Analisi Forense del Malware: Come Funziona

Questa presentazione esplora il funzionamento interno del malware, analizzando le sue tecniche di propagazione, evasione e comunicazione. Esamineremo le funzioni di propagazione via email e peer-to-peer, le tecniche di offuscamento e le modalità di comunicazione con i server di comando e controllo. Concluderemo con uno scenario di intelligence sulle possibili modifiche e aggiornamenti del malware.

Funzioni di Propagazione: Email e P2P

Email (Mass Mailing)

Il malware si propaga tramite email, raccogliendo indirizzi da dischi fissi e cartelle di sistema. Filtra gli indirizzi per rimuovere duplicati e indirizzi indesiderati. Genera dinamicamente il messaggio email con mittente e oggetto casuali, allegando una copia di se stesso, spesso in un archivio ZIP.

Peer-to-Peer (P2P)

Si diffonde tramite la rete KaZaA, trovando la cartella di condivisione e copiando se stesso con un nome file scelto casualmente da una lista. L'estensione del file è anch'essa casuale (.exe, .scr, .pif, .bat).

Tecniche di Evasione e Offuscamento

Offuscamento Stringhe

Usa la cifratura ROT13 per nascondere stringhe sensibili nel codice (nomi di file, chiavi di registro, nomi di mutex, comandi SMTP, contenuti delle email, nomi host, ecc.).

Nomi File Ingannevoli

Si installa come taskmon.exe e droppa il componente backdoor come shimgapi.dll, nomi che possono sembrare legittimi. Anche i nomi usati per la diffusione P2P e negli allegati email sono scelti per sembrare innocui o allettanti.

Compressione/Packing

Utilizza il packer UPX per ridurre le dimensioni dell'eseguibile finale e renderne più difficile l'analisi statica.

Comunicazione con Server C&C / Backdoor

1

Backdoor

Il componente principale per il C&C è la backdoor implementata in xproxy.dll (droppato come shimgapi.dll).

2

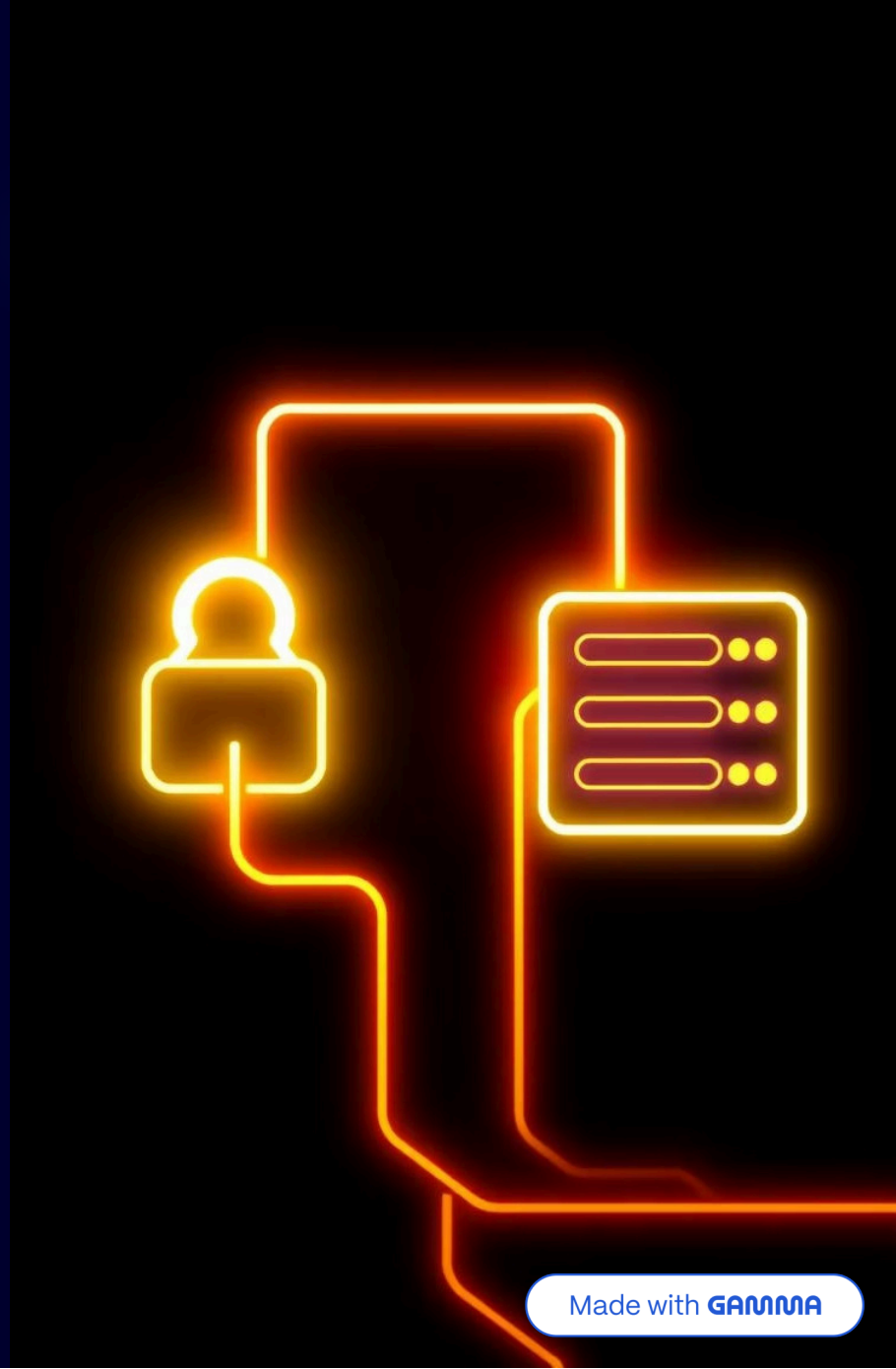
Porte

Questa DLL apre una porta TCP e si mette in ascolto, provando sequenzialmente le porte da 3127 a 3198.

3

Protocollo

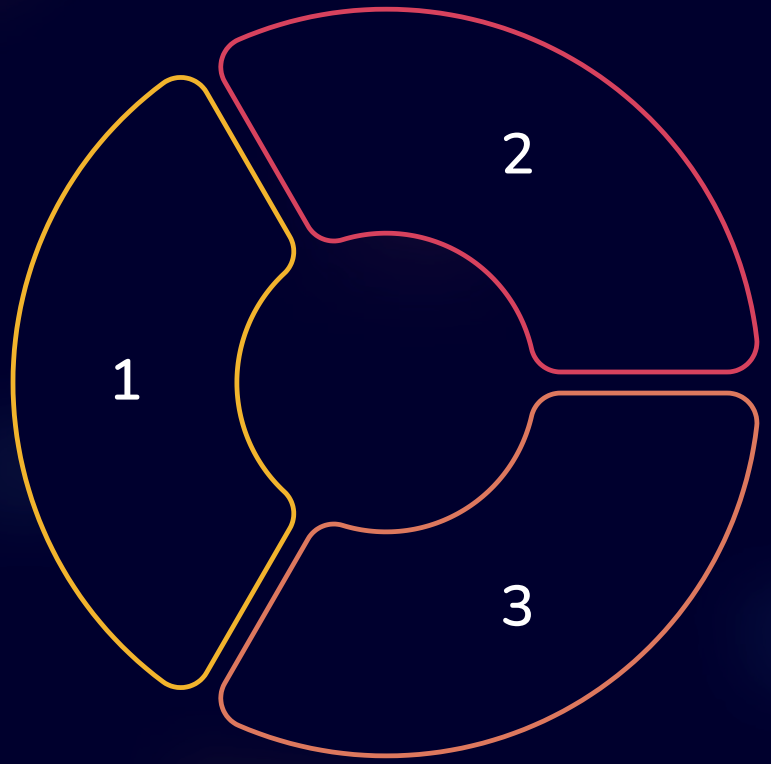
Implementa un server SOCKS4. Questo permette a un attaccante remoto di usare il computer infetto come proxy per instradare il proprio traffico di rete.



Payload Aggiuntivi: DDoS e Installazione

DDoS Attack

Dal 1 Febbraio 2004 al 12 Febbraio 2004, il worm lancia un attacco Denial-of-Service contro il sito www.sco.com. Lancia molti thread che inviano continuamente richieste HTTP parziali al server.



Notepad

Alla prima esecuzione, crea un file temporaneo con dati casuali e lo apre con Notepad, probabilmente per distrarre l'utente o come effetto collaterale non dannoso.

Installazione

Copia se stesso come taskmon.exe nella directory di Sistema o Temp e crea una chiave nel registro per avviarsi ad ogni boot.

Scenario di Intelligence: Possibili Modifiche/Aggiornamenti

1

Target DDoS

Una nuova variante avrebbe probabilmente un target diverso o nessun payload DDoS.

2

Tecniche di Propagazione

Potrebbero essere aggiunti nuovi metodi (es. sfruttamento vulnerabilità, drive USB, social network).

3

Backdoor/C&C

Le porte usate dalla backdoor potrebbero essere cambiate. Il protocollo SOCKS4 potrebbe essere sostituito con un protocollo custom.

Tecniche di Evasione: Aggiornamenti Necessari

Offuscamento

L'offuscamento ROT13 è banale oggi; una nuova variante userebbe tecniche più avanzate.

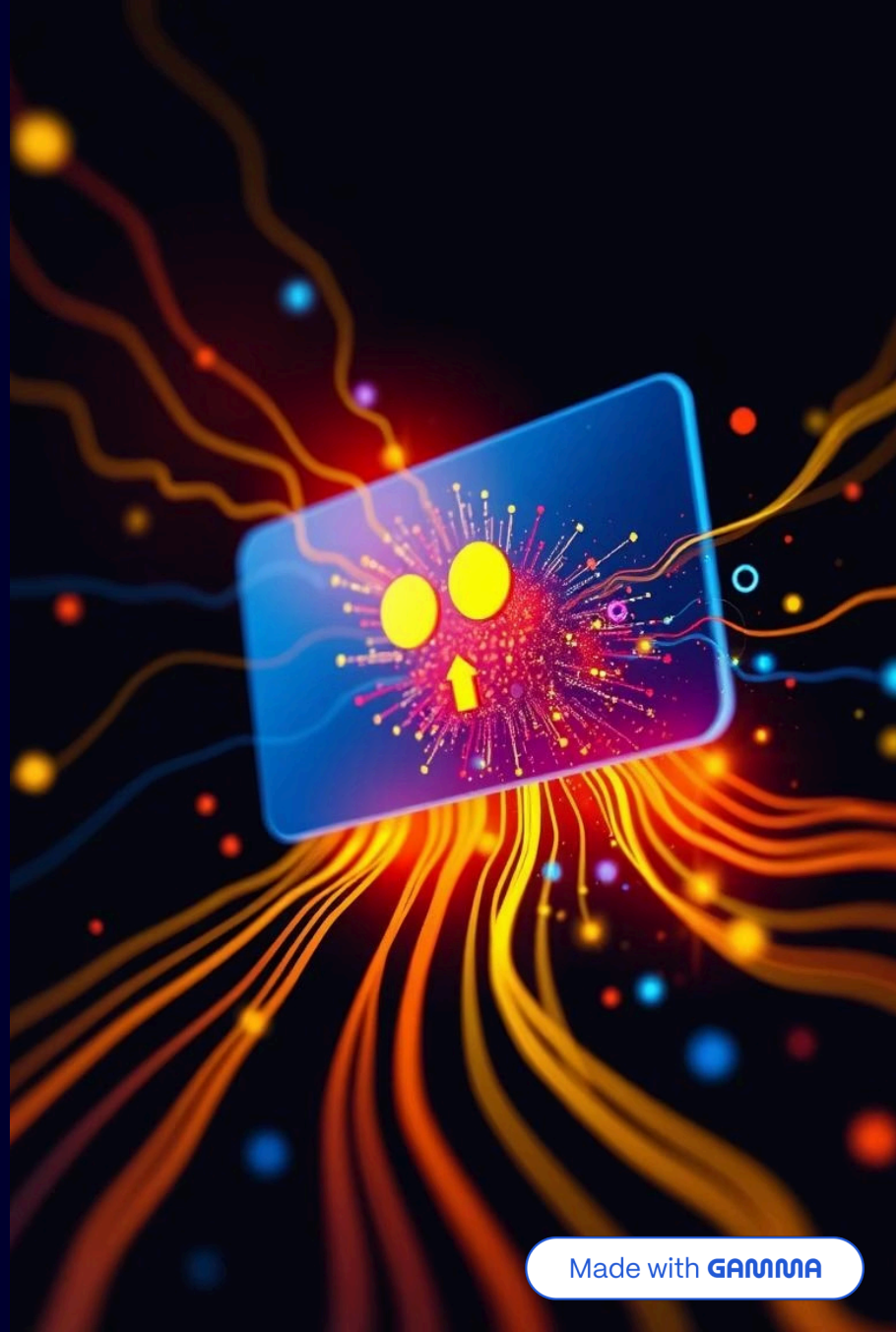
Nomi File

I nomi dei file usati per l'installazione e le chiavi di registro sarebbero probabilmente cambiati.

Payload

Potrebbero essere aggiunti nuovi payload distruttivi o mirati (ransomware, data stealer, cryptominer).

Le tecniche di evasione utilizzate dal malware originale sono obsolete e facilmente rilevabili dai moderni antivirus. Una nuova variante dovrebbe implementare tecniche più sofisticate per eludere i sistemi di sicurezza.



Conclusioni

Il codice fornito corrisponde strettamente alle caratteristiche note del worm MyDoom.A originale. L'analisi rivela le sue capacità di propagazione via email e P2P, il payload DDoS, la backdoor SOCKS4 con capacità di esecuzione remota, e varie tecniche di offuscamento e persistenza tipiche del malware di quell'epoca.

Per contrastare efficacemente le nuove varianti di malware, è fondamentale comprendere le tecniche utilizzate e anticipare le possibili evoluzioni. L'analisi forense e l'intelligence sulle minacce sono strumenti essenziali per proteggere i sistemi informatici.