EGCERT
Egyptian Computer
Emergency Readiness Team

Gatak - Stealthy Actor Harvesting Data

Introduction

Gatak (also known as Stegoloader and GOLD) is a threat actor involves in data theft through watering hole attacks. According to kaspersky, there have been thousands of victims worldwide during 2017.Watering hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected. The malware used in these attacks typically collects information on the user. The name is derived from predators in the natural world, which wait for an opportunity to attack their prey near watering holes.

Once Gatak gets into a corporate network, it usually succeeds at staying under the radar for a long time, harvesting all types of data. In some of the occasions when it was discovered, Gatak is known to drop old ransomware samples in possible false flag operations, according to Symantec.

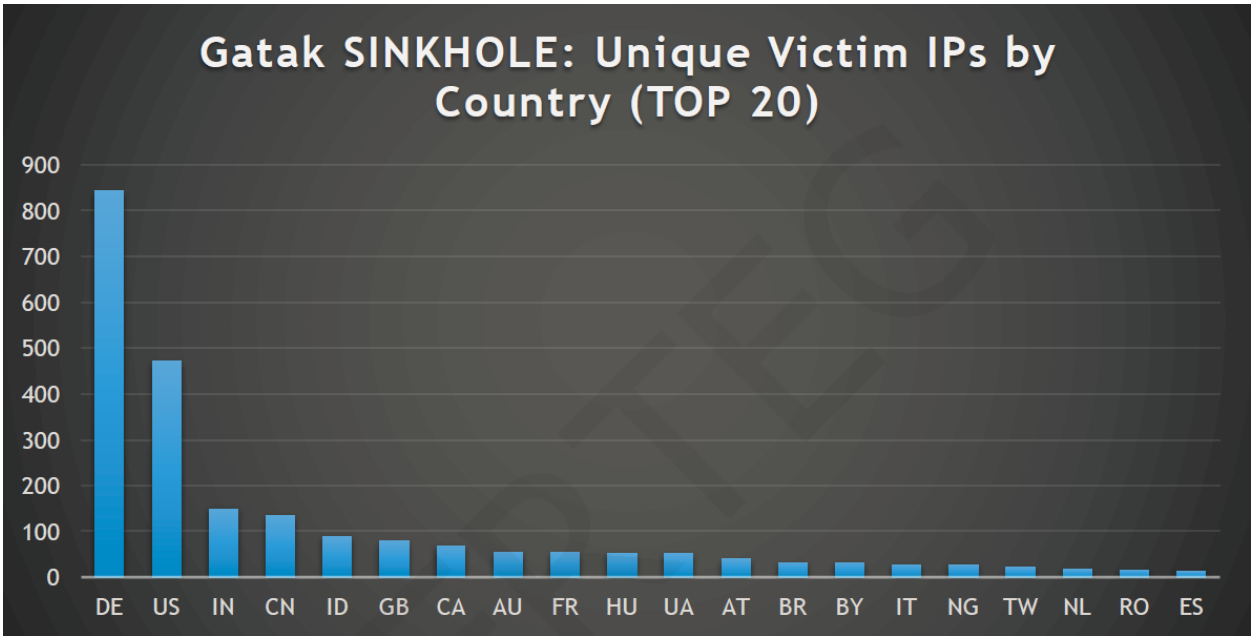
During breaches, Gatak relies on a chain of payloads which correspond to several stages of attack. The payloads dropped by the Gatak group have been previously documented in 2015 and 2016. However, the group is still quite active in 2017 and, according to Kaspersky's statistics, continues to successfully compromise more and more victims. Many of the technical findings presented in the two previously mentioned papers are still valid for the newer versions of Gatak.

Distribution

The analyzed malware samples were bundled with software cracking and key generator tools.
They are distributed on a number of websites (including keyfound[.]us, keygenia[.]org or keygen.
co[.]uk), with the download links generally pointing to an actor controlled "hosting service" named "cloud-host[.]org".

Victims

Between March and December 2017, Kaspersky sinkhole servers received connections from 2572 victims across 65 countries.



Indicators of compromise

Stage 0 hashes

0AE26BA127904EC354F228B316F044A1
0B20B941D2B9372D875410FFEB53C473
166390F58CE9FAB540B23BE309DF4734
1B2E083D3A2C289F242A341B37B7AC76
20B5416FCAA6A644001A89C2F7F095DE
239317A3CCF8654F99B7EB565FF32039
39F6C833CAD0BCEC22E7EFEB90A4BD31
3C7C5D9841810DF49BFD57F98F22BA33
49CC7C51069F3432E56FB2E7E493310D
4AAEA9082910D1E8CE87DE443DCD628E
5AB9EC32B082D879B58740038824EAF5
649466171704540698A5D2E7B3E256EE
6887EC36903D67F73E0557D0959985D8
822DEFE73F6653001DF5272F1A18E9ED
8EF00C2BF607B3C704D0B69A806836EC
923BB7334B6F86B75B9A855DD6F27A21
94EF18510594369D8F91D766C87B7919
96571A9E7A20929384A35465416B123F
9823C41111E810F65C4192499EE5DA29
AA11786F159EA0EBD424483E5582D7CF

AF44041CF28898CE2DB3798B8C2E2411
B80BC6CAB417C8725BB691FC03356C2A
B9CB949FEB5F376C3117DFBB4FE7C8DA
B9F8B5EC5AB4F10C26ACC82180867226
BA875A8E8F0C0F51C3DF69DA66BF2248
BDD03649495A9BD9377E85B16D2E968C
BE749AA22357887710BAF48EFC7F6861
C4ED47F3210E2C50BDEBFC4C004CF35A
CB3B17BCB656314EFE56CC51E8EDB1EE
CCCF6BAD519A23E122262F83C1E72CDC
D03D7655B53EF534577FA6293A636630
D0461537511A001D4B0C526E718D9EFC
D3212CEF40026AB40ABA8DF25CDED0BC
DB434789B4A4122B81475A0DE8578691
E49E7DC3861AD7A7A246DA68345E60DE
F1366F18BEEAC06B56DB4100D494DBDD
FE4C9C9D4C3BE6E6509527F0420F9087
FFDE4C03F625C12BA96393F8768EB45F

Previous hashes
061fbe0cc8d85a8ac16f0cf0343cc5b8
6c241c8894a9945255daa8b4629b5a29
895EE1CC4E6BC79EC692499BC847849F
56242B633C852D12E8F0B44DF0D1D2F3
F0E59155643B02908C317CCCFF5315B8
C360DDB916C8B80475F983D77E41072C
4E81A84ACDCEC24B67D467FD4CE41AD5
d0bb2c24d136d3180f4386f957b6632f (DAEMON_Tools_Pro_Advanced_5_5_0_0388_keygen.exe)
5f671ec819a7cdf6d9300f03abd83223

Domains and IPs
unspoiltportugal.co[.]uk
vmx13321.hosting24.com[.]au
jpnc.co[.]kr
176.53.22[.]206
185.120.77[.]109
178.33.188[.]140
parent.entretienparent[.]ca
flake.snowflakeproductions[.]com
85.234.158[.]245
cam.jeremyjiao[.]org
ww.westwoodelementarycowboys[.]com
23.254.204[.]174
sel.therebootstore[.]com
91.209.77[.]45
inf.carvajal[.]info
91.207.8[.]198
87.117.255[.]171

5.135.233[.]16
bog.judaicabyjosh[.]com
famous.famoustattoos[.]net
inc.kevinmilligangallery[.]com
pisc.piscine-love[.]fr
popa.morgatory[.]com
valter.crabdance[.]com
reader.lifeacademyinc[.]com
mone.neenakahlon[.]com
minitravel.strangled[.]net
img.philippe-benoit[.]com
deid.sharpfans[.]org
cod.chezsimone971[.]com
bpp.bppharma[.]com
igg.niksonic[.]com
veverka.junyks[.]cz
207.36.232[.]49
62.149.166[.]33
190jenasdie[.]com
Transasdkoqw19203[.]com
178.158.115[.]163
dance.2ballerinas.org[.]au
178.211.41[.]252
178.162.182[.]60
188.72.213[.]40
82.80.231[.]51
178.63.114[.]86
178.63.149[.]151
193.169.244[.]64
5.45.179[.]38
50.7.252[.]52
afro.leafdragon.co[.]uk
dcc.entertainingyourself[.]net
han.ribha[.]com
peno.marcorosada[.]com
var.leadsandfeeds.co[.]uk
victor.iglesiacaminonuevo[.]com
wake.sametyuksek[.]com
estel.bruno-meyer[.]fr
rtron.dollarwraps[.]com
aura.breathefreelyblog[.]com
85.234.158[.]245
178.158.115[.]163
87.117.255[.]171
50.7.252[.]52
allkeygens[.]ws
cloud-host[.]org
keyfound[.]us

keygenexpert[.]net
keygenia[.]org
www.allkeygens[.]ws
www.bog.judaicabyjosh[.]com
www.cam.jeremyjiao[.]org
www.deid.sharpfans[.]org
www.estel.bruno-meyer[.]fr
www.igg.niksonic[.]com
www.keyfound[.]us
www.keygenexpert[.]net
www.keygenia[.]org
www.pisc.piscine-love[.]fr
www.popa.morgatory[.]com
www.reader.lifeacademyinc[.]com
www.rtron.dollarwraps[.]com
www.ww.westwoodelementarycowboys[.]com

Command and Control URLs

Stage 0

unspoiltportugal.co[.]uk/report_N_0025_
vmx13321.hosting24.com[.]au/report_N_0036
jpnc.co[.]kr/report_N_0054

Stage 1

176.53.22[.]206:80/safari/confirm?ocr=552927891723
185.120.77[.]109:80/timetable/ballet?bigleti=4200734781
178.33.188[.]140:80/service/related?sector=009637
parent.entretienparent[.]ca:80/service/related?sector=009445
flake.snowflakeproductions[.]com:80/service/related?sector=008643
85.234.158[.]245:80/company/manufacturer?play=86557
cam.jeremyjiao[.]org:80/company/manufacturer?play=36788 SINKHOLED
ww.westwoodelementarycowboys[.]com:80/company/manufacturer?play=67574
23.254.204[.]174:80/index/text?srt=577735781299
sel.therebootstore[.]com:80/index/text?v=909380886394
91.209.77[.]45:80/docs/text?play=874633
inf.carvajal[.]info:80/media/source?num=96494
91.207.8[.]198:80/sound/cat?n=18
87.117.255[.]171/tutor/inst?promo=459087
5.135.233[.]16:80/file/photos?handle=6890077
bog.judaicabyjosh[.]com:80/insight/flourence?banner_id=386514
famous.famoustattoos[.]net:80/booking/read?page=120
inc.kevinmilligangallery[.]com:80/insight/flourence?banner_id=386514
pisc.piscine-love[.]fr:80/sound/cat?n=18 SINKHOLED
popa.morgatory[.]com:80/sound/cat?n=18
valter.crabdance[.]com/tutor/inst?promo=459087 SINKHOLED
reader.lifeacademyinc[.]com:80/encourage/help?pointed=855444
mone.neenakahlon[.]com/calibre/view?present=0987667
minitravel.strangled[.]net/tutor/inst?promo=459087

img.philippe-benoit[.]com/calibre/view?present=0987667
deid.sharpfans[.]org/calibre/view?present=0987667
cod.chezsimone971[.]com:80/encourage/help?pointed=855444
bpp.bppharma[.]com/calibre/view?present=0987667
igg.niksonic[.]com:80/booking/read?page=120 **SINKHOLED**
veverka.junyks[.]cz
207.36.232[.]49
62.149.166[.]33

From OSINT
190jenasdie[.]com
Transasdkoqw19203[.]com (178.158.115[.]163)
dance.2ballerinas.org[.]au (178.211.41[.]252)

Older variants C2s
178.162.182[.]60:443/golfstream
188.72.213[.]40:443/galfstream
82.80.231[.]51:443/galfstream
178.63.114[.]86:443/ikebana/mastered?was=96576598
178.63.149[.]151:443/performed/prod?by=1118766
193.169.244[.]64:443/galfstream
5.45.179[.]38:443/golfstream
50.7.252[.]52:443/galfstream
afro.leafdragon.co[.]uk:443/golfstream
dcc.entertainingyourself[.]net:443/galfstream
han.ribha[.]com:443/golfstream
peno.marcorosada[.]com:443/galfstream
var.leadsandfeeds.co[.]uk:443/golfstream
victor.iglesiacaminonuevo[.]com:443/galfstream
wake.sametyuksek[.]com:443/golfstream
estel.bruno-meyer[.]fr:443/galfstream
peno.marcorosada[.]com:443/performed/prod?by=1118766
rtron.dollarwraps[.]com:443/golfstream

Yara rules

```
rule crime_ZZ_GATAK_fakekeyloggers {
meta:
description = "Rule to detect GATAK fake keyloggers (stage 0)"
author = "Kaspersky Lab"
reference = "https://www.symantec.com/connect/blogs/gatak-healthcareorganizations-
crosshairs"
date = "2017-03-21"
hash = "9b1eba9332b882557d8abc0f0ae8ee752119b62b186fa55b525074a74cbef148"
strings:
$s1 = "edermwerik.pdb" fullword asci
$s9 = "gYbqRbfEoWChLaiJ" fullword ascii wide
$s10 = "eOLSFCCrpmnNCOyf" fullword ascii wide
$s11 = "RdTRVGNkoSeEjibi" fullword ascii wide
$s12 = "cqUgIBXhjpBpitQv" fullword ascii wide
$s13 = "rRzouUXtSLLeCLBH" fullword ascii wide
$s14 = "qrDFzVmkliKzPgxH" fullword ascii wide
$s15 = "eLKIbFSTOuGjgNsZ" fullword ascii wide
$s16 = "nfpqGuJuriTrnSNK" fullword ascii wide
$s18 = "JNxMSbzRNHpbjCUc" fullword ascii wide
$s19 = "fvDaxDySjKlOxhoE" fullword ascii wide
$s20 = "EufleZgouNibARfpp" fullword ascii wide
$s21 = "cqUgIBXhjpBpitQv" fullword ascii wide
$s22 = "drRzouUXtSLLeCLBH" fullword ascii wide
$s23 = "ufleZgouNibARfpp" fullword ascii wide
condition:
(uint16(0) == 0x5a4d and filesize < 1000KB and ( 4 of ($s*) ) )
}
rule crime_ZZ_GATAK_fakekeyloggers_short {
meta:
description = "Rule to detect GATAK fake keyloggers"
author = "Kaspersky Lab"
reference = "https://www.symantec.com/connect/blogs/gatak-healthcareorganizations-
crosshairs"
date = "2017-03-21"
hash = "9b1eba9332b882557d8abc0f0ae8ee752119b62b186fa55b525074a74cbef148"
strings:
$a1 = "rRzouUXtSLLeCLBH" fullword wide
$a2 = "EufleZgouNibARfpp" fullword wide
$a3 = "cqUgIBXhjpBpitQv" fullword wide
$a4 = "qrDFzVmkliKzPgxH" fullword ascii
$a5 = "JNxMSbzRNHpbjCUc" fullword ascii
$a6 = "eLKIbFSTOuGjgNsZ" fullword wide
$a7 = "eOLSFCCrpmnNCOyf" fullword wide
$a8 = "RdTRVGNkoSeEjibi" fullword ascii
$a9 = "nfpqGuJuriTrnSNK" fullword ascii
$a10 = "fvDaxDySjKlOxhoE" fullword ascii
$a11 = "edermwerik.pdb" fullword ascii
condition:
(uint16(0) == 0x5a4d and filesize < 1000KB and ( any of ($a*) ) )
}
```