Cybersecurity Im Zeitalter von Artificial Intelligence

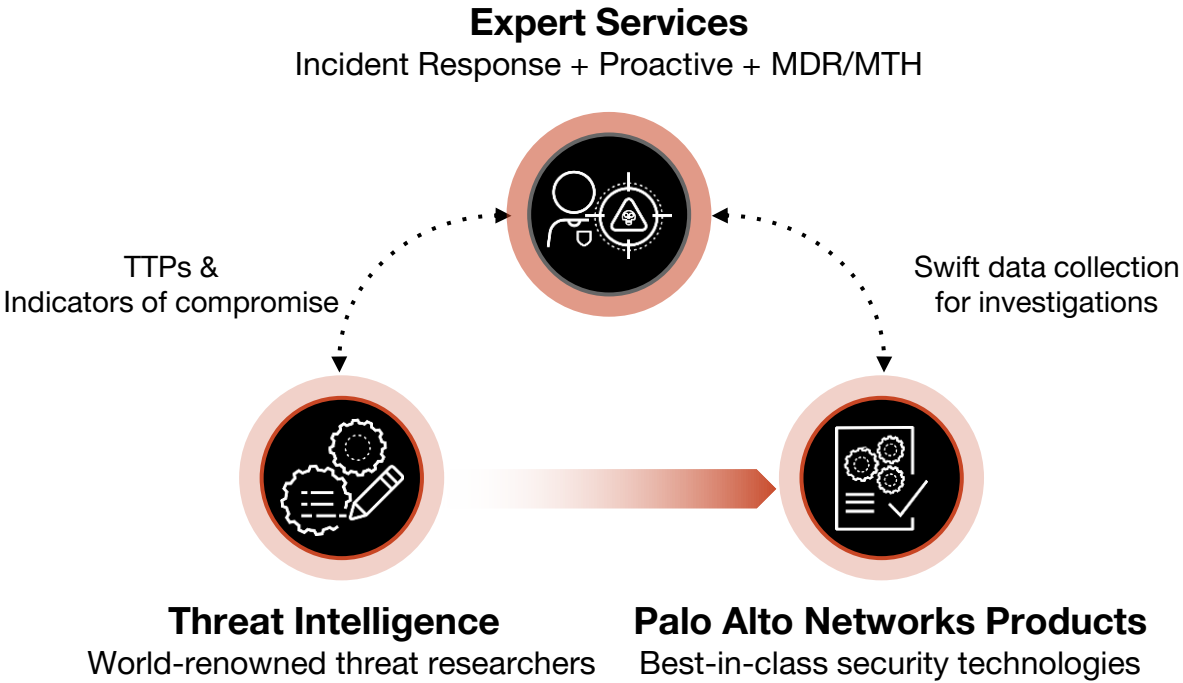
Sind die nützlichen Tools die Gefahr von morgen?

André Reichow-Prehn, Managing Partner Unit 42

June 2024

What Is Unit 42?

Unit 42 Threat Intelligence & Services



Current Threat Landscape

2024 Unit 42 Incident Response Report – Speed Matters

Findings

- In 2021, the median time between compromise and exfiltration was 9 days
- In 2023, the median fell to 2 days

45% of the time, compromise-to-exfiltration happened in less than a day

Defenders must respond within hours.

2024 Unit 42 Incident Response Report – Software Vulnerabilities Still Matter

39% Exploitation of internet-facing vulnerabilities increased to 39% of initial access

- Related to several large automated intrusion campaigns
- Overtook the previous champ: stolen credentials and phishing

Continuously, quickly and comprehensively conduct attack surface management, reduction and patch hygiene.

2024 Unit 42 Incident Response Report – Threat Actors are Increasingly Sophisticated

Threat actors are more organized and specialized. They understand and use IT, cloud and security tools against their targets.

Defenders need to be as organized and automated as attackers, preferably more.

Both Cybercrime and Nation State Activity Impact Europe

PLAY Ransomware attacks on the rise January, 2024

Government agencies and other key industries targeted by Russia backed APT28. April, 2024

Funerals reportedly canceled due to ransomware attack on Austrian town. February, 2024

Ministry of Defence hack, suspected China May, 2024

US indicts Chinese threat group APT31 who targeted EU government entities March, 2024

Blackbasta steals data from Italian healthcare entity. April, 2024

Adversaries Are Creative: Fighting Ursa/APT28

CAR FOR SALE IN KYIV
THE PRICE IS REDUCED!!!

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

Very good condition, low fuel consumption

More high quality photos are here: https://t.ly/

Model	**BMW 5, 2.0 TDI (184 HP)**
Year	April 2011
Mileage	266,000 km
Engine	2.0 Diesel
Transmission	Mechanic
Colour	Black, black leather interior
Package	A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system.
Price	**7,500 Euros**
Custom	NOT CLEARED
Contact	

Observed Targets of Fighting Ursa CVE-2023-23397 Campaigns

Targeted Nations	Targeted Sectors

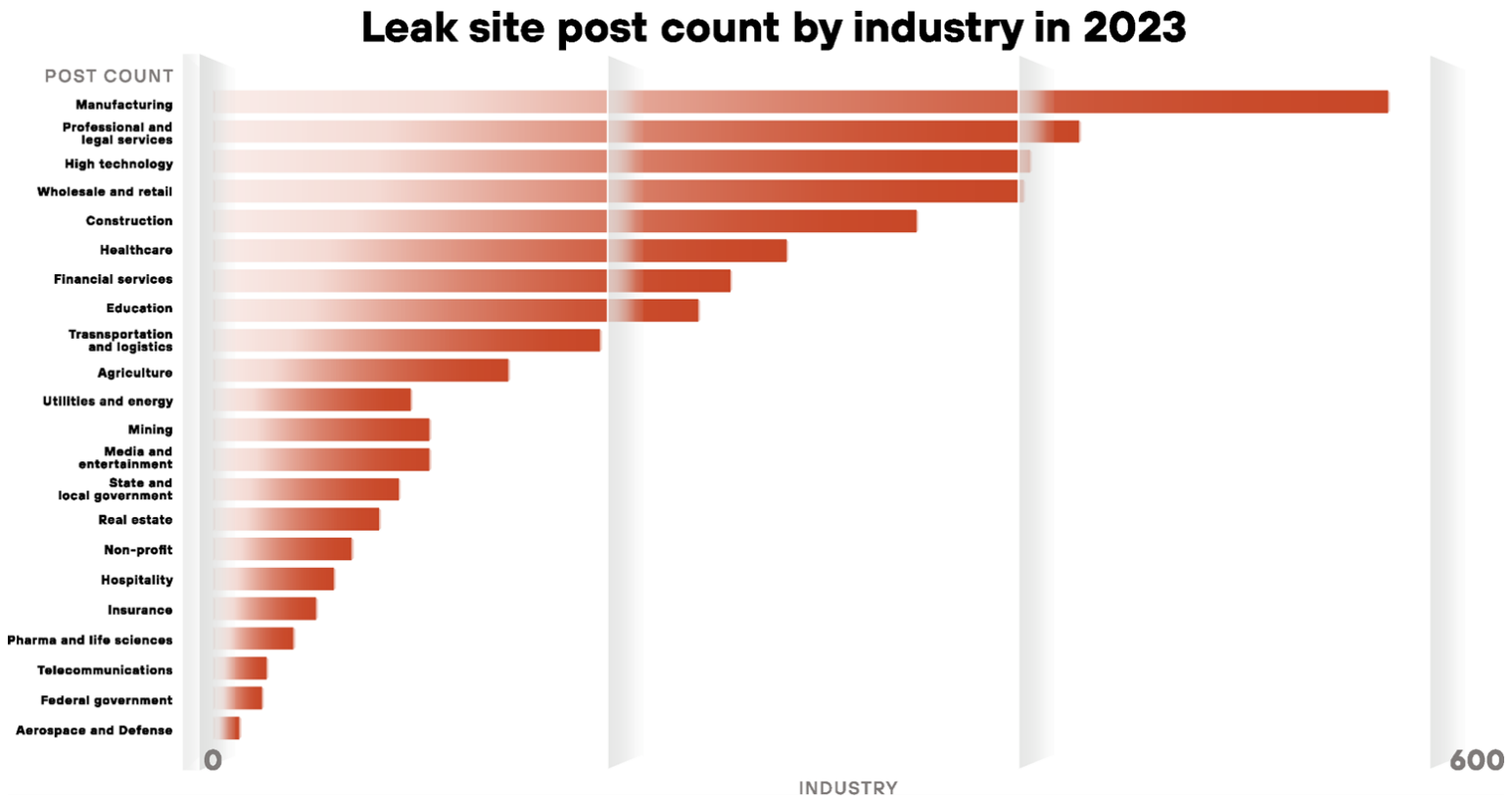
Bulgaria
Czechia
Italy
Jordan
Lithuania
Luxembourg
Montenegro
Poland
Romania
Slovakia
Türkiye
Ukraine
United Arab Emirates
United States
	• Government
	  ○ Ministry of Defense
	  ○ Armed Forces
	  ○ Ministry of Interior
	  ○ Ministry of Foreign Affairs
	  ○ Ministry of Economy
	  ○ State Migration Service
	  ○ Postal Service
	• Energy
	  ○ Petroleum
	  ○ Natural Gas
	  ○ Transit Pipeline
	  ○ Electrical (including hydroelectric)
	• Transportation
	  ○ Air Traffic Management
	  ○ Aviation Infrastructure Management
	  ○ Logistics Management
	• Telecommunications
	• Information Technology
	• Defense Industrial Base

Targeted International Organizations	
North Atlantic Treaty Organization, High Readiness Force Headquarters	

2024 Unit 42 Ransomware Retrospective

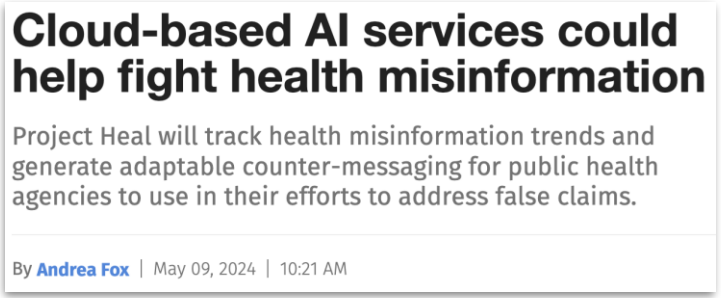
- 2023 saw a 49% increase in victims reported by ransomware leak sites, with a total of 3,998 posts from various ransomware groups.
- Zero-day exploits for high-profile vulnerabilities drove spikes in ransomware infections by groups like CL0P, LockBit and ALPHV (BlackCat).
- Law enforcement agencies intensified their focus on ransomware – led to the decline of groups like Hive and Ragnar Locker, and the near-collapse of ALPHV (BlackCat).
- LockBit ransomware remained the most active group – for two years in a row.
  - However Lockbit is now also impacted by law enforcement actions.
- **Manufacturing was the most affected industry**

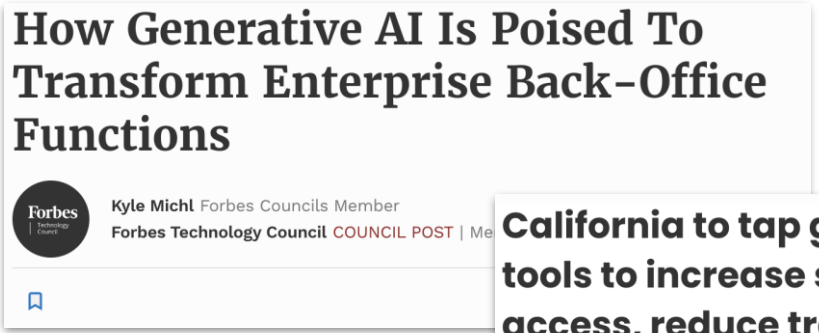
Ransomware By the Numbers

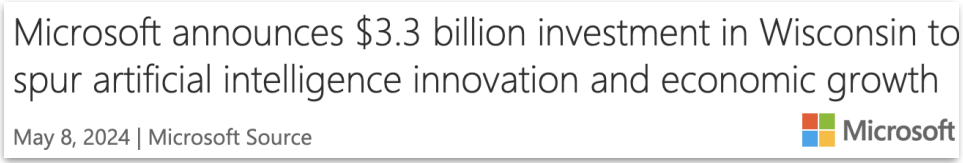


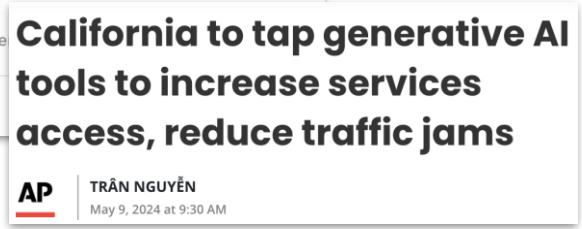
AI in the Spotlight

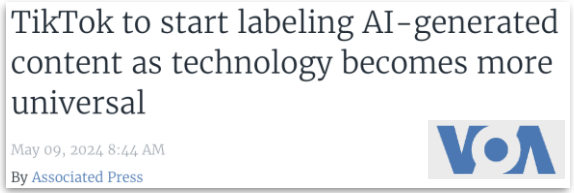
The world is excited about AI …











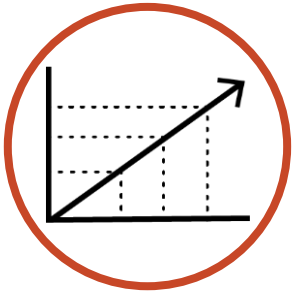
Why Attackers Are Also Excited About AI

Execute hundreds of simultaneous attacks

Solarwinds with directed vs. random network targeting

Exploit several vulnerabilities

Accelerated identification of external exposures and scale the attacks



Scale Attacks

Why Attackers Are Also Excited About AI

A whole new category of vulnerabilities comes with AI

Whole new set of LLM-based issues–new “OWASP AI Top Ten LLM”

Impersonation

Inexpensive and easy to create deepfakes for calls or videos

New Vectors

Why Attackers Are Also Excited About AI

Easier phishing

Tailored and fewer grammar mistakes

Automated malware development

Using AI as an assistant to develop malware or iterate through new feature options rapidly

Accelerate Attacks

However…

1. The current state of “AI” being leveraged across the threat landscape is largely exploratory at this point in time.
    a. Observations have noted that generative AI and Large Language Models (LLMs) could serve as valuable assistants but are **not presently in widespread use for the mass production of malware or the execution of large-scale attacks**
2. ***GPT/LLMs does not autonomously generate intricate malware***. Without proper guidance, it cannot execute complex operations.
    a. Nonetheless, it proves highly valuable as a reliable co-pilot. A good example of a co-pilot in this instance would be to use GPT to review code to encode some malicious code.
3. Evidence of experimentation and discussion of AI and LLM topics is rampant, with ***threat actors often discussing potential ways to leverage AI to bypass anti-virus engines***, or attackers **leveraging generative AI to perform reconnaissance on prospective victims**

How Adversaries are Currently Using AI…

1. Most jailbroken LLM services primarily function as intermediary wrappers, often redirecting requests to either the genuine ChatGPT or Google BARD tools
    a. Common jailbreak which involves tricking the AI into playing a character, thus unlocking it’s knowledge in a roundabout way
2. Criminals have little incentive to create a distinct language model like ChatGPT, as ChatGPT itself serves their purposes effectively.
3. It's evident that criminals are employing AI in much the same manner as the general population.
4. Most prominent in the wild usage includes
    a. Enhancing spear phishing message text
    b. Performing reconnaissance on prospective victims
    c. Attempting to generate code that bypasses AV, etc

Thank You

paloaltonetworks.com