HACKING A BIZNIS

Pohľad do zákulisia organizovaného kyberzločinu

Ľubomír Kopáček – iseco s.r.o. – kopacek@iseco.sk

RANSOMWARE = SUPERÚSPEŠNÝ BIZNISMODEL

- Vo všeobecnosti nepripravené organizácie
- Naivita malých firiem
- Bezradnosť veľkých firiem
- Neadresná zodpovednosť

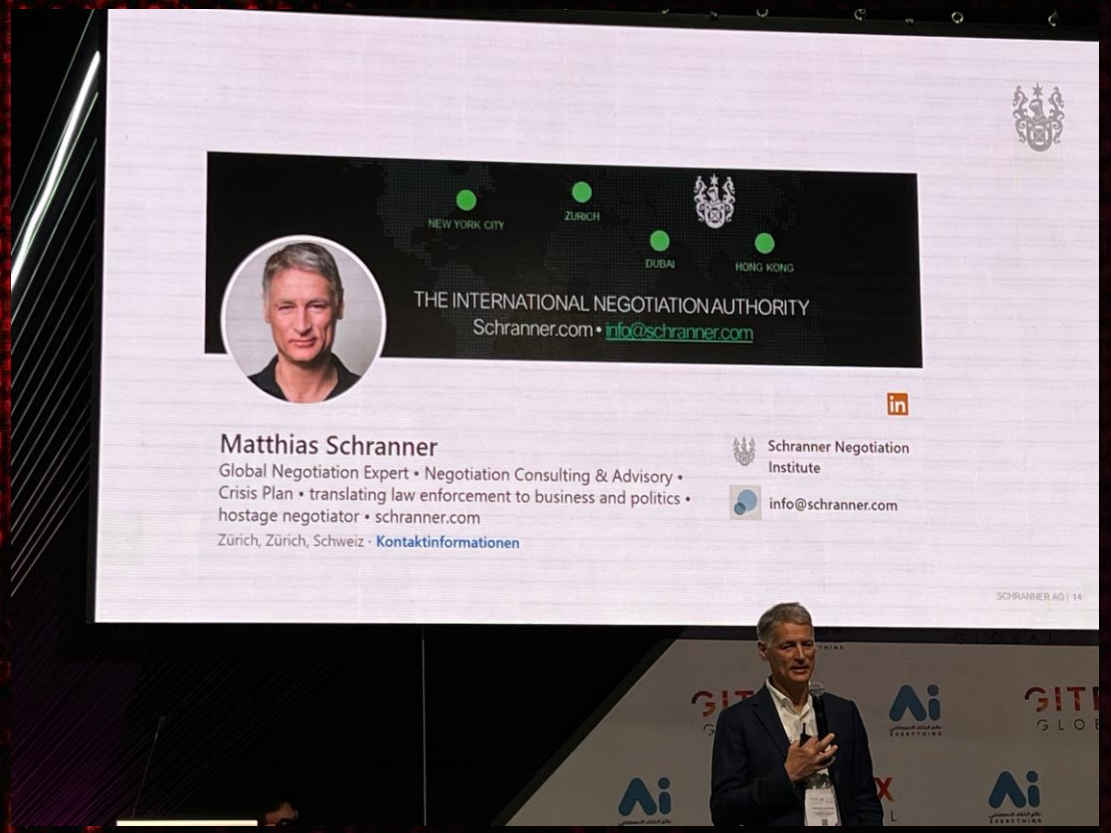
- Ransomware ako služba (RaaS)
- Plný servis a podpora pre technicky neskúsených útočníkov
- Nízke vstupné poplatky vs. vysoký výnos
- “Customer care” pre obete
- Aktívny hiring administrátorov vo firmách

NOVÝ PRVOK NA SCÉNE - NEGOCIÁTORI

- Využívanie služieb negiociátorov je najnovším trendom najmä na strednom východe
- Oficiálna prezentácia služieb negociátorov na výstave GITEX GLOBAL v roku 2021 v Dubaji
- Negociátori odporúčajú ako súčasť obrannej stratégie “byť pripravený platiť”
- Podozrenie, že negiociátori analyticky spracúvajú zoznam potenciálnych cieľov pre konkrétne gangy
- Väzby na gangy nepopierajú ani sami negociátori

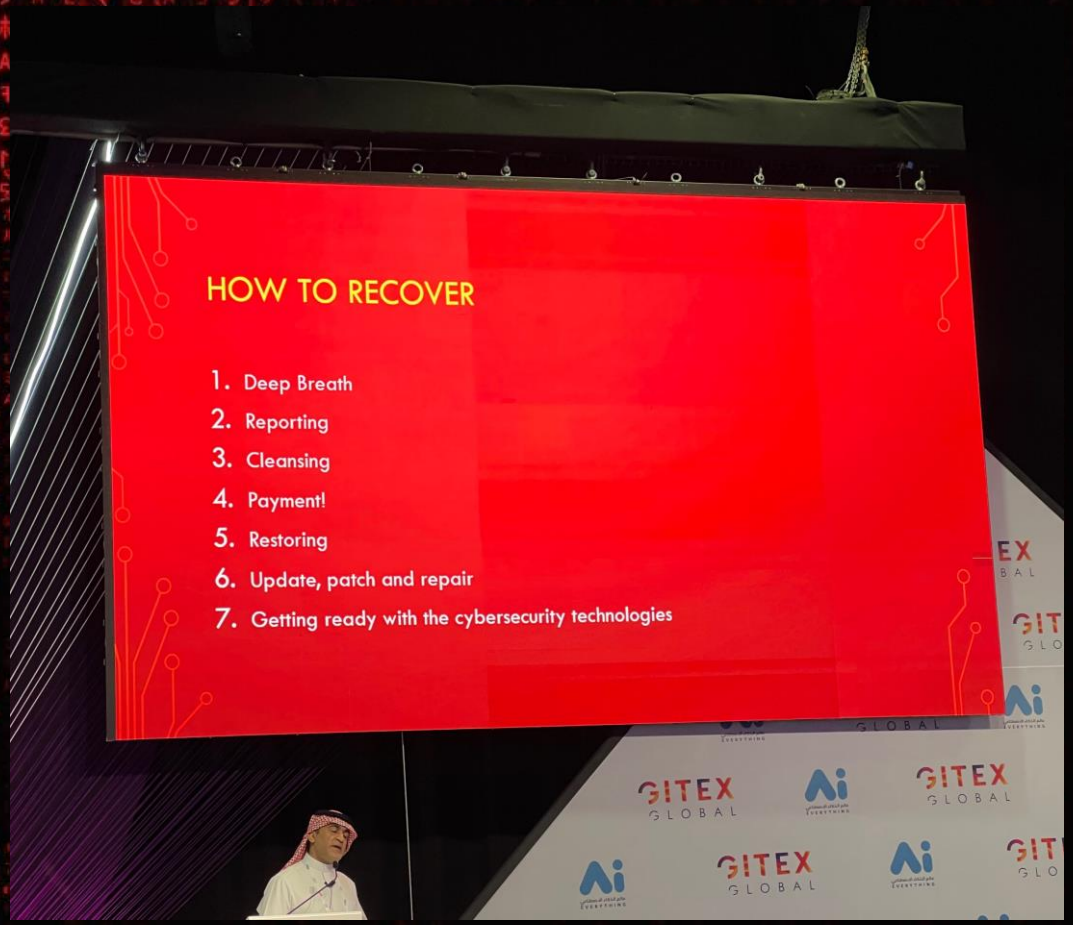
NOVÝ PRVOK NA SCÉNE - NEGOCIÁTORI

- Leader na “trhu” negociátorov švajčiarska firma SCHRANNER NEGOTIATION INSTITUTE
- Zakladateľom firmy je bývalý švajčiarsky policajný dôstojník Matthias Schranner
- Legálnosť pôsobenia negociátorov v rámci EU a USA je diskutabilná
- Platiť = podpora medzinárodného terorizmu

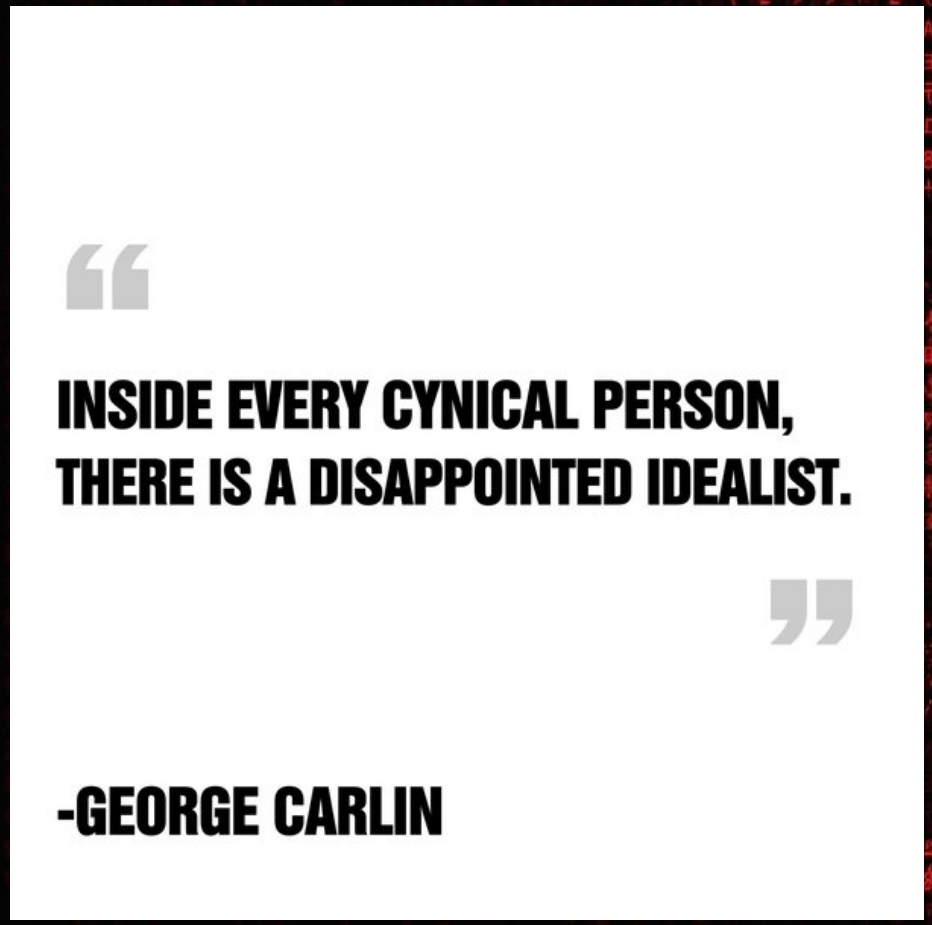


RECOVERY PLAN S PRÍCHUŤOU HUMMUSU

- Oficiálny guideline Ministerstva obchodu Saudskej Arábie odporúča ako jeden z najdôležitejších krokov – platiť!
- Oficiálna prezentácia na GITEX GLOBAL DUBAI 2021
- Majed Alshodari – CISO Ministerstva obchodu SA



ALE NÁS SA TENTO PROBLEM NETÝKA



- Lebo my sa ku kybernetickej bezpečnosti staviame zodpovedne
- Sme perfektne pripravení
- Počúvame odborníkov
- Vzdelávame svojich zamestnancov
- Nevyjednávame s teroristami

ROK 2020 PRÍPAD GARMIN

- Požiadavka na výkupné vo výške 10M USB
- Globálny výpadok všetkých služieb na viac ako 7 dní
- K akcií sa prihlásil ruský gang Evil Corp
- FBI na hlavu šéfa Evil Corp vypísala odmenu 5M USD

- GARMIN využil služby negociátorov Emsisoft z Nového Zélandu
- Službu sprostredkovala americká firma Arete IR, ktorá to ale oficiálne nikdy nepotvrdila (podpora medzinárodného terorizmu)
- Emsisoft dlhodobo podozrievajú autority NZ zo spolupráce s ransomware gangmi

EVIL CORP POD OCHRANOU MOSKVY

- Existujú indície, že Evil Corp je voľbou č. 1 pre ruskú Federálnu bezpečnostnú službu (FSB) pre realizáciu “špeciálnych kybernetických operácií” v zahraničí
- Garantovaná beztrestnosť členov gangu
- Odhaduje sa na základe analýzy blockchainu, že Evil Corp zarobil na ransomware už viac ako 100M USD od roku 2017

https://www.fbi.gov/wanted/cyber/maksim-viktorovich-yakubets

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, “AQUA”	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5’10”	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State’s Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

RUSKÉ GANGY POD OCHRANOU MOSKVY

V prostredí ruského organizovaného kyberzločinu platí zlaté pravidlo, že gangy nesmú realizovať operácie na rusky hovoriacich územiach a štátoch bývalého sovietskeho zväzu.

Ak sa gangy týmto pravidlom riadia a zároveň odvádzajú “výpalné”, majú garantovanú beztrestnosť a samozrejme aj kšefty v záujme štátu – operácie realizované proti zahraničným cieľom.

“VIDIECKE” VS. ”RENOMOVANÉ” GANGY

- “Vidiecke“ gangy používajú staré verzie kódu od “renomovaných“ gangov
- Kód si podľa potrieb upravujú, čo väčšinou znamená jeho vysokú nespoľahlivosť (nemožnosť dešifrovania)
- Taktika dešifrovania na ukážku funkčnosti

- “Renomované” gangy sa snažia v aktuálnych verziách udržiavať relatívne vysokú kvalitu kódu
- “Garantujú” funkčnosť dešifrovania
- Odporúčania negociátorov na spustenie negociačného procesu a “garancie” pre obeť/zákazníka
- Podozrenia z prepojenia negociátorov už vo fáze výberu cieľa

FBI OKRADLA ZLODEJOV

- Prípad ”Colonial pipeline“ z mája 2021
- Zaplatené výkupné 75 BTC (cca 4,4M USD) gangu DarkSide
- FBI vytrasovala prevod 64 BTC z peňaženky gangu DarkSide do peňaženky ku ktorej bližšie nešpecifikovaným spôsobom získala kompletný „seed“
- FBI z tejto peňaženky zabavila všetok obsah, teda 64 BTC + ďalšie kryptomeny v hodnote viac ako 2,3M USD ;)

ĎAKUJEM ZA POZORNOSŤ

Ľubomír Kopáček – iseco s.r.o. – kopacek@iseco.sk