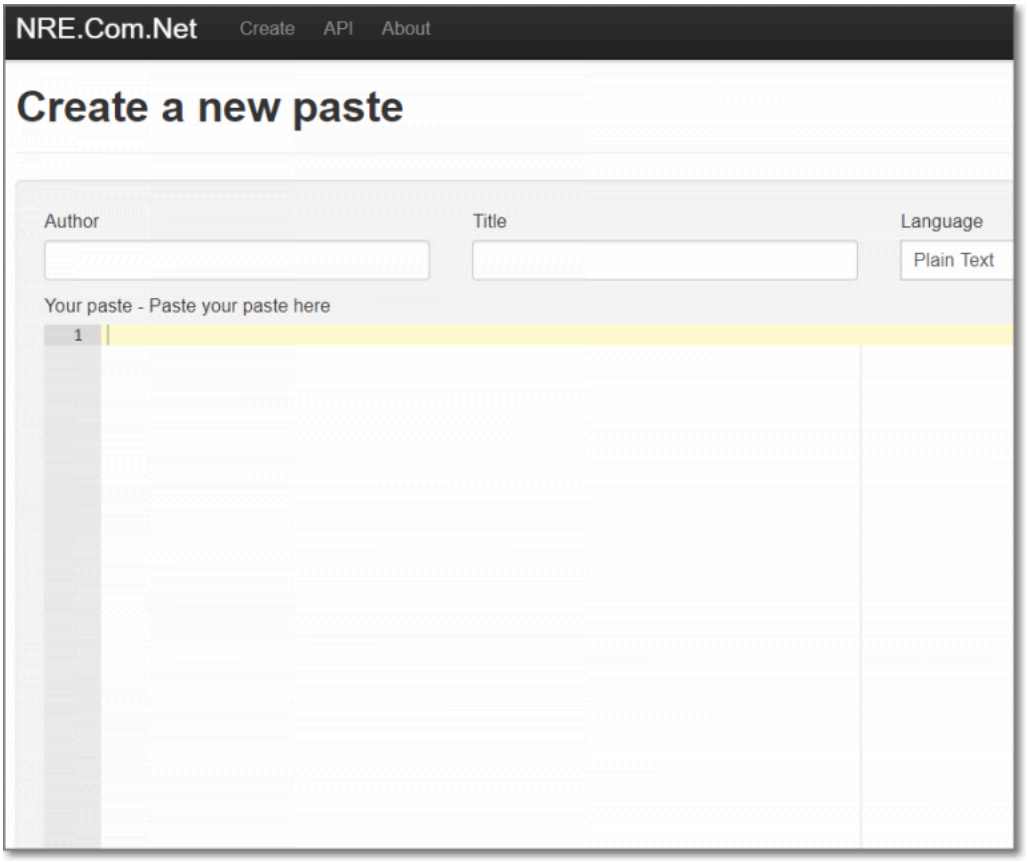
By Paul Kimayong

Published: 2020-10-05 · Archived: 2026-04-05 13:53:09 UTC



Juniper Threat Labs identified several malware campaigns that rely on a pastebin-like service for its infection chain. The domain in question is paste.nrecom.net. The attacks usually start as a phishing email and, when a user is tricked into executing the malware, it downloads the succeeding stage of the malware from paste.nrecom.net and loads it into the memory without writing to disk. Using a legitimate web-service for the malware infrastructure is not new, as we have seen APT group FIN6 using pastebin to host parts of the infection chain and Rocke using it for command and control. Although using legitimate web services is not novel, this is the first time that we have seen threat actors use paste.nrecom.net. Among the malware we have identified are AgentTesla, LimeRAT, Ransomware and Redline Stealer.

What is paste.nrecom.net?



Paste.nrecom has been in service since May 2014. If you are not familiar with pastebin, it is a service where you can post your code or text data with the intent of sharing it with others. Paste.nrecom does the same thing and it also offers an API that allows scripting. This is advantageous to threat actors as they can easily insert and update data programmatically. This service is powered by Stikked, which is an open-source PHP based pastebin.

How do threat actors use it for malicious purposes?

Because it is a text-only service, one would think that it cannot host an executable file (binary data) into it. However, binary data can be represented as a text file by simply encoding it. The common encoding method is using base64. That is exactly what the threat actors did in this case.

malicious paste encoded in base64

To add another layer of obfuscation, they encrypt the binary data with a XOR key. The following file, for example, is encrypted with XOR key, 0x02.

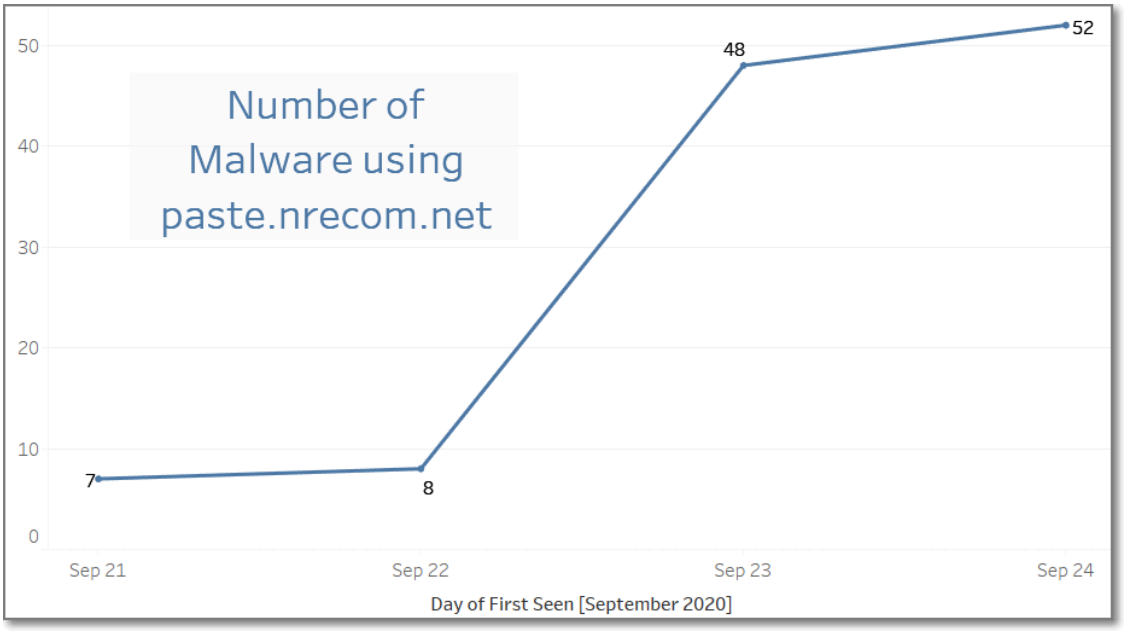
```
λ base64 -d 3529ec57 | xxd | head
00000000: 4f58 9202 0102 0202 0602 0202 fdfd 0202  OX..............
00000010: ba02 0202 0202 0202 4202 0202 0202 0202  ........B.......
00000020: 0202 0202 0202 0202 0202 0202 0202 0202  ................
00000030: 0202 0202 0202 0202 0202 0202 8202 0202  ................
00000040: 0c1d b80c 02b6 0bcf 23ba 034e cf23 566a  ........#..N.#Vj
00000050: 6b71 2272 706d 6570 636f 2261 636c 6c6d  kq"rpmepco"acllm
00000060: 7622 6067 2270 776c 226b 6c22 464d 5122  v"`g"pwl"kl"FMQ"
00000070: 6f6d 6667 2c0f 0f08 2602 0202 0202 0202  omfg,...&.......
00000080: 5247 0202 4e03 0102 dbcd 655d 0202 0202  RG..N.....e]....
00000090: 0202 0202 e202 2002 0903 5202 02f6 0502  ......  ...R.....
```

After base64 decoding, the file is still encrypted with XOR algorithm.

```
λ xxd 3529ec57.dec.XOR.02 | head
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 8000 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: 5045 0000 4c01 0300 d9cf 675f 0000 0000  PE..L.....g_....
00000090: 0000 0000 e000 2200 0b01 5000 00f4 0700  ......"...P.....
```

After all the necessary decoding and decryption, you will then see the executable file, as shown above.

From September 21, 2020, we have seen several malware families taking advantage of this service and quickly ramped up.



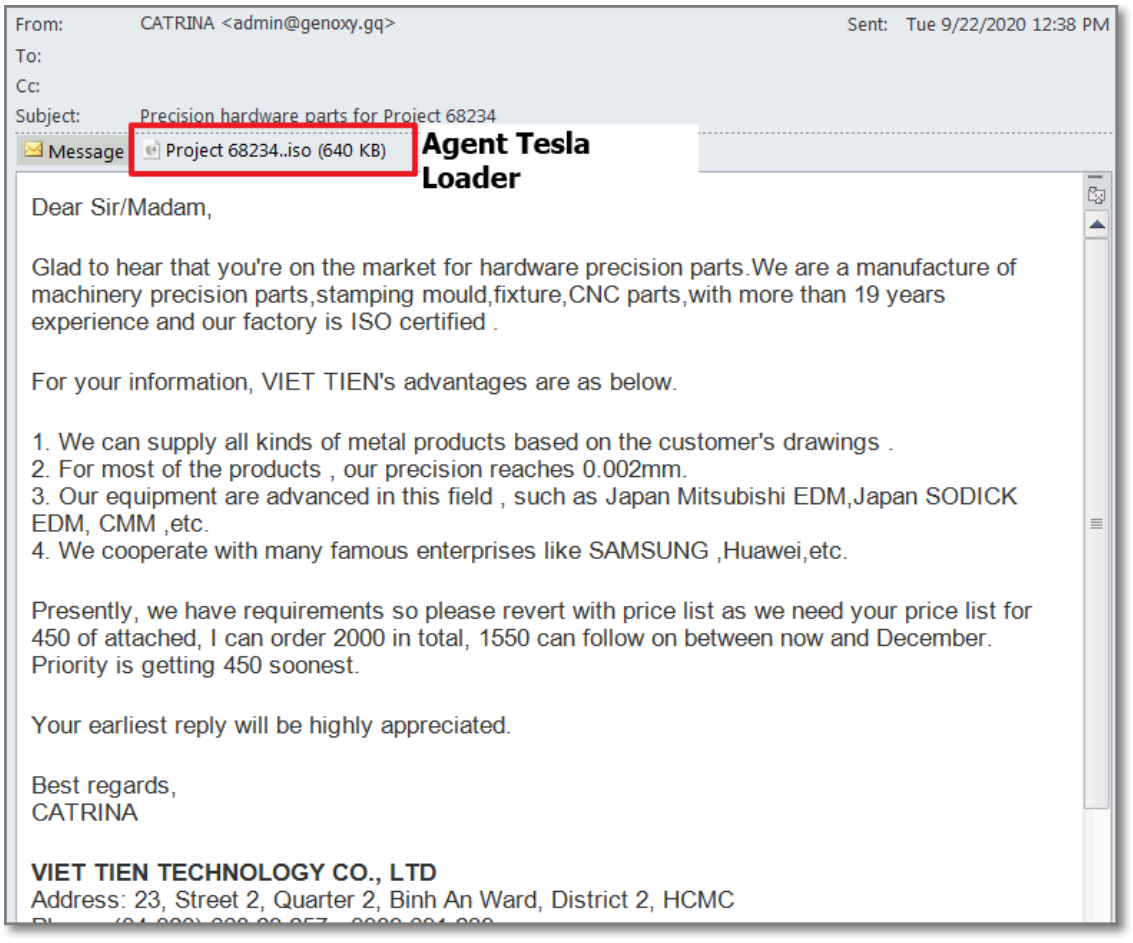
Malware Campaigns

The attack usually starts with a phishing email that includes an attachment, such as a document, archive or an executable. When a user is tricked into installing the malicious attachment (first stage), it downloads the next stages from paste.nrecom.net. We have also seen malware hosting their configuration data in the same service.

Agent Tesla

Agent Tesla is a spyware that is capable of stealing personal data from web browsers, mail clients and FTP servers. It can also collect screenshots, videos and capture clipboard data. Recent versions of this malware are also capable of stealing personal data from VPN clients. It is being sold on the underground markets for as low as $15 and could go up to $70 depending on the additional features.

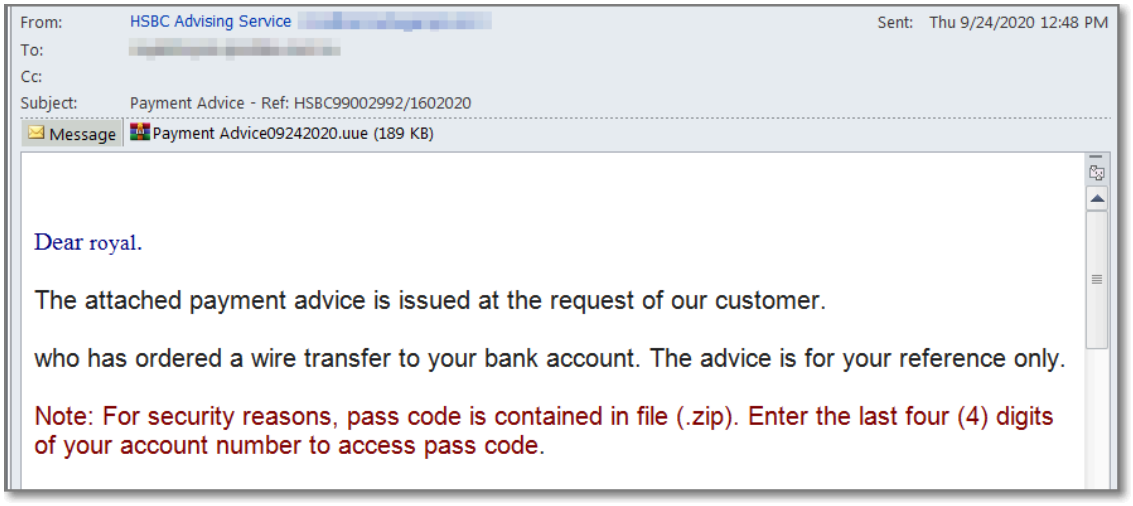
Agent Tesla is among the most active malware using this pastebin-like service. Campaigns usually start with a phishing email with a malicious attachment. Based on the samples we found, these campaigns target multiple industries related to shipping, supply chain and banks. In some cases, the attachments are archives, such as .iso, .rar or .uue like below:



Attachment Sha256: 9c38ab9d806417e89e3c035740421977f92a15c12f9fa776ac9665a1879e5f67

Infection Chain for 9c38ab9d806417e89e3c035740421977f92a15c12f9fa776ac9665a1879e5f67

As you can see from the chain, there are two requests to paste.nrecom because it divides the Agent Tesla payload into two. The first request is the first half of the file and the second request makes the second half. This technique makes it harder for security solutions to analyze the payload.



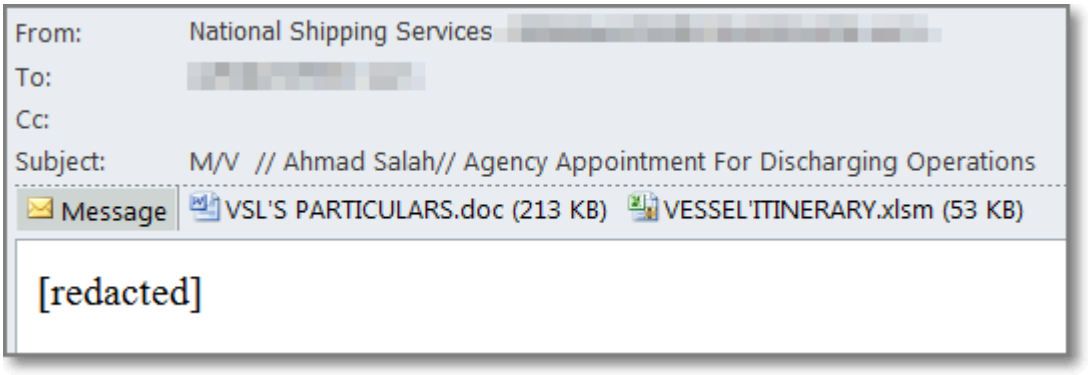
Another sample phishing email has the attachment with Sha256: 199a98adf78de6725b49ec1202ce5713eb97b00ae66669a6d42f8e4805a0fab9

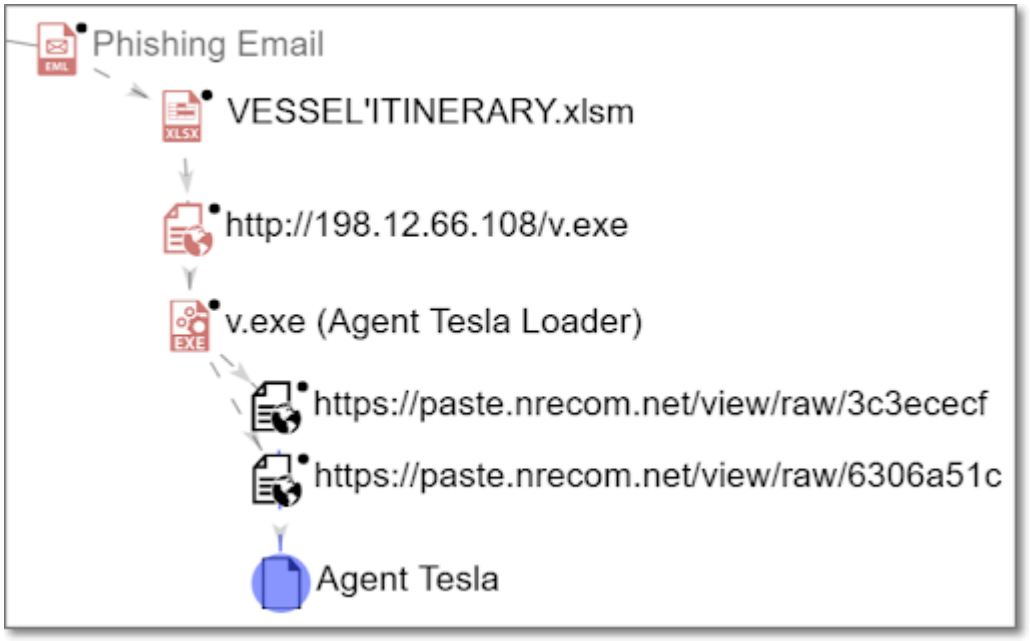
Below are email attachments and files inside some email attachments that we have found to install Agent Tesla using paste.nrecom.

File Name	Sha256
Emirate bank TT copy 2020-09-20 at 07.30.55.uue	f8c02c3f6d22978b3c478d0fb7ad4845609b8ad4a38e0ed2a75721156a6a8e44

Inv C-22464 PO 3871.exe	27f8e739b62c685c4115f49ae146bb75271d0b8fad021436939735bf7492186b
PO#150367285 SECONDO VERGANI SPA Ref#BK043383.exe	3101003430beae11fe082a07878ac2f643a64e3abd82b7b2a787a0e1fde27307
Payment Notification.uue	b7cf6fb7557f435bab1b815a38b1771aea9d118192f6d184111754615e8881af
bank payment copy.exe	136991b95c503e13d7ed77305a305f6f568c9d93273584d19a33014202a6ebbb
Payment docs63878288882788.docx.rar	44221603cb9e19a630e35bd12a9c8bd97a9d2743a6fc5528e81db0718fc3e1b3
Attachment JOIN LEADERS PO332,pdf.exe	167139073c586fd0d7de374611f899e170fd0316463be6c65170496636b3e42d
APROBACION DE TRANSFERENCIA INUSUAL REALIZADA EXITOSAMENTE.tar	0e044c8570122a280c963cac80e0140da78ee0d378cd17cab4ea6f146ce35d15

In some cases, the attached files are Office Documents that download the Agent Tesla loader.

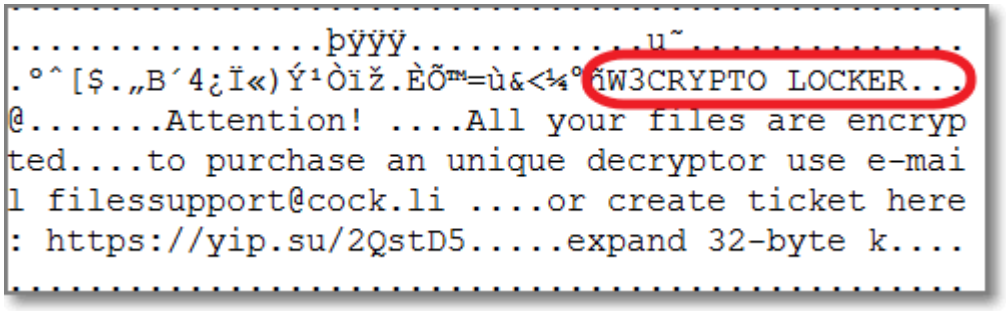




Infection chain for c66e6c6018d3e51e8b39146c6021fb51f59750b93778a063f7d591f24068c880

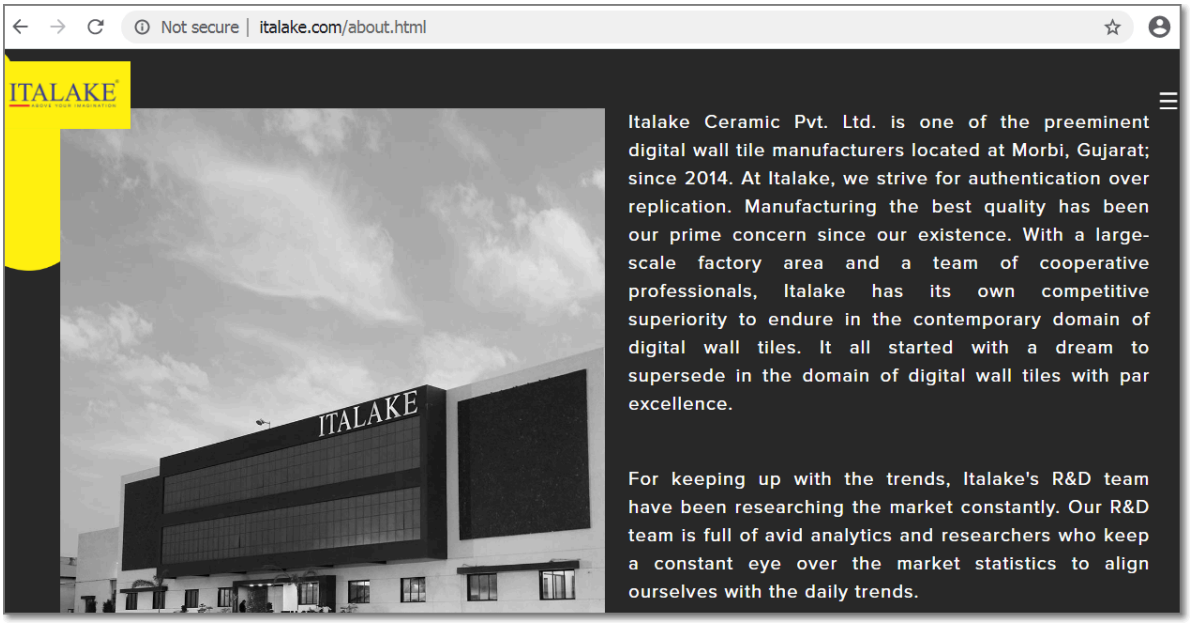
W3Cryptolocker Ransomware

W3Cryptolocker is a relatively new ransomware. Based on our telemetry, this ransomware surfaced in July 2020. We will call this malware W3Cryptolocker, based on a string found in its code.



Strings found in the binary code of this ransomware.

The loader was hosted on a potentially hacked site, italake.com.

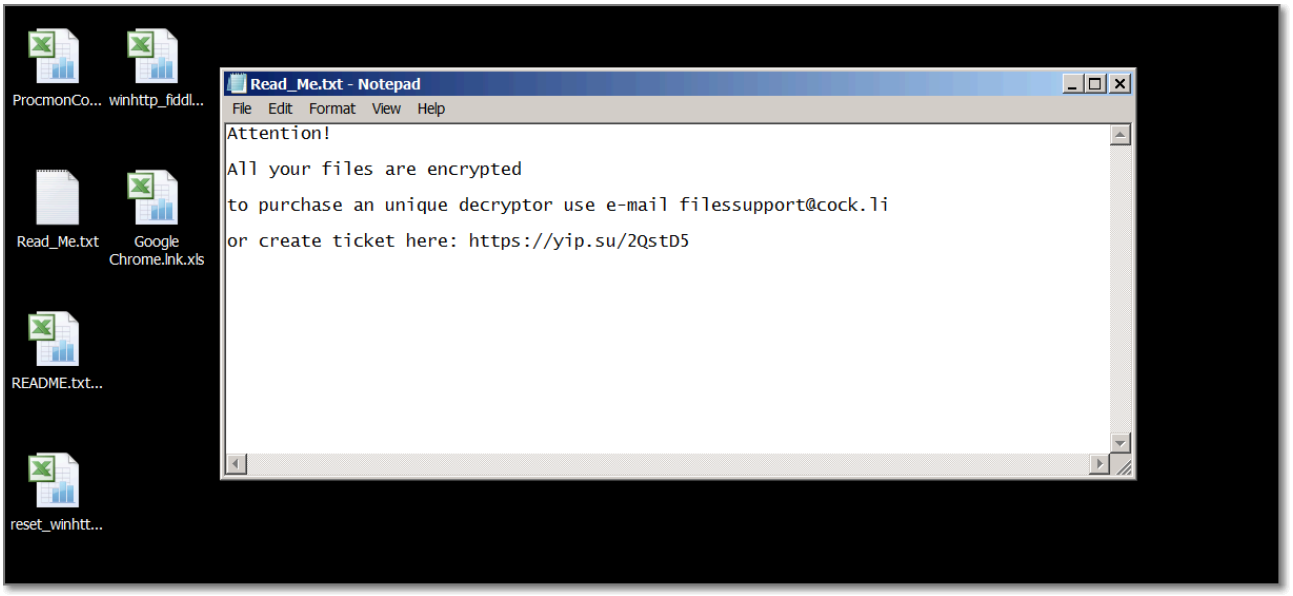


Infection Chain of Ede98ae4e8afea093eae3163888255276588074 89e5559bff6dbf5bc5b554a2c

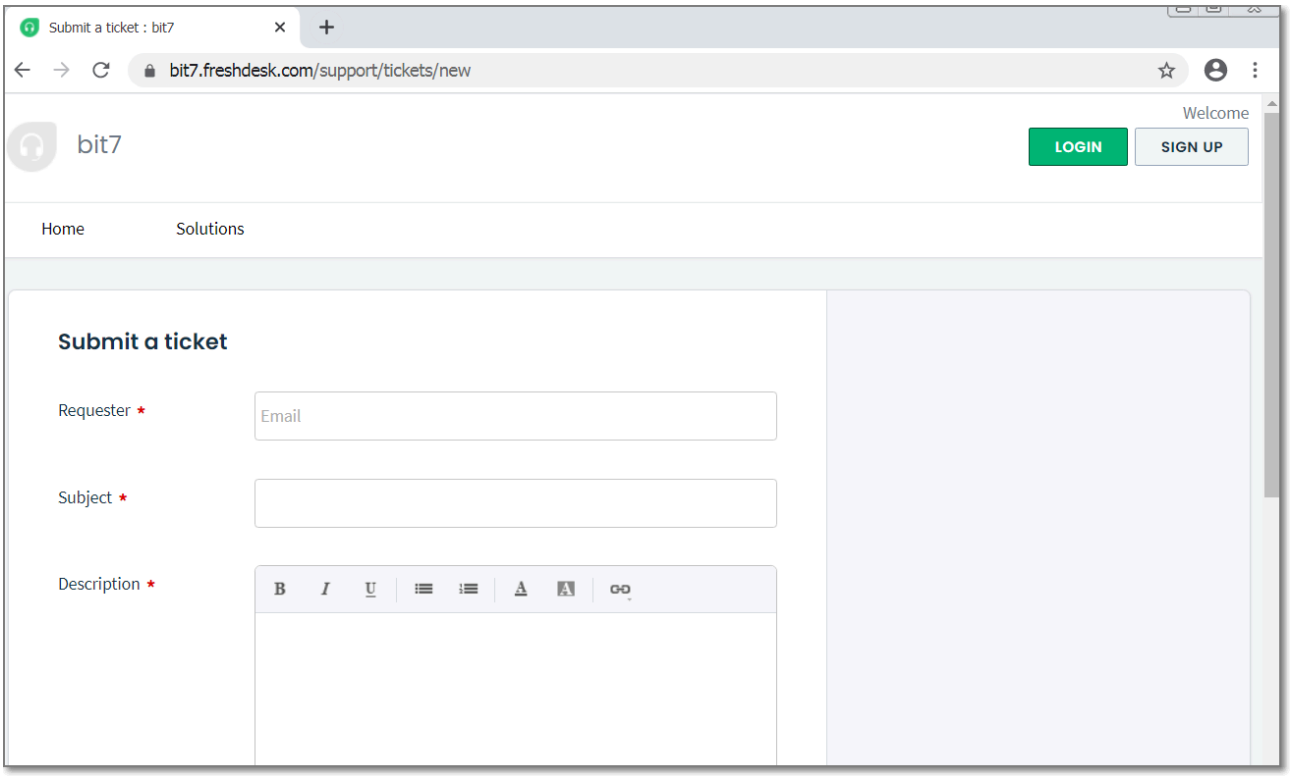
It will encrypt all files in all drives except for files having ".xls" extension and folders having the following strings:

- Windows
- ProgramData
- $Recycle.bin
- System Volume Information

It adds an extension .xls for encrypted files. After it is done encrypting each folder, it creates a "Read_Me.txt" file on each folder with the following message.



Visiting thehttps://yip[.]su/2QstD5 leads you to a freshdesk support site, bit7.freshdesk.com.



Other W3Cryptolocker Samples

- c97852b425e41d384227124d93baf6c2d3e30b52295a828b1eac41dc0df94d29
- 9a0af98d0b8f7eacc3fdd582bbc0d4199825e01eeb20c2a6f98023c33ece74f6
- 01eea2a4628c6b27a5249a08152655246871acafa657e391b73444c05097976e
- 9a08e87e8063b13546e464f73e87b2ca5bde9410fec4e614313e2b8a497592fa
- 8dfe87850bd17b4eb0169b85b75b5f104ae6b84deeb2c81fe6ae5e19685f6c66
- 53124033d521158771eac79ad6f489c6fdd5b25ab96712035c2ca65b3a3c5eed
- aac2024789ffd2bfce97d6a509136ecf7c43b18c2a83280b596e62d988cedb10

- fafabdffa67883587ba1a3c29f6345a378254f720efe8c2f318a4d5acdbce373

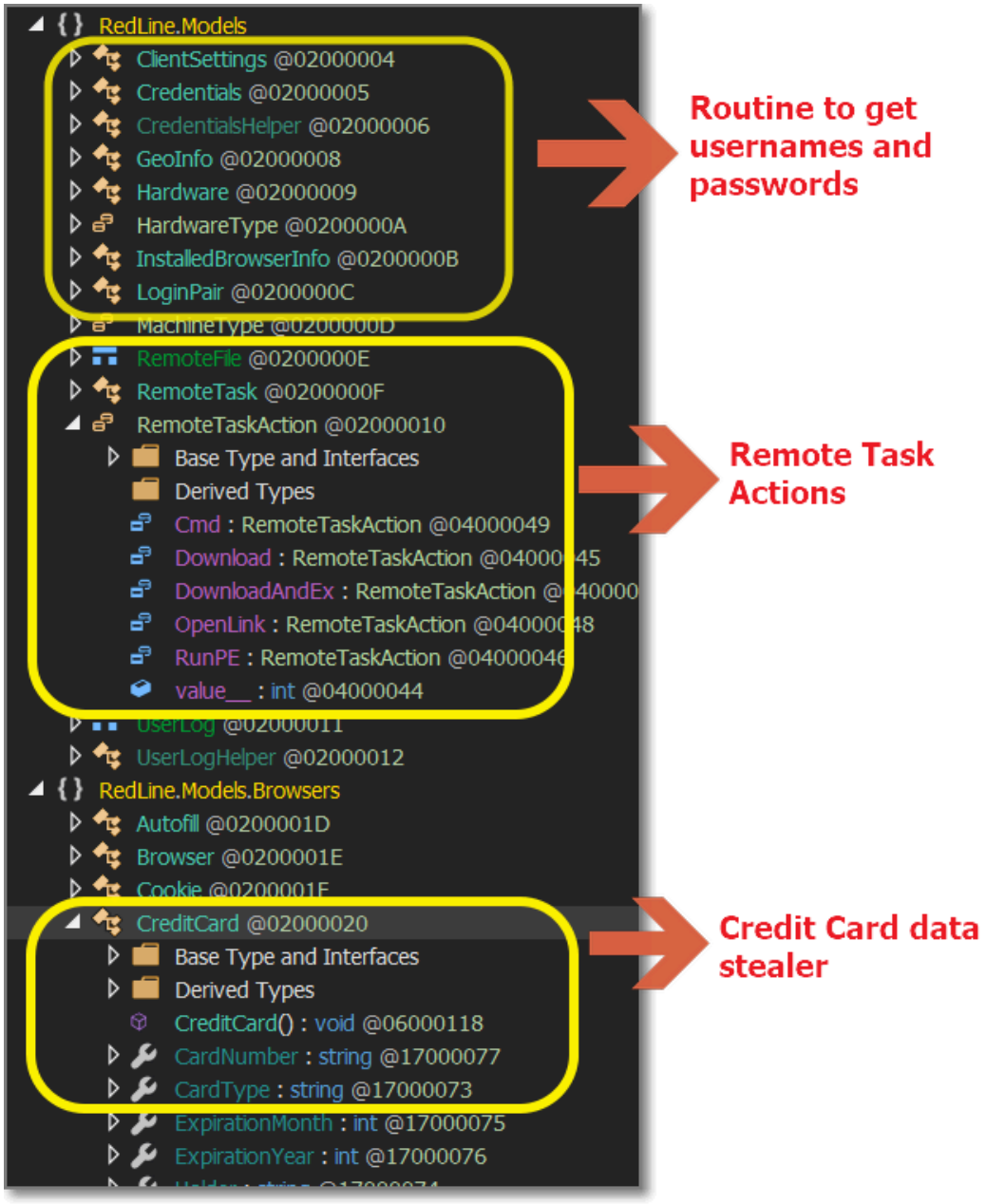
Redline Stealer

Redline Stealer is a malware that surfaced around March 2020 and it was reported to have targeted healthcare and manufacturing industries in the United States. This malware is found being advertised on forums with several pricing options starting from $100/month subscription. It has the following functionality:

- Browser Data Stealer
  - Login and Passwords
  - Cookies
  - Autocomplete Fields
  - Credit Cards
- Remote Task Functions
  - Execute Commands
  - Download Files
  - Download Files and Execute
  - RunPE (Process Injection for fileless infection)
  - OpenLink
- FTP and IM client stealer
- File-grabber
- Collects information about the victim’s system

The sample we found poses as a Bitcoin Miner archived into a RAR file. The archive contains an executable, MinerBitcoin.exe, that downloads the Redline Stealer payload from paste.nrecom.net.

Infection Chain of Redline Stealer: Sha256: a719affc96b41b63f78d03dc3bc6b7340287d25d876e58fd1ab307169a1751dc



Redline Stealer malicious functions

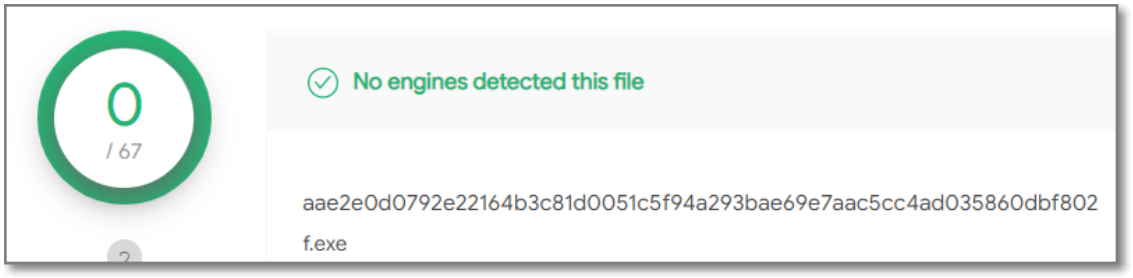
LimeRAT

LimeRAT is a remote administration trojan coded in .NET and is open source. It was a malware used to target Colombian government institutions by the APT-C-36 group. Among its many capabilities, it can be used as:

- Ransomware
- Remote Desktop
- Crypto Mining
- CryptoStealer
- DDOS
- Keylogger
- Password Stealer

Infection Chain of 20ad344d20337f8a782135e59bc1f6e1a7999bcddc50fc1dc3b8b6645abcb91e

Another sample we found is aae2e0d0792e22164b3c81d0051c5f94a293bae69e7aac5cc4ad035860dbf802. At the time of this analysis, this sample still has zero VT detections. It downloads the LimeRAT from https://paste[.]nrecom[.]net/view/raw/93a7cd20.

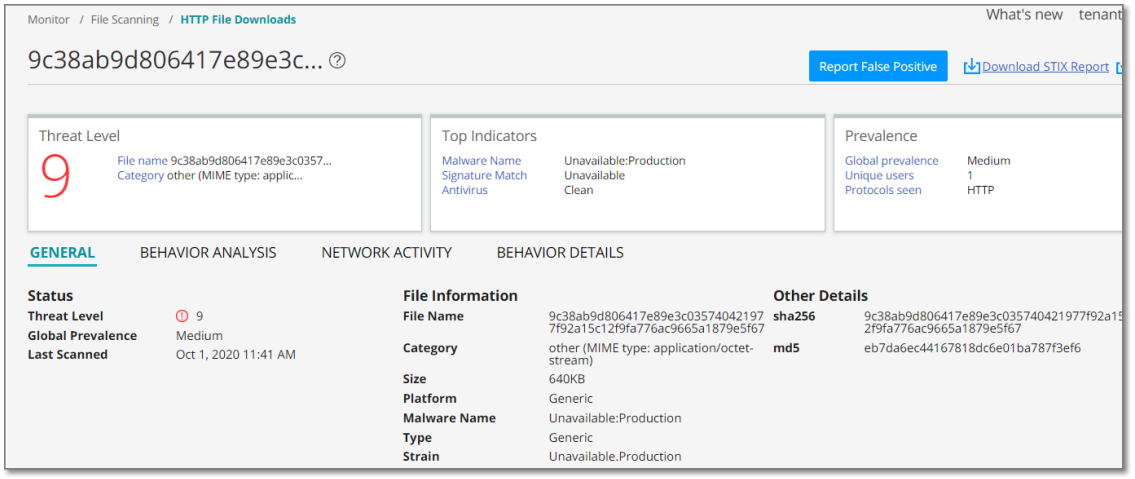


aae2e0d0792e22164b3c81d0051c5f94a293bae69e7aac5cc4ad035860dbf802 with no VT hits

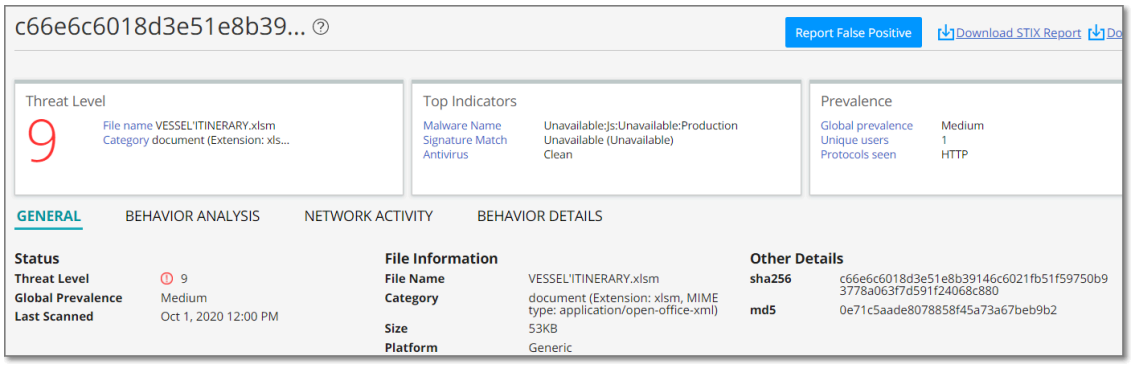
Conclusion

Using legitimate web-services like pastebin or paste.nrecom for malware infrastructure gives cybercriminals an advantage, as these services cannot be easily taken down due to their legitimate use. We recommend Security Operations to add paste.nrecom to potentially web services being abused for malicious purposes. It is recommended to monitor web-services like this one for suspicious content particularly binary data encoded in base64. Juniper's Encrypted Traffic Insights capability on the SRX NGFW does detect the malicious TLS connections to paste.nrecom.net as malicious using machine learning as seen in the screenshot below for W3Cryptolocker loader.

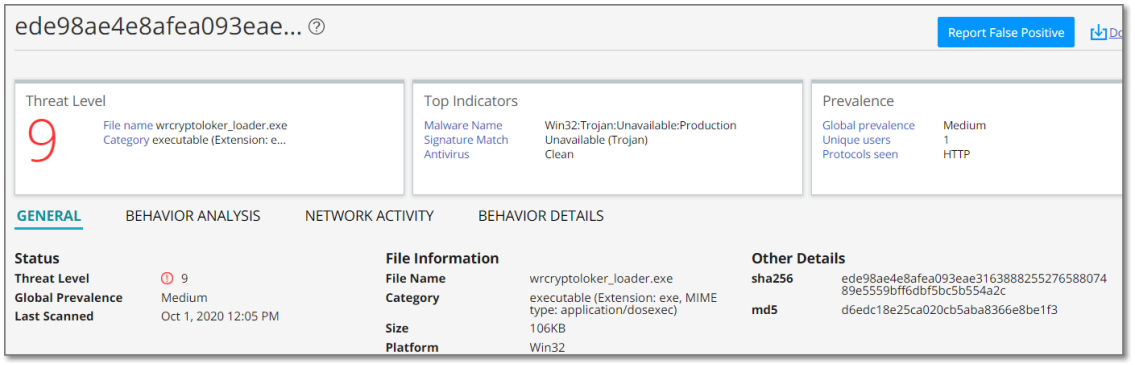
Juniper Advanced Threat Protection (ATP) detects these threats.



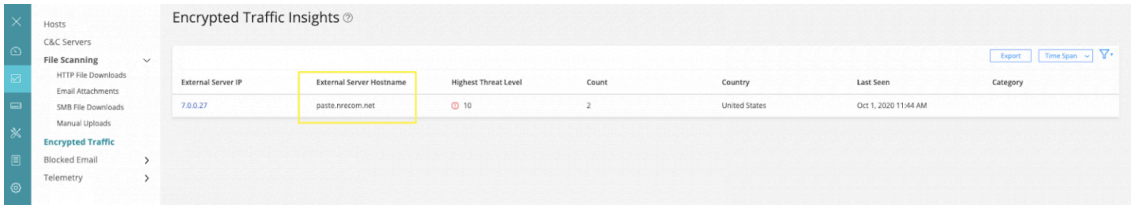
Detection of AgentTesla Loader (Project 68234.iso)



Detection of AgentTesla Loader (VESSL'ITENERARY.xlsm)



Detection of W3Cryptolocker Loader (0022.exe)



Detection of malicious connection to paste.nrecom using Juniper Encrypted Traffic Insights

Indicators of Compromise (IOC)

Domain

Paste.nrecom.net

192.12.66.108

lol.thezone.vip

URL

https://198[.]12[.]66[.]108/v[.]exe

https://lol[.]thezone[.]vip/v[.]exe

https://italake[.]com/assets/css/0022[.]exe

https://paste[.]nrecom[.]net/view/raw/3c3ececf

https://paste[.]nrecom[.]net/view/raw/6306a51c

https://paste[.]nrecom[.]net/view/raw/bfefa179

https://paste[.]nrecom[.]net/view/raw/39468747

https://paste[.]nrecom[.]net/view/raw/c230a816

https://paste[.]nrecom[.]net/view/raw/3529ec57

https://paste[.]nrecom[.]net/view/raw/7900ed08

https://paste[.]nrecom[.]net/view/raw/bd63e76f

https://paste[.]nrecom[.]net/view/raw/658b9281

https://paste[.]nrecom[.]net/view/raw/b44fe71a

https://paste[.]nrecom[.]net/view/raw/93a7cd20

https://paste[.]nrecom[.]net/view/raw/d8aedaf6

https://paste[.]nrecom[.]net/view/raw/91aec4e7

https://paste[.]nrecom[.]net/view/raw/4736837b

https://paste[.]nrecom[.]net/view/raw/aec14685

https://paste[.]nrecom[.]net/view/raw/c7dfc858

https://paste[.]nrecom[.]net/view/raw/bebcab0a

https://paste[.]nrecom[.]net/view/raw/bfbb1544

https://paste[.]nrecom[.]net/view/raw/7f41da66

https://paste[.]nrecom[.]net/view/raw/0d9233c8

https://paste[.]nrecom[.]net/view/raw/4f789f73

https://paste[.]nrecom[.]net/view/raw/6550c073

https://paste[.]nrecom[.]net/view/raw/3066146f

https://paste[.]nrecom[.]net/view/raw/019f27dd

https://paste[.]nrecom[.]net/view/raw/04fba6cb

Sha256

9c38ab9d806417e89e3c035740421977f92a15c12f9fa776ac9665a1879e5f67

Ede98ae4e8afea093eae3163888255276588074 89e5559bff6dbf5bc5b554a2c

cb1da05bac46d1aeb0eeec67b2249aa8f539784c4a9ff9245b4ed4a8937ccd0f

337f28a9250592d0ebc58f5a913114df82e69ef4c44243191204adfa61f9819b

8d804533708c03ed4236be70e113a419ce1c8d8a5c36baa755cb7b787f29f54f

20ad344d20337f8a782135e59bc1f6e1a7999bcddc50fc1dc3b8b6645abcb91e

bc2e03ca292da305602c8755453fa87073810a6359f2ec9a0935fe3bb51ef886

4f31265917db7d9abbdf4b6378da0822158cc9b4bff1904adad63a87cfa82f2e

3d3ab28f09d5736fcd2215fb6395e7b15e6e9f1f86931b1d3d956c70879e9d33

13b630c5c157585f6abcb2fc8e3388c23a09f881c20cdeaffda291fb36a37539

a78cce9dc644987d3404335cefeca9833ea5f69a36b2da05e5a86505c862d867

29f7eb242d7ddcaacfaac36f036081abc28ba48faaaf9fca601725a6ed160637

62fa4dea77f33cfe294110457af90d2ccd0fc32f3d37c9ddf7a0457ed8f315ee

9c0b50ba7ea383bf16b25ea12a830d5c63c5c995ab2f494dc270137ecfd31701

3c940fdf850d0e6211b340564357094fa8ddb81351789bfd43465efa2e52acfd

59bf368c532ca20de17fdaaee2160451ae8c8f7cafd8d3c7adb263dd0978e918

b9e094892d6ed3b3eba5b56416d31b5ea635cf666ddf67ff4eb62475db7371ca

9b876e4ddeaf0d950860db4942d9be1507453ba1065a03672de41dfb287b2511

f8ef2da125ebd0f972969d12f28964a00954bad6e4f804bd1db8c0507e751bc9

f679912dbe6576989cd541b866f5f3a7a2423b1a6f92cc189a12fbffc42b926d

1e4b7d7868d25071db67da87392fd5dafab344a9fa6dc040f7afb0699152fc13

1a8573f9acba3f7d8863043223fb1d6ef4b52ad5bb4cdcb5e178e935b25b40e3

94b9c9154a23db8df436f4cdda225d9bd28dfae325dfe68e034462d70245fb0e

a7f337587cdd0e9a1fb013da274293d207815843f778c714e75693cd2c8e5f11

afb7a097cebd29157285861e7bac37648c92243143b560772e652fa87b8aed6b

e3065a6f8e49ccda273bf283c18b9344cc9ad802c1065b0fdf45cdafe92d1029

d38feef0723f730c8bb5704b4b45c8c0c324b1718b42e80b98244a7e49844331

99121c7c11bb444912d02000ce2e8a39b3e885d66889547ec8fb0c88906c22f4

6194207c32a23bac956afb47f857ebcdcb3aa37e818907e98b27acaf4b83d60f

435f9c7e3e74fa789f423e1a3c794fc8347414495a46de36e82de0e10cc0cf38

41502bc411135eb896c8a8aa7aa337ae437977473bd329ac1d0ccfa639ec4e2c

5d4b172afd897db7dddf983697c620cb1dde6341380b849f81f7606ae2073093

cb6c181823fd61558c1e6cefa9f1634d1676984316caa071c24268df493d3629

518096f15c73866783c6e10fbc9b694c41391ee6b0b3b4608ff24c3f457e21fd

904453d980dceca169497cb717731b046bbbb8c6700b90dbe46dc35c15a8fff2

8aaea85bfddaea3ec7217b5f2fa10daf0ca359f5228c3119185e7af281b42e2b

444d5257fc696b234af3311abf6985a41e6e60c66dc92dab0903cbc60156f398

e7edc16f528c9cf0455d84f412520786f31aae8f67f3f551671f576727d1d141

34a5905fd12478a0ac253f5fb1fb8e32543ea070ef3d1f84ed5e448475f385cb

9db25a250975ebce56643b75440c64705b0ecc1207d5a3d92b8f3d6060af3551

a533b2ceae875b9e14a1980d31fcd0243ef88a66371d6bcfbde7e423e0c2b610

1089bd2bc482573fc05dbea6a3c195802accedcd9ad74c6e4125a7a035c021be

398a9031f8f0eeb85169aa06340a39230beac02dc1a2a004280a1528576197ad

115127b50a0f45aabb993f8ffd5b585e063a98a17e1b687036167409cf2b0ac2

f52802d87fdaca4cc9c0ef7a6b1352163e3679272752d8ea3e7a681de99dfd43

b50d4fd8b572c3a13c4997c83e0bbbc3f7a270e75b79ec09512142f5560f61ab

2b2da9baef3c6f18ac4c4340b3107359f1113ee8ea3c097835c24546f1a3f11f

f638dcb163a2568b12a9ea757335a0cc432bee92c15c77c5e80a294ad31bd792

5946308eb0248dd65c6ddc199f8bf69576b7e1dc95eb28822a265fecb1e56c86

c8ccf5c24239360035df47fef44703d7775346dbf7b1afcf78af6250b8876521

49add5e8057e45261291d45a67b60d0db5376efe9ba6873af53fc79f27243e43

d58b9d22310bf486e4301ed93191810f07cf06ca42b5252e4ded1537680579b6

3e292943cacc062b57a2b1e88340a2d0641e901470f385168b671c90eaf70e2a

3db65b267a1e41ebb307b706f561866dce2752041f482abe93f73144df9a1d4d

cf2dfce39e8f0eb5af3a9d51b5559e2c9be27ea5c1ef899e76281a0ee530307f

878bc771d4c7416170ff358db124e1608f5612b8998199a95c5d60d8f940b26e

b7b028faf0caeca7b7f21de532299867e142fb043d31f996c5f5a3535dea4a47

dd16f5efc0cdb995aa3f7822016ae1e2a4708d5b8b5b4a2f6477f5ef5b82e205

682fdd0b1a94ea8f92981fd6b697a5c4ff817ff6e838285655ede39107ca9ade

3a845e095d227f6318cb0dc973c5ecd2a74555435fcd735b71cd30d4a862c39c

e5eab76057ff57592284f3ea66db174032c69b1808dee70c081e03771d521545

3d9e5f07897b3089600b123a50a005eab5051640661dc4575c2afc0391c97ad8

4f0bc389fcd575a732907732c223219ab0ad44571ca6f83f99358bb9e7467839

f1b40766fbaeb0248b3e629b1904156e3966d2b862d030a8218236904e8cd32f

52f124a478c562251459cacc60b7afa952a8c02df7342c1a951502307ba7b33f

3cc7000f6f2bf315a4fc3fb0ef9035f8683d4660648e23cb178656eae79b2dc5

63cd03b7e7013b0a7bac695d4fb9b5c5c7e9c556eb6eab0a9ec359049fb2621c

022d911560f38d5165ea4196ac74a141531d3e244cdc9be895e539f7143a7bbb

39ba64584fb99652e9d2c05b4afdf139317f5f2a052611b989257047cc12db74

4784f1dbfcafcef10bdfd6c2021b1e74a826917715fd84a91f610a8b6a3bdc4f

7fe854ce78e7ab7cafcc299b4f2a4ee82cc366d47f9a8961727365e45688bb4c

ac97cd95119446e96dd0bc35a4b9dc67f4ef2853e298dc145c7588807022d808

0e044c8570122a280c963cac80e0140da78ee0d378cd17cab4ea6f146ce35d15

6e960e703df3fdea6667d9c5b671e3efc05c692eb6875edc74c5ccc8ade52ac7

c8abcedb3ec20f7ab5d9b98cc32f03b318eba61f344e0537e4d4de673422c6b1

b4e0b3b783072b5266988f11bd5af2235b432619a42466fea81a35cb5edc4eea

23528e75315abed2f7a86fad26036ef1626311c3838153cb8a96bd938f0055ac

0374033592ba3bfa76d5046af2eaf4506166b157aae2c5a396c827b36d4738ca

6462c93c7a2cbad27bd1cd418bed36078860fd7f1399b477991fe3c71c0d7a8c

dcbfc3cecf75ec77de3ac314ca911af1d778e5c432df4cda146c02aa9ae84c47

fc4b29f54e0b3ed0493ba85310a2665ab47e5143f3cb3ce09686f0560dd1ed04

27f8e739b62c685c4115f49ae146bb75271d0b8fad021436939735bf7492186b

28b5ab14ad007650aa5e45f5090119a758eb45f893e400e53e5ea13ac2e5b38e

115127b50a0f45aabb993f8ffd5b585e063a98a17e1b687036167409cf2b0ac2

f52802d87fdaca4cc9c0ef7a6b1352163e3679272752d8ea3e7a681de99dfd43

b50d4fd8b572c3a13c4997c83e0bbbc3f7a270e75b79ec09512142f5560f61ab

2b2da9baef3c6f18ac4c4340b3107359f1113ee8ea3c097835c24546f1a3f11f

f638dcb163a2568b12a9ea757335a0cc432bee92c15c77c5e80a294ad31bd792

5946308eb0248dd65c6ddc199f8bf69576b7e1dc95eb28822a265fecb1e56c86

c8ccf5c24239360035df47fef44703d7775346dbf7b1afcf78af6250b8876521

49add5e8057e45261291d45a67b60d0db5376efe9ba6873af53fc79f27243e43

d58b9d22310bf486e4301ed93191810f07cf06ca42b5252e4ded1537680579b6

3e292943cacc062b57a2b1e88340a2d0641e901470f385168b671c90eaf70e2a

3db65b267a1e41ebb307b706f561866dce2752041f482abe93f73144df9a1d4d

cf2dfce39e8f0eb5af3a9d51b5559e2c9be27ea5c1ef899e76281a0ee530307f

878bc771d4c7416170ff358db124e1608f5612b8998199a95c5d60d8f940b26e

b7b028faf0caeca7b7f21de532299867e142fb043d31f996c5f5a3535dea4a47

dd16f5efc0cdb995aa3f7822016ae1e2a4708d5b8b5b4a2f6477f5ef5b82e205

682fdd0b1a94ea8f92981fd6b697a5c4ff817ff6e838285655ede39107ca9ade

3a845e095d227f6318cb0dc973c5ecd2a74555435fcd735b71cd30d4a862c39c

e5eab76057ff57592284f3ea66db174032c69b1808dee70c081e03771d521545

3d9e5f07897b3089600b123a50a005eab5051640661dc4575c2afc0391c97ad8

4f0bc389fcd575a732907732c223219ab0ad44571ca6f83f99358bb9e7467839

f1b40766fbaeb0248b3e629b1904156e3966d2b862d030a8218236904e8cd32f

52f124a478c562251459cacc60b7afa952a8c02df7342c1a951502307ba7b33f

3cc7000f6f2bf315a4fc3fb0ef9035f8683d4660648e23cb178656eae79b2dc5

63cd03b7e7013b0a7bac695d4fb9b5c5c7e9c556eb6eab0a9ec359049fb2621c

022d911560f38d5165ea4196ac74a141531d3e244cdc9be895e539f7143a7bbb

39ba64584fb99652e9d2c05b4afdf139317f5f2a052611b989257047cc12db74

4784f1dbfcafcef10bdfd6c2021b1e74a826917715fd84a91f610a8b6a3bdc4f

7fe854ce78e7ab7cafcc299b4f2a4ee82cc366d47f9a8961727365e45688bb4c

ac97cd95119446e96dd0bc35a4b9dc67f4ef2853e298dc145c7588807022d808

0e044c8570122a280c963cac80e0140da78ee0d378cd17cab4ea6f146ce35d15

6e960e703df3fdea6667d9c5b671e3efc05c692eb6875edc74c5ccc8ade52ac7

c8abcedb3ec20f7ab5d9b98cc32f03b318eba61f344e0537e4d4de673422c6b1

b4e0b3b783072b5266988f11bd5af2235b432619a42466fea81a35cb5edc4eea

23528e75315abed2f7a86fad26036ef1626311c3838153cb8a96bd938f0055ac

0374033592ba3bfa76d5046af2eaf4506166b157aae2c5a396c827b36d4738ca

6462c93c7a2cbad27bd1cd418bed36078860fd7f1399b477991fe3c71c0d7a8c

dcbfc3cecf75ec77de3ac314ca911af1d778e5c432df4cda146c02aa9ae84c47

fc4b29f54e0b3ed0493ba85310a2665ab47e5143f3cb3ce09686f0560dd1ed04

27f8e739b62c685c4115f49ae146bb75271d0b8fad021436939735bf7492186b

28b5ab14ad007650aa5e45f5090119a758eb45f893e400e53e5ea13ac2e5b38e

---