Bloomberg BNA

Privacy Law Watch Bulletin™

VOL. 17, NO. 2 JANUARY 4, 2017

Cybersecurity

U.S. Report on Russian Cyberattack Tools Insufficient to Fight Future Attacks, Threats

The U.S. technical report detailing tools allegedly used by Russian government-sponsored hackers is inadequate alone to help companies and government agencies prevent future cyberattacks, cybersecurity analysts told Bloomberg BNA Jan. 3.

The report by the Federal Bureau of Investigation and Department of Homeland Security provides only generic recommendations against a sophisticated and constantly evolving threat, they say. Nevertheless, companies can use the basic information as a starting point on the way to developing a robust cybersecurity response plan, they said.

Peter Tran, general manager and senior director at RSA Security LLC, told Bloomberg BNA Jan. 3 that the mitigation strategies in the Joint Analysis Report (JAR) are best practices, ''but given the increased complexity and level of sophistication'' of threats from Russia and others, the mitigation recommendations are merely ''table stakes'' not the investment that is really needed for effective cybersecurity.

Francoise Gilbert, a data privacy attorney and shareholder at Greenberg Traurig LLP in Silicon Valley, agreed. ''The mitigation strategies proposed by the report are generic, and as such are likely to be inadequate for many organizations,'' she told Bloomberg BNA.

Oren Aspir, chief technology officer of cybersecurity services company Cyberbit in Ra'anana, Israel, said that JAR suggests ''the same old mitigation steps that are familiar to any information technology manager or security professional.''

Matthew Gardiner, cybersecurity strategist at Mimecast Co., which specializes in cloud-based e-mail management for Microsoft Corp. products, echoed similar sentiments. Although there is ''nothing wrong'' with JAR's mitigation strategies, they are ''generic and kitchen sink-ish,'' he told Bloomberg BNA.

The JAR should be considered as a ''warning shot with the understanding that the current cyberattack surface will change and require mitigation strategies above and beyond best practice such as the development and adoption of more advanced monitoring and early detection frameworks, technologies and processes such as the use of network behavioral analytics, data science, machine learning and artificial intelligence,'' Tran said.

The report fails to stress the importance of continued efforts—such as periodic training and audits—and quick reactions to an event, Gilbert said. The report should ''shift focus and investment from prevention to detection and response,'' Aspir told Bloomberg BNA.

'Russians Hide in the Noise' President Barack Obama retaliated Dec. 29 against Russia for alleged cyberattacks aimed at interfering with the 2016 presidential campaign. At the same time, the Department of Homeland Security and the Federal Bureau of Investigation released the JAR, which provided ''technical details regarding the tools and infrastructure'' allegedly used by the Russia-sponsored hackers.

According to Tran, ''with approximately 1.5 billion variations of malicious code in circulation over the internet, hacker attribution in general, whether it's a nation state or a cybercriminal, is like taking a blindfolded taste test.'' Identifying the ''exact 'chef' would be next to impossible,'' Tran said.

Neill Feather, president of SiteLock, told Bloomberg BNA that although JAR provides ''strong summary'' of the alleged cyberattacks, ''readers of the report should understand that an indicator of compromise on their network should not be immediately construed as a targeted state-sponsored attack.'' According to Tran, ''using the JAR alone would not guarantee 100 percent attribution of compromise without additional technical indicators and signatures for further forensic investigation.''

Feather said that ''while the Russians are highlighted in the Joint Analysis Report, cybercriminals, especially those with nation state resources, are notorious for their ability to disguise themselves while executing an attack—this makes it nearly impossible to pinpoint their true identity and origin.''

However, a DHS official told Bloomberg BNA on background that ''it's particularly necessary to emphasize that the Russians hide in the noise.'' Russians ''often use internet protocol addresses that are legitimate addresses that are legitimate machines generating legitimate inbound and outbound traffic connections.'' Therefore, the official said, ''simply because the IPs are in the logs does not mean there has been malicious activity'' but it is ''cause for a further look to determine if malware, for example, may be resident.''

According to the DHS official, ''we know the Russians are a highly capable adversary who conduct technical operations in a manner intended to blend into legitimate traffic.''

By Jimmy H. Koo

To contact the reporter on this story: Jimmy H. Koo in Washington at jkoo@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com

 ISSN 0000-0000