SANS

Hack the Reader: Writing Effective Threat Reports

Lenny Zeltser
@lennyzeltser
CISO at Axonius
Author and Instructor at SANS

What are your goals for a threat report?

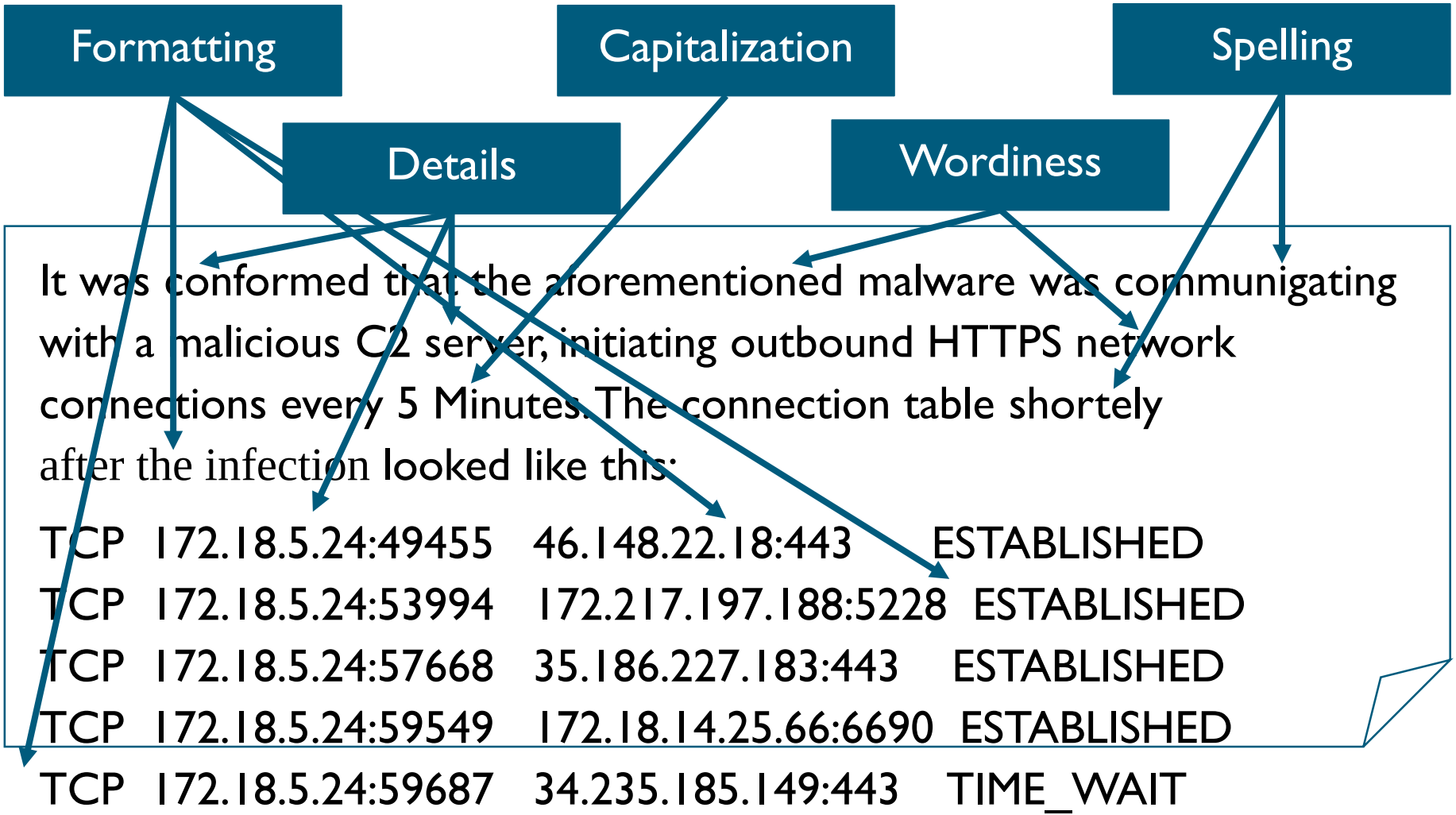
- Share your analysis details and insights.
- Instill confidence in your analysis approach.
- Propose prevention or response steps for the threat.

To succeed with writing, present **your** ideas on the **readers'** terms.

What issues can you spot in this report excerpt?

It was conformed that the aforementioned malware was communigating with a malicious C2 server, initiating outbound HTTPS network connections every 5 Minutes. The connection table shortely after the infection looked like this:

```
TCP   172.18.5.24:49455    46.148.22.18:443       ESTABLISHED
TCP   172.18.5.24:53994    172.217.197.188:5228   ESTABLISHED
TCP   172.18.5.24:57668    35.186.227.183:443     ESTABLISHED
TCP   172.18.5.24:59549    172.18.14.25.66:6690   ESTABLISHED
TCP   172.18.5.24:59687    34.235.185.149:443     TIME_WAIT
```


Formatting
Capitalization
Spelling
Details
Wordiness
It was conformed that the aforementioned malware was communigating with a malicious C2 server, initiating outbound HTTPS network connections every 5 Minutes. The connection table shortely after the infection looked like this:
TCP 172.18.5.24:49455 46.148.22.18:443 ESTABLISHED
TCP 172.18.5.24:53994 172.217.197.188:5228 ESTABLISHED
TCP 172.18.5.24:57668 35.186.227.183:443 ESTABLISHED
TCP 172.18.5.24:59549 172.18.14.25.66:6690 ESTABLISHED
TCP 172.18.5.24:59687 34.235.185.149:443 TIME_WAIT

The revised excerpt is more reader-friendly.

Our analysis confirmed that the malware was communicating with the malicious C2 server 46.148.22.18, initiating outbound HTTPS connections every 5 minutes. See Appendix A for the connection table.

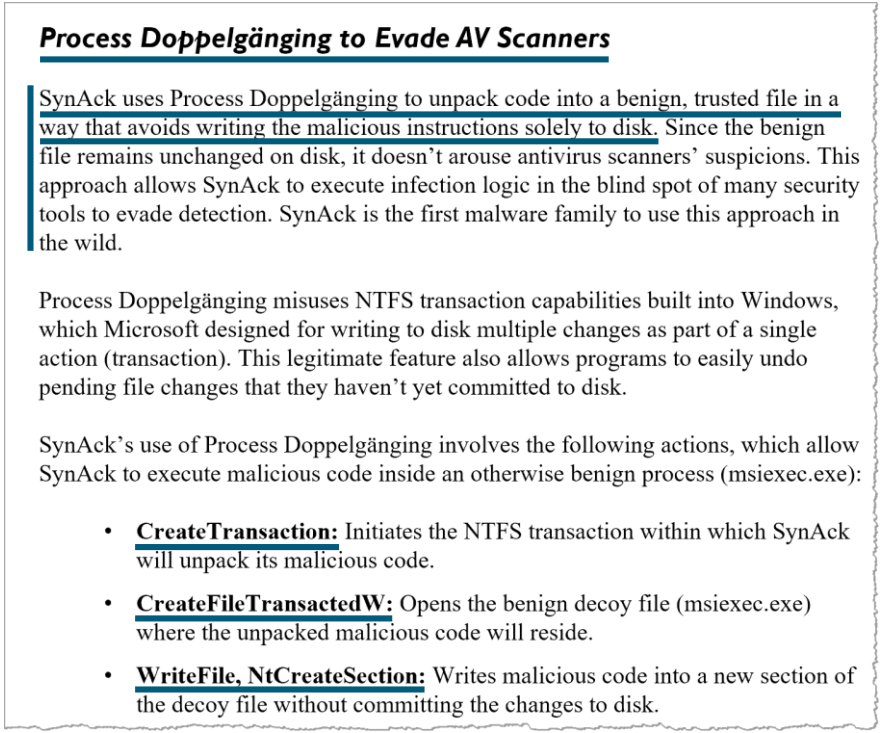
Appendix A: C2 Traffic in a Sample Connection Table

We reconstructed this connection table from the infected system, which included a C2 connection to the malicious server 46.148.22.18:

```
TCP   172.18.5.24:49455    46.148.22.18:443       ESTABLISHED
...
```

Anticipate the needs of different readers by placing your points where they're most likely to look.

- Make sure your executive summary packs a punch.
- Treat the first sentence of each paragraph as its summary.
- Sneak key ideas into the headings.
- Use the table of contents to preview the report.
- Place extras in the appendix.



Process Doppelgänging to Evade AV Scanners

SynAck uses Process Doppelgänging to unpack code into a benign, trusted file in a way that avoids writing the malicious instructions solely to disk. Since the benign file remains unchanged on disk, it doesn't arouse antivirus scanners' suspicions. This approach allows SynAck to execute infection logic in the blind spot of many security tools to evade detection. SynAck is the first malware family to use this approach in the wild.

Process Doppelgänging misuses NTFS transaction capabilities built into Windows, which Microsoft designed for writing to disk multiple changes as part of a single action (transaction). This legitimate feature also allows programs to easily undo pending file changes that they haven't yet committed to disk.

SynAck's use of Process Doppelgänging involves the following actions, which allow SynAck to execute malicious code inside an otherwise benign process (msiexec.exe):

- **CreateTransaction:** Initiates the NTFS transaction within which SynAck will unpack its malicious code.
- **CreateFileTransactedW:** Opens the benign decoy file (msiexec.exe) where the unpacked malicious code will reside.
- **WriteFile, NtCreateSection:** Writes malicious code into a new section of the decoy file without committing the changes to disk.

Why is wordiness a problem for your readers?

Attackers often pack their malicious programs to evade and hide from detection tools, and also to complicate malware analysis. To accomplish this, the attacker might begin by first compiling the malware using a standard software development tool such as Visual Studio. The attacker will then continue by using a packing tool or utility to conceal the program's malicious patterns; the packer accomplishes this by encrypting or obfuscating the file. The resulting file is hard to detect and difficult to analyze. Only later, when the packed executable arrives at the victim's system, having probably bypassed anti-malware or other security measures, will the malware get unpacked by itself into the computer's memory and run the malicious code to infect the system.

Your readers don't have time or patience for unnecessary words.

Attackers often pack ~~their~~ malicious programs to evade ~~and hide from~~ detection ~~tools,~~ and ~~also to~~ complicate ~~malware~~ analysis. ~~To accomplish this,~~ the attacker might ~~begin by~~ first compil~~ing~~e the malware using a standard ~~software~~ development tool such as Visual Studio. The attacker will then ~~continue by~~ us~~ing~~e a packing ~~tool or~~ utility to conceal the program's malicious patterns~~; the packer accomplishes this~~ by encrypting or obfuscating the file. ~~The resulting file is hard to detect and difficult to analyze.~~ Only ~~later,~~ when the packed executable arrives at the victim's system, having ~~probably~~ bypassed anti-malware ~~or other security~~ measures, will the malware ~~get~~ unpack~~ed by~~ itself into ~~the computer's~~ memory and run the malicious code ~~to infect the system~~.

Your readers don't have time or patience for unnecessary words.

Attackers often pack malicious programs to evade detection and complicate analysis. The attacker might first compile the malware using a development tool such as Visual Studio. The attacker will then use a packing utility to conceal the program's malicious patterns by encrypting or obfuscating the file. Only when the packed executable arrives at the victim's system, having bypassed anti-malware measures, will the malware unpack itself into memory and run the malicious code.

The paragraph is now 72 words, down from 119 (39% reduction).

To be succinct:

- Challenge yourself to shorten each paragraph you draft by at least 20%.
- Get to the point faster.
- Scrutinize each ~~and every~~ word.
- When in doubt, cut it out.

Be brief, but not at the expense of the details your readers need.

As a reader of the report, what would you want to know about threats like these?

"WannaCry outbreak infected 200,000 computers across 150 countries in the past 4 days."

"Cyber-espionage group Sofacy (a.k.a. Fancy Bear and APT28) used the first-ever instance of a rootkit targeting the Windows Unified Extensible Firmware Interface (UEFI)."

"A Business Email Compromise (BEC) scheme allowed fraudsters to steal $18.6 million from Tecnimont Pvt Ltd by convincing managers the money was for an acquisition deal."

Your readers are concerned with the following:

- What are the objectives/intent and capabilities of the threat?
- What are the opportunities for the threat to succeed in our environment?
- What's the broader threat context inside our organization and in the industry at large?
- How to counteract the threat?
- How reliable is the analysis of the threat?

For example, help your readers understand how capable the threat is at achieving its objectives.

- Explain the sophistication of the attacker's techniques:
  - Is the adversary skilled or a newbie?
  - How elaborate is the attack infrastructure?
- When discussing malware, describe the tactics the specimen uses to attempt evading defenses, such as:
  - Hiding from analysis tools, such as sandboxes and debuggers
  - Using fileless methods, such as injecting code into legitimate processes
  - Abusing capabilities built into trusted tools (e.g., document macros)

The level of detail will depend on your readers' expectations.

Here's one way to describe to a technical reader the ability of a malware sample to succeed:

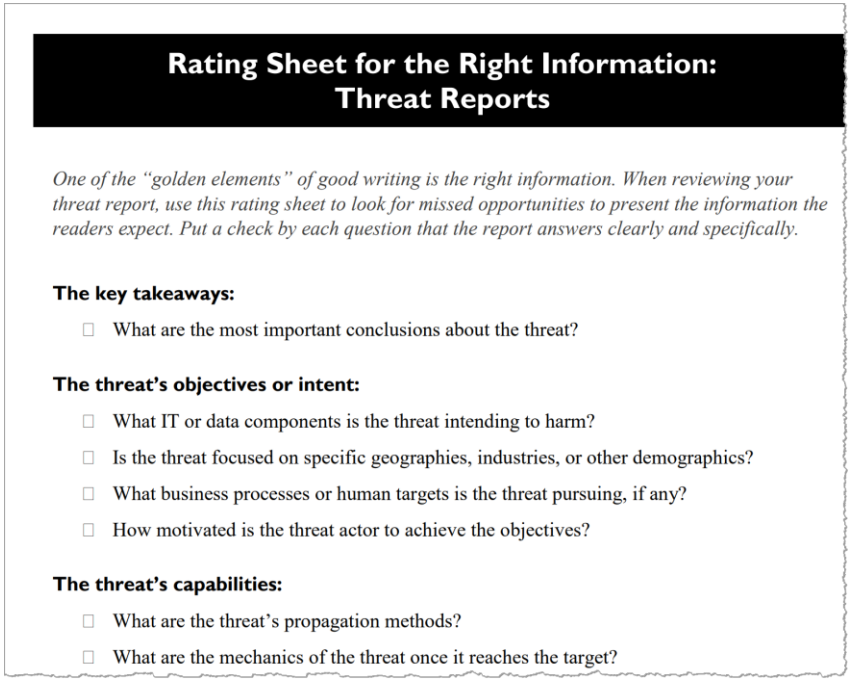
AZORult's ability to survive in the wild is due to its use of several evasion tactics, which over the years have included:

- Abusing Microsoft Office features, such as DDE to infect the system
- Using multiple packers to conceal the nature of malicious files
- Injecting code into memory space of trusted processes
- Abusing Google Update features to maintain persistence on the system
- Digitally signing code to fool many anti-malware scanners

The evolution of these capabilities indicates a skilled adversary who is determined to profit from AZORult despite defenders' countermeasures.

Use the rating sheet to assess the information aspect of your threat reports.

- The sheet reminds you what information to include: sec402.com/threat-sheet
- Use it even for rating others' threat reports to learn.
- Rating others' writing makes you better at spotting your own writing issues.



Rating Sheet for the Right Information: Threat Reports

One of the "golden elements" of good writing is the right information. When reviewing your threat report, use this rating sheet to look for missed opportunities to present the information the readers expect. Put a check by each question that the report answers clearly and specifically.

The key takeaways:

- ☐ What are the most important conclusions about the threat?

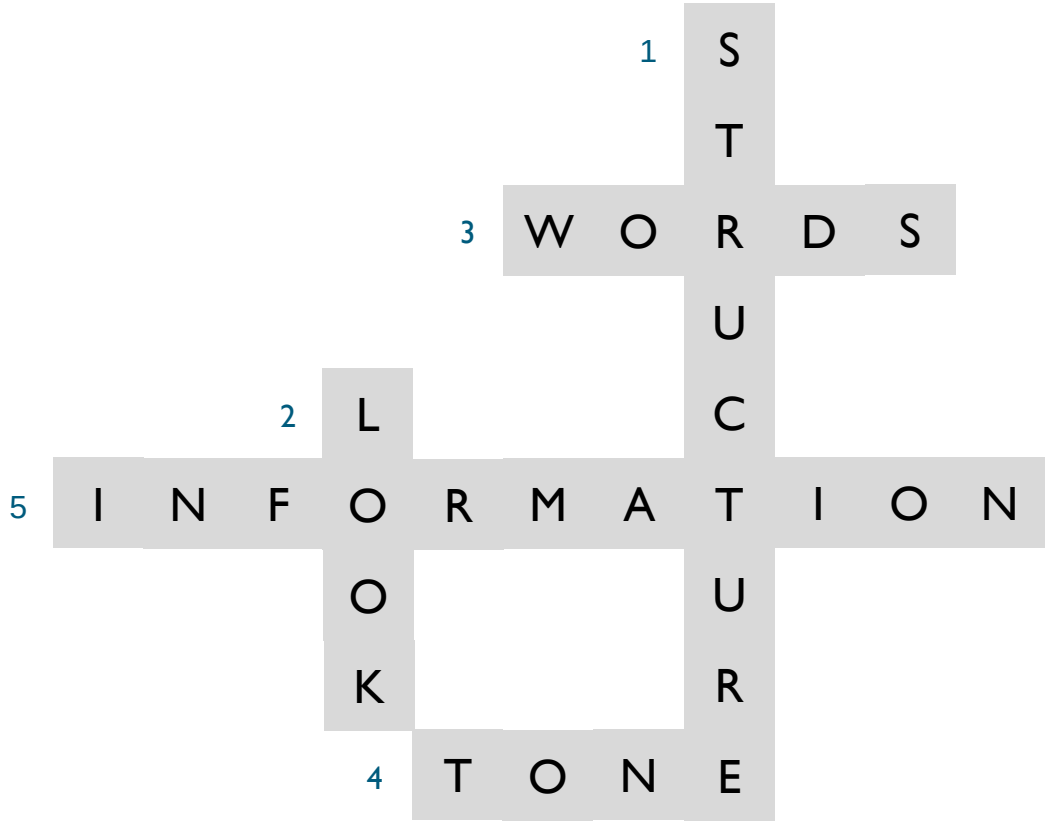
The threat's objectives or intent:

- ☐ What IT or data components is the threat intending to harm?
- ☐ Is the threat focused on specific geographies, industries, or other demographics?
- ☐ What business processes or human targets is the threat pursuing, if any?
- ☐ How motivated is the threat actor to achieve the objectives?

The threat's capabilities:

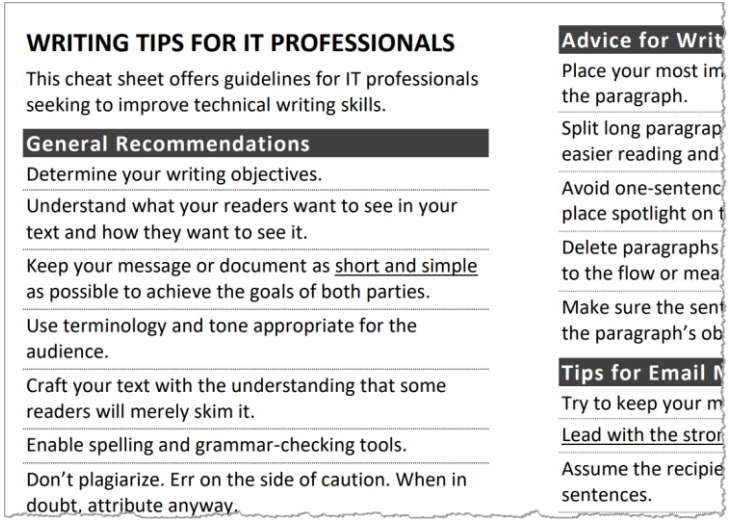
- ☐ What are the threat's propagation methods?
- ☐ What are the mechanics of the threat once it reaches the target?

To connect with your readers, consider the five "golden elements" of good writing.



To strengthen your writing skills:

- Get the threat info rating sheet: sec402.com/threat-sheet
- Review the one-page cheat sheet: sec402.com/cheat-sheet
- Watch the Top 10 Mistakes video: sec402.com/top10-video
- Consider the "Hack the Reader" course: sans.org/sec402



WRITING TIPS FOR IT PROFESSIONALS

This cheat sheet offers guidelines for IT professionals seeking to improve technical writing skills.

General Recommendations

Determine your writing objectives.

Understand what your readers want to see in your text and how they want to see it.

Keep your message or document as short and simple as possible to achieve the goals of both parties.

Use terminology and tone appropriate for the audience.

Craft your text with the understanding that some readers will merely skim it.

Enable spelling and grammar-checking tools.

Don't plagiarize. Err on the side of caution. When in doubt, attribute anyway.

Advice for Writ

Place your most im the paragraph.

Split long paragrap easier reading and

Avoid one-sentenc place spotlight on t

Delete paragraphs to the flow or mea

Make sure the sent the paragraph's ob

Tips for Email M

Try to keep your m

Lead with the stron

Assume the recipie sentences.