

An analysis of CrystalX commercial RAT with prankware features

SL securelist.com/crystalx-rat-with-prankware-features/119283

GReAT

April 1, 2026



Introduction

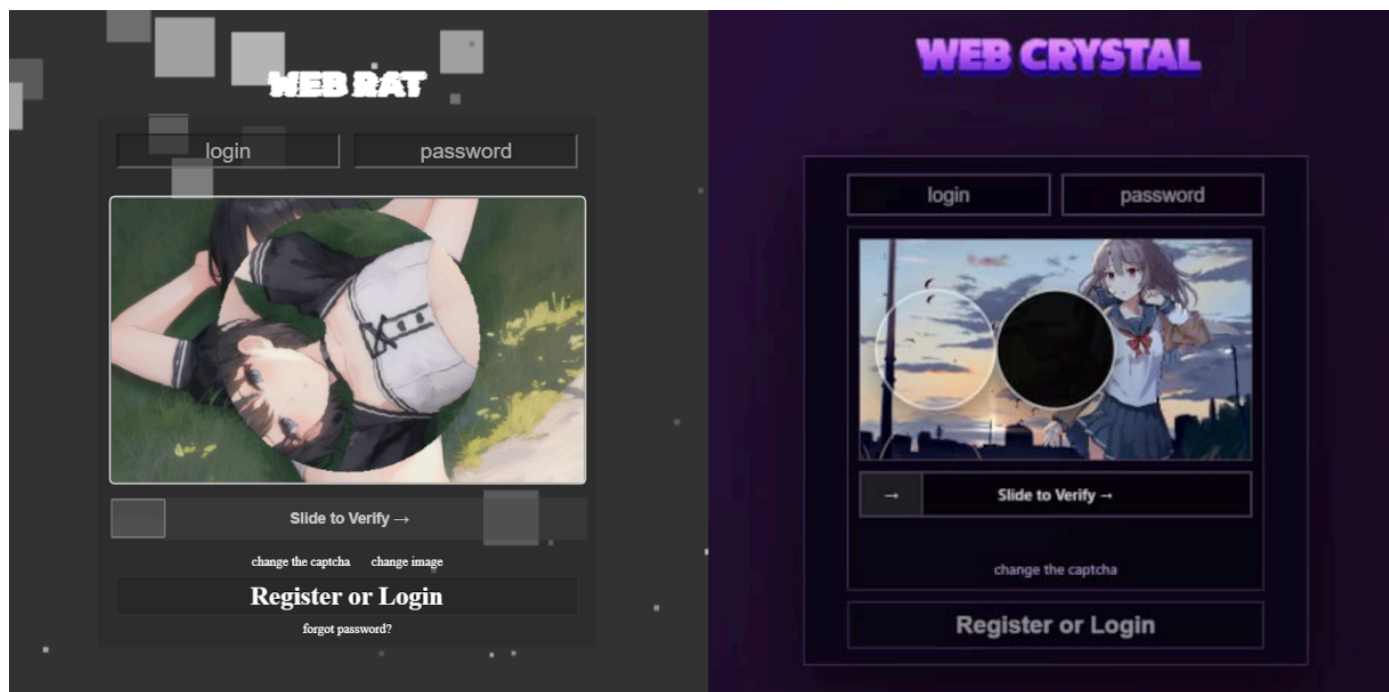
In March 2026, we discovered an active campaign promoting previously unknown malware in private Telegram chats. The Trojan was offered as a MaaS (malware-as-a-service) with three subscription tiers. It caught our attention because of its extensive arsenal of capabilities. On the panel provided to third-party actors, in addition to the standard features of RAT-like malware, a stealer, keylogger, clipper, and spyware are also available. Most surprisingly, it also includes prankware capabilities: a large set of features designed to trick, annoy, and troll the user. Such a combination of capabilities makes it a rather unique Trojan in its category.

Kaspersky's products detect this threat as Backdoor.Win64.CrystalX.*, Trojan.Win64.Agent.*, Trojan.Win32.Agentb.gen.

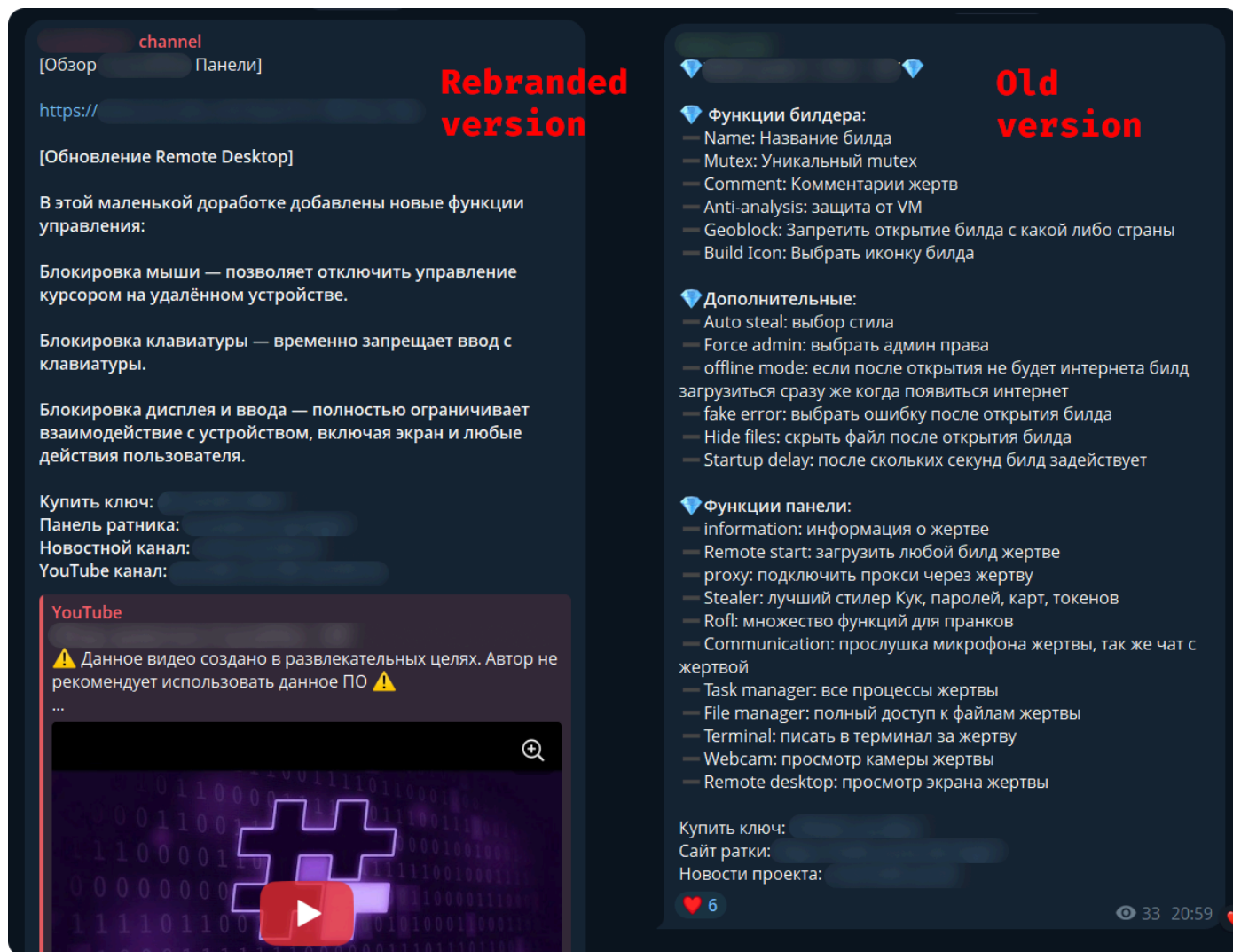
Technical details

Background

The new malware was first mentioned in January 2026 in a private Telegram chat for developers of RAT malware. The author actively promoted their creation, called Webcrystal RAT, by attaching screenshots of the web panel. Many users observed that the panel layout was identical to that of the previously known [WebRAT](#) (also called Salat Stealer), leading them to label this malware as a copy. Additional similarities included the fact that the RAT was written in Go, and the messages from the bot selling access keys to the control panel closely matched those of the WebRAT bots.



After some time, this malware was rebranded and received a new name, CrystalX RAT. Its promotion moved to a corresponding new channel, which is quite busy and features marketing tricks, such as access key draws and polls. Moreover, it expanded beyond Telegram: a special YouTube channel was created, aimed at marketing promotion and already containing a video review of the capabilities of this malware.



The builder and anti-debug features

By default, the malware control panel provides third parties with an auto-builder featuring a wide range of configurations, such as selective geoblocking by country, anti-analysis functions, an executable icon, and others. Each implant is compressed using zlib and then encrypted with ChaCha20 and a hard-coded 32-byte key with a 12-byte nonce. The malware has basic anti-debugging functionality combined with additional optional capabilities:

- **MITM Check:** checking if a proxy is enabled by reading the registry value `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings`, blacklisting names of certain processes (Fiddler, Burp Suite, mitmproxy, etc.), and verifying the presence of installed certificates for the corresponding programs
- **VM detect:** checking running processes, presence of guest tools, and hardware characteristics
- **Anti-attach loop:** an infinite loop checking the debug flag, debug port, hardware breakpoints, and program execution timings

- **Stealth patches:** patches for functions such as `AmsiScanBuffer`, `EtwEventWrite`, `MiniDumpWriteDump`

Stealer capabilities

When launched, the malware establishes a connection to its C2 using a hard-coded URL over the WebSocket protocol. It performs an initial collection of system information, after which all data is sent in JSON format as plain text. Then the malware executes the stealer function, doing so either once or at predefined intervals depending on the build options. The stealer extracts the victim's credentials for Steam, Discord, and Telegram from the system. It also gathers data from Chromium-based browsers using the popular **ChromeElevator** utility. To do this, it decodes and decompresses the utility using base64 and gunzip and saves it to `%TEMP%\svc[rndInt].exe`, then creates a directory `%TEMP%\co[rndInt]`, where the collected data is stored, and finally runs ChromeElevator with all available options.

```

rnd_name_int = math_rand_Intn(99999);
rnd_name = strconv_FormatInt(rnd_name_int, 10);
v260 = 0;
tmp_dir.len = _r1_2;
tmp_dir.ptr = _r0_3;
v260 = runtime_concatstring2(v172, "co", 2, rnd_name.ptr, rnd_name.len);
out_dir = path_filepath_join(&tmp_dir, 2);
out_dir_ptr = out_dir._r0;
out_dir_len = out_dir._r1;
os_MkdirAll(out_dir._r0, out_dir._r1, 493);
v258[0] = main_stealBrowsers_deferwrap2;
v258[2] = out_dir_len;
v258[1] = out_dir_ptr;
*(&v272 + 1) = v258;
p_bytes_Buffer = runtime_newobject(&RTYPE_bytes_Buffer);
v269 = runtime_newobject(&RTYPE_bytes_Buffer);
args[1] = 3;
args[0] = "all";
args[3] = 2;
args[2] = "-o";
args[5] = out_dir_len;
args[4] = out_dir_ptr;
args[7] = 2;
args[6] = "-k";
args[9] = 2;
args[8] = "-v";
_r2_14 = os_exec_Command(elev_exe, elev_exe_len, args, 5, 5);

```

The collected data is exfiltrated to the C2. For Yandex and Opera browsers, the stealer has a separate proprietary implementation with base decryption directly on the victim's system. Notably, the builds created at the time the article was written lack the stealer functionality. OSINT results

show that the author intentionally removed it with the aim to update the stealer arsenal before enabling it again.

Keylogger & clipper

Another option of the RAT is the keylogger. All user input is instantly transmitted via WebSocket to the C2, where it is assembled into a coherent text suitable for analysis. Additionally, the malware allows the attacker to read and modify the victim's clipboard by issuing appropriate commands from the control panel. Moreover, it can inject a malicious clipper into the Chrome or Edge browser. This happens according to the following algorithm:

1. The special malware command `clipper:set:[ADDR1, ...]` with the attackers' crypto-wallets addresses passed as arguments launches the clipper injection thread.
2. A `%LOCALAPPDATA%\Microsoft\Edge\ExtSvc` directory is created (regardless whether Edge or Chrome is the target of the injection), in which a malicious extension is stored, consisting of a manifest and a single JS script named `content.js`.
3. The `content.js` script is dynamically generated, containing regular expressions for crypto wallet addresses (such as Bitcoin, Litecoin, Monero, Avalanche, Doge, and others) and substitution values.
4. The generated script is activated via the Chrome DevTools (CDP) protocol using the command `Page.addScriptToEvaluateOnNewDocument`.

The final script looks as follows:

```

(function () {
  if (window.__wci)
    return;
  window.__wci = 1;

  var R = {
    'BTC': {p: new RegExp('(\\b)((?:bc1|[13])[a-zA-HJ-NP-Z0-9]{25,62})(\\b)', 'g'), r: '[ADDRESS]'},
    // And many more ...
  };

  function redactTextNode(textNode) { /* ... */ };
  function redactSubtree(subtree) { /* ... */ };

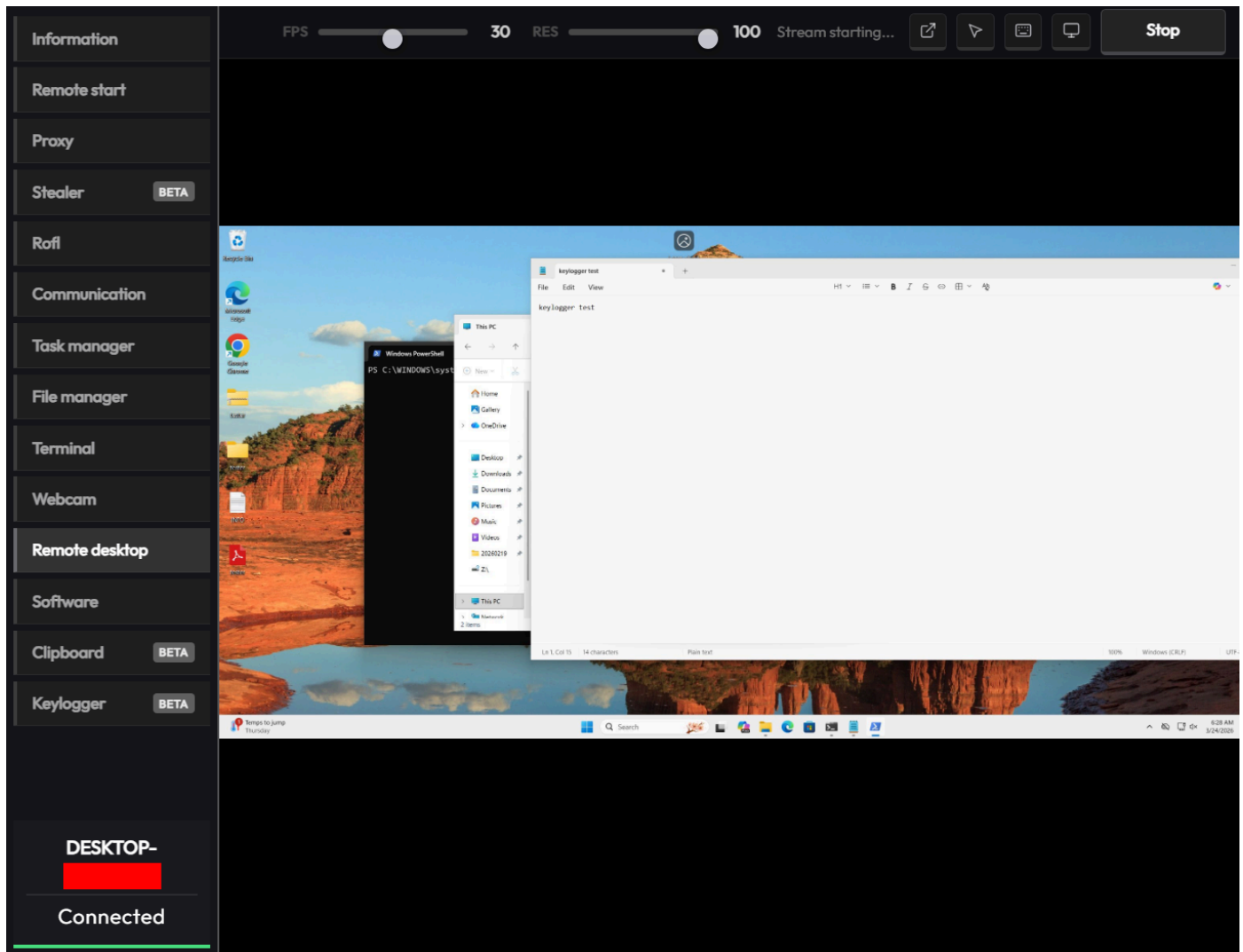
  if (document.body)
    redactSubtree(document.body);

  new MutationObserver(function (ml) {
    ml.forEach(function (m) {
      m.addedNodes.forEach(function (n) {
        if (n.nodeType === 3)
          redactTextNode(n);
        else if (n.nodeType === 1)
          redactSubtree(n);
      });
    });
  }).observe(document.documentElement, {
    childList: true,
    subtree: true
  });
  setInterval(function () {
    if (document.body)
      redactSubtree(document.body);
  }, 5000);
});

```

Remote access

The malware has a large set of commands for remote access to the victim's system. The attacker can upload arbitrary files, execute any commands using `cmd.exe`, and also browse the file system, including all available drives. Moreover, the RAT includes its own VNC that allows the attacker to view the victim's screen and control it remotely. Since both the attacker and the victim use the same session, the panel provides a number of buttons to block user input so that the attacker can perform necessary actions unhindered. The malware can also capture the audio stream from the microphone and the video stream from the camera in the background.



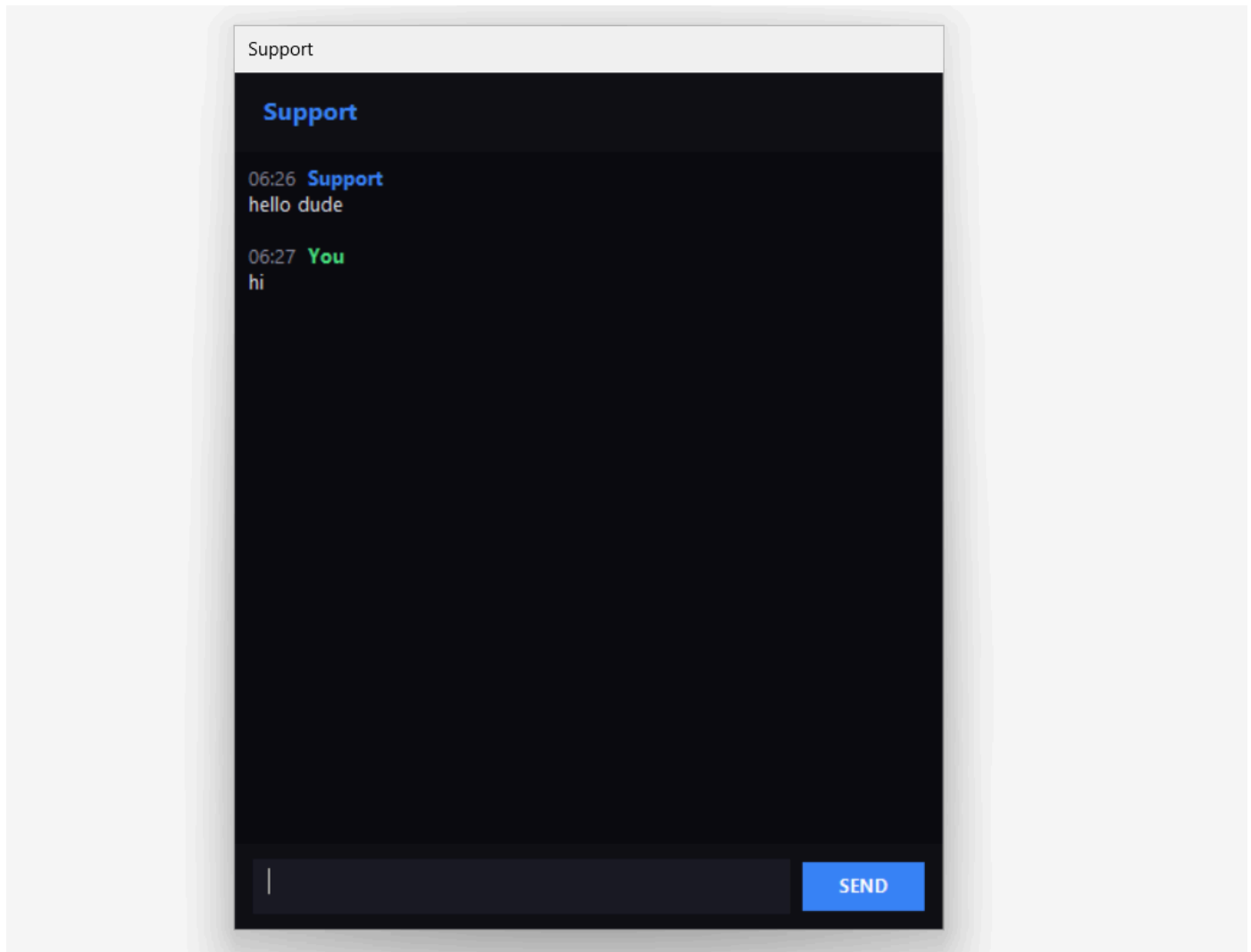
Prank commands

The finishing touch is a separate section of the panel named “Rofi” with commands whose functions consist of various pranks on the victim.

- **Setting a background:** downloading an image from a specified URL and using it as the desktop background.
- **Display orientation:** rotating the screen 90°, 180°, or 270°.
- **System shutdown:** the panel has two different buttons “Voltage Drop” and “BSoD”, but malware analysis shows that both commands perform a regular shutdown using the appropriate utility.
- **Remapping mouse buttons:** swapping left click with right click and the other way round.
- **Peripherals disruption:** disconnecting the monitor and blocking the input from the mouse and keyboard.
- **Notifications:** displaying a window with a custom title and message.
- **Cursor shake:** a special command starts a loop in which the cursor position changes chaotically at short intervals.

- **Disabling components:** hiding all file icons on the desktop, disabling the taskbar, task manager, and `cmd.exe`.

Moreover, the attacker can send a message to the victim, after which a dialog window will open in the system, allowing a bidirectional chat.



Conclusions

The sheer variety of available RATs has perpetuated demand, as actors prioritize flexibility of existing malware and its infrastructure. Thus, CrystalX RAT represents a highly functional MaaS platform that is not limited to espionage capabilities—spyware, keylogging and remote control—but includes unique stealer and prankware features. At the moment, the vector of the initial infection is not precisely known, but it affects dozens of victims. Although to date, we have only seen infection attempts in Russia, the MaaS itself has no regional restrictions meaning it may attack anywhere around the globe. Moreover, our telemetry has recorded new implant versions, which indicates that this malware is still being actively developed and maintained. Combined with the growing PR campaign for CrystalX RAT, it can be concluded that the number of victims can increase significantly in the near future.

Indicators of Compromise

C2 infrastructure

[webcrystal\[.\]lol](#)

[webcrystal\[.\]sbs](#)

[crystalxrat\[.\]top](#)

CrystalX RAT implants

[47ACCB0ECFE8CCD466752DDE1864F3B0](#)

[2DBE6DE177241C144D06355C381B868C](#)

[49C74B302BFA32E45B7C1C5780DD0976](#)

[88C60DF2A1414CBF24430A74AE9836E0](#)

[E540E9797E3B814BFE0A82155DFE135D](#)

[1A68AE614FB2D8875CB0573E6A721B46](#)

- [Malware Technologies](#)
- [Keyloggers](#)
- [Malware Descriptions](#)
- [Spyware](#)
- [Malware](#)
- [Trojan](#)
- [RAT Trojan](#)
- [Trojan-stealer](#)
- [Malware-as-a-Service](#)
- [CrustalX RAT](#)
- [Prankware](#)

A laughing RAT: CrystalX combines spyware, stealer, and prankware features

Your email address will not be published. Required fields are marked *

Name *

Email *

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)