**ARPAE**

**Agenzia regionale per la prevenzione, l'ambiente e l'energia**

**dell'Emilia - Romagna**

*** * ***

**Atti amministrativi**

| | |
|---|---|
| Determinazione dirigenziale | n. DET-2022-48 del 20/01/2022 |
| Oggetto | Sistemi Informativi e Innovazione digitale. Approvazione schema di convenzione con il Dipartimento di Informatica - Scienza ed Ingegneria (DISI) dell'Università di Bologna relativamente al "Progetto tecnico RanFlood" |
| Proposta | n. PDTD-2022-52 del 20/01/2022 |
| Struttura adottante | Servizio Sistemi Informativi E Innovazione Digitale |
| Dirigente adottante | Cattani Stefano |
| Struttura proponente | Servizio Sistemi Informativi E Innovazione Digitale |
| Dirigente proponente | Dott. Cattani Stefano |
| Responsabile del procedimento | Cattani Stefano |

Questo giorno 20 (venti) gennaio 2022 presso la sede di Viale Silvani, 6 in Bologna, il Responsabile del Servizio Sistemi Informativi E Innovazione Digitale, Dott. Cattani Stefano, ai sensi del Regolamento Arpae per l'adozione degli atti di gestione delle risorse dell'Agenzia, approvato con D.D.G. n. 114 del 23/10/2020 e dell'art. 4, comma 2 del D.Lgs. 30 marzo 2001, n. 165 determina quanto segue.

**Oggetto: Sistemi Informativi e Innovazione digitale. Approvazione schema di convenzione con il Dipartimento di Informatica - Scienza ed Ingegneria (DISI) dell'Università di Bologna relativamente al "Progetto tecnico RanFlood"**

VISTE:
- la Legge Regionale n. 44 del 19/04/1995, che istituisce l'Agenzia Regionale per la Prevenzione e l'Ambiente dell'Emilia-Romagna, quale ente strumentale della Regione Emilia-Romagna preposto all'esercizio delle funzioni tecniche per la prevenzione collettiva e per i controlli ambientali, nonché all'erogazione di prestazioni analitiche di rilievo sia ambientale che sanitario;
- la Legge Regionale n. 13/2015 "Riforma del sistema di governo regionale e locale e disposizioni su città metropolitana di Bologna, province, comuni e loro unioni" che rinomina l'Agenzia Regionale per la Prevenzione e l'Ambiente (Arpa) dell'Emilia-Romagna istituita con L.R. 44/1995 in Agenzia Regionale per la Prevenzione, l'Ambiente e l'Energia dell'Emilia-Romagna (Arpae);

PREMESSO:
- che il 06/03/2020 è stato rinnovato per la durata di 5 anni il Protocollo d'intesa per la collaborazione su tematiche di comune interesse tra Arpae e Alma Mater Studiorum - Università di Bologna;
- che il suddetto Protocollo di Intesa prevede, all'art. 5, la possibilità di sottoscrivere singole specifiche convenzioni con l'Università per definire contenuti e modalità di collaborazione nell'ambito dell'attuazione dei progetti di ricerca;
- che finalità del predetto Protocollo è favorire e promuovere un continuo confronto tra le Parti per arricchire le rispettive linee di azione attraverso la promozione di forme di collaborazione nel campo della ricerca e della formazione, nonché dello scambio di esperienze per il raggiungimento di obiettivi di qualità totale nella produzione di servizi e nella promozione e gestione di ricerca ed innovazione attraverso progetti scientifici;
- che è interesse comune delle Parti favorire lo sviluppo della ricerca scientifica informatica, a beneficio della collettività;

CONSIDERATO:
- che l'Università di Bologna ha intenzione di favorire lo sviluppo della ricerca scientifica informatica, a beneficio della collettività;
- che Arpae Emilia-Romagna e il Dipartimento di Informatica Scienza ed Ingegneria (DISI) dell'Università di Bologna hanno dimostrato interesse in ordine alla sottoscrizione di una convenzione relativa al "Progetto tecnico RanFlood" a scopo di ricerca e collaborazione per qualificare e specializzare dipendenti impegnati in attività di elevata qualificazione, definendo gli ambiti di reciproca collaborazione;

RILEVATO:
- che il Progetto sarà svolto presso il Dipartimento di Informatica - Scienza e Ingegneria (DISI) e presso il Servizio Sistemi Informativi e Innovazione digitale di Arpae, secondo le modalità dettagliate nell'allegato tecnico "Progetto tecnico RanFlood" allo schema di convenzione sub A);
- che lo scopo della ricerca e della collaborazione segue due direzioni: quella metodologica, sull'esplorazione dei metodi che possono caratterizzare il contrasto dell'azione dei

ransomware tramite il flooding, e quella sperimentale, sull'efficacia empirica di possibili implementazioni dei metodi indagati, rispetto a diversi scenari reali di esecuzione (e.g., singoli terminali, piccoli network aziendali, etc.);
- che le attrezzature per l'esecuzione del progetto di proprietà di Arpae Emilia-Romagna sono concesse a titolo gratuito;
- che le Parti si impegnano a sostenere tutti gli oneri economici diretti e indiretti relativi al proprio personale e alle proprie strutture per far fronte alle attività tecniche e scientifiche relative allo svolgimento del progetto;
DATO ATTO:
- che le attività previste sono conformi alle attività istituzionali dell'Ente;
- che la convenzione di cui trattasi ha validità di tre anni anni dalla data di sottoscrizione;
- che non sussistono come da regolamento U.E n 2016/679 situazioni di trattamento dei dati personali;
SPECIFICATO:
- che il Responsabile del Servizio Sistemi Informativi e Innovazione di Arpae ha designato Simone Melloni quale responsabile di riferimento per Arpae, relativamente alla gestione del progetto di collaborazione dell'Unità Evoluzione dei Sistemi cloud e Saas;
RITENUTO:
- quindi opportuno che le Parti sottoscrivano uno schema di convenzione con il Dipartimento di Informatica - Scienza ed Ingegneria (DISI) allegato sub A) al presente atto quale parte integrante e sostanziale al fine di collaborare nell'esecuzione del progetto intitolato "RanFlood",
DATO ATTO:
- che Responsabile del Procedimento ai sensi della L. 241/90 è il Dott. Stefano Cattani, Responsabile del Servizio Sistemi Informativi e Innovazione Digitale di Arpae;

DETERMINA

1. di approvare lo schema di convenzione con il Dipartimento di Informatica - Scienza ed Ingegneria (DISI) dell'Università di Bologna, allegato sub A) al presente atto, per formarne parte integrante e sostanziale al fine di collaborare nell'esecuzione del progetto tecnico intitolato "RanFlood";
2. di dare atto che la presente convenzione, sottoscritta in data 13/01/2021 PG/2022/4852, avrà una durata di tre anni decorrenti dalla data di sottoscrizione;
3. di dare atto che il responsabile di riferimento relativamente alla gestione del progetto di collaborazione dell'Unità Evoluzione dei Sistemi cloud e Saas per Arpae è Simone Melloni;
4. che le Parti si impegnano a sostenere tutti gli oneri economici diretti e indiretti relativi al proprio personale e alle proprie strutture per far fronte alle attività tecniche e scientifiche relative allo svolgimento del progetto.

Il Responsabile del Servizio

Sistemi Informativi e Innovazione Digitale

Dott. Stefano Cattani

**CONVENZIONE AI SENSI DELL'ART. 15 DELLA LEGGE 7 AGOSTO 1990, N. 241**

TRA

**L'Agenzia Regionale per la Prevenzione, l'Ambiente e l'Energia dell'Emilia-Romagna, di seguito denominata anche ARPAE Emilia-Romagna,** con sede e domicilio fiscale in Bologna, Via Po 5, Codice Fiscale e Partita IVA n. 04290860370, legalmente rappresentata agli effetti del presente atto dal Responsabile del Servizio Sistemi Informativi e Innovazione Digitale Dott. Stefano Cattani;

E

**Alma Mater Studiorum - Università di Bologna**, con sede legale in Bologna (Italia), alla Via Zamboni n. 33, C.F. 80007010376, P.IVA n. 01131710376, attraverso il **Dipartimento di Informatica – Scienza e Ingegneria** con sede in Bologna (Italia), alla Via Mura Anteo Zamboni 7 - 40126, rappresentato dal Direttore del Dipartimento Prof. Maurizio Gabbrielli, autorizzato alla stipula del presente Contratto con delibera del Consiglio di Dipartimento del 19/04/2021;

d'ora innanzi, per brevità, collettivamente "le Parti"

**Premesso che:**

- il 06/03/2020 è stato rinnovato per la durata di 5 anni il Protocollo d'intesa per la collaborazione su tematiche di comune interesse tra Arpae e Alma Mater Studiorum - Università di Bologna;
- finalità del Protocollo è favorire e promuovere un continuo confronto tra le Parti per arricchire le rispettive linee di azione attraverso la promozione di forme di collaborazione nel campo della ricerca e della formazione sui temi del rapporto ambiente-salute, della tutela del mare, del cambiamento climatico, nonché dello scambio di esperienze per il raggiungimento di obiettivi

di qualità totale nella produzione di servizi e nella promozione e gestione di ricerca ed innovazione attraverso progetti scientifici;

- è interesse comune delle Parti favorire lo sviluppo della ricerca scientifica informatica, a beneficio della collettività;

Per quanto sopra premesso

**ART. 1**

**(Oggetto)**

Le Parti, così come sopra rappresentate, convengono di collaborare nell'esecuzione del progetto intitolato "RanFlood", allegato sub A) alla presente Convenzione (di seguito, per brevità, anche solo "Progetto").

Il Progetto sarà svolto presso il Dipartimento di Informatica - Scienza e Ingegneria (DISI) e presso Arpae-Servizio Sistemi Informativi e Innovazione digitale, secondo le modalità dettagliate nell'allegato tecnico "Progetto tecnico RanFlood".

Lo scopo della ricerca e della collaborazione segue due direzioni: quella metodologica, sull'esplorazione dei metodi che possono caratterizzare il contrasto dell'azione dei ransomware tramite il flooding, quella sperimentale, sull'efficacia empirica di possibili implementazioni dei metodi indagati, rispetto a diversi scenari reali di esecuzione (e.g., singoli terminali, piccoli network aziendali, etc.).

**ART. 2**

**(Descrizione del Progetto e scopo della collaborazione)**

RanFlood rappresenta il primo prototipo di una famiglia di soluzioni per il contrasto degli attacchi ransomware, una categoria di malware creati con l'obiettivo di estorcere un riscatto economico, sequestrando i file contenuti all'interno di un dispositivo.

La variante ransomware più comune, chiamata "crypto ransomware", una volta in esecuzione cifra i file presenti nel computer oggetto d'attacco grazie all'uso della crittografia, rendendoli inaccessibili a chiunque non abbia la chiave di decriptazione. Questa tipologia di attacco lascia operativa la macchina così da rendere possibile il ripristino dei dati, previo pagamento del riscatto per ottenere la chiave di decrittazione.

Le soluzioni "RanFlood", basate sul file flooding, seguono una metodologia innovativa che contrasta l'azione dei ransomware, contendendo l'accesso al disco ed inondandolo di file che il ransomware dovrà a sua volta criptare. Il contrasto è quindi su due fronti: nell'accesso al disco, che diventa più lento perché sia il ransomware sia il programma di contrasto cercano di scrivere sul disco in contemporanea; nella criptazione, da parte del ransomware, dei file appositamente prodotti dal programma di contrasto.

**ART. 3**

(**Attrezzature e modalità di svolgimento della collaborazione**)

Le attrezzature per l'esecuzione del progetto di proprietà di Arpae Emilia-Romagna sono concesse a titolo gratuito.

Sulle workstation dismesse e messe in disponibilità presso la sede di Via Po n. 5, Bologna, del Servizio Sistemi informativi e Innovazione digitale di Arpae sarà installato RanFlood. Una volta infettate in ambiente controllato con ransomware di tipi diversi, rappresentativi delle tipologie comuni, verranno misurati alcuni parametri di reattività ed efficienza del software, tra cui il numero di file salvati in relazione alle varie tipologie di funzionamento (flooding).

Alle attrezzature potranno avere accesso i ricercatori del Dipartimento di Informatica - Scienza e Ingegneria (DISI) ed il personale Arpae individuati dalle Parti, secondo le modalità concordate e riportate nell'allegato A) al presente Accordo.

Il personale delle rispettive Parti coinvolto nelle attività del Progetto nonché l'impegno previsto in termini di mesi/uomo sono indicati nell'allegato A) al presente Accordo.

Entrambe le Parti si impegnano a monitorare e valutare le attività oggetto della reciproca collaborazione.

**ART. 4**

**(Referenti)**

Il Direttore di Dipartimento e il Responsabile del Servizio Sistemi Informativi e Innovazione di Arpae designeranno, ciascuno per la propria competenza, un Responsabile di riferimento per la gestione del progetto di collaborazione.

**ART. 5**

**(Durata e recesso)**

La presente Convenzione decorrerà dalla data di sottoscrizione e avrà durata di tre anni, prorogabile mediante accordo scritto fra le Parti.

Qualora nel corso della durata del presente accordo venissero a modificarsi i presupposti relativi alla collaborazione tra DISI e Arpae o si ritenesse opportuno rivedere l'accordo stesso, le Parti definiranno, di comune intesa, le modalità per tale revisione.

Le Parti possono recedere prima della scadenza mediante comunicazione scritta da notificare con preavviso di almeno 30 giorni mediante posta elettronica certificata (PEC).

**ART. 6**

**(Oneri)**

Le Parti si impegnano a sostenere tutti gli oneri economici diretti e indiretti relativi al proprio personale e alle proprie strutture per far fronte alle attività tecniche e scientifiche relative allo svolgimento del progetto.

.

**ART. 7**

**(Assicurazione)**

Le Parti si danno reciprocamente atto che:

- i referenti dell'Università impiegati nello svolgimento delle attività indicate nel presente Progetto sono coperti da assicurazione dall'Università di Bologna contro gli infortuni che dovessero subire in qualsivoglia sede dette attività si svolgano, così come previsto ai sensi di legge, nonché con assicurazione per responsabilità civile verso terzi (persone e/o cose);
- il personale dipendente da Arpae impiegato nello svolgimento delle attività indicate nel presente Progetto svolge le proprie attività in orario di servizio ed è coperto da assicurazione di legge contro gli infortuni che dovesse subire in qualsivoglia sede dette attività si svolgano, nonché da assicurazione per responsabilità civile verso terzi (persone e/o cose).

**ART. 8**

**(Proprietà dei risultati e pubblicazioni)**

I risultati e la documentazione derivanti dalle attività svolte in esecuzione della presente Convenzione sono di proprietà di tutte le Parti che hanno contribuito a generarle, in quote da determinare in base al contributo intellettuale di ciascuna Parte. Le Parti potranno disporne

pienamente per lo svolgimento delle attività relative alle finalità istituzionali di ciascuna Parte (fra cui anche lo svolgimento di ricerca per conto di terzi o finanziata). L'eventuale sfruttamento economico dei risultati tramite accordi di licenza con terzi sarà regolato in un futuro contratto da negoziare in buona fede fra le Parti al fine di regolare la ripartizione degli utili e delle spese fra le Parti, anche in ragione delle rispettive quote di contitolarità. Sono in ogni caso fatti salvi i diritti morali degli autori.

La Parte che intende pubblicare procederà alla trasmissione della bozza della pubblicazione e/o della presentazione, almeno 30 (trenta) giorni prima dell'invio della stessa a soggetti terzi, affinché si possa tenere conto dell'eventuale possibilità di procedere allo sfruttamento economico o alla protezione dei risultati stessi mediante diritti di proprietà intellettuale o industriale. Nelle eventuali pubblicazioni si dovrà esplicitamente far riferimento alla presente Convenzione e dovrà essere possibile distinguere in maniera chiara e inequivocabile tra dati ufficiali già sottoposti a processo di validazione e dati passibili di future modeste variazioni a seguito del completamento del processo di validazione.

Le Parti declinano ogni responsabilità per un uso improprio dei dati forniti.

## ART. 9

## (Spese e oneri fiscali)

La presente Convenzione è soggetta a registrazione solo in caso d'uso ai sensi dell'art. 4, Tariffa Parte II, D.P.R. 131/1986 a spese della Parte richiedente, ed è inoltre soggetta ad imposta di bollo ai sensi dell'art. 2 – Tariffa Parte I del D.P.R. 642/1972, a carico dell'Università di Bologna e di Arpae in parti uguali. Al versamento all'Erario provvederà l'Università in modalità virtuale (autorizzazione n. 14038 del 13/12/2018).

**ART. 10**

**(Norme applicabili)**

Per quanto non espressamente disposto nella presente Convenzione, troveranno applicazione le norme del Codice Civile.

**ART. 11**

**(Foro competente)**

Tutte le controversie che dovessero insorgere in merito alla formazione, conclusione ed esecuzione della presente Convenzione sono devolute alla giurisdizione esclusiva del Tribunale Amministrativo Regionale competente.

Il presente Accordo è sottoscritto in forma digitale in un unico originale ai sensi dell'art. 24, commi 1 e 2 del D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale).

Per ARPAE:

Il Responsabile del Servizio Sistemi Informativi e Innovazione Digitale, Dott. Stefano Cattani (firmato digitalmente)

Per il Dipartimento di Informatica -Scienza e Ingegneria, Alma Mater Studiorum - Università di Bologna:

il Direttore, Prof. Maurizio Gabbrielli (firmato digitalmente)

**Allegato 1 Progetto tecnico RanFlood**

Responsabili

Servizio Sistemi informativi e Innovazione digitale - Agenzia Regionale per la Prevenzione, l'Ambiente e l'Energia dell'Emilia-Romagna (ARPAE): Simone Melloni; Stefano Cattani.

Dipartimento di Informatica - Scienza e Ingegneria, Università di Bologna (UNIBO): Saverio Giallorenzo; Marco Prandini.

Oggetto della collaborazione

La collaborazione nasce tramite Giallorenzo e Melloni, come co-ideatori di una metodologia, denominata RanFlood, di contrasto ai danni informatici generati dalla diffusione di ransomware (software di criptazione dati sotto riscatto).

La collaborazione ha una durata stimata di 3 anni.

Sono previste le seguenti fasi di implementazione:

1° anno, prototipazione e test iniziali;

2° anno, completamento e test estensivi;

3° anno, test in situ e sviluppi futuri.

L'oggetto della collaborazione è la definizione, lo sviluppo e il testing in vari scenari di decorso dell'attacco (singole postazioni, reti miste e cluster di calcolo) di uno strumento di rilevamento e contrasto alla diffusione di ransomware basato su RanFlood.

Parte del lavoro sarà volto alla divulgazione dei risultati scientifici.

Stima tempo/uomo semestrale

- UNIBO
- 120h tempo-uomo diviso tra:
- 1 dottorando

- 1 assegnista di ricerca,
- 1 ricercatore a tempo determinato
- 1 ricercatore a tempo indeterminato
- ARPAE
- 24h tempo-uomo assegnate a 1 collaboratore tecnico-professionale
- Hardware:
- alcune workstations in dismissione (PC + Monitor + tastiera e mouse)
- Switch (8 porte per mettere in comunicazione le workstation)
- Connessione dati (scheda SIM + telefono o access point)

Tempi e modalità di accesso ai locali

L'accesso ai locali messi a disposizione da Arpae-Servizio Sistemi informativi e Innovazione digitale è consentita previa registrazione in entrata e in uscita dei referenti DISI coinvolti nello svolgimento del Progetto.

La fascia orario di accesso ai locali è così regolamentata:

da lunedì a venerdì dalle ore 9:30 / 17:00 previa comunicazione e-mail.

I frequentatori si impegnano a tenersi costantemente aggiornati e ad osservare le norme nazionali e regionali per la prevenzione e la gestione della situazione di emergenza da Covid-19 e più in generale le disposizioni in materia di prevenzione e protezione dei lavoratori sui luoghi di lavoro. Gli stessi si impegnano a rispettare rigorosamente le indicazioni dei protocolli di sicurezza che Arpae Emilia-Romagna ha predisposto e che saranno loro illustrate, nonché a collaborare con il personale dell'Agenzia ottemperando alle indicazioni eventualmente impartite.

Descrizione dettagliata del progetto di ricerca

Ransomware

I ransomware sono una categoria di malware creati con l'obiettivo di estorcere un riscatto (dall'inglese "ransom") economico sequestrando i file contenuti all'interno di un dispositivo.

La variante meno pericolosa e meno diffusa di ransomware è quella dei "locker ransomware" i quali, bloccano l'accesso alla macchina infettata, lasciando intatti i dati all'interno. Rimuovendo il malware o accedendo ai dati senza passare dal sistema operativo infettato, è tipicamente possibile recuperarli, rendendo vano qualsiasi tentativo di riscatto. Motivo per il quale questa variante è meno diffusa.

La variante più comune viene chiamata "crypto ransomware" che, una volta in esecuzione, grazie all'uso della crittografia, cifra i file presenti nel computer della vittima, rendendoli inaccessibili a chiunque non abbia la chiave di decriptazione giusta. Questa tipologia di attacchi tipicamente lascia operativa la macchina della vittima, così da rendere possibile, previo pagamento del riscatto per ottenere la chiave di decrittazione, il ripristino dei dati.

Al termine della crittazione dei dati, il ransomware mostra all'utente un messaggio di allarme, specificando i termini del riscatto e un limite temporale massimo entro cui è possibile pagare per ottenere la chiave di decrittazione. Alla scadenza di tale limite, nella maggior parte dei casi, il riscatto viene aumentato, minacciando di eliminare la chiave di decrittazione, rendendo quasi impossibile il futuro recupero dei dati (tramite metodi che cercando di indovinare tale chiave).

### Statistiche e attualità

Il primo ransomware passato alla storia è l'AIDS Trojan che nel 1989, distribuito tramite floppy-disk e che criptava solamente il nome dei file. Questo non si diffuse molto e presto si ebbero gli strumenti necessari per decriptare i file. I ransomware come li conosciamo oggi giorno, iniziarono a comparire dal 2005, con Trojan.Gpcoder, che usava una crittografia simmetrica (relativamente facile da decifrare) e che veniva trasmesso tramite allegati all'interno di email. Successivamente, si diffusero altri ransomware come Trojan.Cryzip, che sequestra i file in archivi protetti da password. Nel 2007 emerse il primo locker ransomware in Russia. Più tardi, nel 2013, si registrò la comparsa di uno dei più famosi ransomware: CryptoLocker. Questo malware usava la crittografia asimmetrica RSA. La vittima doveva pagare entro 72 ore un riscatto (circa 100$, in una valuta elettronica chiamata BitCoin), pena l'eliminazione della chiave privata per recuperare tutti i file o l'aumento del riscatto —passando circa dai 2000$ ai 20.000$, a novembre 2013. Alla fine del 2015 l'FBI ha stimato che le vittime pagarono 27.000.000$ ai creatori di CriptoLocker. Nel 2016 si registrarono i primi attacchi realizzati usando script nel browser (Javascript), che garantiva la possibilità di attacchi a diverse piattaforme. Inoltre, nello stesso anno, venne registrato il primo Ransomware-as-a-Service, uno strumento che permette l'acquisto di un ransomware i cui proventi vengono condivisi con i creatori. Alcuni di questi servizi sono Shark e Cerber, quest'ultimo con guadagni di almeno 200.000$ al mese. L'anno successivo venne scoperto un altro dei più famosi ransomware: WannaCry, che sfruttava la falla nei sistemi Windows,

conosciuta come EternalBlue, per infettare i computer non aggiornati. Il riscatto previsto era tra i 300$ e i 600$. WannaCry infettò più di 150 paesi attaccando privati, aziende, governi ed ospedali. Successivamente, un altro importante attacco è quello avvenuto in Ucraina nel 2017 da parte di NotPetya, una variante del ransomware Petya, rilasciato l'anno precedente. Questo attacco fu sferrato con lo scopo non tanto di ottenere un ritorno economico, quanto quello di causare il blocco delle strutture attaccato, dato che, anche in caso di pagamento del riscatto, nessun file poteva essere recuperato. Il settore mobile non è escluso a questo tipo di malware. I cyber-criminali hanno sviluppato dei ransomware che riescono a bloccare l'accesso ai dati all'interno di uno smartphone. Uno di questi è Doublelocker, scoperto nel 2017, diffusosi principalmente come una falsa copia di Adobe Flash Player. Questo ransomware cambia il PIN di accesso allo smartphone, mettendone uno casuale e sconosciuto. Se il riscatto viene pagato, allora l'attaccante può remotamente resettare il PIN. Anche il campo dell'Internet of Things (piccoli dispositivi come sensori e attuatori presenti dell'automazione domotica fino all'Industria 4.0) è minacciato dai ransomware.

Guardando le statistiche aggregate, raccolte dal sito web SafetyDetectives.com[1]—che considera dati provenienti da Beazely, CyberEdge, Datto, Deep Instinct, Europol, Herjavec Group, ITRC, Kaspersky, e Malwarebytes—, il quadro attuale degli attacchi ransomware è tutt'altro che rassicurante. Si stima infatti che, nel 2021, l'impatto sul mercato sarà di 20 miliardi di dollari.

Impatto dovuto in parte al costo del riscatto, mediamente attestato a 6.000 $, che è cresciuto mediamente quasi del doppio rispetto a 4 anni, fa creando notevoli disagi economici alle aziende più piccole.

All'impatto economico diretto, causato dal riscatto, vanno aggiunti i disservizi causati dal malware e la relativa inattività e improduttività. Questi, a volte, provocano danni di gran lunga più consistenti dei riscatti, arrivando ad essere stimati mediamente nel 2021 a **380.000 $** per attacco.

1 https://web.archive.org/web/20201123225536/https://it.safetydetectives.com/blog/ransomware-fatti-tendenze-e-statistiche-del/

Il mezzo di contagio prediletto rimane l'email (spam e phishing). Al secondo posto abbiamo le falle nella sicurezza. Al terzo posto troviamo le password deboli. Da questa classifica, si evince che numerosi utenti vengono ancora ingannati dalle truffe di ingegneria sociale e che non siano formati sulle basilari regole di sicurezza.

Inoltre l'85% dei fornitori di servizi gestiti (MSP) afferma che il sistema operativo Windows viene preso di mira più frequentemente dagli attacchi ransomware. Questo perché i computer basati su Windows sono solitamente più diffusi. Inoltre, parecchi utenti non installano gli aggiornamenti necessari del sistema operativo, lasciandoli le necessarie contromisure che proteggono da questi virus. Il dato, ovviamente, si aggiungere a quello di altri sistemi operativi come macOS e Linux, ma anche quelli sempre più diffusi di tablet e smartphones: Android e iOS.

Considerando che per mettere fuori gioco un'intera azienda è sufficiente un dispositivo infetto che cripti i documenti condivisi su un server o un disco condiviso di rete, il problema dei ransomware risulta prepotentemente attuale.

### RanFlood

Le tecniche basate su file flooding rappresentano una famiglia di strumenti per il contrasto degli attacchi ransomware, che seguono una metodologia innovativa che contrasta l'azione dei ransomware affrontandoli sullo stesso campo di battaglia: l'accesso e la modifica dei file su disco.

Il principio di base è semplice: un ransomware deve accedere ai file presenti su disco per poterli criptare. Le soluzioni basate su file flooding hanno come denominatore comune il fatto di contendere l'accesso al disco da parte del ransomware e di inondarlo di file che il ransomware dovrà criptare a sua volta. Il contrasto è quindi su due fronti: 1) l'accesso al disco, che diventa più lento perché sia il ransomware che il programma di contrasto cercano di scrivere sul disco in contemporanea e 2) il ransomware viene impegnato nel criptare i file appositamente prodotti dal programma di contrasto.

RanFlood rappresenta il primo prototipo di tale famiglia di soluzioni basate sul file flooding. Tale soluzione, totalmente innovativa nel settore, rappresenta un modo semplice ed efficace per rallentare l'azione di questi malware, permettendo quindi di guadagnare tempo per avvertire l'utente di quanto in corso, eventualmente scattare un'istantanea della memoria, ma comunque spegnere la macchina così da fermare l'attacco. RanFlood realizza la mitigazione sfruttando i seguenti fattori:

- Inondazione di file: RanFlood inizia ad inondare il file system della vittima con file ``esca". Lo scopo è quello di far cifrare tali file a discapito di quelli contenenti dati sensibili;

- Riempimento della memoria: La creazione di molti file permette di riempire la memoria principale così da rallentare ulteriormente il ransomware;

- Generazione di processi: La generazione di più processi è un altro fattore molto importante che causa un notevole rallentamento del malware.

Lo scopo di RanFlood è quello di "inondare"' le cartelle dei dischi attaccati con dei file, affinché il ransomware venga impegnato nel criptare quest'ultimi, oltre ad essere rallentato dalla scrittura

simultanea, sul disco, di molti file. Si suppone che il flooding inizi su una determinata cartella del sistema e da lì effettui l'inondazione su tutte le altre cartelle.

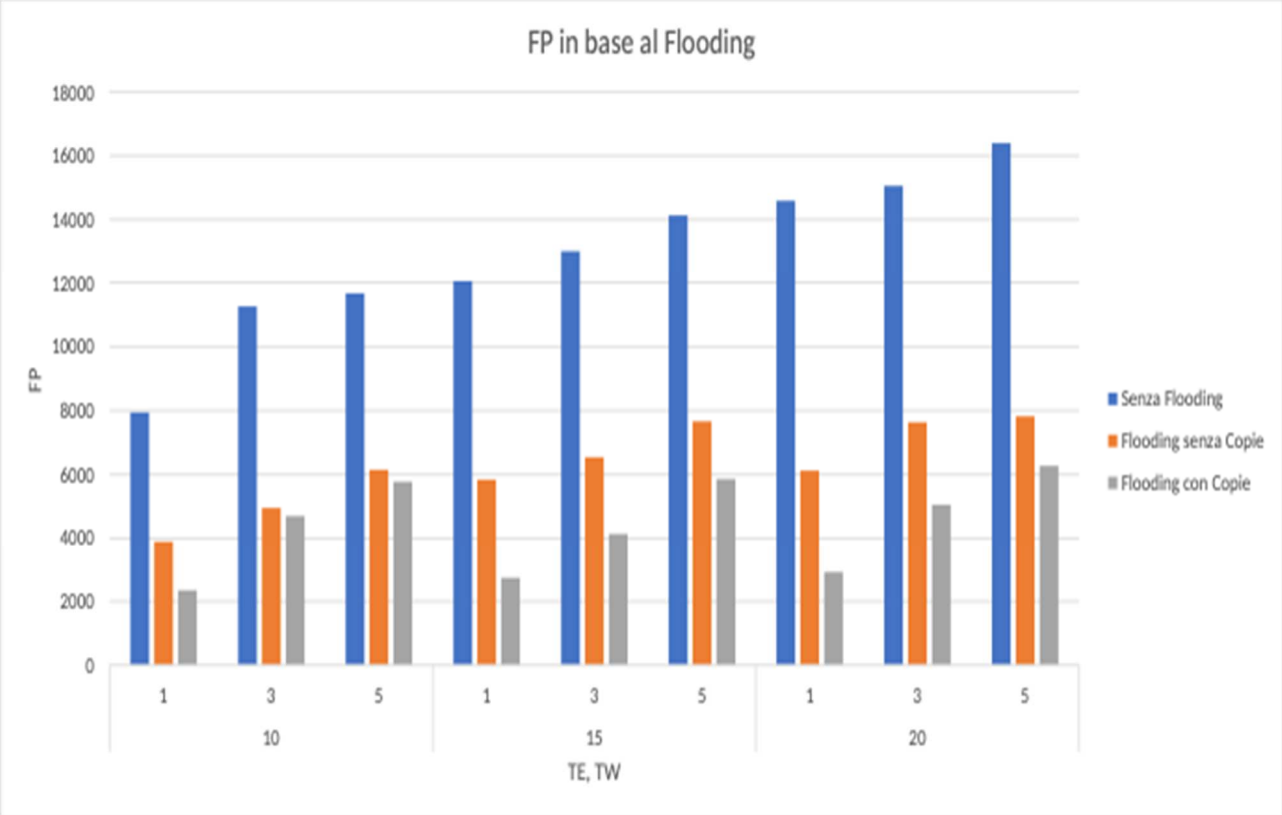
Il programma di flooding è stato realizzato come segue:

- viene letta la cartella dove è stato messo in esecuzione, per ogni file all'interno di questa cartella si controlla se ci sono altre cartelle;
- per ogni directory incontrata si genera una copia del programma avente come cartella di partenza tale directory;
- quando è terminata la prima scansione, si avvia la procedura di flooding sulla cartella corrente.

L'esecuzione del programma termina solamente grazie ad un intervento esterno, poiché il flooding verrà arrestato solamente quando l'utente si accorgerà di essere vittima di un ransomware e adotterà la soluzione più semplice e suggerita di spegnere la macchina.

Sul principio di quanto sopra, RanFlood mette in campo tecniche che permettono di inondare il disco di copie di file dell'utente, così che, anche se i file originali vengono criptati, si continuano a generare delle copie, svolgendo una funzionalità simile a quella di un backup.

Un prototipo di RanFlood è stato oggetto di sviluppo all'interno della tesi triennale di uno studente in Ingegneria Informatica presso l'Università di Bologna—Loris Onori, ora studente magistrale in Ingegneria Informatica presso lo stesso ateneo, incluso nella presente collaborazione. I risultati pratici, riportati in forma grafica sotto, sono promettenti: i file persi senza la protezione di RanFlood (rappresentati dalla colonna blu) sono molti di più di quelli persi con RanFlood senza copia (colonna arancione) e ancora meno quelli persi con la protezione con copia (colonna grigia).




Scopo della ricerca e della collaborazione

Visti gli interessanti risultati prodromici eseguiti da Loris Onori, si è pensato di consolidare tali risultati attraverso lo sviluppo di un prototipo avanzato e di una sperimentazione in ambiente reale (al contrario dei test precedenti, eseguiti in ambienti virtualizzati).

Lo scopo della ricerca e della collaborazione segue due direzioni. Quella metodologica, sull'esplorazione dei metodi che possono caratterizzare il contrasto dell'azione dei ransomware tramite il flooding. Quella sperimentale, sull'efficacia empirica di possibili implementazioni dei metodi indagati, rispetto a diversi scenari reali di esecuzione (e.g., singoli terminali, piccoli network aziendali, etc.). A tal fine verranno utilizzate delle workstation dismesse che sono state utilizzate operativamente in Arpae fino a poco tempo fa. Su tali workstation sarà presente RanFlood e una volta infettate (in ambiente controllato) con ransomware di tipi diversi (rappresentativi delle tipologie presenti nel campo)

verranno misurati alcuni parametri di reattività ed efficienza del software, tra cui il numero di file salvati in relazione alle varie tipologie di funzionamento (flooding).

Si riporta di seguito il dettaglio delle attività della collaborazione:

RANFLOOD (metodologia e metodi)

- versione alpha di RanFlood con feature freeze
  - versione installabile
- esplorazione metodologica e implementazione dei metodi di flooding:
  - random flood - file con contenuto random, nei formati più "bersagliati" dai ransomware
  - duplicate flood - doppioni di file già presenti, possibili varianti:
    - on-the-fly: RanFlood fa copie di file presenti nella directory attaccata. Pro: piccolo impatto sull'uso di memoria. Cons: Probabilmente meno file "recuperati" rispetto a shadow-copy;
    - shadow-copy: RanFlood fa copie di file validi da snapshot salvati in precedenza — più file "recuperati" rispetto a on-the-fly ma occupazione di memoria (ma parametrizzabile), necessità di definire politiche di scelta dei file da salvare rispetto al parametro di memoria (e.g., file aperti più spesso, più di recente, tags dell'utente, etc).

SPERIMENTAZIONE

- selezionare le famiglie di ransomware da testare
- definire le specifiche dei benchmarking scenarios:
  - Single desktop
    - Windows (definire versione (7,8,10) e tipo (Home, Pro, Server)
    - Linux (definire distribuzione (Debian, RedHat) e specifiche (Kernel 4, 5)
    - Definire se includere MacOs nei benchamarks (definire che versione (10.11, 10.12, 11.1)

- Small network
  - Linux cluster, 1 server, 2 clients (si applicano le definizioni del single desktop per Linux)
  - Windows cluster, 1 server, 2 client (si applicano le definizioni del single desktop per Windows)
- definire il protocollo di testing
  - come avviene l'installazione di RanFlood
  - come viene configurato (quali parametri) RanFlood
  - quanti parametri hanno gli scenari
    - quanti files
    - di che tipo e in che proporzione
    - distribuiti dove (e come, con che funzione di distribuzione)
    - di che "peso" (small, medium, large, con che funzione di distribuzione)
    - su che file systems (NTFS, FAT, ext2-3-4)
    - su che tecnologia (SSD, HDD)
    - su che interfaccia (SATA, RAID, USB, IDE)
    - quanto/i tempo/i viene data a una run di test
    - quanto/i delay viene dato a RanFlood prima di intervenire in una run di test
    - quante run per ogni scenario
    - definire le metriche recuperate per ogni run (e.g., file-retrieval rate)
    - che metadati collezioniamo sulle statistiche (e.g., standard deviation)