Lazarus hackers target researchers with trojanized IDA Pro

By Lawrence Abrams

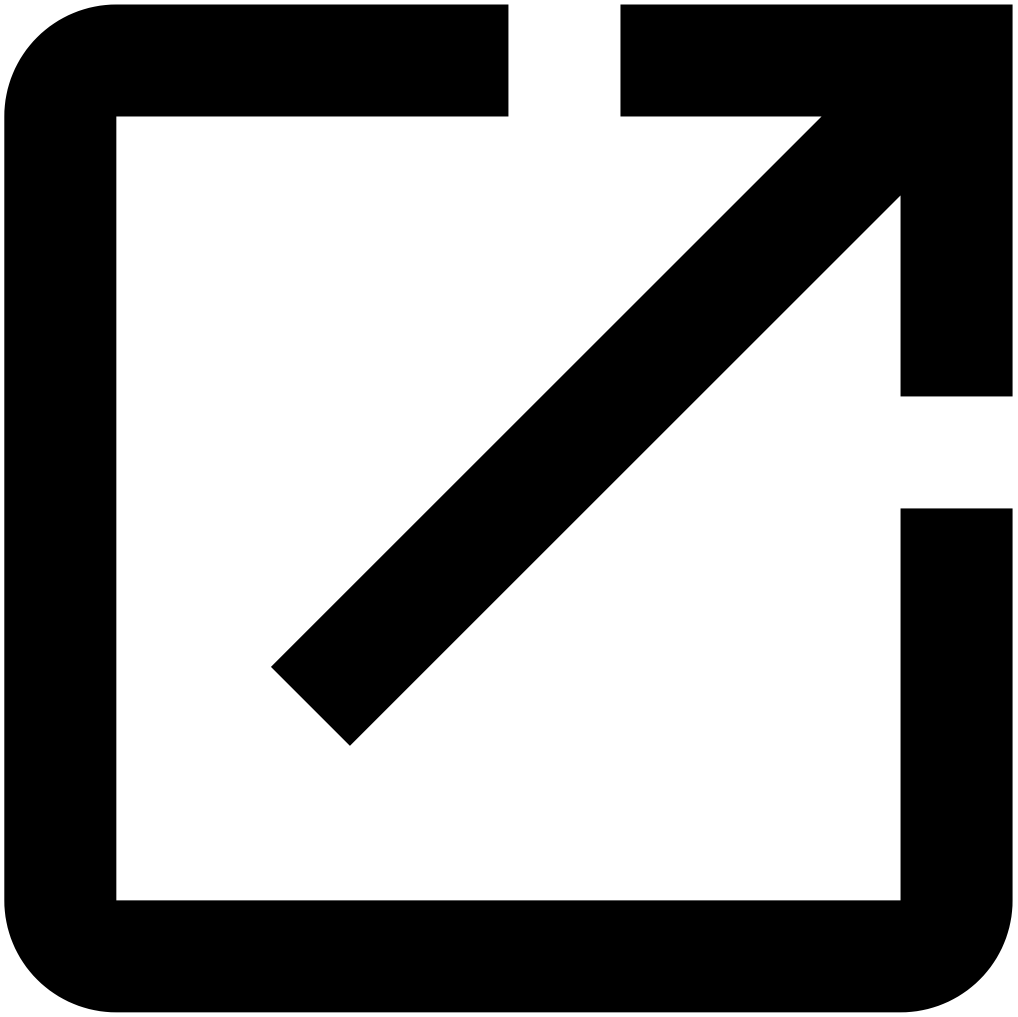
Published: 2021-11-10 · Archived: 2026-04-05 13:52:28 UTC

A North Korean state-sponsored hacking group known as Lazarus is again trying to hack security researchers, this time with a trojanized pirated version of the popular IDA Pro reverse engineering application.

IDA Pro is an application that converts an executable into assembly language, allowing security researchers and programmers to analyze how a program works and discover potential bugs.

Security researchers commonly use IDA to analyze legitimate software for vulnerabilities and malware to determine what malicious behavior it performs.


DIE LINKE.
0:00



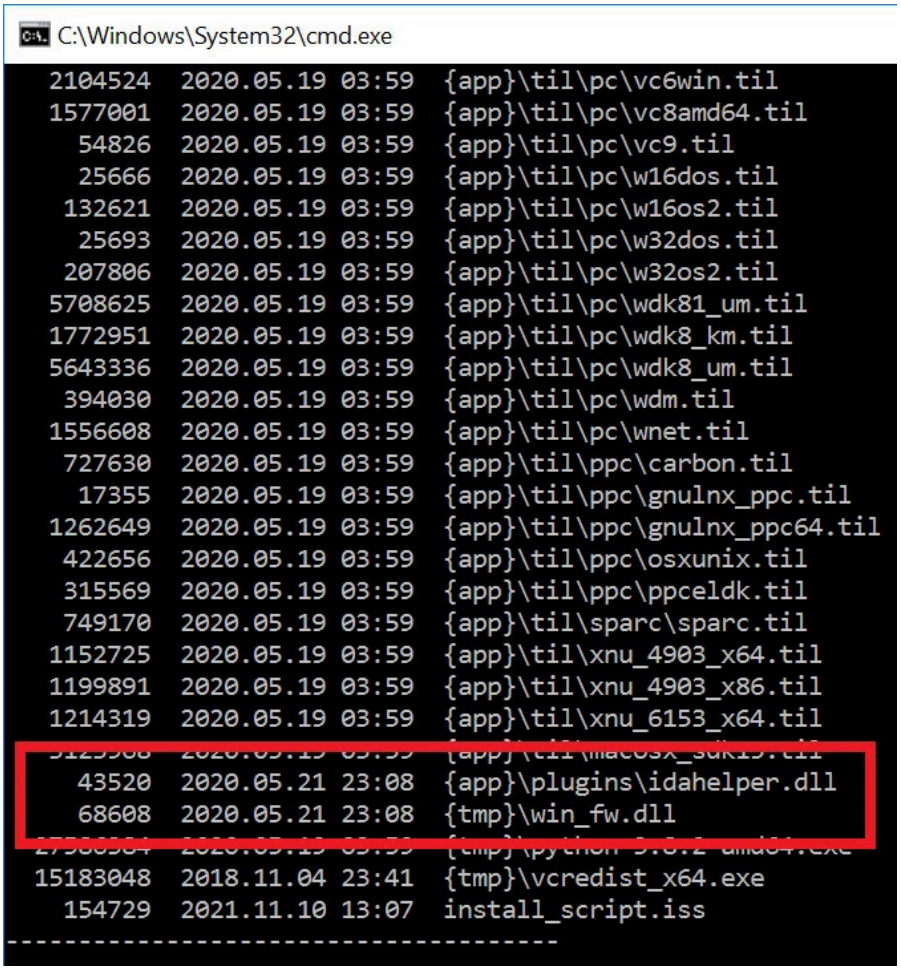
However, as IDA Pro is an expensive application, some researchers download a pirated cracked version instead of purchasing it.

As with any pirated software, there is always the risk of it being tampered modified to include malicious executables, which is precisely what ESET researcher Anton Cherepanov discovered in a pirated version of IDA Pro distributed by the Lazarus hacking group.

Trojanized IDA Pro targets security researchers

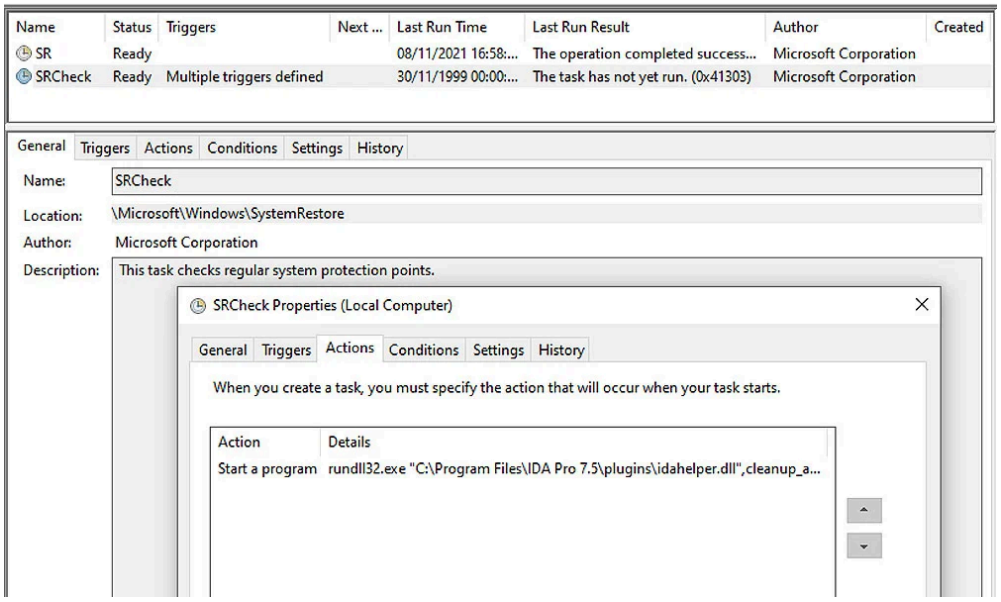
Today, ESET tweeted about a malicious version of IDA Pro 7.5 discovered by Cherepanov that is being distributed online to target security researchers.

This IDA installer has been modified to include two malicious DLLs named **idahelp.dll** and **win_fw.dll** that will be executed when the program is installed.



Malicious DLLs added to pirated IDA Pro
Source: ESET

The win_fw.dll file will create a new task in the Windows Task Scheduler that launches the idahelper.dll program.



New SRCheck scheduled task created by win_fw.dll

Source: ESET

The idahelper.dll will then connect to the devguardmap[.]org site and download payloads believed to be the NukeSped remote access trojan. The installed RAT will allow the threat actors to gain access to the security researcher's device to steal files, take screenshots, log keystrokes, or execute further commands.

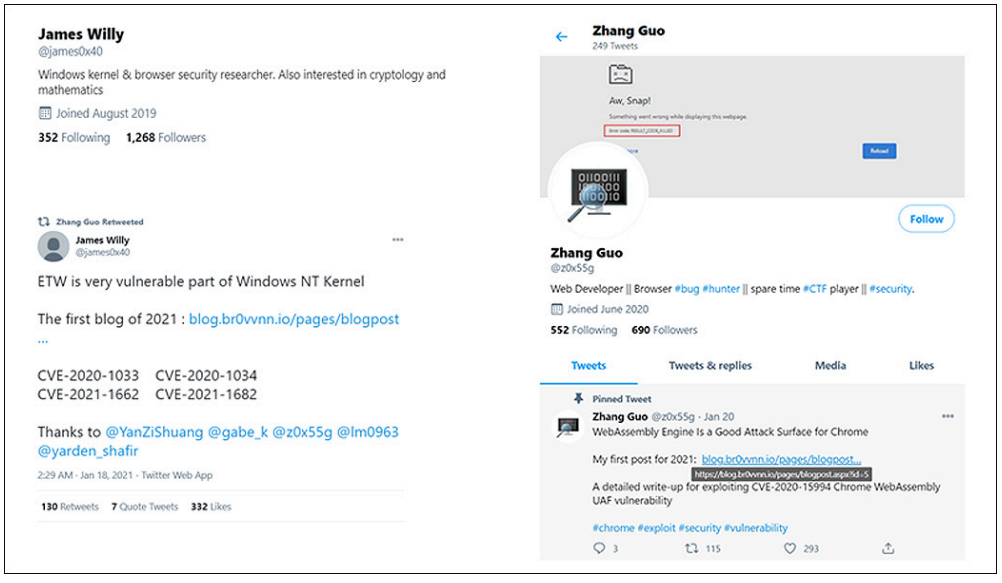
"Based on the domain and trojanized application, we attribute this malware to known Lazarus activity, previously reported by Google's Threat Analysis Group and Microsoft," ESET tweeted regarding connection to Lazarus.

Cherepanov told BleepingComputer that while he does not know how the installer is being distributed, it was discovered recently and appears to have been distributed since Q1 2020

Lazarus has a history of targeting researchers

The Lazarus hacking group, also known as Zinc by Microsoft, has a long history of targeting security researchers with backdoors and remote access trojans.

In January, Google disclosed that Lazarus conducted a social media campaign to create fake personas pretending to be vulnerability researchers.



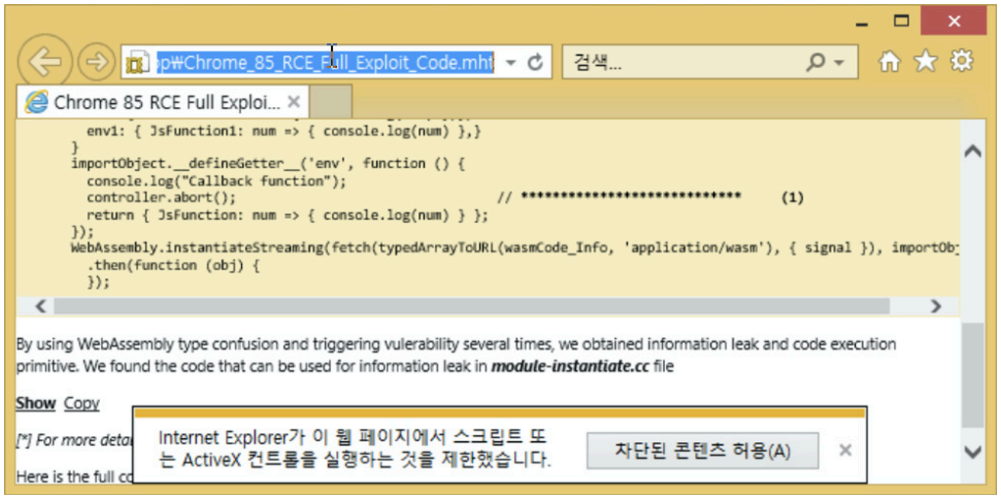
Fake online security researcher personas

Using these personas, the hacking group would contact other security researchers about potential collaboration in vulnerability research.

After establishing contact with a researcher, the hackers would send Visual Studio projects related to an alleged 'vulnerability,' which contained a malicious hidden DLL named 'vcxproj.suo.'

When the researcher attempted to build the project, a pre-build event would execute the DLL, which acted as a custom backdoor installed on the researcher's device.

Other Lazarus attacks also used an Internet Explorer zero-day to deploy malware on security researcher's devices when they visited links sent by the attackers.



Exploiting the Lazarus zero-day in Internet Explorer

While it was never determined what the ultimate goal was for these attacks, it was likely to steal undisclosed security vulnerabilities and exploits that the hacking group could use in their own attacks.

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.
