



Target & WiCyS Challenge

June 15th, 2023

Target has invested to build an industry-leading team of experts and advanced capabilities



Team

Hire experts from all industries, invest in continuous learning



Collaboration

Partner across industries to share intel and best-practices



Culture

Foster a company of shared accountability for security



Cybersecurity Organization

Protect Target's technology and information by fostering a culture of security accountability, enabling our guests to shop with confidence.

Cyber Defense

Threat Intelligence | Detection | Incident Response | Data Loss Prevention
Enterprise Incident Management | Cyber Engineering | Fraud & Abuse

Cyber Solutions

Identity Solutions | Access Solutions | Penetration Testing | Product Intelligence
Vulnerability Management | Endpoint Security | Network Security

Cyber Risk

Policy & Risk | Security Awareness | PCI Security | Controls Assurance
SOX IT | Vendor Security | Cyber Management Office





**CYBER DEFENSE
CHALLENGE**
MADE POSSIBLE BY TARGET



Top 10 Participants

 Alessandra P.	 Anchalee M.	 Isabel M.	 Katherine B.	 Krysten S.
 Natalia D.	 Paulina S.	 Poornima V.	 Robin B.	 Shannon S.




WiCyS Challenge Team

CYBER DEFENSE CHALLENGE MADE POSSIBLE BY TARGET

This unique program will provide hands-on experience, giving WiCyS members a taste of what it's like to be on a Cyber Defense Team. Registration is open thru June 14.

[REGISTER HERE](#) →



The banner features a dark purple background with a glowing blue circuit pattern. On the right, the text 'CYBER DEFENSE CHALLENGE' is prominently displayed in white and red, with 'MADE POSSIBLE BY TARGET' below it. The Target logo (a red bullseye) and the WiCyS logo (a white shield with a power symbol and the text 'women in cybersecurity WiCyS') are also visible.

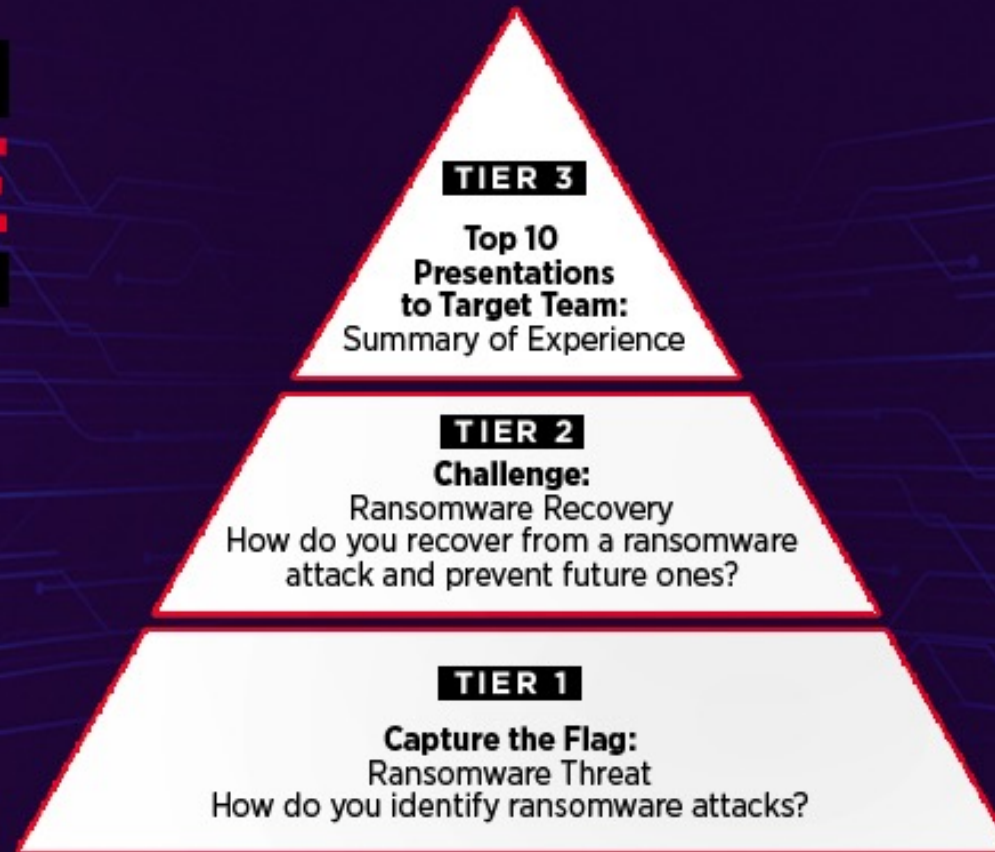
Kelsey Helms	—	Cyber Threat Intel
Ryan Borre	—	Reverse Engineering
Devin Smith	—	CSIRT
Rick Magnuson	—	Cyber Defense
Sara Kalupa	—	Network Security Monitoring
Matt Harkrader	—	Cyber Defense
Sunit Mahajan	—	Cyber Defense

Sonia Bui	—	Cyber Threat Intel
Briana Zavala	—	Cyber Threat Intel
Dan Sherman	—	Cyber Defense
Kurt Rotzler	—	Cyber Defense
Kyle Fenzel	—	Cyber Defense
Mercedes Cox	—	Cyber Fraud & Abuse
Tim Grech	—	Cyber Defense



CYBER DEFENSE CHALLENGE

MADE POSSIBLE BY TARGET



Oh no!
Your files have been encrypted.
All encrypted files have an extension of .shiny

Don't waste your time trying to decrypt the files by yourself, and don't attempt to contact anyone for help, either.
There is no available decryptor for you to use. Only we can help you recover your files.

Do not reset or shut down your computer, it's too late for that.

To recover your files:
1) Go to <http://gold.venom.sting>
2) Follow the instructions on the site

OR

1) Send \$500,000 worth of Bitcoin to this address:
14hahahaEvMFqrCd2J9vsNjaUhjEdYCsTnG3r

But don't wait too long or I may delete your files.

Sting sting,
Shiny Scorpion



WiCyS Challenge

SHINY SCORPION

DETAILS:

Origins:
Eastern Europe

Motivation:
Financial

First Seen:
March 2022

Last Seen:
May 2023



DESCRIPTION:

SHINY SCORPION is an emerging, financially-motivated threat actor, likely operating out of Eastern Europe, and focused on monetization activities such as ransomware and data theft extortion. First observed in 2022 and active through the first half of 2023, SHINY SCORPION has been observed targeting a wide range of industries in the United States and Western Europe, and uses a mix of publicly available offensive security tools such as Cobalt Strike and Brute Ratel C4, as well as smaller set of custom developed malware for encrypting Windows or Linux systems.

MALWARE:

Cobalt Strike
Brute Ratel
Custom ransomware

SHINY SCORPION just launched an attack against a crucial third party company of yours! Luckily, they are performing the right containment measures, are being very transparent, and looking to collaborate with you to make sure their downtime won't affect your business relationship. Help your third party understand the intrusion, recover, and get back into action!



WiCyS Challenge

Help your third party understand the intrusion, recover, and get back into action!

Top 50 members with the highest scores will move onto the next tier!

Start now by visiting here:

<http://ctf.targetcyberchallenge.com/>

Passcode: WiCyS_Target_2023

SHINY SCORPION

DETAILS:

Origins:
Eastern Europe

Motivation:
Financial

First Seen:
March 2022

Last Seen:
May 2023



DESCRIPTION:

SHINY SCORPION is an emerging, financially-motivated threat actor, likely operating out of Eastern Europe, and focused on monetization activities such as ransomware and data theft extortion. First observed in 2022 and active through the first half of 2023, SHINY SCORPION has been observed targeting a wide range of industries in the United States and Western Europe, and uses a mix of publicly available offensive security tools such as Cobalt Strike and Brute Ratel C4, as well as smaller set of custom developed malware for encrypting Windows or Linux systems.

MALWARE:

Cobalt Strike
Brute Ratel
Custom ransomware

WiCyS Challenge Set-up

- **Analysis Tools**

- **CyberChef** - <https://gchq.github.io/CyberChef>
 - The Cyber Swiss Army Knife - web app for encryption, encoding, compression and data analysis
- **Decompiler Explorer** - <https://dogbolt.org>
 - Online decompiler that shows equivalent C-like output of decompiled programs
- **ChatGPT** - <https://chat.openai.com>
- **TIO** - <https://tio.run>
 - Online interpreters for programming languages
- **YARA** - <https://virustotal.github.io/yara/>
 - Malware identification/classification
- **VirusTotal** - <https://www.virustotal.com/>
 - Malware (and more!) analysis and metadata repository
- **Wireshark** - <https://www.wireshark.org/>
 - Make sure to add the USBPCAP plugin during install
- **C/Golang/HTML/JavaScript/Python**
 - Languages used for challenges or to solve challenges



WiCyS Challenge Support

Communications & Support

- Slack Support channel
 - **Introductions**
 - Introduce yourself and make connections
 - **FAQs**
 - Frequently Asked Questions will be posted here
 - **Office Hours (Tues & Thurs 2-4 CST)**
 - Sign-up for 30 min time slots to get help with the challenge
 - **Fun Facts**
 - Industry trends and interesting articles
 - **General**
 - We will post information on Tier 1 and announcements about the challenge