Lumma Stealer actively deployed in multiple campaigns

By Intrinsec

Published: 2023-10-17 · Archived: 2026-04-05 21:27:01 UTC

[et_pb_section fb_built="1" _builder_version="4.16" global_colors_info="{}"][et_pb_row column_structure="1_2,1_2" _builder_version="4.16" _module_preset="default" custom_margin="|6px||6px||" custom_padding="85px|0px||||" global_colors_info="{}"][et_pb_column type="1_2" _builder_version="4.16" _module_preset="default" global_colors_info="{}"][et_pb_text _builder_version="4.22.2" _module_preset="default" text_font="|600|||||||" header_font="|600|||||||" custom_margin="-15px||-1px||false|false" custom_padding="0px|||||" global_colors_info="{}"]

LummaC2 Stealer

[/et_pb_text][et_pb_text _builder_version="4.22.2" _module_preset="default" text_text_color="#000000" custom_margin="|68px||||" custom_padding="27px|0px||||" global_colors_info="{}"]

Key findings

In this report are presented:

Lumma Stealer, also known as LummaC2 Stealer, is a malware-as-a-service sold through Telegram and Russian-speaking cybercrime forums. In this report, the following will be addressed:

- The presence of Lumma in Russian-speaking forums and Telegram.
- Code analysis of different campaigns distributing Lumma stealer using various techniques.
- The infrastructure associated with Lumma stealer, including the old and new versions of C2 panels.A trail, that we uncovered, which indicates a potential use of Lumma by a Russian intrusion set.

Intrinsec's CTI services

Organisations are facing a rise in the sophistication of threat actors and intrusion sets. To address these evolving threats, it is now necessary to take a proactive approach in the detection and analysis of any element deemed malicious. Such a hands-on approach allows companies to anticipate, or at least react as quickly as possible to the compromises they face.

For this report, shared with our clients in July 2023, Intrinsec relied on its Cyber Threat Intelligence service, which provides its customers with high value-added, contextualized and actionable intelligence to understand and contain cyber threats. Our CTI team consolidates data & information gathered from our security monitoring services (SOC, MDR …), our incident response team (CERT-Intrinsec) and custom cyber intelligence generated by our analysts using custom heuristics, honeypots, hunting, reverse-engineering & pivots.

Intrinsec also offers various services around Cyber Threat Intelligence:

- Risk anticipation: which can be leveraged to continuously adapt the detection & response capabilities of our clients' existing tools (EDR, XDR, SIEM, …) through:
  - **an operational feed of IOCs based on our exclusive activities.**
  - **threat intel notes & reports, TIP-compliant.**
- Digital risk monitoring:
  - **data leak detection & remediation**
  - **external asset security monitoring (EASM)**
  - **brand protection**

For more information, go to htbqccsz.elementor.cloud/en/cyber-threat-intelligence/.

Follow us on Linkedin and Twitter

[/et_pb_text][et_pb_button button_url="https://www.intrinsec.com/wp-content/uploads/2023/10/TLP-CLEAR-Lumma-Stealer-EN-Information-report.pdf" button_text="Continue reading" _builder_version="4.22.2" _module_preset="default" custom_button="on" button_border_radius="40px" button_icon=" ||divi||400" box_shadow_style="preset1" global_colors_info="{}"][/et_pb_button][/et_pb_column][et_pb_column type="1_2" _builder_version="4.16" _module_preset="default" global_colors_info="{}"][et_pb_image src="https://www.intrinsec.com/wp-content/uploads/2023/10/Lumma_Stealer-scaled.jpg" alt="Cybersecurity_Energy" title_text="Lumma_Stealer" align="center" _builder_version="4.22.2" _module_preset="default" width="76%" module_alignment="center" global_colors_info="{}"][/et_pb_image][/et_pb_column][/et_pb_row][et_pb_row _builder_version="4.16" _module_preset="default" global_colors_info="{}"][et_pb_column type="4_4" _builder_version="4.16" _module_preset="default" global_colors_info="{}"][et_pb_text _builder_version="4.16" _module_preset="default" text_font="|600|||||||" text_font_size="35px" text_orientation="center" global_colors_info="{}"]

Other analysis

[/et_pb_text][et_pb_divider divider_weight="3px" _builder_version="4.16″ _module_preset="default" width="10%" module_alignment="center" global_colors_info="{}"][/et_pb_divider][et_pb_blog fullwidth="off" include_categories="1584″ excerpt_length="150″ show_author="off" show_date="off" show_categories="off" masonry_tile_background_color="RGBA(255,255,255,0)" _builder_version="4.16″ _module_preset="default" header_font="|600|||||||" body_font="|300|||||||" body_text_color="#000000″ width="80%" module_alignment="center" custom_margin="|||0px|false|false" custom_padding="0px|||0px|false|false" animation_style="fade" animation_duration="2000ms" enable_grid_motion="on" border_radii="on|20px|20px|20px|20px" border_width_top="0px" border_color_top="RGBA(255,255,255,0)" box_shadow_style="preset1″ box_shadow_blur="14px" box_shadow_spread="-3px" global_colors_info="{}"][/et_pb_blog][/et_pb_column][/et_pb_row][/et_pb_section][et_pb_section fb_built="1″ _builder_version="4.16″ _module_preset="default" global_colors_info="{}"][et_pb_row column_structure="1_2,1_2″ admin_label="12 Days of Christmas – Day 05 Contact Form Module 1″ _builder_version="4.16″ background_size="initial" background_position="top_left" background_repeat="repeat" max_width="1516px" custom_margin="||100px||false|false" custom_padding="50px|30px|50px|64px|false|false" custom_css_main_element=" z-index: 9;" border_radii="on|10px|10px|10px|10px" box_shadow_style="preset1″ box_shadow_blur="10px" use_custom_width="on" custom_width_px="1516px" global_colors_info="{}"]

[et_pb_column type="1_2″ _builder_version="4.16″ custom_padding="6px|||" global_colors_info="{}" custom_padding__hover="|||"][et_pb_text admin_label="Lorem Ipsum" _builder_version="4.16″ text_font="Lato|||on|||||" text_text_color="#a7a7a7″ text_font_size="16px" custom_margin="|0%|-20px|0px" custom_padding="0%|0%|0%|0%" custom_css_main_element="float: none !important;" global_colors_info="{}"][/et_pb_text][et_pb_cta title="N'hésitez pas à nous contacter" button_url="/nos-expertises-en-securite-informatique/" button_text="Découvrez nos expertises" admin_label="Where do you want to go today?" _builder_version="4.16″ header_font="Poppins|500|||||||" header_text_align="left" header_text_color="#000000″ header_font_size="32px" header_letter_spacing="0.6px" header_line_height="120%" body_font="Poppins|||||||||" body_text_color="#000000″ body_font_size="17px" body_line_height="30px" use_background_color="off" custom_button="on" button_text_size="18px" button_text_color="#ffffff" button_bg_color="#c41718″ button_border_width="1px" button_border_color="#c41718″ button_border_radius="40px" button_font="Montserrat|500|||||||" button_use_icon="off" button_alignment="left" text_orientation="left" background_layout="light" max_width="568px" max_width_tablet="100%" max_width_phone="" max_width_last_edited="on|tablet" custom_margin="30px|||" custom_margin_tablet="" custom_margin_phone="|||" custom_margin_last_edited="on|desktop" custom_padding="|||" header_font_size_tablet="30px" header_font_size_phone="26″ header_font_size_last_edited="on|phone" header_line_height_tablet="" header_line_height_phone="" header_line_height_last_edited="on|desktop" body_font_size_tablet="" body_font_size_phone="" body_font_size_last_edited="on|phone" button_text_size_tablet="" button_text_size_phone="17px" button_text_size_last_edited="on|phone" custom_css_promo_button="padding: 11px 2.2vw !important;||margin-top: 37px !important;" custom_css_promo_title=" font-weight: 400;|| padding-bottom: 18px;" box_shadow_style_button="preset1″ button_text_color_hover="#c41718″ button_border_color_hover="#c41718″ button_border_radius_hover="2px" button_bg_color_hover="#ffffff" global_colors_info="{}" button_text_size__hover_enabled="off" button_one_text_size__hover_enabled="off" button_two_text_size__hover_enabled="off" button_text_color__hover_enabled="on" button_text_color__hover="#c41718″ button_one_text_color__hover_enabled="off" button_two_text_color__hover_enabled="off" button_border_width__hover_enabled="off" button_one_border_width__hover_enabled="off" button_two_border_width__hover_enabled="off" button_border_color__hover_enabled="on" button_border_color__hover="#c41718″ button_one_border_color__hover_enabled="off" button_two_border_color__hover_enabled="off" button_border_radius__hover_enabled="on|desktop" button_border_radius__hover="40px" button_one_border_radius__hover_enabled="off" button_two_border_radius__hover_enabled="off" button_letter_spacing__hover_enabled="off" button_one_letter_spacing__hover_enabled="off" button_two_letter_spacing__hover_enabled="off" button_bg_color__hover_enabled="on" button_bg_color__hover="#ffffff" button_one_bg_color__hover_enabled="off" button_two_bg_color__hover_enabled="off"]

Laissez-nous un message décrivant vos besoins en sécurité, ou bien contactez-nous si vous souhaitez avoir des informations concernant nos activités. Nous vous répondrons dans les meilleurs délais.

N'oubliez pas de renseigner votre adresse e-mail ou téléphone afin que nous puissions vous recontacter rapidement.

[/et_pb_cta][/et_pb_column][et_pb_column type="1_2″ _builder_version="4.16″ custom_padding="|||" global_colors_info="{}" custom_padding__hover="|||"][et_pb_contact_form captcha="off" email="contact@intrinsec.com" success_message="Votre message a bien été envoyé" submit_button_text="Envoyer" admin_label="Day 05 Contact Form Module 1″ module_id="et_pb_contact_form_1″ _builder_version="4.16″ _unique_id="538efec8-3317-4a98-b5a1-5cf0b096fc6d" form_field_background_color="#ffffff" form_field_text_color="#b3b3b3″ form_field_focus_text_color="#000000″ title_font="Poppins|700|||||||" title_text_align="left" title_text_color="#000000″ title_font_size="24″ title_letter_spacing="0.6px" form_field_font="Poppins|||||||||" form_field_text_align="left" form_field_font_size="16px" background_color="#ffffff" custom_button="on" button_text_size="20px" button_text_color="#000000″ button_bg_color="RGBA(255,255,255,0)" button_border_width="0px" button_border_color="#000000″ button_border_radius="0px" button_font="Poppins|||||||||" button_icon=" ||fa||400″ button_icon_color="#E02B20″ button_icon_placement="left" button_on_hover="off" button_custom_margin="||0px|0px|false|false" button_custom_padding="0px|0px||0px|false|false" text_orientation="left" custom_padding="3.7vw|2.9vw|3.7vw|2.9vw" custom_css_main_element="box-shadow: 0px 4px 47px 0px rgba(160, 190, 212, 0.22);||border-radius: 10px;" custom_css_contact_button=" width: 100%;|| margin: 0;|| padding: 12px 0 !important;" custom_css_contact_fields="border-bottom: 3px solid #dbdbdb !important;|| padding: 20px 0 20px 0px!important;" custom_css_text_field=" height: 242px !important;|| resize: none !important;||border-bottom: 3px solid #dbdbdb !important;|| padding: 20px 0 20px 0px!important;||overflow: hidden;|| display: block;|| margin-bottom: 14px;" border_radii="on|0px|0px|0px|0px" input_border_radius="0px" form_background_color="#ffffff" global_colors_info="{}"][et_pb_contact_field field_id="Name" field_title="Votre nom" fullwidth_field="on" _builder_version="4.16″ form_field_font="||||" form_field_font_size_tablet="" form_field_font_size_phone="" form_field_font_size_last_edited="on|desktop" use_border_color="off" global_colors_info="{}" button_text_size__hover_enabled="off" button_one_text_size__hover_enabled="off" button_two_text_size__hover_enabled="off" button_text_color__hover_enabled="off" button_one_text_color__hover_enabled="off" button_two_text_color__hover_enabled="off" button_border_width__hover_enabled="off" button_one_border_width__hover_enabled="off" button_two_border_width__hover_enabled="off" button_border_color__hover_enabled="off" button_one_border_color__hover_enabled="off" button_two_border_color__hover_enabled="off" button_border_radius__hover_enabled="off" button_one_border_radius__hover_enabled="off" button_two_border_radius__hover_enabled="off" button_letter_spacing__hover_enabled="off" button_one_letter_spacing__hover_enabled="off" button_two_letter_spacing__hover_enabled="off" button_bg_color__hover_enabled="off" button_one_bg_color__hover_enabled="off" button_two_bg_color__hover_enabled="off"][/et_pb_contact_field][et_pb_contact_field field_id="Prénom" field_title="Votre prénom" fullwidth_field="on" _builder_version="4.16″ form_field_font="||||" use_border_color="off" global_colors_info="{}" button_text_size__hover_enabled="off" button_one_text_size__hover_enabled="off" button_two_text_size__hover_enabled="off" button_text_color__hover_enabled="off" button_one_text_color__hover_enabled="off" button_two_text_color__hover_enabled="off" button_border_width__hover_enabled="off" button_one_border_width__hover_enabled="off" button_two_border_width__hover_enabled="off" button_border_color__hover_enabled="off" button_one_border_color__hover_enabled="off" button_two_border_color__hover_enabled="off"

button_border_radius__hover_enabled=”off” button_one_border_radius__hover_enabled=”off” button_two_border_radius__hover_enabled=”off” button_letter_spacing__hover_enabled=”off” button_one_letter_spacing__hover_enabled=”off” button_two_letter_spacing__hover_enabled=”off” button_bg_color__hover_enabled=”off” button_one_bg_color__hover_enabled=”off” button_two_bg_color__hover_enabled=”off”][/et_pb_contact_field][et_pb_contact_field field_id=”Votre_email” field_title=”Votre email” field_type=”email” fullwidth_field=”on” _builder_version=”4.16″ form_field_font=”||||” use_border_color=”off” global_colors_info=”{}” button_text_size__hover_enabled=”off” button_one_text_size__hover_enabled=”off” button_two_text_size__hover_enabled=”off” button_text_color__hover_enabled=”off” button_one_text_color__hover_enabled=”off” button_two_text_color__hover_enabled=”off” button_border_width__hover_enabled=”off” button_one_border_width__hover_enabled=”off” button_two_border_width__hover_enabled=”off” button_border_color__hover_enabled=”off” button_one_border_color__hover_enabled=”off” button_two_border_color__hover_enabled=”off” button_border_radius__hover_enabled=”off” button_one_border_radius__hover_enabled=”off” button_two_border_radius__hover_enabled=”off” button_letter_spacing__hover_enabled=”off” button_one_letter_spacing__hover_enabled=”off” button_two_letter_spacing__hover_enabled=”off” button_bg_color__hover_enabled=”off” button_one_bg_color__hover_enabled=”off” button_two_bg_color__hover_enabled=”off”][/et_pb_contact_field][et_pb_contact_field field_id=”Décrivez-nous_vos_besoins” field_title=”Décrivez-nous vos besoins” field_type=”text” fullwidth_field=”on” _builder_version=”4.16″ form_field_font=”||||” use_border_color=”off” global_colors_info=”{}” button_text_size__hover_enabled=”off” button_one_text_size__hover_enabled=”off” button_two_text_size__hover_enabled=”off” button_text_color__hover_enabled=”off” button_one_text_color__hover_enabled=”off” button_two_text_color__hover_enabled=”off” button_border_width__hover_enabled=”off” button_one_border_width__hover_enabled=”off” button_two_border_width__hover_enabled=”off” button_border_color__hover_enabled=”off” button_one_border_color__hover_enabled=”off” button_two_border_color__hover_enabled=”off” button_border_radius__hover_enabled=”off” button_one_border_radius__hover_enabled=”off” button_two_border_radius__hover_enabled=”off” button_letter_spacing__hover_enabled=”off” button_one_letter_spacing__hover_enabled=”off” button_two_letter_spacing__hover_enabled=”off” button_bg_color__hover_enabled=”off” button_one_bg_color__hover_enabled=”off” button_two_bg_color__hover_enabled=”off”][/et_pb_contact_field][et_pb_contact_field field_id=”source” field_title=”Comment avez-vous connu Intrinsec ?” fullwidth_field=”on” _builder_version=”4.16″ global_colors_info=”{}”][/et_pb_contact_field][/et_pb_contact_form][/et_pb_column][/et_pb_row][/et_pb_section]
