SANS

Top 10 Writing Mistakes in Cybersecurity and How You Can Avoid Them

Lenny Zeltser

Author and Instructor, SANS Institute
VP of Products, Minerva Labs

@lennyzeltser

What's the key to good writing in cybersecurity?

How can you get your readers to:

- Notice your writing?
- Appreciate your insights?
- Follow your advice?

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

Mistake #1: Burying the main point

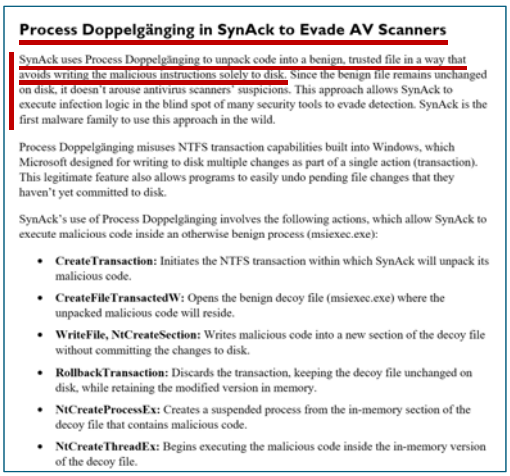
When interacting with malicious infrastructure, it's important to conceal your origin for OPSEC purposes. You can also benefit from appearing to connect from different countries to investigate the malicious infrastructure from multiple regions, which sometimes yields additional findings. That's why tunneling your connections through a VPN is often useful when performing security research.

Your readers want to see the key details up front.

Tunneling your connections through a VPN is often useful when performing security research. This helps conceal your origin, contributing to OPSEC when interacting with malicious infrastructure. Moreover, by using VPN exit nodes in different countries, you can investigate the infrastructure from multiple regions, which sometimes yields additional findings.

Preview your takeaways, in case the readers don't read the full text.

- The topic sentence previews the paragraph.
- The heading previews the section.
- The summary previews the document or the section.



Process Doppelgänging in SynAck 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.
- **RollbackTransaction:** Discards the transaction, keeping the decoy file unchanged on disk, while retaining the modified version in memory.
- **NtCreateProcessEx:** Creates a suspended process from the in-memory section of the decoy file that contains malicious code.
- **NtCreateThreadEx:** Begins executing the malicious code inside the in-memory version of the decoy file.

Mistake #2: Overstuffing the paragraphs

Email scammers use social engineering to hoodwink their victims. These measures often involve including personal details in the messages or faking an association with a company the recipient trusts. In one example, the scammer sends a message with sensitive details—such as the password the recipient once used—to "prove" that the person is in the miscreant's grip. In reality, the scammer probably obtained the data from one of the many breaches that provide swindlers with an almost unlimited supply of sensitive information. In another example, the scammer sends an email that appears to come from a trusted company, such an established shipping firm or a large bank. Since many of the recipients have business relationships with these firms, they'll often…

Your readers want ideas in easy-to-process chunks.

Email scammers use social engineering to hoodwink their victims. These measures often involve including personal details in the messages or faking an association with a company the recipient trusts.

In one example, the scammer sends a message with sensitive details—such as the password the recipient once used—to "prove" that the person is in the miscreant's grip. In reality, the scammer probably obtained the data from one of the many breaches that provide swindlers with an almost unlimited supply of sensitive information.

In another example, the scammer sends an email that appears to come…

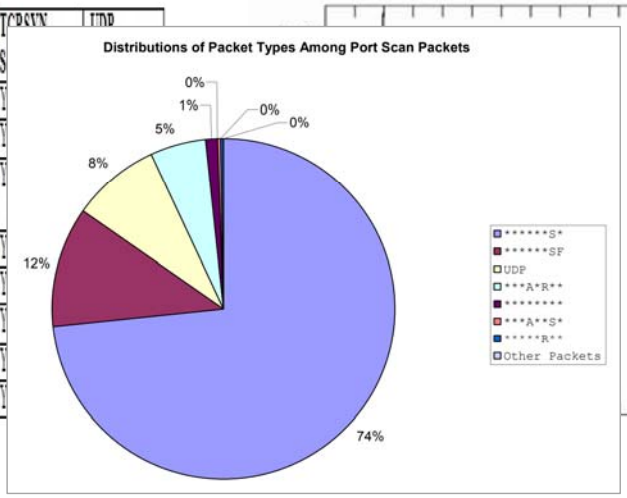
If you're unsure how to structure your ideas:

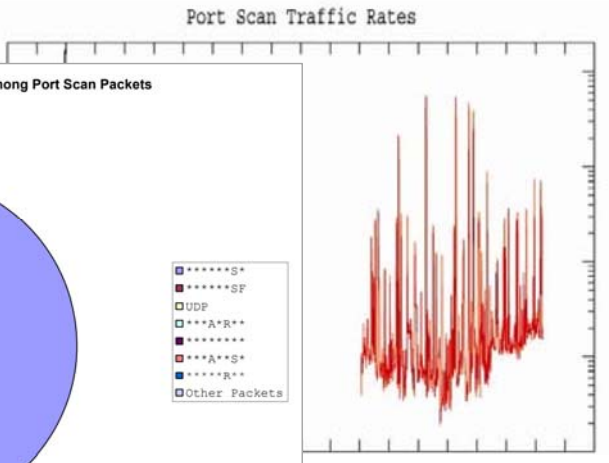
1. Jot down your thoughts without worrying about the paragraph configuration.
2. Group sentences into snippets that describe a discrete idea—one major idea per grouping.
3. Turn each snippet into a paragraph by bringing forward the main point and adjusting the following sentences to support it.

Mistake #3: Including indecipherable graphics

TOOLS COMPARISON – PART I

	L/Update	IP Ranges	Test Methods	ICMP	TCP SYN	UDP
Nmap	1,2011	Unlimited	ICMP	Y		
SuperScan 4.0	8,2003	Unlimited	ICMP	Y		
Advanced Port Scanner	7,2006	Unlimited	ICMP	Y		
AATools	1,2006	Unlimited	ICMP	Y		
AngryIP	3,2009	Unlimited	ICMP	Y		
AWSP	2,2002	Unlimited	ICMP	Y		
Unicornscan	2,2010	Unlimited	ICMP	Y		
GFILANguard	11,2010	3999	ICMP	Y		





9

Your readers want to absorb the graphic's key idea at a single glance.

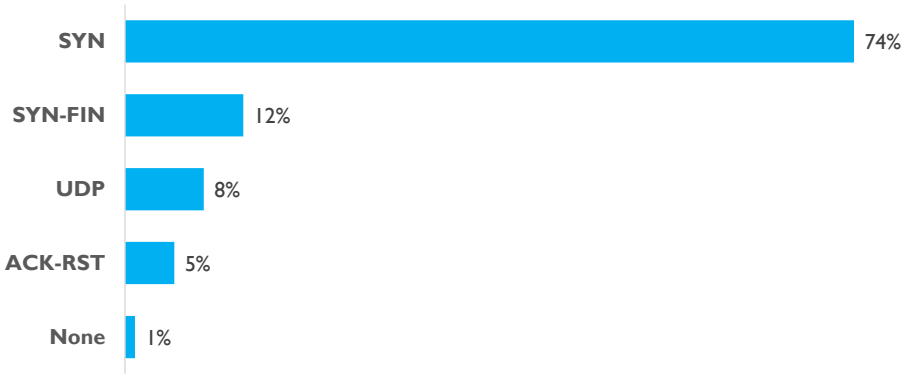


Figure 1: The vast majority of the packets were TCP with only the SYN flag set.

10

To get the most out of graphics:

- Choose a graphic type that communicates the main point.
- Eliminate visual clutter and unnecessary formatting.
- Assign an informative title or caption.
- Refer to the graphic from the body of your text.

Mistake #4: Applying inconsistent formatting

Static Analysis

One of our approaches to analyzing the security posture of the GrandMarine app involved decompiling contents of its APK file using the free tool jd-gui.

Our analysis focused on identifying obvious flaws in the app's interactions with its libraries. JD-GUI also helped us understand *the app's structure* for the subsequent assessment steps.

Network Traffic analysis

Another aspect of the assessment involved examining the Network Traffic between the Grand Marine app and its backend servers…

Your readers want formatting that guides them through the text without distractions.

Static Analysis

One of our approaches to analyzing the security posture of the GrandMarine app involved decompiling contents of its APK file using the free tool JD-GUI.

Our analysis focused on identifying obvious flaws in the app's interactions with its libraries. JD-GUI also helped us understand the app's structure for the subsequent assessment steps.

Network Traffic Analysis

Another aspect of the assessment involved examining the network traffic between the GrandMarine app and its backend servers…

For uniform, helpful formatting:

- Avoid too many fonts, colors, and forms of emphasis.
- Use spacing consistently for paragraphs, headings, and lists.
- Take advantage of style management features of your app.
- Confirm formatting after pasting from another app.
- Maintain uniform capitalization conventions.

Mistake #5: Using more words than necessary

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.

15

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~~e~~ing~~ 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 securi~~ty measures, will the malware ~~get~~ unpack~~ed by~~ itself into ~~the computer's~~ memory and run the malicious code ~~to infect the system~~.

16

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, a 39% reduction.

17

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.

18

Mistake #6: Not using parallel structure

When sharing malware samples with researchers:

- Did the recipient ask for the file in the first place?
- Check whether you're allowed to release the sample.
- Using the password "infected" for zip or 7-zip archives is common.
- Instead of sending the file as an attachment, share a link for downloading it.

Readers want consistent patterns for easier skimming.

When sharing malware samples with researchers:

- Confirm the recipient wants you to provide the sample.
- Check whether you're allowed to release the sample.
- Use a zip or 7-zip archive protected with a password such as "infected".
- Share a link for downloading the file instead of sending it as an attachment.

Use parallelism to save readers from stumbling:

- Look for opportunities to present related ideas as a series, which could be a set of:
  - Bullets
  - Words
  - Headings
- Word each term in the series to be consistent with the others.

Mistake #7: Using FUD to cause anxiety

The *assumption of breach* doctrine dictates that no cybersecurity controls can remain effective against the might of today's advanced and dedicated adversaries. Modern threat actors often have at their disposal the budgetary might of nation-states and global criminal organizations.

Therefore, enterprises of all sizes must rapidly deploy technologies that help detect the inevitable compromise, so the company can commence investigation, containment, and remediation efforts.

Readers want to understand mitigation approaches to realistic and relevant risks.

Given the complexity of modern technologies and the sophistication of today's cyber threats, it's unreasonable to assume that every security measure will function perfectly at all times.

With this in mind, enterprises are increasingly incorporating resiliency principles into their cybersecurity programs, seeking to avoid catastrophic failures even if security incidents occur.

Modern SOC practices and the associated technologies make this possible, allowing enterprises to detect, contain, and remediate security problems before they escalate into major breaches.

23

Exercise caution when using fear to frame problems.

Fear of a cybersecurity breach can motivate your readers to pay attention if you:

- Focus on specific risk factors relevant to the reader.
- Propose a plan to mitigate the fear.
- Avoid indiscriminately raising uncertainty and doubt.

Fear is a reaction to a specific threat that might have a countermeasure, while **anxiety** is a general state of distress. Anxiety can scare people into inaction.

24

Mistake #8: Escalating tensions in difficult situations

Riley,

This is the third time I'm sending you this request to push out the recent Adobe Reader patches ASAP. As I repeatedly stated in my earlier messages to you, this security update fixes multiple vulnerabilities, 43 of which Adobe designated as CRITICAL. As you know, one of the bugs addresses a zero-day issue that threat actors have already began exploiting.

What do I need to do to get you to act?! If these unpatched vulnerabilities lead to a breach, it'll be on you, not me. You've been warned.

25

Readers want interactions that are constructive and non-confrontational.

Riley,

I worry that we're leaving the organization unprotected from active campaigns that are infecting systems through Adobe's recent vulnerabilities. Let's come up with a plan for rolling out these critical updates to minimize the risk that our infrastructure gets breached.

I'll give you a call this afternoon to brainstorm the best way to do this as quickly and smoothly as possible.

26

When expressing dissatisfaction or concerns:

- Remain tactful and courteous.
- Criticize the action or the situation, not the doer.
- Emphasize the negative consequences of what was or wasn't done.
- Clarify what steps will improve the situation.

27

Mistake #9: Including details most readers don't need

Our analysis confirmed that the system was communicating with a malicious C2 server 46.148.22.18, initiating outbound HTTPS connections every five minutes. For example, the connection table shortly after the infection looked like this:

```
TCP   172.18.5.24:49455   46.148.22.18:443      ESTABLISHED
TCP   172.18.5.24:52879   54.208.224.182:443    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   172.18.5.24:59192   172.18.14.25.66:6690  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
```

28

Readers want to see answers to their questions without distractions.

Our analysis confirmed that the system was communicating with the malicious C2 server 46.148.22.18, initiating outbound HTTPS connections every five minutes. For a sample connection table from the infected host see Appendix A.

Appendix A: C2 Traffic in a Sample Connection Table

We reconstructed the following 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
...
```

29

Focus your readers' attention on the details they need.

- Anticipate your readers' questions, which might include:
  - What are the most important takeaways?
  - What happened or what did you discover?
  - How did you arrive at your conclusions?
- Use structural elements, such as the summary, headings, and topic sentences to speak to multiple audiences.
- Move "just in case" details into the appendix or offer to supply them in a separate document.

30

Mistake #10: Not giving credit where credit is due

Determined by whom?

It has been determined that the Hilton Honors email that resembled a phishing message was, in fact, non-malicious.

Which researchers?

Researchers identified a new malware family named Elephant Mouse, which stands out in its ability to evade common memory forensics approaches.

31

Readers want to understand your sources and contributors.

The Doeco information security team determined that the Hilton Honors email that resembled a phishing message was, in fact, non-malicious. Thanks to Sasha Schafer for performing this analysis on such short notice.

Researchers at cybersecurity firm MSSP Corp identified a new malware family named Elephant Mouse, which stands out in its ability to evade common memory forensics approaches.

32

Clarify your references and acknowledge the work of others.

- Explain which information you obtained yourself and which details came from others.
- Include references whenever quoting or paraphrasing others' writing.
- Thank those who contributed to the efforts about which you're writing.

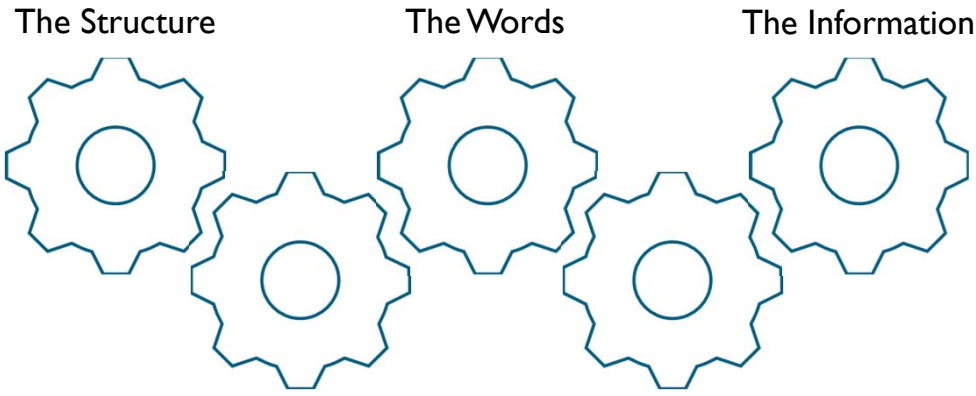
33

Now you know how to avoid the top 10 writing mistakes:

- Burying the main point
- Overstuffing the paragraphs
- Including indecipherable graphics
- Applying inconsistent formatting
- Using more words than necessary
- Not using parallel structure
- Using FUD to cause anxiety
- Escalating tensions in difficult situations
- Including details most readers don't need
- Not giving credit where credit is due

34

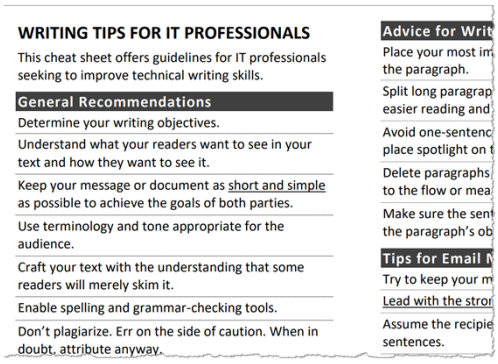
The mistakes you saw span five categories, which form the "golden elements" of writing.



35

To further strengthen your writing skills:

- Explore the one-page cheat sheet: sec402.com/cheat-sheet
- Consider the new writing course for security pros: sec402.com/beta
- Review Additional Resources links at the bottom of the SEC402 page.



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 W

Try to keep your m

Lead with the stror

Assume the recipie sentences.

36

Listen to this webinar and get these slides at:
sec402.com/top10-webinar

Lenny Zeltser
zeltser.com
@lennyzeltser