

Documento di esempio

Documento in parte asteriscato causa dati personali

Perito Informatico
Vincenzo Errichiello
www.errichiellovincenzo.it
info@errichiellovincenzo.it
00393345434768

ALL'AVVOCATO *****

SEDE

Oggetto: perizia informatica per Procedimento Penale nr. ***** R.G.N.R. mod. *****

Il sottoscritto ERRICHELLO VINCENZO, nato a Napoli il 23.05.1979, residente in ***** ,
perito informatico in possesso delle seguenti specializzazioni:

relaziona a seguito della richiesta a nome e per conto dell'Avv. ***** , richiesta tendente ad attuare verifica informatica volta a chiarire le modalità con le quali è avvenuto il collegamento al server tramite il computer in possesso del sig. ***** , nato a ***** , il ***** , ed ivi residente in via ***** e, quindi, le corrispondenti transazioni bancarie effettuate nel periodo dal 01.01.***** al 3***** .

In particolare, la verifica doveva chiarire le modalità di pagamento effettuate con la carta di credito ***** intestata al sig. ***** , nato a ***** il ***** ed ivi residente, in via *****

La procedura di verifica effettuata ha analizzato le caratteristiche tecniche del computer in possesso del sig. *****

*****Elementi eliminati*****

Dopo una prima scansione antivirus in modalità provvisoria con il Trend Micro Security, è stata rilevata la presenza di 23 virus e di 46 file “maligni” catalogati come “spyware”. Uno di questi file “*.exe” è un keylogger, software che invia tutto quello che viene digitato sulla tastiera alla mail: Игры@mail.ru .

***** aggiornamenti del sistema operativo, che dovrebbero essere eseguiti mensilmente, la superficie d’attacco del sistema operativo, così come configurato, è rimasta pari al 100% e, tramite “Footprinting”, sono state raccolte informazioni sull’obiettivo da attaccare per determinare il profilo di protezione della struttura target, protezioni del tutto assenti.

***** * * * * *

Il “Footprinting” è stato effettuato tramite Test eseguito con “Nmap” su rete locale con “switch procure” e laptop attaccante, infrastruttura creata ad hoc.

“Nmap” è un **network security scanner**, ossia un programma che permette di fare una scansione della rete alla ricerca degli “host” e dei servizi che questi offrono, al fine di creare una “mappa” della rete stessa.

“Nmap” non è solo un semplice **port scanner**, ma è uno strumento in grado di fornire numerosi dettagli sulle macchine scansionate. In pochi secondi è stato possibile conoscere il sistema operativo in uso, il tipo di “device”, l’“uptime” (ossia da quanto tempo il computer risultava attivo), le porte e i programmi che forniscono servizi come la porta “80” e la porta “25”, rispettivamente “http server” ed “smtp server”, il fornitore della scheda di rete ed altri elementi utili per la ricerca delle informazioni richieste.

Successivamente è stato effettuato il “Penetration test” con esecuzione da macchina virtuale (VMWare) linux RedHat 5.0 di Nessus: software di scansione e analisi di computer / server per rilevare eventuali vulnerabilità del sistema operativo e/o del software installato.

Lo scopo dell’utilizzo di Nessus è rilevare:

- vulnerabilità che consentono ad un hacker di controllare o accedere ai dati del sistema;
- configurazioni non corrette (mancanza di patch in particolare);
- presenza di password di default, password vuote o password comuni. Nessus utilizza Hydra per effettuare attacchi di tipo dizionario per scovare le password;
- Denial of Service sul protocollo TCP/IP

Nessus ha rilevato 50 vulnerabilità, causa mancanza patch e service pack. Dette vulnerabilità consentono di eseguire codice maligno da remoto e controllare completamente la macchina attaccata.

Le procedure di “Footprinting” e di “Penetration test” sono le più accreditate a livello internazionale per il rinvenimento di informazioni tali da consentire la codifica di atto non autorizzato dall’utente e come tale ascrivibile alla più ampia specie del “Crimeware”, una sottoclasse della categoria più generale di

malware, che riferisce generalmente al *software* non richiesto eseguito sul computer dell'utente con l'intento di generare azioni malevoli.

Esistono quattro metodi principali attraverso i quali il Crimeware può essere distribuito:

- tecniche di social engineering per convincere l'utente ad aprire e-mail malevoli
- attacchi content injection come il cross-site scripting
- sfruttamento di vulnerabilità di sicurezza
- inserimento di crimeware all'interno di software scaricabile dalla rete.

Una volta installato, il crimeware può essere usato per rubare informazioni di aziende e persone, prendere il controllo del computer o server vittima, effettuare attacchi Denial of Service, inviare spam, ed eseguire altre azioni aggiuntive atte ad ottenere benefici finanziari per l'attaccante.

***** elementi personali *****

CONCLUSIONI

Verificata la presenza dei suindicati virus, degli spyware e del keylogger, nonché l'insieme delle vulnerabilità rilevate, risulta che la macchina in possesso del ***** è attualmente controllata da terze persone, per scopi di natura illecita.

Risulta, altresì che tali persone sono in possesso di tutte le password di accesso ai servizi online dell'utente, tra le quali ricomprendere gli accessi ai conti correnti o servizi finanziari in genere.

Risulta, infine, che è possibile eseguire da remoto qualsiasi tipo di operazione informatica dalla macchina in possesso del ***** verso internet, senza la consapevolezza dell'utente possessore, al quale non risulta alcun tipo di malfunzionamento apparente.

Il sottoscritto ritiene che il sig. ***** sia stato vittima di furto di "identità digitale" e vittima di "crimeware", ovvero "malware", azioni illegali imprevedibili all'utente.

Roma, 29. *****

In Fede

Vincenzo Errichiello