4 in 10 dark net cybercriminals are selling targeted FTSE 100 or Fortune 500 hacking services

June 7 2019, by Laura Butler

Credit: CC0 Public Domain

Exposing the abundant availability and increased demand for tailored malware, network access and targeted hacking services, Dr. Mike

McGuire presents his findings at the InfoSecurity Europe conference in Olympia, London on Thursday 6 June.

Highlighting the growing risk posed to business enterprise by the dark net—the part of the internet which is inaccessible when using standard browsers like Google—Senior Lecturer in Criminology at the University of Surrey Dr. Mike McGuire's Behind the Dark Net Black Mirror forms the next installment of his "Into the Web of Profit" research.

The study, underwritten by Bromium, offers unique insights into the current risk to organisations, highlighting the variety of custom malware, network access tools and corporate espionage services available on the dark net which threaten businesses, their employees, customers and partners.

Dr. McGuire's research provides details of first-hand intelligence gathered from covert discussions with dark net vendors, alongside analysis from a panel of global industry experts across law enforcement and government. The study found that 4 in 10 dark net vendors are selling targeted hacking services aimed at FTSE 100 and Fortune 500 businesses. The dark net has become a haven for custom-built, targeted malware, with a 20% rise in the number of dark net listings with a direct potential to harm the enterprise since 2016 and threats tailored to specific industries or organisations outnumbering off-the-shelf varieties 2:1.

Furthermore, access to corporate networks is sold openly, with 60% of vendors approached by researchers offering access to more than ten business networks each. Of the dark net vendors who were engaged, 70% invited researchers to talk on encrypted messaging applications, like Telegram, to take conversations beyond the reach of law enforcement. More than 40% of attempts by researchers to request dark net hacking services targeting companies in the Fortune 500 or FTSE

100 received positive responses from dark net vendors.

Dr. Mike McGuire said: "Almost every vendor offered us tailored versions of malware as a way of targeting specific companies or industries. The more targeted the attack, the higher the cost, with prices rising even further when it involved high-value targets like banks. The most expensive piece of malware found was designed to target ATMs and retailed for approximately $1,500. These services typically come with service plans for conducting the hack, with prices ranging from $150 to $10,000 depending on the company involved and the extent to which the malware was customised for targeted attacks.

"The methods for providing access varied considerably. Some involved stolen remote access credentials that are for sale for as little as $2, while others involved backdoor access or the use of malware. Illicit remote access tools appear to be most popular—we were offered Remote Access Trojans at least five times more often than keyloggers."

"Organisations need to strengthen their defences to protect their endpoints and networks against threats posed by the dark net. Enterprises, researchers and law enforcement must continue to study the dark net to gather intelligence and gain a deeper understanding of the adversaries that we are dealing with, and better prepare ourselves for counteracting the effects of a growing cybercrime economy."

Provided by University of Surrey

Citation: 4 in 10 dark net cybercriminals are selling targeted FTSE 100 or Fortune 500 hacking services (2019, June 7) retrieved 26 June 2024 from https://phys.org/news/2019-06-dark-net-cybercriminals-ftse-fortune.html