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

bleepingcomputer.com/news/security/op-sharpshooter-connected-to-north-koreas-lazarus-group/

Ionut Ilascu

By
Ionut Ilascu

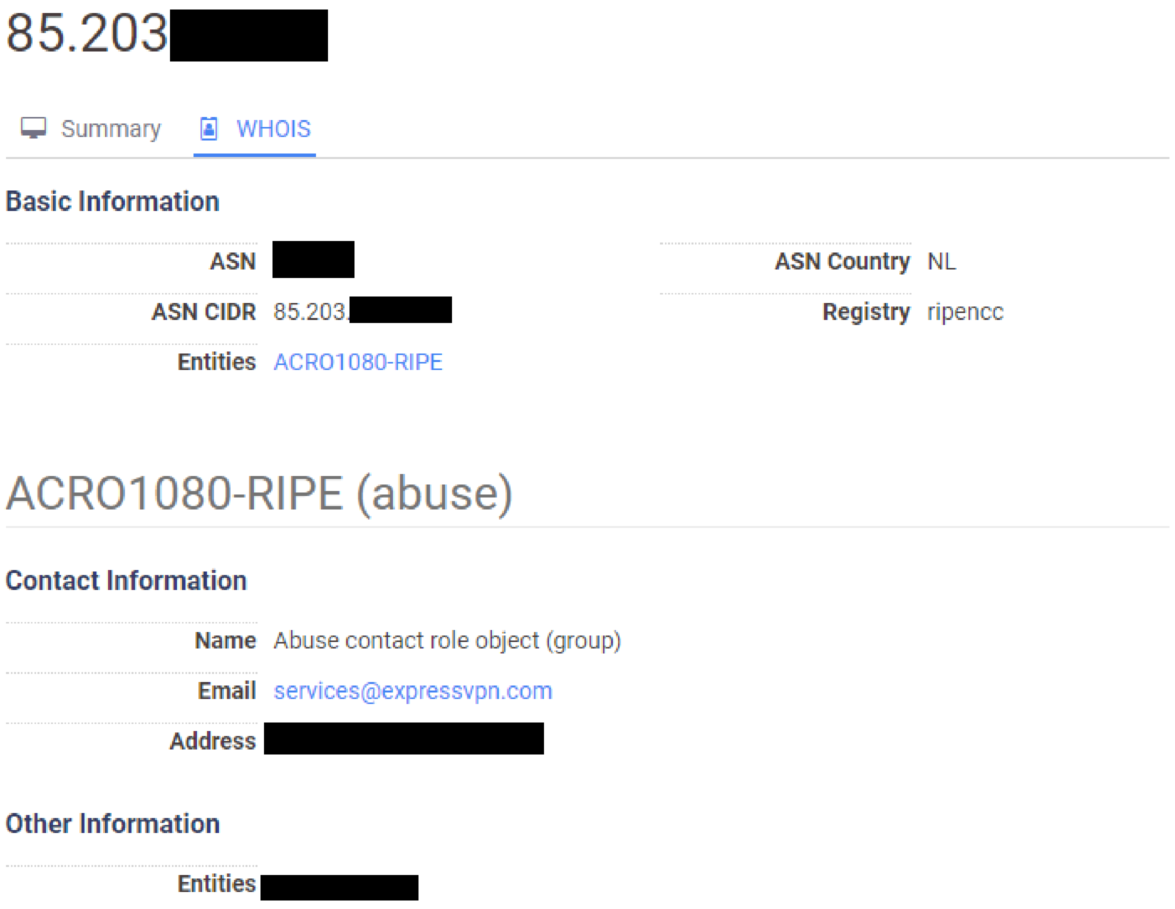
- March 3, 2019
- 11:30 PM
- 0

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.



85.203[redacted]

Basic Information

ASN	[redacted]	**ASN Country**	NL
ASN CIDR	85.203[redacted]	**Registry**	ripencc
Entities	ACRO1080-RIPE		

ACRO1080-RIPE (abuse)

Contact Information

Name	Abuse contact role object (group)
Email	services@expressvpn.com
Address	[redacted]

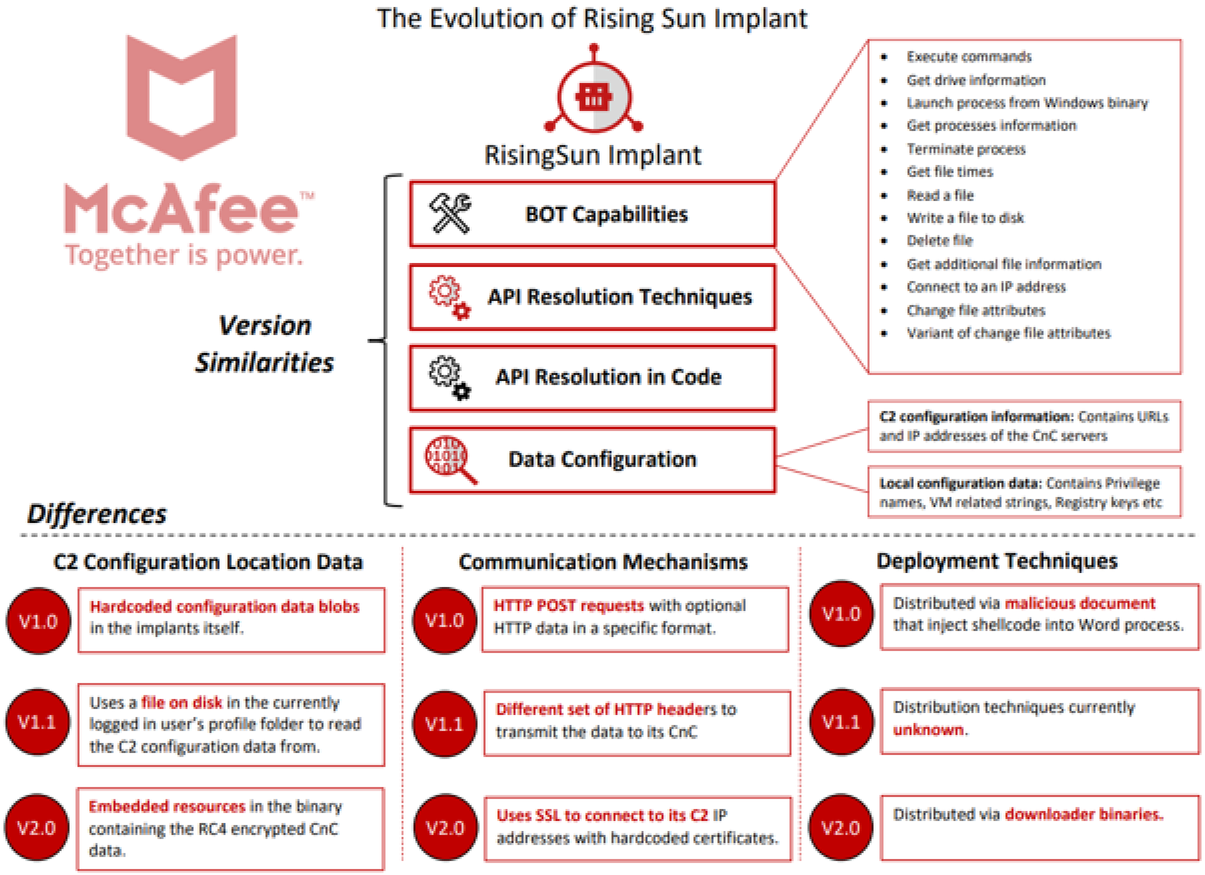
Other Information

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.



The Evolution of Rising Sun Implant

RisingSun Implant

Version Similarities

- BOT Capabilities
- API Resolution Techniques
- API Resolution in Code
- Data Configuration

BOT Capabilities:

- Execute commands
- Get drive information
- Launch process from Windows binary
- Get processes information
- Terminate process
- Get file times
- Read a file
- Write a file to disk
- Delete file
- Get additional file information
- Connect to an IP address
- Change file attributes
- Variant of change file attributes

Data Configuration:

C2 configuration information: Contains URLs and IP addresses of the CnC servers

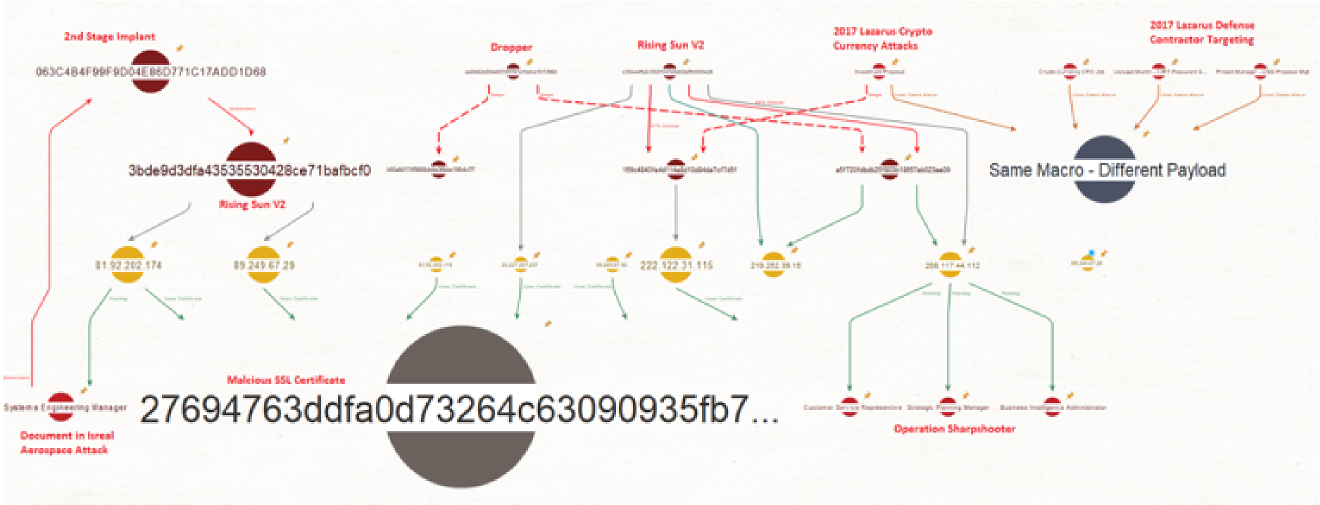
Local configuration data: Contains Privilege names, VM related strings, Registry keys etc

Differences

	C2 Configuration Location Data	Communication Mechanisms	Deployment Techniques
V1.0	Hardcoded configuration data blobs in the implants itself.	HTTP POST requests with optional HTTP data in a specific format.	Distributed via malicious document that inject shellcode into Word process.
V1.1	Uses a file on disk in the currently logged in user's profile folder to read the C2 configuration data from.	Different set of HTTP headers to transmit the data to its CnC	Distribution techniques currently unknown.
V2.0	Embedded resources in the binary containing the RC4 encrypted CnC data.	Uses SSL to connect to its C2 IP addresses with hardcoded certificates.	Distributed via downloader binaries.

"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.

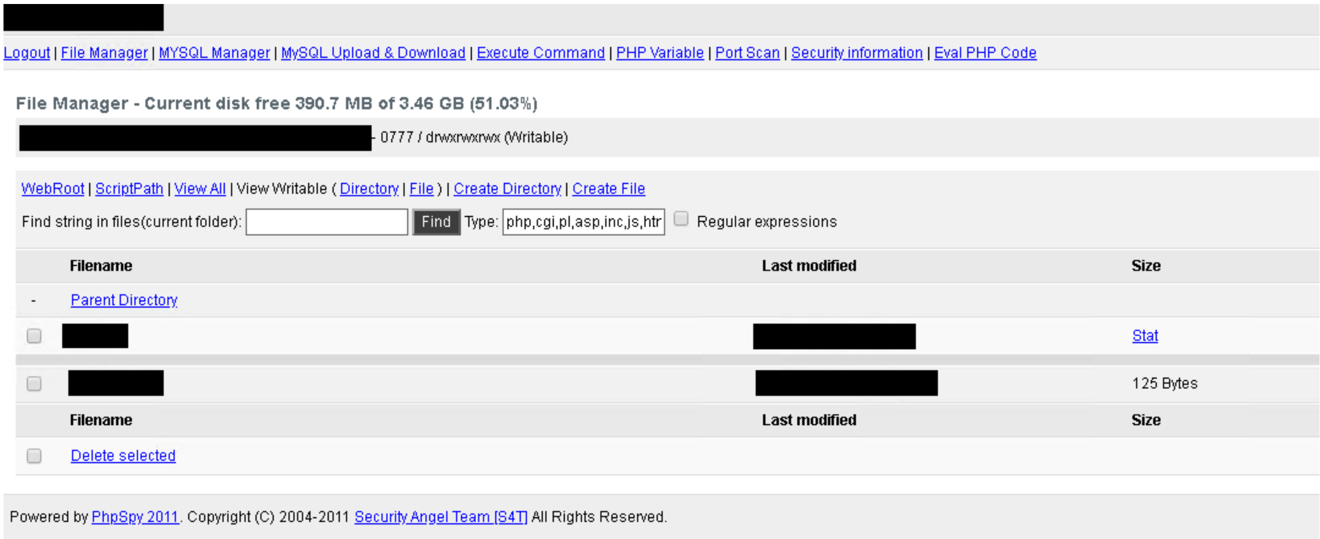

2nd Stage Implant
063C4B4F99F9D04E86D771C17ADD1D68
Dropper
Rising Sun V2
2017 Lazarus Crypto Currency Attacks
2017 Lazarus Defense Contractor Targeting
3bde9d3dfa43535530428ce71bafbcf0
Rising Sun V2
Same Macro - Different Payload
81.92.202.174
89.249.67.29
222.122.31.115
Malicious SSL Certificate
Systems Engineering Manager
27694763ddfa0d73264c63090935fb7...
Document in Isreal Aerospace Attack
Operation Sharpshooter

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.



[redacted]

Logout | File Manager | MYSQL Manager | MySQL Upload & Download | Execute Command | PHP Variable | Port Scan | Security information | Eval PHP Code

File Manager - Current disk free 390.7 MB of 3.46 GB (51.03%)

[redacted] - 0777 / drwxrwxrwx (Writable)

WebRoot | ScriptPath | View All | View Writable (Directory | File) | Create Directory | Create File

Find string in files(current folder): [ ] Find Type: php,cgi,pl,asp,inc,js,htr □ Regular expressions

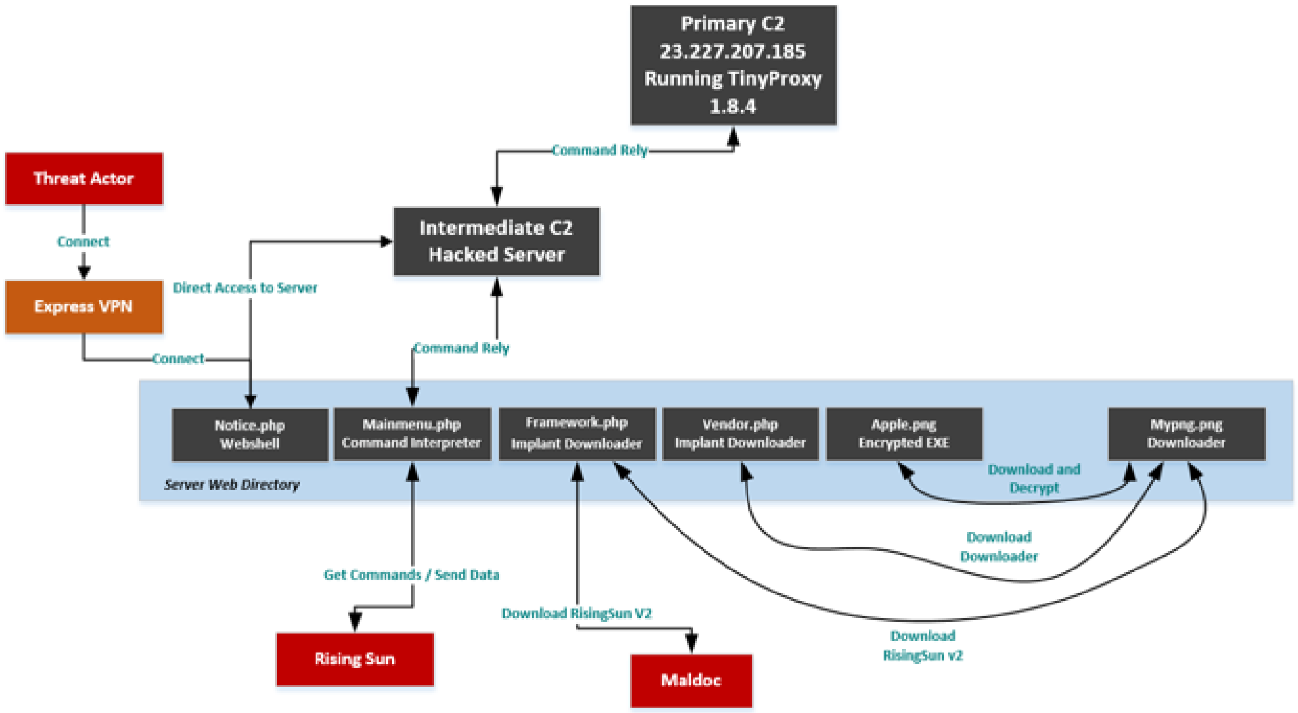
	Filename	Last modified	Size
-	Parent Directory		
□	[redacted]	[redacted]	Stat
□	[redacted]	[redacted]	125 Bytes
	Filename	Last modified	Size
□	Delete selected		

Powered by PhpSpy 2011. Copyright (C) 2004-2011 Security Angel Team [S4T] All Rights Reserved.

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.

Related Articles:

Hackers are now hiding malware in Windows Event Logs

Cyberspies use IP cameras to deploy backdoors, steal Exchange emails

DPRK hackers go after crypto assets using trojanized DeFi Wallet app

BPFDoor malware uses Solaris vulnerability to get root privileges

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.