Gamaredon

Malware Through Outlook Macros

Indicators of Compromise

June 13, 2020

ATLAS CYBERSECURITY

www.atlas-cybersecurity.com

Indicators of Compromise

- Lure Document SHA-256
  - 86e0701349903105boc346df9485dd59d85dd9463c2bee46d974ea1b1d7059d4
- Remote Template (pos.dot) SHA-256
  - feb0596e9735e03ae929d9b5ee862da19e16e5cdf57dd2a795205e591a5594of
- Remote Template from Lure Document Domain
  - document-out[.]hopto[.]org/pos[.]dot
- Remote Template Hosting IP
  - 141[.]8[.]195[.]60
- Remote Template Hosting IP
  - 141[.]8[.]192[.]153

Indicators of Compromise Cont.

- System Information Upload IP
  - 188[.]225[.]25[.]50
- System Information Upload URI
  - libcrash.ddns[.]net/{Computername_SerialNumber}//posolreboot.php
- ExcelMyMacros.vba SHA-256
  - c4089686965df5e52105b6eac06703aa11c4891695278446370f623d531b505e
- wordMacros.vba SHA-256
  - 02e6e2bfaaf6e77cfaccadaf26167135c53cf2c934d17c5a83e5bbcadd85b47d

Indicators of Compromise Cont.

- ExcelMyMacros.txt SHA-256
  - 2f310c5b16620d9f6e5d93db52607f21040b4829aa6110e22ac55fab659e9fa1
- Pteranodon SHA-256
  - c1524a4573bc6acbe59e559c2596975c657ae6bbc0b64f943fffca663b98a95f
- Pteranodon SHA-256
  - 145a61a14ec6d32b105a6279cd943317b41f1d27f21ac64df61bcdd464868edd
- Pteranodon Domains
  - beercraft[.]space
  - skymage[.]fun
  - masseffect[.]space
  - masseffect[.]website
- Pteranodon IPs
  - 185[.]200[.]241[.]88
  - 188[.]225[.]46[.]94