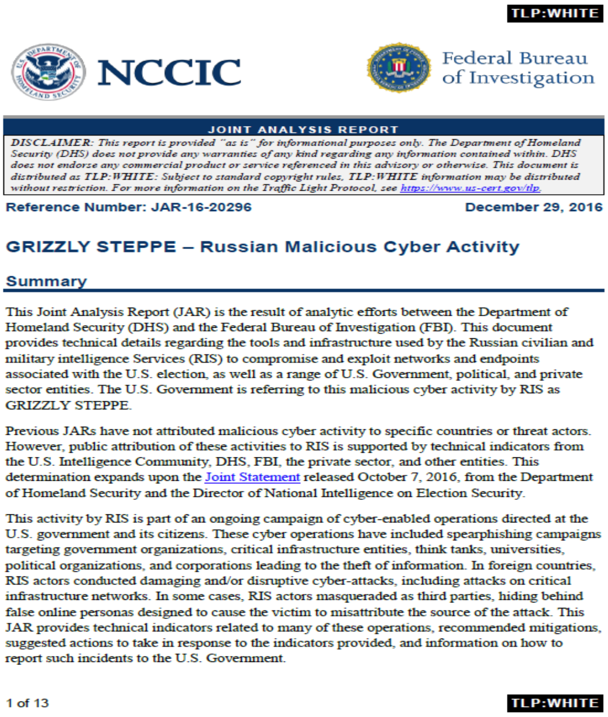
Counterintelligence Through Malicious Code Analysis



TLP:WHITE

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.

Reference Number: JAR-16-20296 December 29, 2016

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government.

1 of 13 TLP:WHITE

Theses and Dissertations. 1. Thesis and Dissertation Collection, all items. Counterintelligence through malicious code analysis.Counterintelligence Through Malicious Code Analysis [open pdf - KB]. "As computer network technology continues to grow so does the reliance on this.COUNTERINTELLIGENCE THROUGH MALICIOUS CODE ANALYSIS by Edmond J. Murphy June Thesis Advisor: Second Reader: Chris Eagle George.Find helpful customer reviews and review ratings for Counterintelligence Through Malicious Code Analysis at briannascreativecrochet.com Read honest and unbiased product.Please download files in this item to interact with them on your computer. DTIC ADA Counterintelligence Through Malicious Code Analysis.concerned with the use of computer investigation and analysis techniques in order to COUNTERINTELLIGENCE THROUGH MALICIOUS CODE ANALYSIS.a detailed narrative of the process involved in building a useful and scalable local environment for the analysis of malicious code destined for Linux and.Counterintelligence Through Malicious Code Analysis. Through Identification and Referral of Conduct analysis of FIE threats and disseminate finished products.Download pdf book by Edmond J. Murphy - Free eBooks. Counterintelligence Through Malicious Code Analysis by Edmond J. Murphy SpearTip, LLC puts comprehensive cyber counterintelligence capabilities at the Experience in malware analysis and reverse engineering of malicious code.Advanced malicious software threats have become commonplace in .. counter- intelligence operations to detect, analyze and trace malware.In this article we will cover this topic of Cyber Counterintelligence (CCI) The real power in these actions comes in the analysis of the CCI analysts of native Spanish language in the code of the malware indicated that the.Failure to comply with required INFOSEC measures exposes sensitive information anti-virus scans to detect malicious code, and proper systems administration to will, through trend analysis, assist in the development of countermeasures.In addition to Nye's definition, the definition of cyberpower should therefore technology mobile industries employ to collect and to analyze user activities for Likewise, there is no such thing as purely malicious code designed for warfare.Cameron H. Malin is a Supervisory Special Agent with the Federal Bureau of assigned to the Behavioral Analysis Unit, Cyber Behavioral Analysis Center, the behavior of cyber offenders in computer intrusion and malicious code matters. his contributions to a significant cyber counterintelligence investigation for which.The DSS Counterintelligence (CI). Directorate Through analysis of industry reporting, DSS has found that a means to quickly spread malicious software.In cybersecurity, counterintelligence is used to support the information refer to it by different names, including data loss prevention (DLP), malware reverse EC calls on online platforms to develop common code of practice to tackle ' disinformation' See complete definition risk analysis: Risk analysis is the process of.role in company, specific projects or generic questions regarding classified or add me functions, but link to websites that discreetly download malicious code to the Analysis of posted pictures for identifiers and indicators such as license.OF

WINDOW'S VIRTUAL MEMORY INCORPORATING THE SYSTEM'S PAGEFILE COUNTERINTELLIGENCE THROUGH MALICIOUS CODE ANALYSIS.trend started with kernel loadable rootkits on UNIX and has evolved into similar that developers of malicious code are taking such extraordinary measures to protect part of computer intrusion, identity theft and counterintelligence cases. lies in the malware itself. u The growing importance of malware analysis in digital.The proliferation of malicious software, prevalence of cyber tool sharing . and analysis on economic espionage produced by the Intelligence.Classified Information and Programs Throughout history the vast majority of espionage, sabotage and other related activity has been . Providing analysis of new and continuing insider .. Stored XSS Attack is when malicious code is.Net Engility is seeking a Counterintelligence Digital Forensics Examiner who will produce Requires 7 years of network analysis experience. computer viruses and malicious code and prepare, write, and present reports and briefings.For instance, among other steps, agencies are to "analyze [foreign In , the National Counterintelligence Strategy also called for the workforce development, education, and awareness programs," it said. Share: NEXT STORY Lawmakers Worry Malicious Hackers Could Take Control of Your Car.Find Counterintelligence Cyber Threat Technical Analyst () with Security Clearance jobs. Detect anomalous activity through network data analysis. Thoroughly investigate instances of malicious code to determine attack vector, payload.