Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
www.melani.admin.ch

Minacce attuali su Internet, autori, strumenti, perseguimento penale e Incident Response

Reto Inversini, scuola universitaria professionale bernese,
in cooperazione con Roman Hüssy.

19. gennaio 2012

Contenuto

Prefazione

Il documento si rivolge a persone incaricate della protezione di infrastrutture e di informazioni elettroniche. In una prima parte sono illustrate succintamente le minacce attualmente esistenti, le modalità della loro classificazione e gli autori che si celano dietro tali minacce. In una seconda parte sono spiegati gli elementi di base per l'istituzione di un CSIRT/CERT (Computer Security Incident Response Team / Computer Emergency Response Team). L'ultimo capitolo spiega con quali mezzi le autorità di perseguimento penale potrebbero intervenire contro le reti bot.

Minacce

Le minacce in provenienza da Internet e alle quali sono esposti Governi, imprese e persone private sono molteplici. Una loro categorizzazione grezza può essere illustrata in forma di piramide.

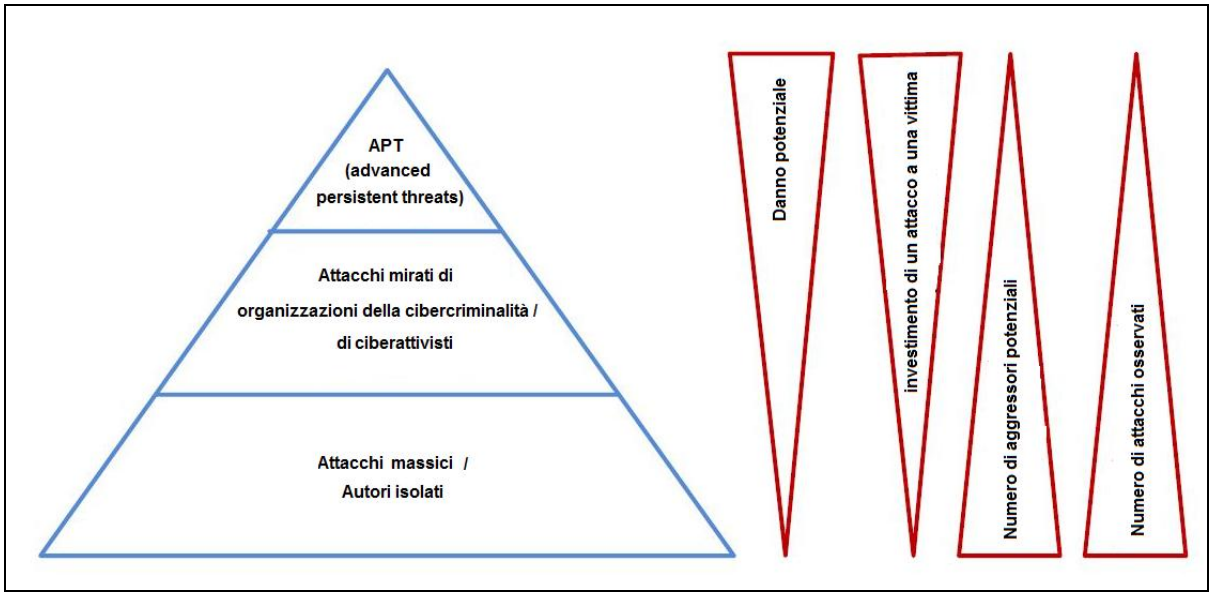

Figura 1: Piramide delle minacce, adattata da sans.org

Al vertice della piramide figura la minaccia più temuta, ovvero l'APT (Advanced Persistent Threat). Questa minaccia provoca un danno molto ingente, che si ripercuote sulla singola organizzazione o su un Paese. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di notevoli risorse. L'obiettivo dell'aggressore è di rimanere il più a lungo irreperibile, di stabilirsi sulla rete della vittima e di derubare le informazioni che ritiene interessanti per sé stesso. In considerazione delle esigenze elevate in fatto di risorse non esistono molti aggressori potenziali. Sono comunque noti diversi esempi di attacchi riusciti della categoria ATP (ad es. Aurora / attacco a Google).

Nel mezzo della piramide si situa la categoria dei cibercriminali e dei ciberattivisti. Anche se dispongono di risorse sensibilmente inferiori, la loro minaccia non va sottovalutata. In genere la tenacia di questi aggressori è minore di quella degli APT. In merito va constatato che le frontiere tra cibercriminalità e APT sono fluttuanti. Occorre in particolare partire dal presupposto che i servizi segreti hanno senz'altro accesso alle infrastrutture dei criminali e

possono se del caso procurarsi molto semplicemente tale accesso. Inoltre è anche possibile affidare incarichi a simili organizzazioni per contrastare con successo ogni partecipazione in caso di scoperta. Il livello più basso della piramide è costituito dagli attacchi massicci e dagli autori isolati. La minaccia dovrebbe essere presa sul serio per il solo fatto dell'enorme quantità di simili attacchi nonostante le risorse limitate che vengono utilizzate per perpetrarli. Anche in questo caso la frontiera verso il livello superiore è permeabile, dato in particolare che gli attacchi massicci sono sovente effettuati o perlomeno commissionati da organizzazioni cibercriminali.

Classificazione degli aggressori

Gli aggressori sono classificati qui di seguito in funzione delle loro possibilità e motivazioni. Ciò consente di accertare quali obiettivi, con quali risorse e con quanta tenacia gli aggressori potrebbero perseguire. In merito va rilevato che si tratta di un'approssimazione grezza.

Servizi segreti – advanced persistent threats

Nome	Servizi segreti / Organizzazioni statali / Advanced Persistent Threat
Descrizione	Un'organizzazione governativa può intervenire essa stessa come aggressore oppure commissionare l'attacco. L'obiettivo è in genere volto al procacciamento di informazioni (spionaggio classico o spionaggio industriale). In caso di crisi o di intensificazione delle tensioni possono essere oggetto di attacco anche le infrastrutture critiche oppure possono essere messe in circolazione in maniera mirata informazioni false.
Motivazione	Procacciamento di informazioni, perturbazione delle infrastrutture critiche, informazioni false.
Risorse tecniche	Occorre partire dal presupposto che tutto ciò che è tecnicamente fattibile può essere effettuato anche da un'organizzazione governativa. Le risorse sono molto elevate, mentre sono disponibili o possono essere reclutati specialisti per ogni possibile attività
Risorse finanziarie	Illimitate, perlomeno finché il risultato dell'attacco è giustificato nell'ottica dell'aggressore.
Razionalità del modo di procedere	Elevata.
Tenacia	Elevata.
Punti di partenza per la difesa	Classificazione dei dati, sistemi ben protetti. Isolamento da Internet di zone della rete

	contenenti dati delicati. Autorizzazione di accesso unicamente sulla base di Least Privilege.
Punti di partenza per il perseguimento	Analisi del malware utilizzato, stretta collaborazione con altri organismi di polizia e con metodi di intelligence. Monitoraggio del traffico di rete in entrata e in uscita.
Capacità di resistenza al perseguimento penale	Molto elevata.
Obiettivi probabili di attacco	• Sistemi con informazioni degne di protezione. • Informazioni critiche. • Sistemi di persone chiave o di responsabili decisionali. • Accessi secondari a sistemi non appariscenti, che possono essere scoperti solo difficilmente. • Attacchi frequenti alla confidenzialità e all'integrità dei sistemi. • Attacchi mirati alla confidenzialità e all'integrità dei sistemi. • Attacchi DDoS in caso di forti tensioni politiche o di crisi. Nella maggior parte dei casi questi attacchi sono però eseguiti da organizzazioni parastatali o da organizzazioni non statali con il tacito consenso di uno Stato o su suo mandato. • Infrastrutture critiche.

Ciberattivisti

Nome	Ciberattivisti
Descrizione	I ciberattivisti protestano con mezzi digitali contro le decisioni di Governi o di imprese che non coincidono con gli ideali degli aggressori. Esempi di siffatti gruppi sono Anonymous o LULZ. In questa sede sono esaminati soltanto i mezzi illegali, nel senso di una chiara delimitazione rispetto alla protesta digitale – importante e autorizzata – effettuata con mezzi legali.
Motivazione	Il motivo primario consiste nel diffondere un messaggio, attirare l'attenzione e/o arrecare un

	danno all'obiettivo dell'attacco.
Risorse tecniche	Le risorse e capacità tecniche variano fortemente. Nel caso di grandi azioni con un grado elevato di attenzione queste risorse possono nondimeno raggiungere notevoli dimensioni (ad es. in occasione degli attacchi nel contesto dei dispacci delle ambasciate US su Wikileaks).
Risorse finanziarie	Limitate. Dato però che queste attività avvengono in genere su base volontaria, questa circostanza non è di grande rilievo per l'aggressore.
Razionalità del modo di procedere	Da bassa a media. Dipende dalla forma organizzativa del gruppo.
Tenacia	Media.
Punti di partenza per la difesa	Sistemi ben protetti. Protezione dell'integrità di sistemi con grande visibilità. Preparazione agli attacchi DDoS, approntamento di tool e infrastrutture corrispondenti (ad es. zona di quarantena).
Punti di partenza per il perseguimento	Collaborazione con gli organismi di polizia come pure con l'intelligence. Identificazione dei coautori; sovente basta mostrare che gli atti sono punibili per indebolire un attacco.
Capacità di resistenza al perseguimento penale	Media
Obiettivi probabili di attacco	• Sistemi con grande visibilità / attenzione. • Gli attacchi sono sovente diretti contro la disponibilità e in parte contro l'integrità (deturpamento di siti Web)

Organizzazioni cibercriminali – attacchi mirati

Nome	Organizzazioni cibercriminali – attacchi mirati
Descrizione	Le organizzazioni cibercriminali possono eseguire attacchi mirati che si approssimano a un advanced persistent threat. Possono attaccare organizzazioni statali o private nell'intento di procacciarsi informazioni da poter rivendere o da sfruttare a proprio vantaggio. Ne sono obiettivo frequente le transazioni finanziarie. Un buon esempio è quello degli attacchi al registro

	nazionale del CO_2 all'inizio del 2011[1].
Motivazione	L'obiettivo primario è di carpire e di rivendere dati (spionaggio industriale) o di sfruttare transazioni finanziarie per scopi propri.
Risorse tecniche	Da medie e elevate, a seconda dell'organizzazione.
Risorse finanziarie	Da medie e elevate, a seconda dell'organizzazione.
Razionalità del modo di procedere	Elevata.
Tenacia	Media.
Punti di partenza per la difesa	Sistemi ben protetti. Isolamento da Internet di zone della rete contenenti dati delicati. Autorizzazione di accesso unicamente sulla base di Least Privilege. Monitoraggio del traffico di rete in entrata e in uscita.
Punti di partenza per il perseguimento	Analisi del malware utilizzato, stretta collaborazione con gli organismi di polizia competenti e l'intelligence. Osservazione delle organizzazioni cibercriminali attuali.
Capacità di resistenza al perseguimento penale	Da media e elevata. Il perseguimento penale perturba comunque le attività degli aggressori, ragione per la quale essi tentano di rimanere sotto il radar delle autorità di perseguimento penale.
Obiettivi probabili di attacco	• Sistemi con informazioni confidenziali che hanno un forte valore di rivendita. • Sistemi con informazioni finanziarie.

Organizzazioni cibercriminali – attacchi non mirati

Nome	Organizzazioni cibercriminali – attacchi non mirati
Descrizione	Questa è la forma classica di cibercriminalità. Gli aggressori tentano di procurasi un utile finanziario dall'attacco alle apparecchiature dell'utente finale. Essi tentano di procurarsi dati di accesso, di commettere estorsioni tramite attacchi DDoS o di inviare spam avvalendosi delle apparecchiature infettate. Il metodo prescelto è sovente costituito

[1] vedi MELANI rapporto semestrale capitolo 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=it

	da Crimeware Kit per mezzo dei quali possono essere create reti bot.
Motivazione	Esclusivamente finanziaria.
Risorse tecniche	Medie, sovente si effettua l'acquisto di Crimeware Kit.
Risorse finanziarie	Da medie a elevate.
Razionalità del modo di procedere	Elevata.
Tenacia	Bassa nei confronti di un singolo obiettivo.
Punti di partenza per la difesa	Monitoraggio del traffico di rete in entrata e in uscita nel caso delle imprese e delle organizzazioni governative. Monitoraggio delle reti degli ISP, informazione degli utenti finali quando emerge una apparecchiatura infettata. Approntamento di informazioni per gli utenti finali.
Punti di partenza per il perseguimento	Sinkholing di domini corrispondenti, utilizzati dalle organizzazioni cibercriminali. Analisi delle reti bot e del malware utilizzato. Analisi e impedimento dei flussi di denaro corrispondenti. Monitoraggio dei money mules per una migliore rilevazione di questi flussi di denaro.
Capacità di resistenza al perseguimento penale	Da media e elevata. Il perseguimento penale perturba comunque le attività degli aggressori, che lo evitano nella misura del possibile.
Obiettivi probabili di attacco	• Apparecchiature insufficientemente protette degli utenti finali. • Applicazioni di e-banking.

Autori singoli

Nome	Autori singoli
Descrizione	L'autore singolo opera per conto proprio, con risorse limitate.
Motivazione	Dipende dall'aggressore.
Risorse tecniche	Basse.
Risorse finanziarie	Basse.

Razionalità del modo di procedere	Dipende dall'aggressore.
Tenacia	Da bassa a elevata a seconda dell'aggressore.
Punti di partenza per la difesa	Sistemi ben protetti.
Punti di partenza per il perseguimento	Perseguimento normale di diritto penale.
Capacità di resistenza al perseguimento penale	Bassa.
Obiettivi probabili di attacco	• Sistemi debolmente protetti nel caso di «Script Kiddies». • Obiettivi ben visibili con grande attenzione in caso di azioni di vendetta.

Strumenti

Oltre a numerosi strumenti (Portscanner, Penetration Testing Tools ecc.), che possono essere utilizzati a scopi perfettamente legali, esistono quattro strumenti specificamente criminali, illustrati succintamente qui appresso. Essi sono accomunati dal fatto che vengono utilizzati a tutti i livelli della piramide (vedi il capitolo minacce).

Crimeware Kit

Per Crimeware Kit si intende una raccolta di strumenti per attacchi elettronici. I Crimeware Kit servono alla realizzazione di malware e dell'infrastruttura necessaria al suo funzionamento, ad esempio per predisporre server di comando e di controllo.

Reti bot

Le reti bot constano di diversi computer infettati che per il tramite dei server di comando e di controllo divengono un potente strumento di attacco per gli APT e per le organizzazioni criminali. È altresì molto probabile che in singoli casi gli aggressori statali facciano capo ai servizi e alle reti bot di organizzazioni criminali per effettuare i loro attacchi. Una rete bot può comprendere fino a parecchi milioni di computer infettati.

Infrastrutture di server di comando e di controllo

A prescindere dai dati ai quali è interessato, oppure indipendentemente dal fatto che intenda inviare spam, derubare dati bancari, effettuare spionaggio, l'aggressore deve poter impartire ordini ai computer infettati e riceverne i dati. A questo scopo sono necessarie Infrastrutture di server di comando e di controllo. Proprio queste infrastrutture costituiscono sovente il maggior punto debole delle reti bot, ragione per la quale è su questo punto che dovrebbero intervenire il perseguimento penale e l'osservazione a scopi di difesa.

Strumenti DDoS

Esistono principalmente due tipi di strumenti che possono essere utilizzati per gli attacchi DDoS:

- strumenti integrati nelle reti bot, nella maggior parte dei casi come modulo caricabile, pilotato da un server di comando e di controllo,

- software pilotato dall'utente, basato nella maggior parte dei casi su Stress Test Tool. Ne è un esempio tipico LOIC[2] , utilizzato volentieri dai ciberattivisti come anonymous.

Protezione da parte di organizzazioni CSIRT/CERT

Le grandi imprese sono viepiù oggetto di attacchi mirati come pure di attacchi su vasta scala. Per questo motivo devono essere istituite organizzazioni e architetture di sicurezza per poter difendersi da queste minacce. Per reagire in maniera adeguata agli attacchi le imprese di dimensioni medie a grandi o le imprese particolarmente esposte (ad es. le imprese attive nelle tecnologie di punta) dovrebbero disporre di un'organizzazione per il trattamento dei Security Incident. Una forma possibile di organizzazione sono il cosiddetto CSIRT (Computer Security Incident Response Team) o il CERT (Computer Emergency Response Team), che si occupano di incidenti rilevanti ai fini della sicurezza nell'infrastruttura IT propria all'impresa.

Un CISRT/CERT opera normalmente seguendo i tre processi principali preparazione (Preparation) – rilevamento e reazione (Detect/React) e protezione (Protection):

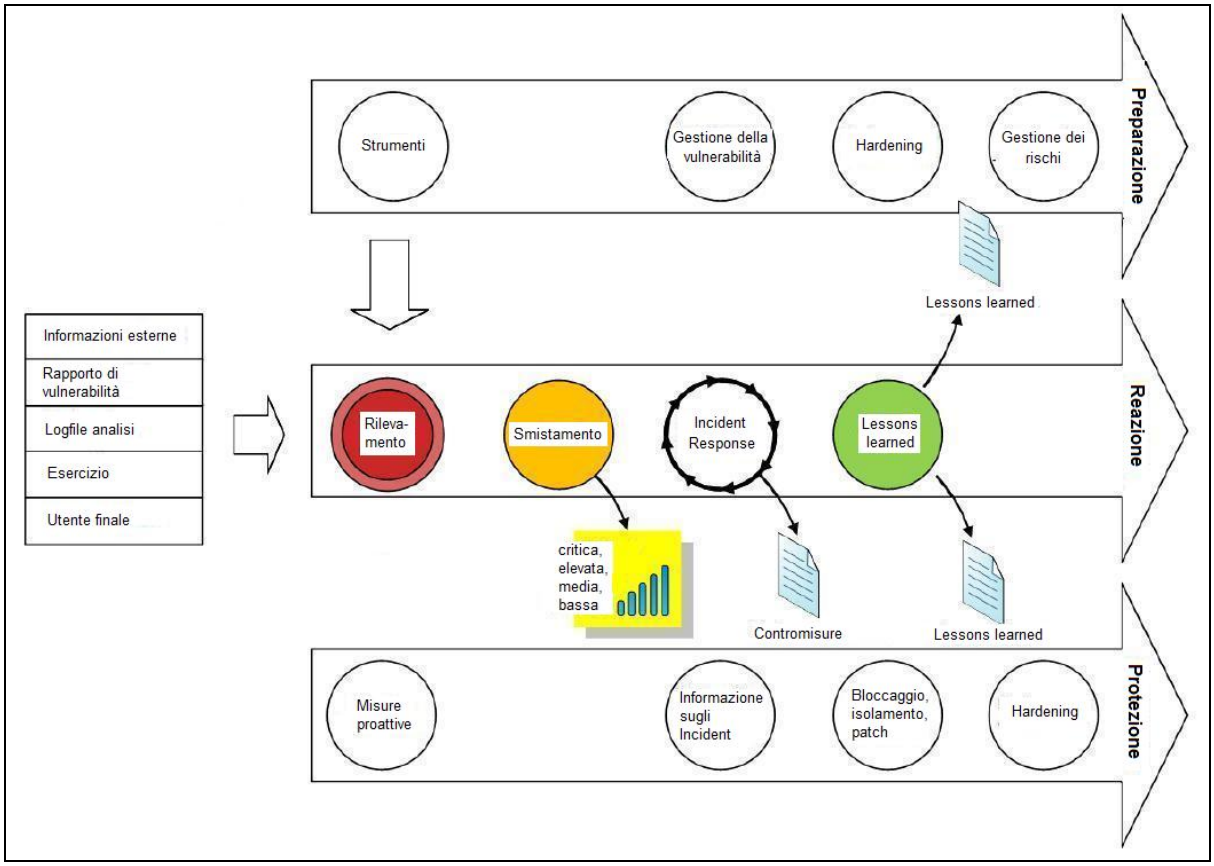

Figura 2: Processi CSIRT/CERT, adattati da cert.org

[2] http://de.wikipedia.org/wiki/LOIC

Il trattamento del vero e proprio Security Incident avviene nel settore rilevamento/reazione, che segue sempre il modello rilevamento-smistamento-reazione-apprendimento. Non va in particolare sottovalutata l'importanza dell'apprendimento da Security Incident, in quanto esso offre la possibilità di un'analisi critica del dispositivo di difesa sulla base di eventi concreti e se del caso la possibilità dell'introduzione di miglioramenti. L'informazione proveniente da eventi a livello di sicurezza effettivamente accaduti costituisce una delle più importanti fonti di input per la gestione dei rischi di un'impresa. Non esiste una ricetta universalmente valida sulle modalità di trattamento degli Incident.

In generale ogni evento in materia di sicurezza è anche diverso. Importa quindi osservare i seguenti punti nella loro esatta sequenza:

1. Occorre effettuare immagini legali del sistema compromesso? Ciò presuppone un equipaggiamento minimo (Write Blocker) e la formazione dell'Incident Response Team.

2. È necessario od opportuno abbandonare alcune apparecchiature all'aggressore per evitare che temi di essere scoperto? Esistono timori che l'aggressore potrebbe vendicarsi qualora fosse scoperto?

3. Come può essere limitato l'attacco? Cosa è necessario a tale scopo? Come si possono evitare ulteriori infezioni o ulteriori deflussi di dati?

4. Chi deve essere informato?

5. Limitazione dell'attacco (isolamento, bloccaggio sui sistemi Gateway, bloccaggio dei dati ecc.).

6. Analisi dell'attacco (analisi del logfile per rilevare possibilmente tutte le apparecchiature infettate, Reverse Engineering del malware).

7. Richiesta di informazioni da fonti di informazione esterne (ad es. MELANI).

8. Esecuzione di meeting regolari di scambio, inizialmente ogni 6 ore e successivamente ogni 12 a 24 ore.

I punti dal 3 all'8 vanno intesi come ciclo da ripercorrere finché l'incidente è concluso.

Le risorse di lavoro necessarie a un CSIRT/CERT sono sistemi per la sorveglianza del traffico di rete, log di sistema e di applicazioni. Può anche rivelarsi utile l'impiego di sistemi di Intrusion Detection (IDS) o di sistemi di verifica dell'integrità. Per raggiungere una protezione sufficiente contro gli aggressori sono indispensabili speciali meccanismi di protezione per l'accesso a Internet. Ad esempio è possibile utilizzare liste di bloccaggio e scanner centrali antivirus. Nel caso di tutte le misure di protezione va però preso in considerazione che gli attacchi possono comunque essere efficaci. In un simile caso il rilevamento rapido di un attacco efficace e una buona reazione sono decisivi per ridurre i danni al minimo possibile.

Dato che i pericoli nel mondo della tecnologia dell'informazione mutano in continuazione, i meccanismi di protezione devono essere costantemente verificati, aggiornati e adeguati. Sono inoltre molto importanti una formazione e un perfezionamento dei collaboratori del

CSIRT/CERT. I gestori di infrastrutture critiche in Svizzera sono informati in merito alle minacce attuali tramite la cerchia chiusa di clienti di MELANI.

Lotta alle reti bot da parte delle autorità di perseguimento penale

Oltre alle strategie di difesa ormai affermate come l'istituzione e l'esercizio di Computer Emergency Response Teams (CERT) o di Computer Security Incident Response Teams (CSIRT) è di grande rilievo il perseguimento penale. La piazza bancaria Svizzera è un emblema di qualità della Svizzera. È la ragione per la quale occorre proteggerlo, in particolare per garantire l'elevata fiducia riposta nelle banche svizzere. Con l'inizio dell'era di Internet le rapine in banca avvengono sempre più online. Da alcuni anni si delinea una tendenza in forte aumento delle operazioni cibercriminali ai danni delle banche, rispettivamente della loro clientela. Numerosi Paesi occidentali – e fra questi anche la Svizzera – sono già stati colpiti da simili attacchi. Nei mesi scorsi gruppi criminali hanno viepiù sferrato attacchi mirati in sequenza contro gli istituti finanziari dei singoli Paesi. È interessante il fatto che alla notizia di un'ondata di attacchi e di corrispondenti informazioni nei media i criminali cambiano il loro obiettivo e attaccano le banche di un altro Paese utilizzando il medesimo modello. In questo senso un gruppo criminale ha attaccato la clientela di più banche nel medesimo Paese. Dopo che le banche e i media furono informati del perdurare degli attacchi i criminali cambiarono Paese prendendo di mira le banche di questo nuovo Paese.

L'informazione della popolazione è di grande importanza in caso di ciberattacco su vasta scala ai danni delle infrastrutture svizzere. Questo compito è attualmente assunto da MELANI. MELANI coordina altresì l'informazione tra le singole imprese interessate. Per poter combattere efficacemente la cibercriminalità è però necessaria la collaborazione tra Interpol, Europol e le autorità dei Paesi interessati. È pure importante un buon coordinamento a livello federale perché i computer infettati (bot) si trovano in diversi Paesi e sono generalmente pilotati da uno o più server di comando e di controllo. I server di comando e di controllo sono operati in quasi tutti i casi dall'estero (Germania, Paesi Bassi o Europa orientale). Per poterli separare dalla rete devono essere attuati rapidamente processi corrispondenti. Oltre al perseguimento penale vero e proprio, che si rivela talvolta estremamente difficile, la separazione delle infrastrutture di server di comando e di controllo rintracciate come pure il Sinkholing di domini notoriamente nocivi costituiscono un mezzo per accrescere il prezzo di attacchi efficaci.

L'interazione senza intoppi delle autorità di perseguimento penale, dei CERT/CSIRT privati e statali, dei servizi segreti e di organizzazioni per la tutela delle infrastrutture critiche (ciberdifesa) deve essere posta al centro perché il compito può essere assolto in comune unicamente da organizzazioni diverse e indipendenti tra di loro. In merito va osservato che queste singole organizzazioni applicano invero metodi diversi e hanno visioni diverse della problematica, ma perseguono tutte un obiettivo comune, ossia quello di non fare cadere Internet in uno spazio senza leggi, dove vige soltanto il diritto del più forte.