Severity

High

Analysis Summary

Gamaredon is a Russia-backed advanced persistent threat (APT) that has been operating since at least 2013. The main goal of this APT is to use the malicious document to gain control of the target machine. The exploit document uses the template injection technique to infect the victim's computer with further malware. When the document is opened, it connects to the hacker's server and downloads the payload file. Gamaredon's tools are simple and designed to collect sensitive information from hacked systems and propagate it further. Its information-gathering efforts are nearly comparable to those of a second-tier APT, whose primary purpose is to collect and disseminate information with their units.

Impact

- Template Injection
- Exposure of Sensitive Data

Indicators of Compromise

URL

- http[:]//194[.]67[.]104[.]123/put[.]php
- http[:]//80[.]78[.]253[.]247/put[.]php
- http[:]//194[.]67[.]108[.]228/put[.]php
- http[:]//194[.]67[.]105[.]103/crab/crevice[.]elg
- http[:]//5[.]63[.]157[.]11/put[.]php
- http[:]//194[.]67[.]104[.]123/get[.]php
- http[:]//5[.]63[.]157[.]11/get[.]php
- http[:]//80[.]78[.]253[.]31/put[.]php
- http[:]//89[.]108[.]64[.]198/put[.]php
- http[:]//89[.]108[.]76[.]215/deserter[.]mdl?id=4266
- http[:]//193[.]124[.]206[.]208/deserter[.]mdl?id=4266
- http[:]//185[.]189[.]69[.]224/deserter[.]mdl?id=4266
- http[:]//194[.]58[.]102[.]70/crab/crevice[.]elg
- http[:]//80[.]78[.]245[.]226/deserter[.]mdl?id=4266
- http[:]//194[.]58[.]104[.]206/deserter[.]mdl?id=4266
- http[:]//31[.]31[.]203[.]61/deserter[.]mdl?id=4266
- http[:]//194[.]58[.]100[.]91/crab/crevice[.]elg
- http[:]//80[.]78[.]254[.]253/deserter[.]mdl?id=4266
- http[:]//176[.]99[.]11[.]252/crab/crevice[.]elg
- http[:]//151[.]248[.]116[.]181/deserter[.]mdl?id=4266
- http[:]//89[.]108[.]70[.]90/deserter[.]mdl?id=4266
- http[:]//80[.]78[.]245[.]226/index[.]php?den=0
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=0
- http[:]//194[.]58[.]104[.]206/depended[.]jas?deluge=4526
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=0
- http[:]//194[.]58[.]104[.]206/crawford/crept[.]db
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=5
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=0
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=0
- http[:]//80[.]78[.]245[.]226/index[.]php?den=0
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=0

- http[:]//80[.]78[.]245[.]226/index[.]php?den=0
- http[:]//193[.]124[.]206[.]208/crawford/crept[.]db
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=0
- http[:]//80[.]78[.]245[.]226/index[.]php?den=0
- http[:]//80[.]78[.]245[.]226/index[.]php?declare=0
- http[:]//194[.]58[.]104[.]206/deluge[.]arc?defiance=3237
- http[:]//194[.]67[.]105[.]103/correct/copyright/court[.]tmp
- http[:]//89[.]108[.]70[.]90/credit/cranny[.]au
- http[:]//89[.]108[.]70[.]90/correct/copyright/court[.]tmp
- http[:]//31[.]31[.]203[.]61/crept/crumb[.]arc
- http[:]//176[.]99[.]11[.]62/frustration[.]3gpp2
- http[:]//185[.]20[.]227[.]235/frustration[.]3gpp2
- http[:]//194[.]180[.]174[.]28/judge[.]wav
- http[:]//89[.]108[.]79[.]146/correction/crude[.]mdm
- http[:]//45[.]76[.]169[.]62/jersey[.]icb
- http[:]//185[.]189[.]69[.]173/baseball[.]dbc
- http[:]//94[.]158[.]244[.]100/jersey[.]icb
- http[:]//185[.]189[.]69[.]23/absorb[.]wm10[.]12[.]2021%2012[:]25[:]28
- http[:]//149[.]248[.]60[.]74/jam[.]j2k
- http[:]//151[.]248[.]112[.]232/custom/crept[.]nds
- http[:]//107[.]191[.]57[.]249/jersey[.]icb
- http[:]//185[.]189[.]69[.]162/jersey[.]icb
- http[:]//194[.]180[.]174[.]198/jug[.]fft
- http[:]//94[.]158[.]244[.]64/barren[.]cbt09[.]12[.]2021%209[:]50[:]19
- http[:]//167[.]179[.]93[.]98/jolly[.]n64
- http[:]//5[.]252[.]178[.]120/barren[.]cbt10[.]12[.]2021%2010[:]13[:]35
- http[:]//194[.]67[.]92[.]215/correction/crude[.]mdm
- http[:]//89[.]108[.]102[.]58/custom/crept[.]nds
- http[:]//151[.]248[.]125[.]115/custom/crept[.]nds
- http[:]//194[.]180[.]174[.]31/judge[.]wav
- http[:]//89[.]108[.]78[.]229/custom/crept[.]nds
- http[:]//194[.]180[.]174[.]198/jersey[.]icb
- http[:]//185[.]46[.]10[.]69/correction/crude[.]mdm
- http[:]//94[.]158[.]245[.]165/fruitless[.]ive15[.]12[.]2021%2017[:]23[:]29
- http[:]//151[.]248[.]125[.]115/correction/crude[.]mdm
- http[:]//134[.]0[.]115[.]88/correction/crude[.]mdm
- http[:]//5[.]252[.]178[.]145/bark[.]act14[.]12[.]2021%2010[:]58[:]34
- http[:]//37[.]140[.]197[.]165/custom/crept[.]nds
- http[:]//194[.]180[.]174[.]28/jersey[.]icb
- http[:]//185[.]189[.]69[.]174/absorb[.]flv
- http[:]//70[.]34[.]217[.]0/disposed[.]lp
- http[:]//37[.]140[.]197[.]251/custom/crept[.]nds
- http[:]//144[.]202[.]91[.]27/baseball[.]dbc
- http[:]//89[.]108[.]98[.]79/crimson/crystal[.]bnk
- http[:]//185[.]189[.]69[.]174/baseball[.]dbc
- http[:]//89[.]108[.]78[.]90/credit/cranny[.]au
- http[:]//89[.]108[.]98[.]88/credit/cranny[.]au
- http[:]//5[.]252[.]178[.]115/absorb[.]flv
- http[:]//89[.]108[.]81[.]75/credit/cranny[.]au
- http[:]//89[.]108[.]81[.]181/crimson/crystal[.]bnk
- http[:]//80[.]78[.]241[.]15/credit/cranny[.]au
- http[:]//185[.]46[.]10[.]25/credit/cranny[.]au
- http[:]//194[.]67[.]105[.]103/credit/cranny[.]au

- http[:]//139[.]180[.]180[.]120/credit/cranny[.]au
- http[:]//80[.]78[.]241[.]15/correct/copyright/court[.]tmp
- http[:]//194[.]67[.]109[.]18/correct/copyright/court[.]tmp

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.