Remsec: Top Level Espionage Platform Covertly Extracts Encrypted Government Comms

By Kaspersky

Published: 2016-08-01 · Archived: 2026-04-05 20:47:28 UTC

In September 2015, Kaspersky Lab's Anti-Targeted Attack Platform flagged an unusual feature in the network of a client organization

In September 2015, Kaspersky Lab's Anti-Targeted Attack Platform flagged an unusual feature in the network of a client organization. The anomaly led researchers to 'Remsec', a nation-state threat actor attacking state organizations with a unique set of tools for each victim, making traditional indicators of compromise almost useless. The aim of the attacks appears to be mainly cyber-espionage.

Remsec is particularly interested in gaining access to encrypted communications, hunting them down using an advanced modular cyber-espionage platform that incorporates a set of unique tools and techniques. The most noteworthy feature of Remsec's tactics is the deliberate avoidance of patterns: Remsec customizes its implants and infrastructure for each individual target, and never reuses them. This approach, coupled with multiple routes for the exfiltration of stolen data, such as legitimate email channels and DNS, enables Remsec to conduct secretive, long-term spying campaigns in target networks.

Remsec gives the impression of being an experienced and traditional actor that has put considerable effort into learning from other extremely advanced actors, including Duqu, Flame, Equation and Regin; adopting some of their most innovative techniques and improving on their tactics in order to remain undiscovered.

Key Features

Remsec tools and techniques of particular interest include:

- **Unique footprint:** Core implants that have different file names and sizes and are individually built for each target – making it very difficult to detect since the same basic indicators of compromise would have little value for any other target.
- **Running in memory:** The core implants make use of legitimate software update scripts and work as backdoors, downloading new modules or running commands from the attacker purely in memory.
- **A bias towards crypto-communications**: Remsec actively searches for information related to fairly rare, custom network encryption software. This client-server software is widely adopted by many of the target organizations to secure communications, voice, email, and document exchange. The attackers are particularly interested in encryption software components, keys, configuration files, and the location of servers that relay encrypted messages between the nodes.
- **Script-based flexibility:** The Remsec actor has implemented a set of low-level tools which are orchestrated by high-level LUA scripts. The use of LUA components in malware is very rare - it has previously only been spotted in the Flame and Animal Farm attacks.

- **Bypassing air-gaps:** Remsec makes use of specially-prepared USB drives to jump across air-gapped networks. These USB drives carry hidden compartments in which stolen data is concealed.
- **Multiple exfiltration mechanisms:** Remsec implements a number of routes for data exfiltration, including legitimate channels such as email and DNS, with stolen information copied from the victim disguised in day-to-day traffic.

Geography/victim profile

To date over 30 victim organizations have been identified, the majority of which are located in the Russian Federation. Many more organizations and geographies are likely to be affected. However, due to the nature of Remsec's operations it's extremely hard to discover every new target.

Based on our analysis, targeted organizations generally play a key role in providing state services and include:

- Government
- Military
- Scientific research centers
- Telecom operators
- Financial organizations

Forensic analysis indicates that Remsec has been operational since June, 2011 and remains active in 2016. The initial infection vector used by Remsec to penetrate victim networks remains unknown.

"A number of targeted attacks now rely on low-cost, readily-available tools. Remsec, in contrast, is one of those that relies on homemade, trusted tools and customizable scripted code. The single use of unique indicators, such as control server, encryption keys and more, in addition to the adoption of cutting edge techniques from other major threat actors, is rather new. The only way to withstand such threats is to have many layers of security in place, based on a chain of sensors monitoring even the slightest anomaly in organizational workflow, multiplied with threat intelligence and forensic analysis to hunt for patterns even when there appear to be none," said Vitaly Kamluk, Principal Security Researcher at Kaspersky Lab.

The cost, complexity, persistence and ultimate goal of the operation: stealing confidential and secret information from state-sensitive organizations, suggest the involvement or support of a nation state.

Kaspersky Lab security experts advise organizations to undertake a thorough audit of their IT networks and endpoints and to implement the following measures:

- Introduce an anti-targeted attack solution alongside new or existing endpoint protection. Endpoint protection on its own is not enough to withstand the next generation of threat actors.
- Call in the experts if the technology flags an anomaly. The most advanced security solutions will be able to spot an attack even as it's happening, and security professionals are sometimes the only ones who can effectively block, mitigate and analyze major attacks.
- Supplement the above with threat intelligence services: this will inform security teams about the latest evolution in the threat landscape, attack trends and the signs to watch out for.
- And last, but not least, since many major attacks start with a spear-phishing or other approach to employees, make sure that staff understand and practice responsible cyber-behavior.

The full report on Remsec has been made available to customers of Kaspersky Lab APT Intelligence reporting service in advance. Learn more at: http://www.kaspersky.com/enterprise-security/apt-intelligence-reporting

Indicators of compromise and YARA rules are available here.

All Kaspersky Lab products detect Remsec samples as HEUR:Trojan.Multi.Remsec.gen

To learn more about Remsec, read the blogpost on Securelist.com

Learn more about how Kaspersky Lab products can protect users from this threat.
