Incident handler's journal

WiCyS Google Cybersecurity Cohort 2025

Carla Jacobsen

Date: Oct. 06, 2025	**Entry:** 001
Description	Small healthcare clinic hit by ransomware attack.
Tool(s) used	Ransomware was deployed. Incident response tools unknown.
The 5 W's	Capture the 5 W's of an incident. • **Who**: Ransomware gang. • **What** : Hit by ransomware attack. • **When** : Tuesday, 09:00:00 AM • **Where** : Malicious email attachment hit company network. • **Why** : Employees tricked by spearphishing email.
Additional notes	Make frequent backups of database information. Some online, some offline. Offline backups will be safe from attacks. Educate employees on phishing and social engineering.

Date: Oct 13, 2025	**Entry:** 002
Description	Employee opens attachment from email and the computer is infected.
Tool(s) used	Hashing tool to hash the file. Something to hide the malicious nature of the file from the email detection rules.
The 5 W's	Capture the 5 W's of an incident. • **Who** - Spear phishing threat actor • **What** - Employee downloaded password protected file and opened it. The file infected the computer. • **When -** 01:11 - 01:20 PM • **Where** - Malicious email attachment • **Why** - Employee opened malicious file.
Additional notes	Malicious file is a backdoor and trojan. Contacts 432 different IP addresses. Some interesting IP addresses include: [108].[177].[119].[100-106, 113, 138, 147, 99] , [178].[79].[208].[1] (flagged as malicious by 1 vendor), [204].[79].[197].[200,203] (flagged as malicious by 1 vendor), [217].[20].[58].[99-101] (flagged as malicious by 1 vendor), [72].[21].[81].[200] (flagged as malicious by 1 vendor), [8].[8].[8].[8] (flagged as malicious by 1 vendor), [87].[248].[202].[1] (flagged as malicious by 4 vendors). Seven flagged by one vendor, one flagged by 4 vendors. 55 contacted URLs. Notable URLs include org[.]misecure[.]com[/]index[.]html (flagged as malicious by 9 vendors), and org[.]misecure[.]com[/]favicon[.]ico (flagged as malicious by 12 vendors). One flagged by 9 vendors and one flagged by 12 vendors. 100 different domains. Notable domains include cs9[.]wac[.]phicdn[.]net (flagged as malicious by 1 vendor), fp2e7a[.]wpc[.]2be4[.]phicdn[.]net (flagged as malicious

	by 1 vendor), fp2e7a[.]wpc[.]phicdn[.]net (flagged as malicious by 1 vendor), org[.]misecure[.]com (flagged as malicious by 10 vendors), misecure[.]com (flagged as malicious by 5 vendors), sinkhole[.]dynu[.]net (flagged as malicious by 3 vendors), sni1gl[.]wpc[.]nucdn[.]net (flagged as malicious by 1 vendor), and wu[.]wpc[.]apr-52dd2[.]edgecastdns[.]net (flagged as malicious by 1 vendor). Five flagged by 1 vendor each, one flagged by 3 vendors, one flagged by 5 vendors, and one flagged by 10 vendors. Network based indicators: contacts several very suspicious domains and ip addresses. Host based indicators: Drops over 8,900 files. Tools: malware kit or phishing kit. TTPs: Phishing.

Date: Oct 14 2025	**Entry:** 003
Description	Continuation of entry 002.
Tool(s) used	Hashing tool to hash the file. Something to hide the malicious nature of the file from the email detection rules.
The 5 W's	Capture the 5 W's of an incident. • **Who** - Phishing threat actor “Clyde West” • **What** - “Clyde” sent an email with a malicious attachment disguised as a resume. • **When** - Wed July 20, 2022 09:30:14 AM • **Where** - HR department • **Why** - HR employee downloaded the file thinking it was a resume.
Additional notes	Malicious email address: 76tguyhh6tgftrt7tg[.]su Malicious email address IP address: [114].[114].[114].[114] Malicious file: bfsvc[.]exe Suspicious indicators in email: unusual randomized email address name, lots of typos, resume is exe attachment Message part 1: There are several things about this email that seem to be suspicious. The email address seems to be a random string of letters seemingly unrelated to “Def Communications”, there are several typos in the email, and the resume is a [.]exe attachment. The SOC team recommends to not open suspicious files such as exe attachments from emails, especially ones from email addresses originating from outside of the corporate network. Facts about the malicious file: Flagged as malicious by 58 different security vendors. Is a backdoor and trojan. Message part 2:

	The file attached to the email is very suspicious and was flagged as malicious by 58 different security vendors as a backdoor and trojan. IP addresses to blacklist: [87].[248].[202].[1] (associated with the file)(flagged by 4 vendors), [114].[114].[114].[114] (IP address of malicious email) Message part 3: The SOC team recommends to immediately blacklist the IP addresses of [87].[248].[202].[1] and [114].[114].[114].[114], which are associated with the malicious email address and the malicious attachment. Domains and URLs to blacklist: *[.]misecure[.]com (flagged as malicious by at least 5 vendors), *[.]dynu[.]net (flagged as malicious by 3 vendors) Message part 4: The SOC team also recommends to immediately blacklist the domains of *[.]misecure[.]com and *[.]dynu[.]net, which are associated with the malicious attachment. Other actions to take: examine the machine and other machines on the company network for further signs of infection and possibly wipe the infected machine if necessary. Message part 5: The SOC team recommends to examine this machine and other machines on the company network for further signs of infection. A company firewall should be set up and malicious email detection rules should be set up in the company email server. Network based indicators: contacts several very suspicious domains and ip addresses. Host based indicators: Drops over 8,900 files.

Date: Oct 14, 2025	**Entry:** 004
Description	Data exfiltration event and extortion.
Tool(s) used	Web application vulnerability exploit. Forced browsing.
The 5 W's	Capture the 5 W's of an incident. • **Who** - external threat actor • **What** - threat actor exfiltrated sensitive customer data. • **When** - Dec 22, 2022 03:13 PM PT • **Where** - web application, customer data server • **Why** - threat actor wanted to use the exfiltrated data to extort by threatening to release the information if not paid
Additional notes	Not to be confused with ransomware.

Reflections/Notes:

1. Were there any specific activities that were challenging for you? Why or why not?
    a. The first one was challenging to try and figure out how all of this works.
2. Has your understanding of incident detection and response changed since taking this course?
    a. Yes, I learned that all of my observations can be important enough to write down. I also learned about the 5 Ws and why they are important.
3. Was there a specific tool or concept that you enjoyed the most? Why?
    a. I liked the virustotal one, it was interesting to see all the suspicious things the file did.