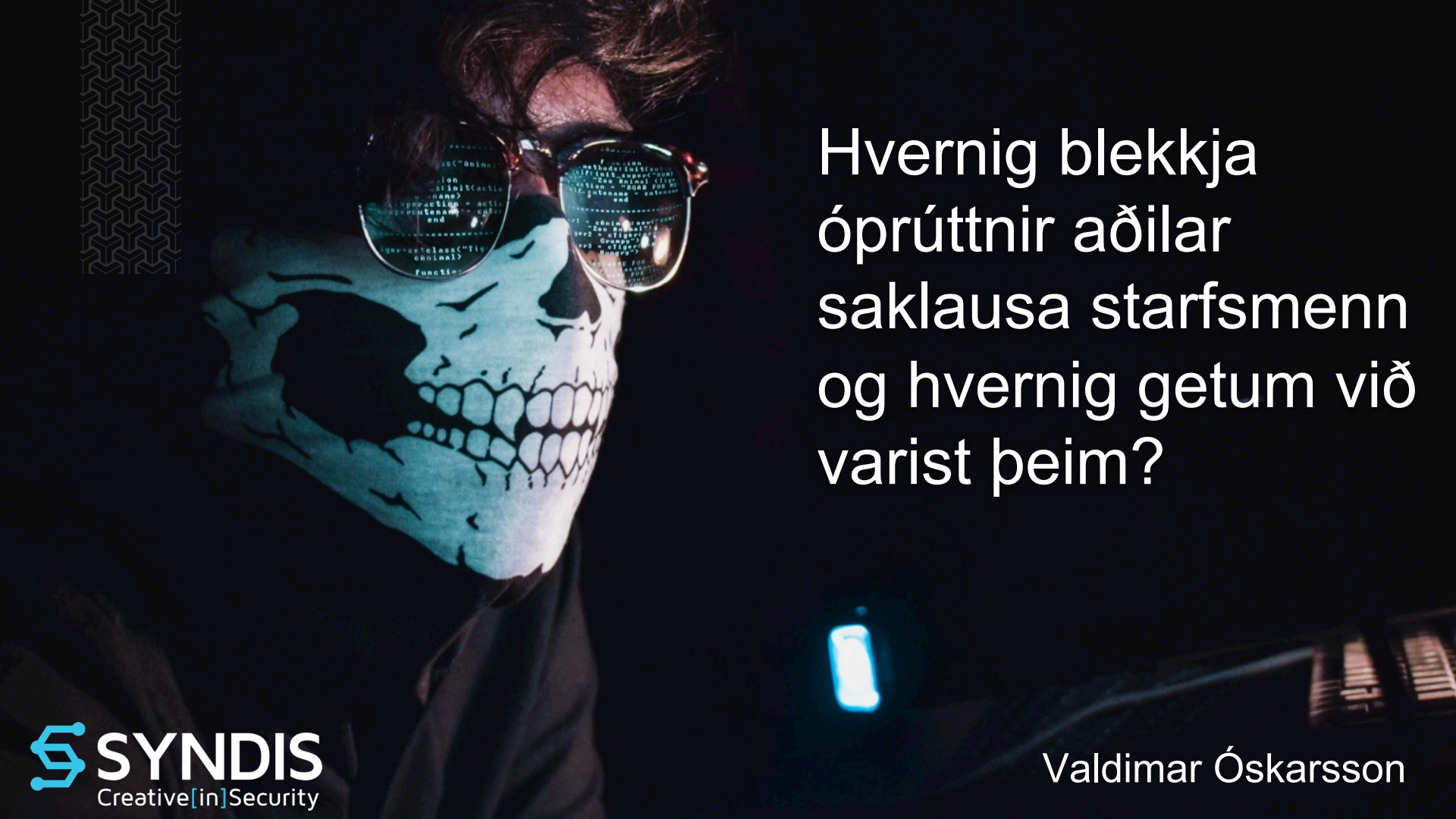


Hvernig blekkja óprúttnir aðilar saklausa starfsmenn og hvernig getum við varist þeim?

SYNDIS
Creative[in]Security

Valdimar Óskarsson

Ógnir – nýjar og gamlar

- Vírusar og „malware“
  - Allt frá „love letter“ til „ransomware“
- Óánægður/kúgaður starfsmaður veitir aðgang
- Skipulagðir einstaklingar eða hópar brjótast inn á tölvukerfi í hagnaðarskyni
- IoT

Hvað hefur breyst?

- Almenn notkun netsins
- Aukið aðgengi að þjónustu á netinu
  - Heimabankar
  - Heilbrigðisupplýsingar
  - Fjármálaupplýsingar
- Aukið aðgengi að þekkingu á netinu

Hvað hefur ekki breyst?

- Starfsmenn
- Fjárhagslegur ávinningur tölvuþrjóta
- Áskorun

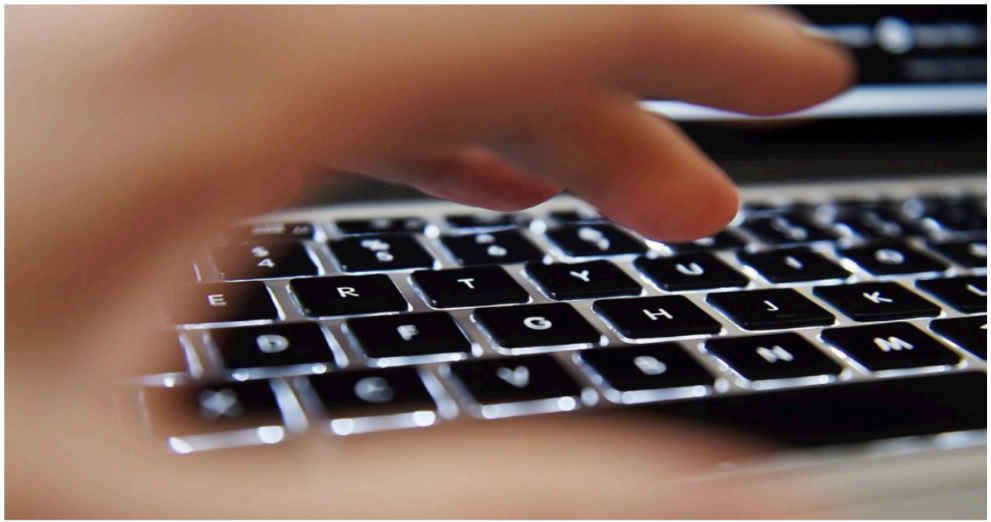
Hvernig vinna tölvuglæpamenn?

- Tölvukerfin eru ekki lengur skotmark
- Tölvuglæpamenn nota sérstakt orðalag, sálfræði og auglýsingar til að fá fólk í lið með sér
- Þetta snýst um að ná viðkvæmum upplýsingum – allar aðferðir leyfðar
- Vilja skjótfenginn gróða

Hvað er að frétta?

Tækni & vísindi | mbl | 15.12.2017 | 11:37

Að lágmarki 100 þúsund íslensk lykilorð aðgengileg



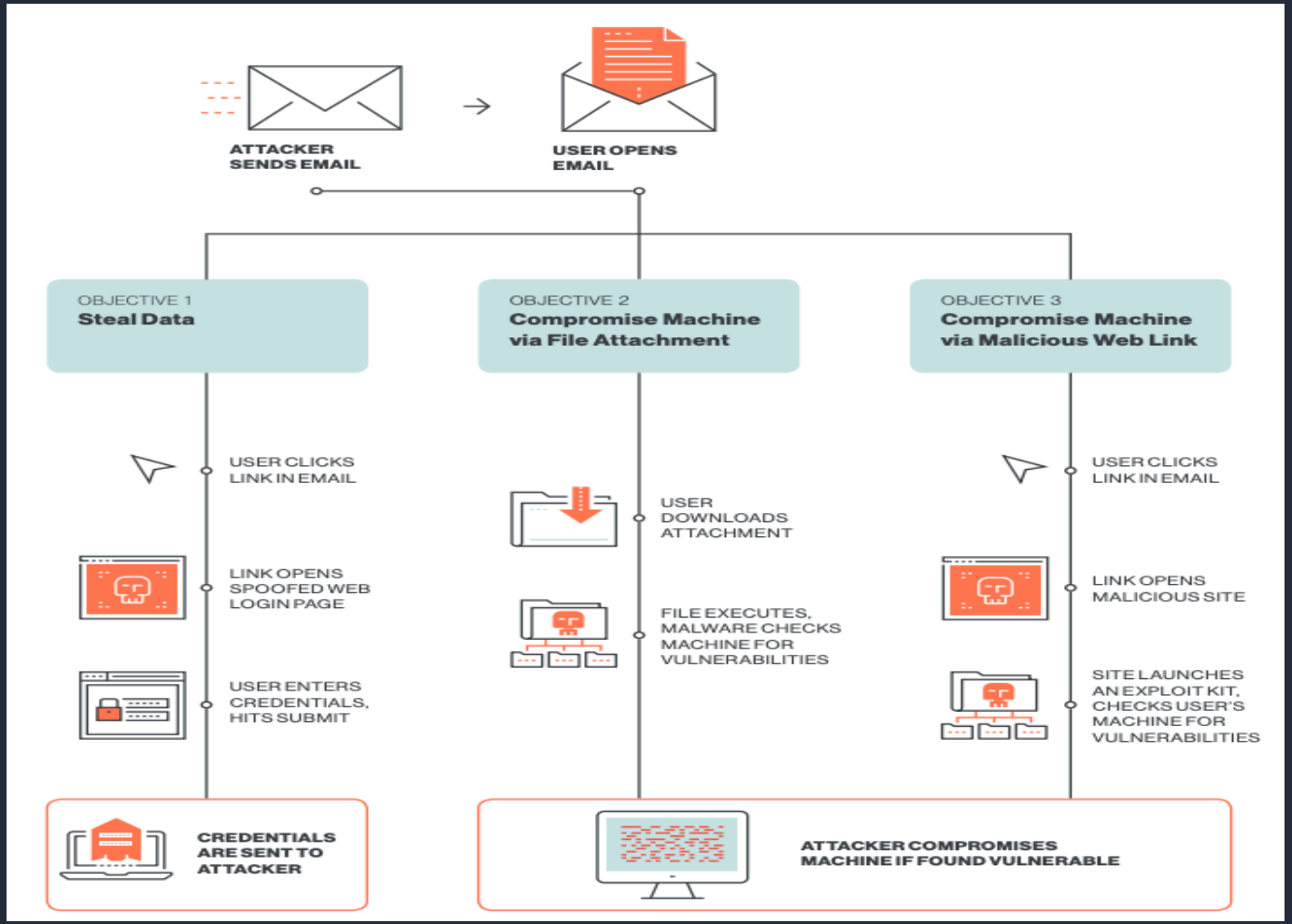
Í lekanum núna er að finna allavega 385 milljón nýrra lykilorða sem ekki hafa komið fyrir sjónir sérfræðinga eða almennings áður. *EPA*

Hvað aðferðir eru notaðar?

- Vefveiðar (Phishing og Spear Phishing) – aðferð til að fá notendur til að gefa upp viðkvæmar upplýsingar

Hvaða aðferðir eru notaðar?

- Vefveiðar (Spear Phishing)
- Bragðvísi (Social Engineering)
- Gagnalekar notaðir (https://haveibeenpwned.com/)
- Óværum komið fyrir á tölvum starfsmanna
- Samfélagsmiðlar skoðaðir
- Óprúttnu aðilarnir velja „fórnarlömbin“ og slá til


ATTACKER SENDS EMAIL
USER OPENS EMAIL
OBJECTIVE 1
Steal Data
OBJECTIVE 2
Compromise Machine via File Attachment
OBJECTIVE 3
Compromise Machine via Malicious Web Link
USER CLICKS LINK IN EMAIL
LINK OPENS SPOOFED WEB LOGIN PAGE
USER ENTERS CREDENTIALS, HITS SUBMIT
USER DOWNLOADS ATTACHMENT
FILE EXECUTES, MALWARE CHECKS MACHINE FOR VULNERABILITIES
USER CLICKS LINK IN EMAIL
LINK OPENS MALICIOUS SITE
SITE LAUNCHES AN EXPLOIT KIT, CHECKS USER'S MACHINE FOR VULNERABILITIES
CREDENTIALS ARE SENT TO ATTACKER
ATTACKER COMPROMISES MACHINE IF FOUND VULNERABLE


Veiðipóstar

Öryggi - Tölvupóstar

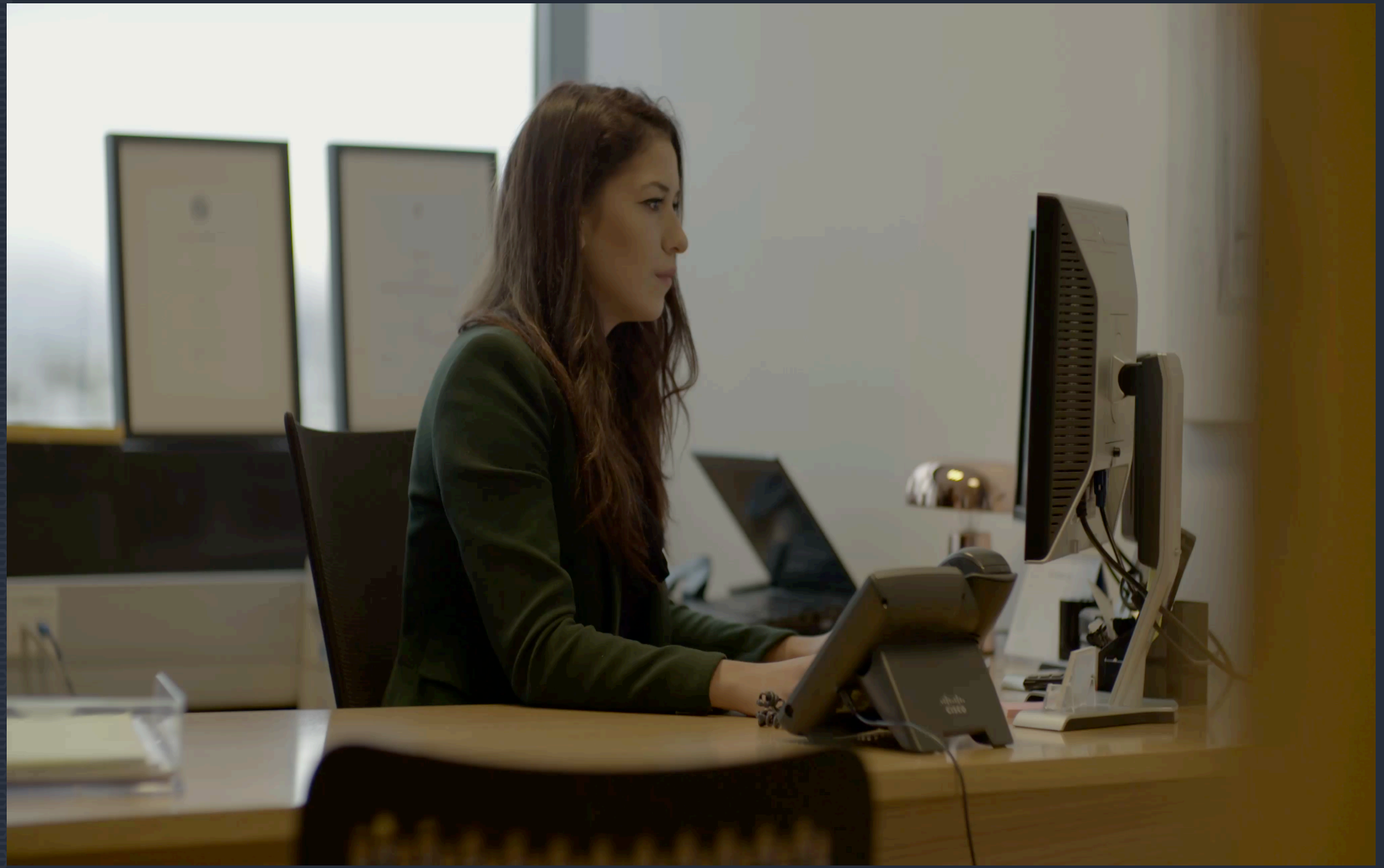
- Frá hverjum er tölvupósturinn? Skoða stafsetningu
- ER VERIÐ AÐ HRÓPA OG ÝTA Á EFTIR?
- Er innihaldið of gott til að vera satt?
- Er verið að biðja um viðkvæmar upplýsingar?
- Er verið að leiða þig á vefslóð sem þú þekkir ekki?
- Áttir þú von á tölvupósti með viðhengi?

Bragðvísi (Social Engineering)

- Einhver reynir að nálgast viðkvæmar upplýsingar
- Ekki vanmeta þær upplýsingar sem þú hefur aðgang að
- Ef einhver hringir og biður um viðkvæmar upplýsingar, fá nafn og númer og hringja tilbaka

Vaxandi ógn í dag

- “CEO fraud“ eða „BEC“
- Markmið að fá starfsmenn til að millifæra pening á bankareikninga óprúttinna aðila
- Gríðarlegt fjárhagslegt tjón fyrirtækja
- Nánast ómögulegt að endurheimta
- Lykilstarfsmenn missa starfið
- Fjármáladeildir fyrirtækja aðal skotmarkið



Hvernig getum við varist?

- „Common Sense“?
- Sérstök fræðsla lykilstarfsmanna
- Prófanir
- Skoða póstfang sendanda tölvupóstins
- Skoða reikningsnúmer vel, skoða eldri yfirfærslur, hefur eitthvað breyst?
- Hvert er móttökuland greiðslu?

Hvernig getum við varist?

- Breyta verklagi þegar um er að ræða háar fjárhæðir
- Skoða orðalag tölvupósta
- Virkja tvíþætta auðkenningu inn á viðkvæm kerfi
- Flókin aðgangsorð
- Engin samnýting aðgangsorða
- „Trust but verify“

Takk fyrir!

SYNDIS
Creative[in]Security