CSO COUNCIL

SPOŁECZNOŚĆ SZEFÓW
BEZPIECZEŃSTWA
I CYBERBEZPIECZEŃSTWA

04/04/23

Cyberekspres

PIOTR MOROZ

home.mycloud.com

503 Service Temporarily Unavailable

Świeżynka

- [WD potwierdził włamanie do swojej sieci.]
- Hackerzy uzyskali dostęp do systemów firmy.
- W związku z incydentem niedostępna m.in. usługa MyCloud

QuokkÅMocha @MochaQuokka · 19 g.
My My Cloud Home drive is down because **@westerndigital** got hacked, and the daft way their file system works, where you can only really access data via their apps, means everything is now unavailable, even though it's a physical drive.
4 4 5 505

Thorsten Ising @ThorstenIsing · 37 min
Hello, **@westerndigital** ... another day without myCloud... when do you plan to get the mycloud logins working again? It's a bit annoying like this.
2 71

Alejandro Lorente @jalc_79 · 2 kwi
The login service for **WD** My **Cloud** Home is unavailable. Thank you @westerndigital for not letting me access my data that I have in the living room

Oczywistości

- Błąd w protokole WiFi ("Cisco also recommends implementing transport layer security to encrypt data in transit whenever possible because it would render the acquired data unusable by the attacker„)
- BingBang: błędy w konfiguracji Azure Active Directory (multi-tenant) pozwoliły manipulować wynikami wyszukiwarki AAD Bing.com i dostęp do wielu aplikacji samego Microsoft …
- Vulkan files – wyciek danych z rosyjskiej firmy pracującej na rzecz rosyjskich służb i powiązanej z grupami APT Sandworm, Cozy Bear
- Można ustalić lokalizację operatora drona DJI na podstawie danych w komunikacji radiowej

Oczywistości

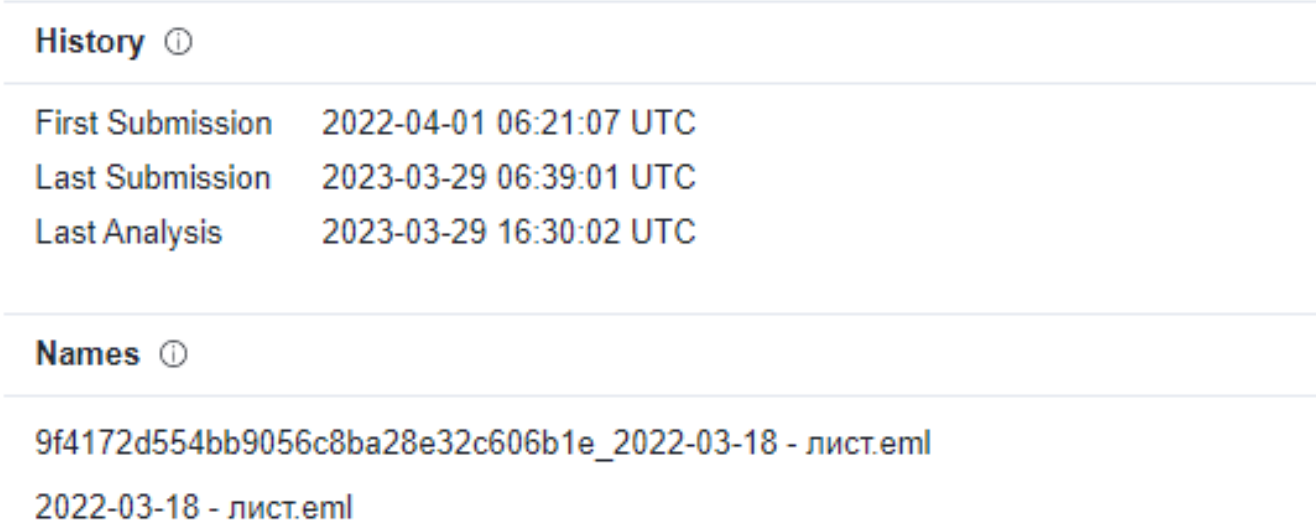
Trojan w (podpisanej) aplikacji desktopowej VoIP firmy **3CX** (ponad 600 tys. firm użytkujących w tym American Express, Coca-Cola, McDonald's, BMW, Honda, Air France, Toyota, Mercedes-Benz, IKEA)
- kolejny atak w łańcuchu dostaw
- wykorzystuje m.in.

pewną lukę z 2013 roku CVE-2013-3900 i na dodatek:

Oczywistości

Podatność CVE-2023-23397 (14 marca 2023) pozwalająca uzyskać NTLM Hash bez interakcji użytkownika

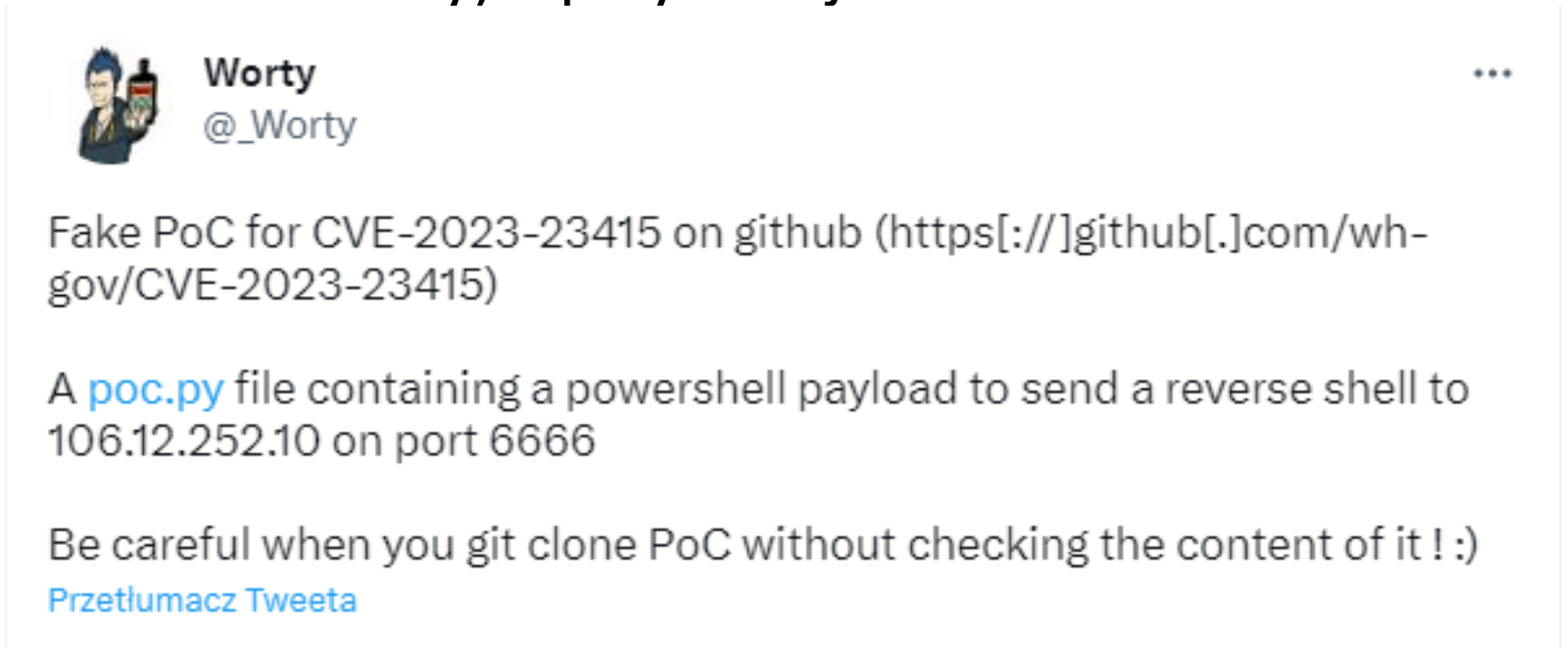
- Aktywnie wykorzystywana przynajmniej od 2022 roku także przeciwko polskimi użytkownikom
- email wykorzystujący podatność pojawił się na VT rok wcześniej:



Attack IP	IP Properties	Equipment Information	Related time	Victims
5.199.162[.]13:443 sourcescdn.net	Lithuania	VPS	Email sending time:2022-03-18 Sample upload time:2022-04-01	State Migration Service of Ukraine
77.243.181[.]10:443 globalnewsnew.com	Germany	VPS	Before 2022-04-01	
45.138.87[.]250:443 ceriossl.info	Romania	VPS	Before 2022-04-01	
101.255.119[.]42	Indonesia	Ubiquiti-EdgeRouter	Email sending time:2022-04-14 Sample upload time:2022-04-14	Romanian Ministry of Foreign Affairs
213.32.252[.]221	Iraq	Ubiquiti-EdgeRouter	Email sending time:2022-09-29 Sample upload time:2022-09-29	Polish arms dealer PIT-RADWAR SA (e-mail sent from Coastal Bank, an Indian bank)
168.205.200[.]55	Brazil	Ubiquiti-EdgeRouter		
185.132.17[.]160	Sweden	Ubiquiti-EdgeRouter		
69.162.253[.]21	United States	Ubiquiti-EdgeRouter		
113.160.234[.]229	Vietnam	Ubiquiti-EdgeRouter	Email sending time:2022-12-29 Sample upload time:2022-12-29	Turkish Defense Technology Company STM
181.209.99[.]204	Argentina	Ubiquiti-EdgeRouter		
82.196.113[.]102	Sweden	Ubiquiti-EdgeRouter		
85.195.206[.]7	Switzerland	Ubiquiti-EdgeRouter		
61.14.68[.]33	Singapore	Ubiquiti-EdgeRouter		

Oczywistości

- Podatność CVE-2023-23415 (Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability) a przy okazji:



Chińscy dostawcy na cenzurowanym?

- Stanowisko Rady do Spraw Cyfryzacji w sprawie zagrożeń ze strony Dostawców Wysokiego Ryzyka: *Zdaniem Rady powyższe kryteria eliminują chińskie firmy z kręgu dostawców kluczowych systemów ICT dla instytucji publicznych w Polsce*
- Tymczasem Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) korzysta z rozwiązań chińskich dostawców i być może inne państwowe instytucje również…

https://www.handelsblatt.com/politik/deutschland/it-infrastruktur-deutschlands-oberste-cybersicherheitsbehoerde-setzt-huawei-technik-ein/29074218.html

AI w natarciu

- Microsoft Security Copilot - AI w cybersecurity
- QRadar Advisor with Watson – 2017 rok …

Tymczasem:

Elon Musk i setki badaczy ostrzegają przed niekontrolowanym rozwojem sztucznej inteligencji

Magisterka łatwiejsza niż dotąd? Programy antyplagiatowe nie nadążają za AI

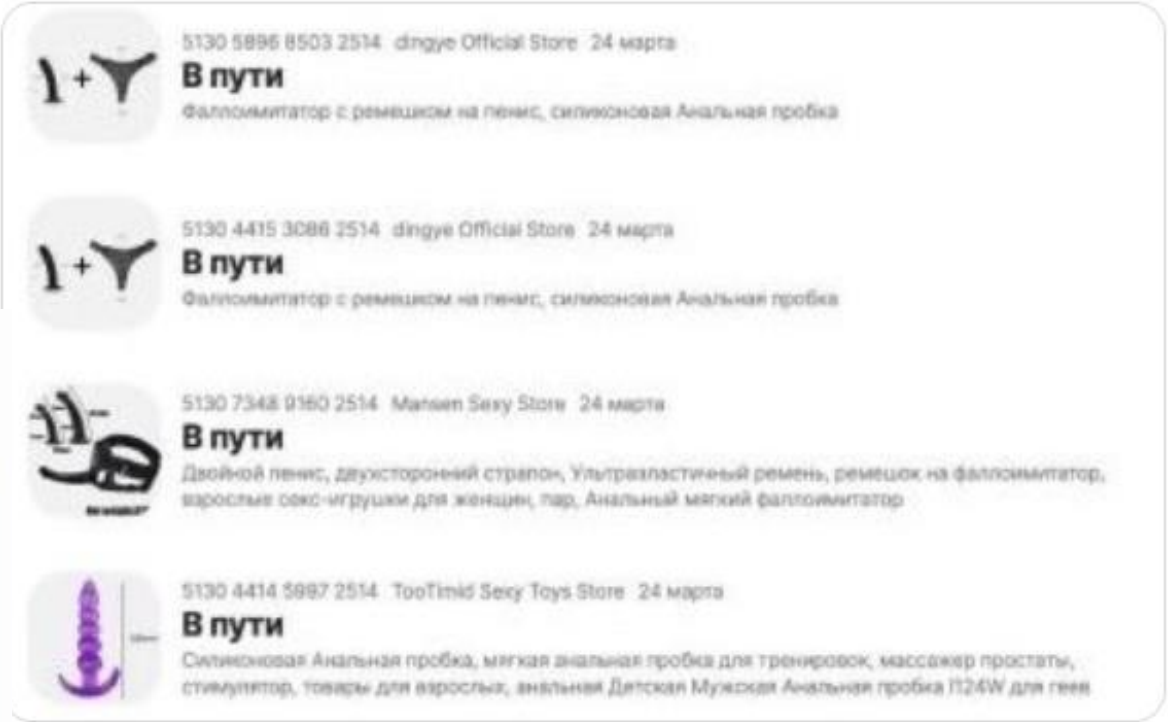
Italian privacy regulator bans ChatGPT

Calls have grown to suspend new releases of popular AI tool.

Mykhailo Lavrovskyi 
@Lavrovskyi

Ukrainians hacked an AliExpress account of a Russian “volunteer” who fundraiser money for the drones for 🇷🇺 army.

Instead of drones, he was delivered dildos worth 25,000 USD 😂



Alissa Pavia @AlissaPavia · Apr 1

The true **reason** why **Italy banned ChatGPT**