Glaaki: architettura di supporto al ransomware Hidden Tear in corso di sviluppo

Pubblicato: 03/03/2020 11:14

Categorie: Cyber Crime, Europe, Threat
Tipo di Informazione: Strategico, Tattico, Tecnico
Distribuzione: **TLP:RED**[1] - Declassificato TLP WHITE in data 12/02/2021

Genesi

Da un opsec fail dell'attore **Glaaki** è stato possibile reperire informazioni su future campagne dell'avversario.

Assessment

Le attività di tracciamento del CIOC di TS-WAY hanno reperito il **codice HTML** del **pannello di login** presente **dietro a un tunnel ngrok** utilizzato dall'avversario italiano **Glaaki** in recenti campagne. Nel codice HTML sono presenti vari riferimenti al ransomware open-source **Hidden Tear** e la pagina in corso di sviluppo si presenta come un pannello di login alle informazioni raccolte dal malware.

Tra le informazioni trapelate dal codice c'è anche un **riferimento all'editor HTML di Altervista**, un servizio di hosting web gratuito e Italiano, apparentemente utilizzato anche dall'avversario. L'uso del servizio è compatibile con la locazione geografica attribuita a Glaaki.

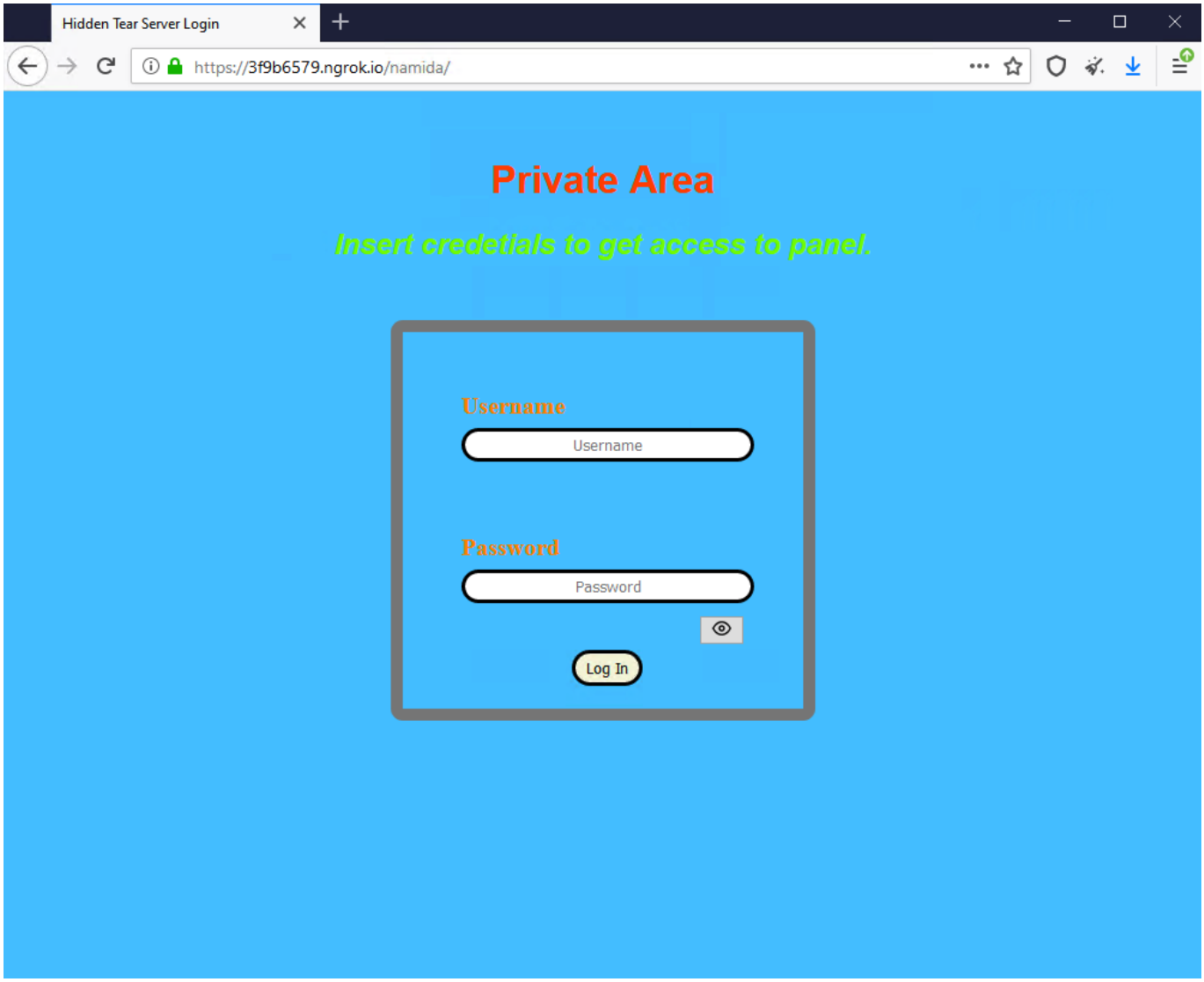
Analizzando le informazioni estratte è possibile attendersi l'**uso del ransomware Hidden Tear in future campagne** dell'avversario.

Questo report in breve

- Reperito il codice HTML di un pannello utilizzato dall'avversario Glaaki come end-point di un tunnel ngrok
- Nel codice sono presenti riferimenti al ransomware open-source Hidden Tear
- Il pannello è stato probabilmente sviluppato usando l'editor HTML di Altervista
- Ci si aspettano future campagne di attacco dell'avversario basate sul ransomware Hidden Tear

Analisi Tecnica

Il pannello web è stato individuato tra gli **endpoint** dei **tunnel ngrok** utilizzati dall'avversario in recenti campagne. Graficamente si presenta come nella figura seguente:



Il nome della directory in cui risiede il pannello è *"namida"* ("lacrima" in giapponese), che richiama il nome del **ransomware "Hidden Tear"**. Nel codice HTML della pagina il malware è citato direttamente:

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="generator" content="AlterVista - Editor HTML"/>
  <title>Hidden Tear Server Login</title>
  <style>
      body{
        background-color: #4DC4FF;
    }
  [... CUT ...]
</html>
```

Il malware **Hidden Tear** è un progetto open-source completamente personalizzabile, che utilizza l'algoritmo AES per la cifratura dei dati e in grado di collegarsi ad una API web custom specificata dallo sviluppatore. È ragionevole concludere che l'avversario stia **sviluppando un pannello personalizzato** per **accedere ai dati raccolti dal ransomware** e stia **predisponendo l'infrastruttura d'attacco** necessaria a **future campagne** basate sullo stesso malware.

Dal codice è presente inoltre un **riferimento all'editor HTML di Altervista**, noto servizio Italiano di Hosting Web gratuito, che l'avversario sta probabilmente utilizzando per lo sviluppo del pannello.

Eventi IOC

1. [1117134] Glaaki custom Hidden Tear login panel (HTML code)

Note

[1] Per maggiori informazioni riguardo le TLP si e' pregati di consultare https://www.us-cert.gov/tlp

Contatti

intel@ts-way.com