XOR Key: KNcUKKaX

Malware Family Name: Trojan.Glupteba

Timeline:

Packet #1148 (23:33:39.356557): Barto-PC first accesses compromised website (wolfgangssteakhouse.co.kr)

Packet #1837 (23:33:44.978479): Barto-PC is redirected from (wolfgangssteakhouse.co.kr) to gate (bnureb0up683ppcbgt1fz9g.isbul.info)

Packet #2104 (23:33:45.849418): Barto-PC (from bnureb0up683ppcbgt1fz9g.isbul.info) is sent to (http://zz1lb82z00y16gdow25fcxm.ilaclama.us/watch.php?fuhgi=MTIyMDU5ODkwNjhkMTQ5ODNkNDI2YWEzNWJjYjNjNTJ)

Packet #2521 (23:33:48.225258): Barto-PC redirected (from zz1lb82z00y16gdow25fcxm.ilaclama.us) to EK landing page (http://f9wb0396aobdotyzddcwdtf.ilaclama.us/VQlXBEpVSwQ.html)

Packet #2561 (23:33:49.033657): Barto-PC accesses EK landing page (VQlXBEpVSwQ.html)

^Hash for EK landing page:
d9f266eb1dbd2bca408c837c3c4eaa39135417649ace63ba20d58c2df88ea19f

Packet #2617 (23:33:54.669953): Nuclear EK sends an SWF exploit to Barto-PC; SWF denotes an Adobe Flash File format that the EK is attempting to exploit

^Hash for EK Flash exploit:
c4b1c55a90877d0618c2dc8bad01b33f1d60f3613b3673bdb08465569bdb8236

Packet #2634 (23:33:56.058965): Nuclear EK sends SilverLight exploit to Barto-PC; SilverLight is a Microsoft framework application that is now available as a plug-in, which the EK is attempting to exploit

^Hash for EK Silverlight exploit:
b4cb839573156364fc2a10a2d0a57cced697f076ce9fe4aa3604ada0b7a77523

Packet #2658 (23:33:57.418697): Nuclear EK delivers Payload to Barto-PC

^Hash for EK payload:
9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d

Packet #2798 (23:34:01.876444): Nuclear EK delivers second Payload to Barto-PC

^Hash for EK payload:
9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d

Resources:

https://www.garykessler.net/library/file_sigs.html

https://isc.sans.edu/diary/Nuclear+EK+traffic+patterns+in+August+2015/20001

https://www.malware-traffic-analysis.net/2014/12/10/index.html

https://resources.infosecinstitute.com/topic/network-traffic-analysis-for-ir-content-deobfuscation/

https://www.malwarebytes.com/blog/detections/trojan-glupteba

https://unit42.paloaltonetworks.com/unit42-understanding-angler-exploit-kit-part-1-exploit-kit-fundamentals/