HackInBo

Cyber Security Incident Response

Davide Dante Del Vecchio
@The_Haiku

Chi sono?

’80: bootstrap!

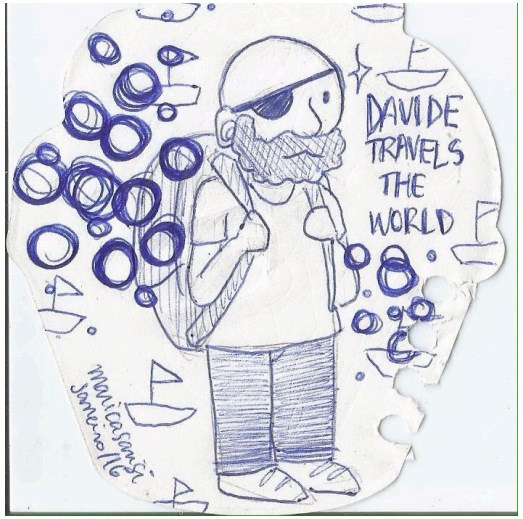
’90: Script kiddie (nick: DanteAlighieri)

Ezine come Newbies, Bfi

Bluesnarfer

Advisory

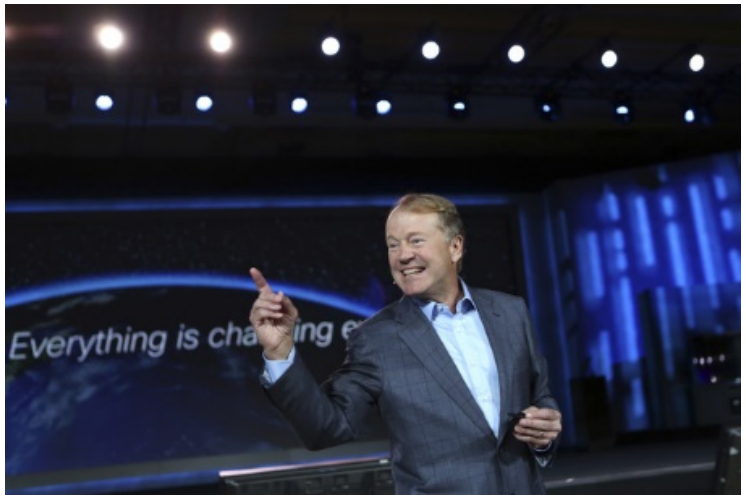
’00: Ethical hacker, incident handler



’10: Security Fuffer Specialist

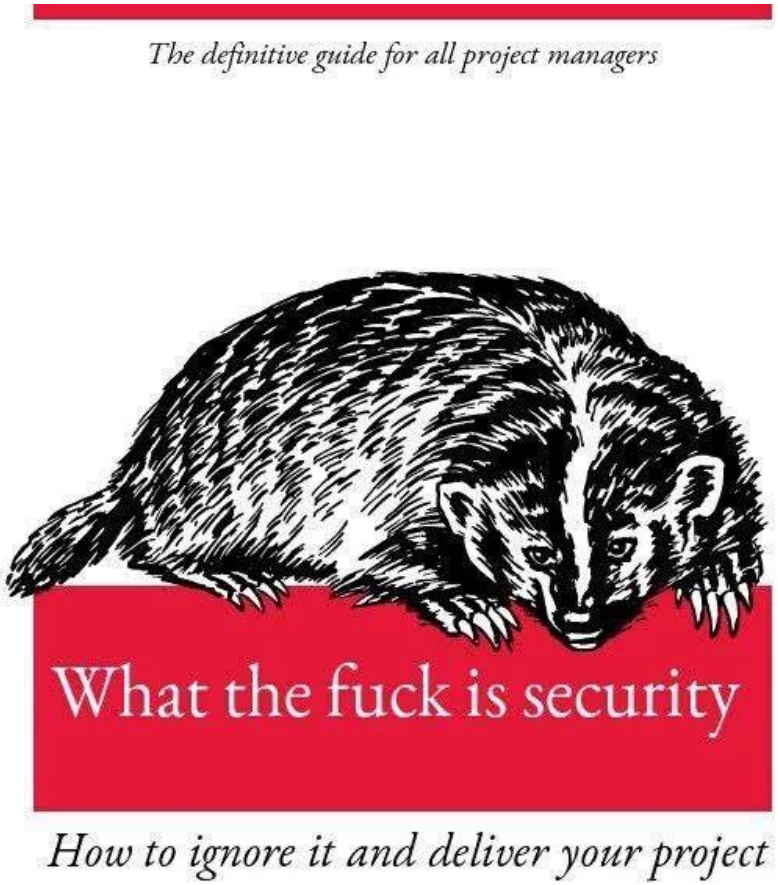
’20: Pensione

Cyber Security Incident Response



"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."

John Chambers, Cisco CEO



L’analisi storica

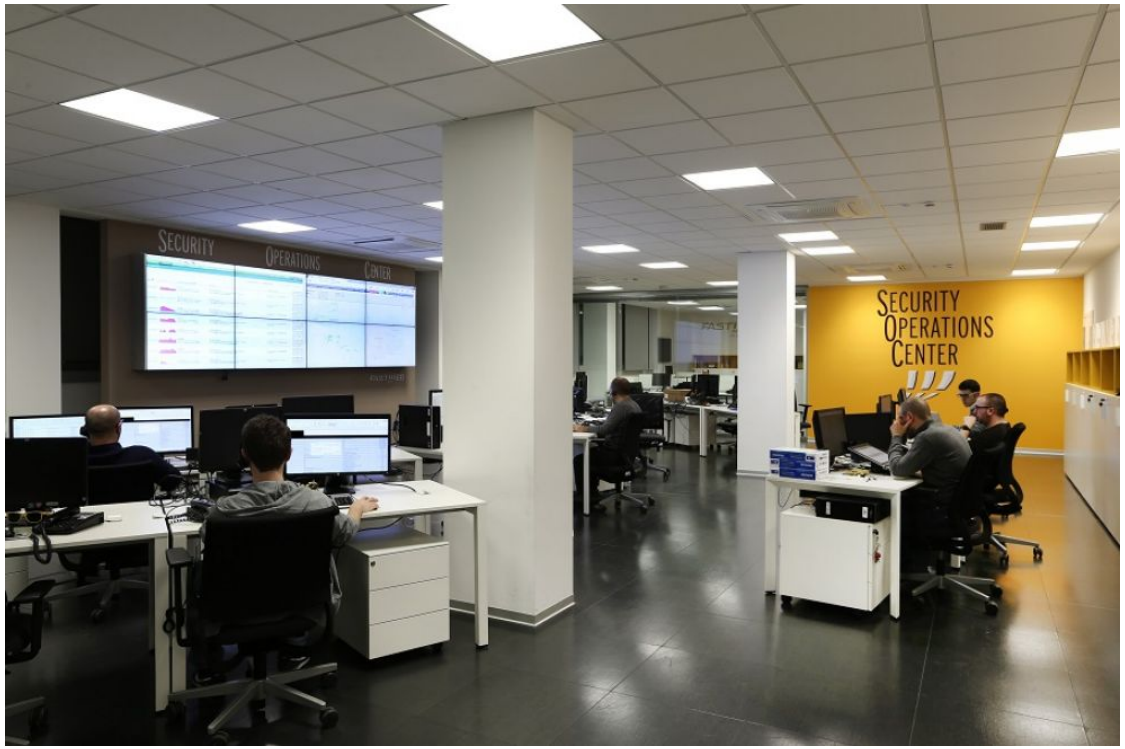
Il dominio di analisi è costituito dai dati raccolti, anonimizzati, storicizzati ed analizzati dal **Security Operations Center**, relativi agli indirizzi IP appartenenti all’ AS Fastweb: oltre 6 milioni di indirizzi pubblici, dietro ognuno dei quali potrebbero celarsi decine o centinaia di computer / server.

Eventi di sicurezza analizzati

2013 ≈ **172.000**

2014 ≈ **5.000.000**

2015 ≈ **8.000.000**



Clusit
Associazione Italiana per la Sicurezza Informatica

Le fonti dell'analisi

Lo studio viene effettuato incrociando e arricchendo i dati storicizzati con informazioni liberamente accessibili

shadowserver

SHODAN
Computer Search Engine

zone-h
unrestricted information

malwr

virustotal

SAFE BROWSING
Google

Come facciamo?

Importiamo nel nostro DW i dati dalle fonti relativi agli indirizzi di cui siamo responsabili

```
"Date","Time","C&C","C&C Port","C&C ASN","C&C Geo","C&C DNS","ATK","ATK ASN","ATK Geo","ATK DNS","TGT","TGT ASN","TGT Geo","TGT DNS"
"2008-11-03","00:24:56","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.242",1213,"IE",""
"2008-11-03","00:28:07","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","172.16.30.19","","-",""
"2008-11-03","00:37:35","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.119",1213,"IE",""
"2008-11-03","01:00:08","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","172.16.30.19","","-",""
"2008-11-03","01:01:01","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.208",1213,"IE",""
"2008-11-03","02:08:14","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be
"2008-11-03","02:12:05","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be
"2008-11-03","02:23:17","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be
"2008-11-03","02:34:49","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be
"2008-11-03","03:16:30","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be
```

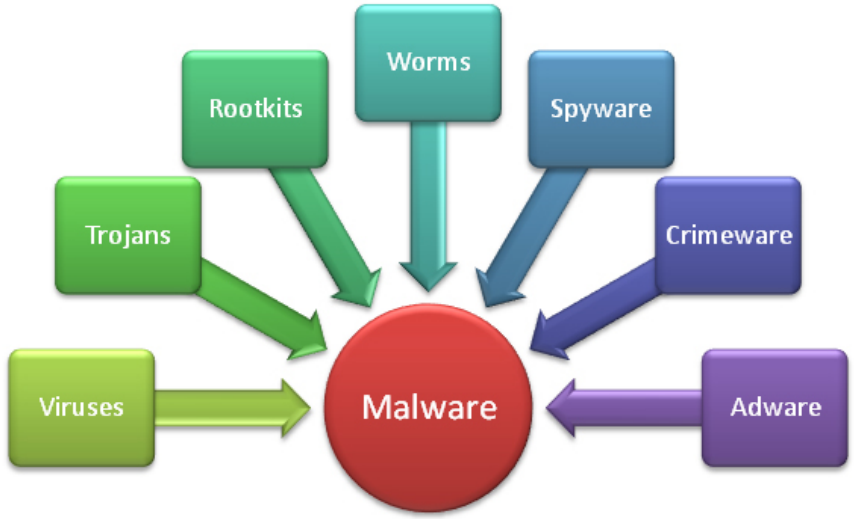
open source™

TIMESTAMP	IP	PORT	ASN	GEO	REGION	CITY	HOSTNAME	TYPE	INFECTION	URL	AGENT	CC_IP	CC_P
0000-00-00 00:00:00	ip	port	asn	geo	region	city	hostname	type	infection	url	agent	cc_ip	cc_pc
2016-01-01 00:00:01	[redacted]	50311	12874	IT	SALERNO	SALERNO	[redacted]		nivdort	/index.php		[redacted]	80
2016-01-01 00:00:03	[redacted]	58215	12874	IT	TORINO	TORINO	[redacted]		gameover-zeus-peer			[redacted]	53
2016-01-01 00:00:14	[redacted]	29056	12874	IT	ROMA	ROME	[redacted]		nivdort	/index.php		[redacted]	80
2016-01-01 00:00:24	[redacted]	62199	12874	IT	PALERMO	MONREALE	[redacted]		nivdort	/index.php		[redacted]	80
2016-01-01 00:00:26	[redacted]	49152	12874	IT	MILANO	MILAN	[redacted]	udp	zeroaccess			[redacted]	1647
2016-01-01 00:00:31	[redacted]	4273	12874	IT	VERONA	VERONA	[redacted]	udp	zeroaccess			[redacted]	16465
2016-01-01 00:00:36	[redacted]	63584	12874	IT	MILANO	MILAN	[redacted]		gameover-zeus-proxy	POST /write		[redacted]	9686
2016-01-01 00:00:36	[redacted]	24761	12874	IT	MILANO	MILAN	[redacted]		nivdort	/index.php		[redacted]	80
2016-01-01 00:00:46	[redacted]	65370	12874	IT	BARI	BARI	[redacted]	udp	zeroaccess			[redacted]	1647
2016-01-01 00:00:47	[redacted]	52972	12874	IT	UDINE	PASIAN DI PRATO			gameover-zeus-dga	GET /		[redacted]	80
2016-01-01 00:00:52	[redacted]	2239	12874	IT	NAPOLI	STRIANO		UDP	salityv3			[redacted]	5560
2016-01-01 00:00:59	[redacted]	56666	12874	IT	TORINO	TORINO			gameover-zeus-proxy	POST /write		[redacted]	6857
2016-01-01 00:01:32	[redacted]		12874	IT	TRENTO	TRENTO	[redacted]		bitdefender-ramdo	/		[redacted]	80
2016-01-01 00:01:49	[redacted]	53935	12874	IT	BARI	BARI	[redacted]	udp	zeroaccess			[redacted]	1647
2016-01-01 00:01:49	[redacted]		12874	IT	BOLOGNA	BOLOGNA	[redacted]		bitdefender-dircrypt	/	Mozilla/4.0 (compatible; MSIE 7.0; .NET4.0E; Media...	[redacted]	80
2016-01-01 00:01:50	[redacted]		12874	IT	MILANO	MILAN	[redacted]		bitdefender-ramnit			[redacted]	
2016-01-01 00:01:56	[redacted]	49819	12874	IT	UDINE	UDINE			gameover-zeus-dga	GET /		[redacted]	80
2016-01-01 00:02:02	[redacted]	53112	12874	IT	ROMA	ROME	[redacted]		nivdort	/index.php		[redacted]	80
2016-01-01 00:02:13	[redacted]	45275	12874	IT	NAPOLI	NAPLES	[redacted]		gameover-zeus-dga	GET /		[redacted]	80

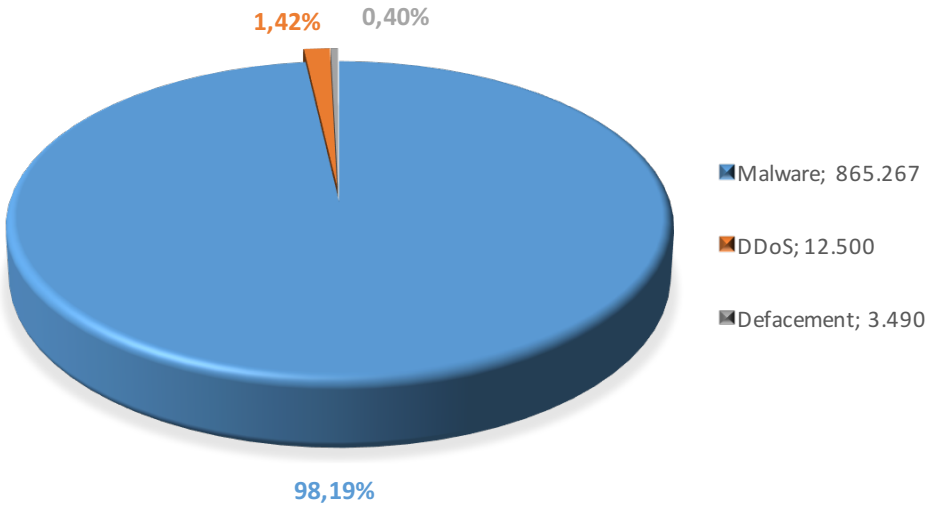
Attacchi statisticamente più probabili

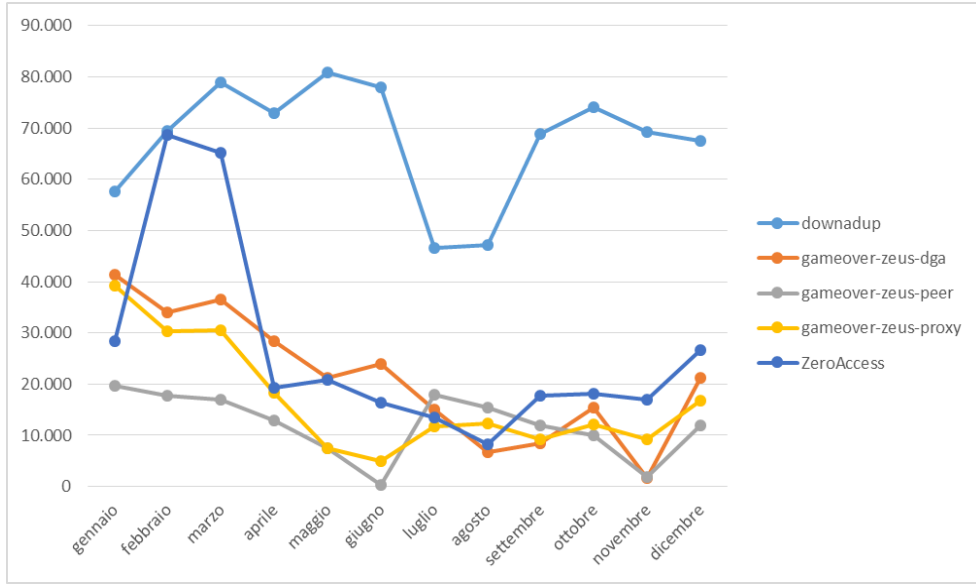
Risultati

Malware



Durante l'anno 2015 abbiamo rilevato quasi 870.000 eventi riconducibili ad host infetti da malware.



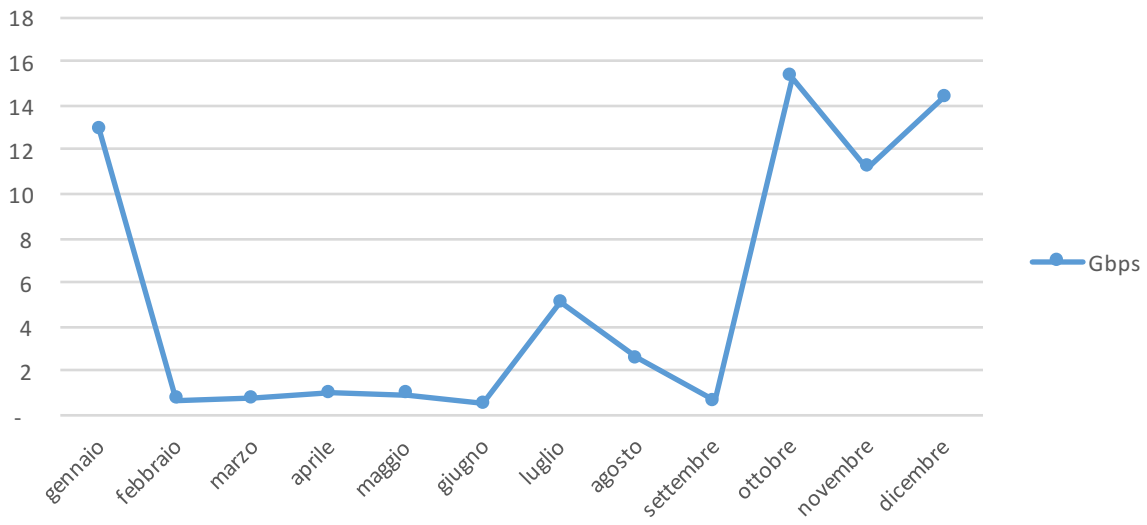


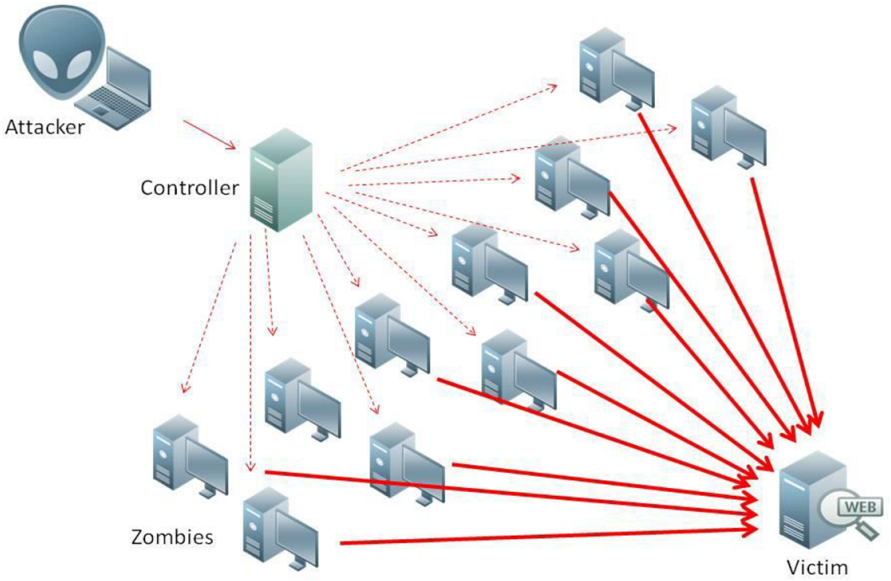
Risultati

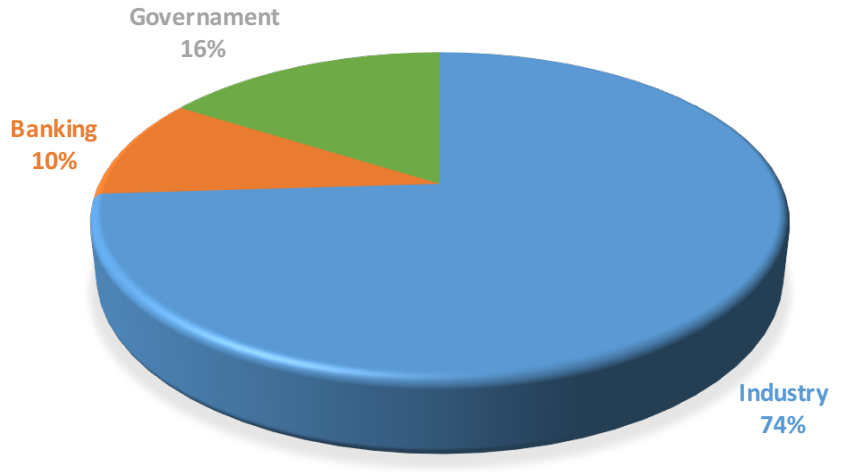
DDoS

2013 ≈ **1.000** → 2014 ≈ **16.000** → 2015 ≈ **12.500**

Picchi di traffico riconducibili ad attacchi DDoS durante il 2015







Cyber Security Incident

Definizione tradizionale

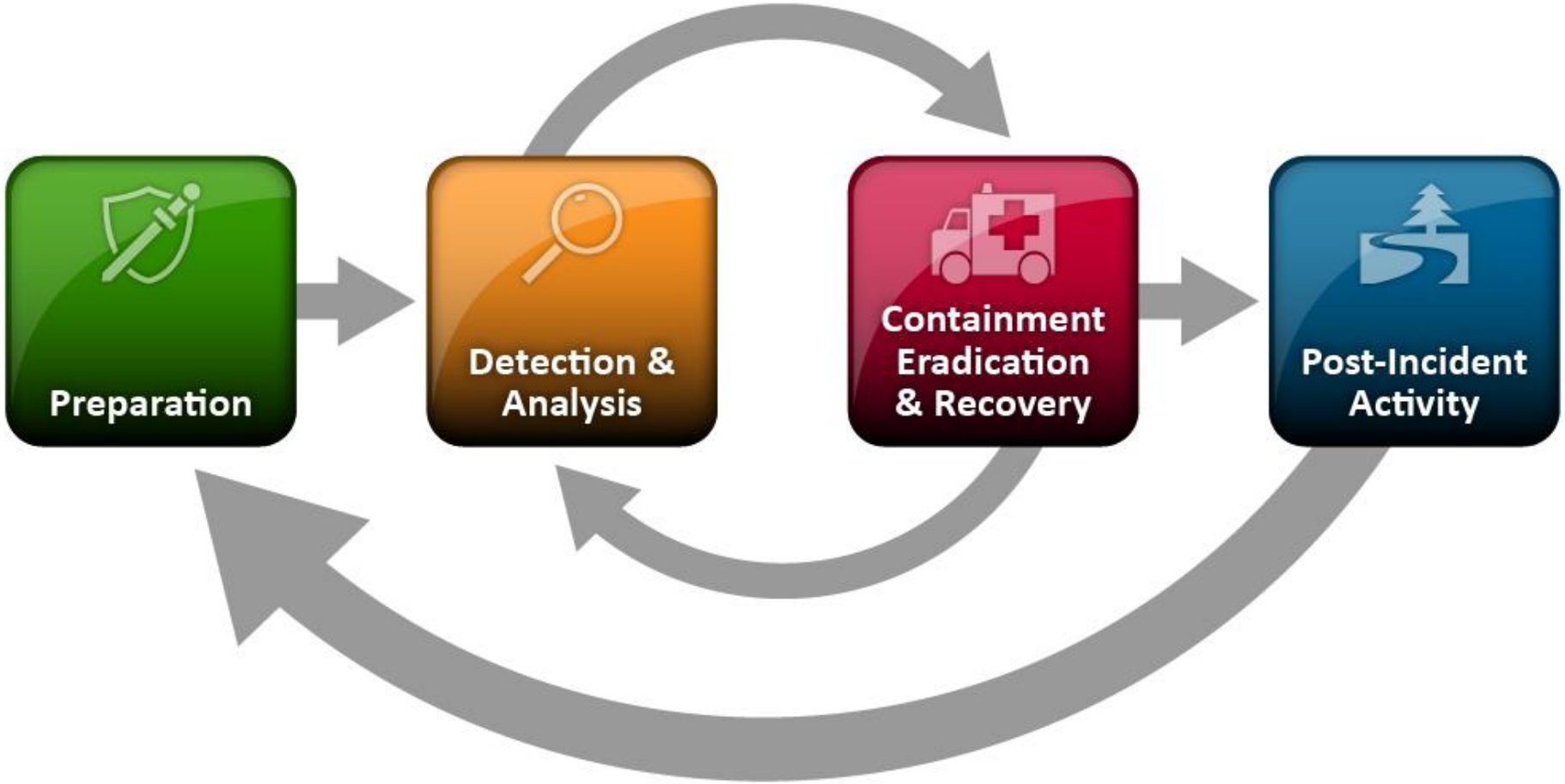
Un’azione malevola o un evento sospetto che: *compromette* o *ha tentato di compromettere*, il perimetro elettronico di sicurezza; *distrugge* o *ha tentato di distruggere*, il funzionamento di un asset informatico.

Cyber Security Incident

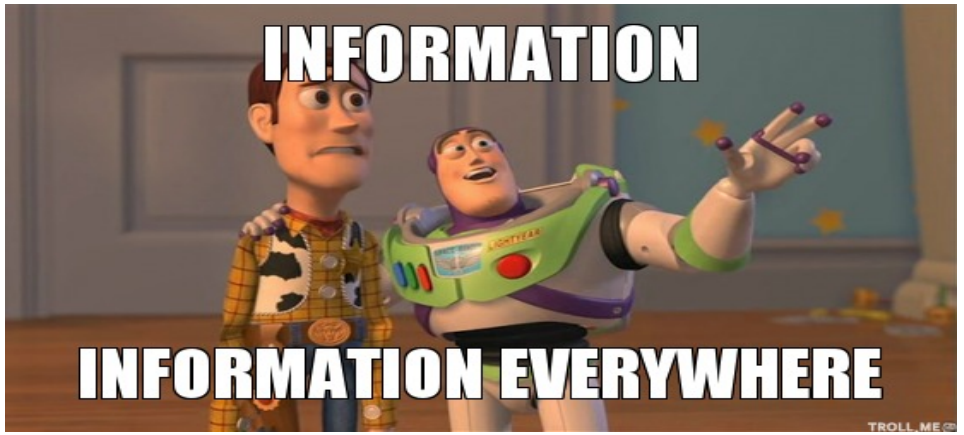
Nuova definizione

Violazione e/o rischio di imminente violazione delle *policy* relative alla sicurezza informatica, delle policy di sicurezza aziendale e/o delle *standard security practice.*

Come si gestisce un Incident?



Preparation



- **Contact information:** il team deve essere informato su tutti i contatti all' interno ed all' esterno dell'organizzazione, dei numeri delle persone reperibili, dei responsabili e dei contatti verso i quali fare *escalation*.
- **On-call information:** il team deve essere informato sui turni di reperibilità all'interno ed all'esterno dell'organizzazione.
- **Incident reporting mechanisms:** il team deve essere in grado di usare gli strumenti software per effettuare il report dell'incident.
- **Issue tracking system:** il team deve avere uno strumento per il tracking degli incident.
- **Encryption software:** il team deve utilizzare tool che garantiscano la sicurezza delle comunicazione intra ed extra organizzazione.
- **War room:** il team deve essere dotato di un punto centrale di comunicazione per gestire e coordinare le comunicazioni.
- **Secure storage facility:** il team deve essere dotato di un repository sicuro dove attingere e/o salvare le informazioni relative agli incident.

Detection & Analisys

Detection & Analisys

I vettori di attacco possono essere innumerevoli, impossibile pensare di poterli gestire tutti, ammesso che li si conoscano.

Ci si focalizza su quelli **statisticamente** più probabili:

- **External/Removable Media.**
- **Attrition:** Un attacco che prevede metodi basati sul brute-force per compromettere, degradare o distruggere sistemi, reti e/o servizi.
- **Web:** Attacchi perpetrati attraverso il sito web come ad esempio sql-injection, xss, auth bypass, etc.
- **Email:** Attacchi perpetrati via mail: invio di malware, exploit, backdoor, etc.
- **Impersonation:** Attacchi perpetrati impersonando pezzi dell'infrastruttura : mitm, spoofing, rogue ap, etc.
- **Improper Usage:** Attacchi perpetrati attraverso l'uso scorretto dei dispositivi: file sharing, etc.
- **Loss or Theft of Equipment:** Perdita o furto di dispositivi aziendali: pc, laptop, tokens, badge, etc.
- **Other.**

Detection & Analisys

Come possiamo rilevare un attacco ? Come ci si accorge di essere vittima di un attacco ?

- IDS / IPS Alert.
- Antivirus Alert.
- System Administrator auditing log.
- OS / Application log.
- Network flow anomaly.

Detection & Analisys

Detection & Analisys

Purtroppo non è sempre facile accorgersi di un attacco ed analizzarlo. Soprattutto quando le evidenze che si ricevono non sono sempre e del tutto accurate (falsi positivi, comportamenti anomali dei sistemi, malfunzionamenti hw/sw). Tuttavia ci sono delle metodologie che ci aiutano in questa attività.

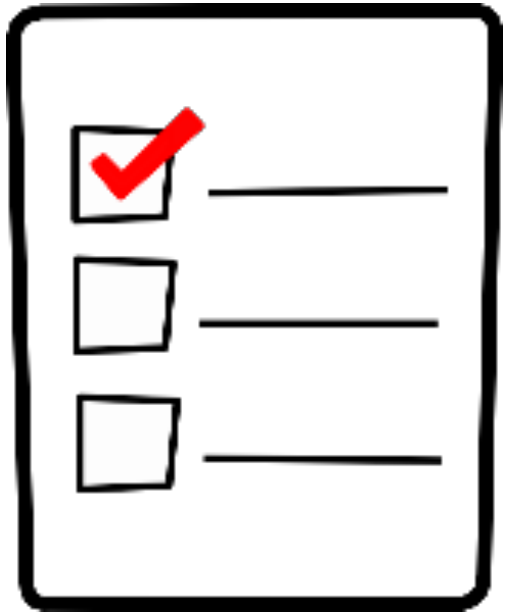
- **Profilare sistemi e reti.**
- **Capire i comportamenti normali.**
- **Creare una policy di Log Retention.**
- **Correlare gli eventi.**
- **Fare in modo che tutti gli host abbiano orari sincronizzati.**
- **Mantenere una Knowledge Base.**
- **Mantenere attivi packet sniffers per collezionare più dati.**
- **Storicizzare e analizzare statisticamente i dati raccolti.**

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Detection & Analisys

Se il team di Incident Response sospetta che sia in corso o sia avvenuto un attacco deve iniziare **immediatamente** a raccogliere evidenze. Più indizi vengono raccolti nel minor tempo possibile più saranno alte le probabilità che si possa capire cosa / come / quando / dove è avvenuto. Normalmente gli strumenti software usati per questo genere di attività sono gli **Issue Tracking System**.
Cosa dovrebbe essere salvato in un ticket relativo ad un incident ?

- **Stato corrente del ticket.**
- **Descrizione generica dell'incident.**
- **Indicatori dell'incident.**
- **Altri incident collegati.**
- **Azioni effettuate.**
- **Chain of custody, se applicabile.**
- **Impatto dell'incidente.**
- **Informazioni di contatto.**
- **Lista delle evidenze relative all'incident.**
- **Commenti.**
- **Ulteriori azioni da intraprendere.**



NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Containment, Eradication & Recovery

Containment

E’ importante che un incident venga contenuto prima che questo saturi le risorse, aumenti il danno effettuato e si espanda a tutta l’infrastruttura informatica dell’Azienda. Le strategie di contenimento permettono di guadagnare il tempo necessario per studiare e mettere in atto strategie di **remediation** studiate ad-hoc. Come si può facilmente immaginare, una delle migliori strategie di contenimento è il ***decision-making*** (spegnere un sistema, disconnetterlo dalla rete, disabilitare eventuali funzionalità, etc.). Le strategie di contenimento variano a seconda dell’incident: una strategia di contenimento per un incident causato da infezione da malware è differente da quella adottata per far fronte ad un incident relativo ad un attacco DDoS.

I criteri che determinano un’appropriata strategia di contenimento sono:

- **Potenziali danni all’infrastruttura.**
- **Preservazione delle evidenze.**
- **Disponibilità dei servizi attaccati.**
- **Tempo e risorse richieste per l’implementazione della strategia.**
- **Durata della strategia di contenimento.**

Eradication and Recovery

La fase che segue il contenimento della minaccia è l'**Eradication**:

Bisogna eliminare i componenti della minaccia che ha provocato l'incident, eventuali vettori di attacco, disabilitare account utente violati, oltre a effettuare tutte le operazioni di patching per gli eventuali bug che sono stati sfruttati per portare a termine l'attacco.

Successivamente si passa alla fase di **Recovery**:

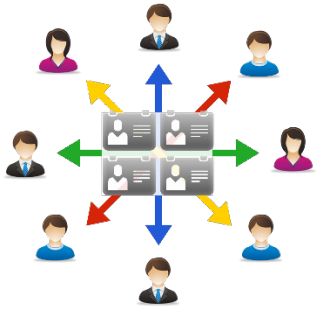
I sistemi vengono riportati ad uno stato di funzionamento normale. In genere durante la fase di recovery i sistemi vengono configurati in modo che generino log quanto più dettagliati possibile e la loro analisi è parte integrante del processo. Ecco perché normalmente la fase di recovery è quella che ha una durata più lunga.

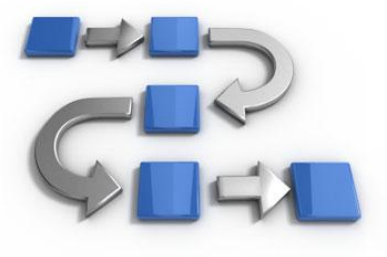
Post-Incident Activity

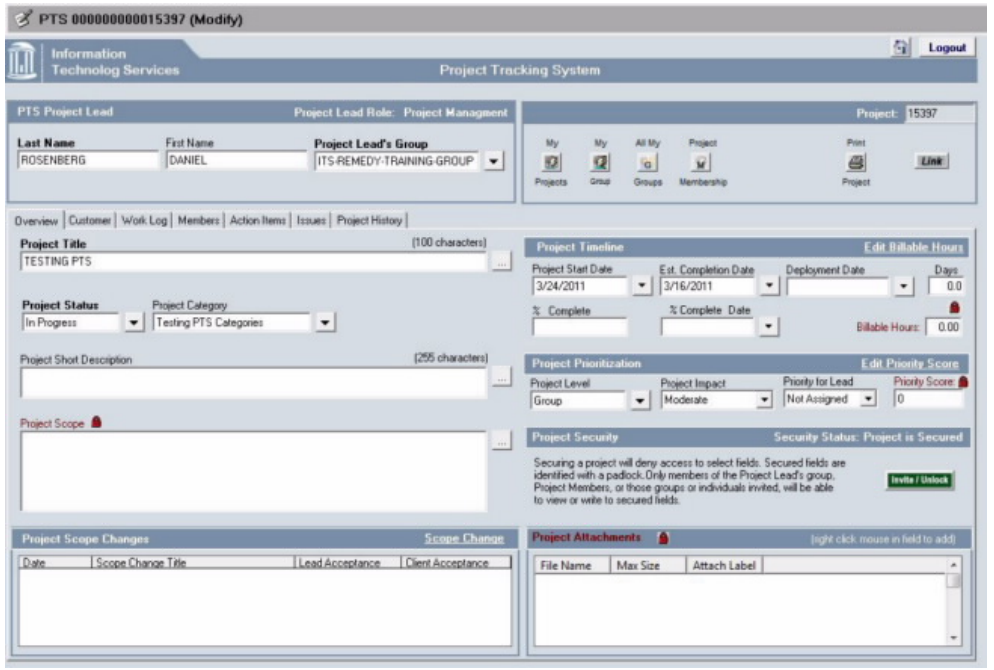
- **Cosa è successo esattamente e a che ora?**
- **Come ha reagito il team? Sono state seguite le procedure? Le procedure sono adeguate?**
- **Cosa sarebbe stato utile sapere prima?**
- **Ci sono azioni che potenzialmente avrebbero inibito la fase di recovery?**
- **Come potrebbe migliorare lo scambio di informazioni ?**
- **Quali azioni correttive possono essere intraprese per evitare incident similari ?**
- **Quali indicatori dovrebbero essere implementati / analizzati per rilevare in anticipo incident simili ?**

Preparation

Attacco DDoS

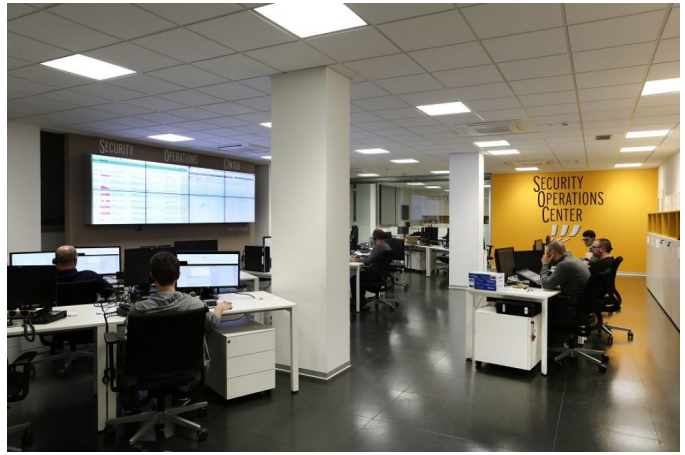






MediaWiki

GnuPG



Detection & Analysis

Attacco DDoS

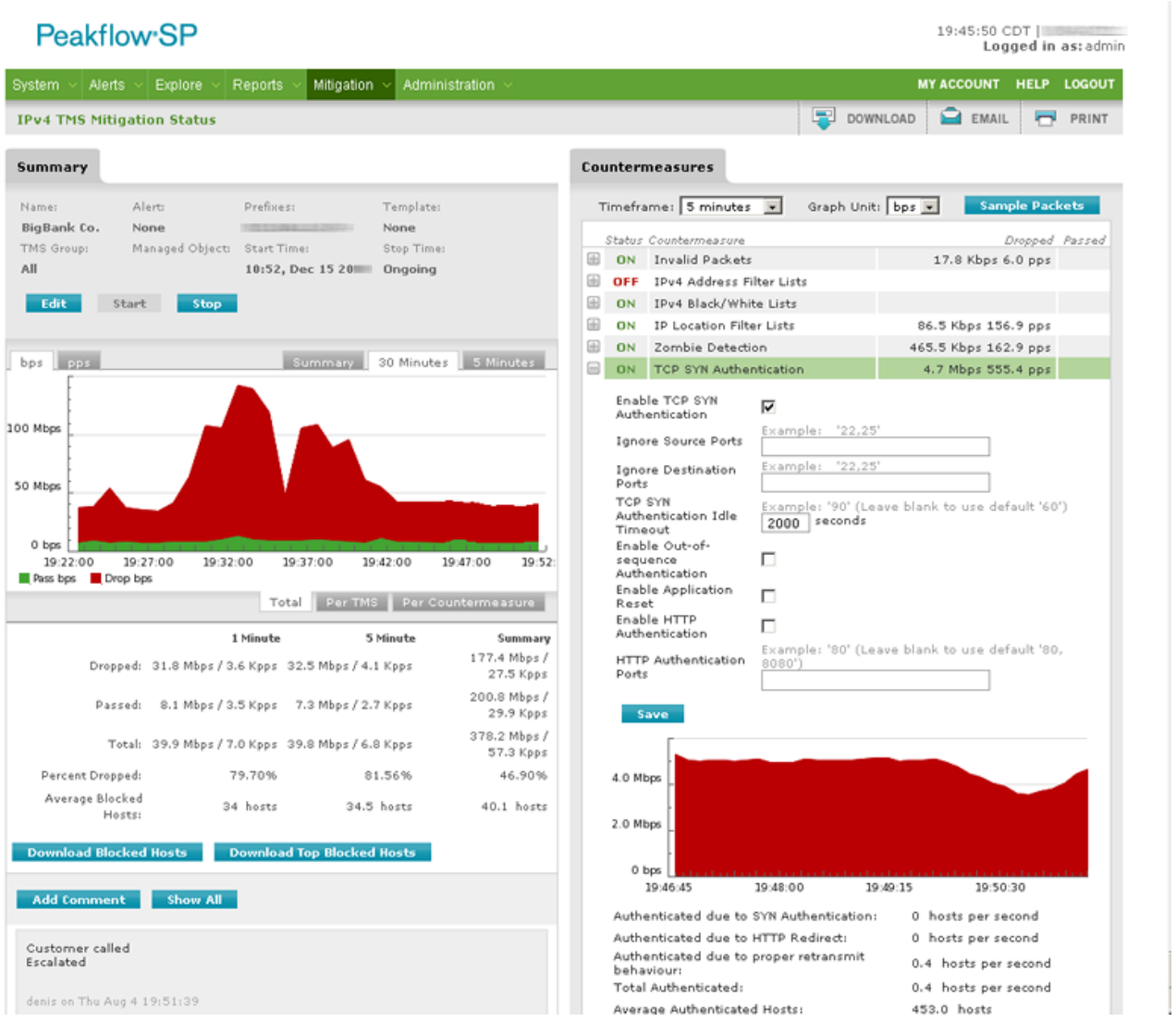
From: Peakflow SP [mailto:peakflowSP@[redacted]]
Sent: venerdì 6 maggio 2016 20:26
To: [redacted]; Fw Enterprise SOC. DDoS
Subject: [Peakflow SP] Profiled Network alert #2272048 incoming to [redacted]

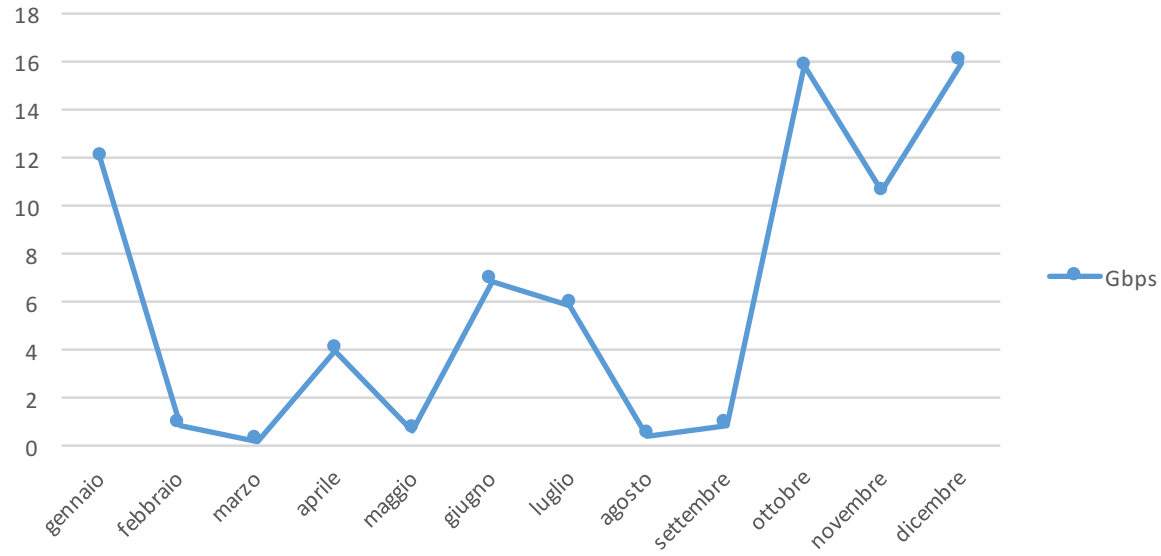
DoS network profiled alert started at 2016-05-06 18:26:10 GMT.

URL: https://[redacted]/page?id=profiled_network_alert&alert_id=2272048
Importance: High
Managed Object: [redacted]
Countries: None
Observed Traffic Rates:
8.35 Gbps (4772.7% over 171.45 Mbps threshold)
2.33 Mpps (7777.3% over 29.55 Kpps threshold)
Impact: 8.35 Gbps/2.33 Mpps

Containment
Eradication
& Recovery

Attacco DDoS





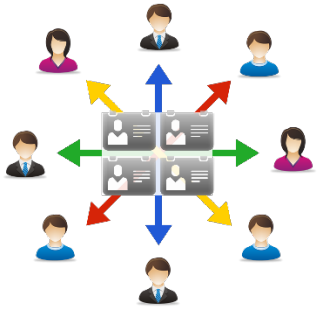
Banda mitigata dalla piattaforma

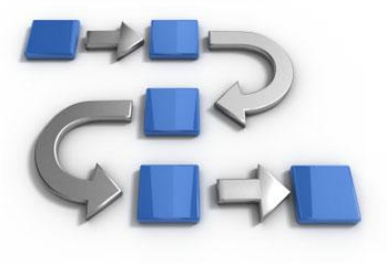
Attacco DDoS

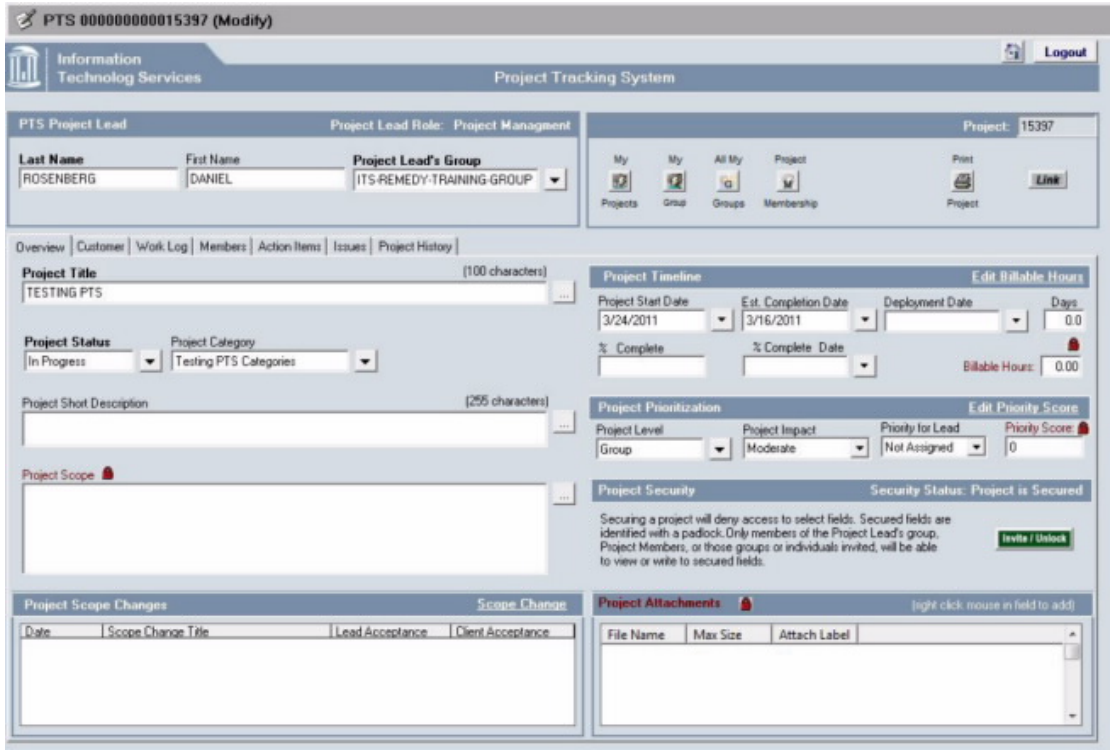
Retrospective !!

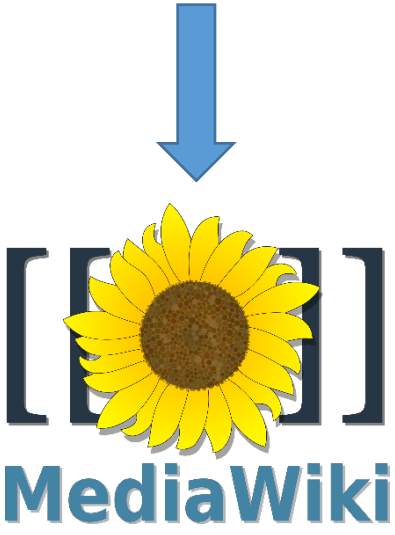
Preparation

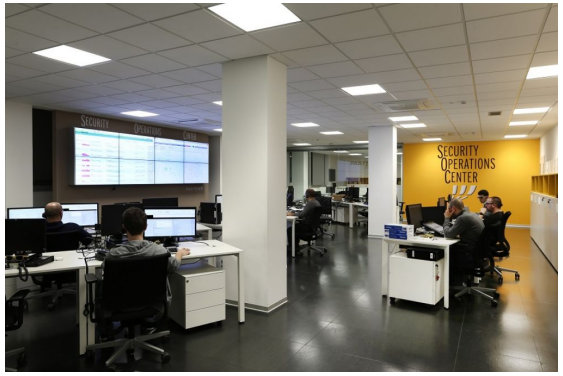
Attacco Malware







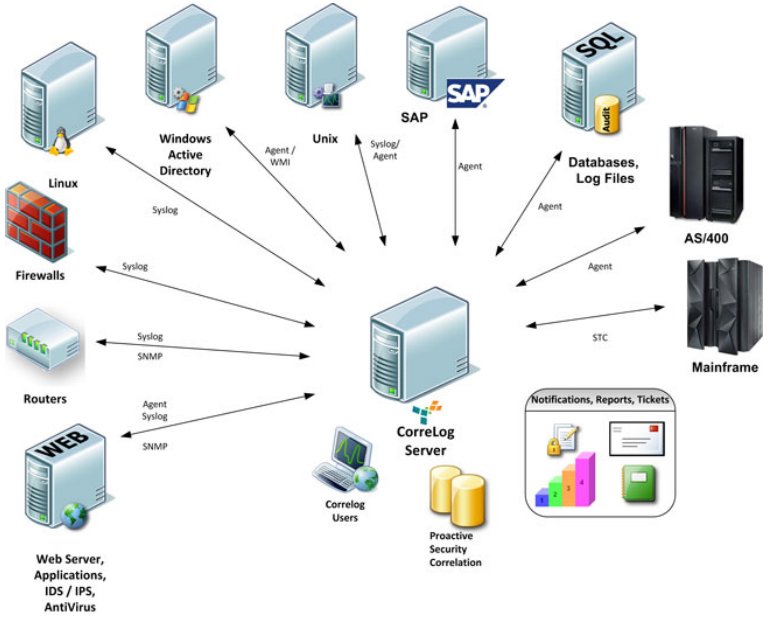


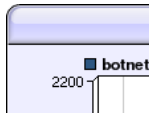


Attacco Malware


```
"Date","Time","C&C","C&C Port","C&C ASN","C&C Geo","C&C DNS","ATK","ATK ASN","ATK Geo","ATK DNS","TGT","TGT ASN","TGT Geo","TGT DNS"
"2008-11-03","00:24:56","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.242",1213,"IE",""
"2008-11-03","00:28:07","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","172.16.30.19","","-",""
"2008-11-03","00:37:35","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.119",1213,"IE",""
"2008-11-03","01:00:08","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","172.16.30.19","","-",""
"2008-11-03","01:01:01","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.208",1213,"IE",""
"2008-11-03","02:08:14","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.208",1213,"IE",""
"2008-11-03","02:12:05","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.242",1213,"IE",""
"2008-11-03","02:23:17","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.119",1213,"IE",""
"2008-11-03","02:34:49","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","172.16.30.19","","-",""
"2008-11-03","03:16:30","194.78.209.104",789,5432,"BE","104.209-78-194.adsl-fix.skynet.be","0.0.0.0","","","","193.1.1.119",1213,"IE",""
```

Screenshot di esempio non reale





Attacco Malware

- Individuare nell'infrastruttura l'host infetto, analizzando il traffico generato verso indirizzi individuati nella precedente fase.
- Bloccare l'host infetto : attraverso il proprio indirizzo IP oppure attraverso la tabella di NAT degli apparati perimetrali.
- Verificare lo stato dell'host infetto: sistema operativo e/o software di protezione non aggiornati ?
- Estrarre il malware per ulteriori verifiche, ad esempio, estrarne una *signature*.
- Implementare una *block policy* per quella relativa signature.
- Ripulire l'host infetto dal malware.
- Abilitare nuovamente l'host nella rete.

Attacco Malware

Retrospective Day

Siete pronti?