

Forum:[Hack Forums](#)

Thread: [Researchers can't identify programming language used in Duqu malware, ask for help.](#)

Rsynced - March 9, 2012, 1:16 pm

SOURCE:

<http://www.networkworld.com/news/2012/030812-researchers-cant-identify-programming-language-257074.html>

Malware experts from Kaspersky Lab have asked the programming community for help identifying the programming language, compiler or framework that was used to write an important part of the Duqu Trojan, in the hope that it could reveal clues about who created it or why.

"When we checked Duqu it looked totally unknown and that was very curious, because it's unclear why something very custom was developed and used," said Vitaly Kamluk, chief malware expert with Kaspersky Lab's global research & analysis team.

BACKGROUND: Duqu authors sprinkle humor in dangerous code

Understanding how a piece of malware was created can offer clues about where to look for it next or the level of resources required for its development, the security expert said.

Related Content

Some parts of the Duqu payload DLL, the component responsible for interacting with the command and control servers, downloading and executing additional modules, and performing other tasks, were written in standard C++, but a big chunk of it was not.

"This slice is different from others, because it was not compiled from C++ sources. It contains no references to any standard or user-written C++ functions, but is definitely object-oriented," said Kaspersky Lab expert Igor Soumenkov in a blog post that describes the particularities of the unfamiliar code.

Kaspersky researchers refer to this portion of the Trojan as "The Duqu Framework" and believe that it might have been created by a different programming team. The unusual code is also particular to Duqu and doesn't exist in Stuxnet, unlike some other parts that were directly borrowed from the infamous industrial sabotage malware.

"The mysterious programming language is definitively NOT C++, Objective C, Java, Python, Ada, Lua and many other languages we have checked," Soumenkov said, adding that Kaspersky's research team has spent countless hours analyzing the code.

The company's researchers even discussed it with third-party experts, but didn't get any closer to solving the mystery. "It looks absolutely alien," Kamluk said.

Finally, Kaspersky Lab appealed to the entire programming community in the hope that someone might recognize the code constructions and figure out what was framework, toolkit or language was used.

The company has received various suggestions in comments on its blog, that range from F, D, Iron Python, High-Level Assembly, Common LISP, Forth, Erlang, Vala, to more exotic tools like RoseRT, which one user claims was used in secure government projects.

"It took us several weeks to check commonly used programming languages and various compilers," Kamluk said. "So, I guess it may also take some time to check other suggestions."

Mafia owner - March 9, 2012, 1:28 pm

its most likely to be custom programming language, it must of taken a lot of effort to code it and of course one person cant do that it must be organized government dirty work or organized criminals.

condom - March 9, 2012, 1:32 pm

hehehehe always someone out their who is bright enough to get the attention of government. that's proof that some hackers can be smart and just as resourceful as the government ?

bplomb - March 9, 2012, 1:35 pm

http://www.securelist.com/en/blog/667/The_Mystery_of_the_Dugu_Framework

Here's some of the coding :p

Fallenour - March 10, 2012, 12:02 pm

Its a custom written language. Probably a mix of orginial C and Assembly 86. It allows for baseline program execution on all systems, while also allowing it to be completely unrecognizable bymost systems due to the fact that none of its framework can have slices pulled from it and properly scanned as malicious coding.

Leon_V._Metcalf - March 10, 2012, 6:35 pm

We can't rely on computers too much. A virus like this can take everything down from a network to a power grid.

Rwkeith - March 10, 2012, 7:47 pm

Creating a programming isn't difficult. It's just knowing the purpose of it's structure, and the tasks that will be handled by it.