EBINAR / WEBINAR / WEBINAR / WEBINAR / WEBINAR / WEBINAR / WEBINAR / WEBI

Ghosts in the Machine:

Detecting Threats in Your Cloud

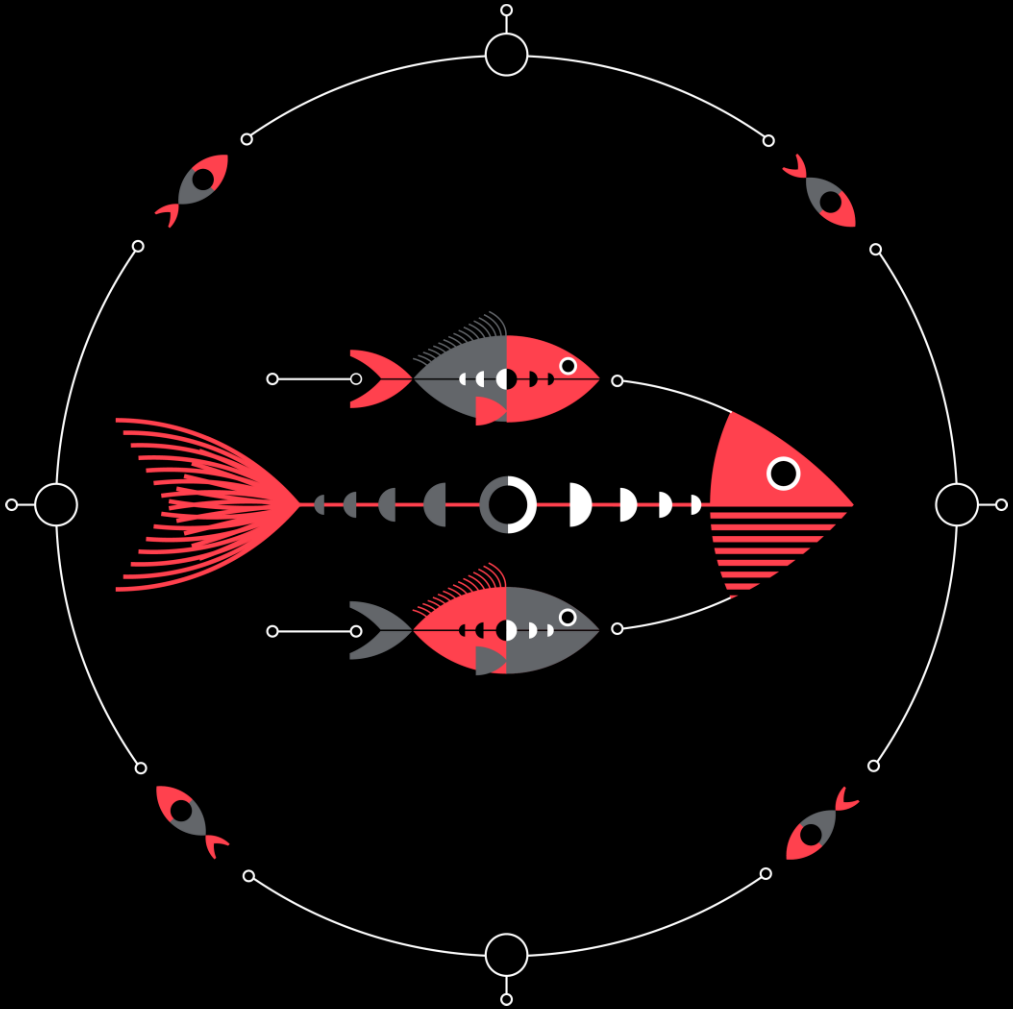
sysdig | SMASHING SECURITY

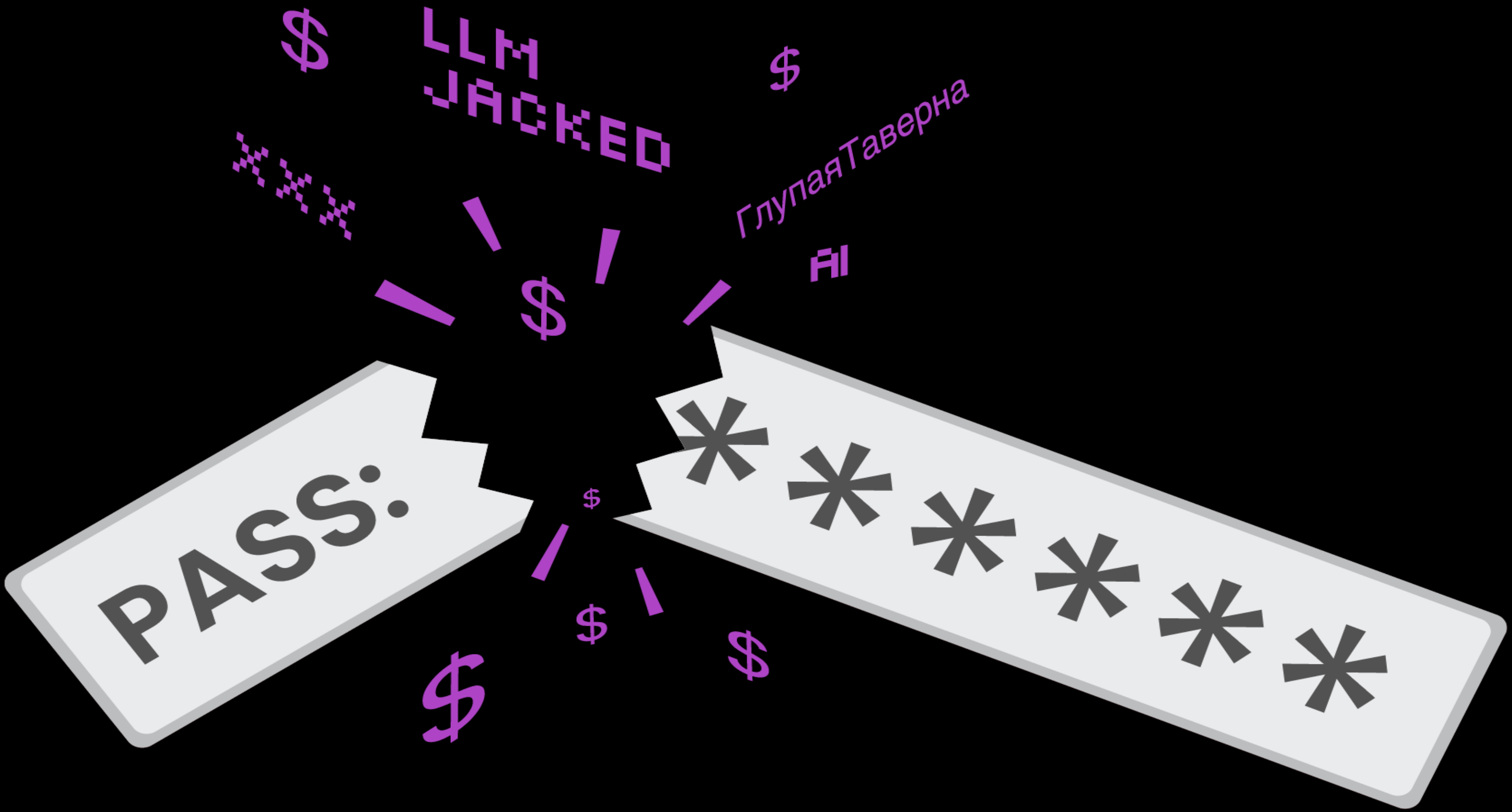
Graham Cluley

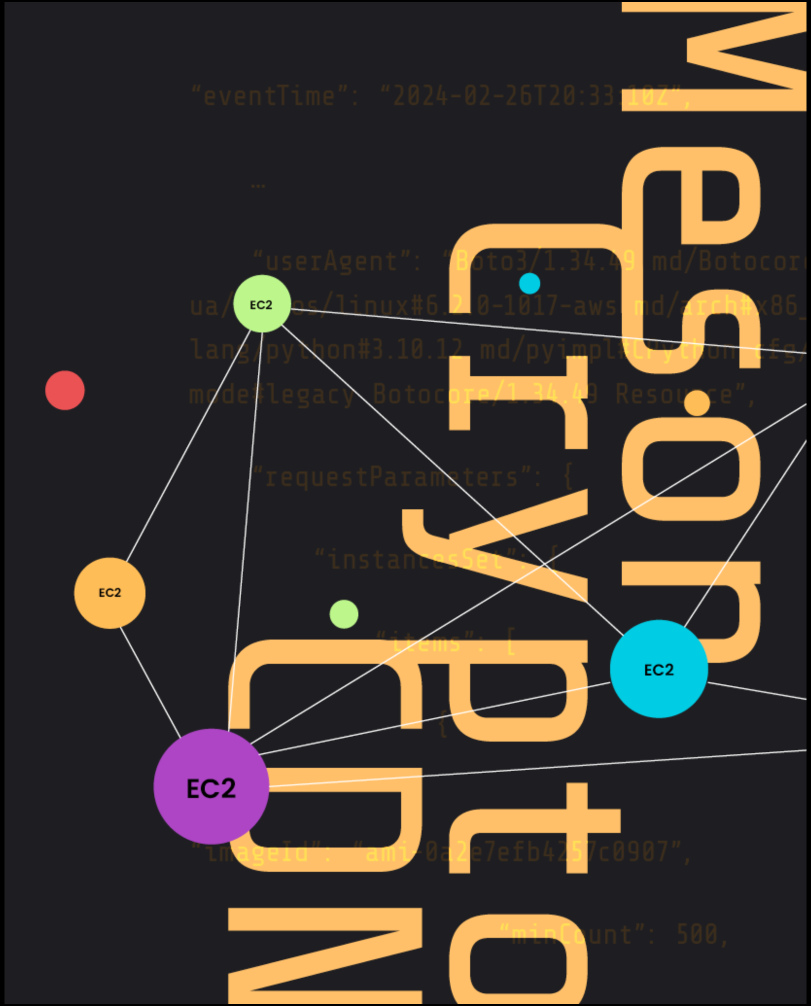
Podcast Host,
Smashing Security

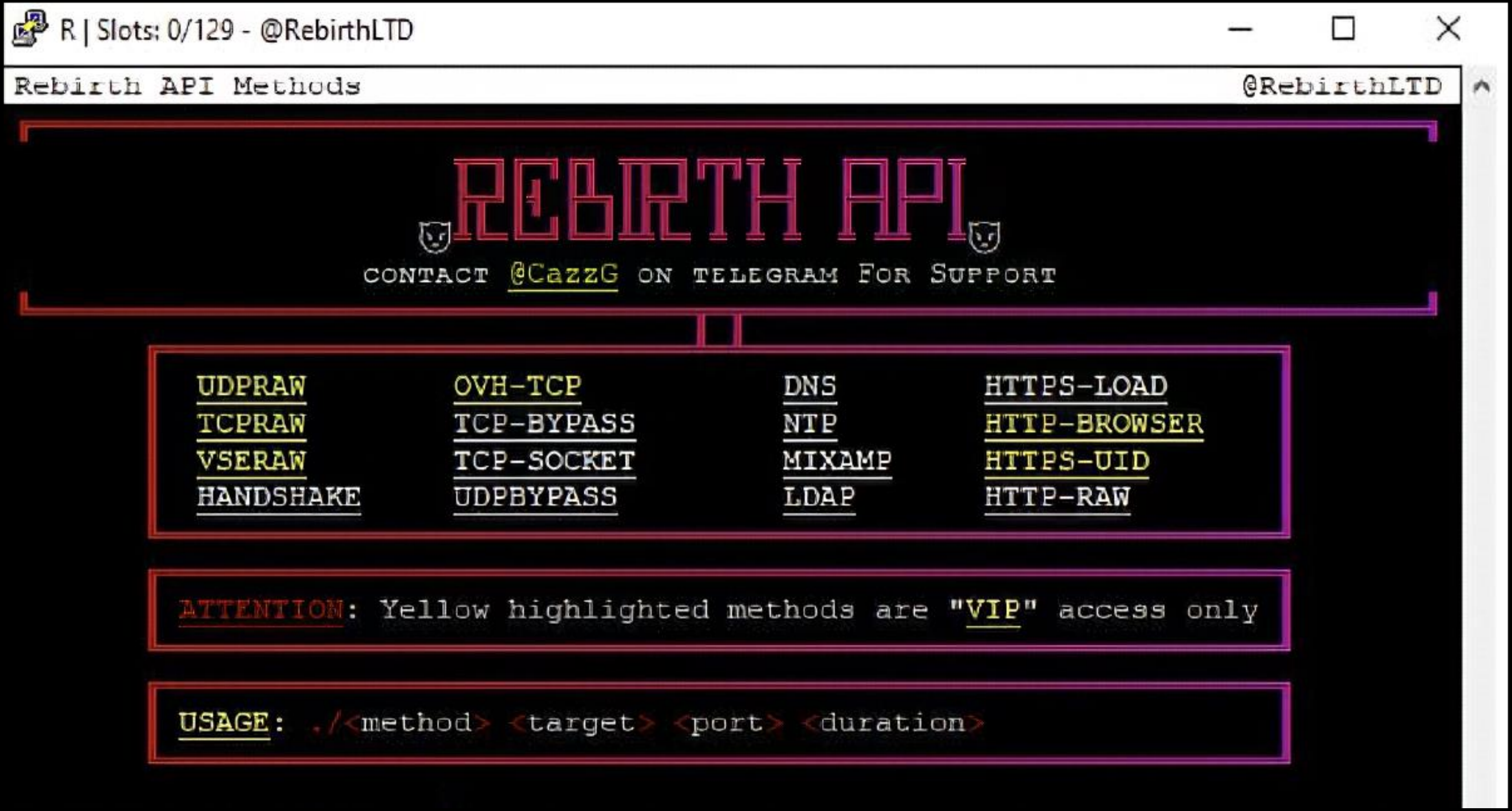
Crystal Morin

Cybersecurity
Strategist,
Sysdig




$
LLM
JACKED
$
XXX
ГлупаяТаверна
AI
$
PASS:
******
$
$
$
$


Meson
Crypto
CDN
EC2
EC2
EC2
EC2
EC2



R | Slots: 0/129 - @RebirthLTD

```
Rebirth API Methods                                              @RebirthLTD

                              REBIRTH API
                 CONTACT @CazzG ON TELEGRAM FOR SUPPORT

        UDPRAW        OVH-TCP          DNS        HTTPS-LOAD
        TCPRAW        TCP-BYPASS       NTP        HTTP-BROWSER
        VSERAW        TCP-SOCKET       MIXAMP     HTTPS-UID
        HANDSHAKE     UDPBYPASS        LDAP       HTTP-RAW

       ATTENTION: Yellow highlighted methods are "VIP" access only

       USAGE: ./<method> <target> <port> <duration>
```

> “Preventing attacks is **simply insufficient** as attackers’ means of defense evasion continue to mature.
>
> - Sysdig Threat Research Team

NEW

<> 2024

Global Threat

Year-in-Review

sysdig

Predictions:

1 SCALABILITY

Due to the ease of scaling in cloud environments, the rate of DDoS attacks will increase in 2025. Denial of service causes mass panic at an enterprise scale and can divert eyes while attackers go deeper.

2 ATTACK SURFACE

The attack surface will continue to grow over the next year, especially with the use of LLMs in every sector. Data that was once compartmentalized will continue to be centralized and fed into LLMs in the hopes of higher productivity. Inadvertently, by pushing massive amounts of data into LLMs, we are, in some cases, creating a new concentration risk and increasing the attack surface and opportunity for attackers.

3 AUTOMATION

The rise of LLMs will contribute to the success of attacks. Attackers will use audio and visual clones to successfully target MFA in 2025. On the other hand, we expect an increase in prompt engineering attacks as attackers continue to get the lay of the land and understand the inner workings of LLMs.

4 COST

We expect the enterprise victim cost of attacks to increase. **According to IBM**, the average cost of a breach in 2024 is $4.68M. However, for public cloud breaches, that figure increases to $5.17M. The US alone had over 1,500 **reported breaches** in the first half of 2024. Considering these projections, we expect that global cyberattacks in 2025 will cost over $100B.

Proactive security programs should always assume compromise. Cyberattacks will continue, likely at a greater frequency, and preventing attacks is simply insufficient as attackers' means of defense evasion continue to mature. Powerful real-time detection and rapid response actions help defenders identify and stop the unknown. Resilience following a cyberattack will keep the business moving.

Cloud attacks will continue to become faster, more sophisticated, and more expensive year over year.

Questions?

sysdig

SECURE
EVERY
SECOND