TRANSLATEXT, Software S1201 | MITRE ATT&CK®

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	TRANSLATEXT has used HTTP to communicate with the C2 server.[1]
Enterprise	T1185		Browser Session Hijacking	TRANSLATEXT has the ability to use form-grabbing and event-listening to extract data from web data forms.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	TRANSLATEXT has used PowerShell to collect system information and to upload the collected data to a Github repository.[1]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	TRANSLATEXT has stolen credentials stored in Chrome.[1]
Enterprise	T1114		Email Collection	TRANSLATEXT has exfiltrated collected email addresses to the C2 server.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	TRANSLATEXT has exfiltrated collected credentials to the C2 server. [1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	TRANSLATEXT has been named `GoogleTranslate.crx` to masquerade as a legitimate Chrome extension.[1]
Enterprise	T1112		Modify Registry	TRANSLATEXT has modified the following registry key to install itself as the value, granting permission to install specified extensions: `HKCU\Software\Policies\Google\Chrome\ExtensionInstallForcelist`. [1]

Domain	ID		Name	Use
Enterprise	T1012		Query Registry	TRANSLATEXT has queried the following registry key to check for installed Chrome extensions: `HKCU\Software\Policies\Google\Chrome\ExtensionInstallForcelist`. [1]
Enterprise	T1113		Screen Capture	TRANSLATEXT has the ability to capture screenshots of new browser tabs, based on the presence of the `Capture` flag.[1]
Enterprise	T1176	.001	Software Extensions: Browser Extensions	TRANSLATEXT has the ability to capture credentials, cookies, browser screenshots, etc. and to exfiltrate data.[1]
Enterprise	T1539		Steal Web Session Cookie	TRANSLATEXT has exfiltrated updated cookies from Google, Naver, Kakao or Daum to the C2 server.[1]
Enterprise	T1205		Traffic Signaling	TRANSLATEXT has redirected clients to legitimate Gmail, Naver or Kakao pages if the clients connect with no parameters.[1]
Enterprise	T1102	.001	Web Service: Dead Drop Resolver	TRANSLATEXT has used a dead drop resolver to retrieve configurations and commands from a public blog site.[1]
		.002	Web Service: Bidirectional Communication	TRANSLATEXT has used a Github repository for C2.[1]

Source: https://attack.mitre.org/software/S1201