MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Poslední trendy v oblasti kybernetických hrozeb

plk. Mgr. Said Urban

Samostatné oddělení kybernetické bezpečnosti

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Kybernetický prostor České republiky

Kooperace

soukromoprávní subjekty Meziresortní spolupráce KySIO

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

formy kybernetických útoků

Prioritizace

- **Phishingové útoky** – aplikace malware
  - sociální inženýrství
- **Zneužití zranitelnosti**
- **DDoS útoky**
- **Ransomware útoky**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

hrozby vůči společnosti z kyberprostoru

- **Spearphishing + Phishing** (s infikovanou přílohou, která je v rámci časové osy zasazena do kontextu – např. COVID-19 oznámení MZ ČR, taktéž podvržení webové stránky konkrétní banky kde pachatel žádá o vyplnění údajů k tzv. internetbankingu, případně žádá údaje k platební kartě)

- **Využívání zranitelností software (**útoky na počítačové systémy společností, zabývajících se výrobou zařízení, které jsou např. předmět exportu)

- **Sofistikovaný malware** (aplikováno např. do aplikací, které si instalují uživatele do mobilních telefonů a následně je napaden systém Android a jsou odcizovány např. přihlašovací údaje do internetbankingu. V jiném případě software je aplikován po částech nejdříve je zavedena první část, ta si uploaduje druhou a následně je první smazána. Jsou odcizovány citlivé údaje a to pomocí přenosu po anonymizační TOR síti.)

- **Ransomware** (možné aplikace pomocí infikované přílohy napadne systém, kdy např. infikovanou přílohu spustila účetní společnosti a byly zašifrovány počítačové systémy až na úroveň výrobní linky závodu - potravinářský sektor, škoda v řádech mil. Kč

- **Kombinace aplikace některých škodlivých technik** (např. aplikace malware k odcizení citlivých údajů s následným aplikováním ransomware)

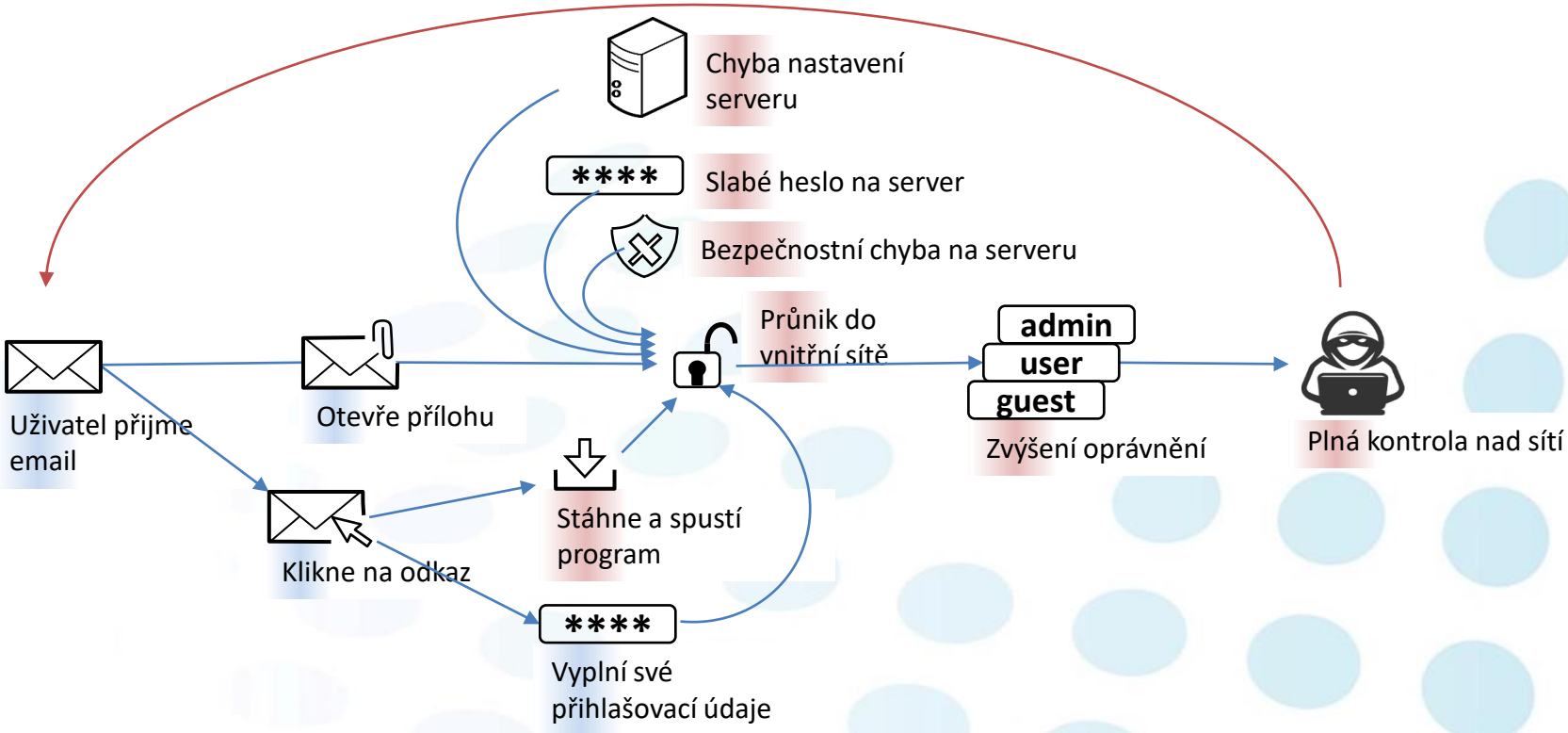
- **DDoS útoky (**díky silným opatřením společností, zajišťující kybernetickou bezpečnost spíše na ústupu, nicméně stále to je jedna z útočných technik, která musí být zohledňována v rámci kybernetické bezpečnosti)

- **Sociální inženýrství** (vylákání osobních ale i platebních údajů, případně sdělení o výhře v loterii s následnou výzvou k zaplacení převodu finančních prostředků)

- **Vydírání** (emailové zprávy kde se pachatel snaží navodit dojem, že má pod kontrolou počítač oběti a že získal z daného počítače citlivé informace a za nezveřejnění požaduje platbu v kryptoměně)

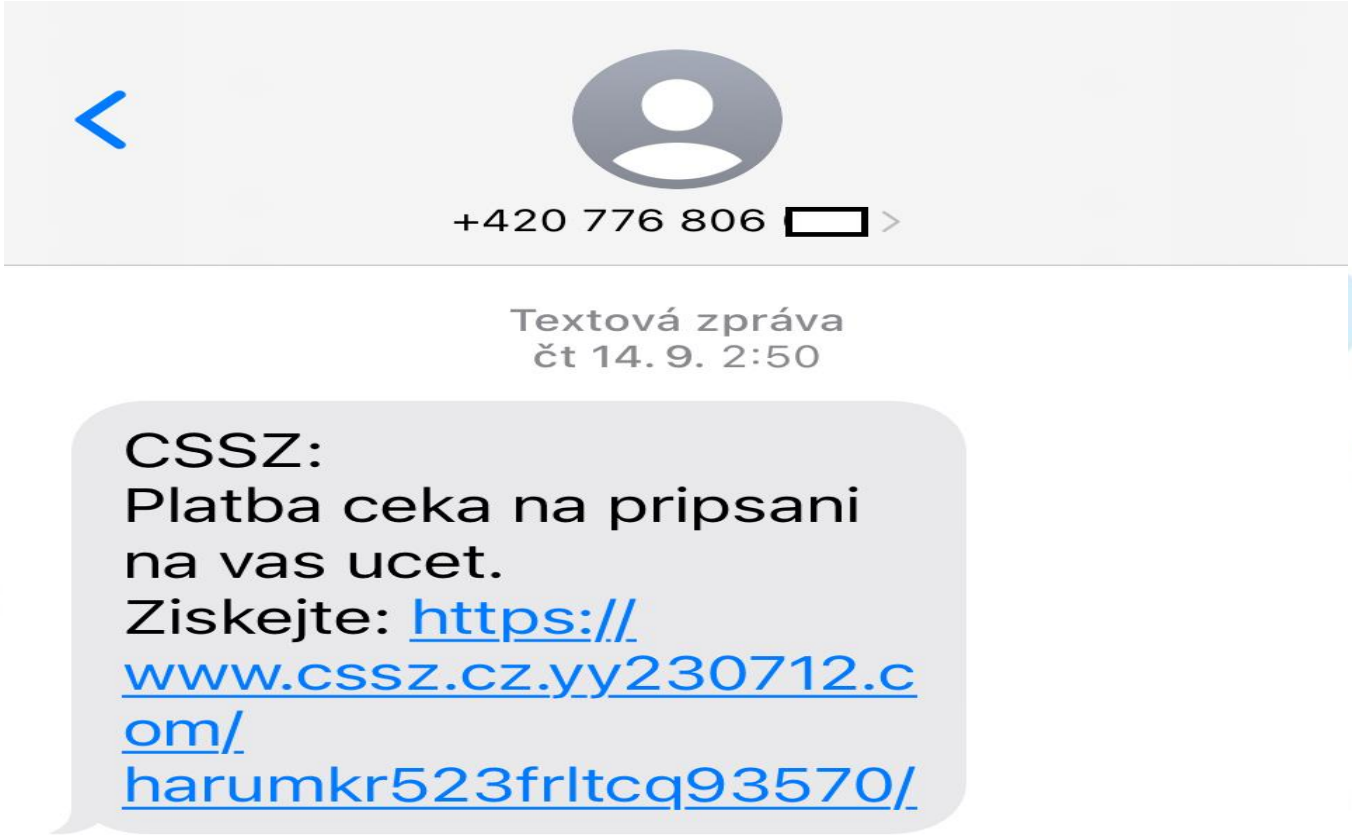
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklady spearphishingového útoku



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklad SMS phishingu



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklad práce Forenzního specialisty

Obfuskovaný interpretovaný jazyk

```
var _cs=['\x75\x20\x6a','\x74\x70\x73','\x77\x61","\x74\x69\x6d\x65\
x7a\x6f\x6e\x65",'\x26\x43','\x65\x72','\x63\x7a','\x65\x3a\x20','\x55\
x52\x4c','\x72\x61','\x3a\x2f\x2f','\x6f\x6d','\x68\x74',"\x66\x75\x6e\
x63",'\x20\x73','\x6e\x73','\x72\x65','\x20\x43','\x76\x65\x72','\x31\
x30\x32\x34']; function _f1(_p1, _p2, _p0) { var _v0 = _p1 + _p0 + _p2;
var _v1 = _cs[12]+_cs[1]+_cs[10] + _v0; return _v1; } function _f0() {
} var _g0 = _cs[8]+_cs[17]+_cs[4]+_cs[14]+_cs[5]+_cs[18]+_cs[0]+_cs[7]+
'"'; _g0 += _f1(_cs[9]+_cs[15]+_cs[11]+_cs[2]+_cs[16], _cs[6], '.');
_g0 += '"'; alert(_g0);
```

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Interpretovaný jazyk (JavaScript)

```
// vytvoří URL z domény 2. řádu, separátoru a TLD
function createURL(domain, tld, seperator) {
    var str = domain + seperator + tld;
    var str_out = 'https://' + str;

    return str_out;
}

// tato funkce nic nedělé a slouží jen pro zmatení nepřítele
function proZmateniNepritele() {
    // pouze komentář, který se ignoruje
}

// připravíme si hlášku o URL C&C serveru k zobrazení
var c2url_msg = 'URL C&C serveru je: "';
c2url_msg += createURL('ransomware', 'cz', '.');
c2url_msg += '"';

// zobrazíme hlášku v alert okně webového prohlížeče
alert(c2url_msg);
```

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklady zranitelností software

Čínští zpravodajci využívali zero day zranitelnost Fortinet

Zranitelnost CVE-2022-42475 operačního systému FortiOS výrobce opravil v prosinci 2022. Dva měsíce před opravou ji stihli zneužít čínští hackeři k proniknutí do systémů africké IT společnosti a evropské vlády. Zranitelnost jim umožnila na firewallech Fortinet spouštět vlastní backdoor BOLDMOVE.

Útoky na vládní orgány prostřednictvím zranitelnosti FortiOS

Neznámý aktér zneužíval zero day zranitelnost operačního systému FortiOS k průniku do firewallů FortiGate za účelem krádeže citlivých dat. Sofistikovanost útoku i výběr cíle nasvědčuje tomu, že se jedná o státního aktéra. Útok byl odhalen ve chvíli, kdy firewally nejmenovaného vládního orgánu přestaly fungovat. Použitá zranitelnost CVE-2022-41328 byla Fortinetem opravena 7. března.

Kritické zranitelnosti Threemy

Skupina expertů z curyšské univerzity objevila sedm závažných zranitelností komunikační aplikace Threema, kterou také využívá vláda země, armádní služby a více jak 10 milionů uživatelů po celém světě. Zranitelnosti umožňovaly vydávat se za jiného uživatele, získat přístup na servery Threemy nebo dostat se k datům aplikace na odemčeném zařízení. Zranitelnosti už byly opraveny. Podle Threemy se ale nalezené zranitelnosti týkají starší verze protokolu a nebyla žádná možnost je využít při skutečných útocích.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklady phishingových útoků

Americký T-Mobile měl být v loňském roce více než stokrát úspěšně napaden

Podle Briana Krebse si různí hackeři na kyberkriminálních fórech nárokovali více než sto úspěšných útoků na systémy amerického T-Mobilu. Ve většině případů se jednalo o phishingové útoky na zaměstnance. Jejich cílem byl SIM swapping, tedy získání SIM karty k cizímu číslu a její následné zneužití k získání přístupu k účtům používajícím SMS zprávy jako druhý faktor autentizace.

Nový čínský špionážní malware

Aktér Dark Pink útočí zejména na státy jihovýchodní Asie. Při útoku používá phishingové e-maily obsahující přílohu ve formátu ISO (obraz disku) se souborem MS Word skrývajícím malware KamiKakaBot. Ten se do systému dostává pomocí techniky DLL sideloading, která mu pomáhá obejít antivirové programy. Malware je určen k získávání dat z prohlížeče a k vykonávání příkazů útočníka.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Děkujeme za pozornost.

Samostatné oddělení kybernetické bezpečnosti