Nell'oscuro mondo dei Malware

Linux Day 2016

Giuseppe Augiero

22 ottobre 2016 - Linux Day 2016 - Facoltà di Ingegneria - Università di Pisa


Malware

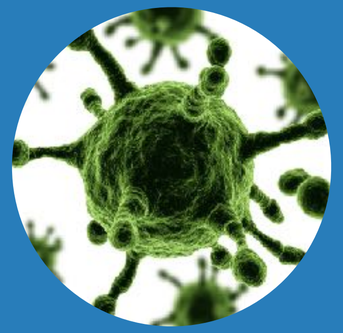
Di cosa parliamo?

Malware

Sequenza di codice progettata per danneggiare intenzionalmente un sistema, i dati che contiene o, comunque, alterare il suo normale funzionamento, all'insaputa dell'utente.

Tipologie di Malware

Virus



- Richiede ospite
- Replicazione automatica

Worm

- Nessun ospite
- Replicazione automatica

Root Kit / Trojan Horse

- Richiede ospite
- Nessuna replicazione

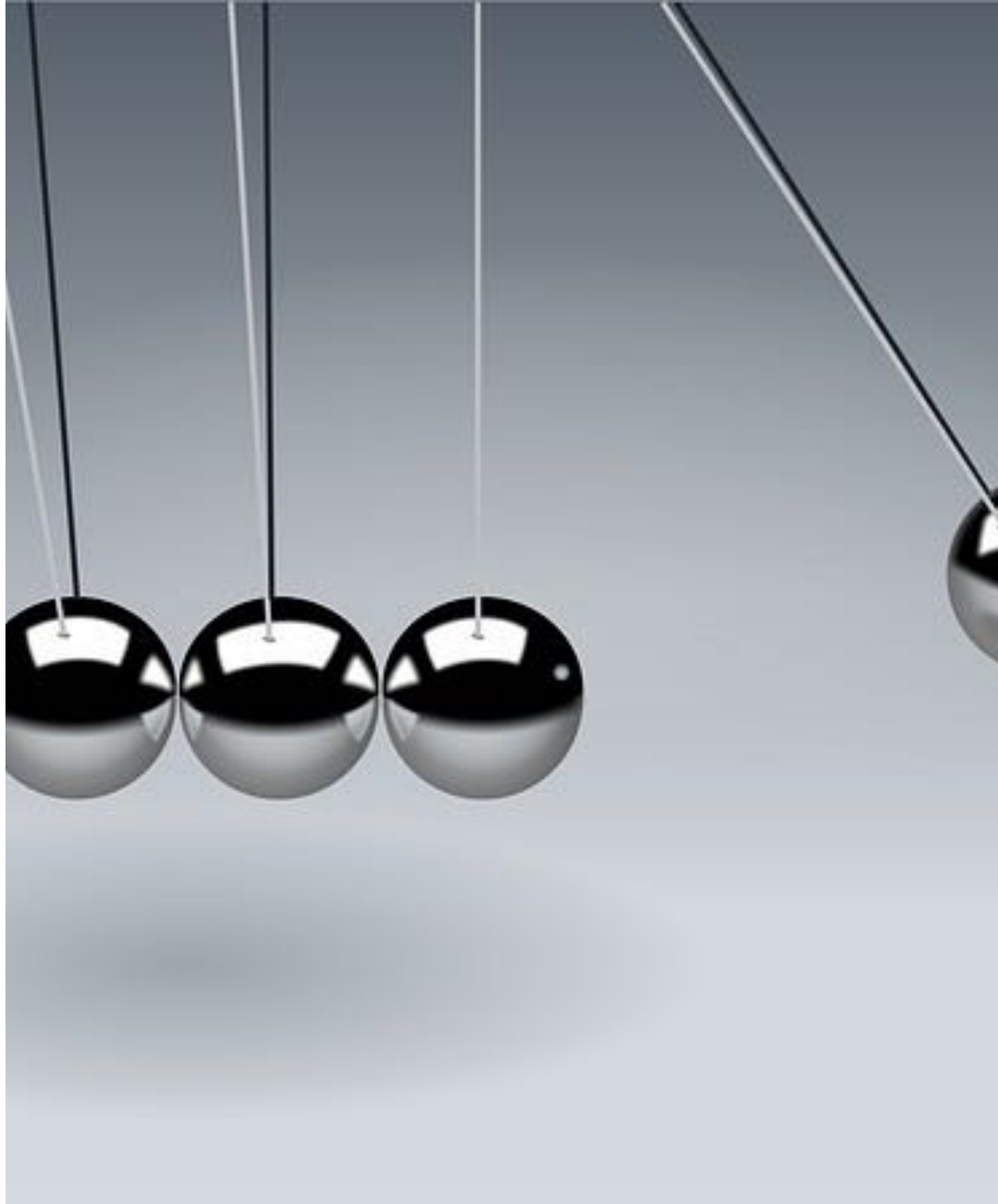
Dialer/Spyware/Keylogger

- Nessun ospite
- Nessuna replicazione

Cosa può fare?

Un worm può essere:

- Non distruttivo.
- Accidentalmente distruttivo.
- Distruttivo.
- DoS (Denial of Service).
- Un metodo per sottrarre di informazioni.



Vettore di infezione

Infettare il target

Sono due i modi che possono essere intrapresi per infettare una possibile vittima. Questa attività è quasi mai autonoma.

Eseguibile

La strada più semplice è utilizzare un binario inviato al target attraverso la posta elettronica o navigazione web o fake.

Exploit

Viene sfruttata la vulnerabilità di qualche software applicativo (lettore pdf, flash, browser, office doc, Java ecc…) o del sistema operativo.

Drive by download

Web

- Buona parte del traffico Internet è composto da traffico Web.
- Sono numerose le vulnerabilità relative ai browser.

Attaccante

- creare (o compromettere) un sito per ospitare exploit.
- exploit dei browser vulnerabili che visitano il sito.
- far scaricare il codice del worm.

Removing admin rights stymies 92% of Microsoft's bugs

By Gregg Keizer FOLLOW
Computerworld | February 4, 2009

RELATED TOPICS

Windows Security

Nine of out 10 critical bugs reported by Microsoft last year could have been made moot, or at least made less dangerous, if people ran Windows without administrative rights, a developer of enterprise rights management software claimed Tuesday.

MORE GOOD READS

Microsoft changes Windows 7 UAC due to new exploit code

Microsoft caves in, will change Windows 7 UAC

Microsoft cites 'click fatigue' for Windows 7 security change


Command
& Control

Command and control

C & C server

- Termine preso in prestito dal mondo militare.
- Definito anche C2

Funzione

- Server centralizzato (illegale) che impartisce comandi ai computer infetti di una botnet.
- Riceve la segnalazione da parte di nuovi computer infetti.
- Possibilità di invio comandi per un attacco DDOS o per inviare spam.
- La comunicazione può avvenire via IRC.

Necessità

Perché occorre un server C2?

- L'esecuzione del malware può avvenire in scenari non ideali:
  - Può essere inviato in maniera non corretta.
  - Può non avere sufficienti privilegi.
  - Può essere inviato a destinazione a pezzi.
  - Può richiedere dal C2 istruzioni operative su cosa fare (per esempio cryptolocker).
  - Può scaricare successivamente la parte che effettua infezione/attacco.

- Le strutture C2 possono essere date in affitto.

Azioni (I)

Escalation

- La piena “installazione” del malware avviene con:
  - l’acquisizione di maggiori diritti.
  - scaricamento (se necessario) del payload.
  - configurazione del malware.
- Lo stato di escalation termina con il contatto del server C2.
  - La comunicazione verso il server C2 avviene attraverso protocolli e tecniche ben distinte rispetto a quelle usate durante la fase di infezione.

Azioni (II)

Exfiltration

- In questa fase avviene il primo e vero databreach.
- I dati presenti sulla macchina infetta:
  - possono essere spediti al C2.
  - possono essere cancellati.
  - possono essere modificati.
  - possono essere cifrati (cryptolocker).

Angler Exploit Kit

Date	Sid	Signature	Rev	SrcIP	SrcPort	DstIP	DstPort
2016-05-17	2819805	ETPRO TROJAN CryptXXX CnC Beacon	3	private	49198	144.76.82.19	443
2016-05-17	2819805	ETPRO TROJAN CryptXXX CnC Beacon	3	private	49197	144.76.82.19	443
2016-05-17	2820097	ETPRO DELETED CryptXXX 2.06 Checkin	1	private	49197	144.76.82.19	443
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49193
2016-05-17	2811284	ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2	2	5.39.35.232	80	private	49185
2016-05-17	2820164	ETPRO CURRENT_EVENTS Angler EK Payload May 10 2016 M2 T1	2	5.39.35.232	80	private	49185
2016-05-17	2811284	ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2	2	5.39.35.232	80	private	49183
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49185
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49183
2016-05-17	2014726	ET POLICY Outdated Windows Flash Version IE	82	private	49183	5.39.35.232	80
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49183
2016-05-17	2816941	ETPRO CURRENT_EVENTS Angler EK Flash Exploit URI Struct Apr 07 IE	3	private	49183	5.39.35.232	80
2016-05-17	2815888	ETPRO CURRENT_EVENTS Possible Angler EK Landing Jan 21 M3	3	5.39.35.232	80	private	49178
2016-05-17	2816511	ETPRO CURRENT_EVENTS Angler EK Landing Mar 02 2016 M1 T1	2	5.39.35.232	80	private	49178
2016-05-17	2816932	ETPRO CURRENT_EVENTS Angler EK Landing with URI Primer Apr 06	2	5.39.35.232	80	private	49178
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49178
2016-05-17	2022772	ET CURRENT_EVENTS Evil Redirector Leading to EK Apr 28 2016	3	72.167.3.128	80	private	49163

Target Compromised, C2

Exploit / Payload Delivered

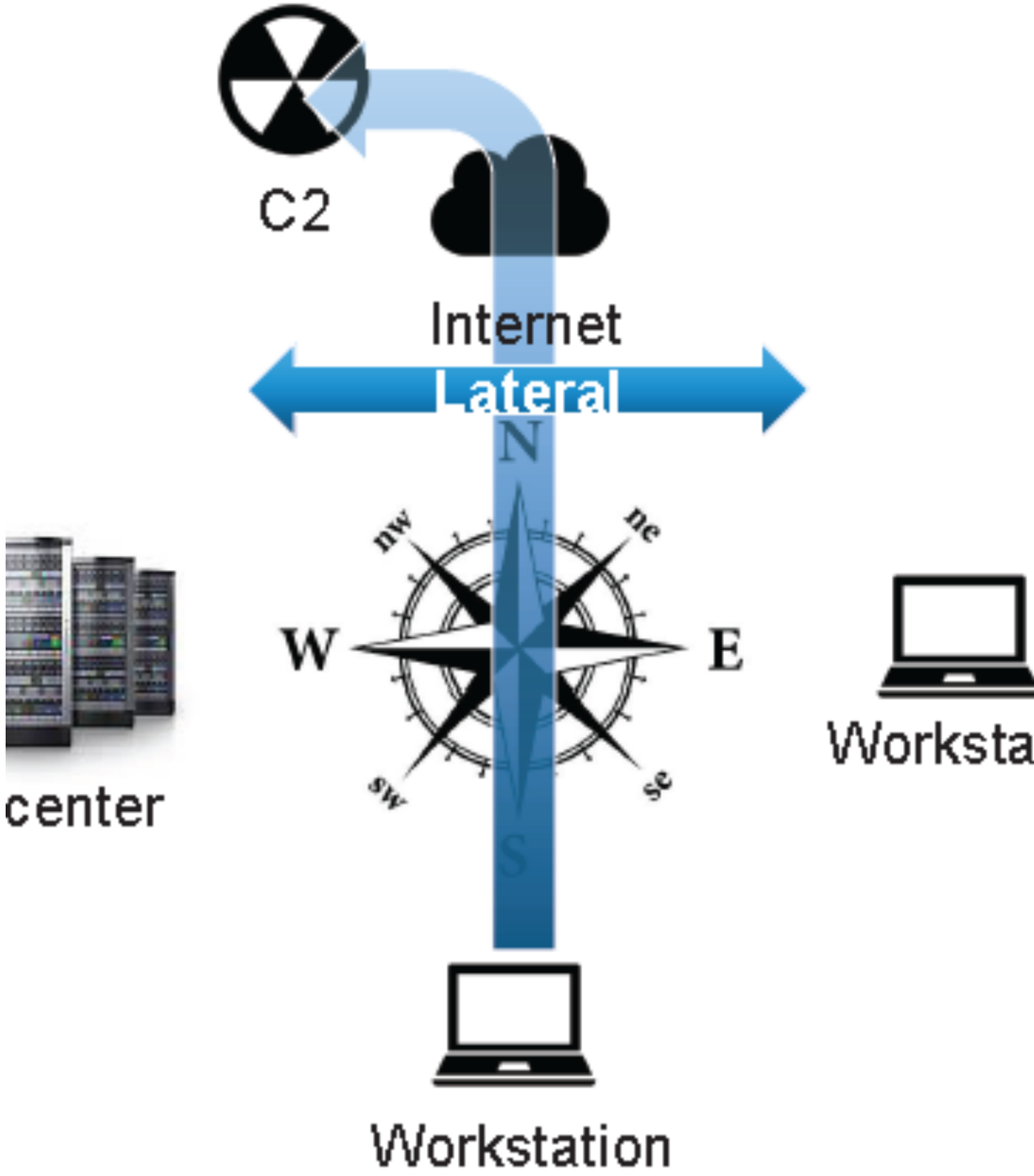
TDS Evaluates Target Client

Redirect to Angler Infrastructure

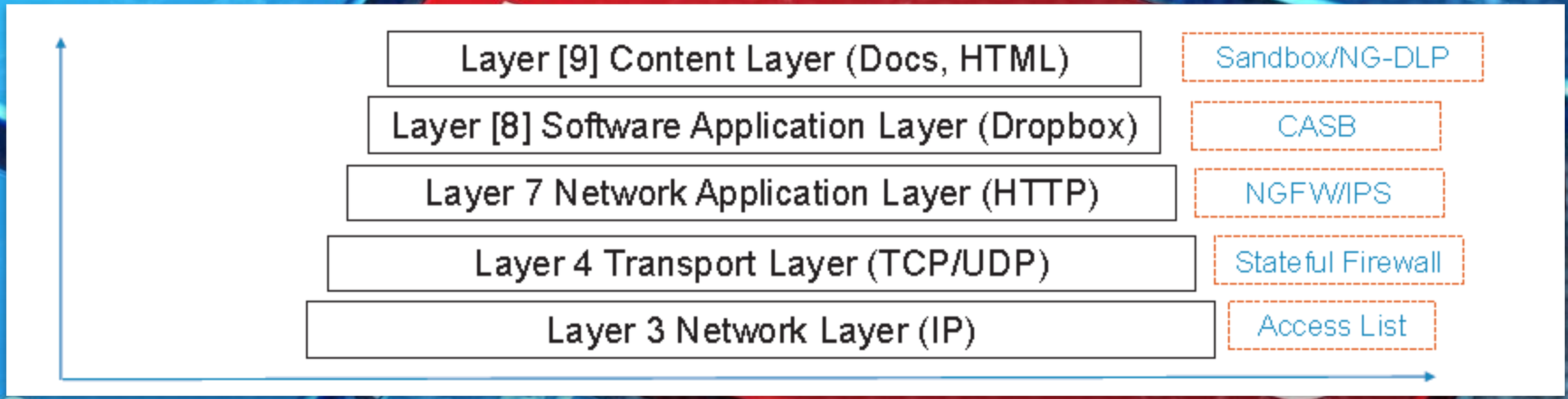
Lateral infection

Di cosa parliamo?

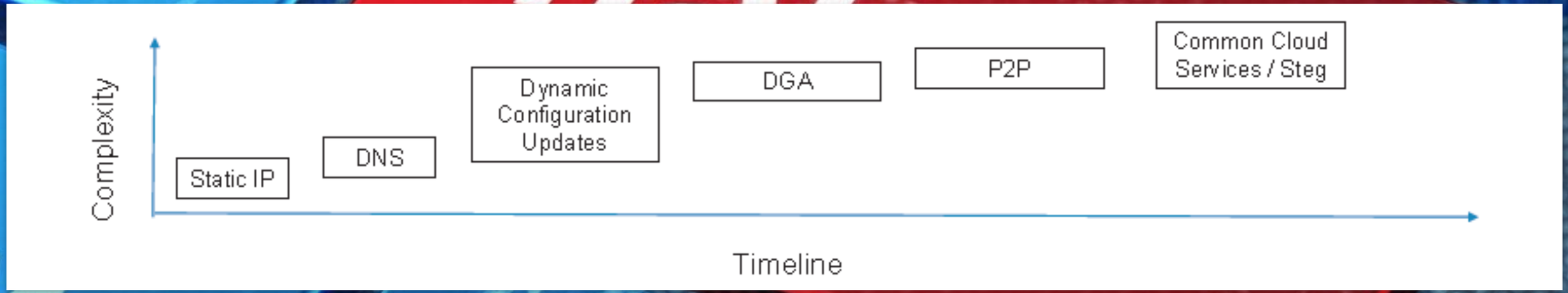
- E' composto da tre fasi:
  - Scansione locale del dispositivo infetto.
  - Scansione di rete e mappatura degli "obiettivi sensibili".
  - Compromissione degli altri dispositivi presenti in rete.
- Può usare protocolli di rete nativi (per esempio SMB) per cancellare o cifrare i dati.
- Può usare protocolli come SMB, RDC, SSH ecc.. per diffondersi.



Evoluzione dell'offuscamento



Evoluzione dell' hosting



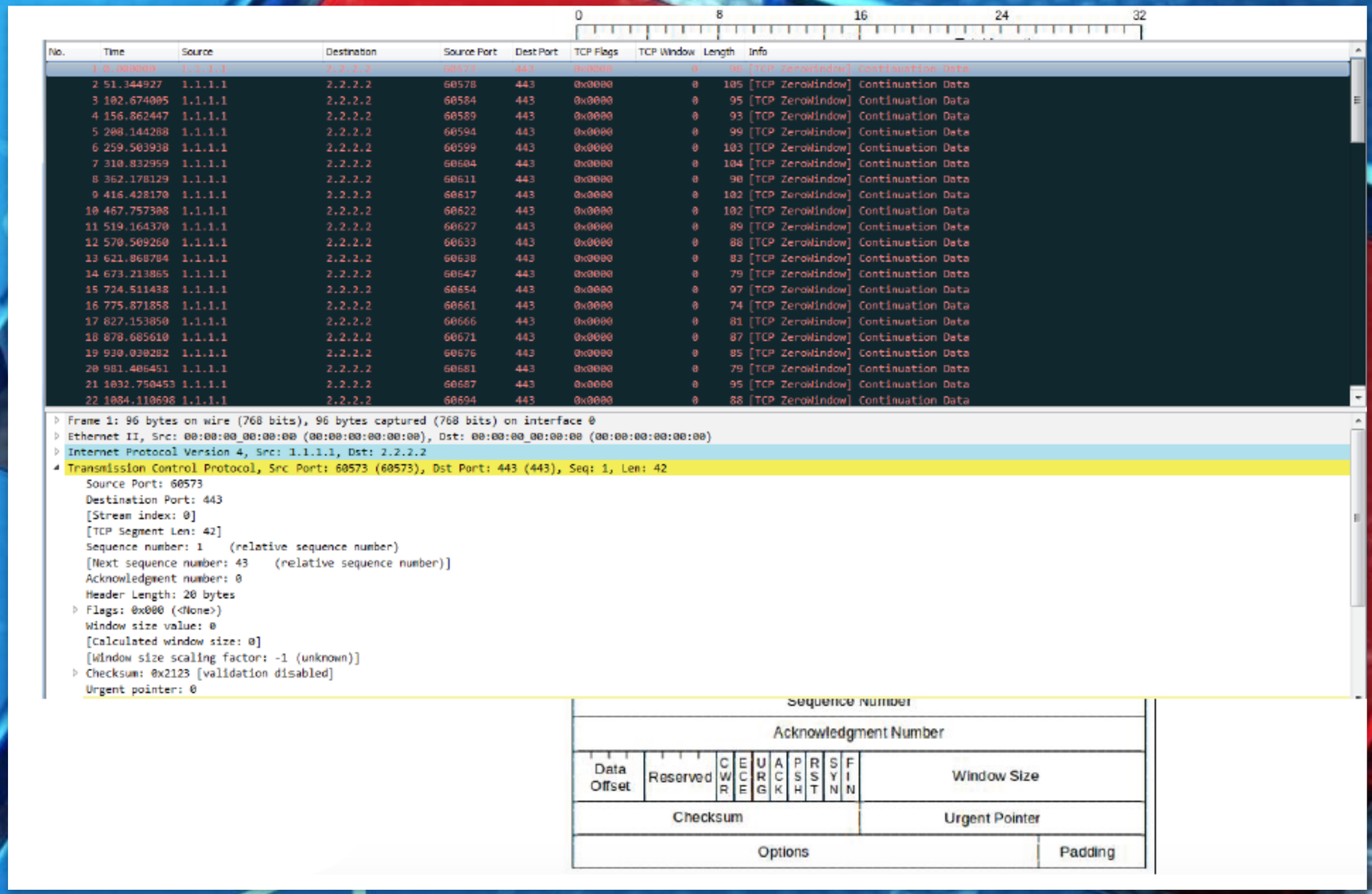
Stenografia

L'arte di saper nascondere

- **La Steganografia è l'arte di nascondere in bella vista**.
- È stata usata per secoli e fornisce una buona soluzione.
- Un malware può sfruttare la Steg per include configurazioni in immagini, nell'audio, nei video, nei metadati e anche protocolli di rete.
- È inoltre possibile sovrapporre la Steg alla crittografia per maggior offuscamento.

- "*Never write if you can speak; never speak if you can nod; never nod if you can wink*."
- Martin Lomasney, Gangster, Politician (1859-1933)

La Steg è una ottima soluzione :(



No.	Time	Source	Destination	Source Port	Dest Port	TCP Flags	TCP Window	Length	Info
1	0.000000	1.1.1.1	2.2.2.2	60573	443	0x0000	0	96	[TCP ZeroWindow] Continuation Data
2	51.344927	1.1.1.1	2.2.2.2	60578	443	0x0000	0	105	[TCP ZeroWindow] Continuation Data
3	102.674005	1.1.1.1	2.2.2.2	60584	443	0x0000	0	95	[TCP ZeroWindow] Continuation Data
4	156.862447	1.1.1.1	2.2.2.2	60589	443	0x0000	0	93	[TCP ZeroWindow] Continuation Data
5	208.144288	1.1.1.1	2.2.2.2	60594	443	0x0000	0	99	[TCP ZeroWindow] Continuation Data
6	259.503938	1.1.1.1	2.2.2.2	60599	443	0x0000	0	103	[TCP ZeroWindow] Continuation Data
7	310.832959	1.1.1.1	2.2.2.2	60604	443	0x0000	0	104	[TCP ZeroWindow] Continuation Data
8	362.178129	1.1.1.1	2.2.2.2	60611	443	0x0000	0	90	[TCP ZeroWindow] Continuation Data
9	416.428170	1.1.1.1	2.2.2.2	60617	443	0x0000	0	102	[TCP ZeroWindow] Continuation Data
10	467.757308	1.1.1.1	2.2.2.2	60622	443	0x0000	0	102	[TCP ZeroWindow] Continuation Data
11	519.164370	1.1.1.1	2.2.2.2	60627	443	0x0000	0	89	[TCP ZeroWindow] Continuation Data
12	570.509260	1.1.1.1	2.2.2.2	60633	443	0x0000	0	88	[TCP ZeroWindow] Continuation Data
13	621.868784	1.1.1.1	2.2.2.2	60638	443	0x0000	0	83	[TCP ZeroWindow] Continuation Data
14	673.213865	1.1.1.1	2.2.2.2	60647	443	0x0000	0	79	[TCP ZeroWindow] Continuation Data
15	724.511438	1.1.1.1	2.2.2.2	60654	443	0x0000	0	97	[TCP ZeroWindow] Continuation Data
16	775.871858	1.1.1.1	2.2.2.2	60661	443	0x0000	0	74	[TCP ZeroWindow] Continuation Data
17	827.153850	1.1.1.1	2.2.2.2	60666	443	0x0000	0	81	[TCP ZeroWindow] Continuation Data
18	878.685610	1.1.1.1	2.2.2.2	60671	443	0x0000	0	87	[TCP ZeroWindow] Continuation Data
19	930.030282	1.1.1.1	2.2.2.2	60676	443	0x0000	0	85	[TCP ZeroWindow] Continuation Data
20	981.406451	1.1.1.1	2.2.2.2	60681	443	0x0000	0	79	[TCP ZeroWindow] Continuation Data
21	1032.750453	1.1.1.1	2.2.2.2	60687	443	0x0000	0	95	[TCP ZeroWindow] Continuation Data
22	1084.110698	1.1.1.1	2.2.2.2	60694	443	0x0000	0	88	[TCP ZeroWindow] Continuation Data

```
Frame 1: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.2
Transmission Control Protocol, Src Port: 60573 (60573), Dst Port: 443 (443), Seq: 1, Len: 42
    Source Port: 60573
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 42]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 43    (relative sequence number)]
    Acknowledgment number: 0
    Header Length: 20 bytes
  ▷ Flags: 0x000 (<None>)
    Window size value: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
  ▷ Checksum: 0x2123 [validation disabled]
    Urgent pointer: 0
```

Crimeware

Crimeware

- Diretto verso tutti.
- Attacco ampiamente distribuito.
- Grande raggio di azione al fine di arrivare allo scopo.

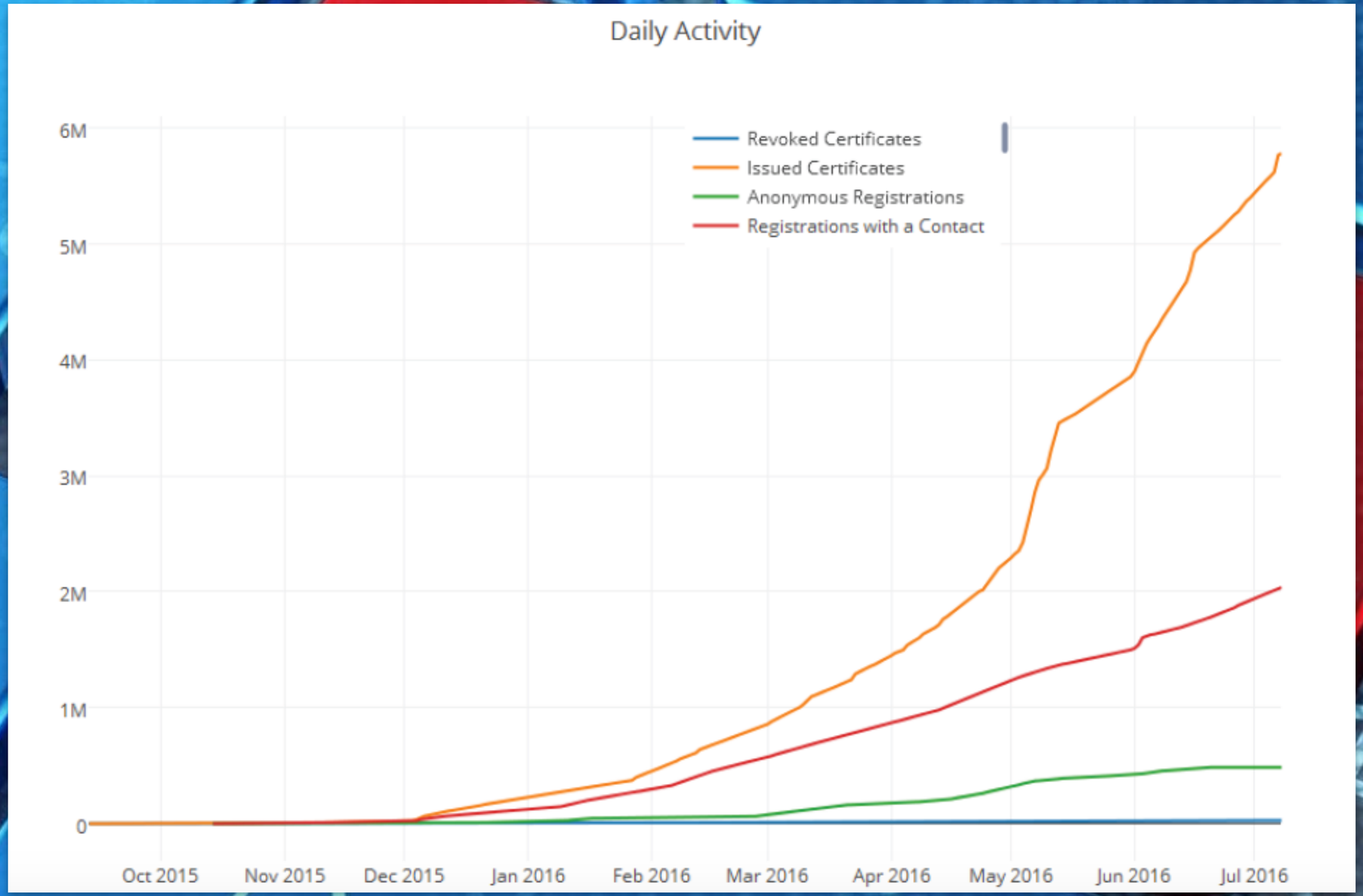
Attacco mirato

- Target ben preciso.
- Vittime ben selezionate.
- Creati ad hoc.
- Piccolo raggio di azione.

Spionaggio mirato

- Spionaggio.
- Soluzione più esotica.
- Molto sofisticato.
- Può usare hardware mirato.

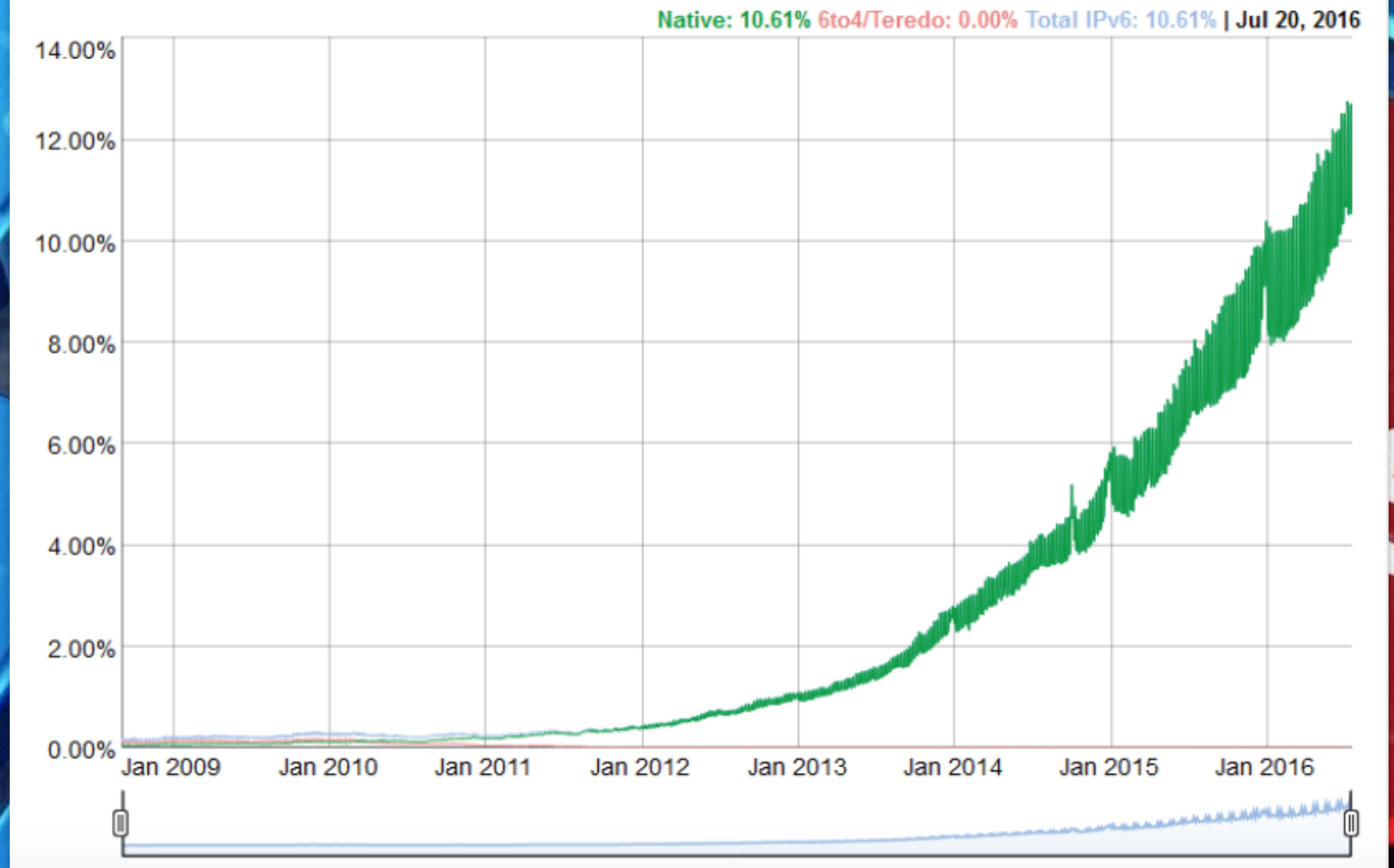
SSL


Daily Activity
6M
5M
4M
3M
2M
1M
0
Revoked Certificates
Issued Certificates
Anonymous Registrations
Registrations with a Contact
Oct 2015
Nov 2015
Dec 2015
Jan 2016
Feb 2016
Mar 2016
Apr 2016
May 2016
Jun 2016
Jul 2016

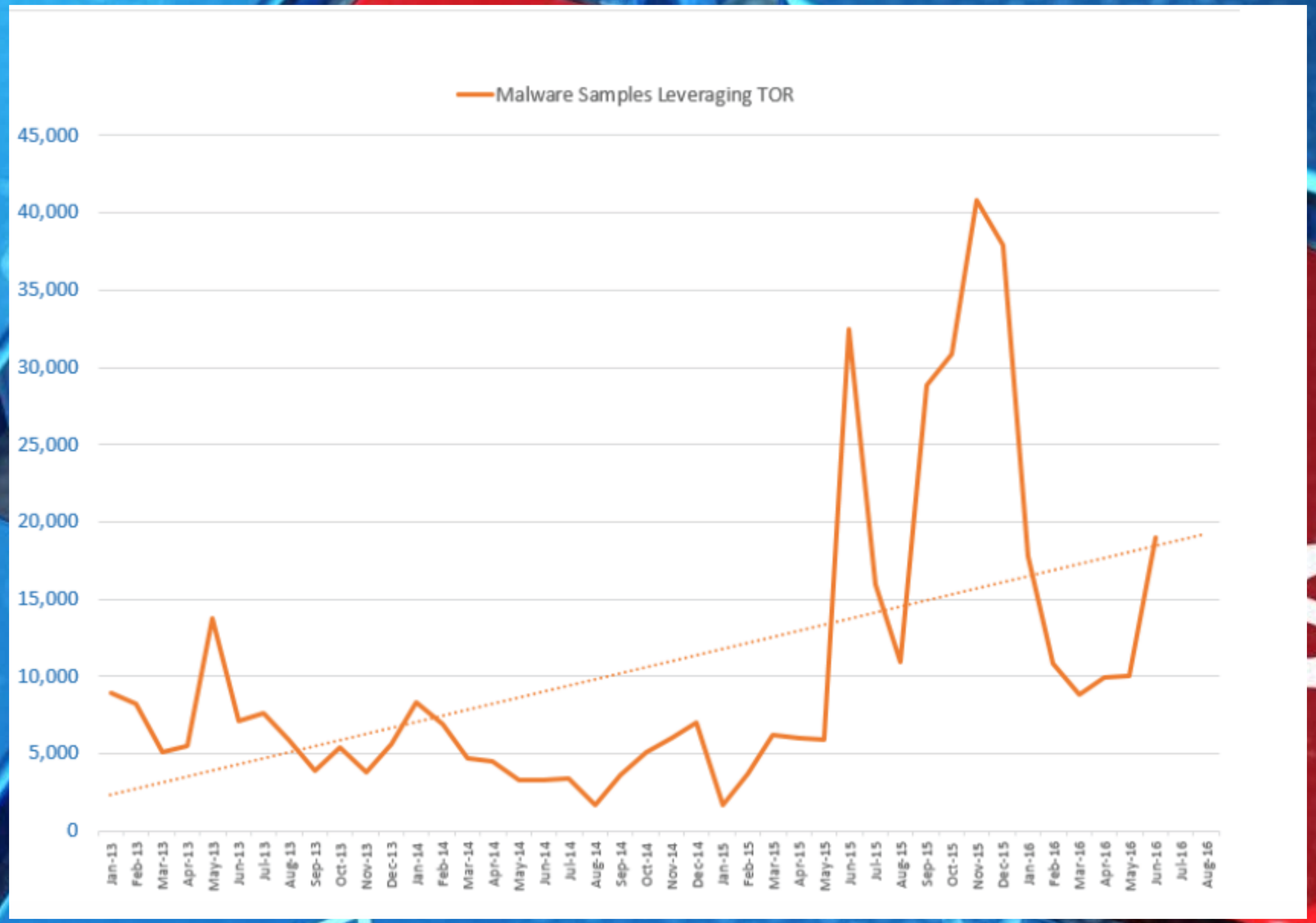
IPv6

IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



TOR


Malware Samples Leveraging TOR
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Jan-13
Feb-13
Mar-13
Apr-13
May-13
Jun-13
Jul-13
Aug-13
Sep-13
Oct-13
Nov-13
Dec-13
Jan-14
Feb-14
Mar-14
Apr-14
May-14
Jun-14
Jul-14
Aug-14
Sep-14
Oct-14
Nov-14
Dec-14
Jan-15
Feb-15
Mar-15
Apr-15
May-15
Jun-15
Jul-15
Aug-15
Sep-15
Oct-15
Nov-15
Dec-15
Jan-16
Feb-16
Mar-16
Apr-16
May-16
Jun-16
Jul-16
Aug-16


Security

Sicurezza

Riconoscimento

- **Riconoscere un malware sta diventando una operazione sempre più complessa e difficile.**
- Qual è la strada migliore da intraprendere?
  - Bloccare l'esecuzione del malware
  - Impedire l'escalation.
  - Evitare che i dati sensibili vadano fuori.
  - Creare maggiori compartimenti stagni.

Meccanismi di difesa (I)

Eliminare ciò che non è buono

- Occorre bloccare:
  - IP
  - Nazioni
  - URLS
- che sono conosciuti come pericolosi.

Meccanismi di difesa (II)

Definire policy corrette sui firewall

- No any any policy.
- Policy per host e per porta.
- Utilizzo di IPS / Layer 7 firewall
  - Blocco di applicazioni non necessarie (p.es.TOR).
  - Bloccare applicazioni non conosciute che generano traffico cifrato.

Meccanismi di difesa (III)

Fingerprint

- Riconoscere i malware attraverso le relative signature.
- Dove è possibile riconosce il malware attraverso un doppio riconoscimento:
  - signature
  - modello comportamentale

Meccanismi di difesa (IV)

Non è possibile difendersi da quello che non si vede

- Usare Ssl “robusto” in modo da evitare Mitm.
- Limitare eventuali “Trusted CA”.
- Usare SSL interception per non ricadere nel security blind spot. :(

Meccanismi di difesa (V)

Certificati

- Bloccare tutti i certificati non validi.
- Verificare le revoche.
- Analizzare i certificati Tls con Suricata o Bro.

Meccanismi di difesa (VI)

Anomaly Detection

- Utilizzare un sistema euristico o di anomaly detection per riconoscere eventuali attività sospette.
- Analizzare i log dei dns alla ricerca di DGA.

Meccanismi di difesa (VII)

Lucidare la ferraglia

- La propria infrastruttura di sicurezza deve essere sempre tenuta alla massima efficienza, configurata nel miglior modo e ben aggiornata.
- “Ascoltate” la vostra ferraglia.

Meccanismi di difesa (VIII)

Ottimi prodotti da usare:

ntop

SURICATA

SNORT®

Consapevolezza

Protezione

Sguardo al futuro

24

Costanza

Fattore Umano

Grazie per l’attenzione

Nell'oscuro mondo dei Malware

Linux Day 2016

Giuseppe Augiero

22 ottobre 2016 - Linux Day 2016 - Facoltà di Ingegneria - Università di Pisa

Email: talk@augiero.it
Twitter: @GiuseppeAugiero
Web: augiero.it