Ukážka útokov na vnútropodnikové systémy, ich znaky a možnosti detekcie

Ladislav Bačo

ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Vládna jednotka CSIRT

- Riešenie incidentov týkajúcich sa ISVS
- Forenzné analýzy
- Analýzy malvéru
- Penetračné testy
- Audity
- Varovania
- Vzdelávanie
- ...

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Anatómia útoku

- Zhromaždovanie informácií o obeti
- Príprava nástrojov a exploitov
- (Spear)phishing
- Exploitácia zraniteľnosti, prístup do zariadenia
- Eskalácia oprávnení, zber hesiel
- Rozšírenie do ďalších zariadení a eskalácia oprávnení
- Ovládnutie doménového kontroléra
- ...

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Zhromažďovanie informácií

- Verejne dostupné informácie: skenovania, DNS záznamy, inzeráty a pracovné ponuky, zverejnené zmluvy (technológie)
- Organizačná štruktúra
- Kontakty na zamestnancov
- Identifikovanie agendy a výber vhodných cieľov

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Phishingový email

- Lákavá ponuka
- Časová tieseň
- Autorita

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Phishingový email

Predmet: Ponuka diarov na rok 2019

Dobry den, p. Mrkvicka.

Radi by sme si dovolili dat Vam do pozornosti ponuku nasej firmy na vyrobu diarov na buduci kalendarny rok 2019.

V portfoliu mame klasicke diare aj motivacne v roznych prevedeniach, vratane luxusnych reprezentativnych.

Samozrejmostou je prisposobenie diarov pre potreby Vasej spolocnosti, moznost umiestnenia loga na jednotlive stranky a na obal, ako aj personalizovane texty v diari.

Pre spolahlivych firemnych zakaznikov navyse ponukame moznost nakupu za velkoobchodne ceny a dalsie vyrazne zlavy a benefity. Zaroven pri objednavkach zadanych do 14.12.2018 garantujeme vyhotovenie a dodanie do Vianoc.

Viac o nasej ponuke najdete na tomto odkaze http://10.3.13.37/2019-diary-special-edition

S pozdravom a prianim pekneho dna

Marketingove oddelenie

Najkrajsie Diare/Beautiful Diaries

Ukážka útoku

- Počítač útočníka
- Počítače dvoch zamestnancov firmy, ich šéfa a doménový kontrolér

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Ako sa chrániť?

- Hrozba pre všetkých (štát, firmy, domácnosti)
- Neotvárať podozrivé emaily a prílohy
- Neklikať na každý odkaz, najprv skontrolovať, kam odkaz smeruje
- Obozretnosť, opatrnosť: ak máte zlý pocit, dôverujte mu a nenechajte vyhrať zvedavosť
- Pravdovravnosť: keď sa niečo stane, nahlásiť to administrátorom alebo bezpečnostnému tímu
- Vzdelávanie zamestnancov

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Ako sa chrániť? Heslá

- Nepoužívať slovníkové heslá
- Ani heslá založené na bežných pravidlách:
  - Jablko => J4blk0&
- Radšej 4 náhodné slová, spojiť do jedného:
  - VlakKonferenciaBateriaVoda
- Prípadne pridať diakritiku (+-)

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Ako sa chrániť? Technické opatrenia

- Môžu pomôcť, no nie sú nepriestrelné. Vždy je to o ľuďoch
- Antivírový program – aktualizovaný, zapnutý
- Aktualizácie operačného systému a programov
- Monitoring, centrálny zber logov, IDS, IPS, SIEM,... ale aj drobné vychytávky ako DeepBlue či Maltrail
- Zakázať, čo nie je potrebné:
  - Javascript a reklamy v prehliadačoch
  - Makrá v dokumentoch
  - Otváranie skriptovacích súborov (.js, .vb, .vbe,...) vo Windows Scripting Host
  - *Spúšťanie neznámych programov (AppLocker)*

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Dokonalosť je dosiahnutá nie vtedy, keď už nie je čo pridať, ale vtedy, keď už nie je čo odobrať.

Antoine de Saint-Exupéry

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Ak si myslíte, že technológie vyriešia Vašu bezpečnosť, potom nerozumiete technológiám alebo bezpečnosti.

Bruce Schneier

+ 421 2 59278 202
ladislav.baco@csirt.sk

Štefánikova 15 - 011 05 Bratislava
www.csirt.gov.sk

Ďakujem
za pozornosť