Paolo Giardini
Consulente per la sicurezza delle Informazioni
Eucip Certified Informatics Professional

Skype
vizi privati, pubbliche virtù

Aperilinux - 25 giugno 2008

Vi ricordate di Kazaa?

Nel 2001 Niklas Zennström, Janus Friis, e Priit Kasesalu creano un sistema P2P per lo scambio di file tramite internet.

Esistono 2 versioni di Kazaa, una free ed una a pagamento. Quella free prevede la ricezione di pubblicità.

Il tutto in odore di spyware (GAIN).

La versione 3 di Kazaa include un client Skype...

Skype story

Nell'agosto 2003 prende l'avvio Skype, società con sede in Lussemburgo, i cui fondatori e proprietari sono Niklas Zennström e Janus Friis. *(Toh!)*

Dal 2003 ad oggi la crescita del numero degli utenti si Skype è stata esponenziale. Si calcolano ad oggi in diversi milioni di utenti.

Ragioni di un successo

- Facilità d'uso
- Multipiattaforma
- Funziona anche in ambienti controllati
- Ottima qualità audio anche con poca banda
- Funzioni accessorie (messaggistica, file transfer,...)
- Non contiene spyware ne popup pubblicitari
- Permette il trasferimento di telefonata da e per linee PSTN (public switched telephone network) con SKYPEIN e SKYPEOUT

Ragioni dei timori

- Facilità d'uso (viene usato anche da inesperti)
- Multipiattaforma (non esiste un ambiente sicuro)
- Funziona anche in ambienti controllati (fw?)
- Alto consumo di banda (supernodo)
- Funzioni accessorie (messaggistica, file transfer,...) vulnerabili a virus e trojan
- Problemi nell'interfacciamento PSTN
- EULA

EULA

(End User License Agreement)

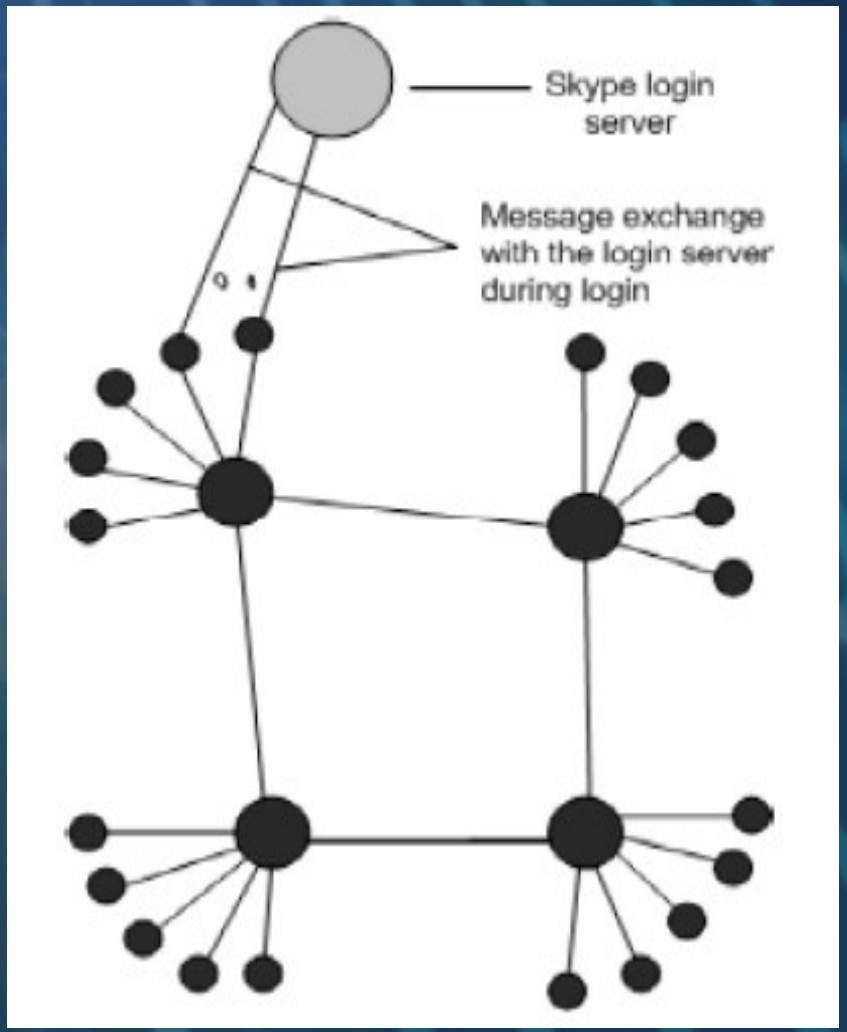
Avete mai perso tempo a leggere i contratti di licenza che vi si presentano quando installate un software?

http://www.skype.com/intl/it/legal/eula

3.3 Uso del computer dell'utente: l'utente concorda che il Software Skype **può utilizzare il processore e la larghezza di banda del computer** (o altro dispositivo del caso) al solo scopo di agevolare le comunicazioni tra l'utente e parti terze. Il Software Skype farà quanto in proprio potere, in misura ragionevole, per proteggere la privacy e l'integrità delle risorse del computer (o altro dispositivo del caso) e delle comunicazioni dell'utente, tuttavia Skype non può dare nessuna garanzia in questo ambito.

Come funziona Skype

- Skype è un programma P2P che si appoggia ai vari client in internet. Questi client sono chiamati NODI.
- Se un NODO possiede determinate caratteristiche (fra le quali un indirizzo IP pubblico non nattato) diviene SUPERNODO.
- Tutte le funzioni di accounting e billing sono demandate ai Server della società



Il Supernodo

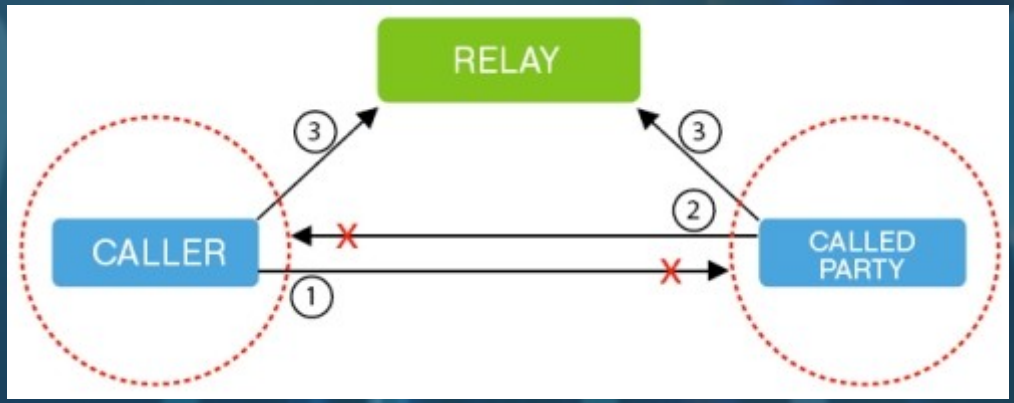
- È un client Skype che non è dietro un NAT e offre servizi al network in modalità trasparente all'utente che potrà solo notare rallentamenti
- Fa da relay ai client dietro firewall
- Contribuisce a mantenere il "Global Index", ovvero il database distribuito degli utenti
- Se viene utilizzato come server di relay consumerà molte risorse

Connect in progress

- All'avvio del programma Skype determina quale tipo di connessione utilizza (IP pubblico, firewall, NAT)
- Cerca quindi di connettersi ad un supernodo per farsi autenticare dal server e far conoscere la propria presenza "online" anche utilizzando tecniche di STUN (Simple Traversal UDP through NAT) e TURN (Traversal using relay NAT) o passando sulla porta 80 o sulla 443
- I client sono in costante contatto con i supernodi
- Gli indirizzi IP dei supernodi sono mantenuti localmente dal client in una lista aggiornata continuamente

Connect!

Una volta "uscito" e messosi in contatto con un supernodo il client ricostruisce la buddy list (contatti) che viene memorizzata nel Global Index. Al momento di iniziare una chiamata se il destinatario è presente nella lista con un ip raggiungibile verrà contattato direttamente, altrimenti verrà richiesto l'intervento di un supernodo per stabilire la connessione. Se i due client potranno farlo, la connessione sarà “punto-punto” altrimenti il supernodo farà da relay.



STUN e TURN

Critto-a-gogo

La crittografia viene usata a piene mani. Ogni comunicazione, IM, Voice, File Transfer, Autenticazione, viene crittografata.
Non vengono usati sistemi di crittografia proprietari (almeno ufficialmente).

Ogni client installato ha all'interno la chiave pubblica di Skype, che viene verificata con la corrispondente chiave privata residente sul server di autenticazione al momento della registrazione.

Registrazione

Al momento della registrazione il client crea una coppia di chiavi RSA e l'hash della password, che vengono memorizzati in locale. Viene quindi stabilita una connessione cifrata AES 256 per comunicare al server lo username scelto, la chiave pubblica e l'hash della password. Se questi soddisfano i requisiti viene generato un certificato per il nuovo utente.

Esistono 2 versioni di certificato, a 1536 bit e 2048 bit. Normalmente viene usato il 1536 mentre il 2048 è per le versioni Premium Service (p.e. skipeout)

Login

Al momento della autenticazione il client genera una chiave di sessione RSA e l'hash della password, che vengono comunicati al server cifrandoli con uno dei 13 o 14 (le fonti sono discordi) certificati pubblici di skype disponibili.

Se le chiavi vengono riconosciute, i dati di login dell'utente vengono passati al Supernodo cifrati con la chiave del server.

A questo punto si popola la buddy list con le chiavi pubbliche degli utenti firmate dal certificato del server.

P2P crittografato

Quando viene stabilita una connessione P2P con un altro client, ogni comunicazione viene crittografata con una chiave di sessione AES 256 creata con i certificati personali degli utenti firmata con la chiave dal server. Ogni chiave ha la durata della sessione, e rimane in memoria fino alla chiusura del client.

Vengono usati anche RC4 per cifrare i pacchetti UDP necessari per stabilire e mantenere la connessione e SHA-1 per generare gli hash

Ma sotto il cofano?

Il protocollo proprietario, quindi per capire come funziona dovrebbe essere utilizzata qualche tecnica di reverse engeneering

però...

- Molto codice, oltre 14 MB il pacchetto .deb! (a cosa serve?)
- Loop inutili, jump calcolati
- Codice ridondante, routine messe ad arte per confondere
- Routine di controllo per decompilatori (se trova softice installato non parte)
- Parte del codice è crittato con una chiave hard coded e decrittato on the fly

Ma sotto il cofano?

alcuni test indicano esistere diversi livelli di protezione del codice
•integrity checks – non è possibile modificare il codice per inserire waypoint ecc.
•alcune parti delle librerie necessarie per il funzionamento del sw non vengono descritte nelle strutture ma vengono caricate solo al runtime
•il codice necessariamente in chiaro è incomprensibile, (tecniche di code obfuscation)
•

Problemi di privacy

E' possibile intercettare una comunicazione Skype?

La risposta può far piacere ad alcuni e paura ad altri (p.e. polizia)

Problemi di privacy

E' possibile intercettare una comunicazione Skype?
La risposta può far piacere ad alcuni e paura ad altri (p.e. polizia)

NO

però:

- Trojan e recorder (mx skype recorder, peccato che non si trovi più il sito)
- Skypein e Skypeout intercettabili al punto di uscita

Problemi di privacy

Dal punto di vista della Polizia Skype è una spina nel fianco, altro che controllo degli Internet Point!

Basta una wireless non protetta, un portatile e skype per essere certi (o almeno abbastanza certi) di non essere controllati.

Da questo punto di vista, ogni tentativo di richiesta di collaborazione a Skype da parte dei vari organi ufficiali è stato vano. Skype ha sempre rifiutato di insererire backdoor o fornire sistemi di decrittazione.

Forse per questo la sede di Skype è in Lussemburgo, USA Docet!

Problemi di sicurezza

Come praticamente tutti i programmi di Instant Messanging anche Skype soffre del problema dei virus, trojan e bestiole simili.

vulnerabilità

- Skype File URI Code Execution Vulnerability 2008-06-05
- Skype Cross-Zone Scripting Security Enhancement 2008-02-06
- Skype skype4com URI Handler Buffer Overflow 2007-12-07
- Skype URI Argument Handling Format String Vulnerability 2006-10-03
- Skype URL Handling File Disclosure Vulnerability 2006-05-19
- Skype Multiple Buffer Overflow Vulnerabilities 2005-10-25
- Skype "skype_profile.jpg" Insecure Temporary File Creation 2005-07-18
- Skype "callto:" URI Handler Buffer Overflow Vulnerability 2004-11-15

virus

Samony.A, W32.Pykspa.D, W32.Pykspa.A, W32.Pykspa.A, WORM_WAREZOV.AP, W32/Skyperise, ...

Fonte http://secunia.com

Giochiamo con Wireshark e Iptables

- Che si può vedere?
  - poco, o meglio, si capisce poco di ciò che passa dato che per la maggior parte è traffico criptato

il primo messaggio scambiato dopo l'installazione contiene la parola “installed”

192.168.2.105 204.9.163.158 HTTP GET http://ui.skype.com/ui/2/2.0.0.72/it/installed HTTP/1.1

Ad ogni successivo avvio viene inviata la parola “getlatestversion”
192.168.2.105 204.9.163.158 HTTP GET http://ui.skype.com/ui/2/2.0.0.72/it/getlatestversion?ver=2.0.0.72&uhash=18cb3c9b58c6938feea08e2caafb09d3d HTTP/1.1

Giochiamo con Wireshark e Iptables

- Cosa si può fare?
  - bloccare UDP non serve
  - bannare gli IP dei server è inutile
  - serve un controllo a livello 7

IPTABLES è inutile in questo campo, meglio rivolgersi a Snort e Squid

SW commerciale

Esistono software commerciali che possono bloccare Skype, o almeno ne chiudono i processi o lo disinstallano forzatamente. Alcuni lavorano a livello 7 riconoscendo i pacchetti skype e bloccandoli. Praticamente tutti solo sw proprietario

- TerminatorX
- Verso Technologies Verso’s NetSpective® M-Class Solution, il sw usato dalla CINA
- La soluzione CISCO, con le versioni IOS PIX superiori a 12
- Sonicwall
- Check Point
- Fortigate
- skypekiller

SW opensource

Si può fare qualcosa anche con il sw open source.
Ad esempio Snort e Squid possono esaminare i pacchetti e applicare le policy definite.
Non si tratta però di una soluzione definitiva, le nuove versioni di Skype implementano sempre nuove tecniche di evasione.

SQUID

Un tentativo è stato quello di bloccare le connessioni dirette verso URL numeriche

```
acl SKYPE url_regex ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+
acl CONNECT method CONNECT

http_access deny CONNECT SKYPE
```

Possiamo stare tranquilli?

Beh.. Insomma.
Se voi state tranquilli sapendo di utilizzare un qualcosa del quale non sapete come funziona e cosa faccia in realtà, che può essere usato per infettare il vs computer o la vostra rete con trojan e virus, che aggiorna si automaticamente (e non possiamo sapere cosa ci sia nella nuova versione), che buca la vostra linea di difesa qualunque cosa abbiate messo su...

Beh, insomma.

Un ultimo consiglio

Se dovessi occuparmi della sicurezza di una entità non mi preoccuperei di come bloccare Skype, MSN, Yahoo, Kazaa, Gnutella, Emule, ...

Mi preoccuperei molto di più sapendo che gli utenti hanno la possibilità di fare quello che vogliono con le macchine assegnate.

La migliore difesa è la prevenzione.

fonti

http://packetprotector.org/forum/viewtopic.php?id=103
http://www.lynanda.com/products/software-for-corporations/traffic-filtering/lynanda-skype-filter
http://share.skype.com/sites/security/trojans_and_viruses/
http://mnet.cs.nthu.edu.tw/paper/Chance/041125.pdf

skype uncovered, silver needle in the skype, vanilla skype - Philippe Biondi e Fabrice Desclaux (2006)
Documentazione pubblica di skype (sul sito)
slide di Andrea “Pila” Ghirardini su Skype e Forensics (2008)
An analysis of the skype P2P Internet Telephony protocol - Salman Baset e Henning Schulzrinne (2004)
Voip and Skype security - Simson Garfinkel (2005)
Skype security evalutation – Tom Berson (2005)
Why and how to block skype - Oscar Santolalla (2007)

Spunti per un prossimo lavoro: come individuare il traffico skype e come bloccarlo con strumenti open source.