Si segnala che il relativo software Beijing OnePass –contiene feature built-in che, nel complesso, risultano particolarmente intrusive: si garantisce la persistenza grazie all'autorun all'avvio di Windows; verifica periodicamente l'interazione umana con il sistema operativo; prova a leggere/creare/modificare i certificati ROOT del registro; disabilita i servizi di sicurezza e di backup; è in grado di connettersi a risorse Internet addizionali; raccoglie il contenuto della clipboard; fa screenshot e keylogging. Inoltre, l'applicazione può agire da backdoor, aprendo una porta e mettendosi in ascolto delle connessioni in entrata, grazie al driver wmControl.exe. Infine, è in grado di eludere i meccanismi di analisi.

Si segnalano e-mail malevoli identificati da un documento malevolo chiamato "Манифест.docx" ("Manifest.docx") che scarica ed esegue due template: uno è macro-enabled e l'altro è un oggetto HTML che contiene un exploit per la CVE-2021-26411 Internet Explorer.
Il documento esca utilizzato in questa campagna è una dichiarazione di un gruppo in Crimea che si oppone alle politiche di Putin contro la penisola.

Si segnala un nuovo trojan, denominato FatalRAT, che sembra essere distribuito tramite gruppi e canali Telegram. FatalRAT esegue diversi test prima di infettare completamente un sistema, controllando l'esistenza di macchine virtuali, lo spazio su disco, il numero di processori fisici, la loro temperatura e altri parametri. Se uno dei test fallisce, viene terminata l'infezione. In caso di esito positivo dei test, il malware decripta ogni stringa di configurazione separatamente. Successivamente impedisce all'utente di bloccare il computer utilizzando CTRL+ALT+CANC e avvia l'attività di keylogging. FatalRAT raccoglie informazioni come l'IP pubblico, i processi in esecuzione e lo username e le esfiltra ai C2. Inoltre identifica tutti i prodotti di sicurezza in esecuzione sulla macchina confrontando la lista dei processi con un elenco predefinito di prodotti di sicurezza. FatalRAT ha la possibilità di cancellare i dati da specifici browser (Edge, Chrome, 360Secure Browser, QQBrowser, SogouBrowser e Firefox) in modo da costringere l'utente a reinserire, per esempio, username e password che il malware catturerà con il suo keylogger. Il RAT è capace di muoversi lateralmente nella rete attraverso il bruteforcing delle password deboli. Tra le funzioni di FatalRAT figura l'esecuzione di comandi shell e lo scaricamento di payload aggiuntivi.

Si segnala che l'infostealer Jupyter (Solarmarker) continua ad essere impiegato nell'ambito di operazioni piuttosto sofisticate, mirate soprattutto alla sottrazione di credenziali e cookie. La nuova versione di questa minaccia modulare scritta in .NET
La catena di infezione, viene avviata con false pagine di file sharing ospitate su siti che forniscono questo servizio gratuitamente; da qui le vittime scaricano un PE (portable Executable) che si rivela essere il primo dropper. In seguito avviene l'installazione e l'avvio del primo modulo (d.m./Mars); questo raccoglie informazioni di sistema, si connette col C&C via richieste HTTP POST e coordina le operazioni successive. Ad esso segue Jupyter, che esfiltra dati di vario tipo, fra cui anche quelli di Firefox e Chrome. Infine, Uranus opera da keylogger.
Mars – che adotta schemi di cifratura molto più robusti per le comunicazioni col C&C – apre a due diverse possibili sequenze di infezione; la prima coinvolge un dropper di secondo livello che contiene un programma PDFSam di decoy; nella seconda, che si articola grosso modo come l'altra, le istruzioni e i dati per il dropper sono cablati e non hanno bisogno di essere scritti su un eseguibile aggiuntivo. Di Mars sono note 5 varianti, chiamate "IN-1," "IN-2," "IN-3," "IN-9" e "IN-10". I settori più colpiti sono quelli sanitario.

PERTANTO SI PREGA DI PRESTARE MOLTA ATTENZIONE ALLO SCARICO DI NUOVI SOFTWARE SENZA PREVENTIVA AUTORIZZAZIONE, DELL'APERTURA DI E MAIL DI CUI NON SI E' CERTI DEL MITTENTE.