Afeefah Manzoor

ITN 216

Hands on 2X2

* Date, start time, and end time of the malicious activity in UTC (GMT).

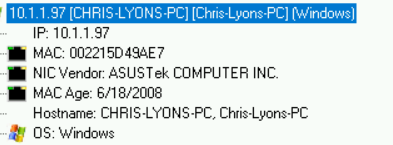




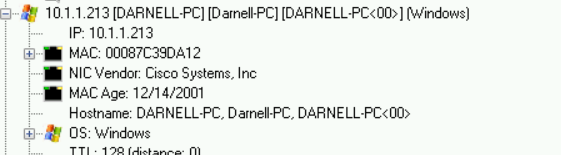
Start: 2017-12-14 at 11:01pm

End: 2017-12-15 at 12:50pm

* IP address of the Windows host from in the pcap.

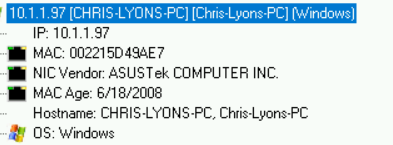


10.1.1.97

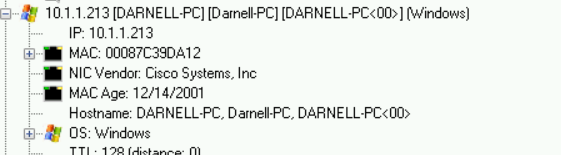


10.1.1.213

* Mac address of the Windows host in the pcap.

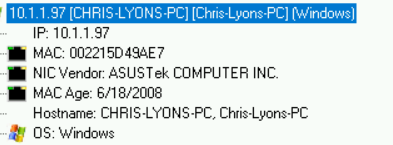


002215d49ae7

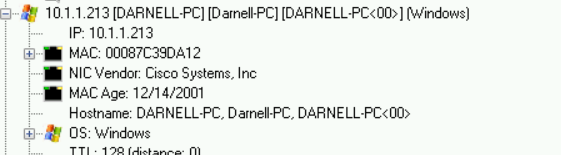


00087c39da12

* Host name for the Windows host in the pcap.



Chris-Lyons-pc



Darnell-pc

* What type(s) of malicious activity were noted.

Spoofing attempted, long host entry exploit attempted, ET trojan detected

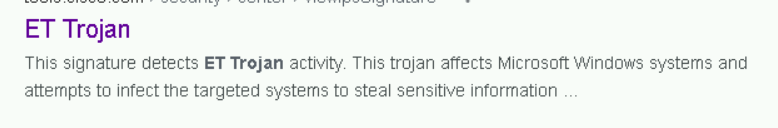
* Indicators of the malicious activity (IP addresses, domain names, file hashes, etc).

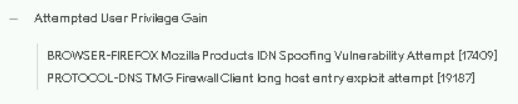
MAC address of Darnell-pc is the same mac addresses of the websites that had an ET trojan detected on them.

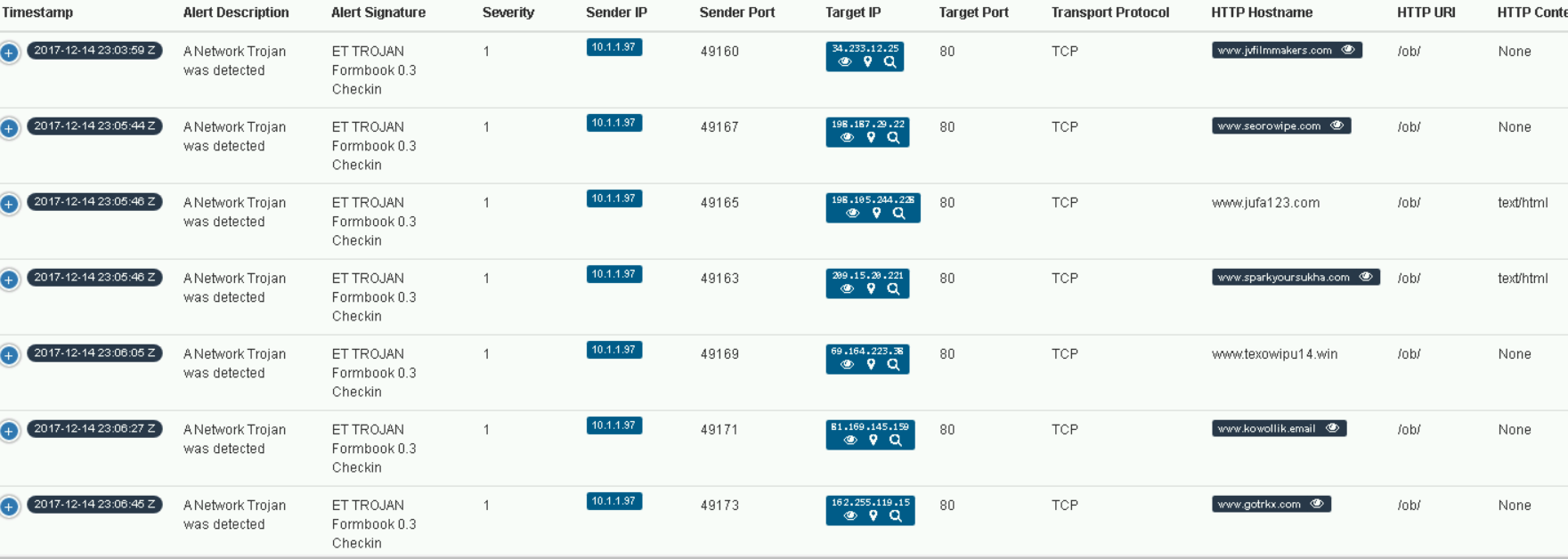
* A summary of what happened.

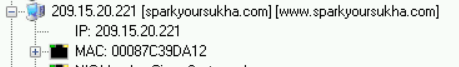
I believe that Darnell-pc was hacked through the email that was sent and contained a image that contained an image was spoofing webisites. Chris-lyons-pc seemed to be hacked by a trojan that was contained in an invoice. The invoice contained a trojan spy.









has the same mac as Darnell-pc



