

# Op 'Sharpshooter' Connected to North Korea's Lazarus Group

By Ionut Ilascu

Published: 2019-03-04 · Archived: 2026-04-05 18:15:46 UTC

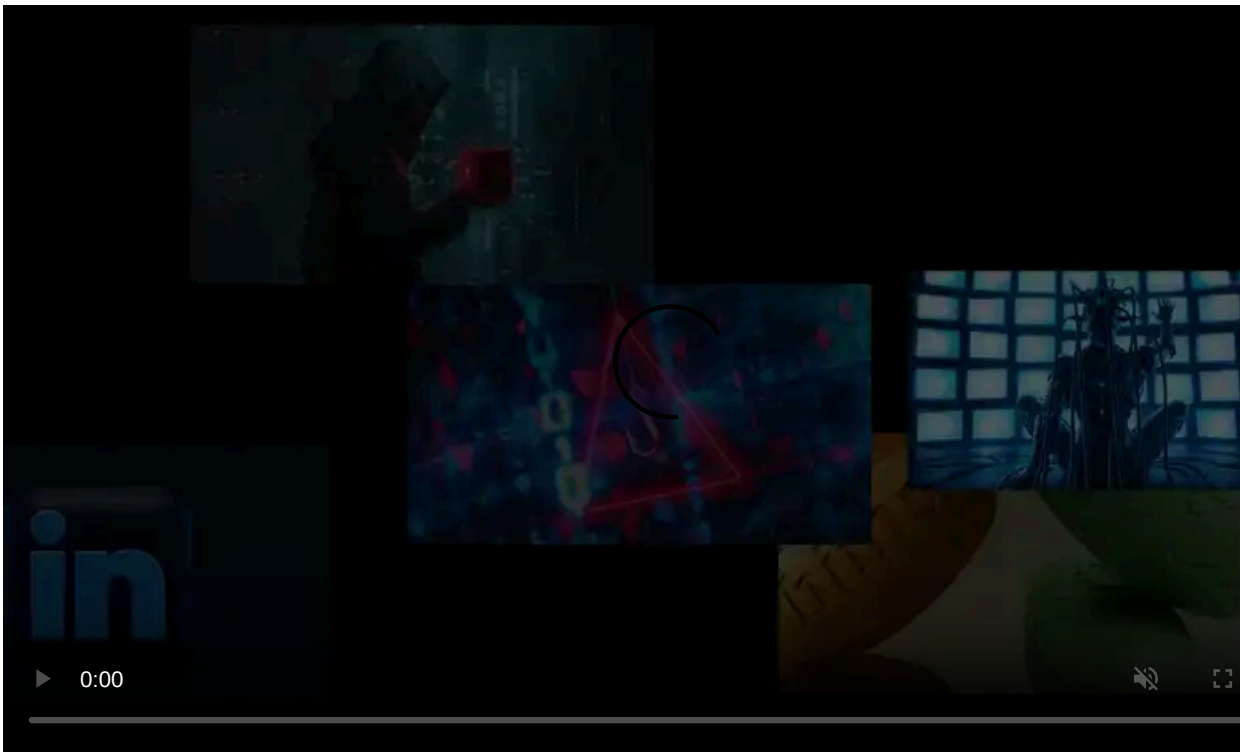


After analyzing code from a command and control (C2) server used in the global cyber-espionage campaign dubbed 'Sharpshooter', security researchers found more evidence linking it to North Korea's Lazarus threat actor.

The assessment was possible with the help of a government entity and revealed that the operation is broader in scope, more complex and older than initially thought.

## The North Korean connection

To hide their true location, the threat actor used the ExpressVPN service that showed connections to the web shell (Notice.php) on a compromised server coming from two IP addresses in London.



Visit Advertiser website [GO TO PAGE](#)

85.203 [REDACTED]

Summary WHOIS

**Basic Information**

|          |                   |             |         |
|----------|-------------------|-------------|---------|
| ASN      | [REDACTED]        | ASN Country | NL      |
| ASN CIDR | 85.203 [REDACTED] | Registry    | ripence |
| Entities | ACRO1080-RIPE     |             |         |

**ACRO1080-RIPE (abuse)**

**Contact Information**

|         |  |
|---------|--|
| Name    | Abuse contact role object (group)                                    |
| Email   | <a href="mailto:services@expressvpn.com">services@expressvpn.com</a> |
| Address | [REDACTED]   |

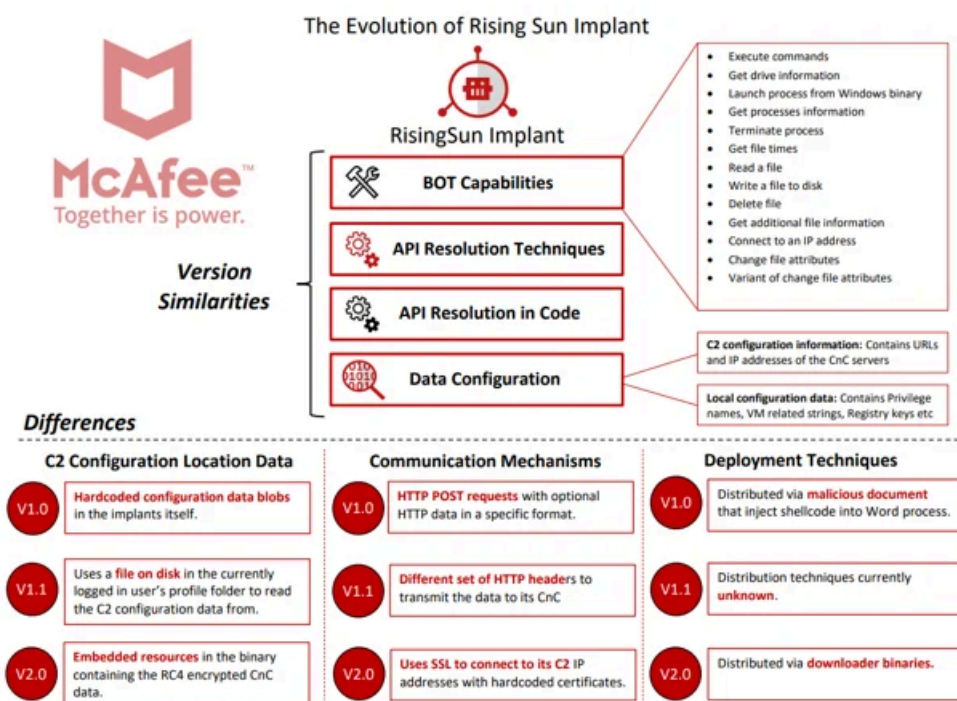
**Other Information**

|          |            |
|----------|------------|
| Entities | [REDACTED] |
|----------|------------|

However, the IP addresses are rarely a reliable indicator of the attacker's origin or for attribution. The connection to the Lazarus group was obvious by inspecting the tools, strategies, and methods already linked to the North Korean actor.

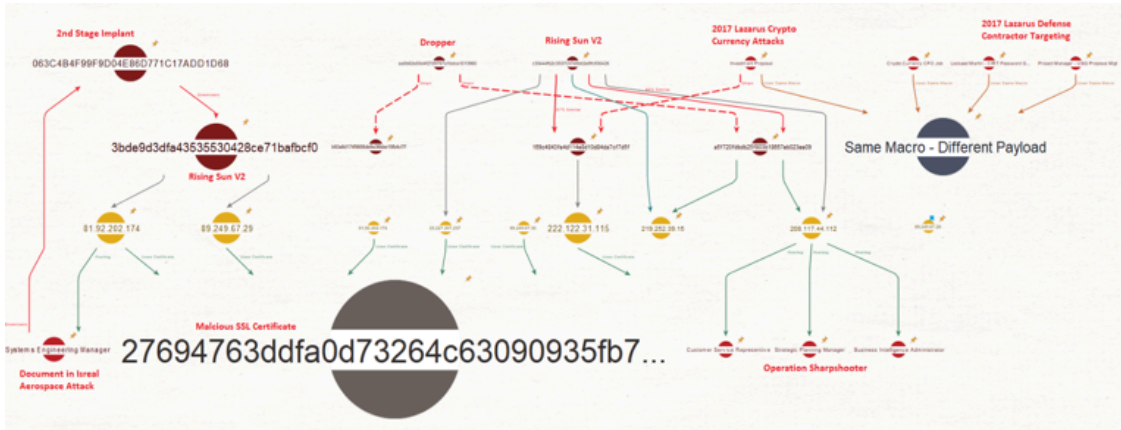
For instance, Rising Sun was observed in attacks before the discovery of 'Sharpshooter' and shared the tactics, techniques, and procedures (TTPs) seen in operations attributed to Lazarus group.

The three variants of the backdoor (v1.0, v1.1, and v2.0) indicate a clear evolution from Duuzer, used by Lazarus, as they all include its core capabilities.



"These [Rising Sun] implants were all based on the original Backdoor Duuzer source code," the researchers say in their report.

The high similarity of the fake job recruitment campaigns both groups used to disguise their attacks, and the fact that Lazarus relied on similar versions of Rising Sun in activity tracked in 2017, point to a connection between the two adversaries.



### Malicious components in the framework

Analyzing the code and data from the C2, Ryan Sherstobitoff and Asheer Malhotra from McAfee, along with the company's Advanced Threat Research Team (ATR), discovered new variants of the Rising Sun backdoor that were used since at least 2016.

"The server was used to distribute and infect victims with an upgraded version of Rising Sun with SSL capabilities," informs a report shared with BleepingComputer.

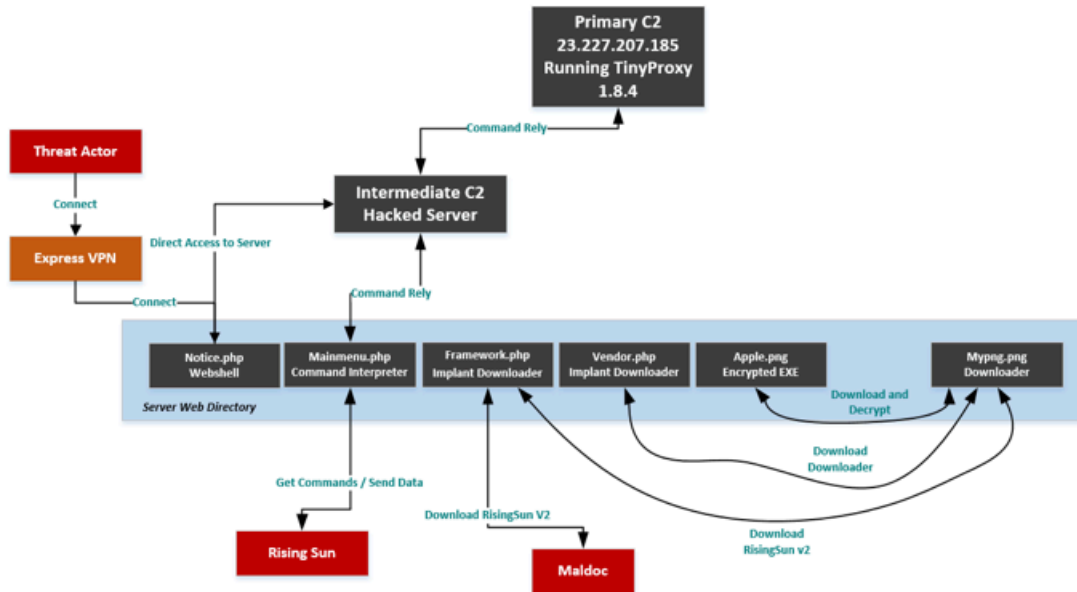
The rare opportunity to examine Sharpshooter's backend operations allowed the researchers to create a fuller picture of the activity and interaction between the various tools used by the threat actor.



Local recreation of Sharpshooter's C2 main panel

Getting access to the C2 information helped the researchers get a clear view of the attacker's operations and utilities. It also provided sufficient details to quickly improve detection of malicious activity from this threat by uncovering new tools otherwise hidden by obfuscation techniques.

An alternative method for discovering them is by analyzing network packets, which is more difficult and requires more time.

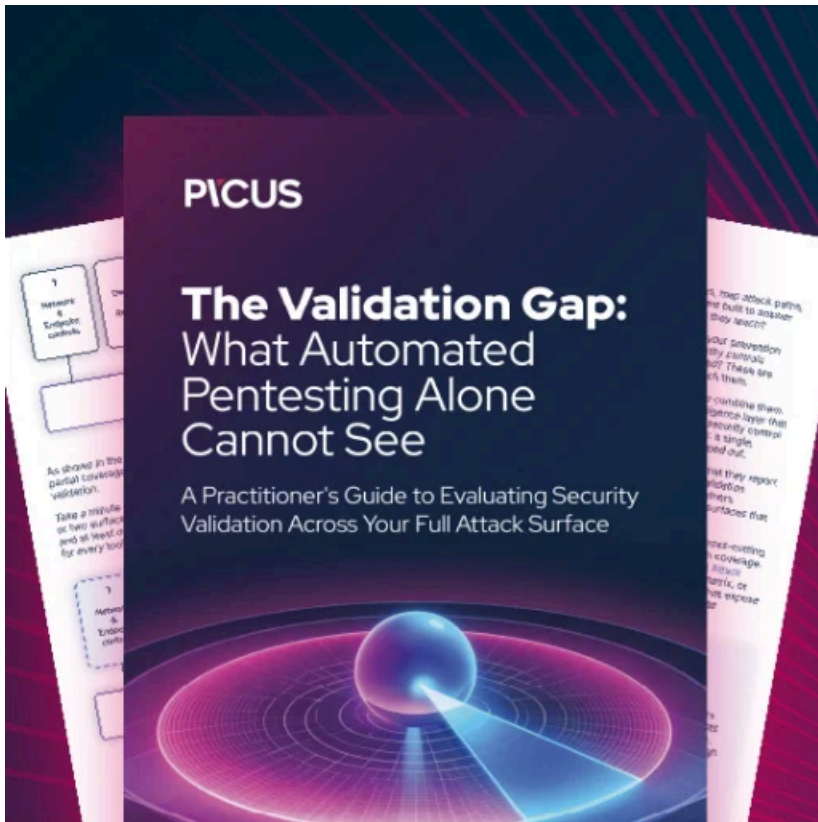


Another finding in the activity of 'Sharpshooter' were a set of unobfuscated connections from IP addresses in Windhoek, a city in Namibia, Africa. One explanation for this could be that that they used the region as a test zone; another would be that the threat actor runs the operation from those locations, although it could also be a false flag meant to point the researchers on the wrong path.

When 'Sharpshooter' was first discovered, it was believed that the operation started in October 2018. However, a log file on the server indicates that the C2 framework has been active since at least September 2017, and probably "hosted on different servers over time."

The threat actor [first detected](#) towards the end of last year when it attacked at least 87 organizations around the world in two months' time. Its activity is ongoing.

McAfee researchers will present their findings at this year's [RSA security conference](#) in San Francisco.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/op-sharpshooter-connected-to-north-koreas-lazarus-group/>