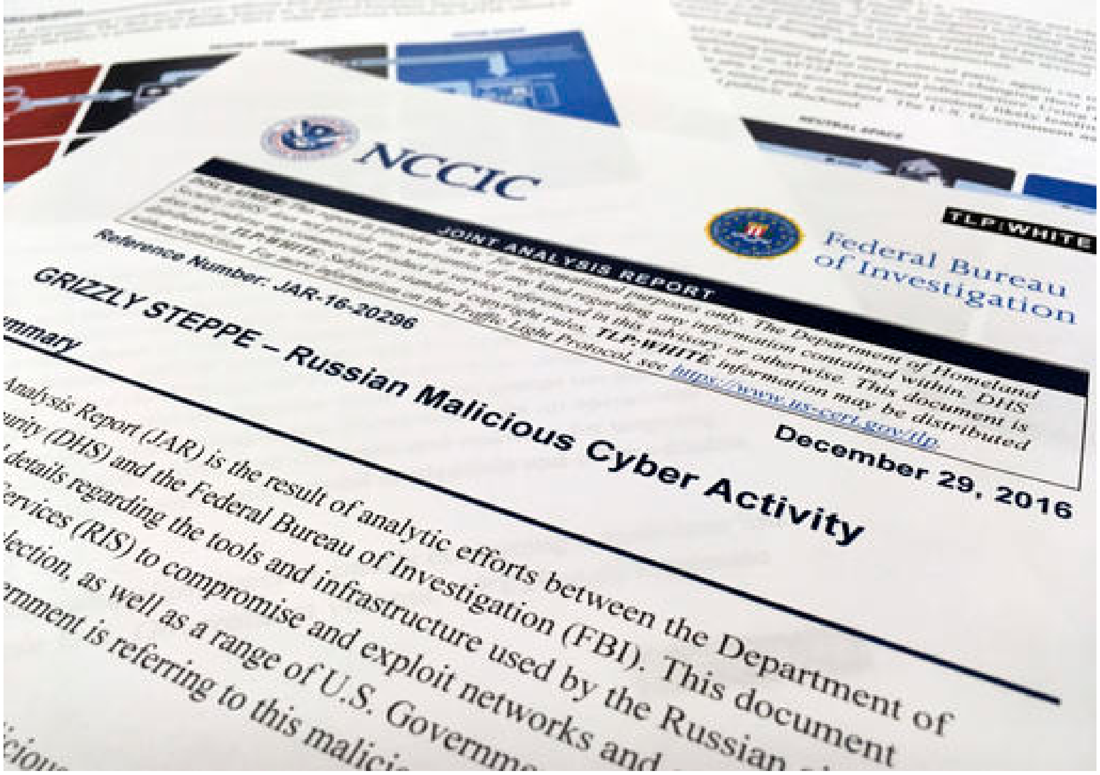
PHYS.ORG

Cyber experts report 'chasing ghosts' after US warning

January 6 2017, by Tami Abdollah



NCCIC

Federal Bureau of Investigation

TLP:WHITE

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

mmary

Analysis Report (JAR) is the result of analytic efforts between the Department of
urity (DHS) and the Federal Bureau of Investigation (FBI). This document
details regarding the tools and infrastructure used by the Russian
ervices (RIS) to compromise and exploit networks and
lection, as well as a range of U.S. Governme
rnment is referring to this malici
iciou

The first page of the Joint Analysis Report narrative by the Department of Homeland Security and federal Bureau of Investigation and released on Dec. 29, 2016, is photographed in Washington, Jan. 6, 2017. Computer security specialists say the technical details in the narrative that the U.S. said would show whether computers had been infiltrated by Russian intelligence services were poorly done and potentially dangerous. Cybersecurity firms ended up counseling their customers to proceed with extreme caution after a slew of false positives led back to sites such as Amazon and Yahoo Inc. Companies and organizations were following the government's advice Dec. 29 and comparing digital logs recording incoming network traffic to their computers and finding matches to a list of hundreds of internet addresses the Homeland Security Department had identified as indicators of malicious Russian intelligence services cyber activity. (AP Photo/Jon Elswick)

After the U.S. government disclosed its first technical report publicly connecting Russia's intelligence services to U.S. hacking, the phones started ringing inside cybersecurity firm Rendition Infosec LLC.

Worried customers were following the government's advice, issued Dec. 29, and comparing digital logs recording incoming network traffic to their computers and finding matches to a list of hundreds of internet addresses the Homeland Security Department had identified as indicators of malicious Russian intelligence services cyber activity.

"They thought they were compromised," said Rendition founder, Jake Williams, who described a "frenzy" of computer security specialists scrubbing their systems for signs of the Russians. The firm sent a cautionary note to businesses telling them, "be very, very careful on applying this," and encouraging them to look for further evidence before raising alarms.

The incident illustrated the difficulties and dangers of imprecise government warnings on cybersecurity, especially when national security concerns are at play and sensitive details may compromise information sources. Alerts that are too vague aren't meaningful. Alerts with details but lacking context might generate false positives, unnecessarily costing businesses and spreading panic among internet users—or worse, damaging the credibility of the government about its future warnings.

A Homeland Security Department official, speaking on condition of anonymity, defended the recent warnings. The official acknowledged the listed addresses included legitimate activity but said businesses were advised to investigate further traffic from those addresses because the Russians are sophisticated adversaries who hide their activities among ordinary internet traffic.

Robert M. Lee, CEO of the Maryland-based industrial security firm Dragos Inc., warned his customers, who span critical infrastructure including water, electric, manufacturing and petro-chemical sites, that the technical information was bad. About one dozen called with concerns.

"Every single company we have as a customer who ran the indicators got alerts, and all the alerts were bad," Lee said. "These addresses were not only not descriptive of Russian activity, they were not descriptive of malicious activity. They were actually common sites."

The Associated Press found that nearly one quarter of the internet addresses identified by the Obama administration as potentially tied to Russian activity had traced back to computer servers that help users browse the internet anonymously. That service, called Tor, was initially funded by the U.S. government and is now used prominently by activists and journalists working in hostile countries who need to keep their identities a secret.

Other internet addresses released by the Homeland Security Department traced to servers at American universities and email provider Yahoo Inc. The government cautioned that the addresses weren't automatically tied to Russian malicious activity, but instead were indicators that computer security experts should investigate further.

One of the businesses that called Williams reported that an address tracked to Microsoft's telemetry server, which sends data to Microsoft when an application crashes. That conversation with his client spun into an hour-long discussion of "can we trust this report at all?" Williams said. "My short answer on this is no."

He added: "This has a real cost to business. I suspect for a lot of them there (was) a lot of money spent chasing ghosts."

Citation: Cyber experts report 'chasing ghosts' after US warning (2017, January 6) retrieved 13 May 2024 from https://phys.org/news/2017-01-cyber-experts-ghosts.html