FLASH CP 000111 MW Downgraded Version

TLP: WHITE
TLP: WHITE
25 March 2020
Alert Number
CP-000111-MW
WE NEED YOUR
HELP!
If you identify any
suspicious activity
within your
enterprise or have
related information,
please contact
FBI CYWATCH
immediately with
respect to the
procedures outlined
in the Reporting
Notice section of
this message.
Email:
cywatch@fbi.gov
Phone:
1-855-292-3937
*Note: This information is
being provided by the FBI to
assist cyber security
specialists protect against
the persistent malicious
actions of cyber criminals.
The information is provided
without any guaranty or
warranty and is for use at
the sole discretion of the
recipients.
The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to

protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: WHITE : The information in this product may be distributed without restriction, subject to copyright controls.

Kwampirs Malware Indicators of Compromise

Employed in Ongoing Cyber Supply Chain Campaign

Targeting Global Industries

Summary:

This is a re-release of FBI FLASH message (CP-000111-MW) previously disseminated on 06 January 2020. Since at least 2016, an ongoing campaign using the Kwampirs Remote Access Trojan (RAT) targeted several global industries, including the software supply chain, healthcare, energy, and financial sectors. The FBI assesses software supply chain companies are a key interest and target of the Kwampirs campaign. This campaign is a two-phased approach. The first phase establishes a broad and persistent presence on the targeted network, to include delivery and execution of secondary malware payload(s). The second phase includes the delivery of additional Kwampirs components or malicious payload(s) to further exploit the infected victim host(s).

Technical Details:

Propagation, Persistence, Backdoor (Module 1):

Upon successful infection, the Kwampirs RAT propagates laterally across the targeted network via SMB port 445, using hidden admin shares such as ADMIN$ and C$. The malware maintains persistence on the infected Windows host by dropping a binary to the hard drive and creating a malicious Windows system service set to auto start upon reboot. The new malicious service scans and catalogs the host configuration, encrypts the data, and transmits it to an external Command and Control (C2) server via an HTTP GET request on port 80.
