DIGITAL FORENSICS SWEDEN

Inom nätverket Digital Forensics Sweden, arbetar vi med att lägga grunden till en nationell kraftsamling för att bygga ett svenskt kompetenscentrum för Digital Forensik. Vi vill samla människor och organisationer som verkar för det goda samhället

Nyhetsbrev #1/24

The Digital Forensics Competence Center of Sweden

DIGITAL-FORENSICS.SE

Nyhetsbrev #1/April 2024

Innehåll

1. **Inledning**

Om 2023 var ett år då Digital Forensics Sweden verkligen syntes utåt, bland politiker både nationellt och inom EU, och rejält stärkte våra internationella kontaktytor och samarbeten, så har inledningen av 2024 varit minst lika intensiv för oss inom Digital Forensics Sweden;

- Heldag den 31/1 på temat ”AI Forensics” arrangerad i samarbete med svenska-centralamerikanska handelskammaren (SWECA) med 8 ambassadörer på visit i Linköping
- Slutarbete med partnerintervjuer och sammanställning av rapport
- Kontakt från SVT om medverkan i SVT Vetenskap, och intervju/inspelning under mars
- Ansökan till Vinnova Avancerad Digitalisering tillsammans med flera av er partner och Peace Park Foundation
- Ansökan om vidareuteckling av demonstratorn och deckargåtan ”Visual Crime Scene” i Norrköping tillsammans med NFC, EastSwedenGame, Intel, Lutra Interactive m fl. Tanken är att skapa en plattform för studier av nya forensiska verktyg och metoder i nära samverkan med forskare. Närmast vill vi koppla på språkmodeller och visualisering genom sk AI-enabled conversations.
- Föredrag för Intels globala AI-enhet
- Föredrag/Panelsamtal med SNS kring IT-säkerhet och digital forensik.
- Samtal med Regeringskansliet kring stärkt förmåga i händelse av beredskapsläge
- Förberedelser för ytterligare 3-4 projektansökningar under april.
- Slutrapportering av projekt med stöd av Region Östergötland
- Förberedelser för en work shop med Skatteverket och CyberCampus där vi hoppas få med fler partners i ytterligare ett nytt projekt.
- Onboarding av ett gäng nya partner i nätverket (Mycket välkomna!)
- Medverkan i Region Östergötlands uppstartade strategiarbete för regionala styrkeområden
- Nätverksträff on-line den 5/3, bl a med föredrag om aktuell rapport från Interpol
- Strategisk planering för långsiktig utveckling och finansiering av Digital Forensics Sweden

Och mycket annat! I detta nyhetsbrev återigen en krönika av vår egen professor i Digital Forensik, Stefan Axelsson vid Stockholms Universitet, samt lite rapport från våra doktorander.

Önskar er alla trevlig läsning, och hoppas på att se så många som möjligt i Norrköping den 7/12!

2. Aktuellt från nätverket

Framåt planerar vi för en fysisk träff, i Norrköping den 13/6 i samarbete med Cyberly, Cybersäkerhetsnätverket i Östergötland. Eventuellt hinner vi också med en on-line-träff innan dess.

Vi vill här också passa på att tipsa om en nyutgiven bok: *Artificial Intelligence (AI) in Forensic Science* (Geradts, Z., Franke, K., 2024, Wiley). Trevlig läsning!

3. Forskningsnytt

Våra bägge doktorander arbetar intensivt med skrivande. Johnny Bengtsson, doktorand på LiU och från NFC rapporter följande:

”Jag är just nu inne i en skriv- och bearbetingsprocess, men klurar även på hur det icke-invasivt går att injicera vilseledande (anti-forensiska) sensor- och aktuatordata i händelseloggningen hos fastighets- respektive hemautomationssystem. Syftet med detta är inte att visa på den praktiska möjligheten – vilket jag redan gjort tidigare – utan denna gång att tydliggöra varför det är så viktigt

att forensiskt ifrågasätta rimligheten i analyserad loggdata. Dessutom slipar jag på en metod som påvisar hur falska händelser skulle kunna detekteras genom dataöverlagring (sensorfusion).”

Kontakta gärna Johnny om ni vill diskutera hans forskning.

Doktoranden Johannes Olegård (Stockholm s universitet) berättar att han som bäst håller på med en spännande artikel. Så här skriver Johannes:

”Artikeln kommer att handla om "When is logging sufficient?"

Det vill säga: hur och var man ska logga för att göra sina IT-system mer "Forensically Ready" inför utredningar av cyberattacker. Förvånansvärt lite har forskats på den frågan [1] och det som finns har haft mer fokus på hur man kan reducera de loggar man redan har [2]. Min artikel är mer inriktad på om vi ens loggar rätt saker till att börja med och vad man teoretiskt borde logga istället. Det är ju lätt att som IT-forensiker se på loggar och andra bevis som en sorts "naturresurs" som ska "hanteras", men i verkligheten kan vi ju faktiskt påverka vad som genereras i förväg (jämför kravet på "spårbarhet" i SUA).

Arbetet är inte klart, men lite preliminärt kan man säga att det hänger främst på att förutsäga vilka forensiska frågor man kommer ställa under en utredning. Olika frågor kräver olika bevis. När det t.ex. gäller attribution (identifiera *vem* som har angripit, eller åtminstone när fel person använder ett konto), så är det svårt att göra annat än anomali detektering (t.ex. IBM QRadar's "User Behavior Analytics"). IT-system "ser" bara konton, inte personen bakom kontot---vilket så klart utnyttjas av angripare. Därmed kommer förmodligen AI förbli centralt i att besvara just den kategorin av utredningsfråga. Vilken data som behöver samlas in hänger då på vilken input (och träningsdata) till en sådan AI ska vara effektiv (i att minska falsk-larm, etc.).

I övrigt såg jag en intressant pre-print (som alltså får tas med en nypa salt) i en av min Google Scholar alerts här om veckan: https://arxiv.org/pdf/2402.01944.pdf . Den handlar om "bigger-picture problem" inom cybersäkerhet och jämför hur olika metoder faktiskt biter på dom. Det intressanta (se figur 2 i artikeln) är att de mer "flummiga" metoderna (t.ex. hotmodellering) och de mer manuella metoderna (t.ex. pentestning) tyvärr fungerar bättre på vissa viktiga problem än de mer teoretiskt starka metoderna (trusted computing, formal specification, etc.). Det ger lite perspektiv.

[1] E. L. Barse and E. Jonsson, “Extracting attack manifestations to determine log data requirements for intrusion detection,” in 20th Annual Computer Security Applications Conference, Dec. 2004, pp. 158–167. doi: 10.1109/CSAC.2004.20. Available: https://doi.org/10.1109/CSAC.2004.20

[2] N. Michael, J. Mink, J. Liu, S. Gaur, W. U. Hassan, and A. Bates, “On the Forensic Validity of Approximated Audit Logs,” in Annual Computer Security Applications Conference, Austin USA: ACM, Dec. 2020, pp. 189–202. doi: 10.1145/3427228.3427272.
Available: https://doi.org/10.1145/3427228.3427272

BR,
Johannes Olegård”

4. ”Utblick” - Gästkrönikör, Stefan Axelsson, Professor Digital Forensik, Stockholms universitet

Det var ett tag sedan nu vi fick lära oss termen 'APT' för "Advanced Persistent Threat". Från början så var det en diplomatisk omskrivning för Kina, innan man officiellt fick säga att Kina lade stor energi på informationsinhämtning (dvs spioneri) via internet. Så man kallade dem "advanced" eftersom de använde avancerande (dyra) metoder och var systematiska i sin inhämtning. Man kallade dem

"persistent" ihärdiga, eftersom de var just de. De gav aldrig upp utan opererade med militär disciplin. Om det inte gick att ta sig in på ett sätt så kom man till slut in på ett annat. Hur tråkigt det än var att pröva metoder som inte fungerade.

Idag så är det många nationer som mer eller mindre öppet använder dessa metoder; de man brukar nämna som stora är bl a Kina, Ryssland, Iran, Nordkorea, Arabstaterna, samt de lite nyare uppstickarna Pakistan och Indien. Vi har fått insikt i hur vissa av dessa opererar genom olika läckage (Snowden osv.) och reverse engineering.

Alldeles nyligen riktades dock återigen ljuset på just Kina eftersom de råkade ut för ett läckage i form av en s.k. informationsdump. En mängd dokument, 570 stycken, läcktes på internet med detaljer kring operationer och verktyg som används av Kina för att spionera både på omvärlden men även internt i Kina. Måltavlorna då är t ex de som kan knytas till stora protester mot Kinas regering, t ex i Hong Kong, de som protesterar i den muslimska regionen Kinjiang i västra Kina osv.

I katalogen över verktyg så hittar man mjukvara som hjälper agenter att t ex identifiera maskerade debattörer på externa sociala medieplattformar som X (Twitter), som hjälper till att bryta sig in i emailplattformar. Även hårdvara beskrivs t ex enheter som ser ut som batterier eller grenuttag, som agerar plattform för att knäcka WiFi-nätverk och agera ankarpunkt för vidare access till dessa.

Vad som är intressant och nytt här är att även Kina, som tidigare förlitade sig enbart på rent militära förband för den här verksamheten, gått samma väg som t ex Ryssland och nu använder privata företag för den här sortens uppgifter (I-Soon i det här fallet). Ryssland har t ex själva på senare tid nästan helt lagt ner sina egna enheter och använder idag nästan enbart kriminella organisationer. (Det finns tecken på att de ägs och drivs av chefer inom underrättelsetjänsten.) De har många fördelar; man behöver t ex inte betala deras lön, infrastruktur osv. under de tidsperioder man inte har uppdrag till dem. Istället finansierar de sig själva med olika typer av cyberbrottslighet (ransomware) mellan uppdragen från underrättelsetjänsten. De har också ofta redan penetrerat nätverk och verksamheter som man är intresserad av och kan rapportera om dessa och vad man hittar, mot en avgift naturligtvis, utan att man behöver lägga tid på att planlägga och genomföra dyra kampanjer. En mer kommersiell bottom up, snarare än myndighetsstyrd top-down inriktning mao.

Det är naturligtvis lite intressant att Kina, som ju definitivt hört till den senare gruppen, även inom detta området nu alltså sett fördelen med en mer kapitalistisk inriktning mot fri marknad med fria aktörer som arbetar lite mer på eget initiativ snarare än enbart på uppdrag uppifrån.

Men hur gör man forensik av allt det här då? Jo, de som spårar olika APT:er har tagit fram och publicerat ett ramverk som jag föreläser om i fortsättningskursen i digital forensik på Stockholms universitet, kallat MICTIC-ramverket. Det uttyds som följer:

M - Malware - Är det en del av en tidigare känd familj? Har man läckt språkinställningar, tidsstämplar, strängar, eller är man onaturligt bra på att tvätta bort alla sådana. (I det senare fallet så har vi CIAs manual som berättar i detalj hur man skall göra det, så det kan också vara en ledtråd.)

I - Infrastructure - Vilka servrar används för att exfiltrera data, vilka domännamn används, vilka länkar till webservrar används osv? Infrastruktur är kostsam att skaffa (oavsett om man hyr den eller använder sig av 5000 komprometerade Sydkoreanska kabelmodem, ett verkligt exempel) så man tenderar att återanvända den flera gånger för olika kampanjer.

C - Control Server - Dvs de servrar som ger kommandon till den malware man lyckats få i in målsystemet. Om man lyckas ta sig in i kontrollservrarna så kan man hitta källkod, styrprogram, loggar. I vissa fall så används de som informella VPN-ankarpunkter i fria, öppna internet i väst. Det är lockande för operatörer i länder där internetaccess är strikt kontrollerad. Man har instanser av operatörer som loggat in på sina egna gmail-konton osv. från kontrollservrar, något som naturligtvis kan leda till mycket intressant information.

T - Telemetry - Trafikanalys av information man inte kan bryta på annat sätt, t ex vilka arbetstider, käll IP-adresser, malwareversioner osv. Mina studenter brukar ofta påpeka att man ju skulle kunna arbeta mitt i natten, men tänker då inte på att det idag är stora professionella organisationer med, upp till, hundratals anställda som ligger bakom. Om man tvingar alla dessa att arbeta på en stor nationell helgdag så kommer man dels att ha en massa uppretade anställda på halsen, och dels bränna sin övertidsbudget på bara en operation. Så det är inte alls säkert att det är så lätt att förställa sig om man vid förstone kan tro. Folk vill ha ledigt på helgen, oavsett vem de arbetar för.

C - Cui Bono - Vem drar nyttan? Dvs man gör en geopolitisk analys av vem som kan tänkas vara intresserad av just denna informationen. När det kommer till Kina så kunde man för några år sedan t ex se en direkt koppling mellan vilka områden som premierades och lyftes fram som fokusområden i den senaste femårsplanen och vilka industrier som fick påhälsning av PLAs tredje/fjärde direktorat några månader senare. (De lär skall ha omorganiserat sig idag.)

Vissa av dessa signaler kan man maskera, eller ändra för att försöka kasta misstankarna på någon annan. Men även det senare går att använda i sin analys, under lång tid så var det populärt bland Indiska operatörer att försöka rikta misstankarna mot Pakistan (och vice versa), vilket var en indikation i sig. Och även om man kan påverka vissa av dessa, så är andra svårare och eftersom det är stora organisationer där inte alla drar jämt och åt samma håll så är det mera sällan man är helt konsekvent i sina försök att missleda, vilket naturligtvis också är en ledtråd.

Detta är naturligtvis ett område där det svänger fort, och signaler kommer och går, men jag tycker ändå att det är intressant att man publicerar sina metoder öppet så att utbildare som jag kan dela med mig av dem i klassrummet. Även de mest avancerade angriparna vi har på internet idag är inte perfekta, och deras angrepp är öppna för utredning, analys och tolkning.

Inte ens APT:erna går säkra för lagens långa arm, eller iaf inte för lagens långa pekande finger. Att få ett stadigt tag i kragen på dem för att kunna slänga dem i finkan, det har, av naturliga skäl, hittills visat sig svårare.

Källor:

* Attribution av APT:er
Attribution of Advanced Persistent Threats - How to Identify the Actors Behind Cyber-Espionage, Timo Steffens, Springer Verlag, 2020.

* Kina läckan, flera men AP har en bra sammanfattning som även citerar Recorded Future AP: An online dump of Chinese hacking document offers a rare window into pervasive state surveillance https://apnews.com/article/china-cybersecurity-leak-document-dump-spying-aac38c75f268b72910a94881ccbb77cb

Även Schneier har en blänkare med lite fler länkar: Schneier on Security - China surveillance company hacked - https://www.schneier.com/blog/archives/2024/02/china-surveillance-company-hacked.html

5. Nästa nätverksträff

Nästa nätverksträff blir ett fysiskt event den 13:e juni på Norrköpings VisualiseringscenterC. Det kommer då även att ges möjlighet att se Visual Crime Scene för de av er som missade detta i julas.

Och till sist, som alltid…Håll gärna ögonen öppna efter nyheter och material som kan relatera till vårt område, värt att tipsa varandra om. Skicka gärna tips till oss i nätverket så delar vi dessa. Länkar fungerar också.

Om Nyhetsbrevet

Nyhetsbrevet har ambitionen att vara kort och koncist och är tänkt att (i huvudsak) vara på svenska.
Vi välkomnar gästskribenter bland er läsare och partners, liksom tips om nyheter och viktiga händelser. Även det som händer på er egen horisont och som ni vill sprida kännedom om, har sin plats här, liksom länkar med tips på event eller texter om förestående produktlanseringar.

Redaktionen förbehåller sig rätten att redigera och förkorta texter liksom att välja vad som kommer med och inte sett till helhet och relevans. Vi tar förstås även gärna emot synpunkter på det som skrivs.

Nyhetsbrevet skickas till de som anmält att de vill vara mottagare av information från Digital Forensics Sweden, och det går bra att dela det vidare till kollegor i branschen. Önskar du inte längre ha nyhetsbrevet eller kallas till våra nätverksträffar, skicka ett meddelande till Niclas Fock (niclas.fock@ai.se) så stryker vi dina kontaktuppgifter ur vårt register.

Tipsa gärna kollegor i din organisation, eller kollegor i branschen så bygger vi ett större och starkare nätverk!

Länkar från 2023:

SVT-play med Johannes Olegård (höst 2023)
https://www.svt.se/nyheter/lokalt/stockholm/har-laser-it-forensikern-upp-en-mobil-pa-nagra-minuter--jwlmsq

SVT Svenska Nyheter med Stefan Axelsson (höst 2023)
https://www.svtplay.se/video/8WAWRv1/svenska-nyheter/fre-27-okt-22-00?id=j1axQ6D

Digital Forensik och AI i ViaPlay ”Efterlyst” 2023-03-09 (kräver inlogg på ViaPlay)
https://viaplay.se/player/default/serier/efterlyst/sasong-61/avsnitt-5

Video-inspelning från IVA-event januari 2023
https://www.iva.se/event/nya-digitala-mojligheter-for-kriminella--vad-kravs-for-att-stoppa-dem/
https://www.ai.se/en/events/can-we-use-digital-tools-combat-digital-crimes

Artikel från Linköpings Science Park om IVA-eventet i januari 2023
https://linkopingsciencepark.se/nya-digitala-mojligheter-for-kriminella-vad-kravs-for-att-stoppa-dem/

Digital Forensics Sweden, Artikel av Linköpings Universitet (2022)
https://liu.se/nyhet/ai-ett-viktigt-verktyg-i-jakten-pa-digitala-brottslingar

DFCC på Almedalen via EastSweden (2022):
https://www.youtube.com/watch?v=vx4I7oQZ5bA

Digital Forensics Sweden, vår egna siter:
https://www.digital-forensics.se
https://dfcc.se

Länkar till Nationellt Cybersäkerhetscentrum
https://www.ncsc.se/aktuellt/

https://www.ncsc.se/publikationer/

Tidigare event med koppling till digitala brottsplatser (Smart Twins):
https://www.youtube.com/watch?v=tibBOONDz0U