



srce

Sveučilište u Zagrebu  
Sveučilišni računski centar

KLASA: 008-03/24-010/001  
URBROJ: 3801-10-010-02-24-11  
Zagreb, 4. ožujka 2024.

Priopćenje za novinare

## Konferencija BSides Zagreb 2024

*Drugo izdanje konferencije okupilo u Srcu više od sto stručnjaka računalne sigurnosti*

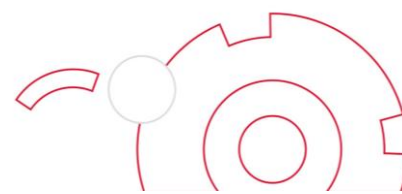
(Zagreb, 4. ožujka 2024.) U Sveučilišnom računskom centru Sveučilišta u Zagrebu (Srcu) u petak je održano drugo po redu izdanje konferencije BSides Zagreb koje je okupilo više od sto stručnjaka računalne sigurnosti.

Program konferencije započeo je prigodnim obraćanjem ravnatelja Srca Ivana Marića koji je istaknuo usmjerenost Srca na ugrađivanje najviših standarda računalne sigurnosti u infrastrukturu koje gradi i održava te sustave i digitalne usluge koje razvija i stavlja na raspolaganje akademskoj i znanstvenoj zajednici. Naglasio je i posvećenost Srca okupljanju zajednica i istaknuo organizaciju konferencije BSides Zagreb kao potvrdu tog pristupa te poželio svima okupljenim uspješno druženje uz razmijene iskustava i znanja u svakodnevnom radu u području računalne sigurnosti.

Program jednodnevne konferencije obuhvatio je osam predavanja, a započeo je vrlo zanimljivim pogledom na umjetnu inteligenciju iz perspektive računalne sigurnosti koji je prezentirao Mackenzie Jackson iz *GitGuardiana* u predavanju pod nazivom „*The AI survival guide: Practical advice for stressed-out security workers*“.

Bojan Ždrnja iz Infiga u predavanju „*QUIC and Furious*“ predstavio je protokol QUIC, pojasnio zašto se koristi te pokazao na zanimljivim primjerima kako se taj protokol može upotrebljavati u dobre svrhe, a kako ga se koristi za zloupotrebu te što je potrebno poduzeti za pravovremeno otkrivanje ili čak sprječavanje tih zloupotreba.

Treće predavanje „*Malware and Cryptography*“ održao je Zhassulan Zhussupov iz *MSSP LABa* tijekom kojeg se bavio istraživanjima u području zaobilaženja AV rješenja i ulogom kriptografije u razvoju malwarea. Predstavio je primjenu klasičnih kriptografskih algoritama za enkripciju korisnih podataka i C2 komunikacije te prikazao praktičnu implementaciju i simulaciju APT napada.





Vlatko Košturnjak iz Diverta održao je predavanje na temu „*Linux improvements in memory corruption based protections*“ u kojem je predstavio nedavna poboljšanja Linuxa usmjerena na zaštitu od mogućih oštećenja memorije na razini hardvera i softvera.

U predavanju „*SIEM vs EDR: the fight for a holistic and combined approach*“ Michel de Crevoisier predstavio je različite postupke izbjegavanja EDR-a koje izvode napadači, pri čemu je naglasio nužnost holističkog i kombiniranog pristupa zajedno sa SIEM rješenjem kako bi se preduhitрили napadi koji postaju sve sofisticiraniji i lukaviji.

Alexander Peslyak iz *Openwalla*, poznatiji kao Solar Designer, predstavio je rezultate istraživanja koje je proveo za projekt Linux Kernel Runtime Guard (LKRG) u predavanju pod nazivom „*Linux kernel remote logging: approaches, challenges, implementation*“. LKRG je modul Linux kernela koji provodi provjeru integriteta kernela i otkriva iskorištavanje sigurnosnih ranjivosti protiv kernela.

U predavanju „*Showing Off Their SCILz: Sandworm Disrupts Power in Ukraine Using Novel Attack Against OT*“ Daniel Kapellmann Zafra iz *Google Mandianta* predstavio je detalje operacije tijekom koje je ruski Sandworm ciljao ukrajinsku organizaciju kritične infrastrukture slojevitim, razornim napadom koji je koristio novu tehniku za utjecaj na okruženja operativne tehnologije (OT) te je dao uvid u moguće posljedice budućih cyber fizičkih napada na temelju analize ovog i drugih OT događaja tijekom posljednjih nekoliko godina.

Program konferencije završio je predavanjem Davora Frkata iz *Bosch Engineeringa* na temu „*Automotive Security Challenges: Supplier's View*“ u kojem je predstavio pogled na sigurnosne prijetnje s gledišta dobavljača i pokazao kako automobilska industrija ubrzava upravljanje ranjivostima i incidentima, koči prijetnje u nastajanju i gura nove sigurnosne značajke i rješenja te s kojim se sve izazovima dobavljači susreću prilikom osvješćivanja proizvođača u automobilskoj industriji o potrebi uspostavljanja holističke sigurnosti sustava vozila.

BSides Zagreb neprofitno je događanje namijenjeno zajednici stručnjaka i entuzijasta informacijske sigurnosti, a organizira se s ciljem međusobnog upoznavanja, razmjene ideja i suradnje. Sudionici ove konferencije, bili oni profesionalci informacijske sigurnosti ili hakeri, sastaju se kako bi razmjenjivali ideje i znanja te raspravljali o aktualnim temama, trendovima i problemima u širokoj temi informacijske sigurnosti. BSides Zagreb održava se drugu godinu zaredom u organizaciji Sveučilišnog računskog centra Sveučilišta u Zagrebu.

Sveučilišni računski centar, Srce

web: <https://www.srce.unizg.hr/pressroom>

e-mail: [press@srce.hr](mailto:press@srce.hr)

