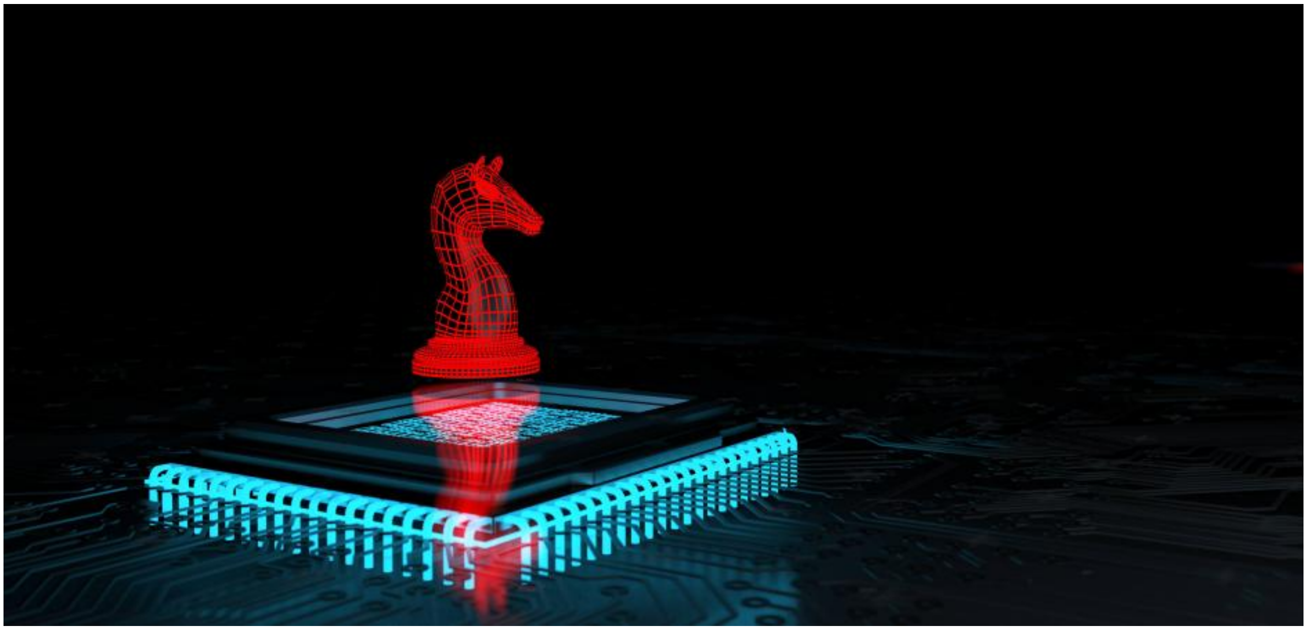
Vjw0rm Is Back With New Tactics

appriver.com/resources/blog/november-2020/vjw0rm-back-new-tactics

Blog

Blog

Chris Lee



Vengeance Justice Worm (Vjw0rm) first emerged in November 2016; it's a hybrid worm/Remote Access Trojan (RAT) that is publicly available and has modular functionality. In January 2019 our team wrote about Vjw0rm here when it was being propagated by a phishing campaign utilizing a banking lure.

Vjw0rm has 3 primary malicious capabilities:

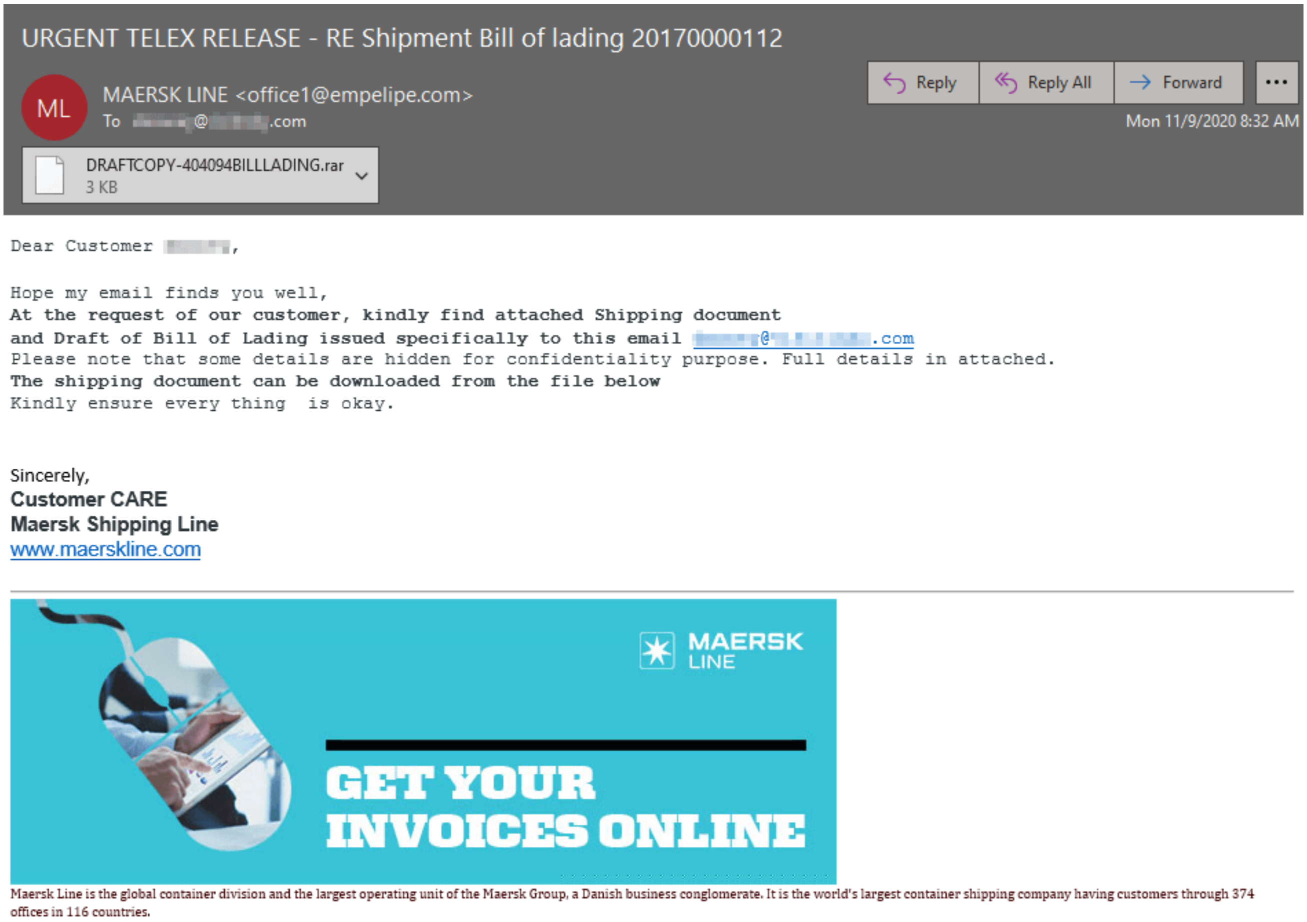
1. Information Stealing - Exfiltrating cookie session data, clipboard strings, and attempts to steal user credentials.

2. Self Propagation - Copies itself throughout the operating system and in the startup folder and can spread via removable drive.

3. Denial of service (DOS) - Domain Name Service (DNS) request manipulation, and the ability to send and receive spam email including advertisement flooding.

This time around we're seeing this malware group using RAR (compressed files created by the WinRAR archiver) files with malicious JS (text file containing javascript code) files embedded. In this campaign the bad actors are spoofing Maersk Shipping Line - A Danish international container shipping company and the largest operating subsidiary of the Maersk Group. Maersk is commonly spoofed because of its wide reach of customers and prevalence in the shipping industry. The lure being used in today's is a shipment bill of lading

Vjw0rm Sample



URGENT TELEX RELEASE - RE Shipment Bill of lading 20170000112

ML MAERSK LINE <office1@empelipe.com>
To [redacted]@[redacted].com

Mon 11/9/2020 8:32 AM

DRAFTCOPY-404094BILLLADING.rar
3 KB

Dear Customer [redacted],

Hope my email finds you well,
At the request of our customer, kindly find attached Shipping document
and Draft of Bill of Lading issued specifically to this email [redacted]@[redacted].com
Please note that some details are hidden for confidentiality purpose. Full details in attached.
The shipping document can be downloaded from the file below
Kindly ensure every thing is okay.

Sincerely,
Customer CARE
Maersk Shipping Line
www.maerskline.com

Maersk Line is the global container division and the largest operating unit of the Maersk Group, a Danish business conglomerate. It is the world's largest container shipping company having customers through 374 offices in 116 countries.

Mitigation Tactics

1. If your organization doesn't regularly receive legitimate RAR files then we suggest banning that file extension globally.

2. User education has never been more important, malicious actors are constantly innovating and pivoting, users need to be on their game and know what to look for and what not to click on. Establish an easy process in your company where users can submit anything suspicious to your IT/Helpdesk team for review.

3. Defense in depth is something that your company should constantly strive for. A great start would be by signing up for our Advanced Email Security!

Indicators Of Compromise

dhanaolaipallets[.]com

79.134.225.11 (Switzerland IP)

SHA256 Hashes

RAR: 4c5550b9ae08885f1b5f1761fdd40722dda2b04a7e432e1649ae3e080d88b4b0

JS: 70c0b9d1c88f082bad6ae01fef653da6266d0693b24e08dcb04156a629dd6f81

Contact us today for a free trial of our Email Threat Protection