EUROPEAN UNION AGENCY
FOR CYBERSECURITY

IZSILJEVALSKA PROGRAMSKA OPREMA (ANG. RANSOMWARE)

VSEBINA

Kaj je izsiljevalska programska oprema.

Potek napada, namestitev in sprožitev.

Faza izsiljevanja.

Posledice izsiljevalskega napada.

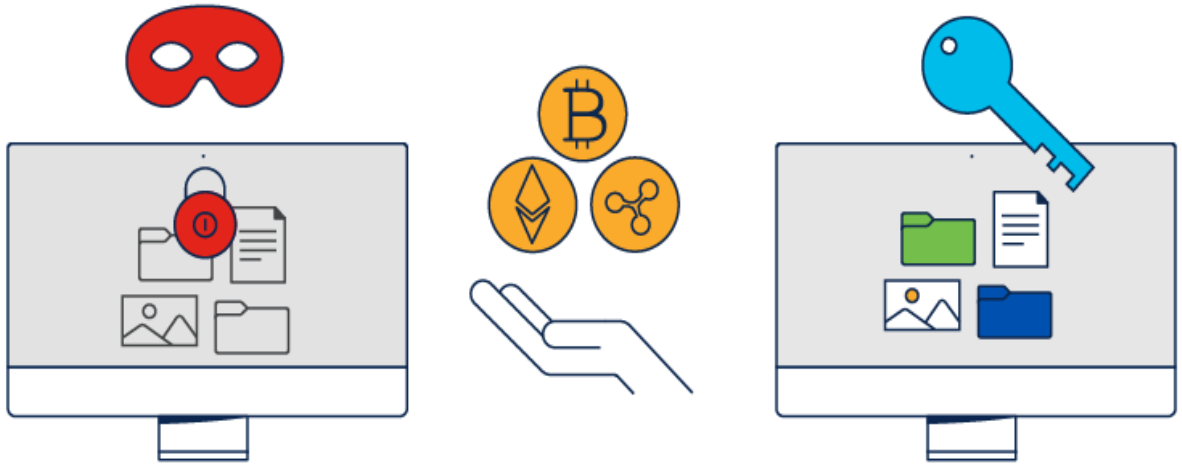
Zaščita pred napadom.

IZSILJEVALSKA PROGRAMSKA OPREMA

Namen: šifriranje podatkov + izčrpavanje/objava

Dvofazni napadi: odtujitev podatkov iz sistema + njihovo šifriranje za izsiljevanje (ang. exfiltration + encryption)

Trend: dvojno in trojno izsiljevanje



Vir: https://www.cisco.com/site/us/en/learn/topics/security/what-is-ransomware.html

POTEK NAPADA

Faza identifikacije potencialnih tarč in zbiranje informacij

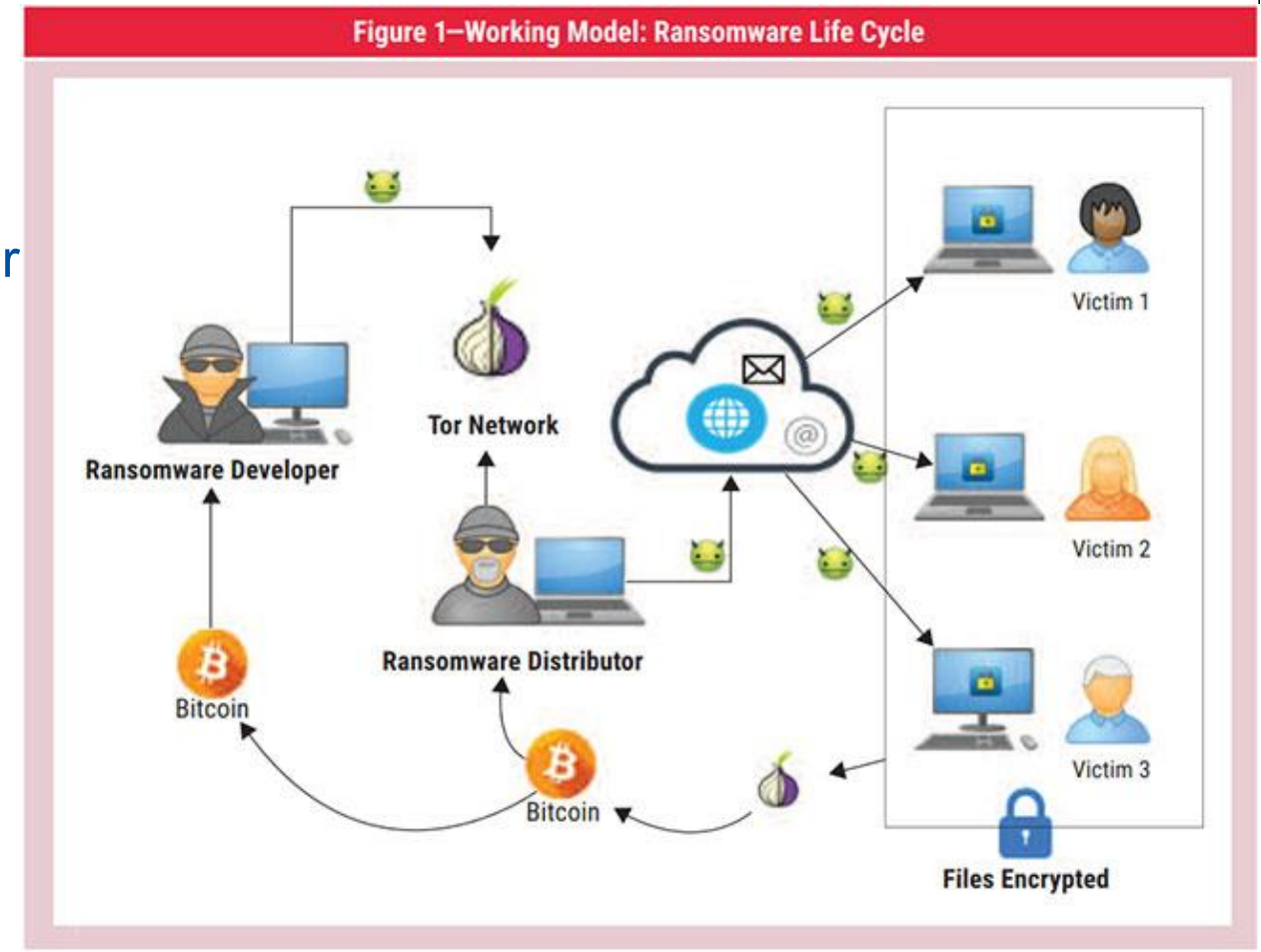
Napadalci raziskujejo, izbirajo ciljne organizacije ter o njih zbirajo ključne informacije

Poizvedovanje – **pasivno** (OSINT, Whois, DNS poizvedbe, iskanje po javnih repozitorijih)

Poizvedovanje – **aktivno** (skeniranje portov, skeniranje za ranljivosti na tarčah, brute-force, credential stuffing)

Socialni inženiring

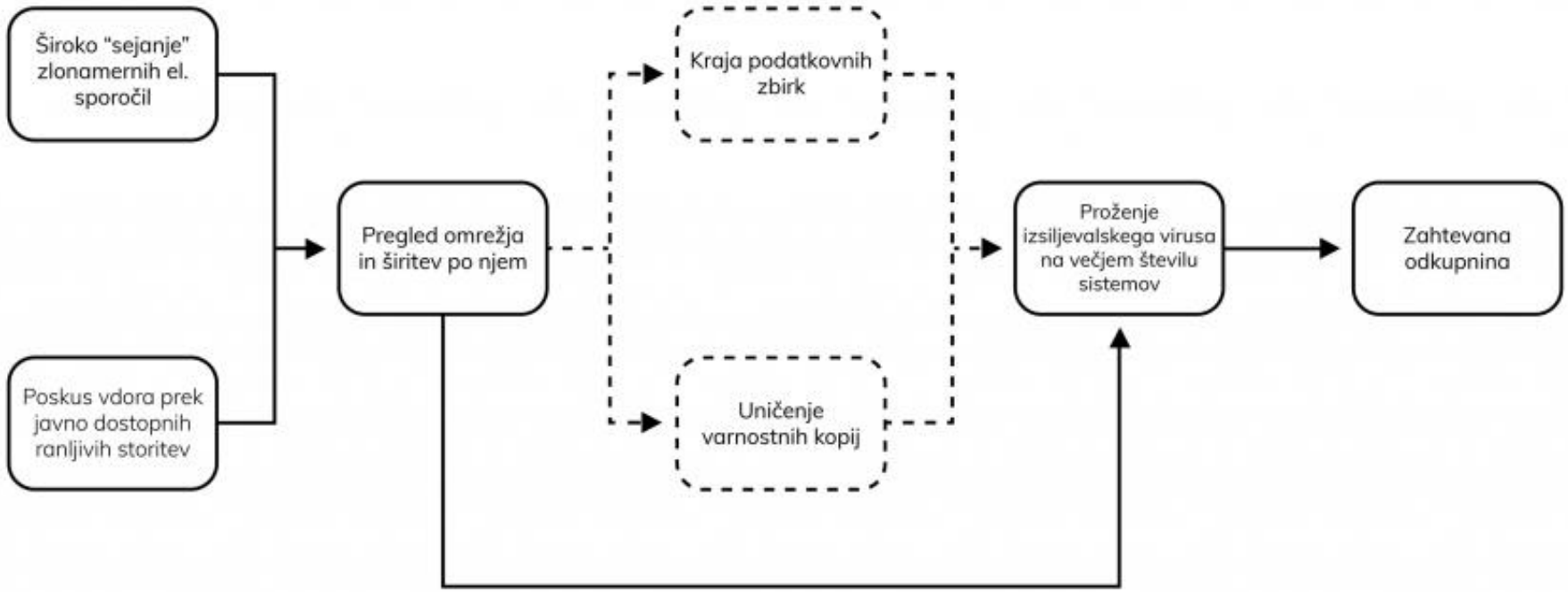
Analiza zgodovine domen, certifikatov…



Vir: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/evidential-study-of-ransomware-cryptoviral-infections-and-countermeasures

POTEK NAPADA

Faza izvedbe napada



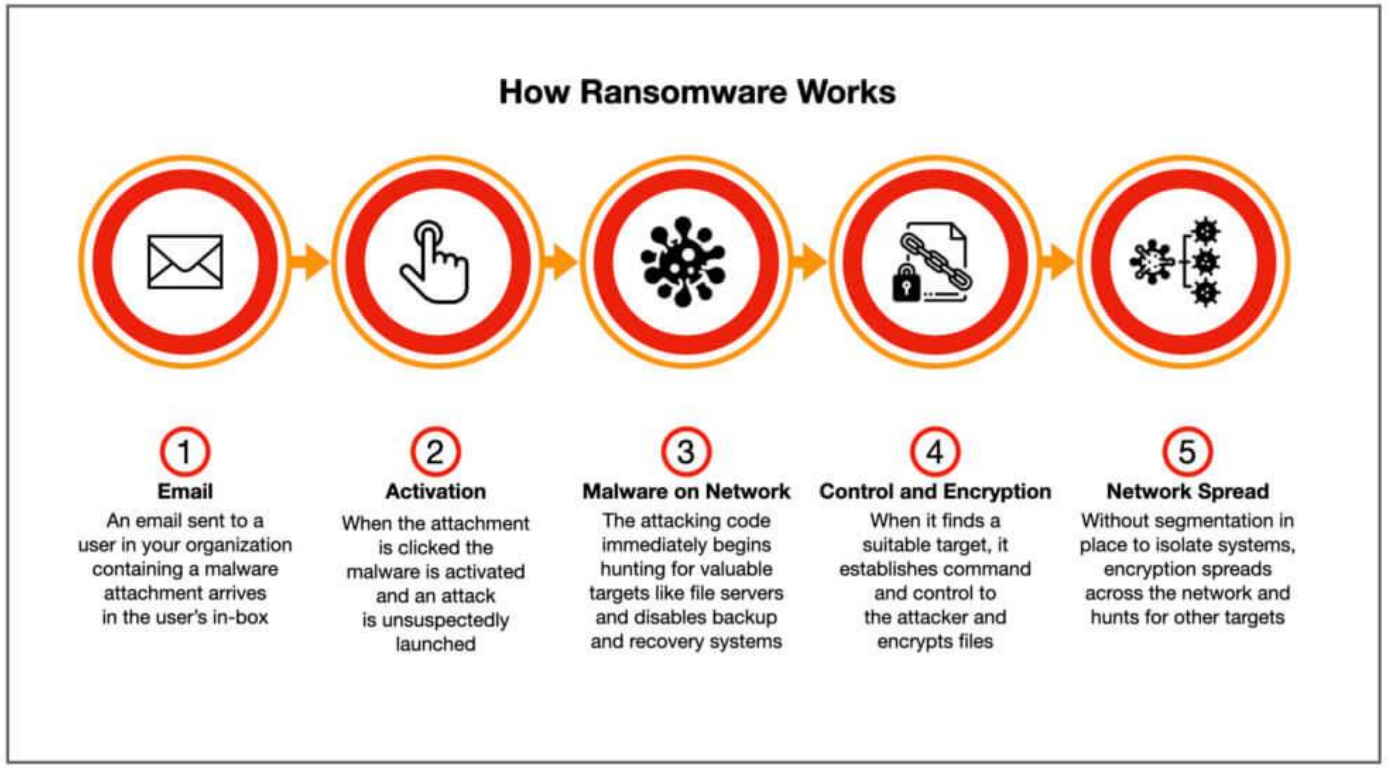
Vir: https://www.cert.si/tz011/T

LATERALNO GIBANJE PO OMREŽJU

Iskanje končnih tarč

Premikanje po omrežju organizacije, pri tem pridobivanje informacij o tem, kje v organizaciji so pomembne informacije, kritični sistemi in katere so potencialne tarče za šifriranje podatkov.

Sproti pridobivajo nadzor nad napravami, strežniki, s čimer se poveča verjetnost, da bodo našli in šifrirali za organizacijo pomembne podatke



Vir: https://concordbridge.org/index.php/2024/05/08/ransomware-attack-targeted-concord-school-system-superintendent-says/

KAKO SE Nnapadalci PREMIKAJO PO OMREŽJU?

Izkoriščanje ranljivosti in šibkosti

Izkoriščajo napačne nastavitve, npr. slaba zaščita skupnih map, uporaba šibkih gesel, nezavarovan oddaljen dostop…

Kraja in uporaba ukradenih gesel npr. z beleženjem tipk (ang. Keyloggerjem) ali pa jih dobijo iz raznih baz predhodno razkrite poverilnice, ki jih uporabijo za prijavo v druge sisteme.

Uporabijo „hash“ t.i. ang. pass the hash, ne uporabijo gesla kot takega, ampak njegovo šifrirano obliko; s tem se prijavijo v drug sistem, ne da bi poznali dejansko geslo.

Vir: https://www.geeksforgeeks.org/blogs/rise-of-ransomware-attacks-during-covid-19-pandemic/

DVIG PRAVIC

Cilj je, da si napadalec dvigne pravice, s čimer pridobi večji nadzor nad kritičnimi sistemi in se tudi lažje premika naprej po omrežju.

KAKO?

Izkoriščanje ranljivosti programske opreme, operacijskega sistema, omrežnih konfiguracij.

Zloraba ukradenih poverilnic npr. privilegiranih računov, si potem sami dodelijo npr. administratorske pravice.

Zloraba legitimnih aplikacij in servisov, ki imajo že neke višje pravice.

Kaj se zgodi, ko napadalec pride v omrežje?

NAMESTITEV IZSILJEVALSKE PROGRAMSKE OPREME IN ODKUPNINA

Napadalci prožijo namestitev zlonamerne kode, ki zašifrira datoteke na ciljnem sistemu.

Izsiljevalska koda je lahko v lažnem sporočilu (ang. phishing) ali na lažni spletni strani.

Lahko pride do namestitve prek obiska kompromitirane ali zlonamerne spletne strani zaradi ranljivosti v brskalnikih, vtičnikih.
Lahko se uporabi izkoriščanje.

Po šifriranju napadalec zahteva plačilo odkupnine.

Vir: https://www.pcmag.com/opinions/never-ever-pay-the-ransom

ŠIFRIRANJE DATOTEK

1

Napadalci uporabljajo precej napredne algoritme za šifriranje datotek, tarče pa tako do zaklenjenih datotek brez ključa za dešifriranje ne morejo dostopati

2

Zašifrira se lahko različne vrste datotek (slike, videe, celotne podatkovne baze…) in se onemogoči normalno delovanje organizacije

3

Lahko se zgodi tudi, da napadalci spreminjajo originalne datoteke, jih prepišejo, s čimer je obnovitev še težja

IZSILJEVANJE IN KOMUNIKACIJA S STRANI NAPADALCEV

Napadalci po šifriranju podatkov vzpostavijo komunikacijo s tarčno organizacijo in zahtevajo odkupnino v zameno za dešifrirni ključ.

Da ostanejo anonimni in jih je težje izslediti, uporabljajo npr. Tor omrežje, komunicirajo pa lahko prek e-pošte, neposrednega sporočanja, posebnih portalov za pogajanje, ki jih vzpostavijo napadalci.

Vir: https://www.lmgsecurity.com/to-pay-or-not-to-pay-ransomware-demands-that-is-the-question/?srsltid=AfmBOoqUK4GhePEdNe5l66oeecfJoivgwPZwROowxhSi004Rbr6dDCzgrity

KAKO JE S PLAČILOM?

Izsiljevalci zahtevajo plačilo v kriptovalutah, ki so decentralizirane in zagotavljajo psevdonimizacijo ter jih je težko slediti.

Določijo kratek rok za plačilo, da spravijo organizacije v stres in pod pritisk.

Pošljejo še nek dokaz o eksfiltraciji podatkov, ki imajo za organizacijo neko vrednost in to izkoristijo za **dodatno izsiljevanje.**

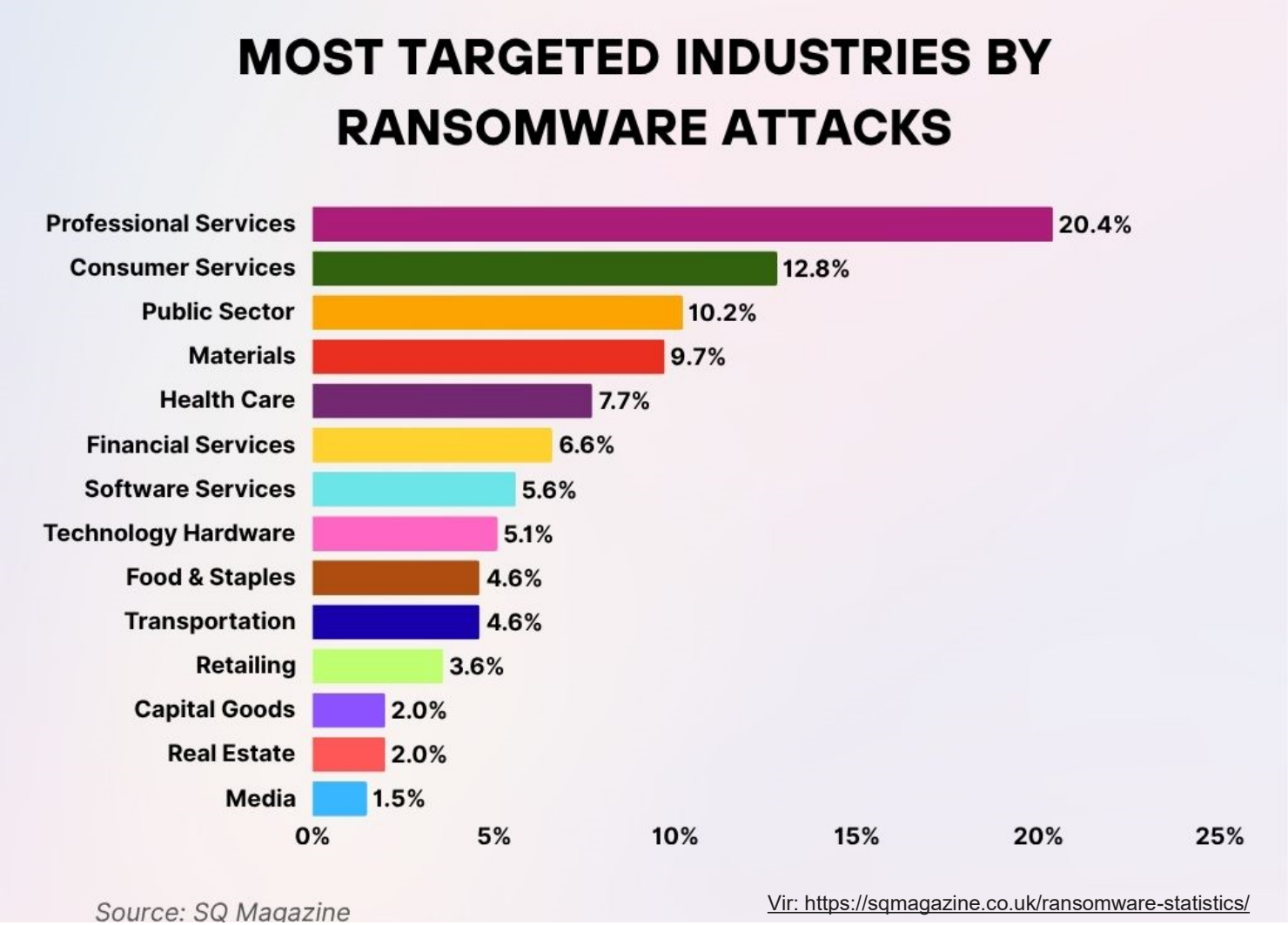
Vir: https://www.darkreading.com/vulnerabilities-threats/how-to-make-a-ransomware-payment---fast

OBNOVITEV IN ZAŠČITA

Organizacija se po zamejitvi napada osredotoči na obnovitev delovanja svojih sistemov, obnovitev šifriranih podatkov in uvedbo ukrepov, da se podoben napad ne bi ponovil

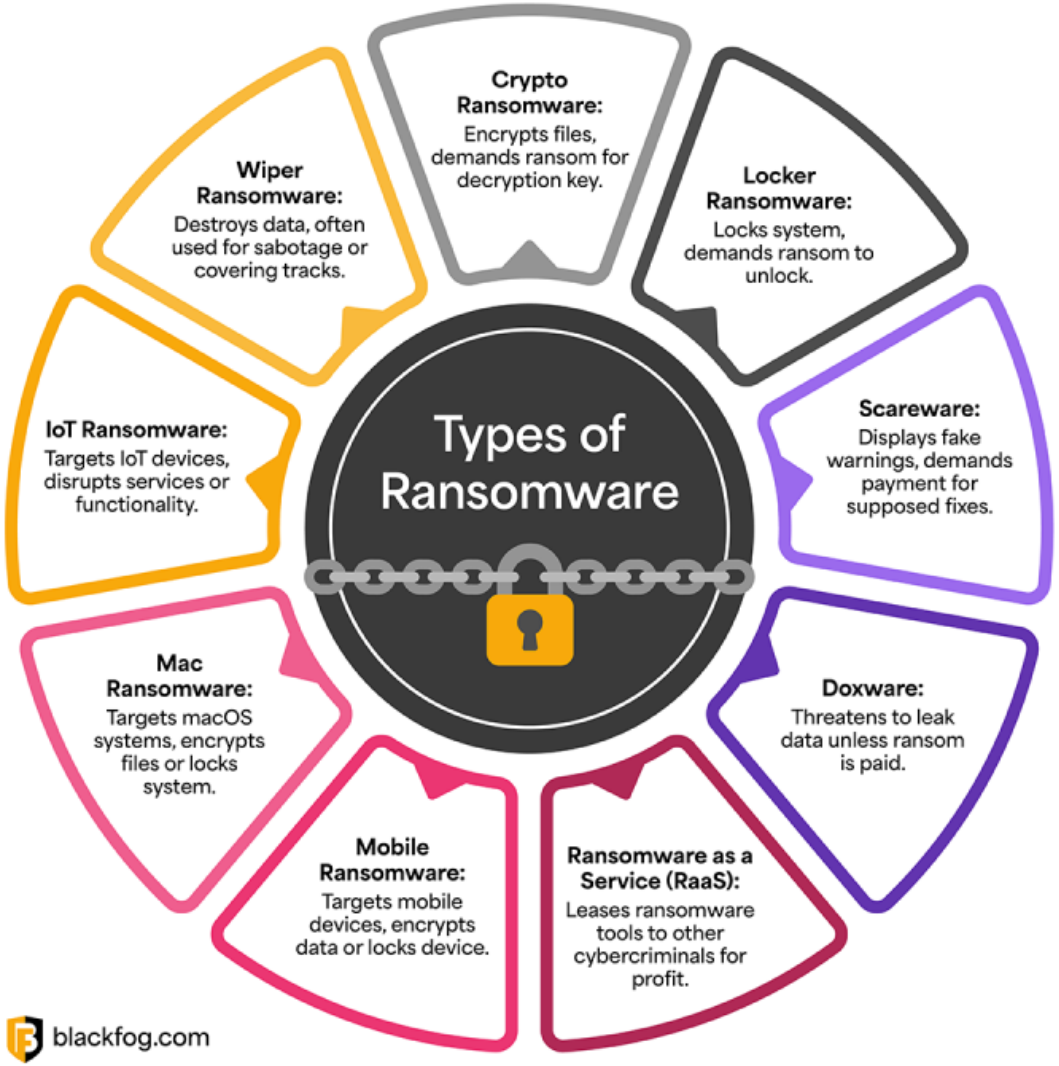
Vir: https://www.tierpoint.com/blog/ransomware-recovery-plan/

NAJBOLJ CILJANI SEKTORJI Z IZSILJEVALSKIM NAPADOM



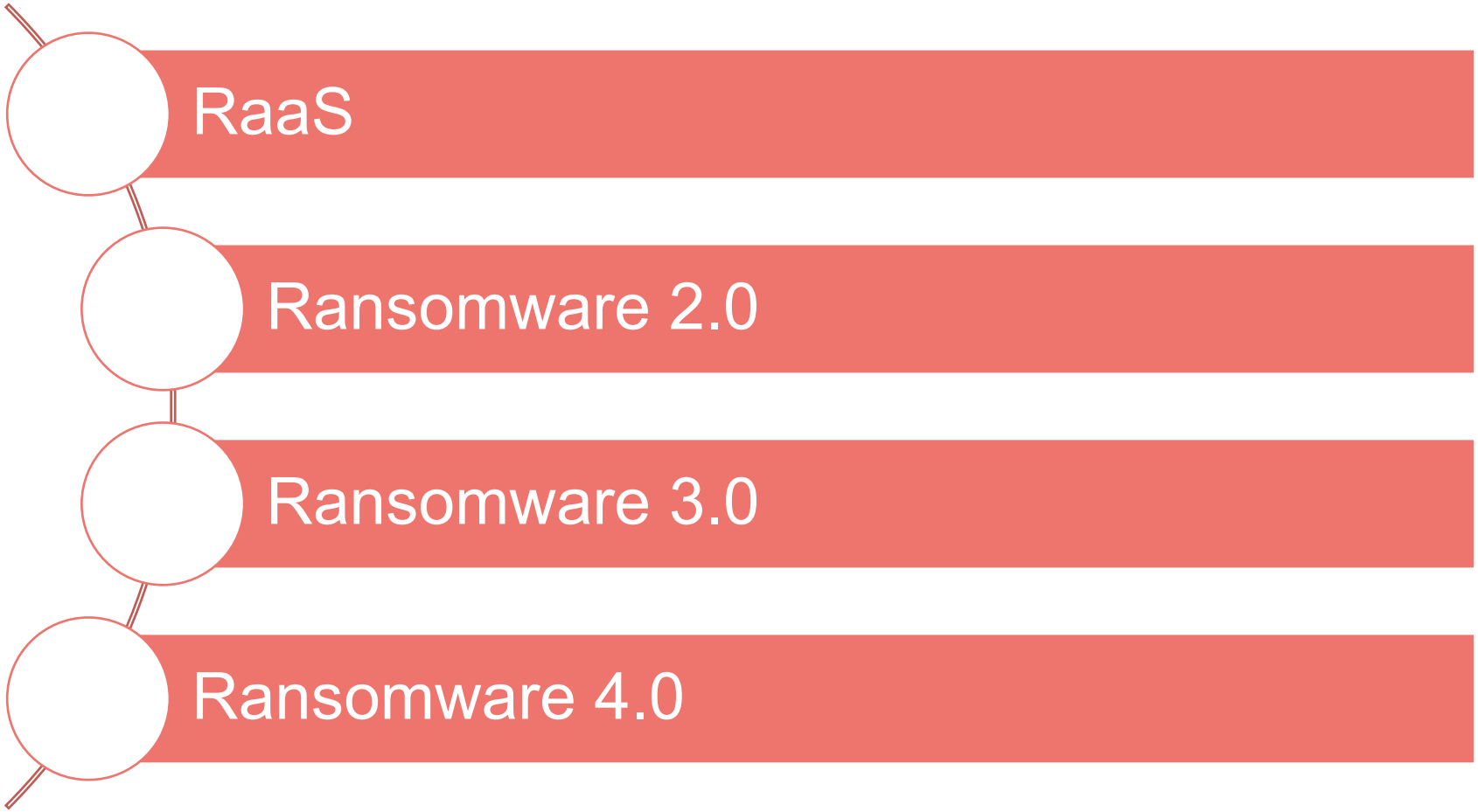
Vir: https://sqmagazine.co.uk/ransomware-statistics/

VRSTE IZSILJEVALSKIH NAPADOV



Vir: https://sqmagazine.co.uk/ransomware-statistics/

EVOLUCIJA IZSILJEVALSKE PROGRAMSKE OPREME



EVOLUCIJA IZSILJEVALSKE PROGRAMSKE OPREME

RaaS ***Ransomware-as-a-Service***	• naročnina na storitve (mesečno), • orodja za izvedbo napada – *RaaS kit*, • nepooblaščen dostop, šifriranje podatkov, zahteva za odkupnino, • *DaskSide, REvil, LockBit, Dharma…*
Ransomware 2.0	• eksfiltracija podatkov – večplastno izsiljevanje, • kraja intelektualne lastnine, kraja poverilnic, grožnje zaposlenim in strankam, uporaba ukradenih podatkov za ciljane *phishing* napade, javno izpostavljanje žrtev.
Ransomware 3.0	• Prodaja ukradenih podatkov, kraja denarja z računov organizacije, osebno izsiljevanje posameznikov, *BEC*, izvajanje DDoS napadov, kraja resursov…
Ransomware 4.0	• Avtomatizacija in večja učinkovitost napadov.

POSLEDICE ZA ORGANIZACIJE

MOTNJE DELOVANJA prekinjeno delovanje, slabša operativnost, nedostopnost kritičnih sistemov, izguba produktivnosti, zamude.

IZGUBA ALI UNIČENJE PODATKOV izziv, če ni ustrezno zagotovljeno varnostno kopiranje – lahko se tudi za vedno izgubijo določeni podatki.

FINANČNE IZGUBE zaradi plačila odkupnine, zaradi stroškov, ki jih organizacija porabi za okrevanje, zaradi regulatornih sankcij, izgube ugleda…

IZGUBA UGLEDA predvsem, če pride v javnost, lahko organizacija izgubi stranke, partnerje, delničarje… ni več zaupanja v organizacijo in zmožnost, da zaščiti svoje podatke… posledično se izgubijo tudi poslovne priložnosti.

ZAKONSKE IN REGULATORNE POSLEDICE glede na vrsto kompromitiranih podatkov, predvsem, če gre za OP ali občutljive podatke; globe so lahko zelo visoke.

VARNOSTNI UKREPI

- Preverjanje in odpravljanje varnostnih ranljivosti.
- Redno nameščanje varnostnih popravkov.
- Zaščita končnih točk (EDR).
- Segmentacija omrežja.
- Načelo minimalnih pravic.
- Redno varnostno kopiranje.
- Zbiranje obveščevalnih informacij (CTI), npr. razkrite poverilnice, lahko pomaga pri odkrivanju potencialne priprave na napad.

KAJ NAM LAHKO ŠE POMAGA

Pripravljen načrt odzivanja na incidente z izsiljevanjem.

Sistemi za zaznavo anomalij ter alarmiranje, omogoča hiter odziv in ukrepanje za zamejitev napada.

Protokol komuniciranja določimo vnaprej, interno in eksterno, koga je treba obvestiti in mu poročati.

Če je do napada že prišlo izvesti forenzično analizo za razumevanje glavnega vzroka, zbiranje dokazov, načrtovanje ukrepov.

Izobraževanje zaposlenih za nenehno utrjevanje znanja glede informacijske in kibernetske varnosti, najpogostejših groženj, prepoznavanju le-teh, prijavi nenavadne aktivnosti ipd.

HVALA

+111 123 456 789

info@enisa.europa.eu