Attacchi di phishing con un trojan “legale”

Mag 20, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, RSS 0

La campagna di phishing sfrutta l’emergenza Covid-19 per distribuire NetSupport Manager, un software di controllo remoto.

Come prendere il controllo di un computer riducendo al minimo le probabilità che l’antivirus invii un allarme quando viene scaricato il trojan? Semplice: basta utilizzare un software di controllo remoto “legale”.

L’allarme relativo a questa strategia è stato lanciato da **Microsoft**, che in un tweet ha segnalato una campagna di diffusione che sfrutta **NetSupport Manager**, un tool di controllo remoto che viene normalmente utilizzato nelle aziende per gestire l’amministrazione a distanza di computer e dispositivi.

> *We’re tracking a massive campaign that delivers the legitimate remote access tool NetSupport Manager using emails with attachments containing malicious Excel 4.0 macros. The COVID-19 themed campaign started on May 12 and has so far used several hundreds of unique attachments. pic.twitter.com/kwxOA0pfXH*
>
> *— Microsoft Security Intelligence (@MsftSecIntel) May 18, 2020*

Il vettore di attacco utilizzato dai pirati informatici non è particolarmente originale: si tratta di file **Excel** che

utilizzano i comandi **Macro** per avviare il download e l’installazione del software. Naturalmente l’utente deve assecondare l’attività dei comandi abilitando la funzionalità Macro.

Poco originale anche l’esca utilizzata: i fogli di calcolo contengono infatti informazioni sulla diffusione del Covid-19 all’interno degli Stati Uniti che sembrano provenire dall’ormai celebre **Johns Hopkins Center**. Una tecnica, quella che sfrutta la pandemia, che sembra però mantenere una buona efficacia anche settimane dopo l’avvio dell’emergenza.

Una volta installato, NetSupport Manager consente ai pirati informatici di controllare in remoto il computer eseguendo qualsiasi tipo di comando a distanza. Agli occhi di un qualsiasi utente, può sembrare un’applicazione legittima che solleva ben pochi sospetti. Tanto più che il nome “Netsupport Client Application” può facilmente passare per un’applicazione di sistema.

Secondo i ricercatori, i cyber criminali utilizzano lo strumento di controllo remoto per installare sul computer compromesso altri programmi e script per “massimizzare” l’impatto.

Condividi l’articolo

Cyber guerriglia incrociata tra Israele e Iran

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/20/attacchi-di-phishing-con-un-trojan-legale/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-di-phishing-con-un-trojan-legale