Locknote @ BSides Dublin 2025

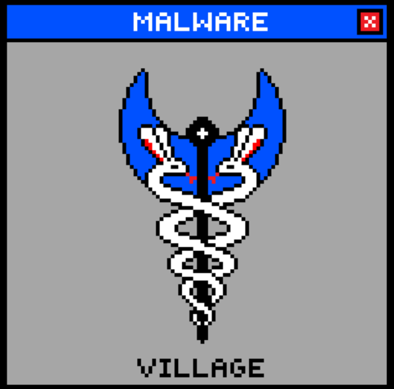
On (Un)Natural Selection: The Evolution of Malware

Lena Yu aka LambdaMamba

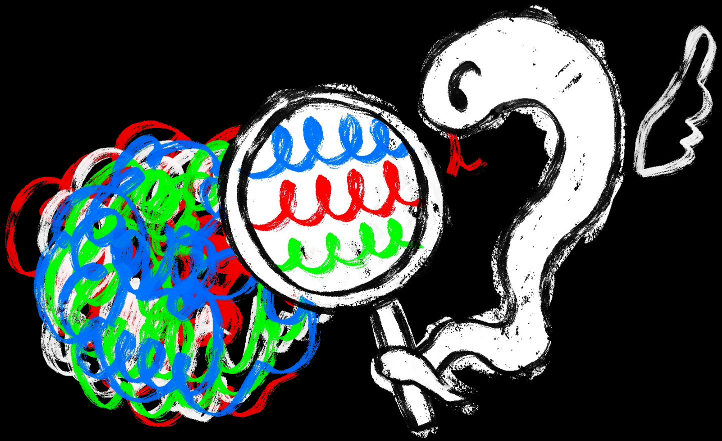
World Cyber Health

Self intro!

- Lena Yu aka LambdaMamba
  - Founder of World Cyber Health
  - Founder of Malware Village
  - Creator of Malmons aka Malware Monsters
- Before Malware...
  - TEE and RISC-V researcher



What does it mean to be "Natural"?



"Natural"

- "Existing in or derived from nature; not made or caused by humankind."

🍃🐝🦠

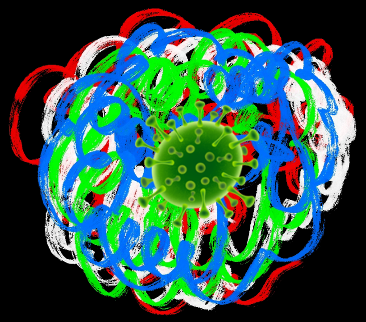
💻📀👾

What is ”Natural Science”?

- Popular definition:
  - “The natural sciences seek to understand how the world and universe around us works.”

“(Un)Natural”

- Both natural and unnatural
  - Manmade entities created through unnatural means
  - Behaves naturally in an unnatural ecosystem

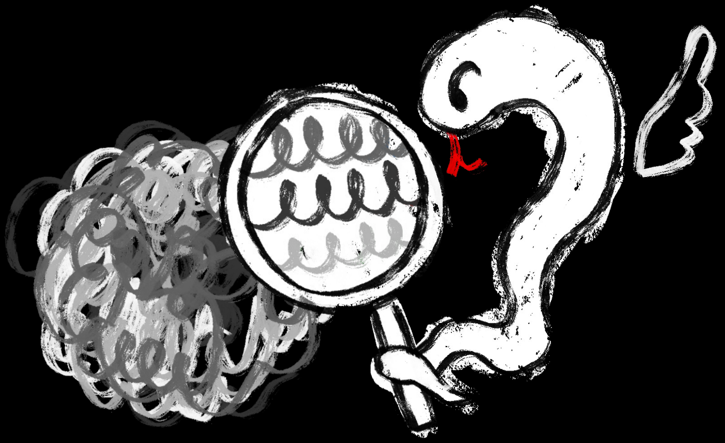


What is ”(Un)Natural Science”?

- My definition:
  - The (Un)Natural Sciences seek to understand how the world and universe work—including the human-made, ’unnatural’ world, which still operates within natural laws on a broader scale.

💻📀👾

The "(Un)Natural Science"



What is Pathogen?

- My definition is:
  - Any biological agent that has evolved or adapted to invade a host organism and cause harm to its biological systems.

What is Malware?

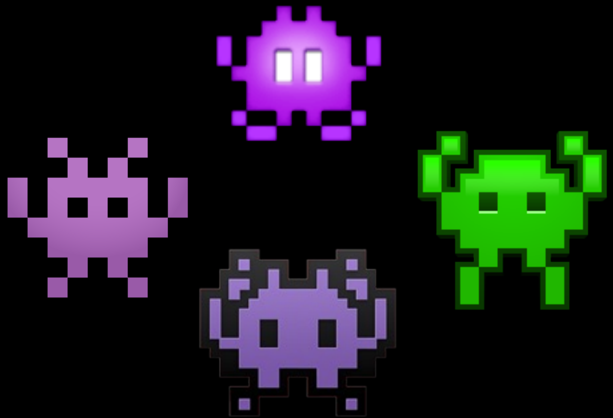
- My definition is:
  - Any software that is intentionally developed to cause harm to the victim device.

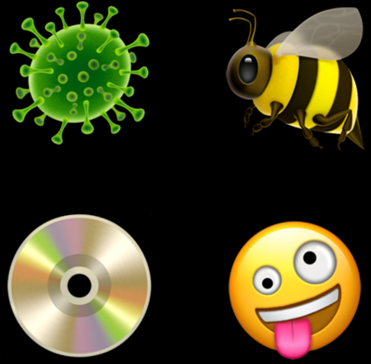
Pathogens vs Malware

- Dependent on “host” for survival
  - Pathogen host: Organisms
  - Malware host: Device
- Causes “harm” for host
  - Pathogen: cell damage, death, etc.
  - Malware: loss of data, resources, etc.

What is (Computer) Virus?

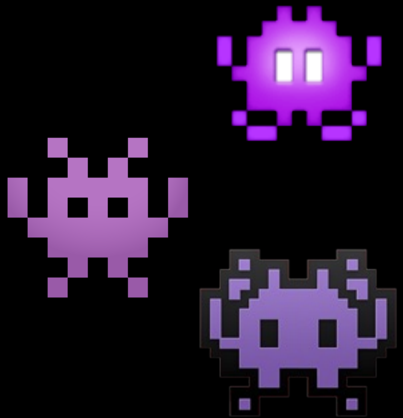
- My definition is:
  - A type of malware that is intentionally developed to infect other files or programs by embedding its code, enabling it to replicate and spread

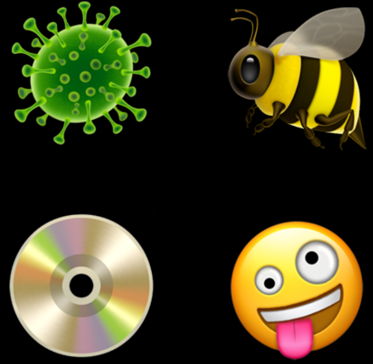




(Computer) Viruses and Malware

- Viruses ⊊ Malware
  - "Viruses are a proper subset of Malware."
  - Every virus is a malware
  - But not every malware is a virus

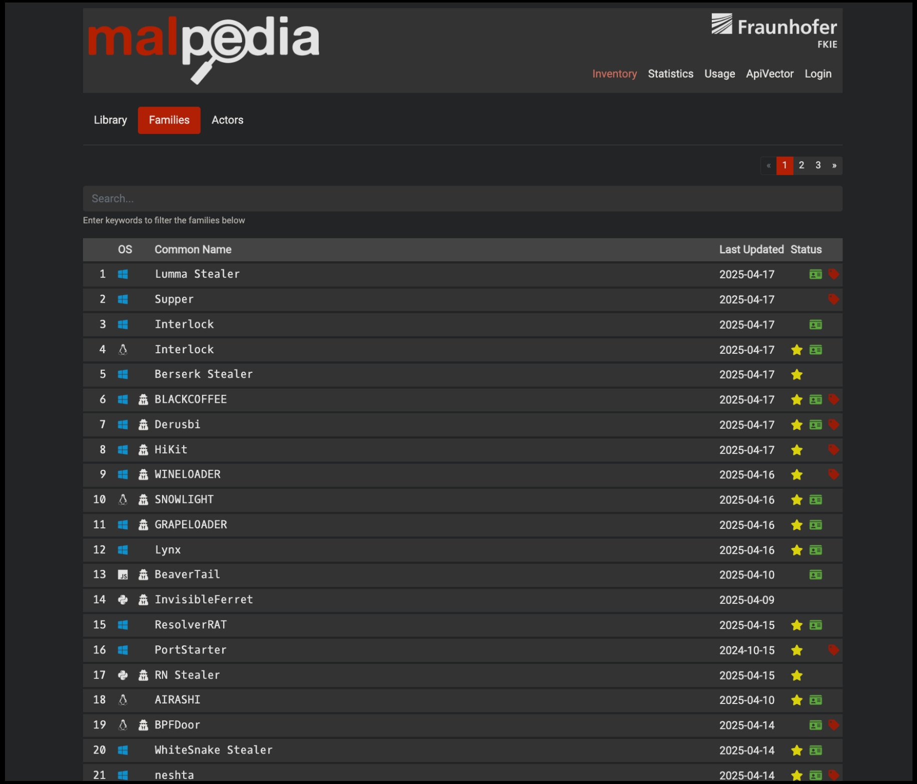




The Digital Ecosystem

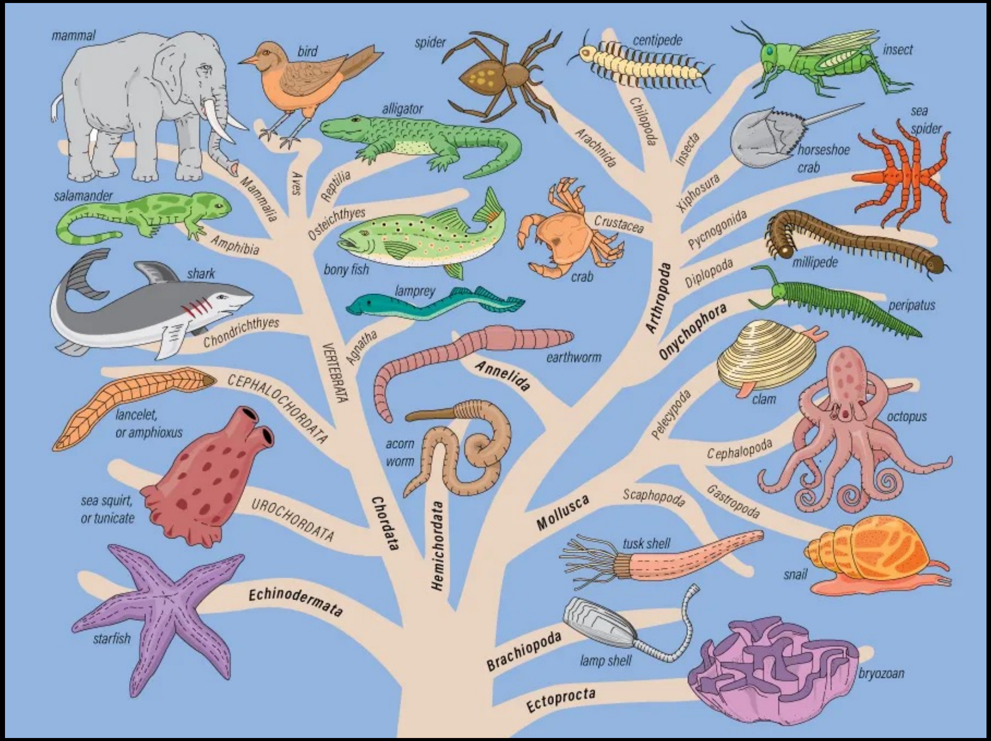
- Where "(Un)natural selection" takes place
  - Personal computers
  - Servers
  - Internet

Malware Families and Species



Enter keywords to filter the families below

	OS		Common Name	Last Updated	Status
1	⊞		Lumma Stealer	2025-04-17	▤ 🏷
2	⊞		Supper	2025-04-17	🏷
3	⊞		Interlock	2025-04-17	▤
4	🐧		Interlock	2025-04-17	★ ▤
5	⊞		Berserk Stealer	2025-04-17	★
6	⊞	🕵	BLACKCOFFEE	2025-04-17	★ ▤ 🏷
7	⊞	🕵	Derusbi	2025-04-17	★ ▤ 🏷
8	⊞	🕵	HiKit	2025-04-17	★ 🏷
9	⊞	🕵	WINELOADER	2025-04-16	★ 🏷
10	🐧	🕵	SNOWLIGHT	2025-04-16	★ ▤
11	⊞	🕵	GRAPELOADER	2025-04-16	★ ▤
12	⊞		Lynx	2025-04-16	★ ▤
13	JS	🕵	BeaverTail	2025-04-10	▤
14	🐍	🕵	InvisibleFerret	2025-04-09	
15	⊞		ResolverRAT	2025-04-15	★ ▤
16	⊞		PortStarter	2024-10-15	★ 🏷
17	🐍	🕵	RN Stealer	2025-04-15	★
18	🐧		AIRASHI	2025-04-10	★ ▤
19	🐧	🕵	BPFDoor	2025-04-14	▤ 🏷
20	⊞		WhiteSnake Stealer	2025-04-14	★ ▤
21	⊞		neshta	2025-04-14	★ ▤ 🏷



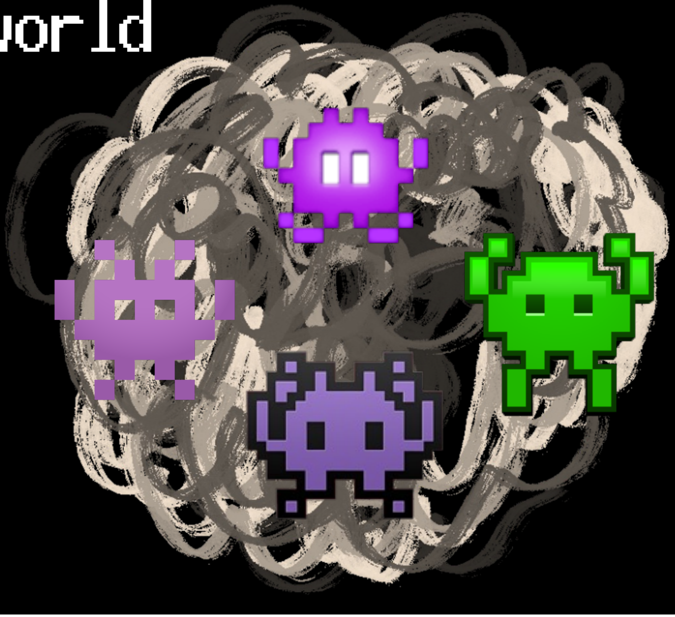
Source – Malpedia

Source – britannica

On "(Un)Natural Selection"

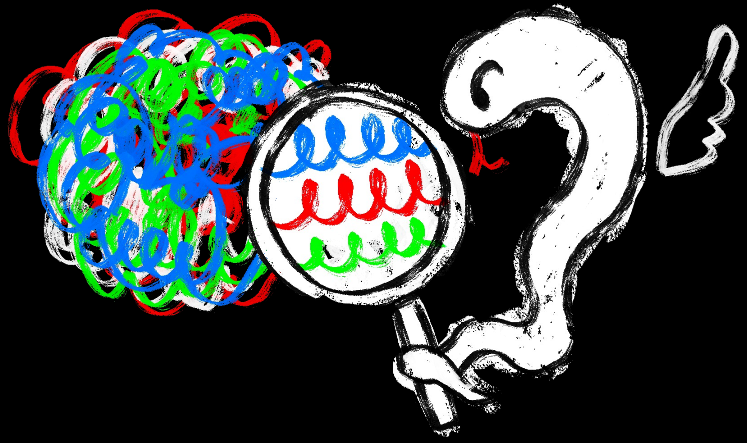
The ”Un(natural) selection”

- Pressures that affect evolution of malware
  - System-wide updates
  - Defender actions
  - Profitability for malware operators
  - Competition with other malware
  - Trends in the real world



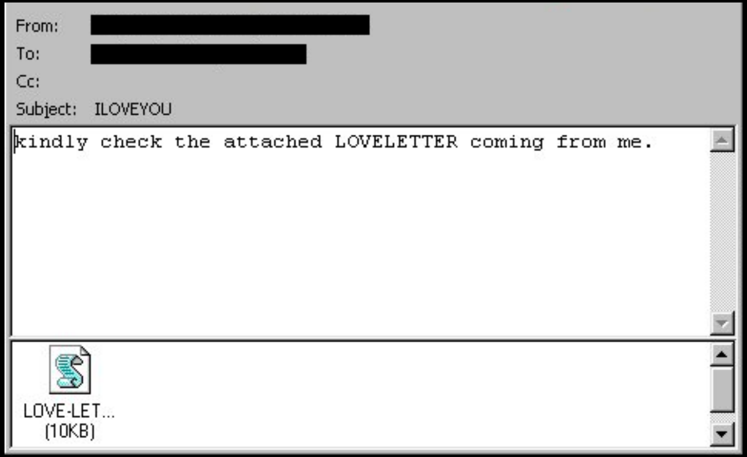
What is EGT?

- “Evolutionary game theory (EGT) is the application of game theory to evolving populations in biology. It defines a framework of contests, strategies, and analytics into which Darwinian competition can be modelled.”



ILOVEYOU

- Mass outbreak in 2000
- Relied on one deterministic action
  - Email attachment
  - Social engineering
  - Send itself to every contact
  - "Pure Strategy"



From: [redacted]

To: [redacted]

Cc:

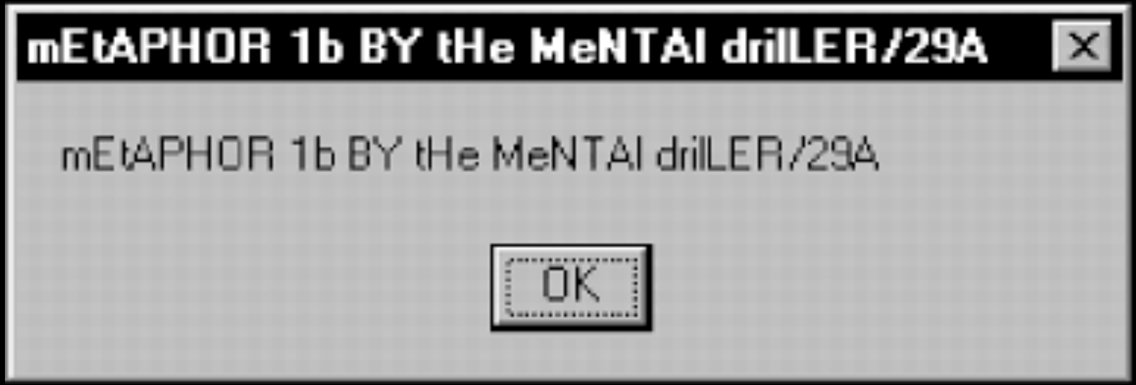
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

Source – Wikipedia

Simile

- Released in 2002
- Introduced randomness
  - 50% chance of infecting file and “metamorphizing”
  - 90% of virus code dedicated to “metamorphosis”
  - ”Mixed Strategy”



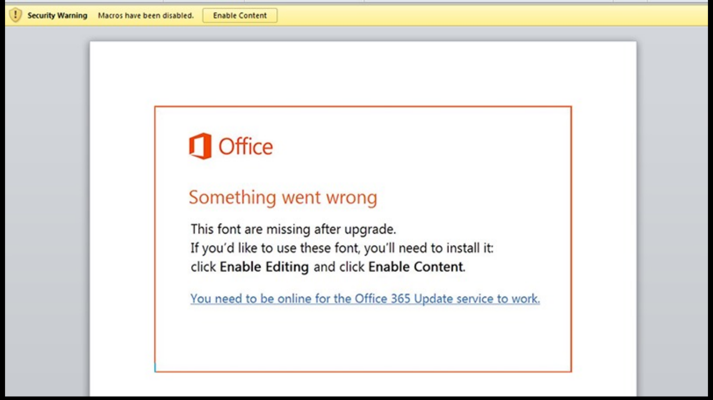
mEtAPHOR 1b BY tHe MeNTAl drilLER/29A

mEtAPHOR 1b BY tHe MeNTAl drilLER/29A

Source – broadcom.com

Emotet

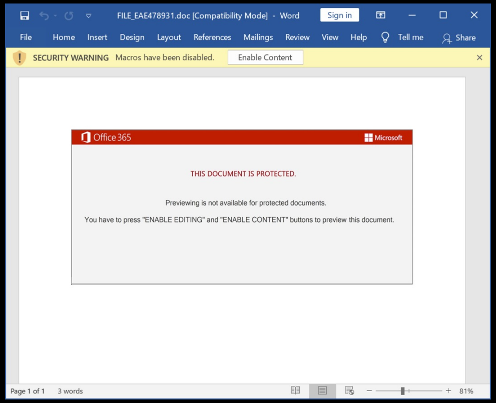
- First detected 2014
  - Ongoing operations
- Retaliates against defender actions
  - Law enforcement took down C2
    - Updated its bots to use new backup C2 servers
  - Tit-for-Tat



Something went wrong

This font are missing after upgrade.
If you'd like to use these font, you'll need to install it:
click **Enable Editing** and click **Enable Content**.

You need to be online for the Office 365 Update service to work.



THIS DOCUMENT IS PROTECTED.

Previewing is not available for protected documents.

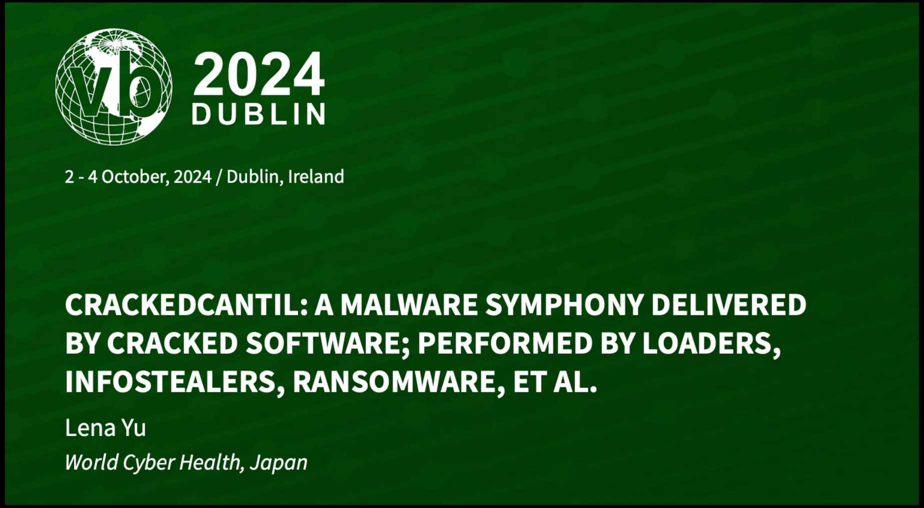
You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.

Source – BlackBerry

Malware Symbiosis

- Different families can collaborate
  - Loaders, infostealers, ransomware
- The CrackedCantil "Malware Symphony"

My Virus Bulletin Paper



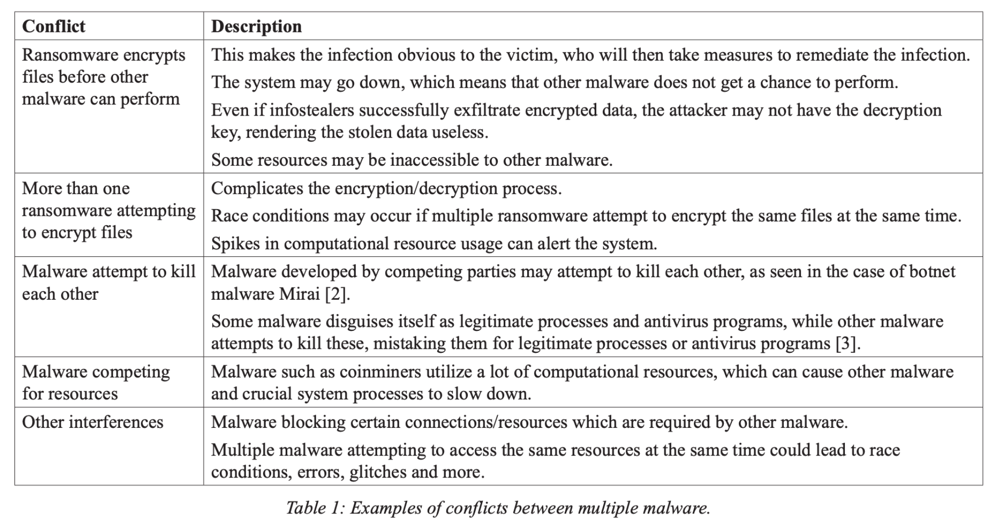
2024
DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

CRACKEDCANTIL: A MALWARE SYMPHONY DELIVERED BY CRACKED SOFTWARE; PERFORMED BY LOADERS, INFOSTEALERS, RANSOMWARE, ET AL.

Lena Yu

World Cyber Health, Japan



Conflict	Description
Ransomware encrypts files before other malware can perform	This makes the infection obvious to the victim, who will then take measures to remediate the infection. The system may go down, which means that other malware does not get a chance to perform. Even if infostealers successfully exfiltrate encrypted data, the attacker may not have the decryption key, rendering the stolen data useless. Some resources may be inaccessible to other malware.
More than one ransomware attempting to encrypt files	Complicates the encryption/decryption process. Race conditions may occur if multiple ransomware attempt to encrypt the same files at the same time. Spikes in computational resource usage can alert the system.
Malware attempt to kill each other	Malware developed by competing parties may attempt to kill each other, as seen in the case of botnet malware Mirai [2]. Some malware disguises itself as legitimate processes and antivirus programs, while other malware attempts to kill these, mistaking them for legitimate processes or antivirus programs [3].
Malware competing for resources	Malware such as coinminers utilize a lot of computational resources, which can cause other malware and crucial system processes to slow down.
Other interferences	Malware blocking certain connections/resources which are required by other malware. Multiple malware attempting to access the same resources at the same time could lead to race conditions, errors, glitches and more.

Table 1: Examples of conflicts between multiple malware.

The "(Un)Natural Historian"

From an “(Un)Natural Historian” perspective

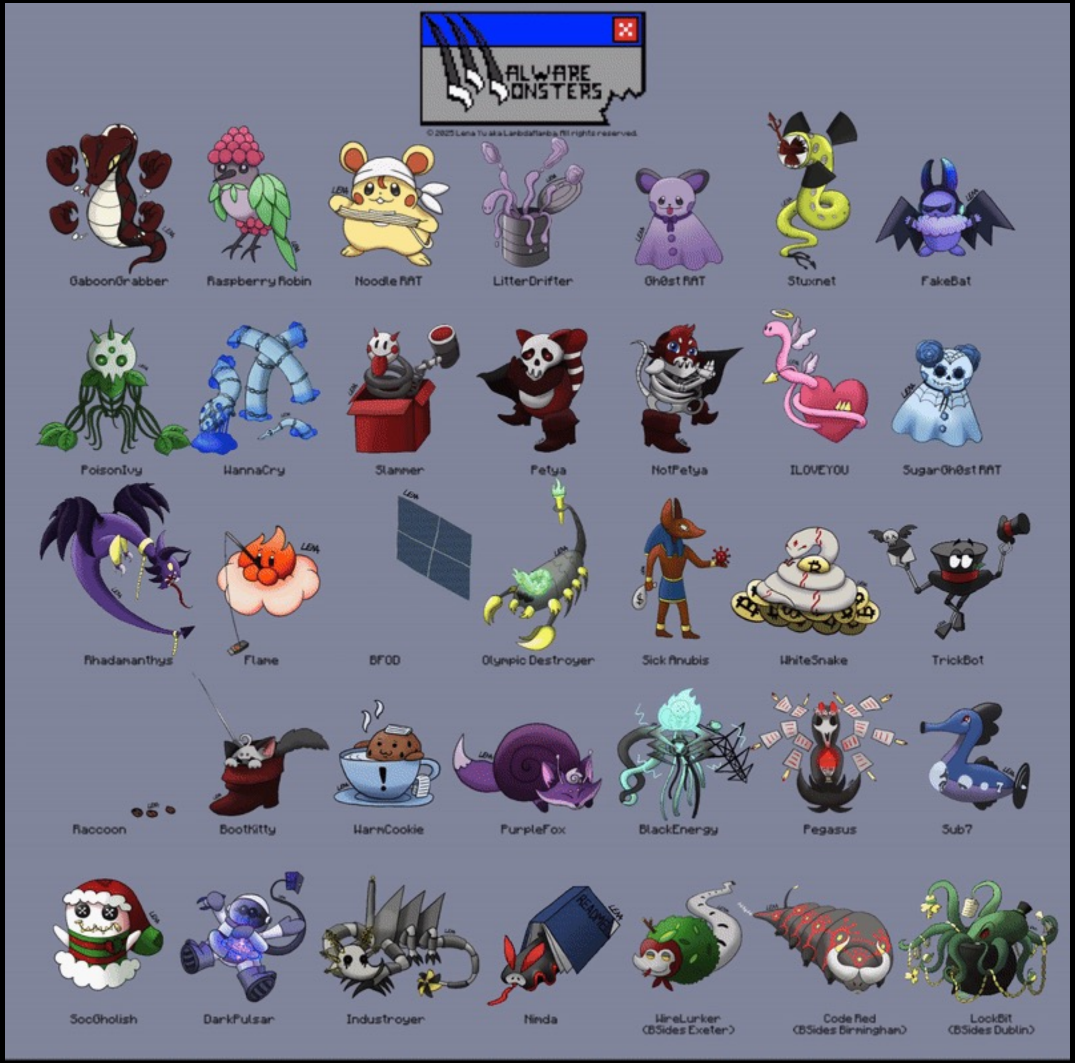
- Treat malware as if it’s a living entity
  - Survive
  - Adapt
  - Evolve
- I made Malmons aka Malware Monsters

Malware Monsters aka Malmons

ALWARE ONSTERS
GaboonGrabber
Raspberry Robin
Noodle RAT
LitterDrifter
Gh0st RAT
Stuxnet
FakeBat
PoisonIvy
WannaCry
Slammer
Petya
NotPetya
ILOVEYOU
SugarGh0st RAT
Rhadamanthys
Flame
BFOD
Olympic Destroyer
Sick Anubis
WhiteSnake
TrickBot
Raccoon
BootKitty
WarmCookie
PurpleFox
BlackEnergy
Pegasus
Sub7
SocGholish
DarkPulsar
Industroyer
Nimda
WireLurker (BSides Exeter)
Code Red (BSides Birmingham)
LockBit (BSides Dublin)

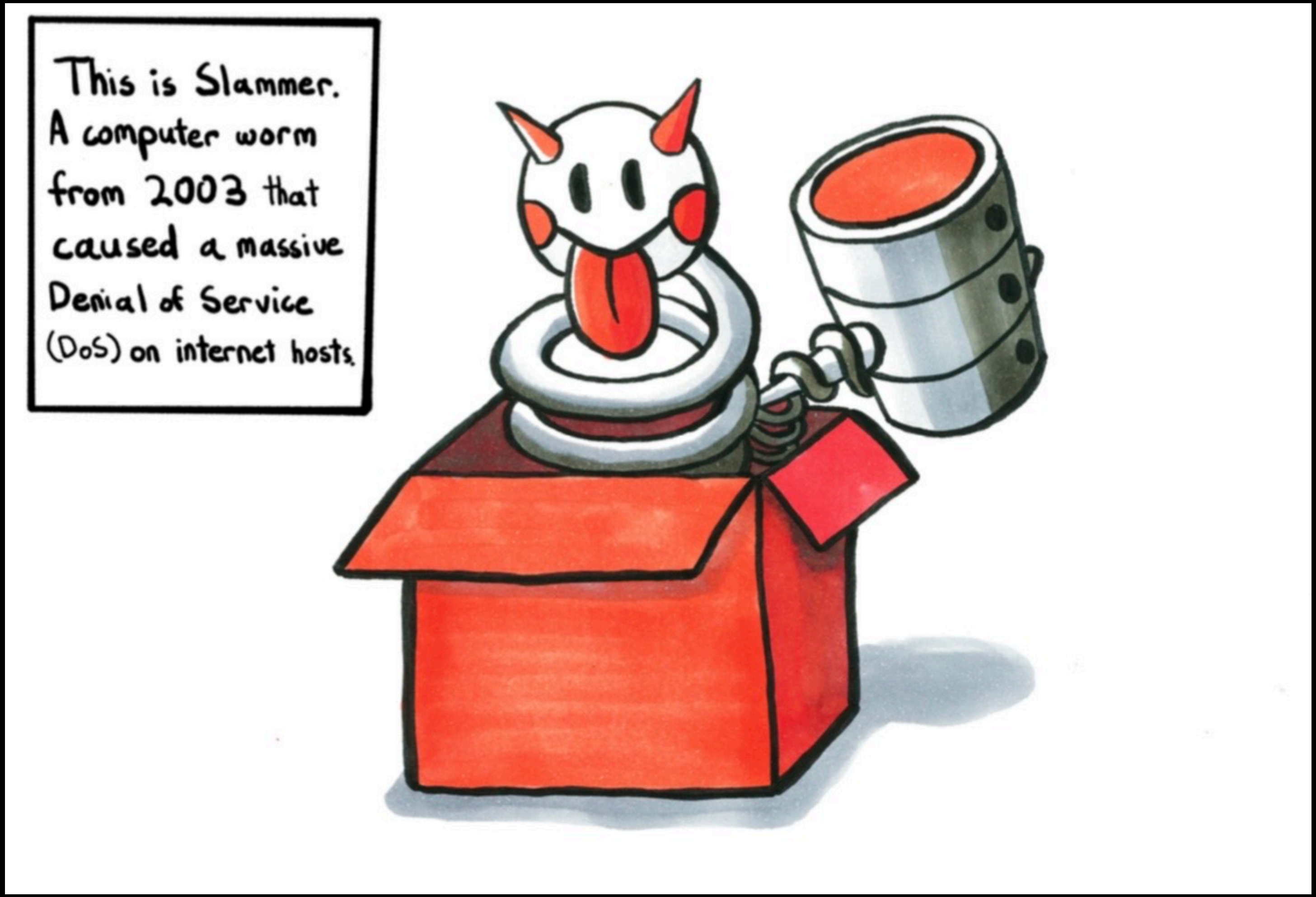
github.com/LambdaMamba/MalwareMonsters

Bringing them to life...



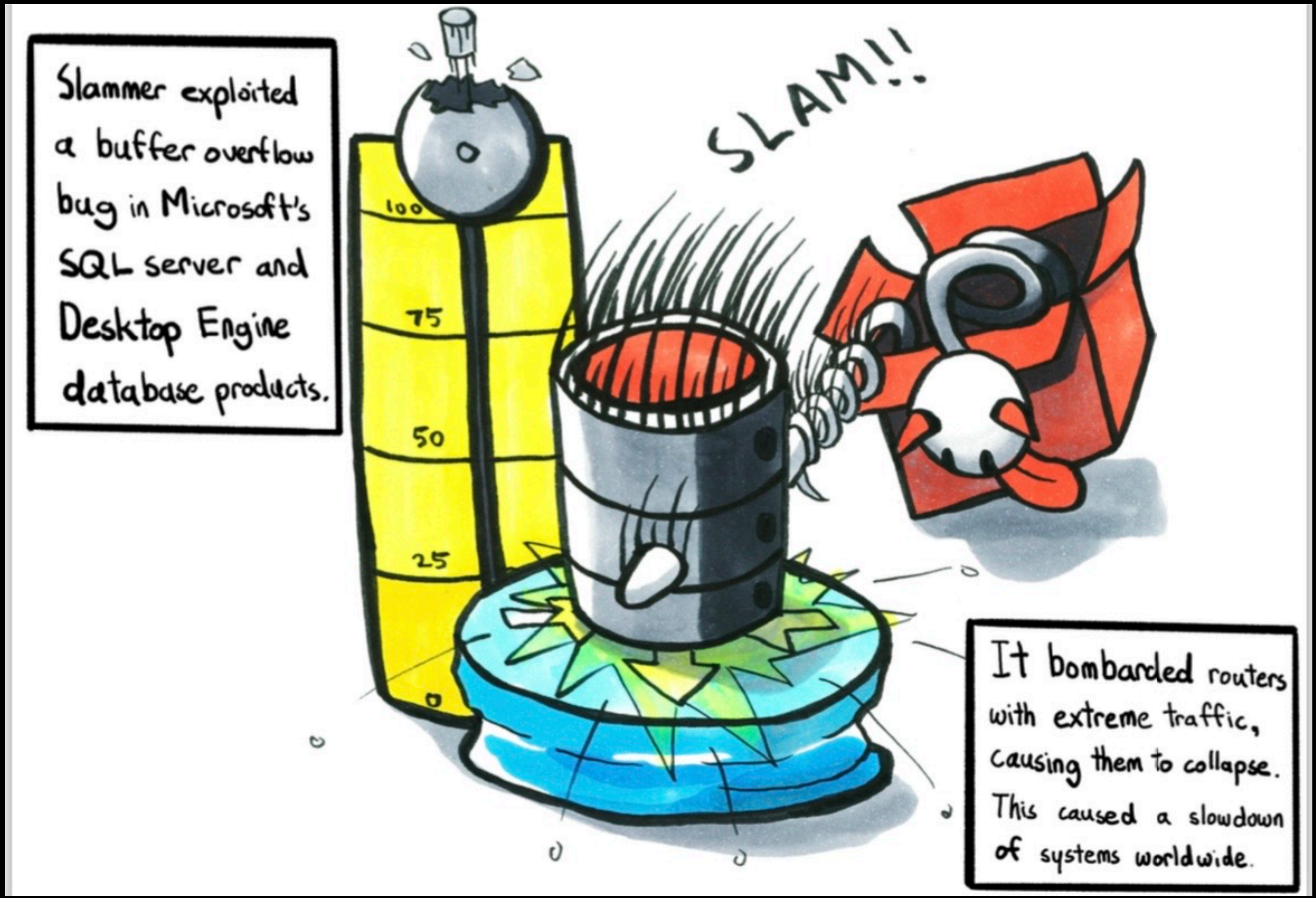
github.com/LambdaMamba/MalwareMonsters

Explaining Malware via Malmons

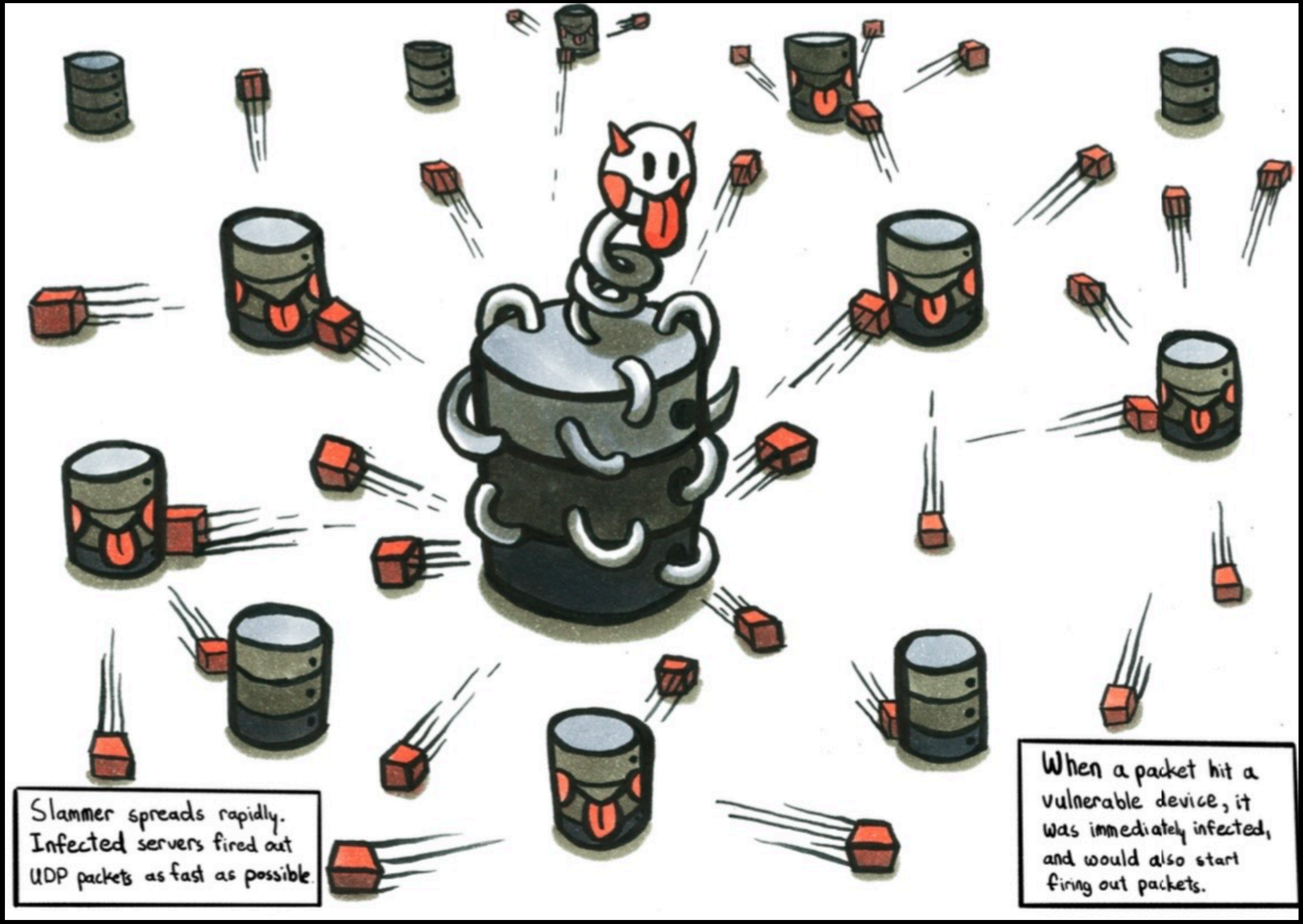


This is Slammer. A computer worm from 2003 that caused a massive Denial of Service (DoS) on internet hosts.

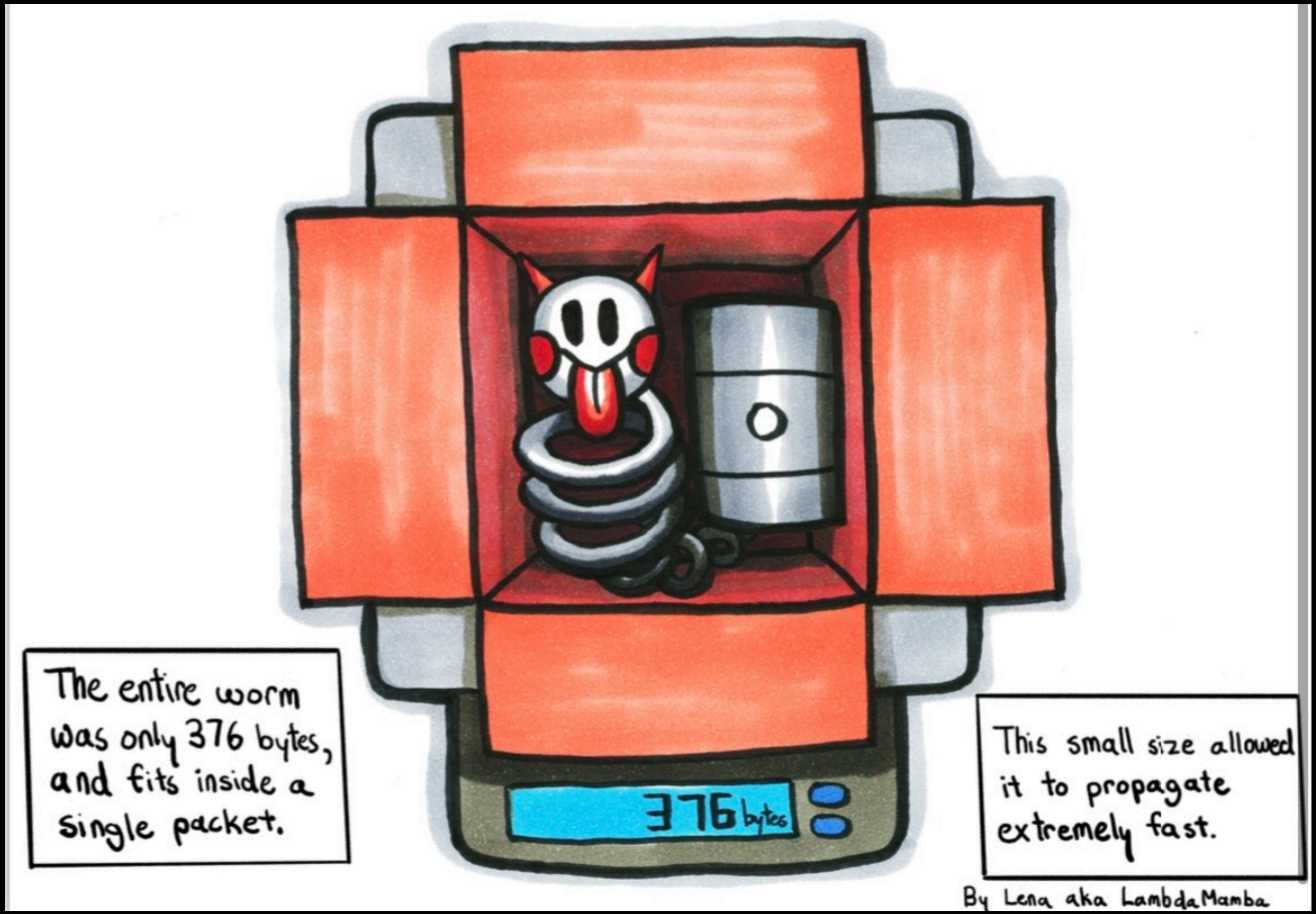
Explaining Malware via Malmons


Slammer exploited a buffer overflow bug in Microsoft's SQL server and Desktop Engine database products.
SLAM!!
100
75
50
25
0
It bombarded routers with extreme traffic, causing them to collapse. This caused a slowdown of systems worldwide.

Explaining Malware via Malmons

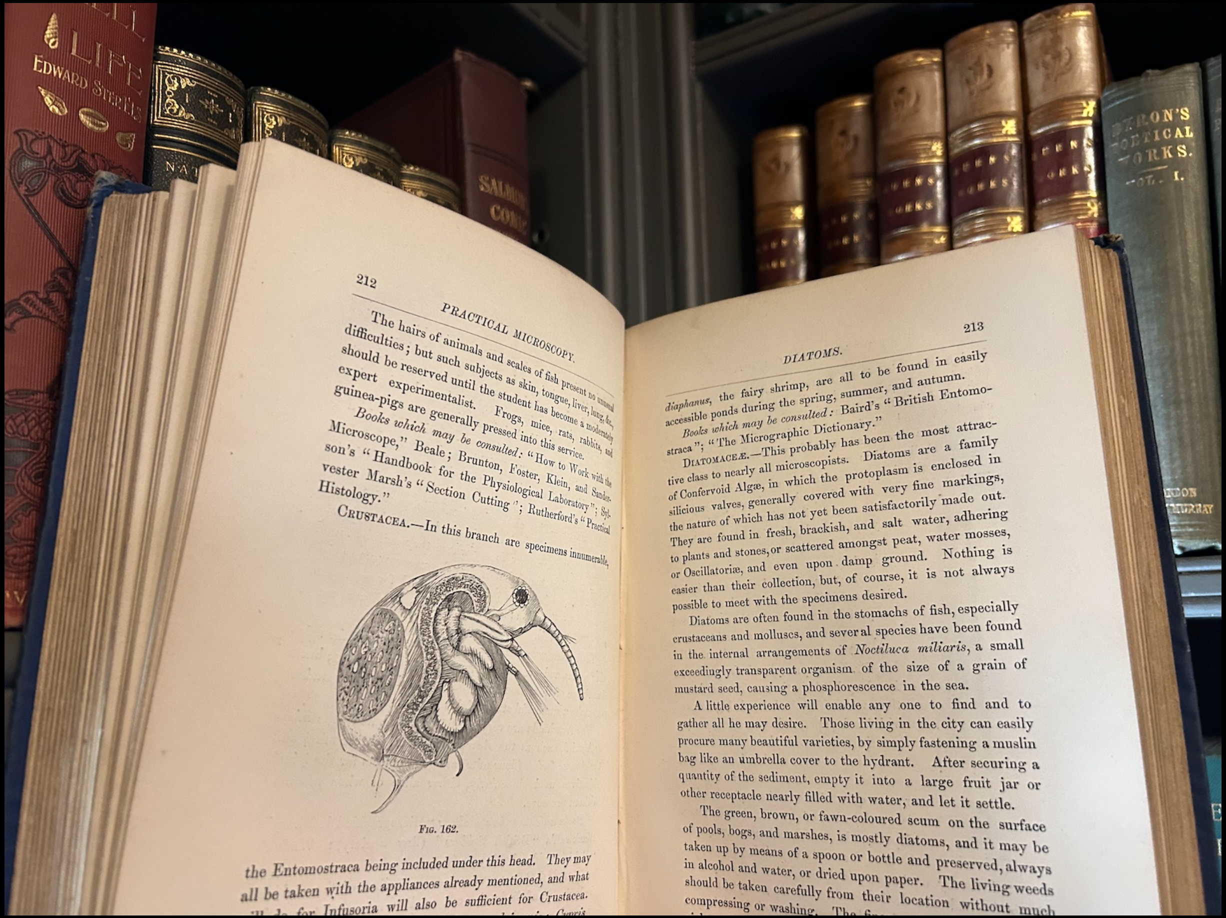

Slammer spreads rapidly. Infected servers fired out UDP packets as fast as possible
When a packet hit a vulnerable device, it was immediately infected, and would also start firing out packets.

Explaining Malware via Malmons


The entire worm was only 376 bytes, and fits inside a single packet.
376 bytes
This small size allowed it to propagate extremely fast.

By Lena aka LambdaMamba

Borrowing Old Book Styles



212 PRACTICAL MICROSCOPY.

The hairs of animals and scales of fish present no unusual difficulties; but such subjects as skin, tongue, liver, lung, &c., should be reserved until the student has become a moderately expert experimentalist. Frogs, mice, rats, rabbits, and guinea-pigs are generally pressed into this service.

Books which may be consulted: "How to Work with the Microscope," Beale; Brunton, Foster, Klein, and Sanderson's "Handbook for the Physiological Laboratory"; Sylvester Marsh's "Section Cutting"; Rutherford's "Practical Histology."

CRUSTACEA.—In this branch are specimens innumerable,

FIG. 162.

the Entomostraca being included under this head. They may all be taken with the appliances already mentioned, and what will do for Infusoria will also be sufficient for Crustacea. *Cypris*

DIATOMS. 213

diaphanus, the fairy shrimp, are all to be found in easily accessible ponds during the spring, summer, and autumn.

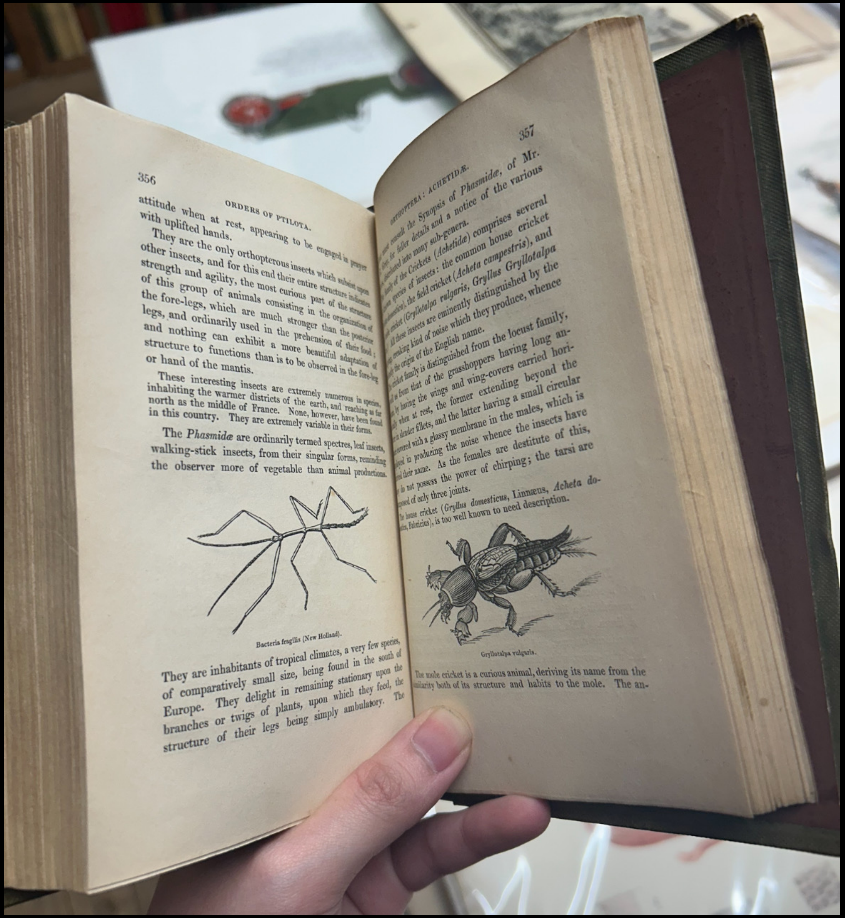
Books which may be consulted: Baird's "British Entomostraca"; "The Micrographic Dictionary."

DIATOMACEÆ.—This probably has been the most attractive class to nearly all microscopists. Diatoms are a family of Confervoid Algæ, in which the protoplasm is enclosed in silicious valves, generally covered with very fine markings, the nature of which has not yet been satisfactorily made out. They are found in fresh, brackish, and salt water, adhering to plants and stones, or scattered amongst peat, water mosses, or Oscillatoriæ, and even upon damp ground. Nothing is easier than their collection, but, of course, it is not always possible to meet with the specimens desired.

Diatoms are often found in the stomachs of fish, especially crustaceans and molluscs, and several species have been found in the internal arrangements of *Noctiluca miliaris*, a small exceedingly transparent organism of the size of a grain of mustard seed, causing a phosphorescence in the sea.

A little experience will enable any one to find and to gather all he may desire. Those living in the city can easily procure many beautiful varieties, by simply fastening a muslin bag like an umbrella cover to the hydrant. After securing a quantity of the sediment, empty it into a large fruit jar or other receptacle nearly filled with water, and let it settle.

The green, brown, or fawn-coloured scum on the surface of pools, bogs, and marshes, is mostly diatoms, and it may be taken up by means of a spoon or bottle and preserved, always in alcohol and water, or dried upon paper. The living weeds should be taken carefully from their location without much compressing or washing. The



356 ORDERS OF PTILOTA.

attitude when at rest, appearing to be engaged in prayer with uplifted hands.

They are the only orthopterous insects which subsist upon other insects, and for this end their entire structure indicates strength and agility, the most curious part of the structure of this group of animals consisting in the organization of the fore-legs, which are much stronger than the posterior legs, and ordinarily used in the prehension of their food; and nothing can exhibit a more beautiful adaptation of structure to functions than is to be observed in the fore-leg or hand of the mantis.

These interesting insects are extremely numerous in species, inhabiting the warmer districts of the earth, and reaching as far north as the middle of France. None, however, have been found in this country. They are extremely variable in their forms.

The *Phasmidæ* are ordinarily termed spectres, leaf insects, walking-stick insects, from their singular forms, reminding the observer more of vegetable than animal productions.

Bacteria fragilis (New Holland).

They are inhabitants of tropical climates, a very few species, of comparatively small size, being found in the south of Europe. They delight in remaining stationary upon the branches or twigs of plants, upon which they feed, the structure of their legs being simply ambulatory. The

ORTHOPTERA: ACHETIDÆ. 357

must consult the Synopsis of *Phasmidæ*, of Mr. Gray, for fuller details and a notice of the various distributed into many sub-genera.

family of the Crickets (*Achetidæ*) comprises several own species of insects: the common house cricket domestica), the field cricket (*Acheta campestris*), and mole cricket (*Gryllotalpa vulgaris*, *Gryllus Gryllotalpa*

All these insects are eminently distinguished by the creaking kind of noise which they produce, whence the origin of the English name.

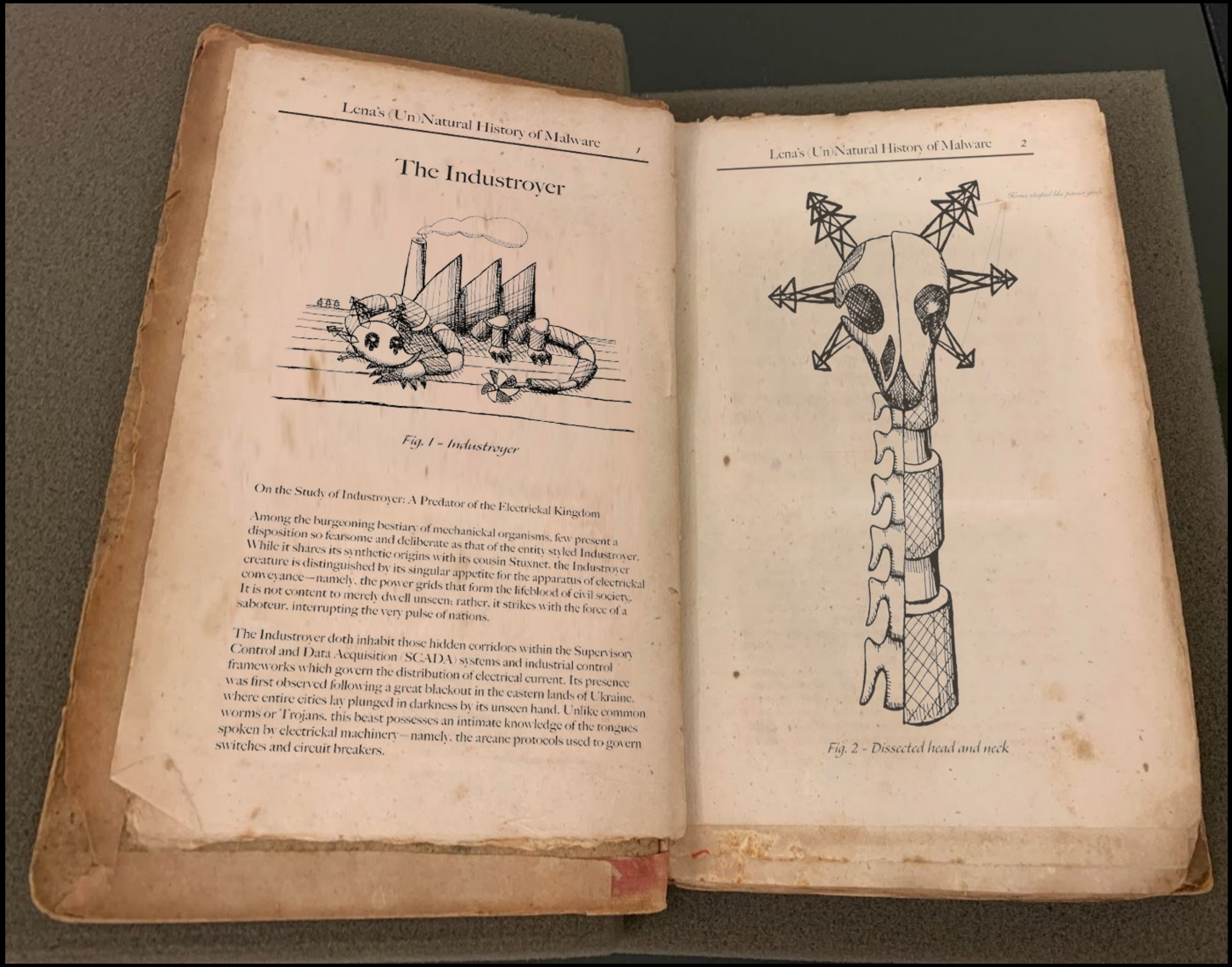
cricket family is distinguished from the locust family, as from that of the grasshoppers having long an- by having the wings and wing-covers carried hori- when at rest, the former extending beyond the in slender fillets, and the latter having a small circular covered with a glassy membrane in the males, which is used in producing the noise whence the insects have their name. As the females are destitute of this, do not possess the power of chirping; the tarsi are posed of only three joints.

The house cricket (*Gryllus domesticus*, Linnæus, *Acheta domestica*, Fabricius), is too well known to need description.

Gryllotalpa vulgaris.

The mole cricket is a curious animal, deriving its name from the similarity both of its structure and habits to the mole. The an-

“The (Un)Natural History of Malware”



Lena's (Un)Natural History of Malware 1

The Industroyer

Fig. 1 - Industroyer

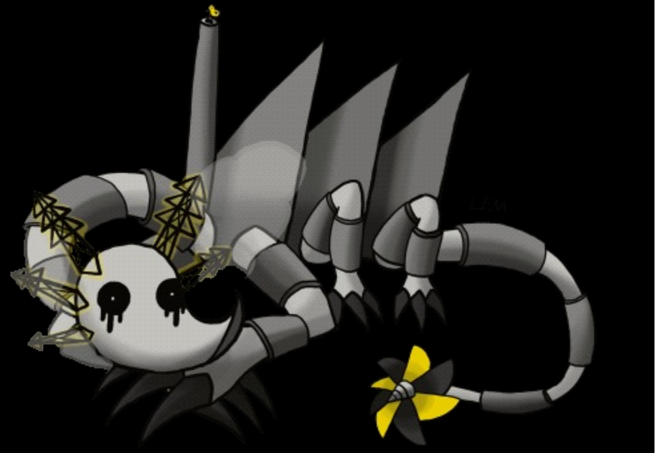
On the Study of Industroyer: A Predator of the Electrickal Kingdom

Among the burgeoning bestiary of mechanickal organisms, few present a disposition so fearsome and deliberate as that of the entity styled Industroyer. While it shares its synthetic origins with its cousin Stuxnet, the Industroyer creature is distinguished by its singular appetite for the apparatus of electrickal conveyance—namely, the power grids that form the lifeblood of civil society. It is not content to merely dwell unseen; rather, it strikes with the force of a saboteur, interrupting the very pulse of nations.

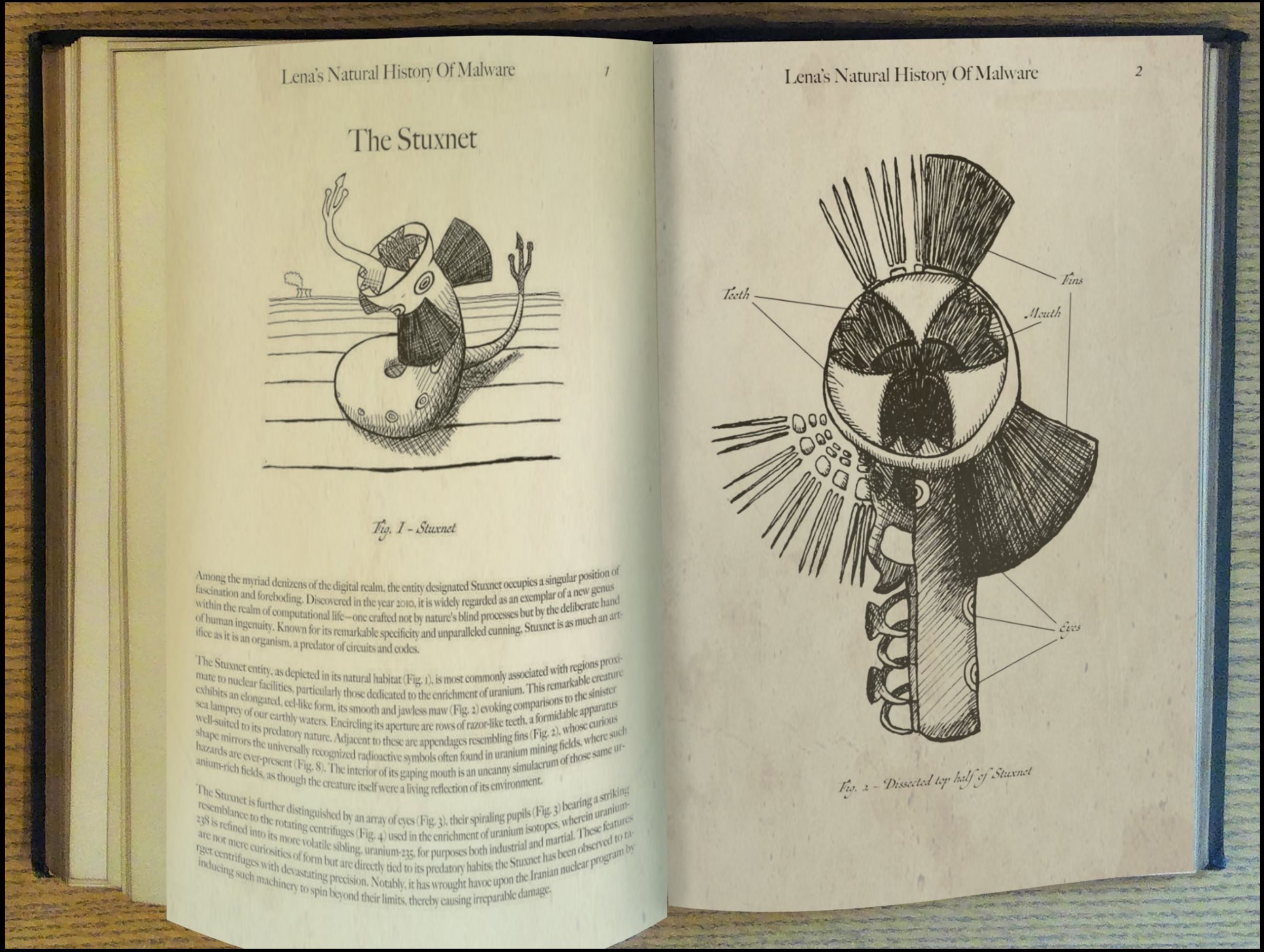
The Industroyer doth inhabit those hidden corridors within the Supervisory Control and Data Acquisition (SCADA) systems and industrial control frameworks which govern the distribution of electrical current. Its presence was first observed following a great blackout in the eastern lands of Ukraine, where entire cities lay plunged in darkness by its unseen hand. Unlike common worms or Trojans, this beast possesses an intimate knowledge of the tongues spoken by electrickal machinery—namely, the arcane protocols used to govern switches and circuit breakers.

Lena's (Un)Natural History of Malware 2

Fig. 2 - Dissected head and neck



“The (Un)Natural History of Malware”



Lena's Natural History Of Malware 1

The Stuxnet

Fig. 1 - Stuxnet

Among the myriad denizens of the digital realm, the entity designated Stuxnet occupies a singular position of fascination and foreboding. Discovered in the year 2010, it is widely regarded as an exemplar of a new genus within the realm of computational life—one crafted not by nature's blind processes but by the deliberate hand of human ingenuity. Known for its remarkable specificity and unparalleled cunning, Stuxnet is as much an artifice as it is an organism, a predator of circuits and codes.

The Stuxnet entity, as depicted in its natural habitat (Fig. 1), is most commonly associated with regions proximate to nuclear facilities, particularly those dedicated to the enrichment of uranium. This remarkable creature exhibits an elongated, eel-like form, its smooth and jawless maw (Fig. 2) evoking comparisons to the sinister sea lamprey of our earthly waters. Encircling its aperture are rows of razor-like teeth, a formidable apparatus well-suited to its predatory nature. Adjacent to these are appendages resembling fins (Fig. 2), whose curious shape mirrors the universally recognized radioactive symbols often found in uranium mining fields, where such hazards are ever-present (Fig. 8). The interior of its gaping mouth is an uncanny simulacrum of those same uranium-rich fields, as though the creature itself were a living reflection of its environment.

The Stuxnet is further distinguished by an array of eyes (Fig. 3), their spiraling pupils (Fig. 3) bearing a striking resemblance to the rotating centrifuges (Fig. 4) used in the enrichment of uranium isotopes, wherein uranium-238 is refined into its more volatile sibling, uranium-235, for purposes both industrial and martial. These features are not mere curiosities of form but are directly tied to its predatory habits; the Stuxnet has been observed to target centrifuges with devastating precision. Notably, it has wrought havoc upon the Iranian nuclear program by inducing such machinery to spin beyond their limits, thereby causing irreparable damage.

Lena's Natural History Of Malware 2

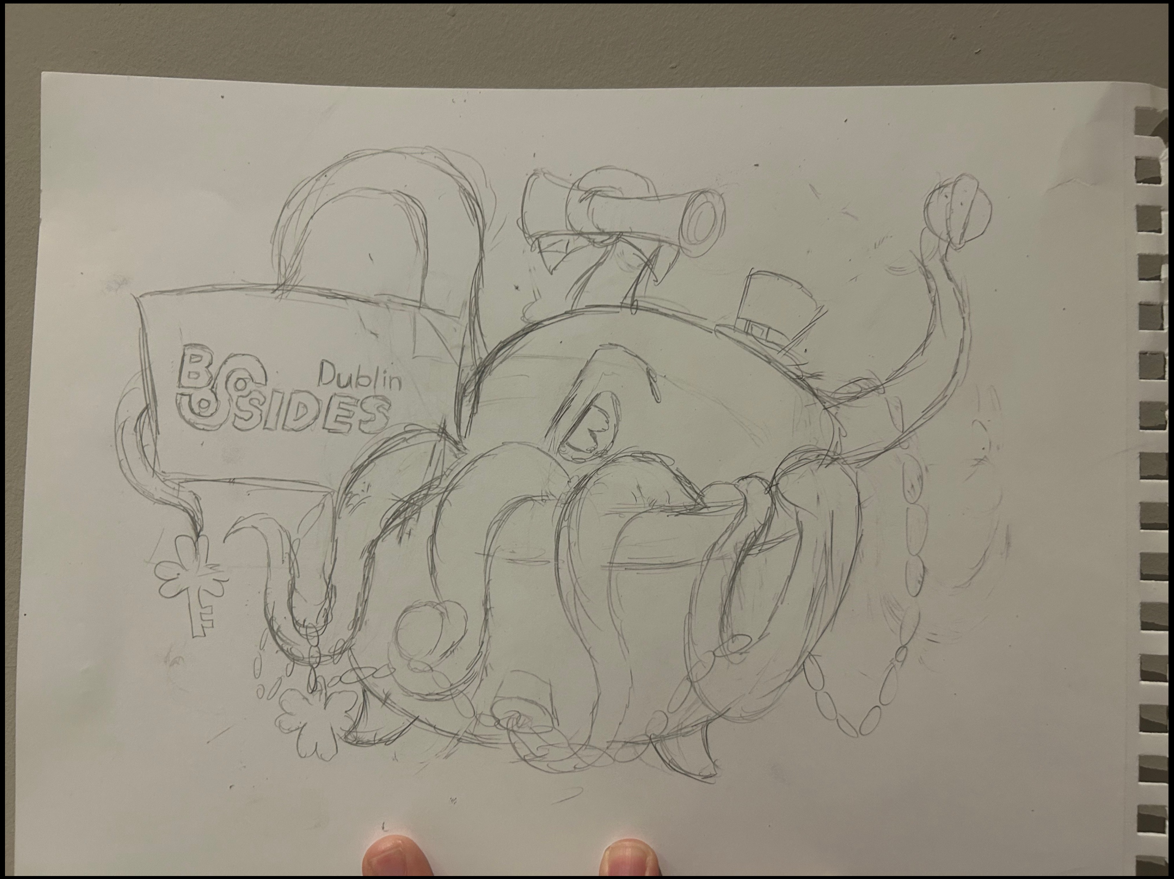
Fig. 2 - Dissected top half of Stuxnet

Malmons for BSides Dublin

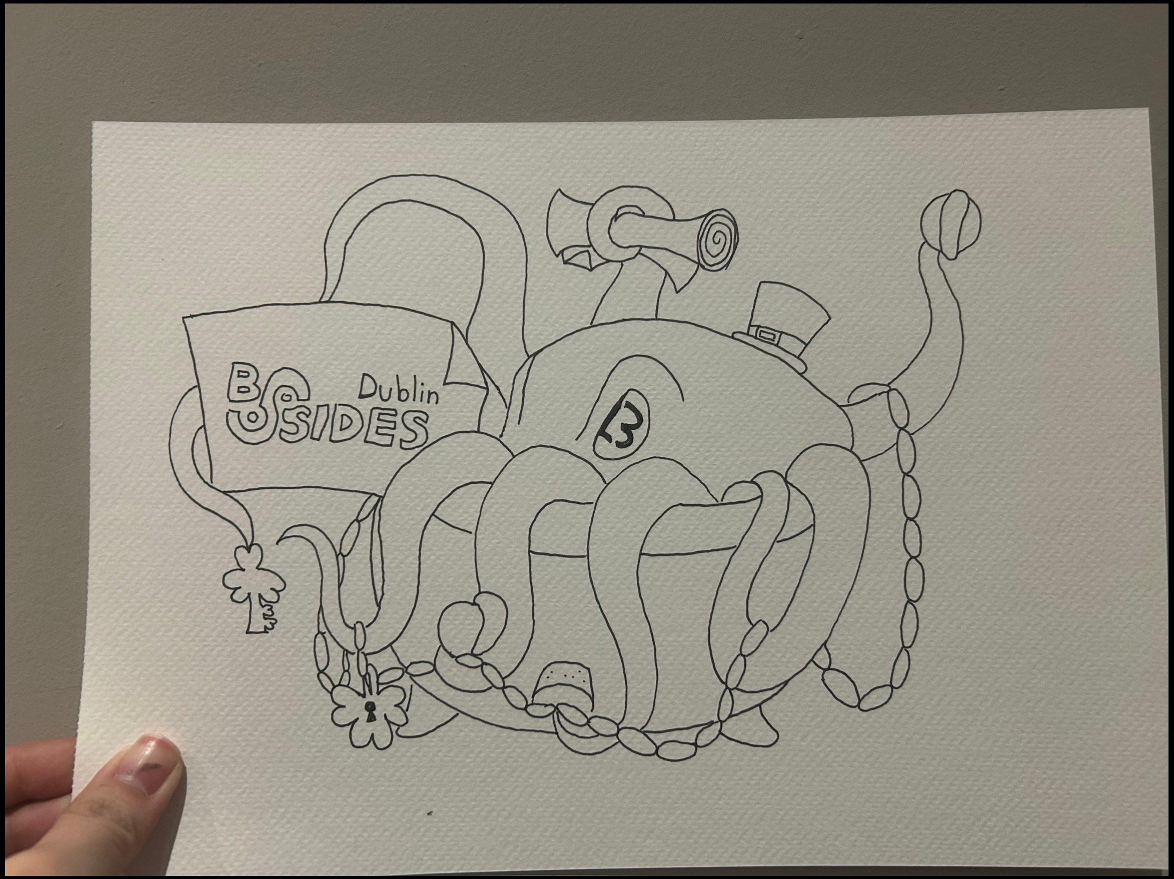
The LockBit Malmons
Full Video: www.youtube.com/shorts/H0lunRYNuc0

Animating the LockBit Malmons

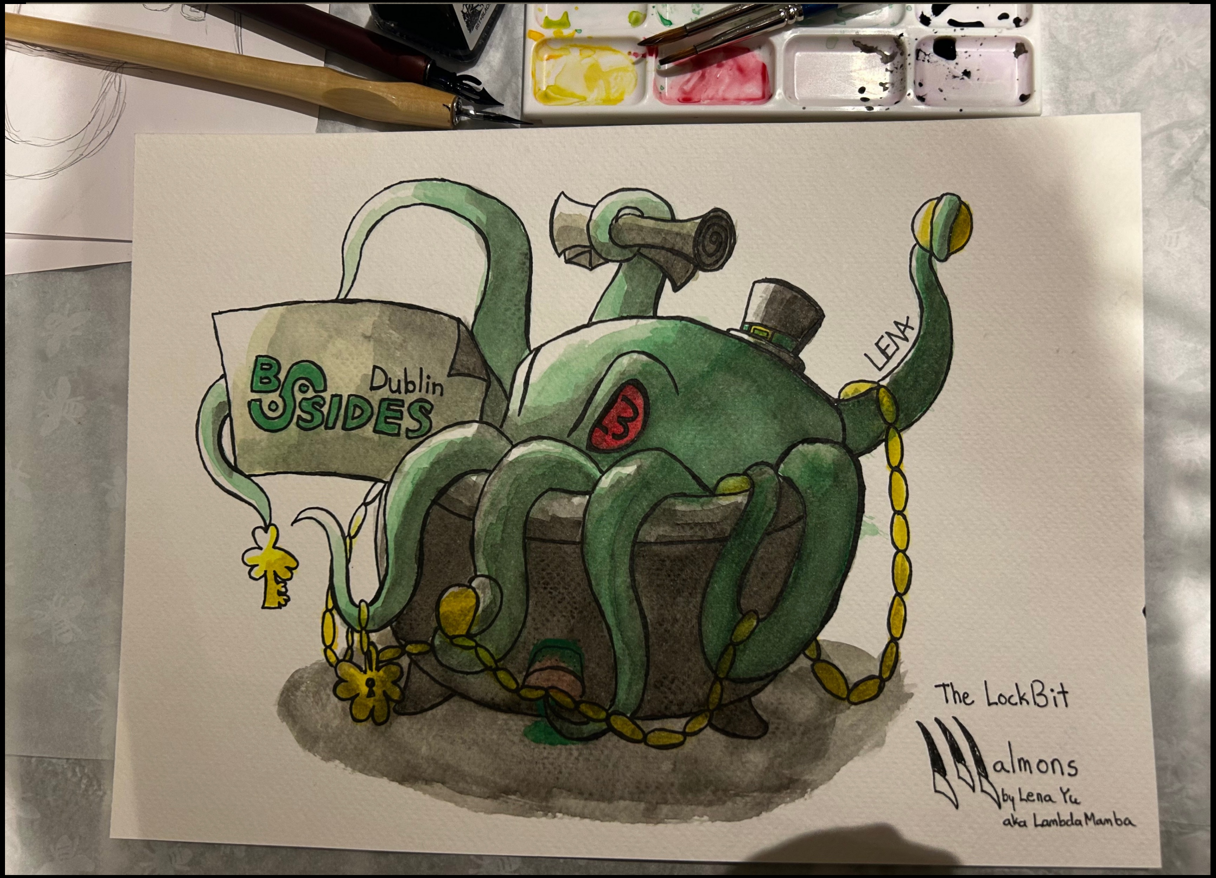
Painting LockBit Malmons



Painting LockBit Malmons

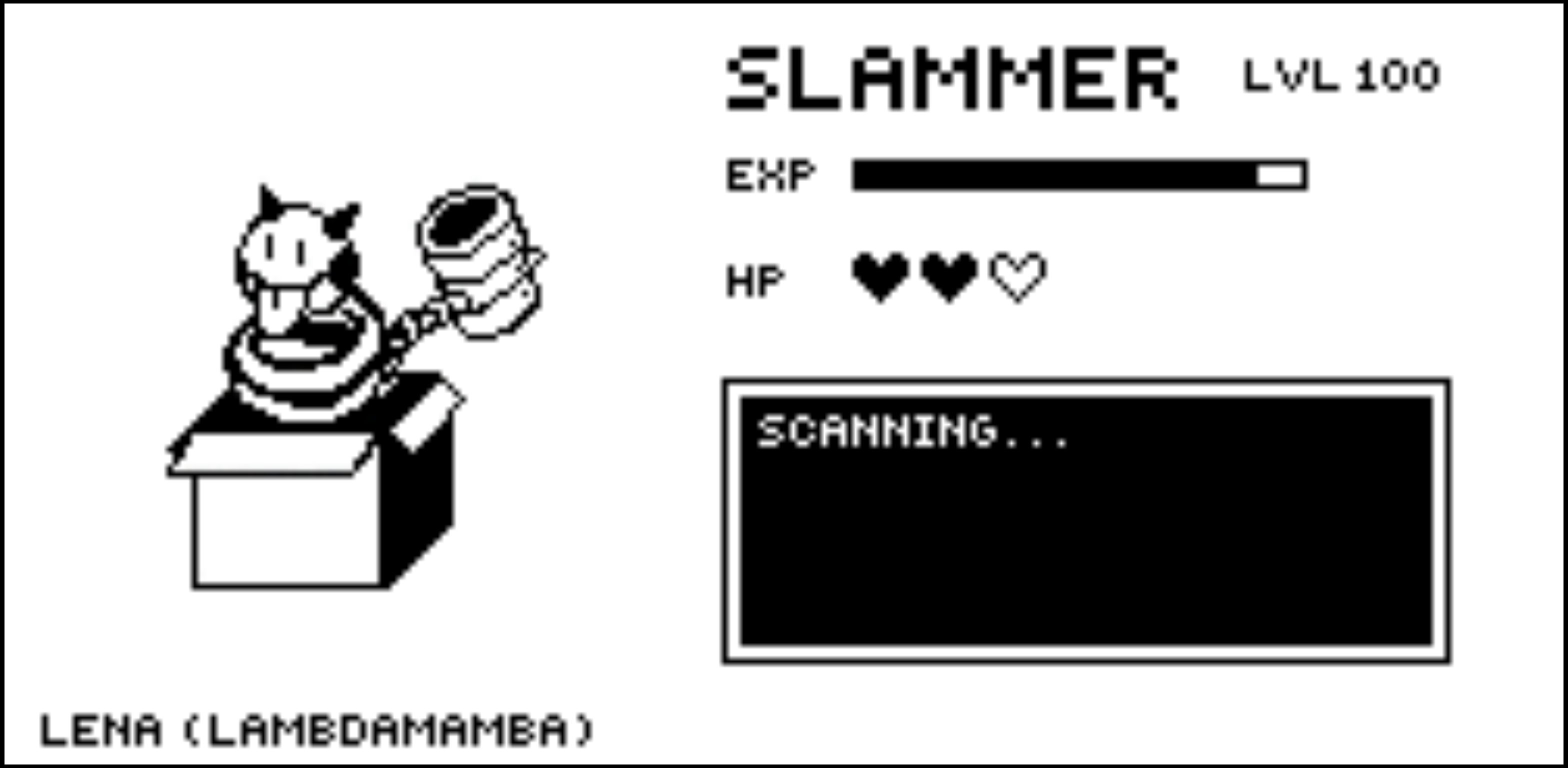


Painting LockBit Malmons



Exploring Dublin

Stay tuned for more Malmons...



Please support our non-profit World Cyber Health (WCH)!

- Our WCH projects:
  - Malware Village
    - MARC I, BOMBE, EMYAC
  - Malmons aka Malware Monsters
  - NO-HAVOC
    - Networked Online Helpline for All Victims Of Cybercrime
  - YEP-HAVOC
    - YEet Prompts at the Helpline for All Victims Of Cybercrime

malwarevillage.org

github.com/LambdaMamba/MalwareMonsters

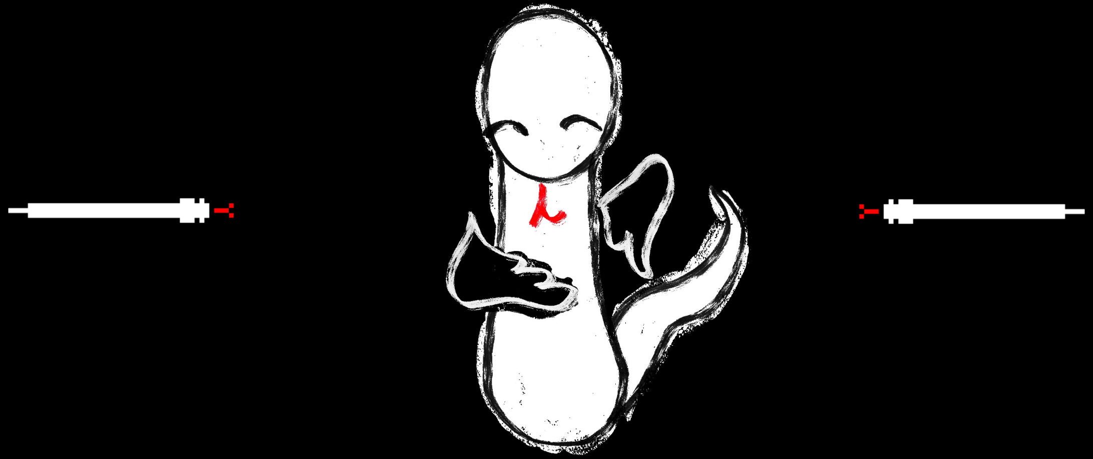
nohavoc.now

Break systems, but not promises!

(Question everything, stay curious!)

Q&A

Website: LambdaMamba.com



Email: lena.yu@worldcyber.health

Twitter: @LambdaMamba

Linkedin: linkedin.com/in/lenaaaa/