Sputnik House Post-Incident Report

|  |  |
| --- | --- |
| Date of investigation | Today |
| Date of incident | 2018-08-12 |
| Outcome | True Positive – Found infection in email |
| Action taken | Determined host, identified infected email attachment, and advised reformatting infected machine |
| Reporting took | Alerts and traffic in the pcap using Wireshark, Snort and Suratica |
| Attack vector | Email attachment |
| Source IP/email | 149.129.222.112 |
| Source port | 80 |
| Destination IP/email | 185.68.93.18 |
| Destination port | 80 |

Narrative

Both alert files show there was an executable from 149.129.222.112 on the 11th of August in 2018 at around 05:21. The first two HTTP requests for "1.rar" and "1.zip" do not return any RAR or ZIP archives. The last HTTP request returns a 200 OK with content labeled as "application/octet-stream." If you follow the TCP stream for the last HTTP request for "a3.dat," you'll find an executable file.

A screenshot of a cell phone

Description automatically generated

The HTTP request in the middle returns a 200 OK with it labeled as “application/zip.” When looking at the TCP stream for that request, there is an executable file.

A screenshot of a social media post

Description automatically generated

After exporting the file, the file hash can be searched on VirusTotal. After checking the status, there were multiple instances of HTTP traffic over TCP port 80. This triggered the following alerts in the Suricata alert file:

• ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1

•ETPRO TROJAN Win32/Marap CnC Beacon

A screenshot of a computer

Description automatically generated

According to these alerts, the machine is infected and the infection is contained within the email attachment. After looking at the first email, it contains a picture attachment. When you view the contents on a text editor, it shows a URL which most likely started the infection.