sysdig SECURE EVERY SECOND.

All I Know About Cybersecurity I Learned From Fungus

A. FunGuy
Cybersecurity Mycologist

(Alexander Lawrence
Field CISO)



You've come to a cybersecurity talk about fungus!

- Congratulations! You're among the top 12% of coolest people at this conference!
- Topics:
  - A fungus that takes another fungus and turns it into something else.
  - A fungus that infects and changes the behavior of the organism.
  - A fungus that lives in a relationship going undetected.
- Call to Action

Background

Who the heck am I to be talking about this:

- Education in Biology
  (Plant & Fungal anatomy and physiology)
- Worked in Cybersecurity for the last 20+ years
  (started around the era of NT4 + System Policy Editor)

It takes a nerdy person, trained by a nerdy person, who are passionate about nerdy things.





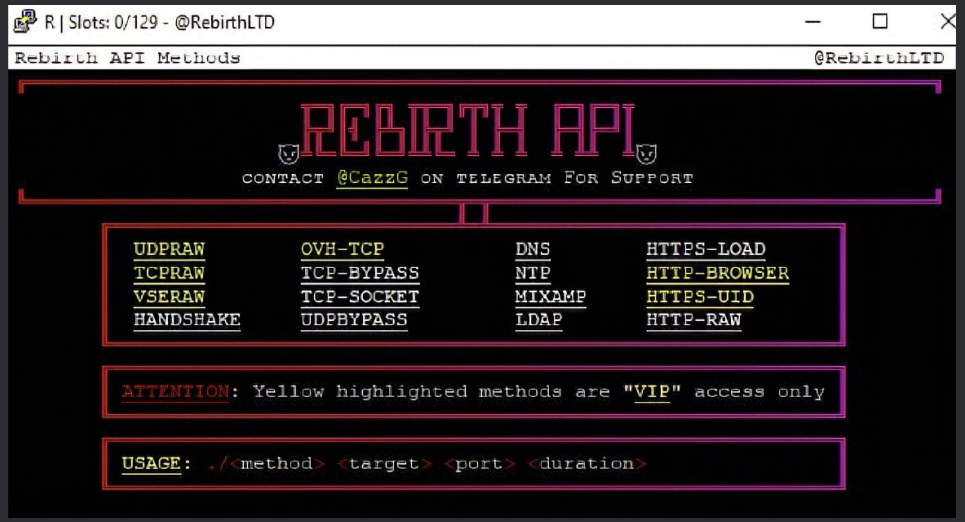
Dr. Tom Volk (1/28/59 - 11/28/22)
University of Wisconsin - La Crosse

Professor with 2 hearts
http://youtu.be/uONRTsReox8

A Change of Heart
http://youtu.be/zU6mmix04PI

Rebirth Botnet + Ophiocordyceps unilateralis

The return of a botnet and the “Zombie-ant fungus” (aka that fungus from “The Last of Us”).



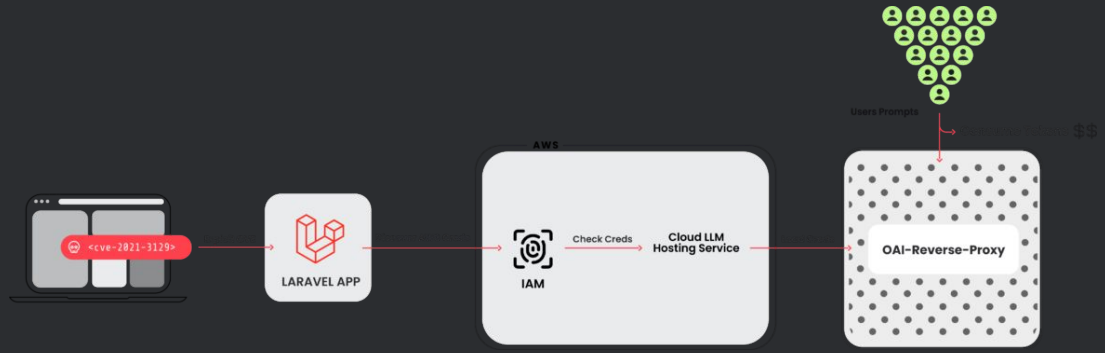


Rebirth Botnet + Ophiocordyceps unilateralis

	Rebirth Botnet	Ophiocordyceps Unilateralis
What is it	DDoS-as-a-Service ● Based on Mirai malware family	Insect pathogen ● Infects tribe of ants: Camponotini
Target	Video game services (though not exclusively limited to)	Significantly alters behavior of infected ant (hence Zombie-ant).
How does it work	● Pay to play with over a dozen offerings. ○ Can buy API access, bigger servers, and higher attacks per second. ● Initially built to target IoT devices; evolved from there. ● Installs via malicious ELFs, executed via shell scripts. ○ Attempts to access sensitive dirs ○ Download via wget ○ Execute chmod, rm -rf, etc…	● Fruiting body grows from head over 4-10 days (while the ant still lives). ● Produces antibacterial agents to protect host after infection. ○ These substances have been adapted to human anti-infection and anticancer agents. ○ Species of infected Camponotini can cause production of different compounds.
How to beat it	Detection via prctl system call + /tmp execution.	● Susceptible to an antifungal fungus infection. ● Don't eat it.
Learn more	https://sysdig.com/blog/ddos-as-a-service-the-rebirth-botnet/	https://en.wikipedia.org/wiki/Ophiocordyceps_unilateralis

LLMJacking + Monotropa uniflora | Cephalanthera austiniae

The LLM takeover and parasitic… PLANTS?!







LLMJacking + Monotropa uniflora | Cephalanthera austiniae

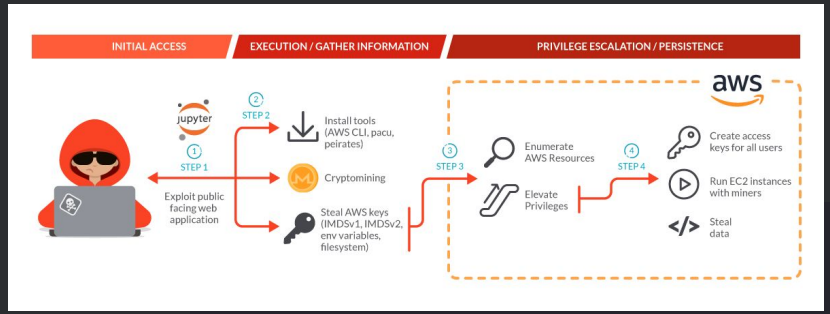
	LLMJacking	Monotropa uniforla | Cephalanthera austiniae

What is it	• Leverages stolen credentials obtained by exploiting a vulnerable version of Laravel (CVE-2021-3129) allowing remote code execution.	• Types of plants which lack chlorophyll
		• 3-Way Relationship:
		  ○ Plant has a parasitic relationship with fungus (such as the aforementioned ascomycetes)
		  ○ Fungus in a mycorrhizal (typically beneficial) relationship with surrounding plants.

Target	LLMs	Mycorhize
How does it work	• Leverages a reverse proxy to rehost LLM access and extract training data. • Attempts to “hide in plain sight.” • Costs of up to $46,000 per day to the LLM Host.	• Evolved to be very specific with host fungus (most parasitic and mutualistic relationships between organisms have coevolved together).
How to beat it	Mitigation techniques focus on real-time threat detection against cloud logs, least privilege design, robust secrets management, etc…	• Can be toxic. • Don’t eat it.
Learn more	https://sysdig.com/blog/llmjacking-stolen-cloud-credentials-used-in-new-ai-attack/	https://en.wikipedia.org/wiki/Monotropa_uniflora https://en.wikipedia.org/wiki/Cephalanthera_austiniae

ScarletEel + Hypomyces lactifluorum

A two phase attack and the “Lobster fungus” (a twofer).







ScarletEel + Hypomyces lactifluorum

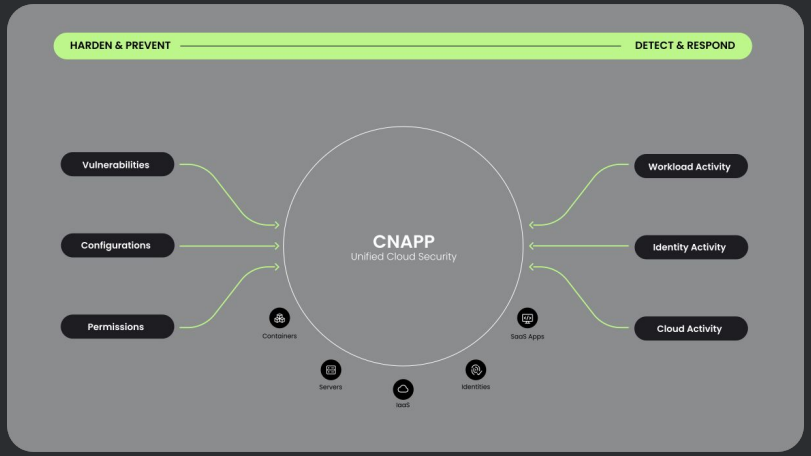
	ScarletEel	Hypomyces lactifluorum

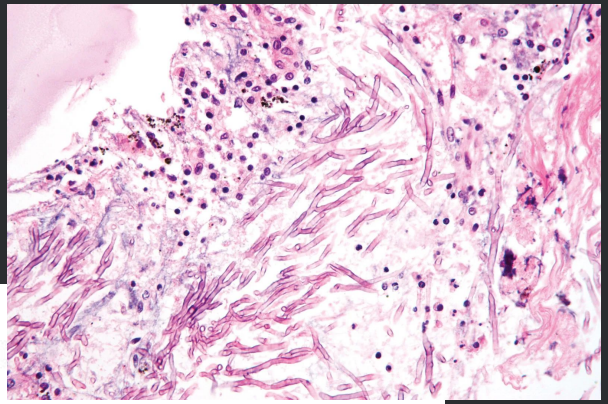
What is it	• Cloud-Native attack
	  ○ Leverages API's, cloud services, and vulnerable compute services.
		• Parasitic ascomycete
		  ○ Famous ascomycete you know: yeast!

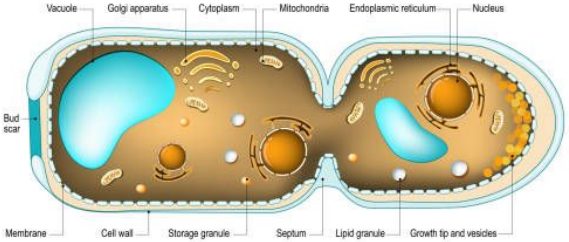
Target	AWS Cloud Infra	Infects Lactarius, Lactifluus, and Russula genus.
How does it work	• Phase 1: Repurposes existing infrastructure for crypto mining ($4,000+ per day in cloud costs). • Phase 2: privilege escalation, persistence, and IP theft. • Leverages Kubernetes and Serverless for complexity and scale. • Uses endpoint redirection for services, curl, key discovery, etc…	• Transforms the host mushroom into something that is no longer a mushroom but is **tasty**. • Infected hosts have a majority of their DNA replaced and completely alters the the metabolites the host produces.
How to beat it	Blend of detective and preventive controls	• Delicious • Eat it.
Learn more	https://sysdig.com/blog/scarleteel-2-0/	https://en.wikipedia.org/wiki/Hypomyces_lactifluorum

CNAPP + Anatomy of hyphal cells

Layers of defense in the natural and technological worlds.







CNAPP + Anatomy of hyphal cells

	CNAPP	Anatomy of hyphal cells
What is it	Layers of defense for modern architectures	The mushroom we see is one very small part of the overall organism. The largest organism on the planet is a honey fungus (Armillaria solidipes) spanning 3.5 square miles weighing as much as 35,000 tons.
Preventative	• CSPM • KSPM • DSPM • Vuln Management • IaC Analysis	Hyphae cells can be multinucleated (nuclei can travel between cells via the septum which connects them) allowing for a diversity of use cases and protections.
Detective	• XDR • CDR • Application Protection • Log Analysis	When there is a break in the hyphae that make up the mycelium a special organelle called a Woronin body will plug the septum preventing further loss of fluids.
Response	• Real Time Prevention • Reaction • Ticketing • SOAR	If you've had "Quorn" products, you've eaten it.
Learn more	https://sysdig.com/learn-cloud-native/cloud-security/cloud-native-application-protection-platform-cnapp-fundamentals/	https://en.wikipedia.org/wiki/Hypha

Call to Action

- Many models for attacks exist.
- Evolving security practices to keep up with Cloud Native are needed.
  - https://www.sysdig.com/555
- Spend time learning, it could be fungus, cybersecurity, or the history of the space program. Inspiration comes from unique places.
- Robust defenses are the best defenses.



https://en.wikipedia.org/wiki/Omphalotus_subilludens

"But evolution has a sneaky way of working on a problem from every angle." - Andy Weir, Project Hail Mary


sysdig
SECURE
EVERY
SECOND